U N I V E R Z I T E T U B E O G R A D U

Dr ĐURO KUREPA
profesor Univerziteta u Beogradu

VIŠA ALGEBRA

KNJIGA DRUGA

DRUGO IZDANJE, ISPRAVLJENO I DOPUNJENO

ZAVOD ZA IZDAVANJE UDŽBENIKA
SOCIJALISTIČKE REPUBLIKE SRBIJE
B E O G R A D

Ovaj udžbenik, kao stalni univerzitetski udžbenik, odobrila je za upotrebu Komisija za udžbenike Univerziteta u Beogradu svojim rešenjem broj 06-2013/1 od 2. jula 1969. godine

U SPOMEN
MOJIM RODITELJIMA

DRUGI DIO

SADRŽAJ

DRUGI DIO

(poglavlja 23—35)

Dalja izgradnja matričnog računa i nekih drugih dijelova algebre

Poglavlje 25.

Metrika u linearnim prostorima (813—834)

Poglavlje 26.

Linearni operatori (835—874)

Poglavlje 27.

Karakteristični polinom. Svojstvene vrijednosti (875—939)

Poglavlje 28.

Ortonormirane matrice (941—955)

Poglavlje 29.

Rješenja zadane jednadžbe prema zadanoj oblasti brojeva (957—1007)

Poglavlje 30.

Linearno programiranje (1009—1043)

Poglavlje 31.

Numeričko ili približno rješavanje jednadžbi i nejednadžbi (1045—1100)

Poglavlje 32.

Neke algebarske strukture (1101—1227)

Poglavlje 33.

Predstavljanje (reprezentacija) algebarskih struktura (1229—1274)

Poglavlje 34.

Algebra tenzora (1275—1316)

Poglavlje 35.

Historijat algebre (1317—1338)

TREĆI DIO

DALJA IZGRADNJA MATRIČNOG RAČUNA I NEKIH DRUGIH DIJELOVA ALGEBRE

UVOD

Matrice su vrlo *pogodno sredstvo* za rješavanje *linearnih* algebarskih problema i drugih problema u vezi s vektorima. Kao što znamo, one se javljaju specijalno u vezi s linearnim homogenim funkcijama i linearnim transformacijama.

Jedna od glavnih zadaća matrica i računanja s matricama sastoji se u tome da se na *pregledan način srede podaci i rezultati, kao i proces kako se od podataka dolazi do rezultata.*

Matrice s *jednim stupcem* (odnosno s jednim retkom) spadaju među *najjednostavnije; iz njih se sve ostale matrice izgrađuju na jednostavan način.* Matrice s jednim stupcem (retkom) nazvali smo *vektorima.* Specijalno, ukazujemo na *preglednost izražavanja i rada služeći se vektorima.* U tom pogledu treba reći da je neka veličina proglašena *vektorom* u *vezi s njenim vladanjem* prema drugim veličinama stanovite *cjeline, organizacije.* Evo dva primjera.

0.1. Primjer. *Tačke* svake ravnine α (naglašujemo: *tačke*!) zovemo *vektorima* u odnosu na *ovo računanje u ravnini* α: *izabrana je neka osobita tačka* O u ravnini α; za svako $A, B \in \alpha$ neka $A+B$ znači simetričnu sliku od O prema središtu dužine AB. Nadalje, neka za *svaki realni broj* $\dot{R}$ i tačku $A \in \alpha$ produkt $\dot{R}A$, odnosno $A\dot{R}$, znači onu tačku T u ravnini za koju je duž OT veća $\dot{R}$ puta od duži OA; pri tom O treba da bude na duži AT ili izvan nje, već prema tome da li je $\dot{R} \leq 0$ ili $\dot{R} > 0$.

Eto, time ravnina α postaje *vektorskim prostorom,* a njene *tačke* vektorima. Za svaki „*vektor*“ $e_1 \in \alpha$, $e_1 \neq 0$ skup Re_1 svih $e_1 \dot{R}$ je pravulja Oe_1; ako je $e_2 \in \alpha \setminus Re_1$, tada imamo tri vektora e_1, e_2 i O; no vektor O zavisi linearno od e_1, e_2, jer je $0\,e_1 + 0\,e_2 = O$. Za svaki drugi „vektor“ v (tj. za svaku tačku „vektorskog prostora“, tj. ravnine α) imamo potpuno određen rastav $v = e_1 v_1 + e_2 v_2$; tako se pojavljuju »*koordinate* v_1, v_2 *vektora* v *u bazi* $e = (e_1\, e_2)$«. Vektor v u bazi e notira se kao stupac v_1, v_2, tj. $\begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$. Taj se stupac može zvati *mjerna vrijednost* ili *mjera vektora* v u odnosu na bazu e.

Uostalom, $v = [e_1, e_2]\begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$.

Sami osnovni vektori e_1, e_2 imaju mjerne vrijednosti $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Za čitavu bazu $e = e_1, e_2$ imamo tako matricu od ta dva stupca $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ u kojoj su položene, kao stupci, mjera prvog osnovnog vektora e_1 i mjera drugog osnovnog vektora e_2; matrica se može zvati *mjera ili mjerna vrijednost baze.*

Tako npr. vektor $2e_1 - 3e_2$ ima mjeru $\begin{bmatrix} 2 \\ -3 \end{bmatrix}$ i ona se slaže iz mjera za e_1 i e_2 ovako: $\begin{bmatrix} 2 \\ -3 \end{bmatrix} = 2\begin{bmatrix} 1 \\ 0 \end{bmatrix} - 3\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Važno je uočiti da je $\begin{bmatrix} 2 \\ -3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ -3 \end{bmatrix}$.

0.2. Drugi primjer: Promatrajmo skup P_2 svih algebarskih polinoma u x stupnja ≤ 2 i sa koeficijentima iz R (R je tijelo realnih brojeva). P_2 je *vektorski prostor nad* R; npr. polinomi 3, $4x^2 - 5x + 2$, $3 - 2x + 6x^2$ jesu »*tačke*« ili članovi toga prostora, dakle »*vektori*«. Tu se samo po sebi nameće da vektore $1, x, x^2$ uzmemo kao »*bazu*« za *predstavljanje*, »*mjerenje*« svih ostalih vektora u P_2. »*Mjera*« od $3 - 2x + 6x^2$ je niz $3, -2, 6$, ili kao stupac $\begin{bmatrix} 3 \\ -2 \\ 6 \end{bmatrix}$. Zadana gornja tri polinoma imaju svoje mjerne vrijednosti u bazi $e = (e_1, e_2, e_3)$:

$$\begin{bmatrix} 3 \\ 0 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 2 \\ -5 \\ 4 \end{bmatrix}, \quad \begin{bmatrix} 3 \\ -2 \\ 6 \end{bmatrix}$$

ili ispisane preglednije u jednoj matrici:

$$\begin{bmatrix} 3 & 2 & 3 \\ 0 & -5 & -2 \\ 0 & 4 & 6 \end{bmatrix}.$$

Sama baza $e = e_1, e_2, e_3$ ima mjernu vrijednost

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

kao sastav mjernih vrijednosti od e_1, e_2, e_3.

Gornja dva primjera pokazuju kako proširenje pojma vektora pridonosi jedinstvenijem razmatranju raznih matematičkih ispitivanja. *Za početak, čitalac može pri riječima vektor, prostor itd.* imati na umu *obične geometrijske vektore u ravnini* i sl.

Tako će se npr. pokazati vrlo plodnom ideja, odnosno slika o tom da *svaka regularna kvadratna matrica može poslužiti kao neke vrste jedinica za mjerenje u odgovarajućem vektorskom prostoru*; u tome baš i jest uloga svake baze e u *vektorskom prostoru* (zamisli kvadar što ga razapinju vektori baze!).

POGLAVLJE 23.

NEKOLIKO KARAKTERISTIČNIH SLUČAJEVA U KOJIMA SE POJAVLJUJU MATRICE

Dosad smo se s matricama sreli posebno u obrađivanju sistema linearnih jednadžbi. U ovom poglavlju vidjet ćemo još nekoliko situacija u kojima se matrice prirodno pojavljuju i primjenjuju.

1. LINEARNA TRANSFORMACIJA LINEARNIH FORAMA

1.1. Primjer. Zadane su tri linearne forme

f_1, f_2, f_3 veličina x_1, x_2, x_3, x_4, x_5:

$$f_1 = a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + a_{14}x_4 + a_{15}x_5, \quad \text{tj.} \quad f_1 \equiv \sum_{5'=1}^{5} a_{15'} \cdot x_{5'}.$$

$$(1) \qquad f_2 \equiv \sum_{5'=1}^{5} a_{25'} x_{5'}$$

$$f_3 \equiv \sum_{5'=1}^{5} a_{35'} x_{5'}.$$

Sistem (1) možemo kraće pisati:

$$\begin{bmatrix} f_1 \\ f_2 \\ f_3 \end{bmatrix} = a \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}, \quad \text{gdje je } a = \begin{bmatrix} a_{11} & \cdots & a_{15} \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ a_{31} & \cdots & a_{35} \end{bmatrix},$$

a se zove *matrica linearnog sistema forama* (1).

Neka između veličina $x_{5'}$ i novih veličina $y_{2'} = y_1, y_2$[1] postoje linearne homogene veze:

$$x_{5'} = \sum_{2'} b_{5'2'} y_{2'} = b_{5'1} y_1 + b_{5'2} y_2$$

ili kraće $x \equiv by$.

[1] Za svaki redni broj r neka $r^{\cdot}$ ili r' označuje svaki od r rednih brojeva iz $[1, r) = \{1, 2, \ldots, r\}$.

Tada zadana veza $f = ax$ formalno prelazi u $a(by)$, odnosno $(ab)y$, pri čemu je ab ova tablica koeficijenata od y_1, y_2:

$$ab = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21}, & a_{11}b_{12} + a_{12}b_{22} \\ \sum a_{22'}b_{2'1} & ; \sum\limits_{2'} a_{22'}b_{2'2} \\ \sum a_{32'}b_{2'1} & , \sum a_{32'}b_{2'2} \end{bmatrix}.$$

Zaključak je općenit. Možemo ga izraziti ovako:

1.2. Teorem. *Ako je S zadan sistem linearnih forama u odnosu na veličine $x_1, x_2, \ldots$ pa se umjesto ovih veličina $x_{n'}$ uvedu njihove linearne forme veličinâ $y_{k'}$, tada sistem S prelazi u istobrojan sistem linearnih formi u odnosu na nove veličine $y_1 \cdots y_k$; matrica novog sistema dobiva se kao produkt matrice polaznog sistema i matrice linearnih formi kojom se bivše veličine $x_{n'}$ izražavaju pomoću novih veličina $y_{k'}$.*

1.3. Tako dolazimo do *najzanimljivijeg postupka* matričnog računa: da se *matrica a množi matricom b tako da se svaki redak od a skalarno pomnoži svakim stupcem od b i time dobiju odgovarajuće vrijednosti produkta ab tih matrica* (to, naravno, vrijedi samo ako prvi faktor ima toliko stupčića koliko drugi faktor ima redića).

Od specijalnog su interesa kvadratne matrice.

2. KVADRATNE MATRICE I PROMJENA KOORDINATNIH BAZA

2.0. Priprema. Znamo da se izborom tri nezavisna vektora $e_{3'} = e_1, e_2, e_3$ svaka tačka prostora, odnosno pripadni radijus-vektor može označiti (markirati) *numerički* kao uređena trojka brojeva. *Promjenom tih vektora $e_{3'}$* mijenja se i analitičko ime vektora. Matrice su izvanredno pogodno sredstvo da se dobije potpuno jasan pregled o vezama između raznih *koordinatnih baza* prostora i pripadnih *analitičkih imena*, odnosno predstavljanja *vektorâ* (a time i tačaka). Vidjet ćemo kako se pri tom uz svaku *regularnu* matricu a pojavljuju na prirodan način: *transponat* a^T, *antimatrica* a^{-1} i *antitransponat* $(a^T)^{-1}$.

Za primjene i bolje razumijevanje ovaj je paragraf od osnovne važnosti.

2.1. Konkretan primjer. U vektorskom prostoru V_2 od dvije dimenzije (recimo u običnoj ravnini) zadana je koordinatna baza $e = (e_1, e_2)$; uvedimo novu vektorsku bazu $e' = (e_1', e_2')$, gdje je npr. (crtaj!)

(1)
$$e_1' = -2\,e_1 + 3\,e_2$$
$$e_2' = -0{,}25\,e_1 + 0{,}5\,e_2.$$

Očigledno, e_1', e_2' su linearne forme od e_1, e_2; sistem (1) možemo pisati i ovako:

(2)
$$\begin{bmatrix} e_1' \\ e_2' \end{bmatrix} = \begin{bmatrix} -2 & 3 \\ -0{,}25 & 0{,}5 \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \end{bmatrix}.$$

Međutim, za nas će vrijediti ovo pravilo: *ako ne kažemo izričito drukčije, onda ćemo vektore koji se pojavljuju stavljati da budu* ***stupci matrica.*** Zato ćemo iz starih vektora e_1, e_2, izgraditi njihovu matricu $[e_1, e_2]$; iz novih vektora e_1', e_2' također ćemo izgraditi matricu $[e_1', e_2']$ i označiti je sa e' ili (e') i sl.

Sistem (1) ćemo ekvivalentno ispisivati ovako:

(3)
$$[e_1', e_2'] = [e_1, e_2] \cdot \begin{bmatrix} -2 & -0{,}25 \\ 3 & 0{,}5 \end{bmatrix}.$$

Tu se pojavljuje matrica koja je građena tako da su *stupci matrice upravo koordinate* ***novih*** *vektora $e'_{2'}$ u* ***staroj*** *bazi.*

Jasno je da su sva tri načina pisanja: (1), (2), (3) *ravnopravna.* No, za ***matrični račun*** *najzgodniji je način pisanja* (3) *i mi ćemo ga se pridržavati,* ukoliko ne kažemo drukčije. Jednadžba (3) se kraće simbolički piše:

(4)
$$e' = ea,$$

gdje je

(5)
$$a = \begin{bmatrix} -2 & -0{,}25 \\ 3 & 0{,}5 \end{bmatrix}.$$

Pri tom je važno uočiti da slovo e u (4) znači bazu, i to pisanu u obliku $[e_1, e_2]$, kao i u koordinatnom obliku $\begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix}$.

2.2. Osnovna napomena o indeksima. *Ako imamo neki vektor oznake e_k pa ako on ulazi u matricu e kao* ***stupac,*** *onda ćemo ispisivati*

$$e_k = \begin{bmatrix} e_{1k} \\ e_{2k} \\ \vdots \end{bmatrix}, \text{ kraće } e_k = [e_{ik}]_i$$ **(drugi indeks se prenosi).**

Bez ove napomene izgubit ćemo se u indeksima!

A čitav smisao simbolike udešen je tako da se na jednakost (4) može gledati kao na množenje matrice $e = [e_1, e_2]$ i matrice a s rezultatom $e' = [e_1', e_2']$.

2.2.1. Formalno (v. (4)), *nova baza e'* izlazi iz *stare baze e* tako da *matrica a vuče i prevodi staru bazu e* (kad kažemo *vuče ili prevodi,* mislimo na to da matrica *djeluje na desnu stranu, a ne na lijevu stranu*). Bitno je da vidimo kako je *matrica a građena*: *njeni vektori* (tj. *stupčići, a ne redići!*) jesu koordinate *novih vektora baze* u odnosu na *staru bazu.* Nadalje, baza e je građena tako da *njeni vektori* zauzimaju *stupce,* i to: *i stvarno, i formalno* u pogledu indeksa. Isto tako za e'.

Kaže se da *nova* baza e' nastaje iz *stare* baze e *posredstvom matrice a,* odnosno e' je proizvod stare baze i prevodne matrice. *Mnemotehnički prije dođe početna baza* nego *matrica za transformaciju*; zato se pravi produkt ea (a ne ae).

Uvedimo sada umjesto netom uvedene baze e' novu bazu e'' posredstvom neke matrice a'; to znači da je

(6) $$e'' = e'\, a'.$$

Tada iz (4) i (5) izlazi (dovesti e' iz (4) u (6)):

(7) $$e'' = (ea)\, a' = e\,(a \cdot a'),$$
$$e'' = e\,(aa').$$

Tu se pojavljuje produkt matricâ a, a'.

Da je dalje

$$e''' = e''\, a'',$$

bilo bi analogno

$$e''' = e\,(a\, a'\, a''), \quad \text{itd.}$$

Tako smo došli do vrlo važnog teorema:

⟶ **2.3. Fundamentalni teorem o koordinatnim bazama.** ***Ako se umjesto koordinatne baze e postepeno uvode nove koordinatne baze $e', e'', \ldots e^{(n)}$, tada se najnovija koordinatna baza može neposredno uvesti počev od prve koordinatne baze; uvodna matrica jednaka je produktu svih parcijalnih uvodnih matrica koje su se u toku procesa pojavljivale prevodeći svaki put netom uvedenu bazu u narednu.***

Pri tom je od bitnog značenja da su pri *svakom* koraku *stupci svake prevodne* matrice upravo koordinate što ih vektori *upravo uvođene nove baze* imaju u odnosu na *upravo napuštenu* bazu.

2.4. Gornje je pravilo bitno. Treba dobro imati na umu *gradnju prevodne* matrice! Inače, ako ne gradimo ispravno prevodne matrice, pravilo nije ispravno. Također treba imati na umu činjenicu da se *svaki put nova baza izražava pomoću napuštene baze* linearno *homogeno* (bez translacija).

2.5. Primjer. U ravnini je zadana koordinatna baza vektorâ

$$e_1 = \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \quad e_2 = \begin{bmatrix} -3 \\ 4 \end{bmatrix}.$$

Uvedimo nove koordinatne baze po redu:

$$\begin{aligned} x &= 2\,e_1 - 3\,e_2 \\ x' &= 5\,e_1 + 3\,e_2 \\ y &= -x + 2\,x' \\ y' &= 4\,x - 3\,x'. \end{aligned}$$

Tada možemo odmah napisati najnoviju bazu y, y'

$$[y, y'] = \underbrace{\begin{bmatrix} 2 & -3 \\ 3 & 4 \end{bmatrix}}_{[e_1,\, e_2]} \cdot \underbrace{\begin{bmatrix} 2 & 5 \\ -3 & 3 \end{bmatrix}}_{\text{oprez! ne } \begin{bmatrix} 2 & -3 \\ 5 & 3 \end{bmatrix}} \cdot \begin{bmatrix} -1 & 4 \\ 2 & -3 \end{bmatrix} = \begin{bmatrix} 13 & 1 \\ -6 & 27 \end{bmatrix} \begin{bmatrix} -1 & 4 \\ 2 & -3 \end{bmatrix} = \begin{bmatrix} -11 & -49 \\ 60 & -105 \end{bmatrix}$$

2.6. Oprez! Svaki put, prevodna matrica mora biti *regularna kvadratna matrica*. Naime, mi idemo iz baze u bazu! A sve su baze *istobrojne*! Sve imaju isti broj, n, nezavisnih vektora. Kad bi jedna od prevodnih matrica bila singularna, prevela bi ona napuštanu vektorsku bazu u skup *zavisnih* vektora pa novi vektori ne bi tvorili koordinatne baze. To izlazi iz osnovnog teorema o rangu produkta matrica i o rangu matrica uopće (isp. pogl. 15, § 8, specijalno 8.8).

2.7. Pojava obratne matrice — povrat iz nove baze u staru. Ako smo umjesto baze e uveli novu bazu e' posredstvom matrice a, tj.

(*) $$e' = ea \qquad \text{(matrica } \textit{vuče} \text{ staru bazu!)},$$

tada, obrnuto, možemo *ići i natrag*: *povratiti se iz nove baze u staru*! Kako? Ako matričnu jednakost (*) „povučemo" sa a^{-1} (*desno* množi sa a^{-1}), izlazi

$$e' a^{-1} = e.$$

Tako vidimo ulogu inverzne matrice: *ako matrica a prevodi bazu e u novu bazu e'*, tada obratna matrica a^{-1} vodi *novu bazu* natrag u *staru bazu*.

Ne samo to! Nego, ako je bilo više uzastopnih etapa uvođenja sve novih i novih baza s prevodnim matricama $a_1, a_2, a_3 \ldots, a_n$, tada ćemo ići natrag *obratnim redom s obratnim matricama*

$$a_n^{-1},\ a_{n-1}^{-1}, \ldots,\ a_2^{-1},\ a_1^{-1}$$

i doći na polaznu bazu.

No, umjesto toga *uzastopnog koračanja*, mogli smo napraviti jedan, i to veliki korak unatrag s matricom $(a_1 \cdots a_n)^{-1}$; tako vidimo da vrijedi

2.7.1. Teorem. $(a_1 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}$
(*pravilo o obrtanju produkta matrica*). (isp. pogl. 12, § 5.3).

2.8. Važna primjedba. Nova uloga matrice. Svaka matrica koja prevodi koordinatnu bazu vektorâ u novu bazu vektorâ mora biti *regularna i kvadratna*. I obratno: *svaka regularna kvadratna matrica a poretka $n \times n$ može se upotrijebiti za prevođenje svake n-člane baze u njen odgovarajući novi položaj $e' = ea$! To je nova uloga matrice*: *stupci regularne matrice a određuju položaj nove baze e' u odnosu na napuštenu bazu e.*

Npr. ako matrica

$$a = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 3 \end{bmatrix} \quad \text{vuče vektorsku bazu} \quad \begin{bmatrix} 5 & -3 & 2 \\ 4 & 5 & 1 \\ -3 & 2 & 3 \end{bmatrix} = e,$$

dolazimo u novu vektorsku bazu

$$e' = \begin{bmatrix} 5 & -3 & 2 \\ 4 & 5 & 1 \\ -3 & 2 & 3 \end{bmatrix} \begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 7 & -4 & 6 \\ 13 & 11 & 3 \\ -4 & 7 & 9 \end{bmatrix}.$$

⟶ **2.9. Završni teorem o matricama i vektorskim bazama.** ***Svaka kvadratna regularna matrica sa n stupaca predstavlja n linearno nezavisnih vektora. Stupci svake kvadratne regularne matrice reda n mogu se upotrijebiti kao rezerva za n nezavisnih vektora*** (da posluže za koordinatnu bazu ako ona ima n članova). ***Svaka takva regularna matrica može se upotrijebiti također za sprovođenje svake n-člane baze u određenu n-članu bazu.***

2.10. Zadaci o promjenama varijabli i koordinata.

1. Zadane su linearne forme $f_1 = 3x + 5y$, $f_2 = 3x - 2y$, $f_3 = 4x + 3y$; u što one prelaze ako se stavi $x = 2u - 3v + 4z$,

$$y = 5u - 2v - 3z?$$

Radi direktno i matrično!

2. Stavimo u prethodnom zadatku dalje $u = 2a - 3b + 4c$

$$v = b$$

U što prelaze izrazi f_1, f_2, f_3? $\quad z = a + 2b$.

3. U ravnini je zadana koordinatna baza $e = (e_1, e_2)$; ako se umjesto vektorâ $e_1\ e_2$ uvedu vektori $e_1' = 5e_1 - 3e_2$, $e_2' = -3e_1 + 5e_2$ kao nova baza $e' = (e_1', e_2')$, prikaži matrično prelaz od e na e'.

4. Ako se u zadatku 3. stavi $e_1'' = 5e_1' - 3e_2'$

$$e_2'' = 4e_1' + 5e_2'$$

da li je $(e_1'', e_2'') = e''$ koordinatna baza? Kako se e'' izražava pomoću baze e?

5. Promatraj matricu $a = \begin{bmatrix} 5 & 2 \\ 4 & -1 \end{bmatrix}$ i shvati je kao prevodnu matricu od stare koordinatne baze nekog dvodimenzionalnog prostora u novu; kako glase novi koordinatni vektori?

3. KAKO SE MIJENJA ANALITIČKO IME — REPREZENTACIJA — VEKTORA PRI PROMJENI BAZE?

3.1. Primjer. Kako glasi prikaz „vektora“ (polinoma)

$$v = 7 - 7x^2 + 18x \tag{1}$$

kao linearnog spoja „vektorâ“

$$4, \quad 5 + 3x^2 - 2x, \quad 4x - x^2? \tag{2}$$

Radi se o tom da se nađu skalari v_1, v_2, v_3 tako da bude

$$\begin{gathered} 4v_1 + (5 - 2x + 3x^2)v_2 + (4x - x^2)v_3 = 7 + 18x - 7x^2, \quad \text{tj.} \\ (4v_1 + 5v_2) + (-2v_2 + 4v_3)x + (3v_2 - v_3)x^2 = 7 + 18x - 7x^2. \end{gathered} \tag{3}$$

Izjednačujući koeficijente:

$$\begin{aligned} 4v_1+5v_2 \qquad &= 7 \\ -2v_2+4v_3 &= 18 \\ 3v_2-v_3 &= -7 \end{aligned} \tag{4}$$

$$v_1=3,\ v_2=-1,\ v_3=4. \tag{5}$$

I zbilja je

$$7-18x-7x^2=4\cdot 3+(5-2x+3x^2)\cdot -1+(4x-x^2)\cdot 4.$$

Sistem (4) se matrično piše

$$\begin{bmatrix} 4 & 5 & 0 \\ 0 & -2 & 4 \\ 0 & 3 & -1 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = \begin{bmatrix} 7 \\ 18 \\ -7 \end{bmatrix}; \tag{6}$$

odatle

$$\begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = \begin{bmatrix} 4 & 5 & 0 \\ 0 & -2 & 4 \\ 0 & 3 & -1 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 7 \\ 18 \\ -7 \end{bmatrix} = \begin{bmatrix} 3 \\ -1 \\ 4 \end{bmatrix}. \tag{7}$$

O čemu se zapravo radilo?

Tu se zapravo radilo o polinomima stupnja <3; svi polinomi stupnja <3 čine određen vektorski prostor P_3; za bazu toga prostora uzimamo obično polinome

$$1,\quad x,\quad x^2. \tag{8}$$

Članovi (2) nove baze e' imaju prema bazi (8) ove „značke"

$$\begin{bmatrix} 4 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 5 \\ -2 \\ 3 \end{bmatrix}, \begin{bmatrix} 0 \\ 4 \\ -1 \end{bmatrix};$$

čitava nova baza $e'=[4,\ 5-2x+3x^2,\ 4x-x^2]$ izražena pomoću baze (8) nosi u toj bazi e „značku"

$$\begin{bmatrix} 4 & 5 & 0 \\ 0 & -2 & 4 \\ 0 & 3 & -1 \end{bmatrix}; \tag{9}$$

tu svaki stupac predstavlja šifru ili značku za odgovarajući „vektor" (2), pa na pregledan i sređen način odmah vidimo o kojem se vektoru radi.

Značka v_e zadanog vektora (1) u bazi e glasi $\begin{bmatrix} 7 \\ 18 \\ -7 \end{bmatrix}$ (ispisuju se, kao stupac, odozgo prema dolje, po redu koeficijenti *sređenog* polinoma). Traži se značka v_e' polinoma (1) u *novoj* bazi e' znajući: *stare* značke tog istog polinoma (1) i značku nove baze; matrica (9) je stara značka nove baze (*nova* baza (2) će preuzeti kao *novu* značku *bivšu* značku $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ *bivše* baze (9), itd). Tu smo vidjeli ideju, a sada da nađemo osnovni zakon.

3.2. Problem. Promatrajmo dvije vektorske baze: staru bazu e i novu e', koja iz stare nastaje kao produkt od e i neke matrice a:

$$e' = ea; \tag{10}$$

to znači da je matrica a značka *nove* baze u *staroj* bazi e, tj. matrica a daje *reprezentaciju nove* baze u *staroj* bazi; koordinate vektora iz e' prema e upravo su *stupci* od a i tako na »*kineski način*«, tj. kao stupci, *upisane* u matricu.

Za svaki vektor v imamo potpuno određenu značku ili zapis v_e prema bazi e te značku $v_{e'}$ prema bazi e':

$$v = ev_e, \quad v = e' v_{e'}\text{[1]};$$

odatle

$$e' v_{e'} = ev_e.$$

Dalje je to s obzirom na (10):

$$(ea)\, v_{e'} = ev_e.$$

Množeći sprijeda sa e^{-1}:

$$av_{e'} = v_e \tag{11}$$

Odatle, množeći s lijeve strane sa a^{-1}:

$$v_{e'} = a^{-1} v_e. \tag{12}$$

Ukratko, imamo zaista fundamentalan rezultat:

—→ **3.3. Fundamentalni teorem o promjeni baza i koordinata:**

(13)

(3.3.0) $$e' = ea$$

(3.3.1) $$v_{e'} = a^{-1} v_e$$

(3.3.2) $$av_{e'} = v_e.$$

Ako regularna matrica a vuče staru koordinatnu bazu e u novu bazu e', tada obratna matrica a^{-1} gura staru reprezentaciju (značku) svakog vektora u novu reprezentaciju, novu značku: prelaz u novu situaciju dešava se istodobno, i to jedna matrica vuče bazu, a obratna matrica gura koordinate. Pri tom matrica a predstavlja zapis, značku ili reprezentaciju nove baze u staroj bazi (tj. stupci matrice a jesu zapisi, značke, u staroj bazi, vektorâ koji će tvoriti novu bazu). Istom matricom kojom se iz stare baze desnom multiplikacijom dobiva nova,

---

[1] Naravno, skalari koji čine niz v_e jesu koeficijenti od $e_{n'}$ kad vektor v rastavimo po vektorima baze e.

baza, dobiva se lijevom multiplikacijom iz nove značke svakog vektora njegova stara značka.

Eto, to je jedan od osnovnih teorema o relativizmu u matematici! Koliko je tu simbolički jezik (13) pregledniji i sažetiji od niza riječi što ih pročitasmo i izgovorismo. Znajmo da svjesno ili nesvjesno neprestano imamo posla sa sadržajem gornjeg teorema, odnosno s relacijama (13).

3.4. Uočimo da za zadane dvije baze e, e' svaki vektor prostora ima i novu značku i staru značku. Skup svih starih značaka je isti kao i skup svih novih značaka — samo su značke drukčije porazdijeljene[1].

„Žuta majica" (jedinična matrica) kao ekipi pripada novoj bazi e'; njena nova značka je jedinična matrica; „žute majice" kao pojedinci nose $e_1', \ldots, e_n'$; njihove su nove značke po redu

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

kao ekipi, njima je kao stara značka pripadala matrica a iz (13).

3.4.1. Primjedba. Specijalno, uočimo da se pri promjenama bazâ nova baza izražava pomoću stare, a kod koordinatâ obratno: stare se izražavaju novima (naravno da je i obratan put osiguran!).

3.5. Uočimo da mijenjanje značke za svaki vektor izaziva potpuno određenu promjenu baza; i obratno: promjena baza, tj. izbor nove baze e' umjesto stare baze e po propisu (3.3.0), izaziva promjenu značke v_e u značku $v_{e'}$ za *svaki* vektor v, i to po propisu (3.3.2); i obratno.

3.6. Primijetimo da svaka baza e pridjeljuje svakoj bazi e' onu matricu a kao značku za koju je $ea = e'$.

Ukratko i fundamentalno imamo:

⟶ **3.7. Osnovni teorem o međuzavisnosti.** ***U relaciji $ea = e'$, gdje je a regularna matrica i gdje su e, e' baze, svaka od te tri veličine e, e', a potpuno je određena ostalim dvjema, koje su inače potpuno slobodne; pri tom za svaki vektor proizlazi relacija***

$$av_{e'} = v_e.$$

⟶ **3.8. Osnovna jednakost o mjernim brojevima i značkama.** ***Ako imamo bilo koje dvije koordinatne baze e, e', tada istoj veličini v pripadaju odgovarajuće značke v_e, $v_{e'}$ i zadovoljavaju relaciju***

(14)
$$ev_e = e' v_{e'}.$$

Naime, imamo

$$v = ev_e, \quad v = e' v_{e'};$$

odatle i (14).

[1] To nam osigurava Cramerovo pravilo. Naime, svakoj staroj znački v_e odgovara nova značka $v_{e'}$ po (3.3.1); svakoj novoj znački $v_{e'}$ pripada stara značka v_e prema propisu (3.3.2).

Jednakost (14) je zaista od prvorazredne važnosti. Ona izgleda banalnom! I izlazi iz identiteta

$$v = v$$

operativno na jednostavan način. U (14) kao da se „neutralizira koeficijent od v i indeks v" (inače treba znati da u izrazu ev_e imamo dva matrična faktora, i to e, v_e).

Međutim, jednakost (14) čini se trivijalnom, jer je izražena na adekvatan način. Trebalo je hiljade godina pa da se izgradi formalan matematički jezik kao što je relacija (14).

4. UZASTOPNO MIJENJANJE KOORDINATA. EULEROVE RELACIJE

Ako umjesto baze e uzmemo bazu e' na osnovu $ea = e'$, tada se stara značka v_e i nova značka $v_{e'}$ *istog* vektora v povezuju ovako:

$$av_{e'} = v_e;$$

u toj relaciji dolaze same značke (matrice); zato je preglednije ako govorimo o staroj znački x[1] i novoj znački x' jednog te istog vektora te o transformaciji koordinata ili značaka:

$$ax' = x. \tag{1}$$

Tu matrica djeluje sprijeda, i to na novu značku.

Ako, analogno, umjesto koordinatâ x' uvedemo nove koordinate (značke) na osnovu veza

$$a' x'' = x', \tag{2}$$

tada, unoseći ovo x' u (1), izlazi:

$$a\,a'\,x'' = x;$$

ako je k tome $a''x''' = x''$, tada bismo dobili

$$a\,a'\,a''\,x''' = x, \quad \text{itd.}$$

$\longrightarrow$ **4.1.** Teorem. *Višekratno uvođenje niza sve novih i novih koordinata, „značaka" (vrsta koordinata) ekvivalentno je jednokratnom prelazu od početnih na najnovije koordinate. Pri tom je matrica te koordinatne promjene jednaka produktu matrica pri etapnim promjenama; produkt se uzima onim redom kako su se matrice pojavljivale. Matrica je prvi faktor, a značka drugi.*

4.2. Primjer. Rotacija u ravnini. Neka u ravnini nova baza e' nastaje iz zadane ortonormirane baze e rotacijom za kut α u pozitivnom smislu.

---

[1] Ako se radi o tročlanoj znački x, onda to znači da je $x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$; slično za stupac. Npr. vektoru $4i - 2j + 7k$ odgovara značka $\begin{bmatrix} 4 \\ -2 \\ 7 \end{bmatrix}$, itd.

Tada su stara značka $\begin{bmatrix} x \\ y \end{bmatrix}$ (stare koordinate x, y) i nova značka $\begin{bmatrix} x' \\ y' \end{bmatrix}$ jedne te iste tačke vezane relacijom $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix}$. (V. Rašajski, [1], s. 97, (6)).

Nova rotacija baze za β dovodi do nove značke $\begin{bmatrix} x'' \\ y'' \end{bmatrix}$ iste tačke, pa je analogno $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix} \begin{bmatrix} x'' \\ y'' \end{bmatrix}$,

odnosno

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \cdot \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix} \begin{bmatrix} x'' \\ y'' \end{bmatrix} =$$

$$= \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta, & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta, & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{bmatrix} \begin{bmatrix} x'' \\ y'' \end{bmatrix}, \text{ tj.}$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \cos(\alpha+\beta), & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta), & \cos(\alpha+\beta) \end{bmatrix} \begin{bmatrix} x'' \\ y'' \end{bmatrix}.$$

Najnovija baza izlazi, dakle, iz polazne baze jednokratnom rotacijom za $\alpha+\beta$.

4.3. Da se radilo o koordinatnom prostoru i pravokutnom Descartesovu sistemu pa da smo novi sistem dobili iz starog rotacijom za kut φ oko trećeg koordinatnog vektora, tada bi veza između starih koordinata x, y, z i novih koordinata x', y', z' glasila:

(1) $$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \\ z' \end{bmatrix}.$$

Da smo umjesto novog koordinatnog sistema uveli neki drugi, recimo rotacijom oko prvog vektora za kut γ, tada bismo za nove koordinate $x'' y'' z''$ iste tačke imali analognu vezu

(2) $$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\gamma & -\sin\gamma \\ 0 & \sin\gamma & \cos\gamma \end{bmatrix} \begin{bmatrix} x'' \\ y'' \\ z'' \end{bmatrix}.$$

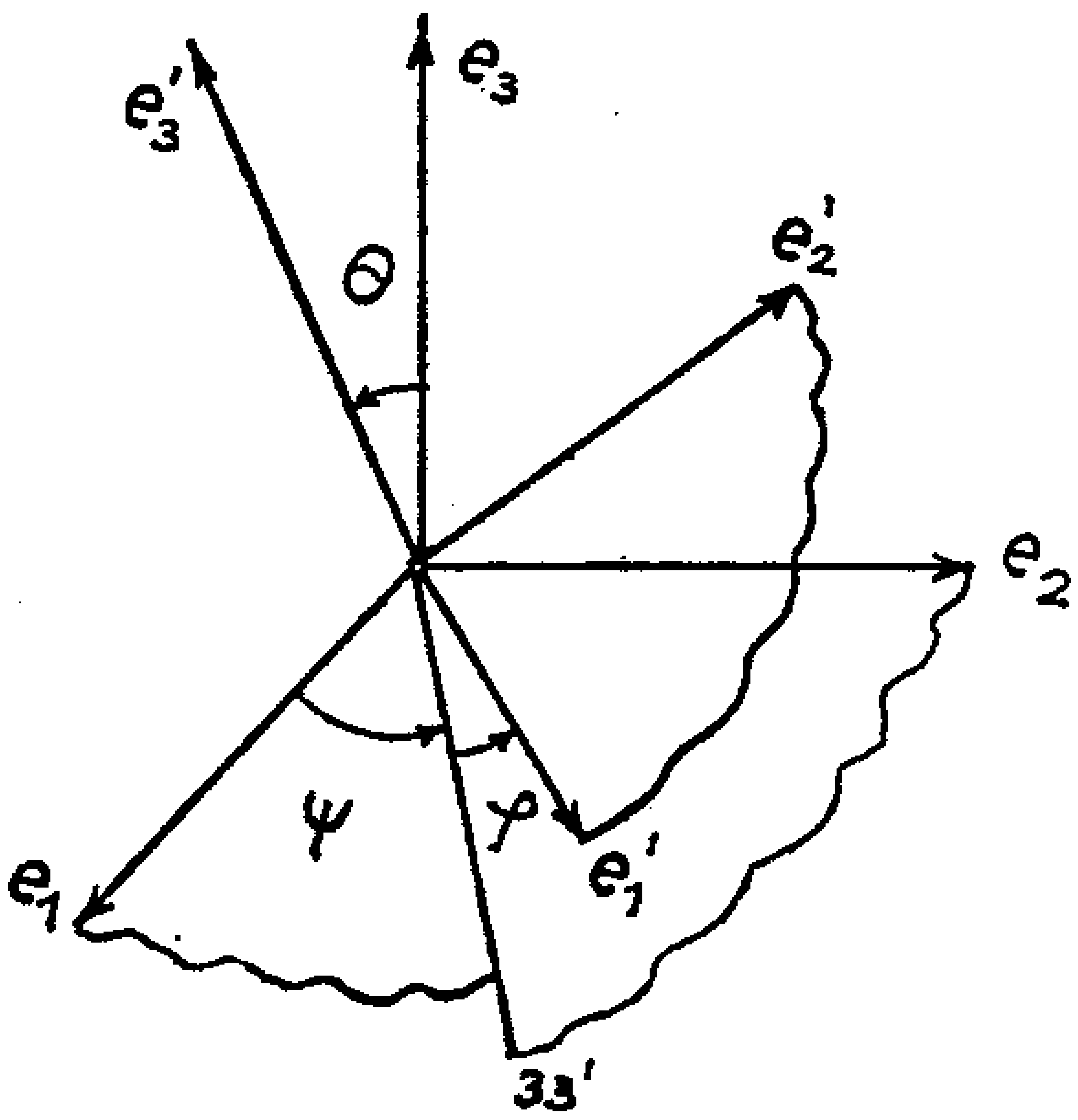
Veza između polaznih koordinata x, y, z i najnovijih koordinata x'', y'', z'' glasila bi ovako:

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = ab \begin{bmatrix} x'' \\ y'' \\ z'' \end{bmatrix},$$

pri čemu su a i b napisane kvadratne matrice u (1), odnosno u (2).

Primijenimo to i dokažimo jedan Eulerov teorem.

4.4. Eulerove relacije. Rotacija koordinatne baze u prostoru. Zadana je uređena dvojka (S, S') ortonormiranih triedara $S=(e_{3'})$, $S'=(e'_{3'})$ s istim početkom O i istom orijentacijom. Prelaz od S na S' može se prema Euleru opisati ovako. Neka je $33'$ pravulja u kojoj se sijeku koordinatne ravnine $e_1 e_2$, $e_1' e_2'$. Tada se rotacijom oko e_3 za kut ψ (kut $\psi = \sphericalangle(e_1, 33')$ vektor e_1 prevodi u f_1, a e_2 u f_2; zatim sa rotacijom za $\theta = \sphericalangle(e_3, e_3')$ (kut nutacije) oko f_1 prevodi: f_1 u f_1, f_2 u g_2, a e_3 u e_3'; najzad se rotacijom za $\varphi = \sphericalangle(33', e_1')$ prevodi f_1 u e_1', g_2 u e_2', a e_3' ostaje na miru — dolazi se, dakle, do zadanog novog triedra e'_1, e'_2, e'_3. No, svaka od spomenutih triju rotacija dovodi do novog koordinatnog sistema i do novih koordinata u tim sistemima; izražavajući pri svakom koraku prethodne koordinate s upravo uvedenima dolazimo do određene matrice, kojoj vrijednosti zavise od kuta ψ, odnosno ϑ, odnosno φ; slažući sve te tri promjene, dolazimo do ove veze među starim koordinatama x, y, z i novim koordinatama x', y', z' jedne te iste tačke T:



Sl. 4.4.

$$(1)\quad \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} \cos\psi & -\sin\psi & 0 \\ \sin\psi & \cos\psi & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \\ z' \end{bmatrix},$$

odnosno izmnoženo:

$$(2)\quad \begin{bmatrix} x \\ y \\ z \end{bmatrix} =$$

$$\begin{bmatrix} \cos\psi\cos\varphi - \sin\psi\sin\varphi\cos\theta & -\cos\psi\sin\varphi - \sin\psi\cos\varphi\cos\theta & \sin\psi\sin\theta \\ \sin\psi\cos\varphi + \cos\psi\sin\varphi\cos\theta & -\sin\psi\cos\varphi + \cos\psi\cos\varphi\cos\theta & -\cos\psi\sin\theta \\ \sin\varphi\sin\theta & \cos\varphi\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x' \\ y' \\ z' \end{bmatrix}.$$

Odatle se vidi kako je pregledna veza (1); izračunavanjem lako se provjeri veza (2). Tako npr. koordinata z izlazi množenjem trećeg retka sa stupcem, tj. $z = \sin\varphi \sin\theta\, x' + \cos\varphi \sin\theta\, y' + \cos\theta\, z'$ (isp. Rašajski [1], s. 102).

4.5. Zadaci o promjenama koordinatnih baza.

1. Vektor x izrazi pomoću vektorâ e_k: 1) $e_1=[1, 0]^T$, $e_2=[0, 1]^T$, $x=[3, 4]^T$; 2) $e_1=[2, 5]^T$, $e_2=[3, 4]^T$, $x=[0, 5]^T$; 3) $e_1=[1, 2, 3]^T$, $e_2=[-3, 2, 5]^T$, $e_3=[0, 3, 1]^T$, $x=[-2, 3, -4]^T$.

2. Pokaži da vektori $e_{n'}$ čine bazu e kao što i vektori $e'_{n'}$ čine bazu e'; nađi vezu između koordinata jednog te istog vektora u ovim dvjema bazama:

   1) $e_1=[2, 1]^T$, $e_2=[3, 1]^T$, $e_1'=[5, 2]^T$, $e_2'=[0, 3]^T$:

   2) $e_1=[1, 2, 1]^T$, $e_2=[2, 3, 3]^T$, $e_3=[3, 7, 1]^T$ tj. $e=\begin{bmatrix}1 & 2 & 3\\ 2 & 3 & 7\\ 1 & 3 & 1\end{bmatrix}$,

   $e'=[3, 1, 4]^T$, $e'_2=[5, 2, 3]^T$, $e'_3=[1, 1, -6]^T$ tj. $e'=\begin{bmatrix}3 & 5 & 1\\ 1 & 2 & 1\\ 4 & 3 & -6\end{bmatrix}$,

   3) $e=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 2 & 1 & 3\\ 1 & 1 & 2 & 2\\ 1 & 1 & 1 & 3\end{bmatrix}$, $\quad e'=\begin{bmatrix}1 & -2 & 2 & -2\\ 0 & -3 & 2 & -3\\ 3 & -5 & 5 & -4\\ 3 & -4 & 4 & -4\end{bmatrix}$.

3. Pokaži da 1) stupci, 2) redići matrice $a=\begin{bmatrix}2 & 5 & 7\\ 6 & 3 & 4\\ 5 & -2 & -3\end{bmatrix}$

   čine bazu (osnovu) u prostoru R_3; nađi koordinate tačke (3, 1, 4) u prvoj, odnosno u drugoj bazi.

4. Nađi „koordinate" „vektora" $3+2x-2x^2$ u bazi 1) $1, x, x^2$;

   2) $3, -2x, 5x^2$; 3) $1, (x-1), (x-1)^2$; nađi matricu prelaženja od prve baze na drugu te od druge na treću kao i veze među koordinatama pomenutog vektora.

5. Iz baze e proizvode se baze $e'=ea$, $e''=eb'$; kakva je veza među koordinatama vektora v u tim trima bazama?

6. U ravnini se koordinatne baze e', e'' dobiju rotacijom baze e oko 0 za 30^0, odnosno 60^0; nađi veze 1) između bazâ e', e''; 2) između koordinata tačke (1, 5) u tim dvjema bazama.

7. 1) U prostoru R_3 zavrti osnovni triedar e za $30°$ oko osi e_2; nađi koordinate tačke $T=(1, 2, 3)$ u toj novoj koordinatnoj bazi e'.

   2) Ako se baza e' zavrti za 15^0 oko e_1', nađi oznaku tačke T u toj novoj bazi e''.

5. MATRICE I VARIJANTNOST DVA NIZA VARIJABILNIH VELIČINA. KONTRAGREDIJENTNE MATRICE. ORTOGONALNE MATRICE

Često dolaze izrazi oblika

(1) $$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

Možemo ga pisati i kao matrični produkt:

$$x^T \cdot y, \quad \text{gdje je } x \text{ stupac od } x_1, x_2, \ldots, x_n.$$

Isto tako

$$y = [y_1 \cdots y_n]^T.$$

Zahtijeva se da izraz (1) uvođenjem novih n varijabli $x'_{n'}$ i n varijabli $y'_{n'}$ posredstvom matričnih množenja

(2) $$x = ax', \quad y = by'$$

prijeđe u analogan izraz

(3) $$\sum x'_{n'} y'_{n'}.$$

Pri tom matrice a, b ne zavise od $x'_{n'}$, $y'_{n'}$.

No, izraz (1) pišemo matrično kao

(4) $$x^T y \quad (x^T \text{ znači redak } x_1, x_2, \ldots).$$

Na osnovu (2) postaje $(4) = (ax')^T (by') = x'^T a^T by'$. Prema zahtjevu (3) treba da bude (★) $x'^T a^T by' = x'^T y'$. Ako u vektorski identitet (★) uvrstimo specijalno $x' = \delta_{.i}$, $y' = \delta_{.j}$, daje on

$$(\delta_{.i}{}^T a^T)(b\,\delta_{.j}) = \delta_{.i}{}^T \delta_{.j} \Rightarrow (a^T)_{i.}\, b_{.j} = \delta_{ij} \Rightarrow (a^T b)_{ij} = \delta_{ij} \quad \text{tj.} \quad a^T b = 1.$$

To znači da za invarijantnost izraza (1) pri supstitucijama (2) mora vrijediti

(5) $$a^T b = 1.$$

Na taj se način dolazi do *nove relacije* (5) među matricama a, b transformacijâ (2) pa da izraz (1) i *poslije* transformacije ostane *istog* oblika.

Iz (5) izlazi

$$a^T = b^{-1};$$

odatle

(6) $$(a^T)^T = (b^{-1})^T$$

$$a = (b^{-1})^T; \quad \text{također se vidi da je} \quad b = (a^{-1})^T.$$

⟶ **5.1. Definicija kontragredijentnih matrica.** *Kontragredijent* zadane matrice a je transponat obratne matrice; označuje se sa $a^\sim$; dakle je po definiciji $a^\sim = (a^{-1})^T$.

5.2. Svojstva operatora $\sim$. Za operator kontragredijencije vrijede analogna pravila kao pri transponiranju i inverziji.

Napose

$$(a^\sim)^\sim = a \ (\textit{idempotentnost}), \ (ab)^\sim = a^\sim b^\sim.$$

Svaka kontragredijentna matrica je regularna. Svaka regularna matrica ima svoju kontragredijentnu matricu.

5.3. Teorem. *Zadana je funkcija* $\sum_{n'} x_{n'} y_{n'}$ *veličinâ* $x_1, \ldots, x_n, y_1, \ldots, y_n$; *ako za neki par kvadratnih matrica* a, b *i promjenu varijabli*

$$x = ax', \quad y = by' \quad \textit{vrijedi identički} \quad \sum x_{n'} y_{n'} = \sum x'_{n'} y'_{n'},$$

onda su matrice a i b kontragredijentne međusobno, tj. $a^T b = 1$; i obratno.

5.4. Izraz tipa (1) imali smo i pri predstavljanju *istog* vektora v u *raznim* bazama e, e' nekog prostora. Naime, prema osnovnoj relaciji (14) iz § 3.8. baš se osnovni teorem i iskazuje da promjenom baza produkt matrice e i matričnog zapisa v_e od v u bazi e mora ostati invarijantan (isp. pogl. 25, § 7.4).

5.5. **Invarijantnost izraza**

$$x^T x \equiv x_1^2 + x_2^2 + \cdots + x_n^2 \tag{7}$$

pri transformaciji. Specijalno za slučaj $x=y$ postaje izraz (1) oblika (7), pa se radi samo o transformaciji $x=ax'$; rezultat iz § 5.3. sada kazuje da je izraz (7) invarijantan pri transformaciji $x=ax'$ jedino onda ako je matrica a sama sa sobom kontragredijentna, tj. ako je $(a^{-1})^T=a$, odnosno $a^{-1}=a^T$. Takve matrice zovu sa *ortogonalnim matricama.*

O njima će biti govora kasnije u poglavlju 28.

Tako npr. za slučaj $n=2$ radi se o linearnim promjenama za koje će izraz

$$x_1^2+x_2^2$$

ostati invarijantan. Rotacije oko ishodišta, tj. transformacije

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} x_1' \\ x_2' \end{bmatrix}.$$

zadovoljavaju tome uslovu.

Uslovu zadovoljavaju i transformacije kojima matrica iz te matrice izlazi zamjenom stupaca, tj.

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} -\sin\alpha & \cos\alpha \\ \cos\alpha & \sin\alpha \end{bmatrix} \begin{bmatrix} x_1' \\ x_2' \end{bmatrix}.$$

Nema drugih transformacija prema kojima bi forma ostala invarijantna.

Analogan problem: *naći sve transformacije pri kojima forma* $\sum_{i=1}^{n} x_i^2$ *ostaje invarijantnom* i važan je i zanimljiv, i mnogo teži.

6. MATRICE KAO OPERATORI NAD VEKTORIMA

Osim dosadašnjih uloga matricâ spomenimo još jednu, koju ćemo inače kasnije u poglavljima 27, 28 i 29. opširnije obraditi. Radi se o tom da je produkt matrice i vektora (stupca) opet vektor.

Na taj način, za zadan prostor R_n od n dimenzija svaka kvadratna matrica a s vrijednostima iz R pridijeljuje svakom vektoru (zapisanom kao stupac) v određen vektor av; simbolički: $v \xrightarrow{a} av$.

Specijalno, $v(1_n)_{n'}=v_{n'}$ gdje je $(1_n)_{n'}$ n'-ti stupac jedinične matrice 1_n.

$\longrightarrow$ Na taj način u *zapisu svake matrice stoji u njenim stupcima zapisano u što su prevedeni vektori jedinične matrice*! I obrnuto, ako znamo nove položaje jedinične matrice $1(n)$, znamo time i svako preslikavanje što ga matrica ima izvesti u prostoru.

Tako npr. rotacija za kut φ u pozitivnom smislu dovodi tačke (0, 1) i (1, 0) ravnine u položaj $(\cos\varphi, \sin\varphi)$, $\left(\cos\left(\frac{\pi}{2}+\varphi\right), \sin\left(\frac{\pi}{2}+\varphi\right)\right)$.

Pisano u stupcima, znači to:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \to \begin{bmatrix} \cos\varphi \\ \sin\varphi \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \to \begin{bmatrix} -\sin\varphi \\ \cos\varphi \end{bmatrix} = [\sin\varphi, \ \cos\varphi]^T,$$

pa

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \to \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} = a.$$

Dobiva se matrica a, koja će svaki vektor $\begin{bmatrix} x \\ y \end{bmatrix}$, tj. svaku tačku (x, y) ravnine prevesti u tačku $a\begin{bmatrix} x \\ y \end{bmatrix}$ rotirajući je za φ oko 0.

Tako npr. matrica [2] znači preslikavanje koje matricu [1], tj, broj 1, dovodi u [2], tada će za svaki drugi broj x tim preslikavanjem preći u $[2]\,x$, tj. u $2x$. Na taj način matrični zapis [2] znači funkciju $x \to 2x$. Pridruživanje $x \to 2x$ i matrično množenje $[2]x$ su ravnopravni.

7. DVIJE SPECIFIČNE ULOGE MATRICA

7.1. Uzmimo najjednostavniji primjer da se vidi ideja. Zadana je matrica $a=[2]$ i veza

$$x' = ax. \tag{1}$$

x i x' su brojevi, dakle specijalni „vektori".

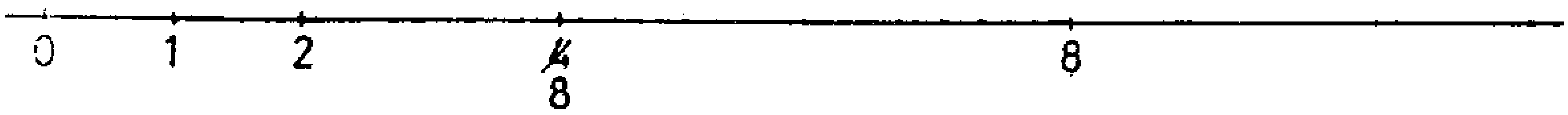
7.1.1. Relaciju (1) možemo u prvom redu protumačiti funkcionalno: matrica a pridružuje vektoru x vektor x'; radi se o funkciji ili preslikavanju $x \to ax$.

7.1.2. D r u g a i n t e r p r e t a c i j a: relacija (1) predstavlja vezu između *stare* koordinate (mjere) x i *nove* koordinate x' za *jednu te istu tačku*, pri čemu je, znači, odabrana druga baza (jedinica) e' umjesto bivše baze e; ali one su u vezi

$$ea^{-1} = e'. \tag{2}$$

Relacija (1) izlazi iz (2); i obratno. No, slike su drukčije.

Prvom relacijom (1) npr. element $x=4$ prelazi u element 8. U drugoj interpretaciji element sa značkom 4 dobiva značku 8: na shemi je precrtana stara značka i upisana nova značka.



Sl. 23.7.1.

7.2. Primjer rotacije u ravnini. Pogledajmo matricu

$$a(\alpha)=\begin{bmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{bmatrix}. \tag{3}$$

Odgovarajuće dvije interpretacije jesu:

(1) Prvo tumačenje (funkcionalno shvatanje): matrica $a(\alpha)$ je zapis preslikavanja koje značke (jedinične vektore) $\begin{bmatrix}1\\0\end{bmatrix}$, $\begin{bmatrix}0\\1\end{bmatrix}$ prevodi u stupac zadane matrice te svaku značku (vektor) $\begin{bmatrix}x\\y\end{bmatrix}$ prevodi u vektor $\begin{bmatrix}x'\\y'\end{bmatrix}$ multiplikativno po obrascu

$$\begin{bmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}x'\\y'\end{bmatrix}; \tag{4}$$

posebno npr. prevodi ona vektor

$$\begin{bmatrix}-5\\-2\end{bmatrix} \text{ u } \begin{bmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{bmatrix}\begin{bmatrix}-5\\-2\end{bmatrix}=\begin{bmatrix}-5\cos\alpha+2\sin\alpha\\ -5\sin\alpha-2\cos\alpha\end{bmatrix}.$$

(2) Drugo tumačenje (promjena baze): matrica je zapis ili značka nove koordinatne baze, koja iz stare nastaje vezom

$$ea=e',$$

tj.

$$[e_1,\ e_2]\,a(\alpha)=[e_1',\ e'],$$

odnosno

$$e_1\cos\alpha+e_2\sin\alpha=e_1'$$
$$e_1-\sin\alpha+e_2\cos\alpha=e_2'.$$

U slučaju da je polazna baza e ortonormirana (oba vektora po veličini jednaka 1 i okomita), onda se vidi da baza e' nastaje iz baze e *rotacijom* oko 0 za $\pi/2$ rad u pozitivnom smislu. To se dokazuje na osnovu matrice (3).

Kada je tako nova baza $e'=(e_1',\ e_2')$ fiksirana, uvest će se nova značka $\begin{bmatrix}x'\\y'\end{bmatrix}$ umjesto značke $\begin{bmatrix}x\\y\end{bmatrix}$ za svaku tačku na osnovu veze

$$\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{bmatrix}\begin{bmatrix}x'\\y'\end{bmatrix}. \tag{5}$$

Obje interpretacije matrice od osnovne su važnosti. Treba dobro razmisliti o prethodnom!

Dobro pogledati (4) i (5) i gledati na stvar kao na proces

$$\text{unos} \to \text{iznos}, \quad \text{podaci} \to \text{rezultat!}$$

U oba slučaja matrica je podatak koji se ubacuje npr. u računski stroj. U oba slučaja matrica je faktor, i to prvi faktor, pa se i to upiše u mašinu. No, u jednoj interpretaciji (4), faktor je „unos"; u drugoj interpretaciji, (5), matrice faktor je „iznos".

7.3. Primjer. U ravnini su, u odnosu na bazu $\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}$, markirana dva radijus-vektora e_1, e_2 i to kao stupci zadane matrice

$$a=\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}. \text{ Što dalje?}$$

Funkcionalna interpretacija: matrica a kao unos zajedno sa svakom tačkom T kao unosom daje $aT=T'$ kao proizvod ili iznos, sve provedeno u šiframa ili značkama. Tako npr. tačka $T=(1, 2)$, tj. tačka sa značkom $\begin{bmatrix}1\\2\end{bmatrix}$ prelazi u tačku kojoj je značka

$$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}1\\2\end{bmatrix}=\begin{bmatrix}7\\13\end{bmatrix}.$$

U drugoj interpretaciji tačka T ostaje na miru no dobiva značku $a^{-1}T=$ $=\begin{bmatrix}0\\1/2\end{bmatrix}$. U kombiniranoj interpretaciji, tačka T ostaje na miru, no mijenja joj se značka i sada glasi $\begin{bmatrix}7\\13\end{bmatrix}$. To znači da je izabrana druga baza e' umjesto bivše baze $e=e_1, e_2$ kojoj pripada matrica $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$. Novu bazu čine stupci matrice

$$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}^{-1}=\frac{1}{2}\begin{bmatrix}4 & -2\\-5 & 3\end{bmatrix}=\begin{bmatrix}\underbrace{\begin{matrix}2\\-\frac{5}{2}\end{matrix}}_{e_1'} & \underbrace{\begin{matrix}-1\\\frac{3}{2}\end{matrix}}_{e_2'}\end{bmatrix}.$$

7.4. Tako je i u općem slučaju.

Korisno se naučiti i funkcionalnom shvatanju matrice i shvatanju u vezi s koordinatnim bazama. A još najplodnije shvatanje je ono kombinirano: izbor nove baze e' (umjesto stare baze e) izaziva i promjene u označivanju i transformaciji prostora, tako da svakom vektoru v pridijelimo onaj na koji prelazi dosadašnja značka od v.

Sve su to oblici matematičke relativnosti.

8. TIPIČAN SLUČAJ POJAVLJIVANJA MATRICE: DISTRIBUTIVNO MNOŽENJE VEKTORA. RAZNE ALGEBRE

8.0. Već smo se u poglavlju 13, § 3. upoznali s raznim slučajevima vektora koji nisu usmjerene duži (isp. pogl. 13, § 2). Zbrajanje i oduzimanje s vektorima odvija se na jednostavan način; također množenje vektora skalarom.

8.1. No, što će biti ako dva vektora pomnožimo međusobno? Radimo u nekoj bazi e. Skicirajmo u ravnini osnovne vektore e_1, e_2[1]; recimo da imamo dva vektora

(1) $$v = 2\,e_1 + 3\,e_2.$$

(2) $$v' = 4\,e_1 - 5\,e_2.$$

Ako formalno računamo kao da radimo s polinomima, ali ipak pazeći na poredak osnovnih vektora, imat ćemo

$$vv' = (2\,e_1 + 3\,e_2)\,(4\,e_1 - 5\,e_2) = (\text{distribucija prema lijevo}) =$$
$$= (2\,e_1)\,(4\,e_1 - 5\,e_2) + (3\,e_2)\,(4\,e_1 - 5\,e_2) = (\text{distribucija prema desno}) =$$
$$= ((2\,e_1 \cdot 4\,e_1) + (2\,e_1 \cdot -5\,e_2)) + ((3\,e_2 \cdot 4\,e_1) + (3\,e_2 \cdot -5\,e_2)) = (\text{komutacija i}$$
$$\text{asocijacija skalara}) = 8\,(e_1 \cdot e_1) - 10\,e_1\,e_2 + 12\,e_2\,e_1 - 15\,e_2\,e_2.$$

Dalje ne znamo! Ne znamo jer nije definirano

(3) $$e_1\,e_1,\ e_1\,e_2,\ e_2\,e_1,\ e_2\,e_2.$$

Ako znamo što znači niz (3), onda možemo ići dalje; treba znati *tablicu ili matricu množenja osnovnih vektora.*

8.2. Tablica množenja vektora. Evo nekoliko takvih tablica:

	e_1	e_2
e_1	1	0
e_1	0	1

Tablica 1.

	e_1	e_2
e_1	e_1	e_2
e_2	e_2	$-e_1$

Tablica 2.

	e_1	e_2
e_1	0	1
e_2	-1	0

Tablica 3.

	e_1	e_2
e_1	1	1
e_2	1	1

Tablica 4.

	e_1	e_2
e_1	5	13
e_2	17	40

Tablica 5.

	e_1	e_2
e_1	e_1	e_1
e_2	e_2	e_2

Tablica 6.

	e_1	e_2
e_1	e_2	0
e_2	0	e_1

Tablica 7.

itd.

Danas, kad imamo vrlo raznolike strojeve za „računanje", jasno nam je da stroju moramo „reći" kako će množiti osnovne vektore, ako želimo da uopće vektore množi. Ta je tablica neophodan uslov za njegov dalji rad.

---

[1] Na višem stupnju lakše je definirati kompleksne brojeve nego ravninu. Isto tako, lakše je definirati tijelo realnih brojeva nego pravulju ili pravac. Pravulja može biti ilustracija i ideja vodilja da se definira R, no poslije toga treba R da posluži da se definira pravulja, ravnina itd. (isp. § 8.7).

8.3. Skalarno množenje vektora u »ortonormiranoj bazi«. Po tablici 1. kao „unos" stroj će dati ovaj proizvod:

$$(2\,e_1 - 3\,e_2)(4\,e_1 + 6\,e_2) = 8 + 18;$$

općenito

$$(v_1\,e_1 + v_2\,e_2)(v_1'\,e_1 + v_2'\,e_2) = v_1\,v_1' + v_2\,v_2',$$

odnosno općenito:

$$\sum v_k\,e_k \cdot \sum v'_k\,e_k = \sum_k v_k\,v'_k,$$

to je obično *skalarno množenje* u *»ortonormiranoj bazi«*.

Osnovna dijadska tablica u tom množenju je jedinična matrica

$$\begin{array}{c|cc} & e_1 & e_2 \\ \hline e_1 & 1 & 0 \\ e_1 & 0 & 1 \end{array}.$$

8.4. Kompleksni brojevi. Po tablici 2. množenja stroj će dati rezultat

$$(2\,e_1 + 3\,e_2)(4\,e_1 + 6\,e_2) = -10\,e_1 + 24\,e_2;$$

općenito

$$(v_1\,e_1 + v_2\,e_2)(v_1'\,e_1 + v_2'\,e_2) = (v_1\,v_1' - v_2\,v_2')\,e_1 + (v_1\,v_2' + v_2\,v_1')\,e_2, \quad \text{itd.}$$

Tako će npr. stroj, radeći po tablici 2, moći davati rezultate, a čovjek koji stvar razumije, moći će njene rezultate odmah prenositi na množenje kompleksnih brojeva. Naime, preslikavanje

$$e_1 \to 1$$

$$e_2 \to i$$

prevodi drugu tablicu množenja na tablicu

$$\begin{array}{c|cc} & 1 & i \\ \hline 1 & 1 & i \\ i & i & -1 \end{array}.$$

Na taj način specijalno vidimo da, radeći po tablici 2. u ravnini, ravnina postaje zapravo jedan zapis, odnosno realizacija množine svih kompleksnih brojeva; specijalno, svi realni brojevi zapisani su na pravulji $e_1 R$, a svi imaginarni brojevi na pravulji $e_2 R$. Naravno, kudikamo je najjednostavnije odabrati e_1 i e_2 „jednako daleko" od O i međusobno okomito; itd.

8.5. Vidimo kako možemo imati proizvoljno mnogo množenjâ vektorâ. Tako bi se npr. za vježbu moglo ispitati koliko ima raznih množenja vektora ako osnovna tablica množenja prima vrijednosti jedino u skupu

$$\{0,\ 1,\ -1,\ e_1,\ e_2,\ \ldots,\ e_m\}.$$

8.6. *Vektorski produkt tročlanih vektora* (isp. 2.6. § 13). Primijetimo da u slučaju tročlane baze e_1, e_2, e_3 tablica množenja

	e_1	e_2	e_3
e_1	0	e_3	$-e_2$
e_2	$-e_3$	0	e_1
e_3	e_2	$-e_1$	0

Opis: $e_1 \times e_2 = e_3$, dalje ciklički i antikomutativno; tablica je antisimetrična.

daje tzv. *vektorsko množenje vektora* kojima su koeficijenti realni brojevi. Tako izlazi da je vektorski kvadrat svakog vektora 0, da je $a \times b = -b \times a$, itd.

Geometrijsko značenje. Za obične geometrijske vektore vektorski produkt dvaju vektora znači veličinu orijentiranog paralelograma što ga određuju ta dva vektora; orijentaciju daje *prvi* faktor; produkt zamišljamo kao vektor okomit na oba faktora, a smjer mu je takav da niz $a, b, a \times b$ daje desno orijentiran trijedar.

8.7. Kvaternioni. (isp. pogl. 17, § 13.5.6). U slučaju četveročlane baze;

$$1, e_1, e_2, e_3$$

nad tijelom R realnih brojeva posebno je poznata *kvaternionska tablica množenja*:

	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	-1	e_3	$-e_2$
e_2	e_2	$-e_3$	-1	e_1
e_3	e_3	e_2	$-e_1$	-1

Opis: 1 djeluje kao obično;

$$e_1 e_2 = e_3$$

i dalje ciklički;

$$e_1 e_2 = -e_2 e_1$$

i dalje ciklički.

Gornja tablica baze nije simetrična.

W. R. Hamilton (1805 — 1865), veliki irski matematičar.

Zanimljivo je da je kvaternione izmislio isti matematičar (Irac Hamilton; gl. sliku!) koji je prvi dao formalnu definiciju kompleksnih brojeva, i to kao vektorski prostor nad tijelom R realnih brojeva s definicijom množenja baze $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ po gornjoj tablici 2; pri tom se radi jednostavnosti stavlja $e_1 = 1$, $e_2 = i$.

Već gornjih nekoliko primjera pokazuje veliku prednost što je imamo služeći se matricama.

8.8. Dijadski produkt dvaju nizova. To je matrica svih produkata po jednog člana iz prvog niza i po jednog člana iz drugog niza. Tako se i tu pojavljuje matrica.

8.9. Zadaci o matricama u vezi sa raznim transformacijama i množenjima vektora

1. Zadan je izraz $I \equiv ax + by$; neka je $a = 3a' + 5b'$, $b = -2a' + 2b'$;

odredi brojeve t, u, v, z tako da bude

$$x = tx' + uy'$$
$$y = vx' + zy' \quad \text{te} \quad I = a'x' + b'y'.$$

2. Izreći slično pitanje za $I = u_1 x_1 + u_2 x_2 + u_3 x_3$

$$u_1 = 3u_1' - 4u_2' + 5u_3'$$
$$u_2 = 2u_1' - 3u_2' + u_3'$$
$$u_3 = 3u_1' - 5u_2' - u_3'.$$

2. Nađi kontragredijentnu matricu $a^{\sim} = (a^{-1})^T$ ovih matrica:

1) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, 2) $\begin{bmatrix} 3 & 5 \\ -1 & 4 \end{bmatrix}$, 3) $\begin{vmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{vmatrix}$, 4) $A, B, C, I, J, K,$

$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \xi, \beta_1, \beta_2, \beta_3, \beta_4$, (isp. 10 § 4.7. zad. 9, 10, 11).

4. Zadana je matica $a = \begin{bmatrix} 3 & -2 \\ 4 & 5 \end{bmatrix}$; šta je rezultat funkcionalne interpretacije a šta koordinatne interpretacije matrice a u odnosu na vektor ili tačku s koordinatama 2, 7? Crtaj!

5. Isto pitanje za matricu $a = \begin{bmatrix} 2 & 5 & 7 \\ 6 & 3 & 4 \\ 5 & -2 & -3 \end{bmatrix}$ i vektor $[2, 5, 8]^T$.

6. Isto pitanje za matricu $a = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 2 \\ 1 & 1 & 1 & -1 \\ 1 & 0 & -2 & -6 \end{bmatrix}$ i vektor $[2, 5, 8, 0]^T$.

7. Za bazu $e = (e_1, e_2)$ definirani su vektori $u = 3e_1 + 5e_2$, $v = -4e_1 + 2e_2$; nađi proizvode uv, vu tih dvaju vektora za svaku od 7 tablica množenja $e_i e_k$ iz § 8.2.

8. Nađi dijadski produkt:
1) niza 1, 2, 3 i niza 7, —2, 4; 2) nizova (a, b, c, d), (a', b', c', d').

9. Nađi 1) skalarni; 2) vektorski produkt vektora

$$u = 2e_1 - 3e_2 + 4e_3, \quad v = 3e_1 + 5e_2 - 6e_3;$$

ako je baza $e = [e_1, e_2, e_3]$ ortonormirana.

10. Zadani su ortonormirana koordinatna baza $e = (e_1, e_2, e_3)$ i vektori $u = 5e_1 - 6e_2 + 8e_3$, $v = e_1 + 2e_2 + 3e_3$; uzmemo li umjesto baze e bazu $e' = (e_2\, e_3\, e_1)$, u što prelaze vektori u, v? Koliko je
1) skalarni; 2) vektorski produkt dobivenih vektora u', v'?

11. Isto pitanje za bazu $e'' = (e_3, e_2, e_1)$.

12. Riješi zadatke u pogl. 25, § 2.11.7.

13. Nađi zbroj, diferenciju i proizvod ovih dvaju kvaterniona

$$u = 2 + 3e_1 - 5e_2 + 6e_3, \quad v = -2 + 5e_1 - e_2 + 3e_4$$

(isp. tablicu 8.7).

L i t e r a t u r a

Anđelić [3]; Birkhoff—Maclane [1]; Bourbaki [1]; Dubreil—Jacotin [1]; Gantmaher [2]; Kurepa S. [1]; Lichnerowicz [1]; Proskurjakov [1]; Zurmühl [1].

POGLAVLJE 24.

MATRIČNE FUNKCIJE. MINIMALNI MATRIČNI POLINOM

0. UVOD

U mnogim pitanjima matematike, fizike i drugih nauka i primjenâ dolazi se u priliku da se upotrebljavaju ne samo matrice nego i *matrične funkcije*. Formalno, polazeći od neke funkcije, $\lambda \to f\lambda$, među skalarima vrši se odgovarajući prelaz $a \to f a$ na matrice (i operatore) na što prirodniji način. Tako npr. znajući da je

$$e^{\lambda} = 1 + \frac{\lambda}{1} + \frac{\lambda^2}{2!} + \frac{\lambda^3}{3!} + \cdots \tag{1}$$

za svaki realni ili kompleksni broj, definira se ta relacija i onda kada λ znači kvadratnu matricu. Granični prelaz definira se na najprostiji mogući način: niz $F_0, F_1, \ldots$ matrica konvergira ako postoji matrica X sa svojstvom da za svako i, k vrijedi

$$\lim_{n} (F_n)_{ik} = X_{ik}.$$

Danas se specijalno češće srećemo sa simboličkim redovima oblika (1) i oblika

$$c_0 + c_1 a + c_2 a^2 + c_3 a^3 + \cdots$$

(Neumannovi redovi)[1].

U § 2.5.2. navest ćemo kako se $f a$ definira ***bez upotrebe graničnog procesa*** — pomoću tzv. *minimalnog polinoma* matrice a. Formalno, najjednostavnije bi bilo definirati $f a$ kao da je f skalar, tj. staviti

$$f \begin{bmatrix} a_{11} & a_{12} \cdots \\ a_{21} & a_{22} \cdots \end{bmatrix} = \begin{bmatrix} f a_{11} & f a_{12} \cdots \\ f a_{21} & f a_{22} \cdots \end{bmatrix}.$$

Tada se sva aditivna i multiplikativna svojstva funkcije f među skalarima prenose i na $f a$ među matricama: zbrajanje matrica i *koordinatno* množenje matrica (svaka komponenta iz jednog faktora množi se s *odgovarajućom* komponentom drugog faktora); ali su tada velike neprilike s tipičnom operacijom: matrično množenje („matrično tkanje" ili svinuto množenje).

[1] F. Neumann [Nojman] (1798—1895), njemački matematičar.

I izrazi od više matrica dolaze često u teorijskoj fizici. Principijelno možemo reći: *definicija izrazâ u kojima dolaze matrice vrši se na što prirodniji način,* ali treba bitno paziti na to da zakon komutacije za množenje više nije na snazi.

1. POJAM MATRIČNE FUNKCIJE

Već smo i dosad matricama pridijeljivali matrice. Npr.

$a \to -a$, $a \to \lambda a$, $a \to a - \lambda$ (λ skalar)

$a \to a^n$ (n redni broj)

$a \to a^T$ (transponirano)

$a \to \bar{a}$ (konjugirana)

$a \to a^* = \overline{a^T} = \bar{a}^I$

$a \to a^{-1}$, $a \to a^k$ (k cio broj ako je a kvadratna i regularna).

Nadalje smo kvadratnim matricama pridjeljivali važan skalar

$$a \to \det a.$$

1.1. Što je matrična funkcija? Sad možemo problem postaviti općenito: *matrici a pridijeliti matricu fa ili skalar fa; specijalno, pridijeliti matrici a matrične polinome u a.*

Definicija. *Matrična funkcija je svaka funkcija kojoj je oblast ili protuoblast ili oboje sastavljeno od matrica.*

Uopće, definicije se od riječi do riječi prenose na matrice, pa zato možemo i bez specifične definicije govoriti o određenim stvarima i funkcijama u oblasti matricâ.

1.2. *Jedan način za dobivanje matričnih funkcija.*

Ako imamo običnu ili skalarnu funkciju

(1) $$x \to f\,x,$$

tada je prva ideja koja se nameće — da se tu varijabla ili neodređenica x shvati da bude i (kvadratna) matrica! Nekad je taj proces sasvim jednostavan. Npr. ako f označuje algebarski polinom! Ako je, naime,

$$f\,x = f_0\,x^0 + f_1\,x + f_2\,x^2 + \cdots f_{n-1}\,x^{n-1} + f_n\,x^n, \quad n = \mathrm{st}\,f,$$

tada se tu uvijek umjesto x može staviti i kvadratna matrica kojoj su vrijednosti iz istog tijela odakle i koeficijenti f_i (jer se inače ne bi moglo množiti npr. $f_2\,x^2$ niti dodati skalar f_0).

Tako npr. za kvadratni polinom

(2) $$2\,x^2 - 3\,x + 5$$

možemo tu staviti umjesto x bilo koju kvadratnu matricu. Recimo da u (2) stavimo

$x=\begin{bmatrix}5 & 9\\ 3 & 4\end{bmatrix}$; onda skalari 2, -3, 5 postaju $\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}$, $\begin{bmatrix}-3 & \\ & -3\end{bmatrix}$, $\begin{bmatrix}5 & 0\\ 0 & 5\end{bmatrix}$,

pa (2) postaje

$$\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}\begin{bmatrix}5 & 9\\ 3 & 4\end{bmatrix}^2+\begin{bmatrix}-3 & \\ & -3\end{bmatrix}\begin{bmatrix}5 & 9\\ 3 & 4\end{bmatrix}+\begin{bmatrix}5 & \\ & 5\end{bmatrix}=\begin{bmatrix}94 & 135\\ 45 & 79\end{bmatrix}.$$

Mnogo je zamršenija stvar s funkcijama koje nisu polinomi. Što bi npr. bilo $\cos\begin{bmatrix}5 & 9\\ 3 & 4\end{bmatrix}$?

1.3. Osnovno pitanje o starim vezama. Postavlja se također osnovno pitanje:

Ako na gornji način od skalarnih izraza i funkcija sagradimo odgovarajuće stvari u oblasti matrica, da li će stare identične veze ostati na snazi i u novoj oblasti?

1.3.1. Npr. u području skalara (brojeva) i funkcija imamo identitete

(3) $$\cos^2 x+\sin^2 x=1 \qquad \text{ili}$$

(4) $$(x-y)(x+y)=x^2-y^2.$$

Hoće li te veze vrijediti i u oblasti kvadratnih matrica?

1.3.2. Pogledajmo, npr. (4) i množimo kao da se radi o matricama x, y:

(4) $$=(x-y)\,x+(x-y)\,y=(x^2-y\,x)+(x\,y-y^2)=$$

$$=x^2+(-y\,x+x\,y)-y^2=(\text{asoc. i kom. za }+),\text{ tj.}$$

(5) $$(x-y)(x+y)=(x^2-y^2)+(x\,y-y\,x).$$

Isporeďivanjem (4) i (5) vidimo ovo:

(6) $$(x-y)(x+y)=x^2-y^2 \Leftrightarrow x\,y=y\,x.$$

Prema tome, već i najelementarnija formula iz obične algebre ne prenosi se bez ograničenja na matričnu algebru. Zato se pri prelazu na matrične izraze svaki put mora preispitati da li stare veze ostaju i dalje na snazi (inače ćemo često nastojati da sačuvamo valjanost starih veza i u novoj oblasti — po principu permanencije).

Npr. kod (6) smo naišli na uslov komutativnosti za množenje.

$\longrightarrow$ **1.4.** Teorem. *Svaki algebarski identitet vrijedi i za komutativne kvadratne konačne matrice. Specijalno, svaki algebarski identitet u jednoj neodređenici prenosi se i na svaku kvadratnu konačnu matricu.*

Tako npr. znamo za fundamentalni algebarski identitet: faktorizacija polinoma p:

(F) $$p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_n x^n =$$

$$= p_n \cdot (x - p_{(1)})(x - p_{(2)}) \cdot \ldots \cdot (x - p_{(n)}), \quad n = \mathrm{st}\, p \neq 0,$$

kraće

$$p(x) = \sum_{m=0}^{n} p_m x^m = p_{\mathrm{st}\, p} \prod_{m=1}^{n} (x - p_{(m)}), \quad n = \mathrm{st}\, p.$$

Prema tome, p_m je koeficijent, a $p_{(m)}$ je nula-mjesto (ništište) polinoma.

Prema gornjem teoremu, može u algebarskom identitetu (F) za faktorizaciju značiti x ne samo svaku realnu neodređenicu x nego i matricu; naravno da su koeficijenti i nula-mjesta vezani Newtonovim obrascima (pogl. 19, § 2.2.2).

Gornji teorem 1.4. posljedica je valjanosti ovih elementarnih ekvivalencija. Za polinome f, g, h vrijedi:

$$f(x) = g(x) \qquad \Leftrightarrow f(a) = g(a) \qquad \text{za matrice}$$

$$f(x) = g(x) + h(x) \Leftrightarrow f(a) = g(a) + h(a)$$

$$f(x) \equiv g(x)\, h(x) \quad \Leftrightarrow f(a) = g(a)\, h(a).$$

Lijevo, x označuje svaki realni broj (ili kompleksni broj); desno, a označuje svaku realnu (kompleksnu) matricu.

Zadovoljimo se da dokažemo prvu relaciju. Najprije je $\mathrm{st}\, f = \mathrm{st}\, g = n$; dalje je $f_0 = g_0, \ldots, f_n = g_n$; odatle izlazi $f_0 a = g_0 a, \ldots, f_n a = g_n a$, dakle i $\Sigma f_i a^i = \Sigma g_i a^i \,(i \leq n)$, tj. $f a = g a$, itd. Obrat isto vrijedi: iz $f a = g a$ izlazi $f x = g x$, itd.

1.5. Primjer.

(1) $$(a + a^{-1})^n = a^n + \binom{n}{1} a^{n-2} + \binom{n}{2} a^{n-4} + \cdots + a^{-n}.$$

Ako stavimo posebno

$$a = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix},$$

lako se vidi da je

$$a + a^{-1} = \begin{bmatrix} 2\cos\varphi & 0 \\ 0 & 2\cos\varphi \end{bmatrix}, \qquad a^m = \begin{bmatrix} \cos m\varphi & -\sin m\varphi \\ \sin m\varphi & \cos m\varphi \end{bmatrix}$$

$$m = 0, \ \pm 1, \ \pm 2, \ldots$$

Stavimo li to u (1) pa izjednačimo članove na dijagonali, dobivamo poznatu formulu

$$2^n \cos^n \varphi = \sum_{k=0}^{n} \binom{n}{k} \cos(n-2k)\varphi =$$

$$= 2\left(\cos n\varphi + n\cos(n-2)\varphi + \frac{n(n-1)}{2!}\cos(n-4)\varphi + \cdots\right.$$

$$+ \cdots) + \binom{n}{\frac{n}{2}} \cos 0 \text{ za parno } n,$$

$$\left. + \cdots + \binom{n}{\frac{n-1}{2}} \cos\varphi\right) \text{ za neparno } n.$$

2. MINIMALNI POLINOM VEZAN ZA ZADANU MATRICU

2.1. Problem. Prvo, grubo rješenje. Neka je a zadana kvadratna matrica; tada imamo i matrice

$$a^0 = \text{jedinična matrica } 1_n, \text{ ako je st } a = n, \text{ te matrice}$$

(1) $$a^1 = a,\ a^2,\ a^3, \ldots$$

Nastaje ovaj problem: može li se koji član a^s niza (1) prikazati kao kombinacija članova s manjim indeksom; dakle:

(2) $$a^s = c_0 + c_1 a + c_2 a^2 + \cdots + c_{s-1} a^{s-1}$$

i da se koeficijenti c_i mogu iz vrijednosti a_{ik} matrice dobiti elementarno (konačan broj prve četiri operacije!)?

Problem zaista izgleda takav da je odgovor: da!

Evo obrazloženja. Matrica a je data. Zato su poznate i vrijednosti — njih n^2 na broju — za svaku matricu a^s; to znači da je dovoljno u (2) promatrati slučaj $s = n^2$ pa da iz pripadnih n^2 jednadžbi

(3) $$(a^s)_{ik} = \delta_{ik} c_0 + a_{ik} c_1 + (a^2)_{ik} c_2 + \cdots + (a^{s-1})_{ik} c_{s-1} \quad (i, k = 1, 2, \ldots, n; s = n^2)$$

nađemo nepoznate koeficijente c_i.

Sistem (3) je sistem linearnih jednadžbi za nepoznanice c_i; koeficijenti nepoznanica i lijeva strana u (3) jesu veličine koje se iz zadanih veličina a_{ik} dobivaju pomoću prve tri računske operacije. Znači da se traženi koeficijenti u (2) dobivaju elementarno iz vrijednosti zadane matrice a.

Sistem (3) ima rješenje. On naime proističe iz (2), a veza (2) stoji jer za $s \geq n^2$ matrice $a^0, a^1, a^2, \ldots, a^s$ linearno su zavisne, pa se mogu naći koeficijenti $c_0, c_1, \ldots, c_{s-1}$ za koje (2) postoji. *Q.E.D.*

Međutim, gornje rješenje problema vrlo je grubo: stepen n^2 je previsok, kao što ćemo odmah vidjeti. Ali u svakom slučaju jednadžba (2) pokazuje da matrica a zadovoljava neku *algebarsku* jednadžbu s koeficijentima iz tijela što ga određuju vrijednosti a_{ik}.

2.2. Definicija minimalnog polinoma matrice. Minimalni polinom kvadratne matrice *a je prvi normirani polinom* (najstariji koeficijent $=1$) nad tijelom što ga rađaju veličine a_{ik} i koji polinom matrica a poništava. Minimalni polinom označit ćemo sa $\mu(a;\lambda)$; λ je neodređenica ili varijabla.

Minimalni polinom je jednoznačno određen: i po stepenu i po koeficijentima. Znači, $\mu(a;a)=0$, $p(a;a)\neq 0$ za svaki polinom p stepena $<\operatorname{st}\mu$.

2.3. Teorem. *Svaki polinom $p(\lambda)$ nad tijelom komponenata matrice a i za koji je $p(a)=0$ kratnik je minimalnog polinoma μ.*

Naime, po osnovnom teoremu o diobi polinoma, jednoznačno su određeni: kvocijent q i ostatak r, za koje je

$$p(\lambda)=\mu(\lambda)\,q(\lambda)+r(\lambda),\quad \operatorname{st} r<\operatorname{st}\mu \text{ ili } r=0. \tag{4}$$

Tvrdnja: $r=0$. U obratnom slučaju iz (4) izlazi

$$r(a)=p(a)-\mu(a)\,q(a)=0 \text{ i } \operatorname{st} r<\operatorname{st}\mu,$$

protivno definiciji od μ.

2.4. U potrazi za minimalnim polinomom μ. Već najjednostavnija matrična funkcija

$$a\rightarrow a+\lambda \text{ ili } a\rightarrow \lambda-a \qquad (\lambda \text{ skalar})$$

dovodi do zanimljivog polinoma u λ, naime do mnogočlana $\det(\lambda-a)$, tj.

$$\begin{vmatrix} \lambda-a_{11} & -a_{12} & \cdots & -a_{1n} \\ \cdot & \cdot & \cdots & \cdot \\ -a_{n1} & -a_{n2} & \cdots & \lambda-a_{nn} \end{vmatrix}. \tag{5}$$

Stepen mu je n. Da slučajno njega matrica a ne poništava? Naime, očigledno matrica λ poništava binom $a-\lambda$ kad se tu stavi a umjesto λ.

2.4.1. Definicija karakterističnog ili svojstvenog polinoma[1] Polinom (5) zove se *karakteristični ili svojstveni polinom matrice a*; označit ćemo ga također sa $\varkappa(a,\lambda)$ te $a(\lambda)$; dakle:

$$\varkappa(a,\lambda):=\begin{vmatrix} \lambda-a_{11} & -a_{12} & \cdots & -a_{1n} \\ \cdot & \cdot & \cdots & \cdot \\ -a_{n1} & \cdot & \cdots & \lambda-a_{nn} \end{vmatrix}=:a(\lambda).$$

To je osnovni polinom! Gradnja mu je jednostavna, bar formalno: u matrici $-a$ dodati po dijagonali neodređenicu λ i onda uzeti operator determinante. Karakteristični polinomi zauzimaju u matematici jedan od nekoliko ključnih položaja.

---

[1] Vrlo se često umjesto (5) polinom $\det(a-\lambda)$ naziva *karakteristični* polinom. Iz teksta će se vidjeti da li ćemo mi to ili (5) misliti pod nazivom »karakteristični polinom«. Jedan oblik iz drugog izlazi množenjem sa $(-1)^n$. Važno je da su nula-tačke iste i za jedan i za drugi oblik.

2.4.2. Vlastite ili svojstvene vrijednosti matrice jesu nula-tačke njenog karakterističnog polinoma. To su, dakle, rješenja u λ jednadžbe $\varkappa(a;\lambda)=0$. Koliko li je važan spektar karakterističnog polinoma! O tome ćemo se uvjeriti u toku daljeg izlaganja! (isp. pogl. 26, § 12.6).

2.4.3. Pimjer kvadratnih matrica. Za kvadratnu matricu a formata (2, 2) karakteristični polinom izgleda

$$\varkappa(a;\lambda)=\begin{vmatrix} \lambda-a_{11} & -a_{12} \\ -a_{21} & \lambda-a_{22} \end{vmatrix}=\lambda^2-(a_{11}+a_{22})\lambda+(a_{11}a_{22}-a_{12}a_{21}),$$

pa je

$$\varkappa(a;a)=\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}^2-\begin{bmatrix} (a_{11}+a_{22})a_{11} & (a_{11}+a_{22})a_{12} \\ (a_{11}+a_{22})a_{21} & (a_{11}+a_{22})a_{21} \end{bmatrix}+$$

$$+\begin{bmatrix} a_{11}a_{22}-a_{12}a_{21} & 0 \\ 0 & a_{11}a_{22}-a_{12}a_{22} \end{bmatrix}=$$

$$=\begin{bmatrix} a_{11}{}^2+a_{12}a_{21} & a_{11}a_{12}+a_{12}a_{22} \\ a_{21}a_{11}+a_{22}a_{21} & a_{21}a_{12}+a_{22}{}^2 \end{bmatrix}+\begin{bmatrix} -a_{11}{}^2-a_{12}a_{21} & -(a_{11}+a_{22})a_{12} \\ -(a_{11}+a_{22})a_{21}-a_{22}{}^2-a_{12}a_{21} \end{bmatrix}=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}=0.$$

Dakle, ako je $\operatorname{st} a=2$, tada je $\varkappa(a,a)=0$.

Zaključak je ispravan i za druge kvadratne matrice; to je sadržina:

—→ Teorem **2.4.4. Hamilton-Cayleyev teorem.** *Svaka kvadratna matrica a konačne oblasti poništava svoj karakteristični polinom* $\varkappa(a;\lambda)$[1], tj.

(1) $$\varkappa(a;a)=0(n),$$

gdje je $0(n)$ konstantna kvadratna matrica 0 reda n.

Međutim, vrijedi još općenitiji teorem, kao što ćemo odmah dokazati.

—→ **2.4.5.** Teorem. *Ako kvadratna matrica a konačna reda n zadovoljava matričnu jednadžbu*

(2) $$p(x)=\sum_{r\leqslant s} p_r x^r=0(n),$$

gdje su p-ovi kvadratne matrice stupnja n, tada matrica a zadovoljava i jednadžbu

(3) $$\det p(x)=0,\quad \text{tj. } p(a)=0(n) \Rightarrow \det p(x)_{x=a}=0. \text{ (isp pogl. 27, § 5.3).}$$

Dokaz (za dokaz teorema 2.4.4. čitati ovdje svuda $a-\lambda$ umjesto $p(\lambda)$). Najprije, kako je u odnosu na x, svaki član *matrice* $p(x)$ stupnja $\leq s$, bit će opći član *determinante* od $p(x)$, prema x, stupnja $\leq ns$; naime, opći član determinante $(3)_1$ dobije se kao determinanta produkta određenih članava polinoma — matrice $p(x)$. Pa neka je

(4) $$\det p(x)=\sum l_k x^k,\quad (k\leq ns).$$

---

[1] Hamilton je teorem dokazao za kvaternione, a Cayley [Kejli] za slučaj $n=2$, 3 s napomenom da je u općem slučaju dokaz isti.

U drugu ruku, promatrajmo adjunktu $Ap(x)$ matrice $p(x)$; elementi matrice $Ap(x)$ jesu algebarski minori stupnja $n-1$ matrice $p(x)$; kako su elementi matrice $p(x)$ prema (2) polinomi u x stupnja $\leq s$, to će adjunkta $Ap(x)$ biti s obzirom na x polinom stupnja $\leq (n-1)s$, recimo

(5) $$Ap(x) = \sum_{r'} p'_{r'} x^{r'}, \quad (0 \leq r' \leq s(n-1))$$

gdje su $p'_{r'}$ određene matrice reda n.

No, uvijek je (pogl. 12, § 4.3):

(6) $$Ap(x) \cdot p(x) = \operatorname{diag}(\det p(x)).$$

S obzirom na (2), (4) i (5) to znači da za svaki skalar x vrijedi

$$\sum_{r'} p_{r'} x^{r'} \sum_{r \leqslant s} p_r x^r = \sum_k l_k x^k \quad (r' \leq (n-1)s, \quad k \leq ns),$$

tj.

(7) $$\Big(\sum_{r' \leqslant (n-1)s} p'_{r'} \big(\sum_{r \leqslant s} p_r x^r\big)\Big) x^{r'} = \sum_{k \leqslant ns} l_k x^k,$$

odnosno — jer je x skalar —

(8) $$\sum_{r'} p'_{r'} p(x) x^{r'} = (\det p(x))(n)$$

(za skalar z npr. za $z = \det p(x)$ znači $z(n)$ odgovarajuću skalarnu matricu reda n).

Iz identiteta (7) s obzirom na x proizlazi jednakost koeficijenta od x^k u $(7)_1$ i u $(7)_2$, i to za svako $0 \leq k \leq ns$. Ispišemo li sve te jednakosti za $k = 0, 1, \ldots, ns$ pa ih po redu množimo zdesna matricama a^k $(k = 0, 1, \ldots, ns)$ i dobivene jednakosti saberemo, proizlazi jednakost slična sa (7), odnosno (8), samo što umjesto x dolazi promatrana matrica a:

$$\sum_{r'} p'_{r'} p(a) a^{r'} = (\det p(x))_{x=a}.$$

Kako je po pretpostavci $p(a) = 0$, to znači da je $(\det p(x))_{x=a} = 0$, što je i trebalo dokazati.[1)]

2.4.5.1. Primjedba. Teorem 2.4.4. a time ni teorem 2.4.5. ne moraju biti ispravni za matrice beskonačne oblasti. Tako npr. matrica S iz pogl. 12, § 6.5.4. ne zadovoljava nikoji polinom $p(x) = 0$.

2.4.6. Pobliže o minimalnom polinomu matrice. Prva procjena o minimalnom polinomu $\mu(a; \lambda)$ matrice a da mu je stupanj $\leq n^2$, $n = \operatorname{st} a$, sada se znatno popravila: $\operatorname{st} \mu \leq \operatorname{st} a$. Međutim, prema § 2.3, polinom $\mu(a; \lambda)$ je djelitelj karakterističnog polinoma $\varkappa(a, \lambda)$, i to potpuno određen djelitelj (naime, polinom $\mu(a, \lambda)$ smo normirali).

---

1) Dokaz je sličan Frobeniusovu, a Frobenius ideju dokaza pripisuje Paschu [Paš].

2.4.7. Teorem. Ako je $\sigma a = \{\lambda_1, \lambda_2 \ldots \lambda_m\}$ skup rješenjâ λ algebarske jednadžbe $\varkappa(a; \lambda) = 0$, tada svakom indeksu $m' = 1, 2, \ldots, m$ pripada određeni broj $m_{m'}$, tako da bude

$$\mu(a; \lambda) = (\lambda - \lambda_1)^{m_1} (\lambda - \lambda_2)^{m_2} \cdots (\lambda - \lambda_m)^{m_m},$$

tj.

$$\mu(a; \lambda) = \prod_{m'=1}^{m} (\lambda - \lambda_{m'})^{m_{m'}},$$

pa je $\mu(a, \lambda)$ određen divizor od $\varkappa(a, \lambda)$.

U tom iskazu sve je jednoznačno! Naime, jednoznačno je određen skup σa; njegov glavni ili kardinalni broj je broj nejednakih prostih faktora polinomâ μ, $\varkappa$. Naime, oba ova polinoma imaju iste linearne normirane djelitelje, ali su im, eventualno, različite kratnosti.

2.4.8. Norma matrice. — 2.4.8.1. Definicija. Konstantni član u minimalnom polinomu matrice a zove se *norma matrice a* i označuje sa $N(a)$ ili Na.

2.4.8.2. Teorem. *Za svaku kvadratnu matricu konačnog poretka vrijedi*

$$\det a = 0 \Leftrightarrow Na = 0.$$

Stvarno, konstantni član u $\det(\mu - a)$ je $(-1)^{\mathrm{por}\, a} \det a$; Na je konstantni član u $\mu(a, \lambda)$; zato prema teoremu 2.4.7. vrijedi

$$(-1)^{\mathrm{por}\, a} \det a = 0 \Leftrightarrow N(a) = 0.$$

Iz te ekvivalencije neposredno izlazi teorem 2.4.8.2.

2.4.9. Teorem. (Frobenius, 1878). *Minimalni polinom $\mu(\lambda, a)$ matrice a je kvocijent karakterističnog polinoma te matrice i najveće zajedničke mjere $f(\lambda)$ svih minora reda $n-1$ matrice $\lambda - a$.*

Dokaz. Promatrajmo polinom

$$g(\lambda) = \frac{\varkappa(a, \lambda)}{f(\lambda)}. \tag{1}$$

Izlučimo li iz matrice — adjunkte $A(\lambda - a)$ najveći zajednički faktor $f(\lambda)$, pa napišemo li

$$A(\lambda - a) = f(\lambda) \cdot b(\lambda), \tag{2}$$

tada je $b(\lambda)$ određena matrica kojoj elementi imaju jedino konstante kao zajedničku mjeru.

No,

$$(\lambda - a)\, A(\lambda - a) = (\det(\lambda - a))\,(n) = \mathrm{diag}\,(\det(\lambda - a)),$$

što zbog (2) postaje

$$(\lambda - a) f(\lambda)\, b(\lambda) = \varkappa(a; \lambda)\ (n). \tag{3}$$

No, polinom $\det(\lambda - a)$ kao linearna forma aglebarskih komplemenata reda $n-1$ matrice $\lambda - a$, tj. kao linearna forma elemenata adjunkte $A(\lambda - a)$, djeljiv je sa $f(\lambda)$, pa iz (3) izlazi da je

$$(\lambda - a)\, b(\lambda) = \frac{\varkappa(a; \lambda)}{f(\lambda)}\,(n) = g(\lambda)\ (n)$$

određen polinom $g(a; \lambda)$, koji matrica a poništava; to prema 2.3. znači da je polinom $g(\lambda)$ djeljiv sa $\mu(a; \lambda)$. Sad još treba dokazati da je i obratno polinom $\mu(\lambda)$ djeljiv sa $g(\lambda)$. Očigledno se može napisati identitet

$$\mu(\lambda)-\mu(x)=(\lambda-x)\,p(\lambda, x), \tag{4}$$

gdje je $p(\lambda, x)$ neki polinom u λ i x; za $x=a$ prelazi (4) u

$$\mu(\lambda)-\mu(a)=(\lambda-a)\,p(\lambda, a),$$

odakle zbog $\mu(a)=0$ (naime $u(\lambda)=\mu(a, \lambda)$ minimalni je polinom od a) proizlazi

$$\mu(\lambda)=(\lambda-a)\,p(\lambda, a). \tag{5}$$

Množeći slijeva tu jednakost sa $f(\lambda)\,b(\lambda)\equiv A(\lambda-a)$ s obzirom na (2) izlazi

$$f(\lambda)\,b(\lambda)\,\mu(\lambda)=A(\lambda-a)(\lambda-a)\,p(\lambda, a),$$

odnosno zbog $A(\lambda-a)(\lambda-a)\equiv\det(\lambda-a)(n)=f(\lambda)\,g(\lambda)$:

$$f(\lambda)\,b(\lambda)\,\mu(\lambda)=f(\lambda)\,g(\lambda)\,p(\lambda, a).$$

Kako je $f(\lambda)\not\equiv 0$, izlazi odatle dijeljenjem sa f:

$$b(\lambda)\,\mu(\lambda)=g(\lambda)\,p(\lambda, a). \tag{6}$$

Jednakost (6) iskazuje da je matrica $b(\lambda)\,\mu(\lambda)$ djeljiva sa $g(\lambda)$, tj. da je svaki njen član djeljiv polinomom g; kako su elementi matrice b međusobno prosti, to znači da je $\mu(\lambda)$ djeljivo sa $g(\lambda)$, za čim i idemo. Time je teorem potpuno dokazan.

2.5. Opće matrične funkcije. — 2.5.1. U § 2.3. pokazali smo da za algebarske polinome $p(\lambda)$ i matricu a relacija $p(a)=0$ ima za posljedicu da je $p(\lambda)$ djeljivo minimalnim polinomom $\mu(\lambda)$ matrice a. Specijalno, za koja god dva polinoma $p(\lambda)$, $q(\lambda)$ eventualna jednakost $p(a)=q(a)$ znači da je $p(a)-q(a)=0$, pa je zato razlika polinoma $p(\lambda)-q(\lambda)$ djeljiva sa $\mu(\lambda)$.

Na osnovu toga postavlja se

D e f i n i c i j a. *Za proizvoljnu funkciju $f(\lambda)$ s realnim ili kompleksnim argumentom definira se i vrijednost $f(a)$* (a je kvadratna matrica) *kao rezultat supstitucije $\lambda\to a$ u bilo kojoj običnoj funkciji $p(x)$ koja se u spektru minimalnog polinoma matrice a podudara sa f.*

Tu dolazi do izražaja pojam spektra polinoma i funkcije uopće.[1] Spektar S_μ minimalnog polioma $\mu\ (a, \lambda)$ ima $\operatorname{st}\mu=\sum m_{m'}$ članova podataka:

$$(S\mu(a)) \qquad \underbrace{\lambda_1, \lambda_1 \ldots}_{m_1}\ \underbrace{\lambda_2, \lambda_2 \ldots,}_{m_2}\ \underbrace{\ldots \lambda_m, \ldots, \lambda_m,}_{m_m}$$

[1] Znajmo da spektar $S_h=Sh$ polinoma $h(x)$ znači neuređen niz svih njegovih nula-mjestâ, pri čemu je svako nula-mjesto računato sa svojom kratnošću. Osim S_h promatramo i spektar bez ponavljanja σ_h i to kao skup sastavljen od svih članova iz S_h.

a u vezi s oblikom

$$\mu(\lambda) = \prod_{m'=1}^{m} (\lambda - \lambda_{m'})^{m_{m'}}$$

polinoma $\mu(\lambda)$ (isp. 2.4.7).

2.5.2. Lagrange-Sylvesterov polinom. No, uvijek ima algebarskih polinoma koji u spektru $S\mu$ imaju isto vladanje kao zadana funkcija f ukoliko je, naravno, f definirano na spektru S_μ, tj. ukoliko su određeni brojevi

$$(*) \qquad f(\lambda_1), f'(\lambda_1), \ldots f^{(m_1-1)}(\lambda_1), \ldots f(\lambda_m), f'(\lambda_m), \ldots f^{(m_m-1)}(\lambda_m)$$

i kao vrijednost funkcije i kao vrijednost njenih derivata.

Postojanje brojeva u $(*)$ za funkciju f upravo je uslov za definiranje značenja $f(a)$ za matricu a, kojoj je minimalni polinom onaj polinom kojem je spektar s ponavljanjem $=(*)$.

No, uvijek postoji polinom stepena $<\operatorname{st}\mu$, koji u spektru $S\mu$ ima vladanje $fS\mu$. To je tzv. Lagrange-Sylvesterov polinom L_f (isp. § 3.6).

2.5.3. Definicija od fa (f je zadana funkcija u realnom odnosno kompleksnom području; a je kvadratna konačna matrica). Vrijednost Lagrange-Sylvesterova polinoma $\lambda \to L_f(\lambda)$ u a proglašava se kao značenje fa, tj. stavlja se

$$fa := L_f(a).$$

Tu se lijeva strana definira desnom.

2.5.4. Sad je npr. jasno da je za svaku konačnu kvadratnu matricu a potpuno određena matrica

$$\cos a, \quad \sin a, \quad e^a, \quad e^{ia}, \quad \text{itd;}$$

također se može dokazati da za te matrične funkcije vrijede analogni obrasci i razvoji kao u realnom i kompleksnom području, npr.

$$e^a = 1 + a + \frac{a^2}{2!} + \frac{a^3}{3!} + \cdots + \cdots$$

3. Zadaci o minimalnim matričnim polinomima i matričnim funkcijama.

1. Uz kvadratnu matricu a reda n promatraj i niz $a^0 = 1(n), a, a^2, a^3 \ldots$; nađi bar jedan član a^r toga niza koji se može izraziti kao linearna kombinacija članova $a^{r'}$ sa $r' < r$; neka je matrica:

$$0)\begin{bmatrix}0&1\\0&0\end{bmatrix}, \quad 1)\begin{bmatrix}1&0\\0&1\end{bmatrix}, \quad 2)\begin{bmatrix}1&1\\0&0\end{bmatrix}, \quad 3)\begin{bmatrix}1&2\\3&4\end{bmatrix}, \quad 4)\begin{bmatrix}2&0\\0&2\end{bmatrix},$$

$$5)\ \operatorname{diag}[2,2,2], \quad 6)\begin{bmatrix}2&1&0\\0&2&1\\0&0&2\end{bmatrix}, \quad 7)\begin{bmatrix}0&0&1\\0&0&0\\0&0&0\end{bmatrix}, \quad 8)\begin{bmatrix}0&0&0\\0&1&0\\0&0&0\end{bmatrix}.$$

2. Napiši karakteristični polinom $\det(\lambda - a)$ matrica iz zad. 1 i provjeri da ga matrica a prevodi u nula-matricu.
3. Odredi minimalni polinom matrica iz zad. 1.
4. Odredi minimalni polinom $\mu(a; \lambda)$ za ove matrice a:

$$1)\ \operatorname{diag}[2, 2, 2, 2],\quad 2)\begin{bmatrix}3 & 1 & -1\\ 0 & 2 & 0\\ 1 & 1 & 1\end{bmatrix},\quad 3)\begin{bmatrix}4 & -2 & 2\\ -5 & 7 & -5\\ -6 & 6 & -4\end{bmatrix},\quad 4)\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},$$

$$5)\begin{bmatrix}0 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 0\end{bmatrix},\quad 6)\begin{bmatrix}0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\end{bmatrix},\quad 7)\begin{bmatrix}\alpha & 1 & 0 & \cdot & 0\\ 0 & \alpha & 1 & \cdot & 0\\ \cdot & \cdot & \cdot & \cdot & 0\\ \cdot & \cdot & \cdot & \cdot & \cdot\\ \cdot & \cdot & \cdot & \cdot & 1\\ 0 & 0 & 0 & \cdot & \alpha\end{bmatrix}.$$

5. (*Izračunavanje obratne matrice* a^{-1}). Nađi a^{-1} služeći se Cayley-Hamiltonovim teoremom množeći jednadžbu $\det(\lambda - a) = 0$, odnosno jednadžbu $\mu(a, \lambda) = 0$ sa a^{-1}. Provedi do kraja primjer ovih matrica:

$$1)\begin{bmatrix}2 & 1\\ 5 & 6\end{bmatrix},\quad 2)\begin{bmatrix}2 & 5 & 7\\ 6 & 3 & 4\\ 5 & -2 & -3\end{bmatrix},\quad 3)\begin{bmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 2\\ 1 & 1 & 1 & -1\\ 1 & 0 & -2 & -6\end{bmatrix},\quad 4)\begin{bmatrix}1 & & 1\\ & \ddots & \\ 0 & & 1\end{bmatrix}.$$

5'. Za regularne matrice a konačnog poretka vrijedi

$$a^{-1} = (N(a))^{-1}\, a^{-1}\, (\mu(a, a) - N(a));$$

time je a^{-1} predočeno kao polinom $p(a)$ stepena $\operatorname{st}\mu - 1$; pri tom je $\mu(a, \lambda)$ minimalni polinom matrice a; $N(a)$ je njegov konstantni član (Laguerre [Lager] 1867).

6. *Formule Frazer-Duncan* (č. Denkan) — *Collar* (č. Kolar). Neka je $p(\lambda)$ suma konvergentna reda ili polinom; neka je a kvadratna konačna matrica reda kojoj minimalni polinom ima n različnih karakteričnih nula-mjesta $\lambda_1, \lambda_2, \ldots \lambda_n$; tada Lagrange-Sylvesterov polinom postoji i jednak je običnom interpolacionom Lagrange-ovu polinomu; po definiciji, tada postoji i $p(a)$, pa je

$$(1)\qquad p(a) = \sum_{i=1} p(\lambda_i) \cdot g_i \text{ gdje je } g_i = \frac{\prod\limits_{k \neq 1} (\lambda_k - a)}{\prod\limits_{k \neq 1} (\lambda_k - \lambda_i)};$$

specijalno za potenciju $p(\lambda) = \lambda^r$ obrazac (1) daje ovu vrlo pogodnu formulu:

$$(2)\qquad a^s = \lambda_1^s g_1 + \lambda_2^s g_2 + \cdots + \lambda_n^s g_n.$$

1) Provjeri obrazac (1) za polinom $p(\lambda)=\lambda^3+2\lambda^2-3$ te

$a=\begin{bmatrix} 4 & 5 \\ -1 & -2 \end{bmatrix}$; 2) izračunaj a^{100}; 3) u slučaju velikog broja s uzima se u praksi umjesto desne strane u (2) izraz $\lambda_m^s g_m$, gdje je λ_m ona karakteristična vrijednost kojoj je modul najveći.

Izračunaj približno na taj način $\begin{bmatrix} 2 & -1 & 0 \\ 9 & 4 & 6 \\ -8 & 0 & -3 \end{bmatrix}^{312}$;

4) eksponencijalni red $e^a=\sum\limits_{n=0}^{\infty}\frac{a^n}{n!}$ prema (1) daje

$$e^a=\sum_{i=1}^{n} e^{\lambda_i} g_i;\ \text{izračunaj } e^a \text{ za } a=\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

7. Ako je spektar $Sa=S_{\mu(a,\lambda)}$ kvadratne konačne matrice a bez ponavljanja pa ako je funkcija $f\lambda$ definirana na spektru Sa, dokaži da tada Lagrange-Sylvesterov polinom $L_f(\lambda)=r(\lambda)$ postoji; nađi izraze $r(\lambda), fa$.

8. Ako je funkcija $f\lambda$ definirana na Sa, ako nadalje minimalni polinom ima oblik $\mu(\lambda)=(\lambda-\lambda_1)^{m_1}\cdots(\lambda-\lambda_m)^{m_m}$, tada polinom $r(\lambda)$ postoji.

Stavimo li $\mu_k(\lambda)=\frac{\mu(\lambda)}{(\lambda-\lambda_k)^{m_k}}=(k=1, 2, \ldots, m)$, tada je

$$r(\lambda)=\sum_{k=1}^{m}\left[\frac{f(\lambda_k)}{\mu_k(\lambda_k)}+\left(\frac{f(\lambda)}{\mu_k(\lambda)}\right)'_{\lambda=\lambda_k}\cdot(\lambda-\lambda_k)+\frac{1}{1!}\left(\frac{f(\lambda)}{\mu_k(\lambda)}\right)''_{\lambda=\lambda_k}(\lambda-\lambda_k)^2\right.$$
$$\left.+\cdots+\frac{1}{(m_k-1)!}\left(\frac{f(\lambda)}{\mu_k(\lambda)}\right)^{(m_k-1)}_{\lambda=\lambda_k}(\lambda-\lambda_k)^{m_k-1}\right]\mu(\lambda).$$

9. Dokaži: 1) Ako je $f(\lambda)=g(\lambda)+h(\lambda)$ pa ako za matricu a postoje matrice $g(a)$, $h(a)$, onda postoji i $f(a)$ pa vrijedi $fa=ga+ha$; 2) Slično za produkt $f(\lambda)=g(\lambda)\cdot h(\lambda)$.

10. Služeći se Lagrange-Sylvesterovim polinomom izračunaj:

1) $\begin{bmatrix} 1 & 1 \\ -1 & 3 \end{bmatrix}^{50}$; 2) $\begin{bmatrix} 3 & 1 \\ -1 & 5 \end{bmatrix}^{1/3}$; 3) e^a, $a=\begin{bmatrix} 4 & -2 \\ 6 & -3 \end{bmatrix}$;

4) e^a; $a=\begin{bmatrix} 4 & 2 & -5 \\ 6 & 4 & -9 \\ 5 & 3 & -7 \end{bmatrix}$; 5) $\ln\begin{bmatrix} 4 & -15 & 6 \\ 1 & -4 & 2 \\ 1 & -5 & 3 \end{bmatrix}$; 6) $\sin\begin{bmatrix} \pi-1 & 1 \\ -1 & \pi+1 \end{bmatrix}$.

11. Dokaži da za svaku konačnu kvadratnu matricu x postoji e^x, $\cos x$, $\sin x$ i da vrijede uobičajena pravila, kao npr. $e^x\cdot e^y=e^{x+y}$, $\cos(x+y)=$ $=\cos x\cos y-\sin x\sin y$, $\sin 2x=2\cos x\sin x$.

12. Dokaži $\det e^x = e^{tr\, x}$ za svaku konačnu kvadratnu matricu; pri tom $tr\, x = x_{11} + x_{22} + \cdots + x_{nn}$.

13. Ako za matricu a i funkciju $f(\lambda)$ postoji matrica fa, tada je $\det fa = \prod_\lambda f(\lambda)$, λ prolazi spektrom S_α matrice a (dakle i kratnost članova spektra dolazi u obzir).

14. *Izvod* ili *derivat matrice.* Ako su elementi a_{ik} matrice a funkcije varijable t, tad se definira izvod $\frac{da}{dt}$ tako da se svaki element derivira tj.

$$\left(\frac{da}{dt}\right)_{ik} = \frac{da_{ik}}{dt}. \text{ Dokaži: 1) } \frac{d}{dt}(a+b) = \frac{da}{dt} + \frac{db}{dt}; \text{ 2) } \frac{d}{dt}(ab) =$$

$$= \frac{da}{dt} b + a \frac{db}{dt}; \ \frac{d}{dt}(a_1 a_2 \cdots a_n) = \frac{da_1}{dt} a_2 a_3 \cdots a_n + a_1 \frac{da_2}{dt} a_3 a_n + \cdots +$$

$$+ a_1 a_2 \cdots a_{n-1} \frac{da_n}{dt}; \text{ 3) } \frac{d}{dt}(a^{-1}) = -a^{-1} \frac{da}{dt} a^{-1}; \text{ 4) } \frac{d}{dt} a^2 =$$

$$= \frac{da}{dt} a + a \frac{da}{dt}; \text{ 5) } \frac{d}{dt} a^3 = \frac{da}{dt} a^2 + a \frac{da}{dt} a + a^2 \frac{da}{dt}; \text{ 6) nađi } \frac{da^n}{dt};$$

$$\text{7) } \frac{d}{dt} e^a = e^a a; \text{ 8) } \frac{d}{dt} e^{(t-t_0)a} = e^{(t-t_0)a} a.$$

15. Nađi: 1) $\frac{d^2}{dt^2} \begin{bmatrix} t^3 & t^2 \\ \cos 3t & \cos^3 t \end{bmatrix}$; 2) $\frac{\partial}{\partial t_1} a$, $\frac{\partial}{\partial t_2} a$, $\frac{\partial^2}{\partial t_1^2} a$, $\frac{\partial^2}{\partial t_1 \partial t_2} a$, za

$$a = \begin{bmatrix} \cos t_1 t_2 & t_1^2 + t_2^2 \\ \sin t_1 t_2 & t_1^2 - t_2^2 \end{bmatrix}.$$

16. Integral matrice definira se ovako $\left(\int_{t_0}^{t_1} a\, dt\right)_{ik} = \left[\int_{t_0}^{t_1} a_{ik}\, dt\right]$;

$$\text{npr. } \int_0^t \begin{bmatrix} 2t & t^2 \\ \cos t & 3 \end{bmatrix} dt = \begin{bmatrix} t^2 & \frac{t^3}{3} \\ -\sin t + t & 3t \end{bmatrix}. \text{ Nađi:}$$

$$\text{1) } \int_2^3 \begin{bmatrix} t & 2t \\ 3t^2 & 5 \end{bmatrix} dt; \quad \text{2) } \int_0^t \begin{bmatrix} \cos t & \sin t \\ t & t^3 \end{bmatrix} dt; \quad \text{3) } \int_1^t \begin{bmatrix} \frac{1}{t} & t^2 \\ \cos t & t^2 \end{bmatrix} dt.$$

Literatura

Gantmaher [1], [2]; Kurepa S. [1]; Mal'cev [1]; Proskurjakov [1].

POGLAVLJE 25.

METRIKA U LINEARNIM PROSTORIMA

U elementarnoj matematici dolaze vektori često, specijalno u vezi s *kutom dvaju vektora*, odnosno s kutom njihovih nosilaca. Naravno, još više se govori o duljini ili *intenzitetu* (modulu) $|\vec{v}| = AB$ vektora $\vec{v} = \overrightarrow{AB}$. Oba ta pojma dolaze naročito pri tzv. skalarnom ili unutrašnjem množenju vektorâ.

1. PODSJET O SKALARNOM MNOŽENJU VEKTORA IZ ELEMENTARNE MATEMATIKE

1.1. Projekcija vektora na pravulju. Definicija. Projekcija vektora $\overrightarrow{AB}$ na pravulju p jest *vektor* $\overrightarrow{A_p B_p}$; A_p je ortogonalna projekcija tačke A na p; slično je B_p ortogonalna projekcija od B na p.

1.2. Skalarna projekcija vektora $\vec{v} = \overrightarrow{AB}$ na orijentiranu pravulju $\vec{p}$ jest ***skalar*** $\vec{v}_{\vec{p}} = (\overrightarrow{AB})_{\vec{p}} = AB \cdot \cos(\vec{p}, \overrightarrow{AB})$. Prema tome, $\vec{v}_{\vec{p}}$ je veličina $|\vec{v}_p|$ vektora $\vec{v}_p$ ili suprotna vrijednost te veličine, već prema tome da li je kut između vektora $\vec{v}$ i pravulje $\vec{p}$ u 1. odnosno 4. kvadrantu ili je u 2. odnosno 3. kvadrantu.

1.3. Signum ili ort vektora $\vec{v} \neq \vec{0}$ jest vektor $\frac{1}{|\vec{v}|}\vec{v}$; označuje se sa sgn $\vec{v}$ ili $\vec{v}^0$; specijalno se definira sgn $\vec{0} = \vec{0}$. Dakle je $\vec{v} = |\vec{v}|$ sgn $\vec{v}$ za svaki vektor $\vec{v}$.

1.4. Projekcija vektora $\vec{a}$ na vektor $\vec{b}$ jest projekcija vektora $\vec{a}$ na orijentiranu pravulju $\vec{b}$; označuje se sa $\vec{a}_{\vec{b}}$; dakle je $\vec{a}_{\vec{b}} = |\vec{a}| \cos(\vec{b}, \vec{a}) =$ ($=$ skalar).

1.5. Teorem. *Projiciranje vektora je distributivna operacija prema zbrajanju vektora* (*to vrijedi i za vektorsko i za skalarno projiciranje*):

$$\left(\vec{a}+\vec{b}\right)_p=\vec{a}_p+\vec{b}_p$$

$$\left(\vec{a}+\vec{b}\right)_{\vec{p}}=\vec{a}_{\vec{p}}+\vec{b}_{\vec{p}}.$$

1.6. **Definicija.** *Skalarni ili unutrašnji produkt vektora $\vec{a}$ i vektora $\vec{b}$ je skalar*

$$\vec{a}\,\vec{b}=\left|\vec{a}\right|\cdot\left|\vec{b}\right|\cos\left(\vec{a},\vec{b}\right).$$

$\longrightarrow$ **1.7. Osnovni teorem o skalarnom množenju.**

(*i*) *Skalarno množenje vektora je distributivno prema zbrajanju vektora:*

(1) $$\left(\vec{a}+\vec{b}\right)\vec{c}=\vec{a}\,\vec{c}+\vec{b}\,\vec{c}$$

odnosno

(2) $$\left(\vec{a}+\vec{b}\right)\left(\vec{c}+\vec{d}\right)=\vec{a}\,\vec{c}+\vec{b}\,\vec{c}+\vec{a}\,\vec{d}+\vec{b}\,\vec{d}$$

(3) $$\sum_{n=1}^{n}\vec{a}_{n'}\sum_{s'=1}^{s}\vec{b}_{s'}=\sum_{\substack{n'=1\cdots n\\ s'=1\cdots s}}\vec{a}_{n'}\,\vec{b}_{s'}$$

(*ii*) *Ako su vektori $e_{n'}$ $(n'=1,\ldots,n)$ ortonormirani, tada pri $n>1$ za vektore*

$$\vec{u}=u_1e_1+\cdots+u_ne_n,\quad \vec{v}=v_1e_1+\cdots+v_ne_n$$

vrijedi

(*S*) $$\left|\vec{u}\,\vec{v}\right|\cos\left(\vec{u},\vec{v}\right)=u_1v_1+u_2v_2+\cdots+u_nv_n.$$

Dokažimo obrazac (1). Projicirajmo $\vec{a},\vec{b},\vec{a}+\vec{b}$ na $\vec{c}$; imamo

$$\left(\vec{a}+\vec{b}\right)_{\vec{c}}=\vec{a}_{\vec{c}}+\vec{b}_{\vec{c}}.$$

Pomnožimo tu jednakost skalarom $\left|\vec{c}\right|$; lijevo se dobije $\left(\vec{a}+\vec{b}\right)\vec{c}$; desno se dobije $\vec{a}_{\vec{c}}\left|\vec{c}\right|+\vec{b}_{\vec{c}}\left|\vec{c}\right|$ jer je množenje skalarom distributivno prema zbrajanju vektora. Time se dobije upravo (1).

Obrazac (2) izlazi iz obrasca (1) pišući $\vec{c}+\vec{d}$ umjesto $\vec{c}$ i primjenjujući distributivnost. Obrazac (3) dobije se indukcijom po n, a onda indukcijom po s.

Osnovna jednakost (*S*) iskazuje da je skalarni produkt $\vec{u}\,\vec{v}$ napisanih vektora $\vec{u},\vec{v}$ moguće prikazati izrazom $\Sigma u_{n'}v_{n'}$. To neposredno izlazi iz zakona distributivnosti (3):

$$\vec{u}\,\vec{v}=\sum_{i=1}^{n}u_{i'}e_{i'}\sum_{k=1}^{n}v_ke_k=\sum_{i,k=1}^{n}u_iv_ke_ie_k=\sum_{i,k=1}^{n}u_iv_k\delta_{ik}=\sum_{i=1}^{n}u_iv_i.$$

2. AKSIOMATSKO UVOĐENJE EUKLIDSKE METRIKE

Radimo s linearnim prostorom $V = V_n(R)$ nad tijelom R realnih brojeva; elementi iz V su vektori.

2.1. Kazat ćemo da je u tom prostoru uvedena *euklidska metrika* ako *svakom* uređenom paru (x, y) elemenata iz V znamo odrediti njihov skalarni produkt xy ili $x \cdot y$ ili $x \circ y$ i da pri tom vrijede ovi uslovi:

S_0 $x \circ y \in R$ (tj. produkt je realan broj).

S_1 (*komutacija*): $x \circ y = y \circ x$.

S_2 (*množenje sa skalarom*) $\dot{R} x \circ y = \dot{R}(x \circ y)$.

S_3 (*distributivnost množenja prema zbrajanju*): $(x+y) \circ z = x \circ z + y \circ z$.

S_4 (*uslov o kvadratu*): $Nx = x \circ x \geq 0$ (Nx se zove *norma* vektora x).

S_5 $x \neq 0 \Rightarrow Nx > 0$.

2.2. Kaže se također da je metrika *pozitivno definitna*. Ako znamo da za neku operaciju $V \times V_{\rightarrow} R$ vrijede samo prva tri uslova, onda se kaže da imamo posla s *metrikom u prostoru*; metrika je *neodrečna* ako vrijedi i uslov S_4, a *pozitivno definitna* ako vrijedi svih pet uslova. Svaki vektorski prostor s euklidskom metrikom zove se *euklidski prostor*.

Na osnovu gornjih zahtjeva S_1—S_5 može se izgraditi čitava *algebra vektorâ*, odnosno geometrija prostora V.

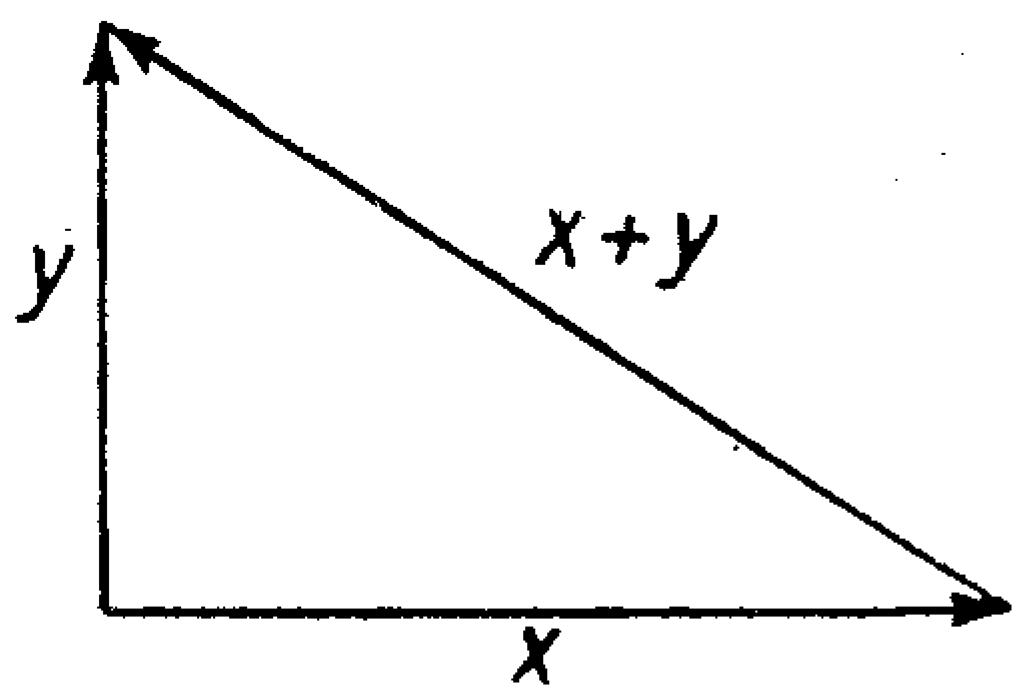
2.3. Veličina ili modul vektora. Za svaki vektor x uvodi se veličina ili apsolutum vektora x kao broj $+(xx)^{1/2}$; označuje se sa $|x|$, tj. stavlja se $|x| = +(Nx)^{1/2}$.

2.4. Kut dvaju vektora *x*, *y* definira se kao broj φ, za koji je $x \circ y = |x| \cdot |y| \cos \varphi$.

Vektor x je ortogonalan na y ako je $x \circ y = 0$; piše se $x \perp y$. Zbog komutacije odmah se vidi da iz $x \perp y$ izlazi $y \perp x$.

2.5. Pitagorin teorem. Nađimo kvadrat sume ortogonalnih vektora:

$$(x+y)^2 = (\text{def.}) = (x+y) \circ (x+y) = (\text{po } S_3) =$$
$$= x \circ (x+y) + y \circ (x+y) = (\text{po } S_1) =$$
$$(x+y) \circ x + (x+y) \circ y = (\text{po } S_3) = x \circ x +$$
$$y \circ x + x \circ y + y \circ y = x \circ x + 0 + 0 + y \circ y =$$
$$= x^2 + y^2,$$



Sl. 25. 2.5.

tj. $(x+y)^2 = x^2 + y^2$, za $x \perp y$ (Pitagorin teorem).

2.6. Kao neposredna posljedica prvih triju aksioma proizlazi pravilo o množenju sumâ vektorâ (slično kao što smo maloprije množili $(a+b)(a+b)$).

Ako imamo bazu $e=(e_{n'})_{n'}$ vektorâ, tada za svaki par vektora x, y imamo rastave:

(2) $$x=\sum_{i=1}^{n} x_i e_i \quad y=\sum_{k=1}^{n} y_k e_k;$$

odatle

$$x \circ y=\left(\sum x_i e_i\right)\left(\sum y_k e_k\right)=\sum_{i,k} x_i e_i \circ y_k e_k=\sum_{i,k=1}^{n} e_i \circ e_k\, x_i y_k, \text{ tj.}$$

—→ **2.6.1.** Teorem. *Za svaku vektorsku bazu* $e=(e_1, e_2, \ldots e_n)$ *u prostoru* $V_n(K)$, *relacije* (2) uključuju

(3) $$x \circ y=\sum_{i,k=1}^{n} a_{ik} x_i y_k, \quad \text{gdje je } a_{ik}=e_i \circ e_k=a_{ki}.$$

Specijalno

(4) $$x \circ x=\sum_{i,k=1}^{n} a_{ik}\, x_i x_k.$$

Ako je baza e ortonormirana, tj. $e_i e_k=\delta_{ik}=\begin{matrix}0\\1\end{matrix}$ za $i \begin{matrix}\neq\\=\end{matrix} k$, *tada je*

(5) $$xy=\sum x_{n'} y_{n'}$$

(6) $$xx=\sum x_{n'}^2.$$

Tu se pojavljuje kvadratna matrica $[a_{ik}]$; ona pokazuje *tablicu množenja vektorâ* $e_{n'}$ koje smo odabrali kao osnovne. Obrazac (3) pokazuje da je produkt $x \circ y$ bilo kojih dvaju vektora određen tom tablicom a.

2.7. Ortonormirane baze vektorâ. To su baze vektorâ veličine 1 i koji su međusobno ortogonalni. Ortonormirane baze dolaze kao specifičnost metrike.

One su specijalno važne. Zato je jasno da će i transformacije (matrice) koje povezuju ortonormirane baze imati izuzetno važnu ulogu — njihov skup je tzv. ortogonalna grupa prostora $R_{n'}$ (isp. pogl. 28).

2.8. Bessel-Parsevalova nejednakost. *Za svaki ortonormirani niz vektora* $e_1, \ldots, e_k$ *i svaki vektor v vrijedi*

(1) $$\sum_{i=1}^{k} (ve_i)^2 \leq Nv;$$

znak jednakosti vrijedi onda i samo onda ako vektori $e_i, \ldots, e_k$ *čine ortonormiranu bazu vektorâ u prostoru.*

Naime, ako vektori $e_1, \ldots, e_k$ ne čine potpunu bazu, možemo dovođenjem još nekih vektora $e_{k+1}, \ldots, e_n$ izgraditi potpunu bazu $e_1, \ldots, e_k, \ldots, e_n$.

U toj bazi za komponente vrijedi

(2) $$Nv=\sum_{i=1}^{n} (ve_i)^2=\sum_{i=1}^{k} (ve_i)^2+\sum_{i=k+1}^{n} (ve_i)^2.$$

Time je relacija (1) dokazana, jer je druga suma na desnoj strani iz (2) upravo višak desne strane u (1) prema lijevoj strani.

Ortonormirane baze imaju osobitu važnost u izučavanju Euklidovih prostora.

2.9. Stepen proizvoljnosti. Primijetimo da je matrica množenja a dobivena na osnovu zahtjeva S_1, S_2, S_3. Ona zasad još može biti proizvoljna! Međutim, dolazi pitanje: promjena baze! Ako umjesto baze e uzmemo novu bazu $e' = (e'_{n'})$, tada će sve veličine x, y, a_{ik}, $e_{n'}$, $e'_{n'}$, $a'_{ik} = e_i' \circ a_k'$ imati svoje notacije, značke (koordinate) i u bazi e i u bazi e'. Kako su one međusobno povezane?

2.10. Bilinearne i kvadratne forme (isp. pogl. 16). Primijetimo da skalarni produkt $x \circ y$ u § 2.6. formula (3) na poseban način zavisi od koordinata vektorâ x i y; on je *bilinearna forma* tih koordinata (tj. homogen polinom st. 2) a koeficijenti su produkti vektorâ $e_{n'}$. Isto tako norma vektora na poseban način zavisi od koordinata vektora: *norma vektora je kvadratna forma* (homogen polinom stupnja 2) njegovih koordinata.

Vektori 1_n jedinične matrice specijalno dobro služe kao baza za množenje u euklidskom prostoru R_n od n dimenzija. Naime, ti vektori čine ortonormiran skup vektora.

2.11. Zadaci o euklidskoj metrici i vektorima.

Podrazumijeva se da radimo u nekoj ortonormiranoj bazi e prostora.

1. Za vektore $\vec{a} = (2, 3, 5)$, $\vec{b} = (1, 3, -2)$ nađi skalarni produkt ab, jedinične vektore, $\operatorname{sgn} \vec{a} = a^0$, $\operatorname{sgn} \vec{b} = \operatorname{sgn} b^0$ kao i veličinu kuta između $\vec{a}$, $\vec{b}$.

2. U $\triangle ABC$ neka A_1, B_1, C_1 znači središte dužine BC odnosno $\overline{CA}$ odnosno $\overline{AB}$; dokaži $\overrightarrow{AA_1} + \overrightarrow{BB_1} + \overrightarrow{CC_1} = \vec{0}$.

3. Odredi broj α tako da vektori
$$\vec{a} = \alpha e_1 + 4e_2 + 2e_3$$
$$\vec{b} = 2e_1 - e_2 + 7e_3$$
$$\vec{c} = \alpha e_1 - 6e_2 + 3e_3$$
budu linearno zavisni.

4. Dokaži da se težišnice trokuta (tetraedra) sijeku u određenoj tački kojom je težišnica podijeljena u omjeru $2:1$ (odn. $3:1$) računajući od vrha.

5. Vektor $\vec{v} = 2e_1 + 5e_2$ rastavi u komponente u smjeru vektora $\vec{a} = 3e_1 - 2e_2$, $\vec{b} = -5e_1 + 4e_2$.

6. Dokaži pomoću vektora teorem o sinusima i teorem o kosinusima: 1) u euklidskoj geometriji; 2) u sfernoj trigonometriji.

7. Vektorski produkt vektora u prostoru R_3 definira se ovako:

$$(xe_1+ye_2+ze_3)\times(x'e_1+y'e_2+z'e_3)=\begin{vmatrix} e_1 & e_2 & e_3 \\ x & y & z \\ x' & y' & z' \end{vmatrix}=(yz'-y'z)e_1+$$

$+(zx'-z'x)e_2+(xy'-x'y)e_3$. Dokaži: 1) $\vec{a}\times\vec{b}=-\vec{b}\times\vec{a}$;

2) $(\vec{a}+\vec{b})\times\vec{c}=\vec{a}\times\vec{c}+\vec{b}\times\vec{c}$; 3) $a\times(b\times c)=\begin{vmatrix} b & c \\ ab & ac \end{vmatrix}$;

4) $a\times(b\times c)+b\times(c\times a)+c\times(a\times b)=\vec{0}$ (Jacobijev identitet);

5) $(a\times b)\cdot(c\times d)=\begin{vmatrix} ac & ad \\ bc & bd \end{vmatrix}$ (Lagrangeov identitet);

6) $(a\times b)\times(c\times d)=b(a\times c)d-a(b\times c)d$.

7′ Da li vrijedi: 1) $(a+b)\times(a-b)=a\times a-b\times b$;

2) $(a+b)\times(a+b)=a\times a+2a\times b+b\times b$,

3) $(a\times b)\times(a\times b)=(a\times a)\times(b\times b)$?

7″ Nađi: 1) $(a+b)\times(a-b)$; 2) $(a\times b)^2+(ab)^2$.

8. Može li biti, $\vec{x}^2=0$, $\vec{x}\neq 0$, ako su komponente vektora $\vec{x}$ kompleksni brojevi?

9. Nađi veličinu, jedinične vektore, skalarni produkt i kut ovih dvaju vektora $\vec{a}=(1, 2, 3, 4)$, $\vec{b}=(3, 1, 2, 5)$.

10. Ortonormiraj vektore: 1) (1, 3), (5, 4); 2) (1, 2, 3), (—2, 3, 5), (4, 1, 0); 3) (1, 2, 1, 3), (4, 1, 1, 1), (3, 1, 1, 0).

11. Obrazuj vektorsku osnovu u R_3 za koju je zadan:
1) $e_1=(2, 3, 4)$, $e_2=(1, 5, 8)$; 2) $e_1=(0, 5, 8)$.

12. Odredi veličine stranica i kutova u $\triangle ABC$, ako je
$A=(1, 2, 1, 2)$, $B=(3, 1, -1, 0)$, $C=(1, 1, 0, 1)$.

13. Dokaži da formula $\vec{x}\circ\vec{y}=\Sigma_i x_i y_i$ vrijedi onda i samo onda, ako je vektorska osnova ortonormirana.

14. Nađi projekciju $pr\vec{x}=a^0\circ\vec{x}$ vektora $\vec{x}$ na vektor $\vec{a}$, ako je

1) $\vec{a}=(2, 3)$, $\vec{x}=(5, 7)$; 2) $\vec{a}=(3, 1, 4)$, $\vec{x}=(5, -1, 6)$;

3) $\vec{a}=(1, 2, 3, 4)$, $\vec{x}=(5, 1, 2, 5)$.

3. AKSIOMATSKO UVOĐENJE HERMITSKE METRIKE

3.0. Kompleksni brojevi postali su svojina čovječanstva i kulture. Njihovom upotrebom stvari se mnogo preglednije razvrstavaju i izučavaju. Zato se uz prostore R_n nad tijelom R realnih brojeva pojavljuju i prostori C_n nad tijelom $C=R(i)$ kompleksnih brojeva. No, zna se da je kvadrat kompleksna broja rijetko kada ≥ 0, pa bi zato osnovna formula iz § 2.6.1. euklidske metrike prenesena na prostor C_n dala nezgodan rezultat da je norma npr. vektora $2-3i$ jednaka $(2-3i)(2-3i)=13-12i$. No, zna se, s druge strane, da je za svaki kompleksni broj z produkt $z\cdot\bar{z}\geq 0$, gdje $\bar{z}$ konjugirano ili spregnuto od z. U tome smislu se stvar modificirala s namjerom da norma ostane ≥ 0. Naime, ako je dana neka baza vektora $e_{n'}$, tada za svaki vektor x imamo vezu

$$x=x_1 e_1+x_2 e_2=\ldots;$$

sada su $x_1, x_2, \ldots$ **kompleksni** brojevi; no

$$x_1\cdot\bar{x}_1\geq 0,\quad x_2\cdot\bar{x}_2\geq 0,\ldots$$

pa stavljajući

(S_4) $$Nx=x_1\cdot\bar{x}_1+x_2\cdot\bar{x}_2+\cdots$$

ostat će sačuvan uslov S_4 za euklidsku metriku.

Tako se došlo do naredne aksiomatike, koja se reducira na gornju metriku u prostorima R_n.

3.1. Aksiomatika hermitske metrike u prostoru C_n. C_n će označavati skup svih n-članih nizova *kompleksnih* brojeva uz uobičajena pravila o računanju. Osim toga, svakom uređenom paru $x, y\in C_n$ pridajemo *hermitski produkt vektora* x i y; označujemo ga sa $H(x, y)$, $x\ominus y$ ili (x, y) ili naprosto sa xy, ukoliko se vidi da je riječ o hermitskom produktu vektorâ. Pri tom zahtijevamo da vrijede ovi postulati:

S_0 $$x, y\in C_n \Rightarrow x\ominus y\in C$$

(tj. hermitski produkt dvaju vektora je kompleksan broj).

S_1 $$x\ominus y=\overline{y\ominus x}$$

(*hermitska komutativnost ili simetrija*).

S_2 $$\dot{C}x\ominus y=\dot{C}\,(x\ominus y).$$

S_3 $$(x+y)\ominus z=x\ominus z+y\ominus z.$$

S_4 $$x\ominus x\geq 0 \text{ za svako } x\in C_n.$$

Hermitska metrika je pozitivno definitna, ako uz S_0—S_4 vrijedi:

S_5 $$x\neq 0 \Rightarrow x\ominus x>0.$$

Formalno, novi postulati su kao i bivši, samo s bitnom razlikom da umjesto proste komutacije dolazi hermitska komutacija.[1] Važno je napomenuti

[1] Poznat je slučaj protivne komutacije $xfy=-(yfx)$, npr. za $f=-$ (oduzimanje) ili $f=\times$ (vektorsko množenje vektora). No, hermitska simetrija nije simetrija centralna, prema 0, nego prema nosiocu realnih brojeva.

da tijelo $C(=R(i))$ kompleksnih brojeva obuhvata tijelo R realnih brojeva kao one svoje članove za koje je $z=z^\star$ i da je svaki prostor $V_n(R)$ sadržan u prostoru $V_n(C)$, premda $V_n(R)$ nije potprostor od $V_n(C)$.

Kad su se tako postavili osnovni postulati, stvar dalje teče kao i u euklidskom slučaju; sve te definicije (hermitska ortogonalnost, norma, kut, ...) prenose se automatski na „unitarne prostore" C_n.

3.2. Definicija. *Hermitski ili unitarni prostori jesu prostori C_n u kojima vrijedi hermitska metrika.*

Tako npr. svaka *obična ravnina* može poslužiti kao materijal za izgradnju hermitskog prostora C_1 — dobiva se brojevna ravnina — nosilac kompleksnih brojeva.

3.3. Prostor C_n i prostor R_{2n}. Prostor C_n sastavljen je od svih n-članih nizova kompleksnih brojeva; no svaki kompleksni broj je uređena *dvojka realnih* brojeva. Na taj način svaki kompleksni niz od n članova u tijesnoj je vezi s nizovima realnih brojeva po $2n$ članova. To znači da su prostori C_n i R_{2n} međusobno tijesno vezani.

3.4. O hermitskom skalarnom produktu. Prema postulatu S_1 hermitsko množenje vektora je hermitski simetrično, a nije prosto simetrično. To odmah ima utjecaja i na prebacivanje skalara iz jednog faktora u drugi.

1. Lema. *Ako su x, y vektori s kompleksnim vrijednostima, tada je za svaki skalar $c \in C$:*

(1) $$c(x \ominus y) = x \ominus c^\star y.$$

Naime, prema postulatu S_2 imamo

$$(cx \ominus y) = c(x \ominus y);$$

odatle, uzimajući operator sprezanja:

$$(cx \ominus y)^\star = (c(x \ominus y))^\star = c^\star (x \ominus y)^\star =$$

$$= (\text{prema } S_1) = c^\star (y \ominus x) = (\text{prema } S_2) =$$

$$= (c^\star y \ominus x) = (x \ominus c^\star y)^\star, \text{ tj. } (cx \ominus y)^\star = (x \ominus c^\star y)^\star;$$

odatle izlazi i (1).

2. Lema. *Za kompleksne brojeve c, d uvijek je*

$$(cx + dy) \ominus z = c(x \ominus z) + d(y \ominus z),$$

$$z \ominus (cx + dy) = c^\star (z \ominus x) + d^\star (z \ominus y).$$

Na taj način, hermitski produkt dvojke vektorâ je linearna forma prvog aktora, ali nije linearna forma drugog faktora.

P r i m j e r. Nađimo u ortonormiranoj osnovi $e=(e_1)$ hermitski produkt jednočlanih vektora

$x=[2+i]$, $y=[4-3i]$. Imamo: $x \ominus y=((2+i)e_1 \ominus (4-3i)e_1)=(\text{po } (S_2))=$

$=(2+i)e_1 \ominus (4-3i)e_1=(2+i)\cdot(e_1 \ominus e_1)(4+3i)=(\text{ako je } e_1 \ominus e_1=1,$

tada je to dalje $=1\cdot(2+i)(4+3i)=5+10i)$.

3. Analogno se dokazuje da je (isp. pogl. 16, § 7.6) za $x=\Sigma x_i e_i$, $y=\Sigma y_i e_i$: $(x \ominus y)=(\Sigma x_i e_i) \ominus (\Sigma y_k e_k)=\sum_{i,k}(x_i \overline{y_k})(e_i \ominus e_k)=$(ako je baza ortonormirana)$=\Sigma x_i \overline{y_k}=$(matrično)$=y\cdot x^\star$ pri čemu uopće za matricu a definiramo

$$a^\star=\overline{(a^T)}=a^{-T} \qquad \text{(isp. pogl. 10, § 7).}$$

—→ 4. L e m a. *Ako su vektori x, y hermitski ortogonalni, tada je*

$$N(x+y)=Nx+Ny$$

(*analogon Pitagorina teorema*).

Uopće, za n vektora, od kojih su dva po dva međusobno okomita, norma je distributivno svojstvo prema adiciji vektora:

$$N(x_1+x_2+\cdots)=Nx_1+Nx_2+\cdots$$

Dokažimo stvar za dva vektora; indukcijom se slično dokazuje općenito.

Naime, $$N(x+y)=(x+y)^\star(x+y)=(x^\star+y^\star)(x+y)$$
$$=x^\star x+y^\star x+x^\star y+y^\star y=Nx+0+0+Ny=Nx+Ny.$$

3.5. Zadaci o unitarnim prostorima.

0. Pročitati § 3 označujući hermitski produkt od x, y sa (xy), (x, y) ili $x\mathrm{H}y$.

1. Nađi normu i jedinični vektor ovih vektora:

   1. $(2, i)$; 2) $(2+i, 3-4i)$; 3) (i, i, i); 4) (i, i, i, i, i);
   5) $(1, i, 1, i, 1, i)$; 6) $(2+3i, 4-i, 5+2i)$.

2. Nađi hermitski produkt (a, b) ovih vektora:

   1) $\vec{a}=(2+i, 3-2i)$, $\vec{b}=(3-2i, 4+5i)$; 2) $\vec{a}=(i, 2, 3-i)$, $\vec{b}=(2+3i, -3+2i, 1)$; 3) $(i, 0, 1)$, $(2, i, 3i)$.

3. Može li biti $(\vec{x}, \vec{x})=0$, $\vec{x}\neq\vec{0}$?

4. Ako je $(\vec{x}, \vec{x})=0$ i $\vec{y}\,\|\,\vec{x}$, onda je $(\vec{y}, \vec{y})=0$.

5. Ako je $\vec{v}\perp\vec{a}, \vec{b}$ tad je $\vec{v}\perp\vec{x}$ za svaki vektor $\vec{x}$ koji se linearno izražava pomoću $\vec{a}, \vec{b}$. Šta to znači geometrijski?

4. KOMPONENTE VEKTORA U EUKLIDSKIM I HERMITSKIM PROSTORIMA

4.1. Problem komponenata za svaki vektor i linearni prostor riješili smo u pogl. 23, § 3, tačka 3). No, u sadašnjim prilikama stvar je mnogo jednostavnija. Radimo npr. u ravnini R_2 jer je opći slučaj analogan. Ako je zadana osnova $e=(e_1, e_2)$, tada za svaki vektor v imamo:

(1) $$v=e_1 v_1+e_2 v_2.$$

Množeći te jednadžbe skalarno, odnosno hermitski po redu sa $e_{n'}$, dobiva se sistem

(2) $$v\ominus e_{n'}=\sum_{i=1}^{n}(e_i\ominus e_{n'})\,v_i.$$

4.2. Tu se pojavljuje tzv. *Gramova determinanta vektorâ* $e_{n'}$; po definiciji, to je determinanta Gramove matrice:

(3) $$\Gamma(e_1,\dots e_n)=\begin{bmatrix} e_1\ominus e_1 & \cdots & e_1\ominus e_n \\ e_2\ominus e_1 & \cdots & e_2\ominus e_n \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ e_n\ominus e_1 & \cdots & e_n\ominus e_n \end{bmatrix};$$

ona je upravo determinanta sistema (2). Kako je e baza, ima sistem (2) za v_i jedno jedino rješenje; to znači da je determinanta sistema, tj. determinante (3), različita od nule pa se skalari v_i nalaze po Cramerovu teoremu. No, ako je baza ortonormirana, tada je $e_i\ominus e_k=\delta_{ik}$, pa iz (2) odmah izlazi:

(4) $$v\ominus e_{n'}=v_{n'}.$$

⟶ **4.3.** Teorem. *Komponente vektora v u bazi e u euklidskom ili unitarnom prostoru dobiju se iz jednadžbi*

$$v_{n'}=\frac{\det E_{n'}}{\det\Gamma(e_1,\dots,e_n)},$$

pri čemu u brojniku stoji determinanta matrice što se iz Gramove matrice dobije zamjenjujući stupac $\Gamma_{.n'}$ od Γ sa $v\ominus e_{n'}$. Ako je baza ortonormirana, tada je

$$v_{n'}=v\ominus e_{n'}.$$

4.4. Riješimo zadatak iz § 3.1. služeći se skalarnim množenjem. Bazu su činili stupci matrice

$$e=\begin{bmatrix} 4 & 5 & 0 \\ 0 & -2 & 4 \\ 0 & 3 & -1 \end{bmatrix},\ \text{vektor je bio zadan kao}\ \begin{bmatrix} 7 \\ 18 \\ -7 \end{bmatrix}.$$

Gramova determinanta je

$$\det\Gamma(e)=\begin{vmatrix} 16 & 20 & 0 \\ 20 & 38 & -11 \\ 0 & -11 & 17 \end{vmatrix}=16\,(38\cdot 17-121)-20\cdot 20\cdot 17=1600.$$

Skalarni produkti od v i $e_{n'}$ jesu:

$$28, \quad 5\cdot 7-36-21=-22, \quad 4\cdot 18+7=79.$$

Sad po Cramerovu pravilu možemo naći $v_{n'}$.

Uspput smo dobili

⟶ **4.5.** Teorem. *Da n vektorâ $(e_{n'})_{n'=1,\ldots,n}$ bude linearno nezavisno, nužno je i dovoljno da njihova Gramova determinanta bude $\neq 0$.*

Naime, ako su vektori $e_{n'}$ linearno nezavisni, onda oni čine bazu u potprostoru što ga oni određuju; to znači da sistem (2) od n jednadžbi ima jedno jedino rješenje za svaki zadani vektor v, a to, kao što vidjesmo, stoji jedino ako je $\det \Gamma e \neq 0$. Obrnuto, ako je $\det \Gamma e \neq 0$, tada za svako v sistem (2) ima jedno jedino rješenje, i to specijalno trivijalno rješenje $0, 0, \ldots, 0$ ako je vektor v nula-vektor; a to znači upravo da su $e_{n'}$ linearno nezavisni.

5. ORTONORMIRAN SKUP VEKTORA

5.1. Definicija. Skup vektora je *ortonormiran* ako je svaki vektor iz toga skupa dužine 1 i svaki okomit na svakom ostalom.

Ortonormirane koordinatne baze su specijalno pogodne, jer su formule u njima jednostavnije. Zato nastaje *problem kako od proizvoljne baze e preći na ortonormiranu bazu.*

5.2. Prvi slučaj: *zadani vektori su dva po dva međusobno okomita.* Dovoljno je umjesto svakog vektora x baze promatrati pripadni ort ili signum od x, simbolički $\operatorname{sgn} x$ ili x^0, tj. jedinični vektor $\operatorname{sgn} x = x^0 = \dfrac{x}{|x|}$, gdje je $|x|$ modul vektora x; kako su vektori baze međusobno linearno nezavisni, bit će $|x| \neq 0$.

5.3. **Opći slučaj: ortogonalizacija zadanih nezavisnih vektora.** Neka je baza $v_1, v_2, \ldots, v_n$ niz od n linearno nezavisnih vektora. Izvedimo iz njih n ortogonalnih vektora $O_1, O_2, \ldots, O_n$ i to ovako: $O_1 = v_1$; neka O_2 bude komponenta vektora v_2, koja je $\perp v_1$; neka je O_3 komponenta vektora v_3, koja je $\perp v_1, v_2$, itd. Vektori $O_1, O_2, \ldots, O_n$ su određeni, međusobno su okomiti i $\neq \vec{0}$; specijalno je svaki od njih $\neq \vec{0}$ (kad bi npr. bilo $O_3 = \vec{0}$, značilo bi da vektor v_3 leži u prostoru vektorâ v_1, v_2, protivno pretpostavci da su vektori $v_1, v_2, \ldots$ nezavisni).

⟶ Teorem o ortonormiranju (*Gram-Schmidtov postupak*)[1]. *Neka su $v_1, v_2, \ldots v_r$ linearno nezavisni vektori. Tada su ovi jedinični vektori $e_1, e_2, \ldots, e_r$ ortonormirani:*

---

[1] E. Schmidt [Šmit] (19/20. st.), njemački matematičar.

$$
\begin{aligned}
&e_1 = v_1^0 = \frac{v_1}{|v_1|}\\
(1)\qquad &e_2 = (v_2 - (v_2 \ominus e_1)\, e_1)^0\\
&e_3 = (v_3 - w_3)^0, \text{ gdje je } w_3 = (v_3 \ominus e_1)\, e_1 + (v_3 \ominus e_2)\, e_2\\
&e_4 = (v_4 - w_4)^0, \text{ gdje je } w_4 = (v_4 \ominus e_1)\, e_1 + (v_4 \ominus e_2)\, e_2 + (v_4 \ominus e_3)\, e_3.\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

Vrijedi:

$$
\begin{aligned}
&v_1 = |v_1|\, e_1\\
&v_2 = (v_2 \ominus e_1)\, e_1 + (v_2 - (v_2 \ominus e_1)\, e_1)\, e_2\\
(2)\qquad &v_3 = w_3 + (v_3 - w_3)\, e_3,\ w_3 = (v_3 \ominus e_1)\, e_1 + (v_3 \ominus e_2)\, e_2\\
&v_4 = w_4 + (v_4 - w_4)\, e_4,\ w_4 = (v_4 \ominus e_1)\, e_1 + (v_4 \ominus e_2)\, e_2 + (v_4 \ominus e_3)\, e_3.\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

Na taj način iz nezavisnih vektora $v_1, v_2, \ldots, v_n$ dolazimo do odgovarajućih *ortonormiranih* vektora $e_{n'}$. Oni razapinju isti prostor kao i zadani vektori $v_{n'}$, jer se ovi, kao što pokazuju gornje formule, izražavaju linearno pomoću $e_1 \ldots e_n$.

5.5. Dokaz formula (1) je očigledan. Najprije se stavlja $e_1 = v_1^0$. Zatim se odredi vektor $O_2 = v_2 + c_{21}\, e_1$, koji je $\perp e_1$, tj. tako da bude $(v_2 + c_{21}\, e_1)\, e_1 = 0$, odakle $c_{21} = -v_2 \ominus e_1$; dakle je vektor $O_2 = v_2 - (v_2 \ominus e_1)\, e_1$ okomit na e_1; no $O_2 \neq \vec{0}$, jer bi inače bilo $O_2 = \vec{0}$, tj. vektori v_2, e_1, dakle i v_2, v_1, bili bi linearno zavisni. Zatim se odredi $O_3 = v_3 + c_{31}\, e_1 + c_{32}\, e_2$ tako da bude $O_3 \perp e_1, e_2$, dakle

$$(v_3 + c_{31}\, e_1 + c_{32}\, e_2)\, e_i = 0 \qquad (i = 1,\ 2), \text{ tj.}$$

$$v_3 \ominus e_i + c_{31}\,(e_1 \ominus e_i) + c_{32}\,(e_2 \ominus e_i) = 0, \quad (i = 1,\ 2);$$

kako je

$$e_1 \ominus e_2 = e_2 \ominus e_1 = 0,\ e_1 \ominus e_1 = e_2 \ominus e_2 = 1,$$

to prethodne jednadžbe daju:

$$c_{3i} = -v_3 \ominus e_i. \qquad (i = 1,\ 2),$$

pa je, dakle, traženi vektor

$$O_3 = v_3 - (v_3 \ominus e_1)\, e_1 - (v_3 \ominus e_2)\, e_2,$$

tj.

$$O_3 = v_3 - w_3, \text{ gdje je } w_3 = (v_3 \ominus e_1) \ominus e_1 + (v_3 \ominus e_2)\, e_2.$$

Zatim se stavi $e_3 = (O_2)^0$. Itd.

5.6. Specijalno se tako mogu ortonormirati stupci zadane regularne matrice.

5.7. Primjedba. Gornji postupak vrijedi i za unitarne i euklidske prostore. Neka čitalac kao vježbu provede gornje dokaze služeći se oznakom (xy), odnosno (x, y), odnosno $x \mathrm{H} y$ umjesto $x \ominus y$ za hermitski produkt od x i od y.

6. HERMITSKO SPREZANJE OPERATORA

6.1. O sprezanju kompleksnih brojeva i matrica. Operator $z \to \bar{z}$. Svakom kompleksnom broju z pridružujemo konjugirani ili spregnuti broj $\bar{z}$, koji s njim ima isti realni, a suprotan imaginarni dio. Npr. broj spregnut sa $2-5i$ jest $\overline{2-5i}=2+5i$.

Slično za matrice. Ako je a matrica, tada smo matricu $\bar{a}$ definirali kao onu za koju je $(\bar{a})_{ik}=\overline{a_{ik}}$.

Operator $z \to \bar{z}$ ima ova jednostavna i zanimljiva svojstva:

(1) $$z=\bar{\bar{z}}$$ (involutivnost);

(2) $$\overline{uz}=\bar{u}\,\bar{z}, \quad \overline{u+z}=\bar{u}+\bar{z}$$

(distributivnost prema množenju i prema zbrajanju);

(3) $$\bar{u}\,z=\overline{\bar{z}\,u}$$ (kosa simetrija);

(4) $z\bar{z}$ je realno ako je z broj.

6.2. Ako pogledamo gornje obrasce, specijalno (1) i (3), tada vidimo da su to obrasci slični onima koji vrijede za oduzimanje; treba samo za $\bar{z}$ staviti $-z$, a za znak množenja znak $+$.

Inače, operacija $u\,\bar{z}$ nas podsjeća na dijeljenje; stvarno je

$$u\,\bar{z}=\frac{u}{z}\,|z^2|.$$

Tako npr. aditivnom identitetu

$$(a+x)-y=x-(-a+y)$$

odgovara množidbeni identitet

(5) $$ax\cdot\bar{y}=x\,\overline{(\bar{a}\,y)}=x\,\overline{\bar{a}\,y}.$$

To znači: iz

$$\bar{z}\,x\,\bar{y}=x\,\overline{(z^\star\,y)} \qquad \text{izlazi nužno } z^\star=\bar{z}.$$

6.3. O hermitskom sprezanju linearnih operatora. Dvojnik $A^\star$ (ili dual ili adjungiran operator) operatora A.

6.3.0. I d e j a i s v r h a.

Svrha nam je da svakom operatoru $A: V \to V$ pridružimo određen operator $A^\star$ povezan sa A, na sličan način kao što smo matrici a pridruživali hermitski pridruženu matricu $a^\star$ (v. 10, § 7.2); odmah ćemo vidjeti da u proizvoljnoj ortonormiranoj bazi operatori A, $A^\star$ imaju hermitski pridružene matrice a, $a^\star$ kao svoje zapise.

6.3.1. Definicija dvojnika $A^\star$. Zadan je vektorski prostor V i linearni operator A: $V \to V$. Za proizvoljno odabrano $x \in V$ napišimo

(6) $$(Ax) \ominus y = x \ominus A^\star y \qquad (y \in V).$$

Ukoliko $A^\star y$ postoji za svako $y \in V$, dobije se time operator $A^\star$: $V \to V$; naziva se *adjungiran operator operatora A*. Odmah ćemo dokazati da $A^\star$ postoji, da je jednoznačno određen, linearan i involutivan.

6.3.2. Postojanje. Treba imati na umu da u (6) stoje i lijevo i desno kompleksni brojevi. Zato prelazeći u (6) na obje strane na spregnute vrijednosti, izlazi, prema hermitskom uslovu (S_1) za množenje vektora:

$$y \ominus (Ax) = A^\star y \ominus x,$$

tj. identički

(7) $$A^\star \vec{y} \ominus \vec{x} = \vec{y} \ominus (A\vec{x}).$$

A (v. 17 § 2.4_3 te poglavlje 26) specijalno, za članove kakve baze e:

(7') $$A^\star e_k \ominus e_i = e_k \ominus (Ae_i) = \overline{Ae_i \ominus e_k}.$$

6.3.2.1. Lema o egzistenciji. $A^\star y = \Sigma (y \ominus Ae_i) \ominus e_i$ pri svakoj ortonormiranoj bazi $e = e_1, e_2, \ldots$

Promatrajmo neku ortonormiranu bazu $e = (e_1, e_2, \ldots)$. Tada za proizvoljni vektor x imamo rastav

(8) $$x = \Sigma x_i e_i,$$

odatle množeći zdesna sa e_k izlazi

$$x \ominus e_k = (\Sigma x_i e_i) \ominus e_k = \Sigma x_i (e_i \ominus e_k) = x_k.$$

Uvršteno u (8), daje to

(9) $$\vec{x} = \Sigma (\vec{x} \ominus e_i) e_i$$

(tu je u zagradi skalar). Za $x = A^\star y$ daje (9) ovo: $A^\star y = \Sigma (A^\star y \ominus e_i) e_i =$ $=$ (radi (7)) $= \Sigma (y \ominus Ae_i) e_i$, za čim smo i išli.

6.3.3. Linearnost operatora $A^\star$. *Operator $A^\star$ definiran u* § 6.3.2. *je linearan.*

To izlazi neposredno iz linearnosti operatora A i obrasca u § 6.3.2.

6.3.4. Jednoznačnost operatora $A^\star$. *Operator $A^\star$ je jednoznačan.* Neka je uz (6) također

(6') $$(Ax) \ominus y = x \ominus (By) \quad \text{za svako} \quad x, y \in V.$$

Oduzimajući (6') od (6) izlazi

(10) $$0 = x \ominus (A^\star - B) y \quad \text{za svako} \quad x \in V \text{ i svako } y \in V.$$

Kako za odabrano $y \in V$ jednakost (10) stoji za svako $x \in V$ mora (v. 13, § 8.12) drugi činilac biti $\vec{0}$, tj.

(11) $$(A^\star - B) y = \vec{0} \quad (y \in V).$$

No, (11) znači upravo da je $A^\star - B =$ konstanta $\vec{0} \in V$, tj. imamo $A^\star = B$, za čim smo i išli.

6.3.5. Lema o involutivnosti

$$(A^\star)^\star = A, \quad \text{tj.} \quad A^{\star\star} = A.$$

Naime, $A^{\star\star} y = (A^\star)^\star y =$ (prema 6.3.2) $= \Sigma (y \ominus A^\star e_i) e_i =$ (radi (6)) $= \Sigma (Ay \ominus e_i) e_i =$ (radi (9)) Ay.

6.3.6. Matrični zapis. Pogledajmo vezu između matričnog zapisa operatora A i njegova sudruga $A^\star$. Nađimo desnu stranu u (7) prema (9). Izlazi najprije (A komutira sa Σ i sa skalarom $(x \ominus x_i)$):

$$Ax = \sum_i (x \ominus e_i) A e_i. \tag{12}$$

(tu je u zagradi skalar!).

Ako u identitet (10) uvrstimo $x = Ae_k$, daje (9) ovaj materijal

$$Ae_k = \Sigma \underbrace{(Ae_k \ominus e_i)} e_i = \sum_i a_{ik} e_i, \quad a_{ik} = Ae_k \ominus e_i$$

za stupac zapisa, pa matrični zapis operatora A u bazi e glasi:

$$a_{ik} = Ae_k \ominus e_i. \tag{13}$$

To je identitet. On daje posebno za operator $A^\star$:

$$a_{ik}^\star = A^\star e_k \ominus e_i. \tag{14}$$

Uvrsti li se (14) i (13) u (7′), izlazi:

$$a_{ik}^\star = \overline{a_{ki}}, \quad \text{tj.} \quad a^\star = a^{-T}.$$

$\longrightarrow$ 6.3.7. ***Teorem: U svakoj ortonormiranoj bazi zapisi od konjugiranih ili spregnutih operatora su hermitski konjugirane matrice.***

6.3.8. Naravno da smo svojstvom 3.3. mogli također *definirati* sprezanje $A \to A^\star$ među linearnim operatorima. Ipak smo odabrali gornju definiciju da služi kao uzor. A metodu koja izvire iz 3.3. možemo upotrijebiti da definiramo:

6.3.9. Transponirani operator $A \to A^T$. Ako operator A u nekoj ortonormiranoj bazi ima svoj zapis a, onda transponirani zapis a^T, po definiciji, pripada operatoru koji se označuje sa A^T i zove se *transponat od A ili simetrična slika od A.* Shematski:

$$\begin{array}{ccc} A & \text{Def.} & A^T \\ \downarrow & & \uparrow \\ a & \longrightarrow & a^T \end{array}$$

Pri tom A^T ne zavisi od posmatrane ortonormirane baze.

6.3.10. Elementarna svojstva operatora $\star$ i T.

(I) $$A^{\star\star} = A, \quad A^{TT} = A$$

(involutivnost).

(II) $$(A+B)^{\star} = A^{\star} + B^{\star}, \quad (A+B)^T = A^T + B^T$$

(homomorfno svojstvo prema $+$).

(III) $$(zA)^{\star} = \bar{z} A^{\star}, \quad (zA^T) = zA^T$$

(za svaki kompleksni broj z)

(IV) $$(AB)^{\star} = B^{\star} A^{\star}, \quad (AB)^T = B^T A^T$$

(okrenuta homomorfija prema množenju).

(V) Za skalarne matrice z je $z^{\star} = \bar{z}$, $z^T = z$.

Ukažimo specijalno na (III): *sprezanje nije homotetično, dakle nije ni homomorfno prema množenju skalarom* z; naime imamo:

$$(zA)^{\star} = z^{\star} A^{\star} \neq z A^{\star}.$$

Ne brkajmo svojstvo III sprezanja i naredno svojstvo homotetičnosti operatora $A^{\star}$:

$$A^{\star} (z\vec{x}) = z A^{\star} \vec{x} \text{ za svaki skalar } z \text{ i svaki vektor } \vec{x}.$$

Svaki operator $A^{\star}$ je linearan ali pridruživanje

$$A \to A^{\star}$$

nije linearno.

6.4. Hermitski operatori *jesu oni za koje je* $A^{\star} = A$. Oni će nas specijalno interesirati. Interes je za njih velik u praksi jer vrijedi:

6.4.1. *Svaki hermitski operator* H *zadovoljava relaciju*

$$H\vec{x} \ominus \vec{x} \in R \text{ (R je skup realnih brojeva).}$$

To je poseban slučaj relacije:

6.4.2. Teorem. $x \ominus Hy = \overline{y \ominus Hx}$ *za svaki hermitski operator* H *i svaki par vektora* x, y.

Dokažimo posljednju relaciju. Radimo matrično. Naime, odabirajući ortonormiranu bazu, operatorsko razmatranje se svodi na matrično. Dokažimo:

6.4.3. Lema. *Za hermitske matrice* h *imamo:*

$$\vec{x}^{\star} (h\vec{y}) = \overline{\vec{y}^{\star} (h\vec{x})}.$$

No,

$$x^\star(hy)=\sum_i \bar{x}_i (hy)_i=\sum_i x_i^\star \sum_k h_{ik} y_k=\sum_{i,k} x_i^\star (h_{ik} y_k)=\sum_{i,k} \overline{x_i (h_{ik} y_k)^\star}=$$

$$=\text{(po obrascima o distribuciji i involutivnosti)}=$$

$$=\overline{\sum_{i,k} x_i h_{ik}^\star y_k^\star}=(\text{zbog } H^\star=H)=\overline{\sum_k y_k^\star \sum_i h_{ki} x_i}=\overline{\sum_k y_k^\star (hx)_k}=\overline{y^\star (hx)}.$$

Time je obrazac dokazan.

7. KOVARIJANTNE I KONTRAVARIJANTNE KOORDINATE VEKTORA

Radi jednostavnosti govorit ćemo o radijus-vektorima u ravnini. No, simbolika će biti takva da se razmatranja mogu neposredno primijeniti u euklidski prostor sa 3, 4, 5, ... dimenzija kao i hermitske prostore.

7.1. Kontravarijantne koordinate. Neka je O bilo koja tačka ravnine, a e_1 i e_2 bilo koja dva linearno nezavisna vektora sa zajedničkim početkom O; to znači da vektori e_1, e_2 ne leže u istom pravcu i da čine bazu $e=(e_1, e_2)$.

Za svaki vektor x postoji jedan jedini par brojeva x_1, x_2 sa svojstvom da bude

(1) $$x=x_1 e_1+x_2 e_2,$$

tj. vektor x se može na jedan jedini način linearno izraziti pomoću osnovnih vektora e_1, e_2.

Brojevi x_1 i x_2 zovu se *kontravarijantne koordinate vektora x s obzirom na zadanu koordinatnu bazu e_1, e_2.*

7.2. Kovarijantne koordinate. No, vektorom x određeni su i brojevi

(2) $$\xi_1=x\ominus e_i \qquad (i=1,\ 2).$$

To su *skalarne projekcije* zadanog vektora na jediničnim vektorima e_1, e_2. Obrnuto: uređenim parom (ξ_1, ξ_2) potpuno je određen vektor x ako imaju biti ispunjene relacije (2). Stvarno, završetak vektora x leži na pravcu koji kroz tačku ξ_1 na koordinatnoj osi e_1 stoji okomito na e_1; isto tako, završetak vektora x leži na okomici kroz tačku ξ_2 na koordinatnoj osi e_2; kao presjecište tih dviju okomica, kraj vektora x je potpuno određen. Uređen par brojeva ξ_1, ξ_2 zove se *kovarijantne koordinate vektora x.*

7.3. Norma vektora v. Norma Nx vektora x definira se kao $Nx=x\ominus x$. Najprije, zbog (1) vrijedi

(3) $$Nx=e_1^2 x_1^2+2 e_1 e_2 x_1 x_2+e_2^2 x_2^2.$$

Prema tome, *Nx je kvadratna forma svojih kontravarijantnih koordinata,* a za matricu a vrijedi $a_{ik}=e_i \circ e_k$; možemo pisati

(4) $$Nx=x^T ax, \quad a_{ik}=e_i \circ e_k.$$

Množeći relaciju (1) zdesna sa e_i, proizlazi s obzirom na (2):

$$\xi_i = x_1 e_1 e_i + x_2 e_2 e_i, \quad (i=1,\ 2). \tag{5}$$

Formulama (5) povezane su kontravarijantne i kovarijantne koordinate međusobno. Formule (5) možemo pisati pomoću matrica:

$$\xi = x^T a, \quad \xi = \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix}, \quad x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}. \tag{6}$$

Vidimo da se u (4) za Nx i u (6) za ξ javlja *ista* matrica a.

S obzirom na (5) postaje relacija (3):

$$Nx = \xi x \tag{7}$$

ili eksplicitno:

$$Nx = \xi_1 x_1 + \xi_2 x_2 = \begin{bmatrix} \xi_1 \, \xi_2 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}. \tag{8}$$

Vrijedi važno pravilo:

⟶ **7.3.1.** Teorem. *Norma vektora jednaka je skalarno-hermitskom produktu njegovih kovarijantnih i kontravarijantnih koordinata.*

7.3.2. Posljedica. *Izraz* $\xi x_1 + \xi_2 x_2$ *kao norma vektora nezavisan je od izbora osnovnih vektora; specijalno, mogu osnovni vektori biti nejednakih dužina.*

7.4. Promjena koordinatne baze. — **7.4.1.** Umjesto baze e osnovnih vektora e_1, e_2 uzmimo novu osnovu e' sastavljenu od vektora e_1', e_2' a na osnovu veze

$$e' = et; \quad \text{tj.} \quad e_i' = t_{1i} e_1 + t_{2i} e_2, \tag{1}$$

naravno da transformacija t mora biti regularna, tj. $\det t \neq 0$.

7.4.2. U novom koordinatnom sistemu neka vektor x iz § 1. ima kovarijantne koordinate ξ_1', ξ_2' a kontravarijantne x_1', x_2'. Radi se o tome da izrazimo vezu među starim i novim kovarijantnima te među starim i novim kontravarijantnim koordinatama. Radimo ovdje kao da smo u hermitskoj „ravnini" C_2.

Pomnožimo li (1) hermitski lijevo sa x, proizlazi

$$x \ominus e_i' = x \ominus t_{1i} e_1 + x \ominus t_{2i} e_2 = \overline{t_{1i}} (x \ominus e_1) + \overline{t_{2i}} (x \ominus e_2),$$

odnosno, s obzirom na definiciju kovarijantnih komponenata u starom i novom sistemu:

$$\xi_i' = \xi_1 \overline{t_{1i}} + \xi_2 \overline{t_{2i}}, \quad \text{tj.} \quad \vec{\xi}' = \vec{\xi} \ominus t. \tag{2}$$

Dakle se *kovarijantne koordinate transformiraju na isti način kao i osnovni vektori: ista transformacija t vrši tu dužnost. K tome kovarijantne koordinate ispisujemo kao redić (a ne kao stupac).*

7.4.3. Treba još odrediti vezu među *starim i novim kontravarijantnim koordinatama* x_1, x_2 i x_1', x_2'; ta se veza određuje iz postojanosti (invarijancije) izraza za Nx, tj. iz identiteta

$$\begin{aligned}\xi_1 \bar{x}_1 + \xi_2 \bar{x}_2 &= \xi_1' \overline{x_1'} + \xi_2' \overline{x_2'} = (\text{ovaj izraz zbog } (2) = \\ &= (\bar{t}_{11} \xi_1 + \bar{t}_{21} \xi_2) \overline{x_1'} + (\bar{t}_{12} \xi_1 + \bar{t}_{22} \xi_2) \overline{x_2'} = \\ &= \xi_1 (\bar{t}_{11} \overline{x_1'} + \bar{t}_{12} \overline{x_2'}) + \xi_2 (\bar{t}_{21} \overline{x_1'} + \bar{t}_{22} \overline{x_2'}).\end{aligned}$$

Izjednačujući početnu stranu i završnu stranu toga lanca, prelazeći na konjugirane vrijednosti, dobivamo tražene formule

$$\begin{aligned} x_1 &= t_{11} x_1' + t_{12} x_2' \\ x_2 &= t_{21} x_1' + t_{22} x_2' \end{aligned} \qquad \vec{x} = t\,\vec{x}'. \tag{3}$$

Odatle

$$\vec{x}' = t^{-1} \vec{x} = t^{-1} [x_1, x_2]^T \quad \text{tj.} \quad [x_1', x_2'] = [x_1\ x_2]\, t^{\sim}. \tag{4}$$

Dakle se kontravarijantne koordinate x_1, x_2 i kovarijantne koordinate ξ_1, ξ_2 ne transformiraju na isti način: dok se posljednje izražavaju istom transformacijom t kojom se transformiraju osnovni vektori (isp. (1)), dotle se nove kontravarijantne koordinate x_1', x_2' izražavaju pomoću starih kontravarijantnih koordinata x_i *kontragredijentnom* transformacijom $t^{\sim} = (t^T)^{-1}$.

—→ **7.4.4. Teorem.** ***Ako umjesto koordinatne vektorske baze $e = [e_1\, e_2 \ldots]$ uvedemo novu vektorsku bazu $e' = [e_1', e_2', \ldots e_n']$ vezom***

$$e' = e\,t,$$

odnosno

$$[e_1' \ldots e_n'] = [e_1 \ldots e_n]\, t, \quad t = [t_{ik}], \quad (i,\ k = 1 \ldots n),$$

tada za svaki vektor

$$x = \sum_{\nu=1}^{n} x_\nu e_\nu = \sum_{\nu=1}^{n} x_\nu' e_\nu'$$

vrijedi

$$[\xi_1', \ldots, \xi_n'] = [\xi_1, \ldots, \xi_n]\, t, \quad \xi_\nu' = x \ominus e_\nu', \quad \xi_\nu = x \ominus e_\nu$$

$$[x_1', \ldots, x_n'] = [x_1, \ldots, x_n]\, t^{\sim}, \quad t^{\sim} = \overline{t^{-1}}:$$

kraće

$$\underset{\to}{\xi}' = \underset{\to}{\xi}\, t, \quad \vec{x}'^T = \vec{x}^T t^{\sim},$$

odnosno

$$\vec{x}' = t^{-1} \vec{x}$$

$$\vec{\xi}' = t^T \vec{\xi},$$

tj. nove kovarijantne (kontravarijantne) koordinate dobijaju se iz starih pomoću iste (kontragradijentne) transformacije. No, unutrašnji produkt jednih i drugih koordinata ostaje isti: $\xi\, \bar{x} = \xi' \bar{x}'$.

Tako vidimo da se uz vektore-stupce $\vec{x}$, $\vec{x}'$ (bolje bi bilo pisati $x\downarrow$, $x'\downarrow$) pojavljuju i vektori-redići $\underset{\rightarrow}{\xi}$, $\underset{\rightarrow}{\xi}'$.

7.4.5. Služeći se terminologijom iz statistike čvrstog tijela, pri čemu izraz $\sum\limits_i x_i \xi_i$ podsjeća na rezultat istodobnog djelovanja dviju sila na neko čvrsto tijelo, a da ne utječu na njegovu ravnotežu, možemo reći da se promjene (varijacije) komponenata x_1, x_2 s jedne strane i komponenata ξ_1, ξ_2 s druge strane kao kompenziraju djelujući jedne protiv drugih. Zato se i kaže da su ξ_1, ξ_2 *kovarijantne* koordinate vektora x, jer se transformiraju *istom* transformacijom kojom i osnovni vektori; za razliku od njih, koordinate x_1, x_2 zvat će se *kontravarijantnima.*

8. Zadaci o komponentama vektora.

1. Nađi skalarni i hermitski produkt ovih vektora zadanih u ortonormiranoj osnovi: 1) (3, 4, 5), (—2, 3, 4); 2) (—2, i, 4), (5, 2, $3i$); 3) (2, $5i$, $3-i$), (i, $5+2i$, $-i$); 4) ($2-3i$, $5+i$, $4i$), (i, $-i$, 1).

2. Odredi Gramovu determinantu i ispitaj da li su ovi vektori međusobno linearno zavisni: 1) (3, 4), (5, 7); 2) (1, 2, 3), (—2, 3, 4), (0, 3, 7); 3) (1, —2, 4), (2, 6, 9), (4, 2, 17); 4) (7, 1, 3, 4), (0, 1, 3, 4), (7, 3, 9, 12), (0, —1, —3, —4).

3. Ortogonaliziraj i ortonormiraj ove vektore:
1) (1, 3), (5, 4); 2) (1, 2, 3), (—2, 3, 5), (4, 1, 0);
3) (1, 2, 1, 3), (4, 1, 1, 1), (3, 1, 1, 0); 4) (1, i, 2), ($2-3i$, $4+3i$, i).

4. Nađi kovarijantne i kontravarijantne koordinate vektora $\vec{a}$ u bazi e, ako je: 1) $\vec{a}=(2, 3)$, $e_1=(1, 0)$, $e_2=(0, 1)$; 2) $\vec{a}=(2, 3)$, $e_1=(2, 0)$, $e_2=(0, 1/4)$; 3) $\vec{a}=(2, 3)$, $e_1=(3, 4)$, $e_2=(-5, 6)$; 4) $\vec{a}=(5, -8, 7)$, $e_1=(1, 1, 0)$, $e_2=(1, 0, 1)$, $e_3=(0, 1, 1)$; 5) $\vec{a}=(1, 1, 1)$, $e_1=(5, 6, 7)$, $e_2=(-3, 6, 1)$, $e_3=(-2, -5, 0)$.

5. Nađi na dva načina kvadrat, odnosno normu vektora $\vec{v}$, ako je:
1) $\vec{v}=[3, 4)$, $e_1=(1, 0)$, $e_2=(0, 3)$; 2) $\vec{v}=(3, 4)$, $e_1=(1, 1)$, $e_2=(3, 4)$,
3) $\vec{v}=(1, -2, 3)$, $e_1=(1, 3, 4)$, $e_2=(5, -1, 4)$, $e_3=(4, -5, 7)$.

6. Zadane su vektorske baze e, e' i vektor $\vec{v}$ u ortonormiranoj bazi; nađi kovarijantne i kontravarijantne koordinate vektora v, ako je:

$$1)\ \vec{v}=(1, -3),\quad e=\begin{bmatrix}1 & 3\\ 2 & 0\end{bmatrix},\quad e'=\begin{bmatrix}3 & 1\\ 0 & 2\end{bmatrix};$$

$$2)\ \vec{v}=(1, 5, 8),\quad e=\begin{bmatrix}3 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 5\end{bmatrix},\quad e'=\begin{bmatrix}6 & 0 & 0\\ 0 & 4 & 0\\ 0 & 0 & 10\end{bmatrix};$$

3) $\vec{v}=(1, 1, -1), \quad e=\begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}, \quad e'=\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}.$

4) $\vec{v}=(3, -4, 2, 1)^T, \quad e=\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad e'=e^T,$

5) $v=[v_1, v_2, .., v_n], \ e'=e^T.$

6) $v=[v_1, v_2, v_3]^T, \ e'=[e_3\, e_2\, e_1].$

7) $v=[v_1, v_2, v_3, v_4]^T, \ e'=[e_4\, e_3\, e_2\, e_1].$

7. U prethodnom zadatku naći matricu prelaženja: 1) od e na e', 2) od starih kovarijantnih koordinata na nove kovarijantne koordinate; 3) od starih kontravarijantnih na nove kontravarijantne koordinate.

1′—7′. Zadaci koji se iz zadatka 1—7 dobiju tako da se u svakom promatranom vektoru koordinata x_k zamijeni sa x_k+i, $i=(-1)^{1/2}$.

8. Čitav § 7 i prethodne zadatke razmotri u simbolici pišući $e_{i'}=e_i'$, $x=\Sigma x^i e_i$ (tu je i indeks i u x^i kao i u e_i), $x_i=xe_i$, $x_{i'}=xe_{i'}$, $t^i{}_k=t_{ik}$.

9. Čitavo izlaganje razmotriti u simbolici da se hermitski produkt od x, y označuje (x, y) umjesto $x\ominus y$.

Literatura

Anđelić [1], [2]; Gantmaher [1], [2]; Kočin [1]; Kurepa S. [1]; Lichnerowicz [1]; Mal'cev [1]; Rašajski [1]; Šilov [1].

POGLAVLJE 26.

LINEARNI OPERATORI

Predstavnik linearnih operatora u prostoru R brojeva je obična *proporcionalnost*:

$$y = Hx^{1)}. \tag{1}$$

Predstavnik linearnih operatora u geometriji jest *projiciranje* (kod vektorskih prostora podloga za projiciranje je potprostor, pa nužno prolazi ishodištem). Formalna generalizacija funkcije (1) bit će *linearni operator*. Funktor H, koji stvari x pridružuje stvar Hx, zadovoljava uslovu

$$H(x+x') = Hx = Hx'$$

(*aditivnost*, odnosno *distributivnost*)

$$H(cx) = c\,Hx \quad (\textit{homotetičnost})$$

Kod linearnih operatora bit će po definiciji upravo tako. No, konstanta c će biti skalar (pripadnik nekog tijela K); produkt (unos) x i proizvod (iznos) Hx bit će vektori, tj. pripadnici neke vektorske organizacije ili vektorskih organizacija nad tijelom K.

Na osnovu dosadašnjeg „znanja" o matricama, vidimo da svaka matrica a, pridružujući iznos ax u obliku produkta, predstavlja potpuno određen linearni operator. To je slično kao što broj 2 može da posluži i za to da predstavi, svojim množidbenim svojstvom, linearno preslikavanje $x \to 2x$.

U ovom poglavlju vidjet ćemo da su matrice vrlo pogodno sredstvo za svladavanje problematike u vezi s linearnim operatorima.

1. PODSJET NA LINEARNE PROSTORE. PROSTORI K_{mn}

1.1. Polazimo od nekog tijela K; to znači da, praktički govoreći u K možemo *elementarno računati*. Kao misaoni oslonac možemo za K uzeti tijelo R realnih brojeva, tijelo C kompleksnih brojeva, tijelo Ip cifara 0, 1, ..., $p-1$ za svaki prost broj, itd.

---

[1] Slovo H treba da nas podsjeti na: homogenost, homotetičnost i homomorfiju; sva ta svojstva zastupljena su kod funkcije (1).

Vektorski prostor nad tijelom K je svaki skup V elemenata u kojem je omogućeno zbrajanje i oduzimanje uz uobičajena pravila[1] te množenje s elementima iz K; to je množenje distributivno s obzirom na zbrajanje u V i s obzirom na zbrajanje u K:

$$a(x+y)=ax+ay \quad \text{za svako} \quad a\in K,\ x\in V,\ y\in V$$

$$(a+b)x=ax+bx \quad \text{za svako} \quad a\in K,\ b\in K,\ x\in V.$$

Nadalje mora biti

$$a(bx)=(ab)x \quad \text{za svako} \quad a, b\in K, \text{ i } x\in V.$$

zatim $1\vec{x}=\vec{x}$ te $0\cdot\vec{x}=\vec{0}$ za svako $\vec{x}\in V$ (isp. pogl. 13, § 3).

Znajmo da tijelo K ima svoju 0 i svoju jedinicu 1; prostor V ima također svoju 0 (može se označiti sa $\vec{0}$ u slučaju potrebe).

1.2. Primjer. Svi vektori položaja sa zadanim polom O kao početkom čine određen vektorski prostor. Skup K^{In} svih n-članih nizova kojima su članovi u K čine također određen vektorski prostor. Međusobno zbrajanje te množenje skalarom vrši se na običan način: nizovi (funkcije) se zbrajaju zbrajajući im odgovarajuće članove (vrijednosti), niz se množi skalarom da se svaki član pomnoži skalarom.

Skup svih realnih funkcija koje su definirane npr. u segmentu $R[0, 1]$ realnih brojeva $0\leq x\leq 1$ čine vektorski prostor.

1.3. Vektorski prostor K_{mn}. Polazeći od nekog tijela K i para (m, n) brojeva, neka

$$K_{mn}$$

znači množinu svih matrica formata $m\times n$ s vrijednostima u K; to znači da je K_{mn} skup svih jednoznačnih preslikavanja umnoška $Im\times In$ u K (potpunija oznaka za K_{mn} bila bi $K^{Im\times In}$). Skup K_{mn} je linearni prostor, pri čemu se adicija u K_{mn} i množenje $\dot{K}\cdot\dot{K}_{mn}$ definira na uobičajeni način.

Specijalno imamo prostor K_{1n} redaka i prostor K_{n1} stupaca. Ako ne bude zabune, sa K_n ćemo označivati bilo koji od ta dva prostora. Ta su dva prostora izomorfna, i to operacijom transponiranja:

$$x\in K_{1n} \xrightarrow[1]{} x^T\in K_{n1},\ K_{1n}{}^T=K_{n1}.$$

Pri tom, naravno,

$$(x+y)^T=x^T+y^T$$

$$(\alpha x)^T=\alpha(x^T).$$

[1] Tačna definicija nalazi se u pogl. 13, § 3. Znajmo da je V u prvom redu grupa koju pišemo aditivno (*zbrajanje vektora*!).

2. DEFINICIJA LINEARNOG OPERATORA VEKTORSKOG PROSTORA V PREMA VEKTORSKOM PROSTORU V'

2.1. Definicija. Neka je (V, V') uređena dvojka linearnih prostorâ u odnosu na **isto** tijelo K. Svako jednoznačno preslikavanje H od V ka V'

$$H: V \longrightarrow V',$$

koje je:

1) aditivno: $\quad H(x+y)=Hx+Hy,$

2) homotetično $\quad Hax=a\,Hx \quad$ za svako $\quad a\in K$

zove se *linearno preslikavanje* ili *linearni operator* u prostoru V s vrijednostima u V'. Govori se o homomorfizmu prostora V prema prostoru V'.

U specijalnom slučaju, kad je i obratno preslikavanje jednoznačno, zove se H *izomorfno preslikavanje* od V prema V' (isp. pogl. 13, § 4.6 kao i pogl. 17, § 2.4). Znak HV označuje skup svih Hx kad $x\in V$. Za dano $y\in HV$ neka $H^{-1}y$ označuje svako $x\in V$ za koje je $Hx=y$; sa $H^{-1}\{y\}$ označit ćemo *skup svih takvih* $x\in V$ *za koje je* $Hx=y$. Slično za kakav skup $Y\subset HV$ označit ćemo sa $H^{-1}Y$ uniju (zbir) svih skupova $H^{-1}\{y\}$ za $y\in Y$:

$$H^{-1}Y=\bigcup_{y\in Y}H^{-1}\{y\}.$$

2.1.1. Primjedba. Svako linearno preslikavanje $H: V\rightarrow V'$ je određena homomorfija grupe $(V, +)$ prema grupi $(V', +)$; to je upravo sadržaj uslova s aditivnim svojstvom za H. Zato se mogu odmah primijeniti stavovi o homomorfizmu grupa i grupoida. Treba primijetiti da u općem slučaju V' nije homomorfno sa V, jer će HV obično biti *pravi* dio od V' i nije $=V'$ (v. pogl. 17, § 2.4).

2.2. Primjeri linearnih preslikavanja. Konstantno preslikavanje $x\rightarrow 0$ je linearno. Identično preslikavanje $x\rightarrow x$ također; preslikavanje $(x_0\, x_1\, x_2)\longrightarrow x_0$ je linearno preslikavanje (projiciranje) prostora K^{I_3} u K. Rotacija oko 0 također. Ako neprekidnoj realnoj funkciji f s oblasti $R[0, 1]$ pridružimo funkciju

$$\int_0^x f(t)\,dt \quad x\in R[0, 1] \quad \text{odnosno broj} \quad \int_0^1 f(t)\,dt$$

dobivamo dva linearna preslikavanja vektorskog prostora V svih funkcija f u sama sebe, odnosno u tijelo R realnih brojeva.

2.3. Karakterističan primjer matrica. Svaka matrica a stupnja ili formata

$$(n, s) \quad \text{tj.} \quad a\in K_{ns},$$

predstavlja određen linearni operator od prostora K_{s1} od s dimenzija ka prostoru K_{n1} od n dimenzija. Specijalno, ako je a regularna matrica formata $n\times n$, tada ona preslikava K_{n1} na čitavo K_{n1}.

Naime, neka je $v\in K_{s1}$, tj. v je određen stupac $v=v\!\downarrow$ od s članova; tada je za svaku matricu $a\in K_{ns}$ produkt $av\!\downarrow$ određen i očigledno je $av\!\downarrow\in K_{n1}$. Nadalje je $a(v\!\downarrow+w\!\downarrow)=av\!\downarrow+aw\!\downarrow$, $a(\lambda v\!\downarrow)=\lambda av\!\downarrow$ za svaki skalar λ.

2.4. Linearne forme u prostoru — dual zadanog prostora. — 2.4.1. Definicija. *Svaki linearni operator vektorskog prostora $V(K)$ u prostor skalara K zove se linearna forma u prostoru V; tako je npr. traženje prve koordinate* (druge koordinate) svakog vektora linearna forma. Ako su F, G dvije linearne forme $V \to K$, tada ćemo, naravno, pod $F+G$ razumijevati onaj operator za koji je $(F+G)x = Fx+Gx$ za svako $x \in V$; isto tako, za svaki skalar λ definira se λF po poslu $(\lambda F)x = \lambda(Fx)$.

Sad se odmah vidi da i sve linearne forme prostora V čine, sa svoje strane, potpuno određen vektorski prostor; zove se *dual od* V i označuje sa $V^\star$.

$\longrightarrow$ **2.4.2. Ako je** $\dim V < \infty$, **prostori** V **i** $V^\star$ **su izomorfni** (mada su sastavljeni od tako različitih elemenata).

Skicirajmo dokaz za slučaj da je $\dim V = 2$. Neka je $e = (e_1, e_2)$ baza u V; tada za svaki vektor $x \in V$ imamo koordinate x_1, x_2 po rastavu $x = x_1 e_1 + x_2 e_2$; pri tom je $x_1, x_2 \in K$ (tj. x_1, x_2 su skalari). No, za svaku linearnu formu $F: V \longrightarrow K$ imamo tada $Fx = x_1 Fe_1 + x_2 Fe_2$; ako, dakle, znamo skalar Fe_1 i skalar Fe_2, znamo i formu F; i obratno: za uređen par skalarâ $\varphi_1, \varphi_2 \in K$ postoji jedna jedina linearna forma F za koju je $F_{e1} = \varphi_1$, $F_{e2} = \varphi_2$.

A sad promatrajmo recimo ove dvije linearne forme e^1 i e^2 za koje je

$$\begin{matrix} e^1 e_1 = 1, & e^2 e_1 = 0 \\ e^1 e_2 = 0 & e^2 e_2 = 1 \end{matrix} \quad \text{ili u matričnom zapisu} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ tj. } e^i e_k = \delta_{ik}.$$

Onda one čine bazu u dualu $V^\star$; naime, za svaku linearnu formu F vrijedi

$$(\star) \qquad Fx = Fe_1 e^1 x + Fe_2 e^2 x = (Fe_1 e^1 + Fe_2 e^2) x$$

jer relacija $(\star)$ vrijedi u bazi (e_1, e_2) prostora V (zamijeni $x = e_1, e_2$).

Prema tome, $\dim V^\star = 2 = \dim V$. Uostalom, zbog rečenog, pridruživanje

$$\left.\begin{matrix} x \in V \\ x = x_1 e_1 + x_2 e_2 \end{matrix}\right\} \Rightarrow \begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix} \text{ u } V^\star$$

jest izomorfija između V i $V^\star$; pri tom matricom $\begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix}$, *po definiciji*, zapisujemo operator X, za koji je

$$Xe_1 = x_1, \; Xe_2 = x_2.$$

Moglo bi se i pisati $X = x_1 e_1 + x_2 e_2$.

Ovaj je primjer vrlo instruktivan; pojmovno je malo teži. No, on je karakterističan za matrično zapisivanje (prikazivanje) operatora. To će nas neprestano dalje pratiti.

2.4.3. Duali 2, 3 reda prostora V.

2.4.3.1. Definicija. Dual $(V^\star)^\star$ dualna prostora $V^\star$ zove se *dual drugog reda* V i označuje se sa $V^{\star\star}$ ili $V^{(\star 2)}$. Isto tako se definira

$$V^{\star\star\star} := V^{(\star 3)} := (V^{\star\star})^\star, \ldots, V^{(\star n+1)} := (V^{(\star n)})^\star \; (n = 1, 2, \ldots).$$

Na taj način imamo niz $V^{(\star n)}$ $(n = 0, 1, 2, \ldots)$ pri čemu stavljamo $V^{(\star 0)} = V$.

2.4.4. Prostor $V^{\star\star}$ kao proširenje od $V^{\star}$.

Neka je $v \in V$ zadano; promatrajmo preslikavanje f_v:

(1) $$y \in V^\star \to f_v(y) = y(v) \in K.$$

Ono je linearno preslikavanje od $V^\star$ u K, pa je dakle $f_v \in V^{\star\star}$, tj. imamo preslikavanje

(2) $$v \in V \to f_v \in V^{\star\star}.$$

Preslikavanje (2) je jednolisno:

$$v, w \in V, v \neq w \Rightarrow f_v \neq f_w.$$

Naime, $\vec{u} := v - w \neq 0$ pa je dovoljno posmatrati: neku bazu e u V kojoj je u član i ono linearno preslikavanje $a | V$ za koje je $au = 1 \in K$, $ax = 0 \in K$ za svako

$$x \in e \text{ pri } x \neq u.$$

Očigledno je $a \in V^\star$. No, $a \neq 0$ jer je posebno $a(v-w) \neq 0$, tj. $av - aw \neq 0$ i $f_v \neq f_w$.

Na taj način vidimo da na prirodan način imamo izomorfizam (2) između V i podprostora f_V svih $f_v (v \in V)$ prostora $V^{\star\star}$.

Preslikavanje (1) definirali smo ne služeći se bazom. Zato je prirodno da preslikavanje (1) interpretiramo odnosno poistovetimo sa v jer je v uzročnik i nosilac preslikavanja (1). No, tim dogovorom imamo

$$v \in V \Rightarrow v \in V^{\star\star}, \quad \text{tj.} \quad V \subset V^{\star\star}.$$

2.4.5. Povratni (refleksivni) prostori.

Ako je $V = V^{\star\star}$, prostor V se zove *povratan* (*refleksivan*), a ako je $V \neq V^{\star\star}$, prostor V se se zove *nepovratan* (*irefleksivan*).

2.4.6. Teorem $\dim V < \infty \Leftrightarrow V = V^{\star\star}$.

Dokaz. Neka je e baza u V; definirajmo $e^\star$ kao skup svih funkcionala oblika g_x:

$$x \in e \to g_x v = \delta_{xv} = {}^{1}_{0} \text{ pri } x {}^{=v}_{\neq v}.$$

Ako je $\dim V < \infty$, onda je e konačno pa je $e^\star$ baza u $V^\star$ istobrojna sa e (dokaz sličan kao u t. 2.4.2). Ako je $\dim V = \infty$, $e^\star$ je beskonačan podskup neke beskonačne osnove M prostora $V^\star$.

No, postoji $g \in V^{\star\star}$ za koje je $gx = 1 \in K$ za svako $x \in M$; naravno, $g | V^\star$ je jednoznačno određen. Međutim, $g \neq f_v$ za svako $v \in V$. Naime, $v = \sum_x v_x x \, (x \in e)$ i pri tom $v_x \neq 0$ može biti ispunjeno samo na konačnom ili praznom podskupu e_0 od e.

Dakle je $v = \sum_x v_x x$; pri $x \in e_0$ te pri $y \in V^\star$ imamo

$$f_v y = y(v) = y\Big(\sum_{x \in e_0} v_x x\Big) = \sum_{x \in e_0} y(v_x x) = \sum_{x \in e_0} v_x y(x).$$

Posebno pri $y \in e^\star \setminus e_0^\star$ bit će $f_v y = v_y y(y) = 0$. Naprotiv $gy = 1$ i za svako takvo y.

2.4.7. Primjedba. Prema teoremu 3.4.6 nijedan vektorski prostor sa ∞ dimenzija nije refleksivan; zato se $V^\star$ definira drukčije i to kao skup svih omeđenih linearnih homogenih funkcija $V \to K$ (v. S. Aljančić [1] str. 238).

2.5. Zadaci o linearnim operatorima.

1. Odredi koja su od ovih preslikavanja f linearni operatori a koja nijesu: 1) $fx = 2x$, $x \in R$; 2) $fx = 2x + 1$, $x \in R$; 3) $fx =$ konstanta c; 4) $fx = 2x$, $x \in V(R)$; 5) $fx = \frac{d}{dt} x$, x prolazi skupom svih realnih izvodljivih funkcija; 6) $fx =$ projekcija od x na vektor $e_1 = (1, 0, 0)$ prostor R^3; 7) $fx =$ projekcija od x na ravninu e_1, e_2 prostora R^3; 8) f je rotacija ravnine R^2 oko 1) tačke $(0, 0)$, 2) oko tačke $C \in R_2 \setminus \setminus \{0, 0\}$; 9) f je rotacija prostora oko prve koordinatne osi.
2. U zatvorenom intervalu $R[a, b]$ realnih brojeva zadana je funkcija $K(t, s)$ za koju postoji $F(t) = \int_a^b K(t, s) x(s) ds$; je li F linearan operator?
3. Ako je $e = (e_1, e_2, e_3)$ vektorska baza prostora R_3, a (v_1, v_2, v_3) bilo koja uređena trojka članova iz R^3, tada postoji jedna jedina linearna forma L za koju je $Le_{3'} = v_{3'}$ $(3' = 1, 2, 3)$; dokaži i generaliziraj za svaki prirodni broj n.
4. Neka je a zadan član euklidskog vektorskog prostora R_n; neka je (a, x) skalarni produkt od a, x; 1) je li preslikavanje $x \in R_n \to (a, x)$ linearan operator? 2) Dokaži da za svako linearno preslikavanje $f : R_n \to R$ vrijedi $fx = (a_f, x)$ gdje je a_f određen član iz R_n zavisan od a; za $f \neq f'$ vrijedi $a_f \neq a_{f'}$; 3) Je li skup svih $L_a (a \in R_n)$ izomorfan sa R_n?
5. Isto pitanje za unitarni prostor C_n (isp. § 3.2).
6. Odredi nekoliko članova dualnog prostora $V^\star$ ako V znači: 1) R; 2) R^2; 3) prostor svih polinoma $p(x)$ stepena ≤ 2.
7. Dokaži: ako je $(e_1, e_2, \ldots, e_n)$ baza linearnog prostora V_n, tada funkcije $e^{n'}$ za koje je $e^{n'}(e_k) = \delta^{n'}{}_k$ $(n', k = 1, 2, \ldots, n)$ čine odgovarajuću bazu dualnog prostora $V_n^\star$ (isp. § 2.4.2 za $n = 2$).

3. NEKOLIKO SVOJSTAVA LINEARNIH OPERATORA

Neka je

$$H : V \to V'$$

proizvoljno linearno preslikavanje prostora V u prostor V'; to znači specijalno da je $HV \subset V'$. Dokazat ćemo nekoliko jednostavnih svojstava svakog takva preslikavanja H; posebno, da je i HV linearni prostor; nadalje, da je za svaki potprostor $P' \subset V'$ skup $H^{-1} P'$ određen potprostor u V; posebno, da je $H^{-1}\{0\}$ određen potprostor u V. Svojstva su zaista slična svojstvima obične proporcionalnosti.

3.1. Teorem.

(1) $$H(-x) = -Hx,$$

tj. protivni elementi x, $-x$ *iz* V *prelaze u protivne elemente* Hx, $-Hx$ *u* V'. *Specijalno,* 0 *iz* V *prelazi u* 0[1] *iz* V' *tj.* $H0=0$ (isp. pogl. 17, § 4.2).

(2) $$H(k_0 x_0 + k_1 x_1) = k_0 Hx_0 + k_1 Hx_1 \quad i\ uopće \quad H(\sum k_{n'} x_{n'}) =$$
$$= \sum k_{n'} Hx_{n'} \quad za\ svaki\ niz \quad k_{n'} \in K \quad i \quad x_{n'} \in V.$$

Po definiciji, $-x$ znači da je $x+(-x)=0$. Odatle

$$H(x+(-x)) = H0.$$

odnosno zbog distributivnosti:

(1) $$Hx + H(-x) = H0.$$

Dokažimo da je

(2) $$H(-x) = -Hx.$$

Dokažimo najprije da je

(3) $$-x = -1 \cdot x.$$

U stvari, imamo $1 \cdot x = x$ (aksiom o prostoru), pa

$$x + (-1)x = 1 \cdot x + (-1)x = (1 + (-1))x = 0x = 0.$$

Dakle je $x+(-1)x=0$; a to upravo znači da je $(-1) \cdot x = -x$, jer je $-x$ rješenje jednadžbe $x+y=0$.

Dokažimo sada (2). No,

$$H(-x) = (\text{prema } (3)) = H([-1] \cdot x) = (\text{homotetija!}) =$$
$$= [-1]Hx = (\text{prema } (2)) = -Hx.$$

Time je relacija (2) dokazana.

Na osnovu (2) prelazi (1) u jednakost

(4) $$Hx + (-Hx) = HO.$$

No, po definiciji, lijeva strana u (4) je upravo O (zapravo O'); a to znači da je $O' = HO$. Time je teorem 3.1 (1) dokazan.

$$H(k_0 x_0 + k_1 x_1) = (\text{aditivnost}) = H(k_0 x_0) + H(k_1 x_1) = k_0 Hx_0 + k_1 Hx_1.$$
$$H(k_0 x_0 + k_1 x_1 + k_2 x_2) = H(k_0 x_0 + k_1 x_1) + H(k_2 x_2),$$

dalje kao maloprije.

Tako se induktivno dokazuje da vrijedi i teorem 3.1 (2).

---

[1] Bilo bi pravilnije nulu u V' označiti sa O'; također bi adiciju u V' trebalo označivati recimo sa $+'$, da je možemo razlikovati od adicije $+$ u V; isto za znakove $\cdot$ i $\cdot'$; na taj način, linearnost operatora H od V prema V' izražavala bi se ovako: $H(x+y) = Hx +' Hy$, $H(\lambda x) = \lambda \cdot' Hx$. No, radi jednostavnosti postupili smo kao u tekstu.

$\longrightarrow$ **3.2. Teorem.** ***Svaki linearni operator L linearnog prostora V u linearni prostor V' ima za rezultat skup LV, koji je određen prostor u V', pa je zadano preslikavanje L homomorfija od V na čitav potprostor LV; obrnuto, za svaki potprostor $W' \subset LV$ skup $L^{-1} W'$ je određen prostor u V; specijalno, $L^{-1}\{0\}$ je određen potprostor prostora V; za svako $\vec{x} \in V$, homomorfija L je konstanta na $L^{-1}\{0\}+x$; te „parcele" $L^{-1}\{0\}+V$ polaznog prostora V jesu elementi novog prostora $V/L^{-1}\{0\}$ induciranog u V, pa je zadani linearni operator L izomorfija između tog diobenog prostora i prostora LV.***

Dokažimo npr. da iz x', $y' \in LV$ izlazi $x'+y' \in LV$. Pa neka je

$$x' = Lx,\ y' = Ly \quad \text{sa} \quad x, y \in V.$$

Tada je $\quad x'+y' = Lx + Ly =$ (po svojstvu distributivnosti) $=$ $= L(x+y) = Lz$, gdje je $z \in V$, jer je $(V, +)$ grupa. Dakle je $z \in V$, a time $Lz \in LV$, tj. $x'+y' \in LV$. Ostala svojstva skupa LV na osnovu kojih je LV određen potprostor u V' dokazuju se neposredno. Završni dio teorema dokazan je u poglavlju o grupama (osnovna veza između homomorfizma i izomorfizma (pogl. 17, § 12.5.5).

Tako npr. ako je L projiciranje prostora R^{I3} na R, tada je $L^{-1}\{0\}$ ravnina okomita x-os u početku koordinata.

3.3. Uzastopno izvođenje linearnih operatora. Ako je L linearno preslikavanje vektorskog prostora V prema V', a L' linearno preslikavanje od V' prema nekom vektorskom prostoru V'', tada je *složeno preslikavanje* $L'L$ linearno preslikavanje od V prema V''. Specijalno, ako je L linearno preslikavanje od V u sama sebe, tada je to i $L^2 = L(L)$ i $L^n = L(L^{n-1})$ za svaki prirodni broj $n > 1$. To je neposredna posljedica od 3.2. Vrijedi

$$L^m L^n = L^{m+n} \text{ i } (L^n)^m = L^{n.m}.$$

4. ODREĐENOST, RANG I DEFEKT LINEARNOG OPERATORA

4.1. Osnovni teorem o određenosti. ***Linearni operator potpuno je određen time ako je određen na nekoj bazi prostora. Drugim riječima, ako za dva linearna operatora L, B prostora V znamo da se podudaraju u nekoj bazi $e = (e_1, e_2, \ldots)$ toga prostora V, tada je $L\dot{V} = B\dot{V}$.***

Dokaz. Prema definiciji baze, svakom vektoru $v \in V$ pripada potpuno određen rastav

$$(*) \qquad v = v_1 e_1 + v_2 e_2 + \cdots = \sum v_i e_i,$$

gdje je $n = \dim V$.

Iz $(*)$ izlazi

$$Lv = L(v_1 e_1 + v_2 e_2 + \cdots) = (\text{aditivnost}) = L(v_1 e_1) + L(v_2 e_2 + \cdots) = \cdots$$

i najzad

(1) $$Lv = v_1\, Le_1 + v_2\, Le_2 + \cdots v_n\, Le_n.$$

Analogno za svaki drugi linearni operator B izlazi

(2) $$Bv = v_1\, Be_1 + v_2\, Be_2 + \cdots + v_n\, Be_n.$$

No, ako je

$$Lv_1 = Be_1,\quad Le_2 = Be_2,\ \ldots,\ Le_n = Be_n,$$

tada su desne strane u (1) i (2) jednake, pa moraju biti jednake i lijeve strane, tj. $Lv = Bv$ za svako $v \in V$.

Na osnovni teorem 4.1. pozivat ćemo se vrlo često.

4.2. Jezgro ili nula-prostor linearnog operatora. Definicija. Neka je L linearni operator $V \to V'$. Skup svih rješenja x jednadžbe $Lx = 0$ zove se *homomorfno jezgro operatora* L; možemo ga označiti sa

$$L^{-1}\{0\}.$$

Lako se vidi da je homomorfno jezgro određen prostor u V; način dokazivanja te činjenice je tipično rasuđivanje u matematici, fizici itd. pri obrađivanju linearnih problema.

Naime, ako je

$$Lx = 0,\quad Ly = 0,$$

tada predmnoženjem prve jednadžbe skalarom ξ a druge skalarom η i zbrajanjem dobivenih jednakosti izlazi:

$$\xi\, Lx + \eta\, Ly = \xi \cdot 0 + \eta \cdot 0$$

(svojstvo homotetije: skalar i operator komutiraju):

$$L\xi\, x + L\eta\, y = 0$$

(svojstvo aditivnosti):

$$L(\xi\, x + \eta\, y) = 0,$$

tj. *svaki linearni spoj svakog para iz jezgra opet je u jezgru.* To upravo znači da je jezgro prostor.

4.3. Defekt linearnog operatora. Što je jezgro operatora L veće, to znači da je to teže iz njegova totalnog iznosa (rezultata) LV prosuditi kakva je situacija u prostoru V.

Zato se i može postaviti ova

4.3.1. Definicija. *Defekt (razlučivanja) linearnog operatora L jest dimenzija njegova jezgra*; označuje se sa *def L*. Dakle,

$$\operatorname{def} L = \dim L^{-1}\{0\}.$$

Npr. ako trodimenzionalni prostor projiciramo na pravac, defekt je 2.

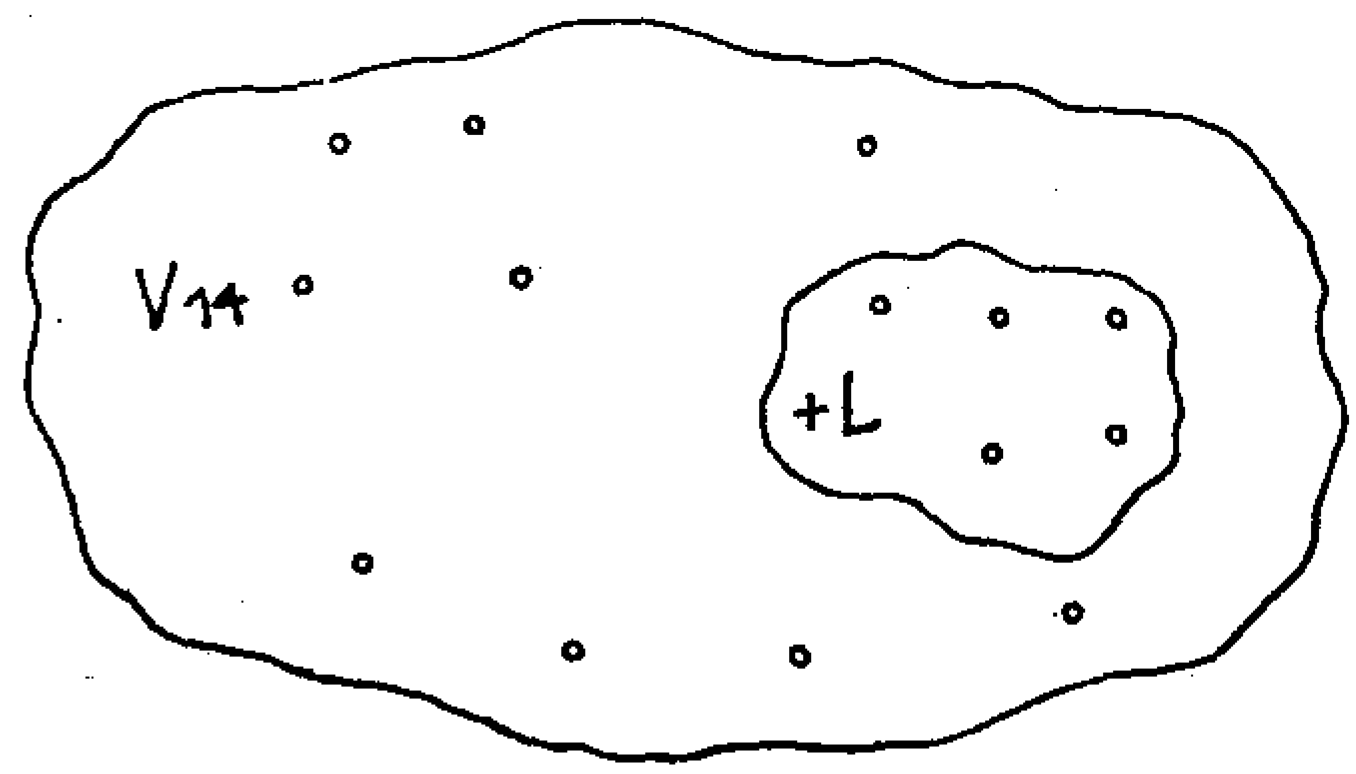
4.4. Rang (vjernosti) operatora L, po definiciji, jest dimenzija totalnog iznosa LV. Rang se označuje sa rL ili rang L. Dakle,

$$\operatorname{rang} L = \dim LV.$$

⟶ **4.5. Osnovni teorem o dimenzijama u vezi s linearnim operatorima.**[1] ***Za svaki linearni operator*** $L: V \to V$ ***vrijedi***

$$\dim V = \operatorname{rang} L + \operatorname{def} L;$$

ili određenije: za svaku bazu e prostora V ***sa svojstvom da je skup*** $e_0 = e \cap L^{-1}\{0\}$ ***baza u jezgri*** $L^{-1}\{0\}$, ***njegov komplement*** $e' = e \setminus e^0$ ***preveden je operatorom*** L ***u bazu*** Le ***prostora*** LV. ***Shematski:***



Sl. 26. 4.5.

Shema vektorskog prostora V_{14} (14 dimenzija) i učinka nekog linearizma L koji je poništio pet nezavisnih vektora i njihovu čitavu zajednicu V_5 slistio u + (shematska oznaka za nulu). Onih preostalih devet članova x predstavljaju shematski devet nezavisnih smjerova za razne položaje $L^{-1}\{0\} + x$, iz kojih se izgrađuju razredi kongruentni sa $L^{-1}\{0\}$. Tih devet razreda služi kao baza za izgradnju novog prostora, u kojem čitavo $L^{-1}\{0\}$ igra ulogu nule (isp. pogl. 27, § 15.8. kao i pojam kvocijentne grupe, pogl. 17, § 11.5). Eto, to je jedan od fundamentalnih uvida što ih daje teorija grupa u teoriji linearnih operatora.

D o k a z. Neka je $n = \dim V$; neka je $e = (e_1, e_2, \ldots, e_n)$ bilo koja baza u prostoru V koja obuhvata neku bazu e^0 jezgra $L^{-1}\{0\}$. Tada se prema osnovnom teoremu o podbazama (13, § 4.7) na taj način baza e cijepa na dva dijela: na skup e^0 prvih i skup e' drugih njenih elemenata, tj. e^0 je skup svih članova baze e koje operator V prevodi u O;

$$e' = e \setminus e^0.$$

No, e^0 je upravo presjek baze e i jezgra; prema osnovnom teoremu o istobrojnosti baza (pogl. 13, § 4.5.1) znači to da je dimenzija jezgra = kard. broj od e^0, tj. $\operatorname{def} L = ke^0$. Dokažimo sada da proizvod Le' čini bazu u LV.

Najprije, prema relaciji (1) svako Lv se može prikazati linearno pomoću $Le_1, \ldots, Le_n$, tj. pomoću Le', jer je $Le^0 = \{0\}$.

Dakle, na bar jedan način Lv se prikazuje linearno-homogeno pomoću članova iz e'; no to nije moguće postići na više načina, jer bi inače skup Le' bio zavisan, tj. postojao bi homogen linearni 0-spoj

(3) $$\sum_x k_x Lx = 0 \quad \text{sa} \quad x \in e'.$$

[1] Čitava stvar o maksimalnom broju linearno nezavisnih rješenja raznih homogenih jednadžbi neposrepno izlazi iz ovog osnovnog teorema. Dokaz teorema je tipičan s obzirom na prikazivanje prostora V kao direktne sume od dva potprostora.

Iz (3) izlazi:

$$L \sum_x k_x x = 0, \quad (x \in e'),$$

tj. vektor $v' = \sum k_x x$, $(x \in e')$, bio bi u jezgru operatora L No, pretpostavili smo da je podskup e^0 baza u jezgru, pa bi zato vektor v' imao svoj jednoznačan prikaz u e^0; drugim riječima, vektor v' imao bi svoj zapis i u e^0 i u e', što je moguće jedino ako je v' nula-vektor. Time je dokazano da je Le' baza u LV.

4.6. Teorem o određenosti linearnog operatora. ***Linearni operator koji djeluje u linearnom prostoru jednoznačno je određen vrijednostima što ih uzima na nekoj bazi prostora. Drugim riječima, ako je e baza prostora V_n, pa ako za linearno preslikavanje L znamo u što ono prevodi vektore x baze e, tj. ako je poznato pridruživanje $x \to Lx\,(x \in e)$, znamo time u što L prevodi svaki vektor v iz V_n. Specijalno, ako su $e_1, e_2, \ldots, e_n$ linearno nezavisni vektori u V_n, pa im pridružimo određene vektore $e'_{n'}$:***

$$e_{n'} \to e'_{n'} \in V_n,$$

određeno je time jedno jedino linearno preslikavanje prostora V_n u sama sebe (odnosno na sama sebe ako su vektori $e'_{n'}$ linearno nezavisni).

5. MATRICA KAO LINEARNO PRESLIKAVANJE

5.1. Pogledajmo kakvu matricu, npr.

$$a = \begin{bmatrix} 3 & 2 & -3 \\ 4 & 1 & 2 \end{bmatrix}. \tag{1}$$

Za svaki tročlani stupac x određen je time produkt ax kao dvočlani stupac. Tima ta matrica a vrši preslikavanje prostora $R_{3,1}$ (svih 3-članih stupaca kojima su članovi iz tijela R realnih brojeva) u prostor $R_{2.1}$ dvočlanih stupaca.

Posebno, stupci matrice a su ono u što prelaze jedinični stupci

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \text{ tj. stupci jedinične matrice } 1_{(3)} \tag{2}$$

Smještavanjem članova (2) u one članove u $R_{2,1}$ koji su stupci u a određeno je smještavanje

$$x \to ax \quad \text{svakog} \quad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \in R_{3\,1}. \tag{3}$$

Naime, smještavanje (3) je jedno linearno preslikavanje od $R_{3,1}$ prema $R_{2,1}$, što zbog

$$x = x_1 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

daje

$$ax = x_1 . a_{\cdot 1} + x_2 \cdot a_{\cdot 2} + x_3 \cdot a_{\cdot 3}.$$

Očigledno je zaključak isti ako znakovima 3 i 2 damo značenje kakvih god prirodnih brojeva.

5.2. Obrnuto, ako je L određeno linearno preslikavanje od $R_{3,1}$ prema $R_{2,1}$, tada se posebno zna slika $L\begin{bmatrix}1\\0\\0\end{bmatrix}$ od $\begin{bmatrix}1\\0\\0\end{bmatrix}$, te slika $L\begin{bmatrix}0\\1\\0\end{bmatrix}$ i slika $L\begin{bmatrix}0\\0\\1\end{bmatrix}$; time je određena i matrica $L_{(1)} = \left[L\begin{bmatrix}1\\0\\0\end{bmatrix}, L\begin{bmatrix}0\\1\\0\end{bmatrix}, L\begin{bmatrix}0\\0\\1\end{bmatrix}\right]$, koja ima isti učinak kao L i prebacuje jedinične stupce u isti položaj u koji ih prebacuje L; a time za svaki član $x \in R_{31}$ vrijedi $L_{(1)}x = Lx$, tj. kao operatori $L_{(1)}$ i L jesu funkcionalno jednaki. Na taj način vidimo da svakom linearnom operatoru L od prostora $R_{3,1}$ prema prostoru $R_{2,1}$, odgovara posve određena matrica $L_{(1)} \in R_{2,3}$ s istim učinkom:

(4) $$Lx = L_{(1)} \cdot x \quad \text{za svako} \quad x \in R_{3,1}$$

Z (uočiti jednakost (4); prema današnjem shvatanju, između L i x ne stoji ništa, no može se umjesto x pisati (x); na desnoj strani između $L_{(1)}$, x stoji znak $\cdot$ *za matrično množenje*).

5.3. Međutim, svaki vektorski prostor $V_3 = V_3(R)$ dimenzije 3, odnosno V_2 dimenzije 2, u kojima se množi članovima iz tijela R, izomorfan je s prostorom $R_{3,1}$ stupaca, odnosno s R_{21}. Pri tom je izomorfija potpuno određena izborom koordinatne osnove $e_1, e_2, e_3 \in V_3$ i pridruživanjem

$$e_1 \to \begin{bmatrix}1\\0\\0\end{bmatrix}, \quad e_2 \to \begin{bmatrix}0\\1\\0\end{bmatrix}, \quad e_3 \to \begin{bmatrix}0\\0\\1\end{bmatrix}.$$

Slično za $V_2 \to R_{2,1}$.

5.4. Neka npr. $V_3(R)$ znači skup svih funkcija oblika

$$b_1 \cos x + b_2 \sin x + b_3 \cdot 5, \quad \text{gdje je} \quad b_{3'} \in R.$$

Neka je isto tako $V_2(R)$ skup svih

$$c_1 + c_2 i \quad \text{sa} \quad c_{2'} \in R; \; i^2 = -1.$$

Odaberimo kao koordinatnu bazu u V_3 elemente („vektore")

$$e_1 = \text{funkcija } \cos x$$

$$e_2 = \sin x$$

$$e_3 = 5.$$

Neka u V_2 bude $e_1' = 1$, $e_2' = i = (-1)^{1/2}$. Tada npr. članu (funkciji)

(4) $$2\cos x - 3\sin x + 3 \in V_3$$

odgovara tačka

$$x = \begin{bmatrix} 2 \\ -3 \\ 3 \end{bmatrix} \in R_{3,1};$$

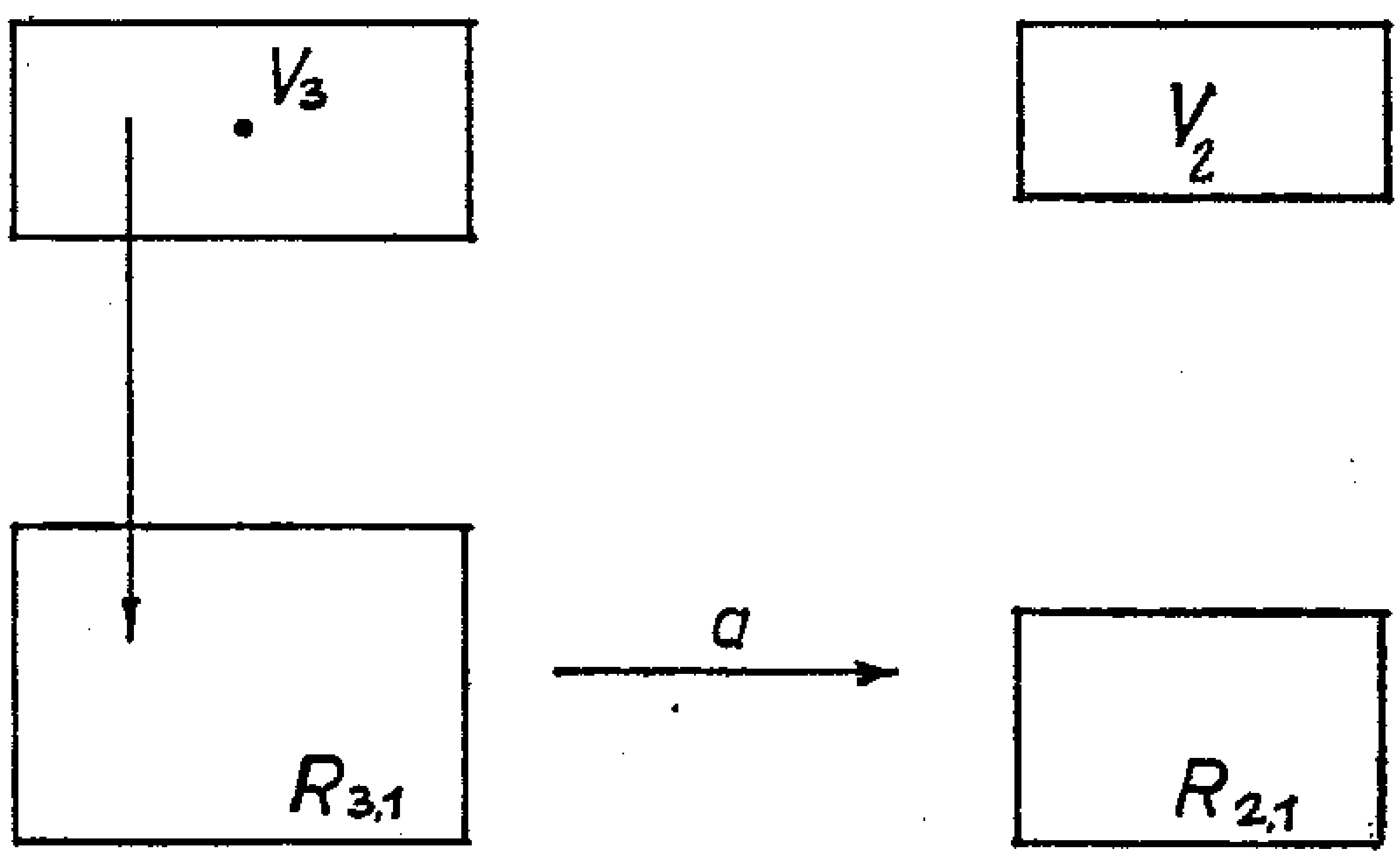
tu tačku matrica a kao operator gura (množenje sprijeda) u položaj

$$ax \in R_{2,1}, \text{ tj. u } \begin{bmatrix} 3 & 2 & -3 \\ 4 & 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ -3 \\ 3 \end{bmatrix} = \begin{bmatrix} -9 \\ 11 \end{bmatrix};$$

a izomorfijom između V_2 i $R_{2,1}$ smještava se

$$\begin{bmatrix} -9 \\ 12 \end{bmatrix} \text{ iz } R_{21} \text{ u } -9 + 11\,i.$$

I na taj način, idući poprijeko odmah od V_3 u V_2, dolazi element (funkcija) $2\cos x - 3\sin x + 3 \in V_3$ u položaj (element) $-9 + 11\,i$ prostora V_2 svih kompleksnih brojeva.



Sl. 26. 5.4.

Možemo reći da gornja matrica (1) predstavlja transformaciju svakog vektorskog prostora $V_3(R)$ snabdjevenog bazom $e_{3'}$ u svaki prostor $V_2(R)$ snabdjevenog bazom $e'_{2'}$ i pri čemu vektori e_1, e_2, e_3 baze polaznog prostora dolaze u vektore imena, zapisa,

$$3\,e'_1 + 4\,e'_2, \quad 2\,e'_1 + e'_2, \quad -3\,e'_1 + 2\,e'_2 \quad \text{u prostoru} \quad V_2(R).$$

5.5. Da smo u prostoru $V_3(R)$ za bazu uzeli elemente

$$e_1 = 5\cos x - 2\sin y + 4, \qquad e_2 = 2\cos x + 3\sin x - 1,$$

$$e_3 = \cos x - \sin x,$$

onda bi ista šifra, isto ime 2, —3, 3 iz starog sistema sada pokrivala drugo biće, naime element

$$b = 2(5\cos x - 2\sin y + 4) - 3(2\cos x + 3\sin x - 1) + 3(\cos x - \sin x)$$

zajednice V_3; a pod cifrom a za preslikavanje od V_3 ka V_2 sad bi *taj* element b (a ne onaj pod (4)) došao u položaj šifre —9, 11 u V_2, tj. u položaj $-9+11\,i$.

5.6. Vidimo ovo: svaka matrica $a \in R_{2,3}$ predstavlja potpuno određeno linearno preslikavanje $x \to a \cdot x$ od $R_{3,1}$ ka prostoru $R_{2,1}$; time se dobije ***svaki*** linearni operator L od prostora $R_{3,1}$ ka prostoru $R_{2,1}$ stupaca i vrijedi

$$1+1+1+2 \qquad Lx = L_{(1)} \cdot x \, (x \in R_{31}).$$

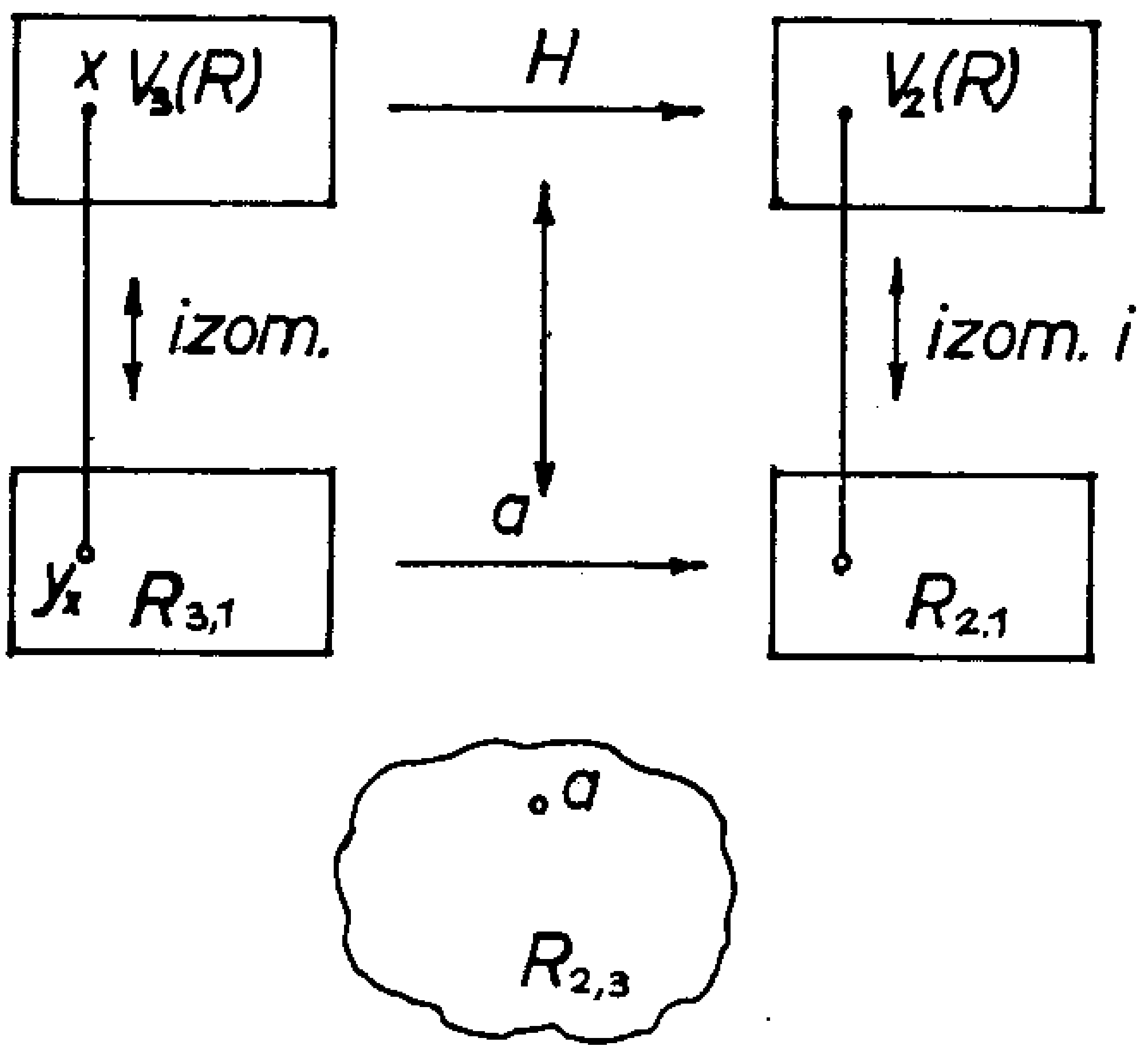
5.7. Nadalje, za svaki vektorski prostor $V_3(R)$ dimenzije 3 u kojem je odabrana baza

$$e = (e_1, e_2, e_3) \text{ i svaki vektorski prostor } V_2(R) \text{ s bazom } e' = (e'_1, e'_2)$$

svakoj matrici $a \in R_{23}$ odgovara *jedan jedini* linearizam $L: V_3 \to V_2$, kojem je a odraz; i obrnuto, svakom linearnom operatoru

$$H: V_3(R) \to V_2(R)$$

odgovara jedna jedina matrica $a \in R_{23}$, koja odražava vjerno (sl. 5.7) dolje ono što H radi gore: odgovarajuće izomorfne slike iz V_3 u $R_{3,1}$ prevodi u $R_{2,1}$ koje su upravo „ispod" rezultata u V_2 što ih u V_2 ubacuje H.



Sl. 26. 5.7.

5.8. Uočimo da je $R_{2,3}$ aditivna komutativna grupa (zbrajanje je matrično).

5.9. Uočimo da je $R_{2,3}(R)$ sa svoje strane vektorski prostor — prostor matricâ itd.

5.10. Isto zaključivanje vrijedi ako u gornjoj shemi shvatimo 2, 3, R kao varijable; 2 i 3 prolaze nezavisno skupom prirodnih brojeva, a R, umjesto da označuje tijelo realnih brojeva, može označivati bilo koje tijelo (brojevno ili nebrojevno).

Na osnovu svega toga jasan je iskaz naredne osnovne činjenice.

—→ **5.11. Osnovni teorem o matricama kao linearnim operatorima.**

***(i)* Neka je K kakvo algebarsko tijelo; neka za svaki uređeni par (n, s) rednih brojeva K_{ns} znači skup svih matrica s vrijednostima u K i s oblasti $n \times s$; radi se, dakle, o matricama formata, tipa $n \times s$. Tada je K_{ns} komutativna grupa u odnosu**

na zbrajanje matrica. Neka je LK_{ns} množina svih linearnih operatora $H: K_{n1} \to K_{s1}$; uvedemo li u LK_{ns} adiciju na način distributivan:

$$(H+H')\,x = Hx + H'\,x$$

za svako H, $H' \in LK_{ns}$ i svako $x \in K_{s1}$, dobije se komutativna grupa $(LK_{sn}, +)$; ta je grupa izomorfna s grupom matrica $(K_{ns}, +)$.

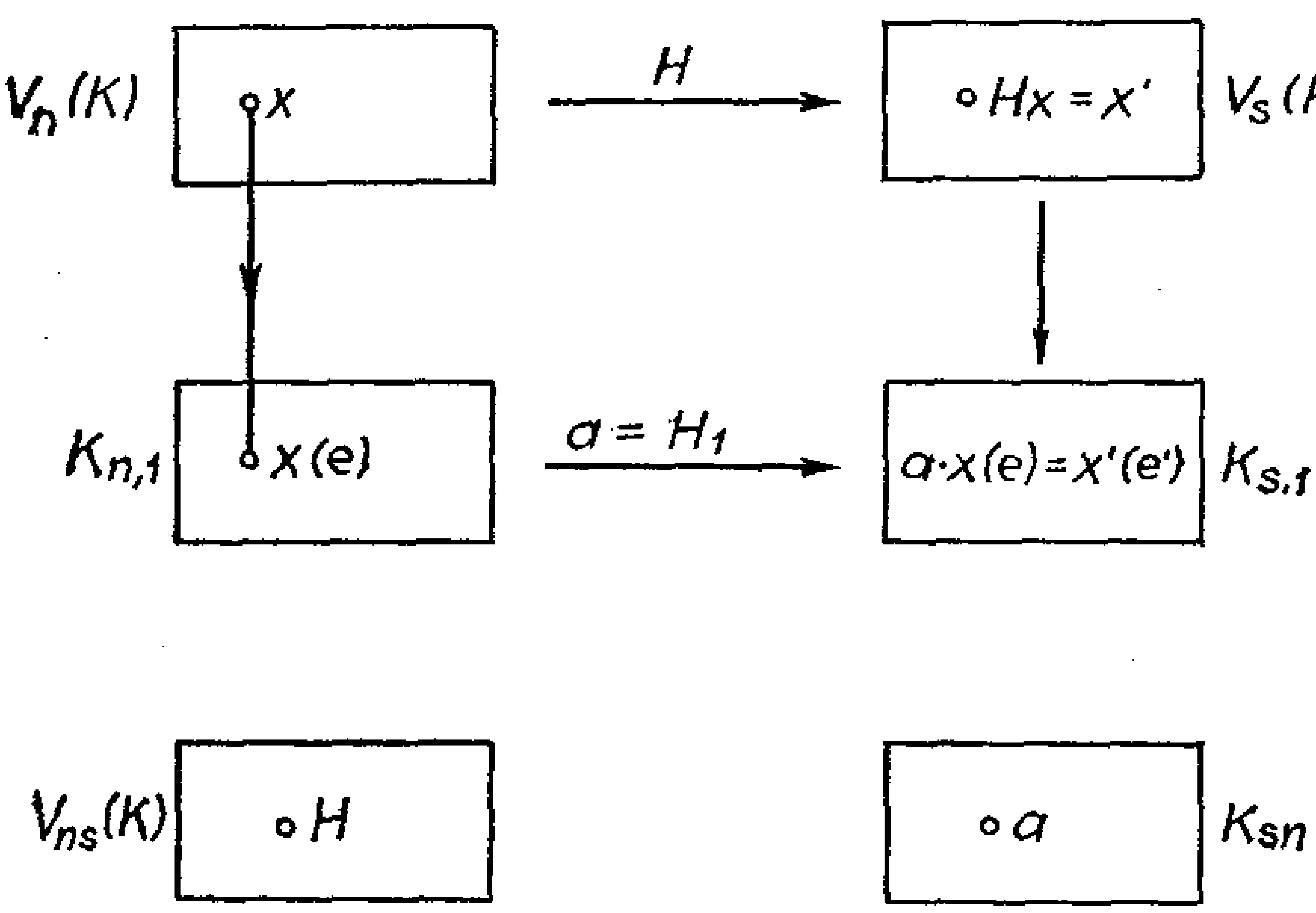
Specijalno, ako sa $H_{(1)}$ označimo matricu sastavljenu od vektorâ $H\mathbf{1}_{n'}$ koje operator H pridružuje vektorima jedinične matrice $\mathbf{1}_n$, tada je pridruživanje $H \to H_{(1)}$ jedna izomorfija između grupâ $(LK_{ns}, +)$, $(K_{sn}, +)$. Ujedno za svako $H \in LK_{ns}$ i pripadno $H_{(1)} = a \in K_{sn}$ vrijedi

$$Hx = H_{(1)} \cdot x, \quad (x \in K_{n1}),$$

pri čemu na desnoj strani stoji matrično množenje od a i x.

(ii) Ako je $V_n(K)$ proizvoljan vektorski prostor dimenzije n nad tijelom K, tada je prostor $V_n(K)$ izomorfan s prostorom K_{n1} svih matrica s oblasti $n \times 1$ i s vrijednostima iz K; ako je i $V_s(K)$ proizvoljan vektorski prostor nad K i dimenzije s, tada skup LV_{ns} svih linearnih preslikavanja od $V_n(K)$ prema $V_s(K)$ čini aditivnu grupu koja je izomorfna s matričnom grupom $(K_{sn}, +)$.

(iii) Izabere li se baza $e = e_1, \ldots, e_n$ u $V_n(K)$ i baza $e' = (e', \ldots, e'_s)$ u $V_s(K)$, tada je rečeni izomorfizam između grupa $(V_{n,s}\ +)$ linearnih operatora $H: V_n(K) \to \to V_s(K)$ i matrične grupe $(K_{sn}, +)$ jednoznačno određen: svakom linearnom operatoru $H: V_n(K) \to V_s(K)$ odgovara posve određena matrica $a(H) \in K_{sn}$, koja služi kao izomorfna reprezentacija operatora H i djeluje multiplikativno od K_{n1} ka K_{s1}. **Shematski:**



Sl. 26.5.11.

(IV) Ako je $e = (e_{n'})$ koordinatna baza u $V_n(K)$, a $e' = (e_{s'})$ koordinatna baza $V_s(K)$, pa ako za $x \in V_n(K)$ sa x_e ili $x\ (e)$ označimo stupac koordinatâ vektora x s obzirom na bazu e; slično za bazu e' u $V_n(K)$ i stupac $x'_{s'} = x'(e')$ za svako $x' \in V_s(K)$, tada linearnom operiranju »gore«

$$x' = Hx \ (x \in (V_n(K))$$

odgovara množenje pripadnom matricom $a = H_{(1)}$ dolje:

$$x'_{e'} = a \cdot x_e \quad (x_e \in K_{n,1}).$$

D o k a z. Izomorfizam prostorâ $V_n(K)$ i K_{n1} dokazan je u pogl. 13, § 4.6; uostalom, sad ćemo ga i usput dobiti. Naime, uz oznaku u teoremu preslikavanje $x \to x(e)$ je izomorfizam između prostora V_n i $V_n(e)(: = K_{n1})$; isto vrijedi za $x' \to x'(e')$.

Pa neka je $H: V_n \to V_s$ određen linearni operator. Time specijalno znamo položaje $He_{n'}$, u koje H prevodi vektore $e_{n'}$ baze e; u fiksiranoj bazi e' imamo jednoznačan rastav

(1) $$He_{n'} = \sum_{s'} a_{sn} e'_{e'} = a_{1n'} e'_1 + a_{2n'} e'_2 + \cdots + a_{sn'} e'_s;$$

(pazi na indeks n' lijevo i desno!) Tu se, eto, pojavljuje određena matrica

(2) $$a = [a_{s'n'}] \text{ poretka } (s, n).$$

S druge strane, za proizvoljan vektor $x \in V_n$ imamo, za fiksiranu bazu $e = (e_{n'})$, jednoznačan rastav $x = \sum x_{n'} e_{n'}$. Operator H šalje x u

$$Hx = H \sum x_{n'} e_{n'} = (\text{distributivnost}) = \sum H(x_{n'} e_{n'}) = (\text{homotetičnost}) =$$
$$= \sum x_{n'} He_{n'}.$$

Dakle,

(3) $$x' = Hx = \sum_{n'} x_{n'} He_{n'}.$$

Zbog (1):

(4) $$x' = Hx = \sum_{n'} x_{n'} \sum_{s'} a_{s'n'} e'_{s'} = \sum_{s'} (\sum_{n'} a_{s'n'} x_{n'}) e'_{s'}, \qquad \text{tj.}$$

(5) $$x' = \sum_{s'} (a_{s'.} \circ x(e)) e'_{s'},$$

jer zagrada u (4) naznačuje skalarni produkt retka $a_{s'.}$ i stupca $x(e)$ što kao značka pripada vektoru x prema bazi e.

Prelazeći sada na pripadne stupce i u V_s i znajući da su $e'_{s'}(e')$ jedinični stupci, pokazuje (5) da je

$$x'(e') = a \cdot x(e).$$

A za tim smo i išli.

Još samo da vidimo u kakvoj su vezi osnovni vektori $e_{n'}$ i stupci matrice a. To se vidi iz (1); znajući naime, da su $e'_{s'}$ vektori baze e', znači to da je $e'_{s'm} = \delta_{s'm}$ za svako $m \leq s$. Zato, prelazeći u (1) na komponente, izlazi

$$(He_{n'})_m = \sum_{s'} e_{s'n'} \delta_{s'm} = a_{mn'},$$

jer su svi drugi produkti pod $\sum$ jednaki 0. Dakle je

$$(He_{n'})_{s'} = a_{s'n'}, \quad \text{tj.} \quad (He_{n'})(e') = a_{.n'}.$$

Dakle uistinu, linearizam H šalje bazu e tako u V_s da pripadne komponente čine odgovarujeće stupce matrice a.

Obrnuto, znajući matricu a, koja djeluje kao multiplikativni operator iz $V_n(e)=K_{n1}$ u $V_s(e')=K_{s1}$, određeni su time u V_s s obzirom na bazu e' vektori $v_1, \ldots, v_n$, kojima koordinate čine stupce u matrici a. S druge strane, tih n vektora $v_{n'}$ treba da bude baš ono u što traženi linearni operator H treba da prevede osnovne vektore $e_{n'}$ iz V_n. A takav linearni operator jednoznačno je određen (isp. § 5.2).

Time je teorem potpuno dokazan.

5.12. Primjedba. Imajmo na umu da zadan linearni operator

$$H: V_n \to V_s \quad \text{prevodi} \quad V_n \text{ u } V_s$$

bez obzira na to da li uopće s kakvim koordinatnim bazama u tim prostorima radimo; jedno je sigurno: za svako $\dot{V}_n$ zna se tačno za $H\dot{V}_n \in V_s$; u tome se i sastoji upravo definicija od H kao jednoznačnog preslikavanja.

No, treba naročito naglasiti ovo: *izbor baze e u V_n i izbor baze e' u V_s ima za posljedicu da se operator H može prikazati i određenom matricom a*; naravno, $a=a(H, e, e')$. tj. *a zavisi i od H i od e i e'.*

Na taj način imamo osnovnu vezu

$$a=a(H, e, e'). \tag{5}$$

U toj vezi za isti određeni par (V_n, V_s) vektorskih prostora[1] dolaze četiri stvari:

1. Potpuno određena baza e u V_n, tj. potpuno određen niz (a ne samo skup)

$$e_1, \ldots, e_{n-1}, e_n$$

od n linearno nezavisnih vektora, koji razapinju prostor V_n, odnosno na koji je prostor V_n nataknut.

2. Potpuno određena baza e' u linearnom prostoru V_s, tj. potpuno određen niz $e'_{s'}$ od s linearno nezavisnih vektora koji razapinju V_s.

3. Određen linearni operator H od V_n ka V_s.

4. Određena matrica a s oblasti $s \times n$.

5.13. Od posebnog je interesa gledati kako izgledaju *sve* matrice koje vezom (5) odgovaraju jednom jedinom operatoru H, ali mijenjajući specijalno bazu e; naime, ako samo mijenjamo e u (5), dok H i e' ostavimo na miru, tada se a nužno mijenja.

To će nas posebno zanimati u slučaju kad H prevodi prostor u sama sebe (autolinearizam).

[1] Prostor V_n može, ali ne mora biti koordinatni prostor, tj. snabdjeven osnovom vektora; ako je snabdjeven bazom, može ona biti različita od baze e.

6. LINEARNI OPERATORI UNUTAR ZADANOG VEKTORSKOG PROSTORA I MATRICE

6.1. Neka je K jedno algebarsko tijelo (npr. tijelo realnih ili kompleksnih brojeva); neka je K_{n1}, odnosno K_{nn} skup svih matrica, formata $n \times 1$, odnosno formata $n \times n$ s vrijednostima u K. Tada svako $a \in K_{nn}$, tj. svaka kvadratna matrica a reda n djeluje u prostoru K_{n1} kao linearni operator u obliku *množitelja* na stupce (vektore) iz K_{n1}:

$$\text{iz } x \in K_{n1} \quad \text{i} \quad a \in K_{nn} \quad \text{izlazi} \quad ax \in K_{n1}.$$

Osim toga, skup K_{nn} zatvoren je i s obzirom na *zbrajanje* i s obzirom na *množenje*; s obzirom na zbrajanje K_{nn} je komutativna grupa; s obzirom na množenje K_{nn} je asocijativan grupoid s obostrano neutralnim elementom: jediničnom matricom 1_n. Skup svih regularnih elemenata iz K_{nn} (tj. onih elemenata $a \in K_{nn}$ za koje iz $\{x, y\}_{\neq} \subset K_{nn}$ proizlazi $ax \neq ay$) čini množidbenu grupu koja se zove *puna linearna grupa* K_n.[1]

6.2. Specijalno, K_{n1} je skup svih n-članih ili n-djelnih vektora koje pišemo u obliku stupaca. K_{n1} je vektorski prostor od n dimenzija u odnosu na tijelo K.

6.3. *Skup* LK_{n1}. Neka je LK_{n1} skup svih linearnih operatora iz K_{n1} u K_{n1}.

6.4. Tada se radi o tome da se usporede: skup K_{nn} kvadratnih matrica i skup LK_{n1} linearnih operatora. I te matrice i ti operatori djeluju na isti skup — na vektorski prostor K_{n1}[2].

6.5. Svaka matrica a daje neposredan uvid u to što ona radi s osnovnim jediničnim vektorima $(1_n)_{n'}$: a ih prevodi u svoje stupce, tj.

$$a \cdot (1_n)_{n'} = a_{\cdot n'}. \tag{1}$$

Matrica a je linearni operator u prostoru K_{n1}; naime, za vektore x, y iz K_{n1} imamo očigledno

$$a \cdot (x+y) = a \cdot x + a \cdot y.$$

Isto tako

$$a \cdot \dot{K} \dot{K}_{n1} = \dot{K}(a \dot{K}_{n1})$$

(homotetija! skalar $\dot{K}$ može se izlučiti i staviti ispred a).

---

[1] Podsjetimo se da *tijelo K nema nula-djelitelja*, tj. produkt dvaju članova iz K daje 0 jedino u slučaju ako je bar jedan od njih $=0$. U K_{nn} može produkt dvaju članova biti 0, mada nijedan faktor nije $=0$. Npr. slučaj $n=3$:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0 \\ 3 & 4 & 5 \\ 6 & 7 & 7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Uslov da K nema nula-djelitelja služi za inverziju matrice; naime, za svako $a \in K_{nn}$ imamo det $a \in K$.

[2] Imaj na umu slučaj $n=2$ i $K=$tijelo racionalnih brojeva ili cifarsko tijelo $I2$.

→ 6.6. **Osnovni teorem.** *Svaka kvadratna matrica a reda n predstavlja onaj linearni operator H koji jedinične vektore* $(\mathbf{1}_n)_{\cdot n'}$ *prevodi u stupce matrica; i obrnuto: znajući za linearni operator H rezultate* $H(\mathbf{1}_n)_{\cdot n'}$, *tada matrica* $[H(\mathbf{1}_n)_{\cdot 1}, H(\mathbf{1}_n)_{\cdot 2}, \ldots]$, *kojoj su ti rezultati stupci, reprezentira H; imamo pridruživanje*

$$(2) \qquad H \longleftrightarrow [H(\mathbf{1}_n)_{\cdot 1}, H(\mathbf{1}_n)_{\cdot 2}, \ldots, H(\mathbf{1}_n)_{\cdot n}]$$

i funkcionalnu jednakost

$$(3) \qquad Hx = [\cdots H(\mathbf{1}_n)_{\cdot n'} \cdots] \cdot x$$

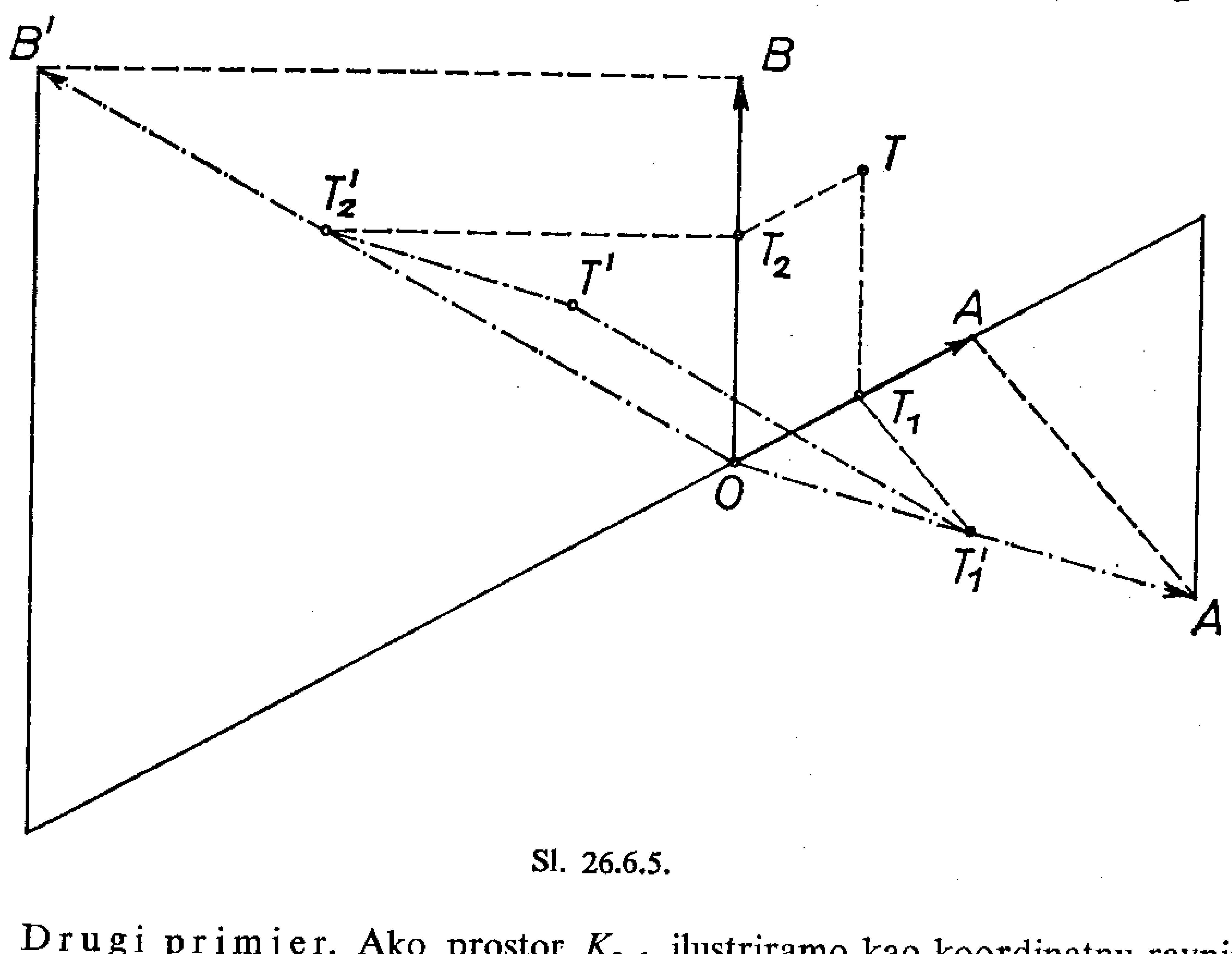
za svaki vektor $x \in K_{n1}$.

To je osnovna veza. Naglašavamo da u (3) *nadesno stoji matrično množenje*; na taj se način H — proizvod Hx od x prikazuje kao *matrični umnožak* pripadne matrice (1) i vektora x.

Primjer. Promatrajmo matricu

$$a = \begin{bmatrix} 3 & 5 \\ 7 & 4 \end{bmatrix}.$$

Kako glasi pripadni linearni operator H? U što H prevodi npr. $\begin{bmatrix} 2 \\ -6 \end{bmatrix}$? Prema (3) imamo $H\begin{bmatrix} 2 \\ -6 \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 7 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ -6 \end{bmatrix} = \begin{bmatrix} -24 \\ -10 \end{bmatrix}$.



Sl. 26.6.5.

Drugi primjer. Ako prostor $K_{2,1}$ ilustriramo kao koordinatnu ravninu s dva nezavisna radijus-vektora (*općenito nejednake dužine*), onda će npr. matrica $\begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$ predstavljati ono linearno preslikavanje H ravnine pri kojem će kraj A vektora 1_1 prijeći u tačku $A'=(2, -1)$, a tačka $(0, 1)=B$ u tačku $(-3, 2)=B'$.

Za svaku dalju tačku T ravnine slika $T'=HT$ dobije se geometrijski tako da se zna da T' u koordinatnoj bazi $e'=1'_1, 1'_2$ ima iste šifre (koordinate) koje ima T u polaznoj bazi e. Dakle: odrediti $T_1=OA\cap$ paralela sa OB kroz T; zatim odrediti T_1' kao sjecište od OA' s paralelom kroz T_1' sa AA'; tako se dobije T_1' — projekcija tražene tačke T na os OA', i to projekcija u smjeru druge osi OB'.

Slično se određuje projekcija T_2' na OB'; a time se odredi i T'.

6.7. Znajmo da je konkretan linearni operator H potpuno određen svojim vladanjem na nekom skupu od n nezavisnih vektora $e_{n'}$; time je H određeno i za svaki vektor x (isp. teorem 4.6). Kako izgleda matrica a, koja vrši istu funkciju kao i H?

U prvom redu, mora dakle biti

$$a\cdot e_{n'}=He_{n'}. \tag{4}$$

No tih n jednadžbi znači isto što i matrična jedna jedina jednadžba

$$a\cdot[e_1, \ldots, e_n]=[He_1, \ldots, He_n]. \tag{5}$$

A odatle se a može naći množeći zdesna sa $[e_1, \ldots, e_n]^{-1}$; izlazi:

$$a=[He_1, \ldots, He_n]\cdot[e_1, \ldots, e_n]^{-1}; \tag{6}$$

označimo to sa H_e.

Naravno, matrica $[e_1\cdots e_n]$ je regularna, jer su vektori nezavisni; zato postoji $[e_1\cdots e_n]^{-1}$, pa račun teče dalje.

Na taj način vidimo da isti linearni operator H određuje matricu (6), koja je s njim funkcionalno jednaka:

$$H\longleftrightarrow[He_1, \ldots, He_n][e_1\cdots e_n]^{-1}\equiv H_e \tag{7}$$

$\longrightarrow$ **6.8. Teorem.** $\boldsymbol{H(x)=H_e\cdot x}$. *Istom linearnom operatoru $H: K_{n1}\to K_{n1}$ odgovaraju sve matrice H_e, i to jedna, upravo H_e, za svaku bazu $e=(e_{n'})_{n'}$ vektora. Već i permutacija vektora u nizu $e_{n'}$ općenito ima za posljedicu da se dobije drukčija matrica H_e. No, sve su te matrice, kao linearna preslikavanja, zapisi ili predodžbe jednog te istog operatora H.*

Fiksiranjem baze e (np. tako da se radi o stupcima $1_{n'}$) *imamo potpuno određeno tolikovanje*

$$H\longleftrightarrow H_e \tag{8}$$

između množine LK_{n1} svih linearnih operatora $K_{n1}\to K_{n1}$ i množine K_{nn} svih matrica reda n.

7. SKUP K_{nn} MATRICA KAO ALGEBRA. SKUP LK_{n1} LINEARNIH OPERATORA OD K_{n1} U SAMA SEBE KAO IZOMORFNA ALGEBRA

7.0. Pogledajmo izbliže skup K_{nn} svih matrica $n \times n$ i skup LK_{n1} svih linearnih operatora H u vektorskom prostoru K_{n1} u sama sebe. Maloprije smo promatrali preslikavanje $H \to H_e$; tu je e određena baza u prostoru K_{n1}; H je proizvoljan linearni operator od $K_{n1} \to K_{n,1}$; H_e je njegov zapis (matrica); specijalno, za jediničnu matricu $e = 1_n$, $H\,1_n$ je matrica stupaca $H((1_n)_{\cdot n'})$:

$$H\,1_n = [H(1_n)_{\cdot 1}, \ldots, H(1_n)_{\cdot n}]; \quad \text{naravno,} \quad 1_n = [(1_n)_{\cdot 1}, (1_n)_{\cdot 2}, \ldots, (1_n)_{\cdot n}].$$

No, skup K_{nn} matrica ima i *svoju internu* organizaciju; npr. one obrazuju grupu prema zbrajanju matrica; one dopuštaju množenje skalarima (tj. elementima iz tijela K); nadalje, što je vrlo zanimljivo: one čine grupoid s obzirom na vlastito, matrično, množenje: ako je a, $b \in K_{nn}$, tada je i $a \cdot b \in K_{nn}$; sve te operacije vrijede i u $LK_{n,1}$, kao što ćemo vidjeti.

7.1. Nekoliko slučajeva preslikavanja $H \longleftrightarrow H_{(1)}$, odnosno veze: operator $\longleftrightarrow$ matrica za bazu $\mathbf{1} = \begin{bmatrix} 1 & & 0 \\ & 1 & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$.

Radi se o predstavljanju operatora H matricom H_1.

7.1.1. Konstantna homomorfija 0 reprezentirana je nula-matricom; i obrnuto.

7.1.2. Identična homomorfija $x \to x$ prevodi specijalno svaki vektor $(1_n)_{\cdot n'}$ u sama sebe, tj. $H(1)_{\cdot n'} = (1)_{\cdot n'}$, pa zato pripadna matrica glasi $[(1_n)_{\cdot 1}, \ldots, (1_n)_{\cdot n}] =$ = jedinična matrica 1_n; i obratno.

7.1.3. Ako je $H(1_n)_{\cdot n'} = \text{skalar } \lambda_{n'} \cdot (1_n)_{\cdot n'}$, tada je matrična reprezentacija

$$= \begin{bmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \ddots \end{bmatrix} = \text{diag}\,[\lambda_1, \lambda_2, \ldots, \lambda_n]; \text{ i obratno.}$$

7.1.4. D e f i n i c i j a. Operator koji se može predstaviti *dijagonalnom* matricom u bar jednoj bazi zove se *dijagonalni operator.*

7.2. Suma dvaju linearizama. Produkt skalara i linearizma — 7.2.1. Ako su H, H' dva linearizma $K_{n1} \to K_{n1}$ (tj. iz K_{n1} u K_{n1}), tada se suma $H + H'$ tih linearizama *definira* na evidentan način:

(1) $$(H + H')\,x = Hx + H'x \quad \text{za svako} \quad x \in K_{n1}.$$

7.2.2. Definicija produkta skalara i linearizma: $\dot{K}H$ znači da je

$$(\dot{K}H)\,x = \dot{K}\,(Hx) \quad \textit{za svako } x \in K_{n1}; \text{ pri tom } \dot{K} \in K.$$

7.2.3. Rezultat je u oba slučaja opet linearizam iz K_{n1} u K_{n1}. Dokažimo to! Dokažimo najprije aditivnost sumiranja:

$$(H+H')(x+y)=(\text{po definiciji})=H(x+y)+H'(x+y)=(\text{jer su } H,\ H'$$
$$\text{homomorfije})=(Hx+Hy)+(H'x+H'y)=(\text{jer su tu članovi } \textit{komutativne}$$
$$\text{grupe } (K_{n1},+))=Hx+(Hy+H'x)+H'y=Hx+(H'x+Hy)+H'y=$$
$$=(Hx+H'x)+(Hy+H'y)=(H+H')x+(H+H')y.$$

Dakle je zaista $H+H'$ *aditivno* preslikavanje. Analogno se vidi da je $H+H'$ i homotetično:

$$(H+H')(\dot{K}x)=(\text{po definiciji})=H(\dot{K}x)+H'(\dot{K}x)=(\text{po homotetičnosti za}$$
$$H,\ H')=\dot{K}(Hx)+\dot{K}(H'x)=\dot{K}(Hx+H'x)=\dot{K}(H+H')x.$$

7.3. Teorem. *Množina LK_{n1} svih linearnih operatora unutar prostora K_{n1} je vektorski prostor nad tijelom K.*

7.4. Izomorfizam vektorskih prostora K_{nn} i LK_{n1}. Tako imamo vektorski prostor LK_{n1} linearnih operatora ili linearizama i vektorski prostor K_{nn} svih kvadratnih matrica reda n.

Između ta dva prostora udesili smo tolikovanje

$$H \longleftrightarrow [H(1_n)_{\cdot 1}, \ldots, H(1_n)_{\cdot n}]. \tag{2}$$

Dokažimo sada da je to tolikovanje linearizam između tih prostora, tj. da suma dvaju operatora odgovara sumi pripadnih matrica:

$$H+H' \Leftrightarrow [H(1_n)_{\cdot 1}\cdots H(1_n)_{\cdot n}]+[H'(1_n)_{\cdot 1}\cdots H'(1_n)_{\cdot n}] \tag{3}$$

i da je uslov proporcionalnosti ili homotetičnosti zadovoljen:

$$\dot{K}H \Leftrightarrow \dot{K}[H(1_n)_{\cdot 1}\cdots H(1_n)_{\cdot n}]. \tag{4}$$

Dokažimo (3). Po propisu (2) sumi $H+H'$ kao operatoru odgovara matrica

$$[(H+H')(1_n)_{\cdot 1}, \ldots, (H+H')(1_n)_{\cdot n}].$$

Ovo je dalje po definiciji (1) jednako

$$[H(1_n)_{\cdot 1}+H'(1_n)_{\cdot 1}, \ldots, H(1_n)_{\cdot n}+H'(1_n)_{\cdot n}]=$$

$=$(po definiciji sume matrica)$=$

$$=[H(1_n)_{\cdot 1}, \ldots, H'(1_n)_{\cdot n}]+[H'(1_n)_{\cdot 1}, \ldots, H'(1_n)_{\cdot n}].$$

A to je upravo tražena desna strana u (3). Analogno se dokazuje (4).

Dakle je zaista tolikovanje (2) jedna izomorfija. Time vidimo da prostor K_{nn} kvadratnih matrica *vjerno* predočuje sve linearne operatore u prostoru K_{n1}.

7.5. Komponiranje operatorâ. No, pojavljuje se još jedna osnovna operacija: *slaganje ili uzastopno izvođenje* dvaju linearnih operatora. Ako na rezultat Hx operatora H djeluje operator H', dolazi se do $H'(Hx)$ i kaže da je to rezultat $(H'H)x$ *složenog operatora* $H'H$ (pazi na redoslijed!).

Kako se to *slaganje* ili *komponiranje* preslikavanjâ odražava među pripadnim matricama? Gledajmo i razmišljajmo!

Složenom operatoru $H' H$ po propisu (2) odgovara matrica

(5) $[(H' H)(1_n)_{\cdot 1}, \ldots, (H' H)(1_n)_{\cdot n}] = [H' H(1_n)_{\cdot 1}, \ldots, H'(H(1_n)_{\cdot n})] = ?$

Neka je matrica a reprezentacija operatora H; tada je

$$H(1_n)_{\cdot k} = a_{\cdot k} = a_{1k}(1_n)_{\cdot 1} + a_{2k}(1_n)_{\cdot 2} + \cdots;$$

zato je

$$H'(H(1_n)_{\cdot k}) = H' a_{\cdot k} = a_{1k} H'(1_n)_{\cdot 1} + a_{2k} H'(1_n)_{\cdot 2} + \cdots$$

Uzimajući tu komponente po redu, vidi se da je to $= a' \cdot a_{\cdot k}$, gdje je a' matrica koja reprezentira operator H'.

Na taj način daje (5) kao rezultat

$$[\cdots a' \cdot a_{\cdot k} \cdots] = a'[a_{\cdot 1}, \ldots, a_{\cdot n}] = a' \cdot a.$$

Dakle,

⟶ **7.6. Teorem.** ***Slaganju $H'H$ linearnih operatora H, H' po redu kako su izvođeni odgovora množenje pripadnih matrica H_1, H_1', pri čemu je redoslijed faktora pri množenju matrica onakav kao kod pripadnih operacija.***

Specijalno, ako su linearni operatori H, H' regularni (u $\neq$ tačkama primaju $\neq$ vrijednosti), tada je i njihov slog $H' H$ regularan; nadalje je tada i H i H' automorfizam prostora K_{n1}, tj. uzima svaki element prostora.

Na taj način vidimo da, s formalnog stajališta »*osebujno*« pravilo o *množenju* matrica (isp. pogl. 10, § 1.5.4.4) odražava jednu od najopćenitijih matematičkih radnji: *slaganje* (komponiranje) stanovitih funkcija (ovdje: slaganje operatorâ).

7.7. Na taj način vidimo da *regularne* matrice iz K_{nn} predstavljaju *automorfizme* vektorskog prostora K_{n1}, tj. takve linearne operatore koji uzimaju svaku vrijednost u prostoru K_{n1}, i to samo jedanput.

Ukratko, vidimo da su kvadratne matrice vjerno i pogodno sredstvo za predstavljanje linearnih operatora unutar zadanog vektorskog prostora.

Uočimo jednu vrlo zanimljivu stvar u vezi sa strukturom LK_{n1} linearnih operatora i cjelinom K_{nn} kvadratnih matrica.

7.8. Algebra K_{nn} i algebra $LK_{n,1}$. Umjesto svega što smo maloprije govorili kaže se da je K_{nn} *jedna algebra*; LK_{n1} također. Pri tom vrijedi

7.9. Definicija linearne algebre. Zadan je vektorski ili linearni prostor $(V, \dot{+})$ nad tijelom K; ako taj vektorski prostor dopušta interno množenje $\cdot$ tako da pri tom vrijede pravila o distributivnosti prema zbrajanju vektora:

$$x(y \dot{+} z) = xy \dot{+} xz$$

$$(y \dot{+} z)x = yx \dot{+} zx$$

te pravilo o skalarno-vektorskoj komutativnosti:

$$\alpha x \cdot \beta y = (\alpha\beta)(x \cdot y),$$

tada se govori o *linearnoj algebri* $(V, \dot{+}, \cdot)$ *nad tijelom* K.

7.9.1. Komutativne algebre. Linearna algebra je *komutativna,* ako joj je množenje komutativno.

7.9.2. Asocijativne linearne algebre. Kaže se da je linearna algebra *asocijativna,* ako je množenje asocijativno.

7.9.3. Algebre s jedinicom. Kaže se da *algebra ima jedinicu* ako postoji element e u algebri sa svojstvom $ex=xe=x$ za svaki vektor x, tj. za svaki član iz algebre. Tada se govori također o jediničnoj algebri.

7.9.4. Algebre s dijeljenjem. To je svaka linearna algebra u kojoj i jednadžba $ax=b$ i jednadžba $ya=b$ ima rješenje; pri tom su a, b proizvoljni članovi algebre i $a\neq 0$.

Samo se po sebi razumije što bi značilo govoriti o nekoj algebri s *jednoznačnim* dijeljenjem.

7.9.5. Linearna algebra kao prsten. Ako je $(V, \dot{+}, \cdot)$ linearna asocijativna algebra nad kolom ili prstenom K, tada je $(V, +, \cdot)$ određeno kolo (isp. pogl. 6, § 5.2) kojemu su članovi iz K određeni lijevi, odnosno desni endomorfizmi: svako $\alpha\neq 0$ iz K određuje endomorfizam

$$V\cdot \to \alpha V\cdot$$

kao i endomorfizam

$$V\cdot \to V\cdot\alpha \quad \text{grupe} \quad (V, +)$$

(isp. pogl. 17, § 22.1).

7.9.6. Proširenje pojma prstena ili kola. U vezi sa § 7.9.5 često se govori o prstenu ili kolu kad god je riječ o uređenoj trojki $(A, +, \cdot)$ sa svojstvima da je $(A, +)$ komutativna grupa, $(A, \cdot)$ grupoid i da je operacija $\cdot$ distributivna prema operaciji $+$; u tome slučaju govori se o asocijativnom kolu i o neasocijativnom kolu, već prema tome da li je grupoid $(A, \cdot)$ asocijativan ili nije asocijativan.

7.9.7. Uz tako prošireni pojam prstena, sada vidimo da je gornja definicija 7.9 linearne algebre ekvivalentna s ovom izrekom:

Linearna algebra nad tijelom K je svaki prsten kojemu su članovi iz K određeni lijevi, odnosno desni endomorfizmi.

7.9.8. Homomorfizam, izomorfizam itd. algebara razumiju se sami po sebi: terminologija grupoidâ, grupâ, vektorskih prostorâ, itd. prenosi se bez daljeg na algebre.

7.9.9. Povrat na algebre K_{nn}, LK_{n1}. Na osnovu definicije u § 7.9. sada nam je jasno da imamo *dvije algebre*: *algebru* K_{nn} i algebru LK_{n1}; one su izomorfne; napose, preslikavanje (2) je jedan izomorfizam između njih. Na osnovu tog tolikovanja situacijama u algebri K_{nn}, kojoj su *elementi matrice*, odgovaraju odgovarajuće situacije u algebri LK_{n1}, kojoj su *elementi linearni operatori* ili *linearizmi* unutar prostora K_{n1}.

Ono što te strukture odlikuje prema dosadašnjim strukturama jest upravo *matrično množenje*, odnosno *slaganje operatorâ*, koje je *dvostruko linearno*: *ulijevo i udesno*, tj.

$$a(b+c)=ab+ac \quad \text{te} \quad (b+c)a=ba+ca.$$

7.10. Linearni operatori unutar bilo kojeg vektorskog prostora. Promatrajmo sada umjesto specijalnog vektorskog prostora K_{n1} bilo koji vektorski prostor $V = V_n(K)$ od n dimenzija; K je rezerva skalara s kojima prostor dopušta množenje. Prema osnovnom teoremu iz pogl. 13, § 4.6.1. prostori $V_n(K)$ i K_{n1} su izomorfni. Specijalno, ako je $e = (e_{n'})_{n'}$ bilo koja baza u V, tada za svaki vektor $v \in V$ imamo *jednoznačan* rastav na komponente:

$$v = \sum v_{n'} e_{n'};$$

time je određen stupac $v._{n'}$ iz K_{n1}; označimo ga sa $v(e)$. Pridruživanje

$$x \longrightarrow x(e)(x \in V)$$

je izomorfizam između $V_n(K)$ i K_{n1}.

Posebno, svakom linearnom operatoru H *unutar* $V_n(K)$ odgovara operator H_e unutar $V(e) = K_{n1}$:

$$y = Tx \quad \text{unutar} \quad V \Leftrightarrow y_e = H_e x_e \quad \text{unutar} \quad K_{n1}.$$

Za poznavanje *linearnih* zbivanja unutar vektorskog prostora $V_n(K)$ *dovoljno* je zato znati što se i kako se događa unutar prostora K_{n1}. No, linearni operatori u K_{n1} izvrsno su svladavani *matricama algebre* K_{nn}. Zato će ta algebra K_{nn} biti izomorfan odraz strukture tzv. linearne algebre što je čine svi linearni operatori unutar prostora $V_n(K)$.

8. PREDSTAVLJANJE ISTOG LINEARNOG OPERATORA KAO MATRIČNO MNOŽENJE U RAZNIM BAZAMA

8.0. Svaki linearni operator H određen je vrijednostima što ih prima u bilo kojoj bazi e (isp. § 4.1). Te se vrijednosti notiraju kao *matrični zapis operatora* — dobiva se matrica H_e. No, tih matrica ima beskonačno mnogo. Kakva je veza između *raznih* matričnih zapisa jednog te *istog* operatora?

Radimo s prostorom K_{n1} vektorâ koji su zapisani kao stupci (odatle dvostruki indeks n, 1 jer su elementi u K_{n1} matrice formata $n \times 1$). Neka je H proizvoljan linearni operator ili linearizam unutar K_{n1}.

8.1. No, za svaku bazu $e = (e_{n'})$ linearizam H je jednoznačno određen svojom potfunkcijom $H|e$, tj. H je određeno vrijednostima $H(e_{n'})$ što ih H pridjeljuje elementima baze. To smo i ranije istakli (§ 4.1); istaknimo to i ovdje, jer su ovdje stvari jednostavnije utoliko što i argument i vrijednost preslikavanja pripadaju jednostavnijoj vrsti vektora. Za svaki vektor $v \in K_{n1}$ imamo jednoznačan rastav

(1) $$v = \sum_i e_i v_i,$$

pri čemu su v_i skalari, tj. $v_i \in K$.

Označimo sa v_e stupac $v_1, \ldots, v_n$.

Iz (1) izlazi:

(2) $$Hv = H_e \cdot v_e, \quad \text{gdje smo stavili} \quad H_e = [H(e_1), \ldots, H(e_n)],$$

$$v_e = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}.$$

Na taj se način zadani linearizam H prikazuje kao potpuno određeno *matrično množenje*; matrica H_e je sastavljena od vektora He_i, u koje operator H preslikava vektore baze e.

To je osnovni korak. To vrijedi za *svaku bazu*.

8.2. Na taj način za svaku bazu e imamo preslikavanje

(3) $$x \longrightarrow x_e$$

(davanje novih oznaka vektorima na osnovu baze e), pa se linearni operator $x \to Hx$ prikazuje kao preslikavanje

(4) $$y_e = H_e \cdot x_e \quad (x \in K_{n1})$$

predočeno *matričnim množenjem* (tu i „iznos" (rezultat) $H_e \cdot x_e$ mjerimo istom mjerom, inače bi rezultat bio neispravan; zato u (4) pišemo y_e umjesto y, da se bolje markira da radimo baš u bazi e).

Obrazac (4) vrijedi za svaku bazu e.

8.3. Neka je e' neka druga baza. Tada je prema (4):

(4′) $$y_{e'} = H_{e'} \cdot x_{e'}.$$

No, za baze e, e' potpuno je određena matrica c za koju je

(5) $$e' = ec;$$

stupci u c su značke od $e'_{n'}$ u odnosu na bazu e. Prema osnovnom teoremu 3.3 iz pogl. 23 vrijedi istodobno

(6) $$cv_{e'} = v_e \quad \text{za svako} \quad v \in K_{n1}.$$

Specijalno, stavljajući u (6) za v slovo y i x pa unoseći pripadne vrijednosti u (4), dobivamo

$$cy_{e'} = H_e c x_{e'}.$$

Odatle, množeći sprijeda sa c^{-1}:

(7) $$y_{e'} = (c^{-1} H_e c)\, x_{e'}.$$

Usporedi li se (7) i (4), izlazi:

$$H_{e'} x_{e'} = (c^{-1} H_e c)\, x_{e'} \quad \text{za svako} \quad x_{e'} \in K_{n1}.$$

To znači da je

(8) $$H_{e'} = c^{-1} H_e c.$$

To je traženi rezultat.

—→ **8.4. Osnovni teorem o matričnim množidbenim prikazivanjima linearnog operatora.** 1 *Za svaku bazu* $e=(e_{n'})_{n'}$ *vektorskog prostora* K_{n1} *potpuno je određeno preslikavanje* $v \to v_e$ *prostora na sama sebe; pri tom je* v_e *zapis (tj. vektor koordinatâ) od* v *za bazu* e (isp. pogl. 23, § 3.3); *ako za linearni operator* $H: K_{n1} \to K_{n1}$ *označimo s* H_e *matricu zapisâ, prema bazi* e, *svih* n *vektora* $He_{n'}$, *tada je* $(Hv)_e = H_e \cdot v_e$ *za svaki vektor* v.

2. *Za dvije proizvoljne baze* e, e' *prostora* K_{n1} *veza između bazâ* e, e', *zapisâ* $v_e, v_{e'}$ *za svako* $v \in K$ *i tablicâ* $H_e, H_{e'}$ *očitava se iz*

$$e' = e \cdot c, \quad cx_{e'} = x_e, \quad H_{e'} = c^{-1} H_e c, \quad tj.$$

$$H_{e \cdot c} = c^{-1} \cdot H_e \cdot c.$$

3. *Ako je* a *jedan matrični zapis linearnog operatora*

$$H: K_{n1} \to K_{n1},$$

tada se skup svih matričnih zapisâ operatorâ H *sastoji upravo od matricâ* $c^{-1}ac$, *pri čemu* c *prolazi skupom svih regularnih matrica reda* n *i s vrijednostima u* K.

Prethodni teorem je vjerojatno najvažniji teorem o linearnim operatorima.

Dokaz prva dva dijela teorema sadržan je u prethodnim izlaganjima ovog paragrafa. Treći dio dokazat ćemo u narednom paragrafu o sličnim matricama (teorem 9.3), jer je funktor $c^{-1}ac$ dviju matrica tako karakterističan da ga treba obraditi zasebno.

8.5. Determinanta linearnog operatora. Oblik

$$H_{ec} = c^{-1} H_e c, \tag{9}$$

do koga smo došli za matricu zapisâ operatora H vrlo je važan jer nam daje uvid u svojstva operatora H, koja bi na drugi način bila teže uočljiva. Specijalno ćemo zato moći prenijeti s matrica na operatore sva ona svojstva koja se ne mijenjaju pod utjecajem simultanog djelovanja s lijeve i desne strane suprotnih operatora. Takav je slučaj s »*determinantom*« operatora H, kao što ćemo odmah vidjeti.

Iz jednakosti (9) izlazi za pripadne determinante:

$$\det H(e') = \det c^{-1} \det H(e) \det c;$$

no $\det c^{-1} = (\det c)^{-1}$ (v. pogl. 12, § 5.2); na taj način gornja jednakost postaje

8.5.1. Teorem

$$\det H(e') = \det H(e).$$

Riječima: *sve matrice koje predstavljaju jedan te isti linearni operator imaju jednake determinante.*

8.5.2. Definicija determinante operatora. *Determinanta matrice* H_e *zove se determinanta linearna operatora* H *i može se označiti sa* $\det H$.

8.5.3. Sada također definiramo da je regularnost operatora H ekvivalentna s uslovom $\det H \neq 0$.

8.6. O punoj linearnoj grupi prostora $K_{n,1}$. Rasuđivanja o predstavljanju linearnih operatora prostora K_{n1} pokazuju kako u igru ulaze regularne matrice iz algebre K_{nn}; naime, one vrše vezu između bilo kojih dviju baza promatranog prostora. Sve te regularne matrice čine tzv. *punu* linearnu grupu za prostor K_{n1}. Pomoću njih se u linearnoj algebri K_{nn} svih matrica formata $n \times n$ svrstavaju matrice u razrede; *razred je sastavljen od svih matrica koje u svim mogućim koordinatnim bazama predstavljaju jedan te isti linearni operator.*

9. SLIČNOST MATRICA. DVIJE INTERPRETACIJE SLIČNOSTI

9.1. Definicija sličnih matrica. Kaže se da je matrica a *slična matrici* b ako postoji *regularna* matrica f, za koju je $f^{-1}af=b$; piše se $a \sim b$.

9.2. T e o r e m. *Sličnost među matricama jest određena relacija ravnopravnosti*: relacija $\sim$ je refleksivna, simetrična i prelazna.

Skup svih matrica koje su slične s matricom a podudara se sa skupom svih matrica koje su slične sa b, ako je $b \sim a$.

Refleksivnost se vidi iz jednakosti $a = 1_n^{-1}\, a\, 1_n$. Simetričnost se vidi iz činjenice da iz $b=f^{-1}af$ izlazi (kako?) $fbf^{-1}=a$, tj. $a=g^{-1}bg$, gdje je $g=f^{-1}$.

Svojstvo prelaznosti relacije sličnosti: ako je a slično b, b slično c, onda je a slično c. No, $a \sim b$ znači $a=f^{-1}bf$; isto tako $b \sim c$ znači da je $b=h^{-1}ch$; unesemo li ovo u prethodnu jednakost, izlazi:

$$a=f^{-1}(h^{-1}ch)f = (\text{zakon udruživanja!}) = (f^{-1}h^{-1})\,c\,(hf) = (\text{v. gl. teorem pogl. 12, § 5.3}) = (hf)^{-1}c\,(hf) = k^{-1}ck, \text{ gdje je } k=hf.$$

Dakle je $a=k^{-1}ck$, tj. a je slično sa c.

9.2.1. Razredi sličnih matrica. Na taj način *sve* kvadratne matrice određenog reda n možemo svrstati u razrede, pri čemu svaki *razred obuhvata sve međusobno slične matrice i ništa više.* Svaki razred R je invarijantan prema c — »*konjugaciji*« $x \to cxc^{-1}$, i to za svaku regularnu matricu c. To znači da je $c\dot{R}c^{-1} \in R$. To je jasno, jer je $\dot{R} \sim c\dot{R}c^{-1}$.

9.3. T e o r e m. *Slične matrice imaju isti rang i međusobno su ekvivalentne.*

To je neposredna posljedica teorema 8.8. o rangu produkta matrica i teorema 8.9. o ekvivalentnim matricama iz pogl. 15.

9.3.1. *Ekvivalentne matrice ne moraju biti slične.*

Možemo se pitati da li su ekvivalentne matrice nužno slične. Sjetimo se da je matrica a ekvivalentna s matricom b ako jednakost $b=xay$ ima rješenje u nesingularnim matricama x, y. Za sličnost matrica b i a traži se još da vrijedi *dodatni uslov* $xy=1$, što je veliko ograničavanje.

Uostalom, ekvivalentne matrice mogu biti i nekvadratne; naprotiv, *sličnost matrica definirana je samo za kvadratne matrice.* Zato npr. ekvivalentne nekvadratne matrice ne mogu biti slične. Takve su npr. matrice

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

No, odmah ćemo vidjeti da ekvivalentnost ne uključuje nužno sličnost ni za kvadratne matrice (v. konac § 9.4).

9.4. Prva interpretacija sličnosti matrica. Imajmo na umu ono što smo maloprije saznali u § 8.4. Slične matrice predstavljaju *jedno te isto* linearno preslikavanje vektorskog prostora, ali izraženo u *raznim koordinatnim bazama.* Isto tako, dvije matrice koje nisu slične međusobno predstavljaju dva različita linearna preslikavanja (bez obzira na izabrane koordinatne baze).

Tako su npr. preslikavanja

(1) $x \to x$ (identično preslikavanje) i

(2) $x \to 2x$ dva različita linearna preslikavanja;

pripadne matrice ne mogu biti slične. Recimo da radimo s prostorom V_2 od 2 dimenzije; tada su pripadne matrice gornjih dvaju preslikavanja (1), (2):

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1_2 \quad \text{te} \quad \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}.$$

Dokažimo i formalno da $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ ne može biti slično sa 1_2, tj. da ne postoji matrica c za koju bi bilo

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = c^{-1}\, 1_2\, c.$$

Stvarno ovaj produkt je dalje $= c^{-1} \cdot c$ (jer je $1_2 \cdot c = c$); dalje je ono $= 1_2$. No, naravno, nije

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 1_2. \quad \text{Dakle matrice} \quad \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

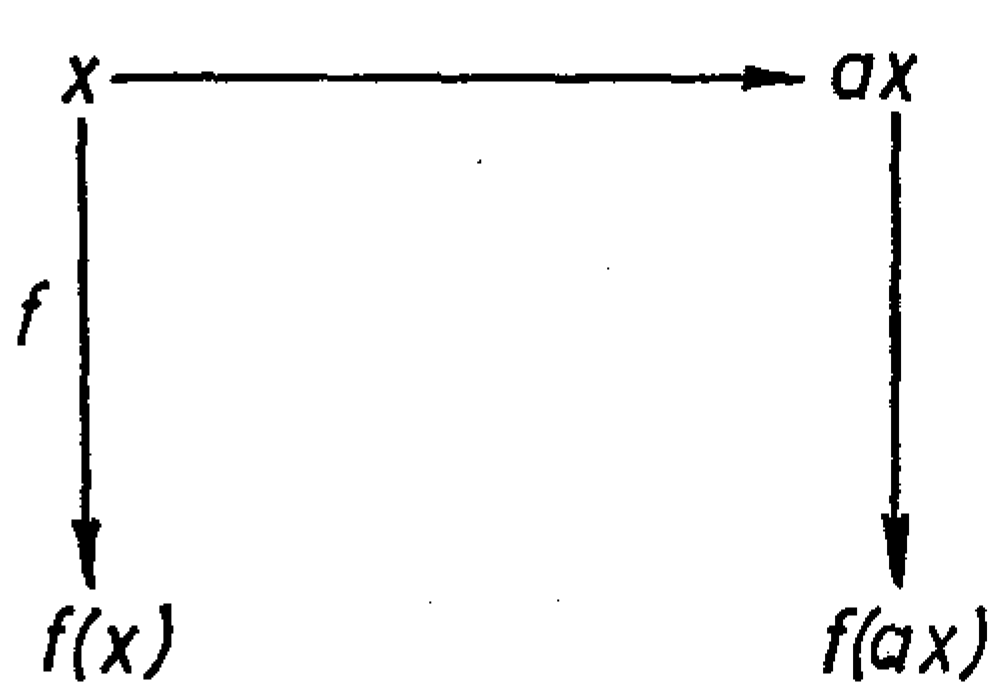
nisu slične u smislu gornje definicije, mada su ekvivalentne.

9.5. Druga interpretacija sličnosti matrica. — 8.5.1. Znajmo da svaka kvadratna matrica a preslikava koordinatni vektorski prostor $V(e)$ u sama sebe (e je stanovita baza prostora), i to po shemi:

$$x \to ax \quad \text{ili} \quad y = ax \, (x \in V(e)).$$

No, ako je f kakva kvadratna regularna matrica, tada i f preslikava prostor $V(e)$ u sama sebe (čak i *na* sama sebe); specijalno, x prelazi u fx, y prelazi u fy; shematski:

Nastaje *pitanje*: *kako se može od fx preći na fax*? Priložena shema prikazuje ovo: idući od fx natrag na x (operator f^{-1}), pa dalje na ax (operator a), pa dalje na fax (operator f), doći će se do traženog preslikavanja $fx \to fax$. Ono je dakle (prati prstom hod na slici), jednako uzastopnom izvođenju preslikavanja f^{-1}, a, f, tj. faf^{-1} **(argument se piše nadesno! Zato se funkcionalni operatori nižu zdesna nalijevo!)** Tako, dakle, operator faf^{-1}



Sl. 26.9.5.

naznačuje *transformirano* preslikavanje a, i to transformirano pomoću preslikavanja f. Uostalom preslikavanje $fx \to fax$ očigledno je isto što i preslikavanje

$$fx \to fa(f^{-1}f)\,x, \text{ tj. } fx \to faf^{-1}(fx), \text{ tj. } y \to faf^{-1}y$$

(nije važna *oznaka* argumenta, nego područje po kojem se on kreće!) No, ako je f regularno, tada je $fV = V$, tako da je preslikavanje $x \to (faf^{-1})\,x$ zbilja jedno preslikavanje čitavog prostora V *na* sama sebe. To znači da, u suštini, preslikavanja $x \to ax$ i $x \to (faf^{-1})\,x$ nisu bitno različita: jedno nastaje iz drugog na jednostavan način (isp. pogl. 17. o grupama, § 14).

9.6. Teorem. *Slične matrice imaju istu determinantu* (isp. pogl. 26, § 8.5). Naime, ako su a i b slične matrice, onda znači da postoji regularna matrica c sa svojstvom $b = c^{-1}ac$; odatle (pogl. 11, § 9)

$$\det b = \det c^{-1} \det a \det c = (\det c^{-1} \det c) \det a = \det (c^{-1}c) \det a = \det a.$$

9.7. Determinanta linearnog operatora ili linearizma H je (isp. pogl. 26. § 8.5) determinanta bilo koje matrice koja predstavlja H; označuje se sa $\det H$. Zato je skalar $\det H$ jednoznačno određen bez obzira na koordinatnu bazu prostora.

9.8. Opća napomena. Zasad to spominjemo ovdje da se priviknemo na prelaženje s matrica na operatore i obratno. Sada, kad je potpuno dokazan osnovni teorem iz prošlog paragrafa (vidi pogl. 26, § 8.4), vidimo da možemo uvijek govoriti bilo o matrici bilo o operatoru, jer jedno se svodi na drugo. Ovo neka bude opća napomena za orijentaciju.

9.9. Zadaci o sličnim matricama. 1. Dokaži da su matrice

$$\begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}, \begin{bmatrix} \cos\alpha + \sin\alpha & -\sin\alpha \\ 2\sin\alpha & -\sin\alpha + \cos\alpha \end{bmatrix} \quad \text{slične.}$$

2. 1) Da li su matrice $\begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ slične?

2) Isto za matrice: *a*) $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, *b*) $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix}$, $r > 0$.

3. Dokaži da su matrice

$$a = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad b = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \frac{1}{2} & 1 & 1 & 0 \\ \frac{1}{6} & \frac{1}{2} & 1 & 1 \end{bmatrix}$$

slične pa nađi matricu f tako da je $f^{-1}af = b$.

4. 1) Dokaži da su matrice $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ slične.

2) Isto za $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$.

5. U prostoru V polinoma stepena $\leq n-1$ neka a bude operator deriviranja $ap=p'$, $p\in V$. Nađi matricu toga operatora
   1) u bazi $1, x, \ldots, x^{n-1}$;
   2) u bazi $1, 1+x, x+x^2, x^2+x^3, \ldots, x^{n-2}+x^{n-1}$;
   3) u bazi $1, 1+x, 1+x+x^2, \ldots, 1+x\cdots x^{n-1}$.

10. KONGRUENTNE MATRICE

10.1. Definicija. Kaže se da je matrica *a kongruentna matrici b*, simbolički $a\equiv b$, ako postoji *regularna* matrica c, za koju je

$$c^T ac = b.$$

10.2. Specijalno, vidimo da matrice koje su kongruentne s jediničnom matricom imaju oblik $c^T c$, odnosno cc^T. (isp. pogl. 10, § 6.6. o Gaussovu produktu matrice).

10.3. Neposredno se dokazuje da je relacija kongruentnosti među matrisama jedna ekvivalentna relacija:

$$a\equiv a$$

$$a\equiv b \quad\Rightarrow\quad b\equiv a$$

$$a\equiv a', \quad a'\equiv a'' \quad\Rightarrow\quad a\equiv a''.$$

Dokažimo treću relaciju. No, $a\equiv a'$ znači da je $c^T ac=a'$ za bar jednu regularnu matricu c. Isto tako, $a'=a''$ znači da je $c'^T a' c'=a''$. Pišemo li tu gornji izraz za a', dobije se

$$a''=c'^T (c^T ac)\, c'=(cc')^T a\,(cc').$$

11. SLIKA O UČINKU LINEARNOG OPERATORA NA JEDINIČNOJ LOPTI

11.1. Neka je A linearni operator u prostoru V (zamišljaj slučaj da je V npr. ravnina R_2 ili prostor R_3). Da dobijemo bar približan uvid u djelovanje operatora A, možemo ga pratiti u njegovu poslu na kakvom užem, određenijem skupu. Već znamo jedan podatak u tom pogledu: *A ostavlja $\vec{O}$ na miru*: $A\vec{O}=\vec{O}$; nadalje, A dovodi u $\vec{O}$ čitav jedan prostor za sebe: jezgro $A^{-1}\{\vec{O}\}$ operatora A; to se jezgro kreće: od $\{\vec{O}\}$ za *regularne* operatore A, pa do čitava prostora za *posve singularan* nula-operator.

11.2. Jedan od jednostavnijih i analitički lako obradivih skupova jesu lopte; npr. za jediničnu loptu S je $Nx=1$ ili $x^\star x=1$ za svako $x\in S$ (za pripadnu jediničnu kuglu je $Nx\leq 1$; Nx znači normu od x).

Jedinična lopta S kao podatak ili unos u stroj ili operator A daje skup AS kao iznos ili proizvod; kako on izgleda?

Radimo matrično: neka je a matrica (odnosno matrični zapis od A): S kao unos je skup svih x za koje je

$$x^\star x = 1. \tag{1}$$

a S kao iznos je skup svih

$$y := ax, \qquad \text{za koje je} \qquad x \in S. \tag{2}$$

No, ako je a regularna matrica, tada iz (2) izlazi $a^{-1} y = x$, pa jednakost 1) postaje

$$(a^{-1} y)^\star (a^{-1} y) = 1$$

$$y^\star (a^{-1})^\star a^{-1} y = 1^{1)}. \tag{3}$$

11.3. Promatrajmo jednostavan slučaj da je a realno i simetrično: $a^T = a$. Tada je i a^{-1} simetrično, pa (3) postaje (ako je realno tada je $a^\star = a^T$):

$$y^T a^{-2} y = 1. \tag{4}$$

Eto, to je analitički zapis onog što operator a napravi od jedinične lopte (1)! U jednostavnom slučaju da A radi npr. $x \to 5x$ prešla bi jedinična lopta u loptu s $r = 5$. Matrično, proces $x \to 5x$ je zapisan (u koordinatnom prostoru R_3) dijagonalno $\begin{bmatrix} 5 & & \\ & 5 & \\ & & 5 \end{bmatrix}$, jer se sva tri jedinična vektora rastežu u tom omjeru.

11.4. Primjer. Ako je

$$a = \begin{bmatrix} 3 & & \\ & 5 & \\ & & 6 \end{bmatrix}, \tag{5}$$

znači to da se prvi jedinični vektor ispruža u 3-struk, drugi u 5-struk, a treći u 6-struk. Nađimo jednadžbu (4) za slučaj (5).

Tada je

$$a^{-1} = \begin{bmatrix} 3^{-1} & & \\ & 5^{-1} & \\ & & 6^{-1} \end{bmatrix}, \text{ tj. } a^{-2} = \begin{bmatrix} 3^{-2} & & \\ & 5^{-2} & \\ & & 6^{-2} \end{bmatrix},$$

pa (4) glasi

$$y^T \begin{bmatrix} 3^{-2} & & \\ & 5^{-2} & \\ & & 6^{-2} \end{bmatrix} y = 1,$$

odnosno, pišući

$$y^T = [y_1\, y_2\, y_3]$$

$$(3^{-1} y_1)^2 + (5^{-1} y_2)^2 + (6^{-1} y_3)^2 = 1. \tag{6}$$

---

[1] Vidimo kako se tu pojavljuje operator $(a^{-1})^\star$; zove se *kontragredijent* od a: važnost mu je vrlo velika.

Rezultat je troosni elipsoid; osi su mu: 3, 5 i 6, upravo članovi dijagonale iz zapisa (5).

11.5. Primjer. Ako je operator A predočiv zapisom

$$\begin{bmatrix} 2 & & \\ & 3/4 & \\ & & 0 \end{bmatrix}, \tag{7}$$

znači to da on u odgovarajućoj bazi e_1, e_2, e_3, prema kojoj je zapis učinjen, vrši ovakve promjene: e_1 izduži dvostruko, e_2 skrati u omjeru 3 : 4, a e_3 stegne na 0; time on čitavu pravulju Re_3 stegne na 0 i u tom smjeru vrši projiciranje. Svaka kružnica S_1 s jedinične lopte S_2, za koju je $S_1 \perp e_3$, biva projicirana u smjeru e_3, a onda deformirana u elipsu s osima 2 i 3/4. Time čitava lopta S prelazi u nutrašnjost i omeđenje elipse

$$(2^{-1} y_1)^2 + (0{,}75^{-1} y_2)^2 = 1.$$

Da je umjesto 2 u gornjem zapisu stajalo 0, značilo bi to da operator projicira i u smjeru vektora e_1, pa bi konačni rezultat od jedinične lopte bio zatvoreni segment od $-0{,}75$ do $0{,}75$ na pravulju Re_2 što ga određuje vektor e_2.

11.6. Problem dijagonalizacije operatora. Gornja dva primjera bilo je lako obraditi jer smo operator bili zadali u dijagonalnom zapisu (5), odnosno (7). Stvar se obrađuje slično svaki put kad nam je pri ruci *dijagonalni zapis*. Zato se postavlja *osnovni problem*: *ako je operator A zadan, treba pronaći kakav njegov dijagonalni zapis, tj. odrediti jednu bazu $e = (e_{n'})$ u kojoj će operator biti zapisan i ostvaren kao dijagonalna matrica.*

Ukoliko, naravno, takav zapis postoji! Ali kako odrediti da li postoji dijagonalni zapis i kako ga pronaći? (Isp. pogl. 16, § 2 i čitavo naredno pogl. 27).

12. SKALARNI PRODUKT $Ax \circ x$ KAO SLIKA O LINEARNOM OPERATORU A

12.1. Linearni operator A pridjeljuje svakom vektoru x određen vektor Ax; da se može dobiti što slikovitija predodžba o operatoru A, možemo pogledati što on radi s određenim skupom S u prostoru. U prostorima s metrikom možemo gledati kuglu s polumjerom 1 i specijalno njenu površinu — loptu — koja je analitički predočena sa

$$x^\star x = 1, \quad \text{tj.} \quad Nx = 1 \qquad (\text{norma od } x = 1)^{1)}. \tag{1}$$

12.2. Na taj način imamo parove vektora x, Ax, pa je prirodno promatrati i njihov skalarni produkt

$$y = x^\star\, ax = (Ax, x), \quad Nx = 1 \tag{2}$$

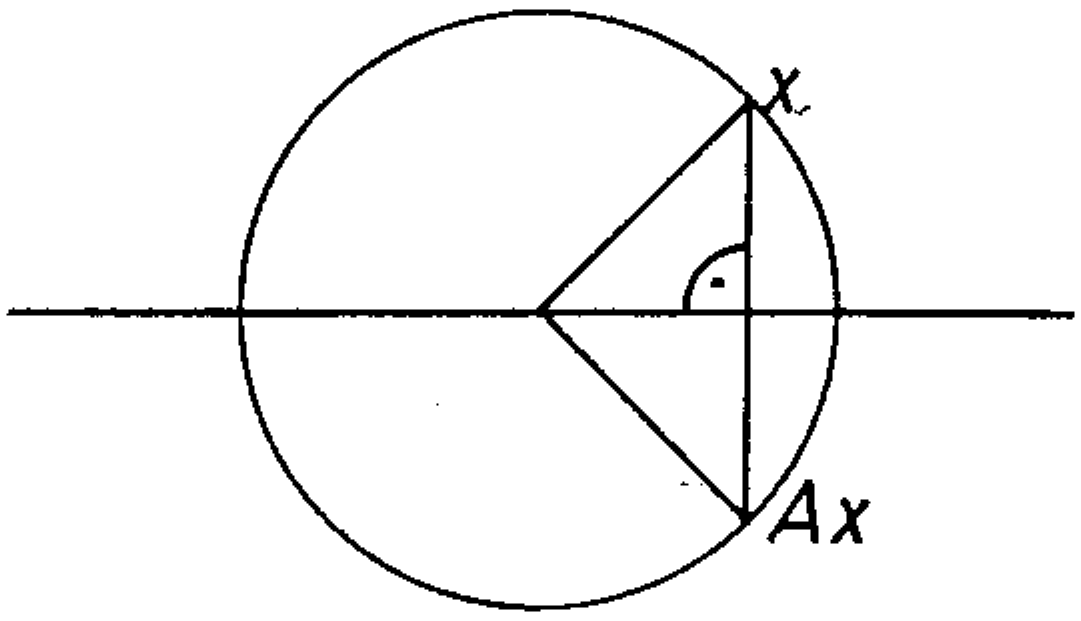
kao pratioca operacije $x \to ax$.

---

1) Prema tome, izlaganja u ovom paragrafu vrijede npr. za sve euklidske i hermitske prostore.

Tu je a matrica kojom je operator A zapisan u nekoj koordinatnoj bazi. Na taj način imamo određenu funkciju (2) na jediničnoj lopti (1).

12.3. Primjer. Ako u ravnini R_2 operator A znači simetriju prema pravulji p, tada broj (2) predstavlja kosinus od $2 \sphericalangle (p, x)$. Ako svaki put broj (2) nanesemo na jedinični vektor x, tj. promatramo vektor



Sl. 26.12.3.

$$(\vec{Ax}, x)\, \vec{x^0}, \tag{3}$$

gdje je

$$\vec{x^0} = \frac{\vec{x}}{(Nx)^{1/2}},$$

dobije se slikovit prikaz o mijenjanju broja (1); može se nanositi i recipročna vrijednost broja (2) i promatrati umjesto vektora (3) vektor

$$\frac{1}{Ax \circ x} \vec{x^0}. \tag{4}$$

Naravno, slike od (3) i (4) su zrcalno položene prema jediničnoj lopti (1).

12.4. Pitanje ekstrema skalarnog produkta $x^\star ax$ na jediničnoj lopti. Specijalno se postavlja pitanje o ekstremalnim vrijednostima skalarnog produkta (2) na *jediničnoj* lopti. Zor nas upućuje da funkcija (2) ima bar jedan ekstrem, tj. da na lopti (1) postoji bar jedna tačka ξ za koju je $\xi^\star a \xi$ veće ili manje nego brojevi (2) za neku okolinu broja ξ[1].

Zanimljivo je da je ta slika o postojanju tačke ξ ekvivalentna s činjenicom da svaki algebarski polinom ima bar jedno nula-mjesto.

12.5. I baš ta mjesta ξ na jediničnoj lopti S za koja skalarni produkt $Ax \circ x$ postaje ekstremalnim određuju tzv. *invarijantne pravulje linearnog operatora A* (pogl. 24, § 11.2).

Tako npr. za gornji primjer prostora R_2 ekstremi očigledno nastupaju u sjecištima $S_1 \cap p$ kružnice S_1 i pravulje p te na krajevima okomitog dijametra; ekstremne su vrijednosti 1 i -1.

$\longrightarrow$ **12.6. Teorem.** ***Ako funkcija $x \to ax \circ x = x^\star ax$ na lopti $Nx = 1$ ima u tački ξ stacionarnu vrijednost, i to λ, tada je $a\xi = \lambda\xi$; i obrnuto: ako je $N\xi = 1$ pa ako su vektori $a\xi$, ξ na istoj pravulji, dakle $a\xi = \lambda\xi$ (λ je skalar), tada funkcija $y = ax \circ x$ uzima u ξ stacionarnu vrijednost i ona je $= \lambda$; pri tom prostor uzimamo realnim, odnosno da je $a^\star = a$.***

---

[1] No, lopta je bikompaktan prostor; funkcija $|x^\star ax|$ je neprekidna realna funkcija na tom prostoru: a jedan elementarni teorem teorije skupova kaže da svaka neprekidna realna funkcija u svakom bikompaktnom prostoru ima svoj minimum i svoj maksimum (isp. Đ. Kurepa [1], str. 355, teorem 29.6.2).

12.7. Pretpostavimo da preslikavanje (2) uzima ekstremalnu vrijednost λ za $x=\xi$. Radimo matrično.

Uvedimo numeričku realnu varijablu t i promatrajmo funkciju

$$\Phi(t)=(\xi+ty)^{\star}\, a\,(\xi+ty)-\lambda\,(\xi+ty)^{\star}\,(\xi+ty), \tag{5}$$

kojom uspoređujemo učinak A-operatora i kratnika λI jediničnog (identičnog) operatora I. Vidi se da je

$$\Phi(t)=(\xi^{\star}+ty^{\star})\,(a\xi+tay)-\lambda\,(\xi^{\star}+ty^{\star})\,(\xi+ty),$$

$$\Phi(t)=\xi^{\star}a\xi+ty^{\star}a\xi+t\xi^{\star}ay+t^2y^{\star}ay-\lambda\xi^{\star}\xi$$

$$-\lambda ty^{\star}\xi-\lambda t\xi^{\star}y-\lambda t^2y^{\star}y.$$

To je u t kvadratna funkcija. Nađimo joj derivat $\frac{d}{dt}\Phi$, i to posebno za $t=0$:

$$\frac{d}{dt}\Phi(t)=y^{\star}a\xi+\xi^{\star}ay+2\,ty^{\star}ay-\lambda y^{\star}\xi-\lambda\xi^{\star}y-2\lambda ty^{\star}y, \tag{5'}$$

odnosno za $t=0$:

$$\Phi'(0)=y^{\star}a\xi+\overline{(ay)^{\star}\xi}-\lambda y^{\star}\xi-\lambda\overline{y^{\star}\xi}$$

(jer je $u^{\star}v=\overline{v^{\star}u}$)

$$\Phi'(0)=(y^{\star}a\xi+\overline{y^{\star}a^{\star}\xi})-\lambda\cdot 2\,Re\,(y^{\star}\xi),$$

$$\Phi'(0)=2\,Re\,(y^{\star}a\xi)-2\lambda\,Re\,(y^{\star}\xi)$$

($\mathrm{Re}\,z=$ realni dio od z).

$$\Phi'(0)=2\,Re\,(y^{\star}\,(a\xi-\lambda\xi). \tag{6}$$

Tako smo dobili izraz koji pokazuje kako se brzo mijenja funkcija $\Phi(t)$ oko 0. Ako za $t=0$ funkcija $\Phi(t)$ ima biti ekstremalnom za dano ξ, mora vrijediti $\Phi'(0)=0$, tj. prema (6):

$$2\,Rey^{\star}\,(ax-\lambda x)=0. \tag{7}$$

Kako to mora vrijediti za svako y i za promatrano posebno $x=\xi$, mora biti

$$a\xi-\lambda\xi=0. \tag{8}$$

Odatle

$$\xi^{\star}a\xi=\lambda\xi^{\star}\xi,$$

što zbog $\xi^{\star}\xi=N\xi=1$ daje

$$\xi^{\star}a\xi=\lambda. \tag{9}$$

Tako smo došli do uslova (8), koji kaže da onaj vektor za koji funkcija (2) postaje ekstremalnom zadovoljava karakterističnu jednadžbu promatranog operatora; jednakost (9) kaže da je sam ekstrem dostignut na jediničnoj lopti.

12.8. A sad idemo obratnim putem: iz (9) izlazi (8), iz (8) izlazi (7), iz (7) izlazi $\Phi' 0 = 0$ uz značenje (6), pa relacija (5') pokazuje da funkcija (5) ima u $t=0$ stacionarnu vrijednost, i to $\Phi(0)$. No $\Phi(0) = \xi^\star a\xi - \lambda\xi^\star\xi$ što zbog (8) i $\xi^\star\xi = 1$ daje $\Phi(0) = 0$. Drugim riječima, za funkciju $y = x^\star ax$ na jediničnoj lopti znači uslov (8) da je ξ stacionarno mjesto za tu funkciju sa stacionarnom vrijednosti λ.

Time je zanimljivi teorem 12.6. potpuno dokazan.

12.9. Proces dijagonalizacije (isp. pogl. 16, § 2. i pogl. 27). Uzmimo sada slučaj $a^\star = a$ (hermitski operator). Jednakost (9) pokazuje da je skalar λ realan broj. Na taj način imamo realni broj λ i jedinični vektor ξ, za koji vrijedi (9), odnosno (8). Radi daljeg postupka označimo $\lambda = \lambda_1$, $\xi = l_1$. Dakle je

$$al_1 = \lambda_1 l_1 \qquad Nl_1 = 1.$$

A sada promatrajmo skup svih tačaka x polazne jedinične lopte za koje je $x^\star l_1 = 0$: to je presjek jedinične lopte i prostora $\perp l_1$; time se dobije jedinična lopta za dimenziju manje; pripadna potfunkcija polazne funkcije $x \to x^\star ax$ kao linearni operator ima opet svoj ekstrem λ_2 dostignut u nekoj tački l_2, pa će opet vrijediti

$$al_2 = \lambda_2 l_2, \qquad Nl_2 = 1, \qquad l_1 \perp l_1.$$

A onda bismo u toj podlopti tražili podloptu sastavljenu od svih tačaka x za koje je $x^\star l_2 = 0$ itd.

12.10. Zaključujemo da vrijedi

⟶ **Teorem.** ***Postoji niz od n realnih brojeva***

$$\lambda_1, \lambda_2, \ldots, \lambda_n$$

i niz pripadnih jediničnih vektora $l_1, l_2, \ldots, l_n$, koji čine ortonormiranu bazu l' i za koje je

$$a\, l_i = \lambda_i l_i. \tag{10}$$

12.11. Kako glasi matrični zapis $A_{e'}$ operatora A u toj novoj bazi e'? Glasi onako kako izgleda u toj bazi matrica stupaca u kojima su zapisani učinci operatora nad vektorima l_i. No $l_i \to \lambda_i l_i$, dakle je matrični zapis:

$$\begin{bmatrix} \lambda_1 & 0 & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix} = \operatorname{diag}[\lambda_1, \lambda_2, \ldots, \lambda_n]. \tag{11}$$

To je krupan rezultat. Došli smo do ortonormirane baze e', u kojoj je operator zapisan dijagonalno! Veza sa starim zapisom $A_e = a$ dobije se na osnovu fundamentalnog teorema 8.4. Zapisi vektora od maloprije u polaznoj bazi čine ortonormiranu matricu u, pa je veza

$$A_{e'} = u^{-1} au. \tag{12}$$

Uostalom, iz jednadžbi (10) i ortonormiranosti vektora e_i proizlazi direktno veza (12) (isp. pogl. 16, § 5.3.4). O tome će se u novom poglavlju 27. iscrpno govoriti!

13. VEKTORSKO MNOŽENJE VEKTORA KAO KOS OPERATOR[1)]

Promatrajmo slučaj *kososimetričnih realnih matrica* a reda 3. ($a^T = -a$). Uz gornju oznaku, vidi se da je ax kao geometrijski vektor jednak vektorskom produktu $y \times x$.

Dovoljno je promatrati pridruživanje

$$y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 0 & -y_3 & y_2 \\ y_3 & 0 & -y_1 \\ -y_2 & y_1 & 0 \end{bmatrix}$$

između kososimetričnih takvih matrica a i množine svih vektora prostora R_3. Naime, matrica a šalje stupac

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \text{ u}$$

$$ax = \begin{bmatrix} 0 & -y_3 & y_2 \\ y_3 & 0 & -y_1 \\ -y_2 & y_1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_3 y_2 - x_2 y_3 \\ x_1 y_3 - x_3 y_1 \\ x_2 y_1 - x_1 y_2 \end{bmatrix}.$$

A to je po definiciji »*vektorski produkt*«

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

vektorâ y i x; obično se radi lakšeg pamćenja piše:

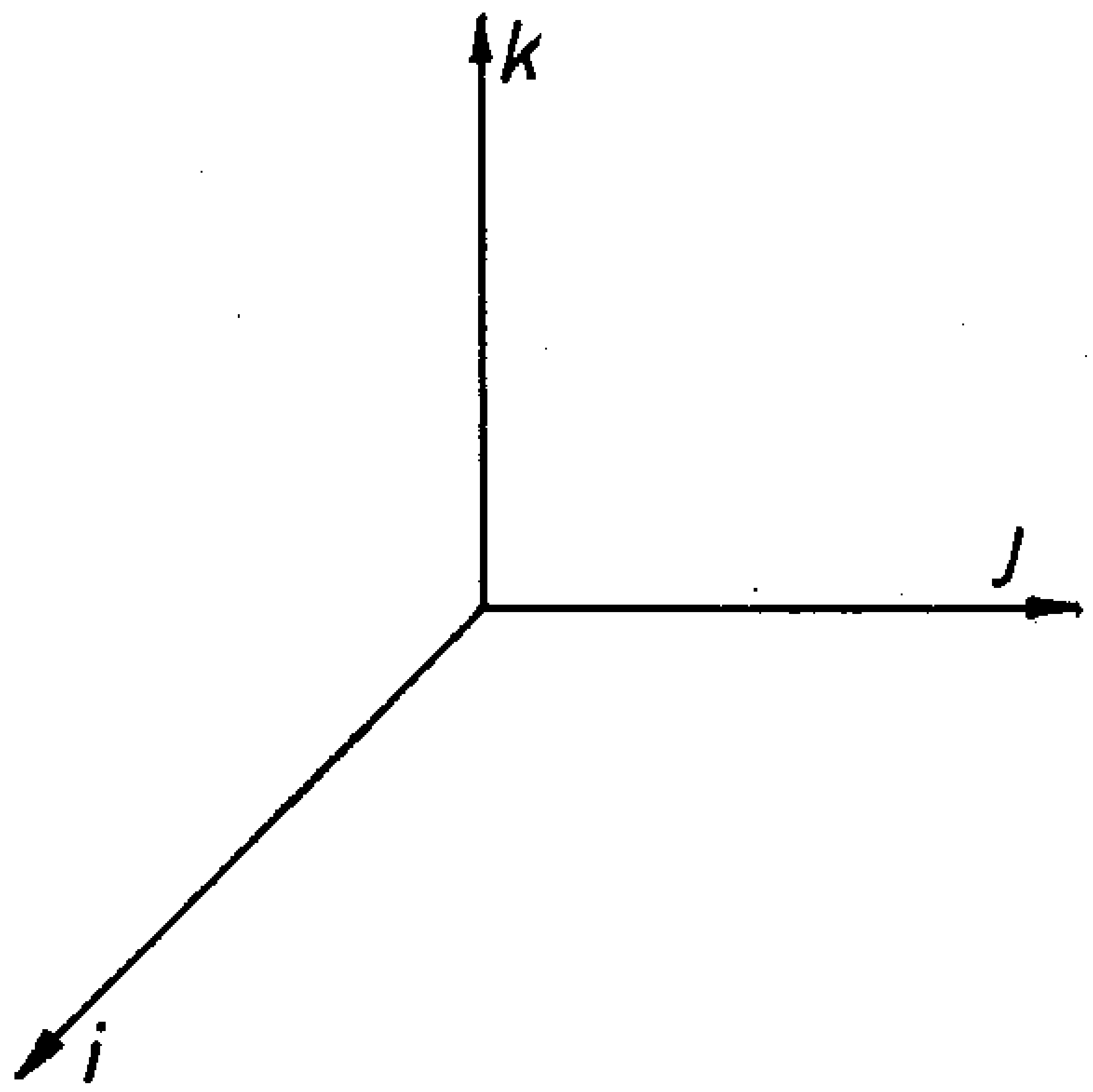
$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \det \begin{bmatrix} e_1 & y_1 & x_1 \\ e_2 & y_2 & x_2 \\ e_3 & y_3 & x_3 \end{bmatrix},$$

[1)] Isp. pogl. 23, § 8.6.

gdje je (e_1, e_2, e_3) ortonormirana vektorska baza *desne* orijentacije (ako smo vektore zadali kao retke, onda se piše

$$y \times x = \det \begin{bmatrix} i & j & k \\ y_1 & y_2 & y_3 \\ x_1 & x_2 & x_3 \end{bmatrix},$$

pri čemu i, j, k označuju elemente osnovnog triedra desne orijentacije (isp. pogl. 23, § 8.6).



Sl. 13.

14. ZADACI O LINEARNIM OPERATORIMA

1. U euklidskom prostoru R_2 (tj. u ravnini) zadani su koordinatni vektori e_1, e_2; u bazi (e_1, e_2) prikaži pomoću matricâ: 1) projiciranje $\| e_2$ na e_1; 2) projiciranje $\| e_1$ na e_2; 3) koliki je produkt tako dobivenih matrica; 4) koji operator taj produkt predstavlja?

2. Formuliraj pitanje poput prethodnog radeći u euklidskom prostoru R_3 s koordinatnom bazom $e = (e_1\, e_2\, e_3)$ i promatrajući projiciranje p_i na prostor što ga određuju vektori $\{e_1, e_2, e_3\} \setminus \{e_i\}$ $(i = 1, 2, 3)$; projiciranje je $\| e_i$.

3. Poopći na R_n za $n = 4, 5, \ldots$

4. U prostoru $R_3[x]$ polinomâ $p(x)$ stepena < 3 prikaži deriviranje $p \to Dp$ pomoću matrice služeći se bazom 1) $(1, x, x^2)$; 2) $x, x^2, 1$. Nađi $D^2 p, D^3 p, D^4 p, \ldots$ Poopći na $R_n[x]$ za $n = 1, 2, 4, 5, 6, \ldots$

5. Zadan je vektorski prostor V_3 s bazom $e = (e_1\, e_2\, e_3)$; ako je linearni operator A: $V_3 \to V_3$ predstavljen, u bazi e, matricom a, kojom je matricom taj operator A predstavljen u bazi

   1) (e_2, e_3, e_1); 2) (e_3, e_2, e_1); $(e_1 - e_2, e_2 - e_3, e_1 + 2e_3)$;

   4) $(e_1 + e_2 - 3e_3, e_1 - 2e_2, -e_1 + e_2 + e_3)$?

6. Zadana je baza $e=(e_1, e_2, \ldots, e_n)$ prostora V_n; prikaži u toj bazi matricom ovaj linearni operator A:

   1) $Ae_1=e_2,\ Ae_2=e_3, \ldots, Ae_{n-1}=e_n,\ Ae_n=e_1$;
   2) $Ae_1=e_1,\ Ae_\nu=0$ za $\nu \neq 1$;
   3) $Ae_1=e_2,\ Ae_2=e_1,\ Ae_\nu=e_\nu$ za $\nu>2$;
   4) A permutira e_3, e_7 a ne dira ostale e_ν;
   5) $Ae_1=e_1,\ Ae_2=e_1+e_2,\ Ae_3=e_1+e_2+e_3, \ldots$

7. Kojom je matricom u bazi $e_1=(1, 0, 0)$, $e_2=(0, 1, 0)$, $e_3=(0, 0, 1)$ prikazan linearan operator H za koji je $He_1=(3, 2, 1)$, $He_2=(0, 0, 0)$, $He_3=(0, 0, 0)$? Kojom je matricom prikazan taj operator u bazi $e'=(e_1'=(0, 0, 3),\ e_2'=(1, 1, 0),\ e_3'=(1, 2, 3))$?

8. U prostoru V_3 zadani su vektori $e_1=(1\ 0\ 0)$, $e_2=(0\ 1\ 0)$, $e_3=(0\ 0\ 1)$; odredi sve regularne linearne operatore H za koje je $H\{e_1, e_2, e_3\}=\{e_1, e_2, e_3\}$. Obrazuju li oni grupu u odnosu na uzastopno izvođeje operatorâ? Obrazuju li oni linearnu algebru? A ako zahtijevamo da bude $H\{e_1, e_2\ e_3\} \subset \{e_1, e_2\ e_3\}$?

9. Isto pitanje za proizvoljnu bazu iz V_3.

10. Isto pitanje za V_n.

11. Odredi matricu operatora E_{12} za koji je $E_{12}\, e_j=e_1\, \delta_{2j}$.

12. Isto pitanje za operator E_{ik} za koji je $E_{ik}\, e_j=e_i\, \delta_{kj}$; naravno $i, k \in \{1, 2, \ldots, n\}$. Odredi det E_{ik}.

13. U prostoru K_{22} matricâ formata (2, 2) promatraj onaj operator A koji bazu $e_1=\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}$, $e_2=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$, $e_3=\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}$, $e_4=\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}$ prevodi u $\begin{bmatrix}3 & 2\\ 1 & 0\end{bmatrix}=Ae_1$, $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=Ae_2$, $\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}=Ae_3$, $\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}=Ae_4$. Kako glasi matrični prikaz operatora A u bazi $e=(e_1, e_2, e_3, e_4)$?

14. Isto pitanje za operator B za koji je $Be_i=\begin{bmatrix}3 & 2\\ 4 & 5\end{bmatrix}$ pri $i=1, 2, 3, 4$.

15. Promatraj prostor K_{22} iz zad. 13 i neki član $k \in K_{22}$; pridružimo li svakom $x \in K_{22}$ veličinu 1) kx; 2) kx^T; 3) kx^{-1}; 4) $k^{-1}xk$; 5) kxk; 6) k^2x; 7) k^3x,

    koje je od tih 7 preslikavanja linearan operator?

16. Promatraj prostor $R_3[x]$ svih polinoma $p(x)$ stupnja <3 odnosno prostor $R[x]$ svih polinoma s koeficijentima u tijelu R realnih brojeva. Da li je preslikavanje $p(x) \to (1+x-x^2)\, p(x)$ linearan operator?

17. U prethodnom prostoru $R_3[x]$ promatraj bazu $(e_1=1,\ e_2=x,\ e_3=x^2)$' odnosno bazu $(e_1'=1,\ e_2'=1+x,\ e_3'=1+x+x^2)$;

1) odredi matrični zapis a operatora $p(x) \to \text{Der}\, p(x)$ i to u bazi e i u bazi e';
2) kako glasi prevodna matrica od e na e'?
3) Nađi koordinate vektora $1+x+x^2$ i u jednoj i u drugoj bazi;
4) što znači $a^T p$ za polinome $p(x)$ za koje je st $p<3$?

18. Čine li sve neprekidne funkcije f: $R \to R$ linearnu algebru u odnosu na obično množenje funkcija?

19. Čine li svi vektori u ravnini linearnu algebru u odnosu na
1) vektorsko množenje; 2) skalarno množenje. Postoji li jedinica?

20. Čine li polinomi iz $R[x]$ linearnu algebru nad $(R, +, \cdot)$ u odnosu na množenje polinomâ? A polinomi koji se poništavaju u skupu:
1) $\{0\}$; 2) $\{5\}$; 3) $\{0, 2\}$; 4) $\{1, -1, 3, 4\}$?

21. Što znači da matrice formata (2, 2) i s vrijednostima iz
1) Q; 2) R; 3) $R(i)$ čine multiplikativnu linearnu algebru u odnosu na množenje? 1) Jesu li one divizione? 2) Imaju li jedinicu?

22. Odredi determinantu, rang i defekt pojedinih operatora iz prethodnih primjera.

23. U prostoru $R[x]$ svih polinoma promatraj deriviranje D i množenje M skalarom m; nađi u bazi $1, x, x^2, \ldots$ matricu operatorâ $MD-DM$, $M^2D-MD^2, \ldots$ Jesu li ti operatori regularni?

24. Napiši nekoliko matrica koje su kongruentne s matricom

$$a=\begin{bmatrix} 1 & -1 \\ 3 & 4 \end{bmatrix}.$$

Je li a kongruentno s $-a$, $3a$, ka?

25. Kako izgledaju matrice koje su međusobno i slične i kongruentne? Navesti primjer.

26. Neka $a^{(ik)}$ odnosno $a_{(ik)}$) nastaje iz matrice a transpozicijom redaka (stupaca) i, k; da li je nužno
1) $a^{(ik)}$, 2) $a_{(ik)}$, 3) $(a^{(ik)})_{(ik)}$, 4) $(a_{(ik)})^{(ik)}$ slično sa a?

27. Za svaku permutaciju p brojeva $1, 2, \ldots, n$ svaka (n, n)-matrica a slična je s matricom $b=[a_{p_i p_k}]$, pri čemu $i, k=1, 2, \ldots, n$.

28. Ako su a, b slične matrice, tada skup svih rješenjâ x jednadžbe

$$b=x^{-1}ax$$

čini multiplikativan grupoid; dokaži; šta to znači geometrijski?

Literatura: v. poglavlje 23.

POGLAVLJE 27.

KARAKTERISTIČNI POLINOM. SVOJSTVENE VRIJEDNOSTI

1. INVARIJANTNI SMJEROVI. KARAKTERISTIČNI POLINOM ZADANE MATRICE

1.0. Priprema i uvodni primjer. Svaka kvadratna matrica a reda n je određen linearni operator u vektorskom prostoru $V_n(e)$ s bazom e; odnosno, a je reprezentacija određenog linearnog operatora A koji djeluje unutar prostora.

Nastaje osnovno pitanje: *može li se, izborom pogodne vektorske baze e', taj operator A prikazati u dijagonalnom obliku?*

1.1. Tako npr. ako je $e=(e_i)$ zadana vektorska baza, pa ako linearni operator A definiramo tako da bude $Ae_n'=c_n'e_n'$, gdje su c_n' određene konstante, onda će operator A biti zaista predstavljen dijagonalnom matricom

$$a=\begin{bmatrix} c_1 & & 0 \\ & c_2 & \\ 0 & & \ddots \end{bmatrix};$$

svaka matrica $f^{-1}af$ koja je slična sa a predstavlja to *isto* preslikavanje A, ali u nekoj *drugoj* koordinatnoj bazi e'. Da smo bili pošli od te baze, e', i od matrice $f^{-1}af$, onda bismo, prelazeći na gornju bazu e, došli do traženog dijagonalnog oblika diag $[c_1, c_2, \ldots]$.

1.2. Uopće, neka endomorfno preslikavanje A ima svojstvo da stanoviti smjer ne mijenja, tj. da je stanoviti vektor $x \neq 0$ preslikan u proporcionalni (tj. paralelni) vektor λx; prema tome je $Ax=\lambda x$ (λ je skalar); tada, uzimajući npr. taj vektor $x=e_1$ u vektorsku bazu, pripadna matrica a imat će u početnom stupcu vrijednosti $a_{11}=\lambda$, dok će sve druge vrijednosti u tom stupcu biti $=0$. I matrica a će održavati smjer x, jer će pripadni stupac $x(e)$ ona prevesti u stupac $\lambda x(e)$.

1.3. Bit će, dakle,

$$a\,x(e)=\lambda\,x(e), \text{ odnosno } a\,x=\lambda\,x \text{ za bar jedno } x\in V(e).$$

1.4. Osnovni problem. Tako smo došli do osnovnog problema: *za zadanu kvadratnu matrica a potražiti nenulte vektore x i skalare λ za koje je*

$$ax = \lambda x. \tag{1}$$

Odatle

$$(\lambda - a)\, x = \vec{0}. \tag{2}$$

Da bude $x \neq \vec{0}$, treba, a i dovoljno je da bude

$$|\lambda\, 1_n - a| = 0 \quad \text{ili eksplicitno det } (\lambda\, 1_n - a) = 0, \quad \text{tj.} \tag{3}$$

$$\begin{vmatrix} \lambda - a_{11} & -a_{12} & -a_{13} \ldots \\ -a_{21} & \lambda - a_{22} & -a_{23} \ldots \\ \ldots & \ldots & \ldots \end{vmatrix} = 0. \tag{4}$$

Ta jednadžba ima vanredno važnu ulogu. Zove se *karakteristična ili svojstvena jednadžba matrice a*; polinom na lijevoj strani zove se *karakteristični ili svojstveni polinom matrice a.*

1.4.1. Primjer. Za matricu $a = \begin{bmatrix} 4 & 10 \\ -0{,}2 & 1 \end{bmatrix}$ jednadžba (4) glasi:

$$\begin{vmatrix} \lambda - 4 & -10 \\ 0{,}2 & \lambda - 1 \end{vmatrix} = 0, \quad \text{tj.} \quad (\lambda - 4)(\lambda - 1) + 2 = 0,$$
$$\text{odnosno} \quad \lambda^2 - 5\lambda + 6 = 0.$$

Nula-mjesta toga polinoma jesu

$$2,\ 3. \tag{5}$$

Nađimo pripadna rješenja x jednadžbe (2). Za $\lambda = 2$ jednadžba (2) glasi:

$$\begin{bmatrix} -2 & -10 \\ 0{,}2 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \text{ tj.} \quad \begin{matrix} -2x_1 - 10x_2 = 0 \\ 0{,}2x_1 + \quad x_2 = 0; \end{matrix} \text{ dakle je } x_2 = -0{,}2\, x_1.$$

Tako npr. vektor $e = \begin{bmatrix} 1 \\ -0{,}2 \end{bmatrix}$ je jedno rješenje. Eto, uzimajući taj vektor u koordinatnu bazu, matrica će se pojednostaviti.

Za drugo rješenje $\lambda = 3$ jednadžba (2) glasi:

$$\begin{bmatrix} -1 & -10 \\ 0{,}2 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = 0, \text{ tj.} \quad \begin{matrix} -x_1 - 10x_2 = 0 \\ 0{,}2x_1 + \ 2x_2 = 0, \end{matrix} \text{ tj. } x_1 = -10\, x_2,$$

gdje je x_2 proizvoljno; specijalno, za $x_2 = 1$ izlazi vektor $[-10,\ 1]^T$,

$$\text{tj.} \begin{bmatrix} -10 \\ 1 \end{bmatrix}.$$

Na taj smo način dobili vektore-stupce $[1,\ -0{,}2]^T$, $[-10,\ 1]^T$ i njihovu matricu

$$f = \begin{bmatrix} 1 & -10 \\ -0{,}2 & 1 \end{bmatrix}.$$

Očigledno imamo jednadžbe

$$af_1 = 2f_1$$
$$af_2 = 3f_2,$$

gdje je

$$f_1 = \begin{bmatrix} 1 \\ -0{,}2 \end{bmatrix}, \quad f_2 = \begin{bmatrix} -10 \\ 1 \end{bmatrix}.$$

Ili kraće:

$$af = f \operatorname{diag}[2,\ 3], \text{ gdje } \operatorname{diag}[2,\ 3] = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}.$$

Odatle, množeći s lijeve strane sa f^{-1}, izlazi

(*) $$f^{-1}af = \operatorname{diag}[2,\ 3].$$

Na taj je način matrica a prevedena na dijagonalni oblik, i to služeći se matricom f. Funkcionalno, znači to ovo: ako stupce f_1, f_2 matrice f uzmemo za novu koordinatnu bazu e', onda to prema pogl. 23, § 3.3 znači da je $e' = ef$, gdje je e polazna vektorska baza; nove koordinate x' izlaze iz starih x transformacijom $x \to ax'$; to znači da se stare koordinate dobivaju iz novih množenjem sa f; zato prema pogl. 26, § 8.4 prelazi polazna matrica a u sličnu matricu $f^{-1}af$, koja je, kao što smo vidjeli, $= \operatorname{diag}[2,\ 3]$. Uostalom, jednakost (*) se lako provjeri direktnim izračunavanjem.

Najprije iz

$$f = \begin{bmatrix} 1 & -10 \\ -0{,}2 & 1 \end{bmatrix} \text{ izlazi } f^{-1} = \begin{bmatrix} -1 & -10 \\ -0{,}2 & -1 \end{bmatrix}$$

pa je zato

$$f^{-1}af = \begin{bmatrix} -1 & -10 \\ -0{,}2 & -1 \end{bmatrix} \begin{bmatrix} 4 & 10 \\ -0{,}2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -10 \\ -0{,}2 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} -1 & -10 \\ -0{,}2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 2 & -30 \\ -0{,}4 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} = \operatorname{diag}[2,\ 3].$$

Dakle uistinu, uzimajući invarijantne smjerove matrice $a = \begin{bmatrix} 4 & 10 \\ -0{,}2 & 1 \end{bmatrix}$ za novu bazu, prelazi ta matrica a u dijagonalni oblik $\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$, pri čemu su se na dijagonali pojavila upravo rješenja karakteristične jednadžbe (4).

Da vidimo kako stvar izgleda općenito.

1.5. Sekularna jednadžba. Jedan od osnovnih problema matričnog računa sastoji se u tome da se za zadanu matricu a nađe njen spektar.

U slučaju da je matrica a formata (3, 3) realna i simetrična (tj. $a^T = a$), zove se pripadna karakteristična jednadžba također *vjekovnom ili sekularnom jednadžbom*; već 1773. pokazao je Lagrange [Lagránž] da vjekovna jednadžba ima samo realna rješenja.[1]

[1]) Sekularna jednadžba pojavljuje se u djelu Laplace, *Mécanique céleste* (Nebeska mehanika) I, 2, § 56, pri ispitivanju sekularnih smetnji planeta. Analognu ulogu ima danas karakteristična jednadžba matrice pri ispitivanju smetnji planeta, atomskih čestica, malih titranja itd.

1.6. Teorem. *Slične matrice imaju iste karakteristične polinome* (4).

Neka je c regularna matrica; promotrimo tada matricu $\lambda - c\,a\,c^{-1}$ i pripadnu determinantu $\det(\lambda - c\,a\,c^{-1})$. Dokažimo da je ona $= \det(\lambda - a)$.

No,

$$\det(\lambda - c\,a\,c^{-1}) = (\det c)^{-1} (\det c) \det(\lambda - c\,a\,c^{-1}) =$$

$$= (\det c)^{-1} \det(\lambda - c\,a\,c^{-1}) \det c = \det[c^{-1}(\lambda - c\,a\,c^{-1})\,c] =$$

$$= \det[(c^{-1}\lambda - a\,c^{-1})\,c] = \det(c^{-1}\lambda\,c - a) = \det(\lambda - a).$$

1.6.1. Zato je jasno da možemo i za svaki linearni operator A promatrati karakteristični polinom $A(\lambda)$ kao $\det(\lambda - a)$, gdje je a matrica koja predstavlja operator A za neku bazu vektora.

2. NEKOLIKO OSNOVNIH NAZIVA, DEFINICIJA I ČINJENICA

2.0. K označuje neko algebarsko tijelo ili korporaciju; to je rezerva za skalare (najobičniji slučaj u praksi: Q, R, C, tj. skup racionalnih, odnosno realnih odnosno kompleksnih brojeva). V, odnosno $V_n(K)$ označuje proizvoljan vektorski prostor, i to od n dimenzija. Za svako $t_1 \in V$, $t_1 \neq 0$ zove se $K\,t_1$ pravulja ili prava prostora, i to ona pravulja što je određuje (element) t_1 zajedno sa $\vec{0}$. Naravno, $\vec{0} \in K\,t_1$. Za svaku eventualnu tačku $t_1 \in V \setminus K\,t_1$ imamo pravulju $K\,t_2$ te kombiniranu sumu

(1) $$K\,t_1 + K\,t_2 \text{ svih } \dot{K}\,t_1 + K'\,t_2;$$

to je ravnina prostora V, i to ravnina što ju određuju tačke t_1, t_2 i $\vec{0}$ ($\vec{0}$ se uvijek podrazumijeva).

Ako izvan ravnine (1) postoji još koja tačka t_3 prostora, onda se analogno definira trodimenzionalni prostor

(2) $$K\,t_1 + K\,t_2 + K\,t_3 \text{ itd.}$$

Prostor ima n dimenzija ako ima n tačaka $t_n' \neq 0$ sa svojstvom da svako t_n' leži izvan prostora što ga razapinju preostale tačke iz $(t_1, t_2, \ldots, t_i, \ldots, t_n)$.

2.1. Invarijantni prostor i maksimalni invarijantni prostori linearnog operatora. Neka je A linearni operator s oblašću D, koja je dio (pravi ili nepravi) od $V_n(K)$.

Definicija. *Svaki prostor V' sa svojstvom $A\,V' \subset V'$ zove se invarijantni potprostor za operator A.* To znači da iz $x \in V'$ izlazi $A\,x \in V'$.

Naravno da odatle ne izlazi da mora biti *svaki* element x u V' fiksan, nepomičan (invarijantan), tj. $A\,x = x$.

2.1.1. *Maksimalni* (*minimalni*) *invarijantni potprostor operatora A* je svaki invarijantni potprostor koji nije sadržan u opsežnijem (užem) invarijantnom potprostoru $\subsetneq V$ odnosno $\subsetneq \{0\}$).

Tako je npr. za projiciranje prostora na koju ravninu α ravnina invarijantna pri projiciranju (čak je i svaki element ravnine α invarijantan). Za linearni operator $x \to 3x$ svaki potprostor je invarijantan. Ako r označuje rotaciju ravnine oko 0 za $\pi/2$, tada u α (osim trivijalnog potprostora $\{0\}$) ne postoji nijedan potprostor koji bi bio invarijantan za taj linearni operator r.

2.2. Invarijantne pravulje. Specijalno je važno ispitivanje invarijantnih pravulja prema operatoru A.

Definicija. Pravulja p je invarijantna prema operatoru A ako je Ap opet u p. Zanimljivo je spomenuti da je tada Ap ili $=p$ ili se reducira na $\vec{0}$.

No, ako je pravulja p invarijantna prema A, tj. $A\dot{p}\in p$ znači to da je $A\dot{p}=\lambda\dot{p}$; stvarno, ako je pravulja $p=Kt_0$, onda je

$$\dot{p}=ct_0 \text{ sa } c\in K; \text{ isto tako}$$

$$A\dot{p}=c' t_0 \text{ uz } c'\in K.$$

Eliminacijom vektora t_0 iz prethodnih dviju jednadžbi izlazi

$$A\dot{p}=\frac{c'}{c}\dot{p}, \text{ i to za svako } \dot{p}.$$

2.2.1. Rastezanje (dilatacija). Teorem. *Ako je pravulja p invarijantna za linearni operator A, onda je nužno $A\dot{p}=\lambda\dot{p}$ za neki skalar $\lambda\in K$.* To znači da operator A predstavlja na pravulji p *rastezanje* ili *homotetiju* s koeficijentom λ.

2.2.2. Problem dijagonalizacije. Važno je uočiti da je koeficijent rastezanja λ jednoznačno određen invarijantnom pravuljom p.

Zato, ako slučajno operator A ima n invarijantnih različitih pravulja $p_{n'}$ koje određuju V, bit će time automatski određen niz λ_ν od n skalara sa svojstvom $A\dot{p}_\nu=\lambda_\nu\dot{p}_\nu$; pa ako na svakoj pravulji p_ν odaberemo tačku $e'_{n'}\neq 0$, dobit ćemo time *bazu* $e=(e_i)_i$ u promatranom vektorskom prostoru V; naravno, $Ae_\nu=\lambda_\nu e_\nu$. No, svakoj tački $x\in V$ pripada jednoznačan rastav $x=\Sigma x_{n'} e_{n'}$; time se dobiva stupac-vektor

$$x(e)=\begin{bmatrix} x_1 \\ \vdots \\ x_\nu \\ \vdots \end{bmatrix}$$

i prostor $V(e)$ svih tih stupaca. Operator A se sada u toj bazi e zapisuje kao matrica $[Ae_1(e), Ae_2(e); \ldots]$, tj. kao dijagonalna matrica $\begin{bmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \ddots \end{bmatrix}$.

Time je postignuto željeno pojednostavnjenje; *operator A je zapisan dijagonalno.* Zato je jasno da će dijagonalni operatori u množini svih operatora koji deluju u prostoru K_n od n dimenzija biti relativno jednostavni. Međutim, u praksi i primjenama, a i u teoriji, baš su dijagonalni operatori vrlo česti, a time često imamo posla i s matricama koje su slične dijagonalnima.

2.3. Kako doći do invarijantnih pravulja? Karakteristični ili svojstveni polinom. Ako je $\dot{p}$ invarijantna pravulja, tada je potpuno određen skalar $\lambda \in K$ sa svojstvom $A\dot{p} = \lambda\dot{p}$ (isp. 2.2.1). Odatle:

$$\lambda\dot{p} - A\dot{p} = 0$$

$$(\lambda - A)\dot{p} = 0.$$

Za matrice A znamo da odatle mora biti $\det(\lambda - A) = 0$; međutim, ako A nije matrica, tada možemo A odrediti pomoću baze $e = (e_{n'})$ i A zapisati matrično kao $A(e)$. Tada gornji rezultat postaje $\det(\lambda(n) - A(e)) = 0$, i to za svaku bazu e; umjesto toga piše se po definiciji

(3) $$\det(\lambda(n) - A)) = 0.$$

Tako smo našli vrelo za skalare λ: treba riješiti karakterističnu jednadžbu (3).

Prije zapisa toga rezultata i njegova obrata evo nekoliko osnovnih definicija.

2.4. Svojstveni (karakteristični) vektori, svojstvene (karakteristične) vrijednosti ili značenja linearnog operatora. — 2.4.1. Svojstven par skalar-vektor u odnosu na operator A je *svaki* par (λ, x) skalara λ i vektora x za koji je

(1) $$Ax = \lambda x.$$

2.4.2. Svaki vektor x za koji vrijedi (1) zove se *svojstven ili karakterističan vektor* operatora A. Primijetimo da relacija (1) i relacija $x \neq 0$ jednoznačno određuju λ.

2.4.3. Svaki skalar λ za koji jednadžba $Ax = \lambda x$ ima bar jedno rješenje $x \neq 0$ zove se *svojstveno ili karakteristično značenje (vrijednost) operatora A.*

2.4.4. Skup svih vektora za koje vrijedi $Ax = \lambda x$ (za dano svojstveno λ) zove se *svojstven prostor matrice* (operatora) A (vezan za svojstvenu vrijednost λ); označit ćemo ga sa $K(A)$ odnosno $K_n(A; \lambda)$.

Time želimo istaknuti i tijelo K, u kojem leže skalari λ, i dimenziju prostora na kojem operator deluje.

2.5. Determinanta operatora A je determinanta matrice koja ga predstavlja (isp. pogl. 26, § 9.7).

2.6. Karakteristični ili svojstveni polinom matrice i linearnog operatora. Karakteristični polinom matrice (operatora) A je determinanta operatora $\lambda - A$; tu λ znači operator, odnosno skalarnu matricu koja svakoj tački prostora pridjeljuje tačku λx; tu bi bilo bolje umjesto λ pisati $\lambda(n)$. Uostalom, uvijek će se iz razlaganja vidjeti da li λ znači skalar ili operator; tako će npr. znak 2, osim što označuje broj 2, označivati i skalarnu matricu $2(n)$ reda n. Ako je potrebno, to će se reći izričito. Treba biti načisto da simboli u matematici imaju i pozicionu, relativnu vrijednost (najjednostavniji slučaj: poziciona vrijednost brojki).

Karakteristični (svojstveni) polinom operatora A označuje se sa $A(\lambda)$ ili $\varkappa(\lambda, A)$ dakle,

(2) $$A(\lambda) = \det(\lambda - A) = (-1)^n \det(A - \lambda).$$

Specijalno, za matricu a je

$$\lambda - a = \begin{bmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{bmatrix} - \begin{bmatrix} a_{11} \cdots a_{1n} \\ \cdots\cdots \\ a_{n1} \cdots a_{nn} \end{bmatrix}, \text{ tj.}$$

(4) $$a(\lambda) = \begin{bmatrix} \lambda - a_{11} & -a_{12} \cdots & -a_{1n} \\ \cdots & \cdots & \cdots \\ -a_{n1} & -a_{n2} \cdots & \lambda - a_{nn} \end{bmatrix}.$$

To je polinom n-tog stupnja, tj. $\operatorname{st} a(\lambda) = \operatorname{st} a$.

2.7. Karakteristična ili svojstvena jednadžba matrice (linearnog operatora) A. To je jednadžba $\det(\lambda - A) = 0$ s obzirom na skalar λ kao nepoznanicu.

2.8. Rezolventa (operatora) A jest $(\lambda - A)^{-1}$; svaki skalar λ za koji $(A-\lambda)^{-1}$ postoji zove se *regularan* skalar u odnosu na A.

2.9. Spektar operatora A jest skup σ_A sastavljen od svih rješenja karakteristične jednadžbe; ako se pri tom svako rješenje računa sa svojom kratnošću dobije se spektar S_A^- s ponavljanjem.

2.10. Primjedba. Naravno da se umjesto nepoznanice λ može uzeti oznaka x, t ili nešto drugo; često dolazi s kao oznaka nepoznanice, odnosno varijable, pa se govori o *s-polinomu* i *s-jednadžbi* misleći na $a(s)$, odnosno $a(s) = 0$.

2.11. Algebarsko vrelo svojstvenih vrijednosti matrice.

—→ **Osnovni teorem.**

(i) ***Svaki svojstveni broj operatora A zadovoljava svojstvenu ili karakterističnu jednadžbu toga operatora, tj. iz $Ax = \lambda x$, $x \neq 0$ izlazi $A(\lambda) = 0$.***

(ii) ***Za svaki linearni operator (kvadratnu matricu) reda $n < \infty$ nad tijelom C kompleksnih brojeva postoji bar jedna svojstvena vrijednost λ_0, tj. $\det(A - \lambda_0) = 0$, za neko $\lambda \in C$.***

(iii) ***Za svaki skalar λ za koji vrijedi $A(\lambda) = 0$ postoji bar jedan vektor $x \neq 0$ za koji je $Ax = \lambda x$ i jedna pripadna invarijantna pravulja prostora C_n od konačno mnogo dimenzija.***

D o k a z. Radimo matrično (a primišljaj i operator!).

(i) To je dokazano u § 1.4 (ako A znači matricu).

Najprije $A(\lambda)=0$ je *algebarska* jednadžba s realnim ili kompleksnim koeficijentima; po „osnovnom poučku algebre" ima ta jednadžba bar jedno rješenje $\lambda_0 \in C$, tj. $A(\lambda_0)=0$.

(ii) No, jednakost $A(\lambda_0)=0$ znači da je kvadratna matrica $\lambda_0 - A$ singularna; zato postoji bar jedan vektor $x_0 \neq 0$ za koji je

$$(\lambda_0 - A)\, x_0 = 0 \qquad \text{(isp. pogl. 11, § 10), tj.}$$

(5) $$\lambda_0 x_0 = A\, x_0 .$$

Tako je nađen svojstven par (λ_0, x_0).

Pravulja $K x_0$, tj. skup vektora $c x_0$, gdje c prolazi tijelom K, iz kojeg su skalari, jest prostor; dokažimo da je to *invarijantan* potprostor za operator $\lambda_0 - A$.

Naime, množeći (5) brojem c sprijeda i znajući da za linearne operatore konstantni faktor *komutira* s oznakom operatora (ovdje je formalno $cA = Ac$), izlazi

$$A(c x_0) = \lambda_0 (c x_0),$$

tj. i $c x_0$ je svojstven vektor.

2.11.1. Ilustracije gornjem teoremu. Jedinični operator i njegovi skalarni kratnici ostavljaju svaku pravulju invarijantnom kao cjelinu. Rotacija ravnine R_2 za $\pi/2$ oko 0 ne ostavlja na miru ni jedne pravulje; no R_2 je kompleksna pravulja C_1; tada je, naravno, C_1 invarijantna pravulja.

Neka je (S, R) prostor svih izvodljivih funkcija od zatvorena realnog odreska, npr. $[0, 1]$ prema R. Ako u tom prostoru Af znači: *svako* $f \in (S, R)$ *pomnožiti određenom funkcijom*, npr. funkcijom $t \to t$ ili $t \to \cos t$; onda u tom prostoru nema ni jednog svojstvenog vektora $\neq 0$, tj. nema izvodljive funkcije $f \neq 0$ za koju bi bilo $t f(t) = \lambda f(t)$ (λ konstanta) za svako $t \in S$.

Zato treba znati cijeniti sadržinu gornjeg teorema, koji osigurava bar jedan svojstven broj za svaku endomorfiju u konačno dimenzionalnim prostorima.

$\longrightarrow$ **2.12. T e o r e m.** ***Nejednakim svojstvenim vrijednostima, tj. nejednakim rješenjima karakteristične jednadžbe odgovaraju linearno nezavisni svojstveni vektori i linearno nezavisni invarijantni prostori.***

Provedimo dokaz indukcijom. U prethodnoj tački dokazali smo da za svako λ_0 pripada bar jedan vektor $x_0 \neq 0$; znači da on generira čitav jedan prostor. Pretpostavimo da smo dokazali da je za svakih m nejednakih svojstvenih vrijednosti svakog karakterističnog polinoma svakih m pripadnih svojstvenih vektora linearno nezavisno. Dokažimo sada da je stvar istinita i za broj $m+1$ nejednakih svojstvenih vrijednosti.

Pa neka je A neki operator sa bar $1+m$ svojstvenih vrijednosti $\lambda_0, \ldots, \lambda_m$; neka su $x_0, x_1, \ldots, x_m$ pripadni svojstveni vektori $\neq 0$. Metnimo ih na operacioni stol za linearnu nezavisnost: provjeriti zaključak

(6) $$\sum_{k=0}^{m} c_k x_k \equiv \vec{0} \Rightarrow c = c_1 = \cdots c_m = 0$$

za *svaki* niz tih skalarnih c-ova.

Djelujmo sada sprijeda operatorom A na (6); zbog homomorfnog (homogenolinearnog) karaktera, prelazi A i preko Σ i preko skalarâ c_k i smješta se ovako:

$$(7)\qquad \begin{array}{ccc} \sum_{k=0}^{m} c_k A x_k = A\vec{0} & & \text{(dalje: lijevo po definiciji} \\ \Downarrow \qquad\qquad \Downarrow & & \text{desno po} \\ \sum_{k=0}^{m} c_k \lambda_k x_k = \vec{0} & & A\vec{0} = A\,0\cdot\vec{0} = 0\; A\vec{0} = \vec{0}): \end{array}$$

Uklonimo iz $(6)_1$ i (7) recimo x_m; pomnožimo prvu jednadžbu u (6) sa λ_m i oduzmimo od (7):

$$(8)\qquad \sum_{k=0}^{m-1} c_k(\lambda_k - \lambda_m)\, x_k = \vec{0}.$$

No, (8) je linearan spoj od m svojstvenih vektora $x_0, x_1, \ldots, x_{m-1}$; po učinjenoj pretpostavci, oni su nezavisni; dakle iz (8) izlazi $c_k(\lambda_k - \lambda_m) = 0$ za $k < m$; specijalno, $c_0(\lambda_0 - \lambda_m) = 0 \Rightarrow$ (zbog $c_0 \neq 0$) $\Rightarrow \lambda_0 - \lambda_m = 0$, a to je protivno pretpostavci da su svi $\lambda_0, \ldots, \lambda_m$ nejednaki. Q. E. D.

$\longrightarrow$ **2.13.** Teorem. *Ako linearni operator djeluje u euklidskom ili hermitskom prostoru V i ima $\dim V = n < \infty$ nejednakih svojstvenih vrijednosti, tada je dijagonalizacija operatora provediva.*

Naime, tada imamo n svojstvenih parova (λ_i, e_i), $e_i \neq 0$, pa vektori e_i čine bazu po invarijantnim pravcima.

Iz teorema 2.12. proizlazi

$\longrightarrow$ **2.14.** Teorem. *Skup (A, K) svih vektora x za koje jednadžba $Ax = \lambda x$ ima bar jedno skalarno rješenje λ čini vektorski prostor; ako sa (A, λ) označimo skup svih x za koje gornja jednadžba vrijedi za fiksno λ, tada je*

$$(A, K) = \sum_{\lambda} (A, \lambda).$$

Pritom λ prolazi množinom σ_A svih nejednakih svojstvenih vrijednosti operatora A; ne gledajući na poredak sumacije, svaki element iz (A, K) jednoznačno je rastavljiv na sumu elemenata iz takvih $(A, \lambda) \neq \{0\}$. Drugim riječima, (A, K) je direktna suma prostorâ (A, λ), $(\lambda \in \sigma_A)$.

2.14.1. Primjedba. Na taj smo se način upoznali kako uspoređivanje operatora A s kratnikom jediničnog operatora $x \to x$ dovodi do zanimljivog cijepanja prostora (A, K) u ***maksimalne*** invarijantne potprostore od (A, K) prosto vezane za nejednake brojeve λ.

2.15. Što je s kratnim rješenjima karakteristične jednadžbe?

Teorem. Neka je a realna ili kompleksna kvadratna matrica formata (n, n) i $n < \infty$; ako je λ_0 nula-mjesto kratnosti m karakterističnog polinoma, tj.

$$a^{(\mu)}(\lambda_0) = 0,\ \mu = 0, 1, \ldots, m-1, \text{ te } a^{(m)}(\lambda_0) \neq 0,$$

tada skup svih rješenja x za $ax = \lambda_0 x$ čini prostor M dimenzije $\leq m$. Tu može stajati znak $<$ (pogl. 27, § 4.8).

D o k a z. Najprije sva ta rješenja x očigledno čine prostor: iz $x, y \in M$ izlazi $x+y \in M$ te $cx \in M$ za svaki broj c. Neka je $d = \dim M$. Izaberimo u prostoru M bazu od d vektora i proširimo je na bazu e cijelog prostora u kojem radi operator A; u toj bazi e matrični zapis operatora A ima oblik

$$\left[\begin{array}{ccc|c} \lambda_0 & & & \\ & \ddots & & \\ & & \lambda_0 & \\ \hline & 0 & & \end{array}\right];$$

to znači da karakteristični polinom glasi

$$\left[\begin{array}{ccc|c} \lambda-\lambda_0 & & & \\ & \ddots & & \\ & & \lambda-\lambda_0 & \\ \hline & 0 & & \end{array}\right],$$

tj. djeljiv je sa $(\lambda-\lambda_0)^d$, dakle je $d \leq m$, jer očigledno

$$a^{(k)}(\lambda_0) = 0 \quad \text{za svako } k < d. \qquad \text{Q. E. D.}$$

2.16. Ciklički invarijantni potprostori. 1. Najjednostavnije je stvoriti invarijantni prostor ovako: poći od nekog vektora e_0 i promatrati niz

(1) $$A^0 e_0 = e_0, \ A e_0 = e_1, \ A^2 e_0 = e_2 = A e_1, \ A^k e_0 = A e_{k-1} = e_k, \ldots$$

Neka je $A e_{k-1} (\equiv e_k)$ *prvi* član u tom nizu koji *linearno zavisi* od prethodnih; i neka je

(2) $$e_k = -c_0 e_0 - c_1 e_1 - \cdots - c_{k-1} e_{k-1} =$$
$$(-c_0 - c_1 A - c_2 A^2 - \cdots - c_{k-1} A^{k-1}) e_0;$$

na taj način dobivamo k *nezavisnih* vektora

(3) $$e_0, \ e_1 = A e_0, \ e_2 = A e_1, \ \ldots, \ e_{k-1} = A e_{k-2},$$

oni generiraju potpuno određen prostor; možemo ga označiti sa

(4) $$(e_0; A),$$

jer on zavisi od izvodnog člana e_0 i od operatora A. Neposredno se dokazuje da je (4) invarijantan prema A. No, zanimljiv je *zapis operatora A* u bazi koja proširuje bazu (1). Radi jednostavnosti pretpostavimo da se cijeli prostor V podudara s cikličkim prostorom (4).

2.16.2. Uzimajući tada zapise (3), tj. koeficijente, u stupce matrice, dobiva se ovaj zapis

$$(c) \qquad y_e = \begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & 1 & -c_{k-1} \end{bmatrix}$$

Oblik zapisa je zanimljiv. U posljednji stupac dolaze koeficijenti linearnog spoja (2) s koeficijentima koji formalno imaju znak — iz razloga što ćemo ga odmah navesti. Ostala mjesta su 0, a neposredno ispod dijagonale su 1.

2.16.3. Gornji je zapis zanimljiv iz dva razloga:

2.16.3.1. Prvi razlog. Prostor se može razbiti na određen niz cikličkih invarijantnih potprostora čija je on direktna suma.

2.16.3.2. Drugi razlog. Polinom

$$5(\lambda) \qquad c_0 + c_1\lambda + c_2\lambda^2 + \cdots + c_{k-1}\lambda^{k-1} + \lambda^k$$

je karakteristični polinom podoperatora A ograničenog na prostor $(e_0;\ A)$; izraz (5) je upravo *minimalni* polinom što pripada operatoru koji je definiran u $(e_0,\ A)$ i tu se podudara sa A.

2.16.4. Dokaz druge tvrdnje, u 2.16.3.2, je očigledan. Naime, u prvom redu vektor je $e_k = A^k e_0$, pa $5(\lambda) e_0$ za $\lambda = A$ daje

$$5(A) e_0 = (c_0 + c_1 A + c_2 A^2 + \cdots + c_{k-1} A^{k-1} + A^k) e_0 = 0 \cdot e_0 = \vec{0},$$

(prema (2)) = tj.

$$5(A) e_0 = 0.$$

Odatle, djelujući sprijeda sa A:

$$A\,5(A) e_0 = A\,0;$$

dakle

$$5(A) A e_0 = 0.$$

tj.

$$5(A) e_1 = 0, \text{ itd. } 5(A) e_2 = 5(A) e_3 = \cdots = 0.$$

Drugim riječima, operator $5(A)$ poništava se u bazi $e_0, e_1, \ldots,$ dakle je $5(\lambda)$ takav polinom da stavljanjem matrice ili operatora A umjesto λ dobivamo uvijek $\vec{0}$. Ujedno je stepen k i najniži s takvim svojstvom, jer je npr. e_{k-1} nezavisan od $e_0, e_1, \ldots, e_{k-2}$. Najzad, $5(\lambda)$ je normiran. Dakle je $5(\lambda)$ minimalan polinom (pogl. 22, § 2.2). To je ujedno i karakteristični polinom, jer smo vidjeli da stepen mora biti $\geq k$.

Time je druga tvrdnja dokazana.

2.16.5. Dokaz prve tvrdnje, u 3.1, je duži, pogotovu ako se radi o raznim pooštrenjima. Tako će npr. biti važno uočiti da postoji bar jedan vektor u prostoru čiji ciklički prostor ima svojstvo da minimalni polinom pripadnog podoperetora bude jednak minimalnom polinomu $\mu(\lambda, A)$ u čitavu prostoru.

2.17. *Matrica pratilica ili suputnica zadanog normiranog polinoma.*

Definicija. Polinomu $c_0 + c_1\lambda + \cdots + c_{k-1}\lambda^{k-1} + \lambda^k$ pripada kao njegova *pratilica* matrica oblika (c) od maloprije. Označit ćemo je sa y_c.

$\longrightarrow$ Teorem. *Podoperator A_x, kojem je oblast invarijantni prostor (x, A) sa bazom x, $A\vec{x}$, $A^2\vec{x}$, ... od prvih k nezavisnih članova toga niza, zapisuje se matrično pomoću suputnice polinoma* $5(\lambda)$.

3. SVOJSTVENE VRIJEDNOSTI KVADRATNIH I HERMITSKIH MATRICA REDA 2 NAD TIJELOM REALNIH ILI KOMPLEKSNIH BROJEVA

3.1. Po definiciji, kvadratnoj matrici $a = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ pripada karakteristična jednadžba

$$\det[\lambda - a] = 0, \text{ tj. } \begin{vmatrix} \lambda - a_{11} & -a_{12} \\ -a_{21} & \lambda - a_{22} \end{vmatrix} = 0$$

ili napisano u izračunatom obliku:

$$\lambda^2 - (a_{11} + a_{22})\lambda + (a_{11}a_{22} - a_{12}a_{21}) = 0. \tag{2}$$

Rješenje te jednadžbe glasi:

$$\lambda_{1,2} = \frac{a_{11} + a_{22}}{2} \pm \frac{1}{2}\left[(a_{11} - a_{22})^2 + 4\,a_{12}a_{21}\right]^{1/2}. \tag{3}$$

U općem slučaju, kad su komponente a_{ik} matrice a ma kakvi realni brojevi, brojevi λ_1 i λ_2 su kompleksni nestvarni, jer je jasno da diskriminanta

$$(a_{11} - a_{22})^2 + 4\,a_{12}a_{21} \tag{4}$$

kvadratne jednadžbe (2) može biti i ≥ 0 i ≤ 0.

2. Istaknimo dva izrazita slučaja:

3.2.1. Prvi slučaj. *Matrica a je simetrična*: $A = A^T$, tj. $a_{ik} = a_{ki}$, napose je $a_{11} = a_{21}$, pa diskriminanta (4) postaje

$$(a_{11} - a_{22})^2 + 4\,a_{12}^2,$$

dakle suma dvaju kvadrata, pa je ≥ 0. Tada su svojstvene vrijednosti realne.

3.2.2. Drugi slučaj. *Matrica A je kososimetrična*: $A = -A^T$, tj.

$$a_{ki} = -a_{ik}, \quad \text{napose} \quad a_{ii} = -a_{ii},$$

dakle

$$a_{ii} = 0, \ a_{21} = -a_{12};$$

tada korijeni λ_1, λ_2 prema (3) postaju

$$\lambda_{1,2} = \pm(-4\,a_{12}{}^2)^{1/2} = \pm 2\,a_{1,2}\; i,$$

tj. obje svojstvene vrijednosti su čisto imaginarne.

⟶ **3.4. Teorem.** ***Ako je kvadratna matrica realna i simetrična i reda 2, tada su njene svojstvene vrijednosti realne; ako je realna matrica kososimetrična i reda 2, njene su svojstvene vrijednosti čisto imaginarne.***

3.4. Korist koju imamo znajući svojstvene vrijednosti matrice (operatora) A pokazali smo u pogl. 26, § 12.10: uzeti koordinatnu bazu u smjeru tih različitih svojstvenih vrijednosti pa se matrica reducira na dijagonalnu.

3.5. Jedna od najljepših pravilnosti u teoriji realnih kvadratnih matrica sastoji se u tome da analogan teorem vrijedi bez obzira na format promatrane kvadratne matrice, odnosno da se analogno svojstvo može dokazati za opće simetrične operatore: spektar hermitskog operatora u Hilbertovu prostoru je zatvoren skup realnih brojeva (v. Smirnov V, p. 345).

3.6. Zanimljivo je i vrlo važno da gornji iskazi za matrice s kompleksnim vrijednostima vrijede kad se umjesto obične simetrije i antisimetrije promatra hermitska simetrija i antisimetrija, a ne vrijede u slučaju nerealnih matrica *a* uz pojam obične simetrije.

To ćemo dokazati u narednom paragrafu.

4. SPEKTAR SIMETRIČNIH I ANTISIMETRIČNIH REALNIH MATRICA. SPEKTAR HERMITSKIH I ANTIHERMITSKIH KOMPLEKSNIH MATRICA

⟶ **4.1. Osnovni teorem. (1)** ***Svaka svojstvena vrijednost svake hermitski simetrične konačne matrice a je realan broj: ako je $a = a^* = \overline{a^T}$, tada iz det$[\lambda - a] = 0$ proizlazi $\lambda \in R$ (≡skup realnih brojeva) (isp. § 8.6).***

(2) ***Ako je A hermitski antisimetrična i konačna matrica, tj. ako je $a = -a^*$, tada je spektar od A čisto imaginaran, tj. iz det$[\lambda - a] = 0$ izlazi da je broj λ čisto imaginaran: $\lambda \in i\,R$.***

(3) ***Svojstveni prostori što pripadaju nejednakim svojstvenim vrijednostima hermitske matrice (antihermitske matrice) međusobno su ortogonalni. Ako matrica ima n različitih svojstvenih vrijednosti, tada se iz svojstvenih vektora može izgraditi ortogonalna baza*** (isp. § 4.7).

4.2. Osnovni teorem o realnim simetričnim (antisimetričnim) matricama. *Spektar svake realne konačne simetrične (antisimetrične) matrice je realan (čisto imaginaran). Svojstveni prostori što pripadaju nejednakim svojstvenim vrijednostima matrice međusobno su okomiti; oni određuju ortonormiranu bazu, ukoliko su svojstvene vrijednosti sve jednostruke.*

Ch. Hermite [Ermit], (1822—1901) znameniti francuski matematičar

Kako je teorem 4.2. očigledno specijalan slučaj prvog teorema, dokažimo ovaj.

4.3. Pređimo sad na dokaz teorema 4.1.(1). Neka je λ svojstvena vrijednost matrice a i x jedan pripadni svojstven vektor:

$$a x = \lambda x, \quad x \neq \vec{0}.$$

Tad imamo:

$$x^{\star} (a x) = x^{\star} (\lambda x) = \lambda x^{\star} x, \quad \text{tj.}$$

$$x^{\star} (a x) = \lambda x^{\star} x.$$

No, $x^{\star} x \neq 0$, pa iz te jednakosti izlazi

$$\lambda = x^{\star} (a x)/x^{\star} x.$$

Prema pogl. 25, § 6.4.1, tu je realan i brojnik i nazivnik; dakle je $\lambda \in R$.

4.4. Promatrajmo sada antihermitsku matricu a; no tada je produkt $i a$ hermitska matrica; stvarno iz $a^{\star} = -a$, tj. iz

$$\alpha_{rs} + i \alpha'_{rs} = -(\alpha_{sr} - i \alpha'_{sr})$$

izlazi, množeći sa i:

$$i \alpha_{rs} - \alpha'_{rs} = -i \alpha_{sr} - \alpha'_{sr},$$

tj. $(i a)^{\star} = i a$.

S druge strane, neka je λ svojstvena vrijednost od a; onda je $a x = \lambda x$ također $(i a) x = (i \lambda) x$. Prema teoremu (1) broj $i\lambda$ mora kao svojstvena vrijednost hermitske matrice $i a$ biti realan, tj. $i \lambda \in R$, dakle $\lambda \in i R$. Time je i drugi dio teorema dokazan.

4.5. Dokažimo još i treći dio teorema 4.1. Pa neka su λ, μ dvije *nejednake* svojstvene vrijednosti; dakle,

(1) $$a x = \lambda x \text{ za bar jedno } x \neq 0$$

$$a y = \mu y \text{ za bar jedno } y \neq 0.$$

Treba dokazati da je $x \perp y$, tj. $x^{\star} y = 0$. Pomnožimo (1) sprijeda sa y, odnosno x; izlazi:

(2) $$y^{\star} a x = y^{\star} \lambda x,$$

$$x^{\star} a y = x^{\star} \mu y.$$

Odatle zvjezdovanjem: $(x^\star a y)^\star = (\mu x^\star y)^\star \Rightarrow$ (po 25 § 6.3.10 i zbog $a^\star = a$, $\mu^\star = \mu$):

$$y^\star a x = \mu y^\star x.$$

Oduzmemo li ovu jednakost od (2), izlazi:

$$0 = (\lambda - \mu) y^\star x.$$

Odatle, dijeleći sa $\lambda - \mu \neq 0$, proizlazi tražena relacija $y^\star x = 0$.

4.6. Još se radi o onom dodatku o bazi. Ako matrica ima $n = \mathrm{st}\, a$ različitih svojstvenih vrijednosti, onda je dovoljno na svakoj invarijantnoj pravulji odabrati jedinični vektor pa će se dobiti ortonormirana baza.

Time je osnovni teorem dokazan u potpunosti.

4.7. Gornji teorem 4.1. zbilja je dragocjen. Međutim, teorem još nije potpun u tom smislu što i ne dira u *bitno pitanje da li matrica i onda kad su joj svojstvene vrijednosti višestruke dopušta n invarijantnih linearno nezavisnih pravulja.* — Koliko je stvar važna, vidi se iz ovih primjera.

4.8. Promatrajmo matricu

$$J = \begin{bmatrix} 5 & 1 & 0 \\ & 5 & 1 \\ & & 5 \end{bmatrix};$$

njen karakteristični polinom je

$$\det(\lambda - J) = \begin{vmatrix} \lambda - 5 & -1 & 0 \\ & \lambda - 5 & -1 \\ & & \lambda - 5 \end{vmatrix} = (\lambda - 5)^3.$$

Znači da je broj 5 trostruka i jedina svojstvena vrijednost matrice. Nađimo svojstvene vektore kao rješenja od $(5 - J)\vec{x} = \vec{0}$:

$$\begin{bmatrix} 0 & -1 & 0 \\ & 0 & -1 \\ & & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \vec{0}.$$

Izlazi

$$0 \cdot x_1 - 1 \cdot x_2 + 0 \cdot x_3 = 0$$

$$0 \cdot x_1 + 0 \cdot x_2 - \quad x_3 = 0 \qquad \text{Odatle: } x_1 \text{ proizvoljno}$$

$$0 \cdot x_1 + 0 \cdot x_2 + 0 \cdot x_3 = 0 \qquad x_2 = 0 = x_3.$$

Prema tome, *svi svojstveni vektori* su oblika $\begin{bmatrix} x_1 \\ 0 \\ 0 \end{bmatrix}$ i daju tek *jednu* invarijantnu pravulju. Primijetimo da je minimalni polinom matrice J jednak

$$(\lambda - 5)^3, \quad \text{tj.} \quad \mu(\lambda, J) = \varkappa(\lambda, J).$$

4.9. Jordanove klijetke. Isto vrijedi za matrice

$$J(\lambda_0, n) = \begin{bmatrix} \lambda_0 & 1 & & & \\ & \lambda_0 & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_0 & 1 \\ & & & & \lambda_0 \end{bmatrix}$$

za svaki skalar λ_0. Te se matrice zovu *Jordanove klijetke*[1].

Dom $J(\lambda_0, n) = n \times n$; posebno ćemo stavljati $H(n) = J(0, n)$.

Isti zaključak vrijedi i za matrice J^T (*donje Jordanove klijetke*) =

$$= \begin{bmatrix} \lambda_0 & & 0 \\ 1 & \ddots & \\ & \ddots & \lambda_0 \\ 0 & & 1 \end{bmatrix};$$

te matrice nastaju iz kvadratne skalarne matrice tako da svako polje neposredno ispod dijagonale popunimo sa 1. Tu je broj λ_0 jedina svojstvena vrijednost, kratnosti n; no pripadni prostor svih svojstvenih vektora zajedno sa $\vec{0}$ daje tek jednu jedinu pravulju!

4.10. Primijetimo da svaka konačna kvadratna kompleksna matrica ima bar jedan invarijantan smjer, jer karakteristični polinom ima bar jedno kompleksno ništište. Naprotiv, beskonačna matrica može biti bez ikojeg invarijantnog smjera.

4.11. Iz svega toga izlazi da ćemo znati procijeniti vrijednost saznanja da svaka hermitska matrica ima ne samo realan spektar nego i da matrica dopušta n invarijantnih pravulja, na kojima možemo usaditi ortonormiranu bazu. To će čak vrijediti za sve tzv. *normalne matrice* tj. za rješenja jednadžbe

$$a\,a^{\star} = a^{\star}\,a. \qquad \text{(isp. § 9.1).}$$

Idemo to dokazati!

Ali prethodno nekoliko zanimljivih općih pravilnosti!

5. SVOJSTVEN POLINOM, SVOJSTVENE VRIJEDNOSTI I SVOJSTVENI VEKTORI JEDNOSTAVNIH MATRIČNIH FUNKCIJA

5.0. Priprava. Znamo od kolike je važnosti karakteristični polinom

$$a(\lambda), \text{ odnosno } \varkappa(a, \lambda) = \det[\lambda - a]$$

zadane kvadratne matrice a. Njegova nula-mjesta sačinjavaju tzv. spektar Sa matrice a; pri tom se svako nula-mjesto računa sa svojom kratnosti; ne uzimamo li u obzir kratnosti, dobije se spektar σa *bez ponavljanja*.

---

[1]) C. Jordan [Žordan] (1838—1922), francuski matematičar.

Kako su svojstvene vrijednosti i svojstveni vektori zadane matrice od osnovne vrijednosti, upoznat ćemo se sa *stanovitim povezanostima među tim veličinama za razne matrice.*

5.1. Lema. *Ako je*

(1) $$a x = \lambda x,$$

gdje je a proizvoljna kvadratna matrica, λ skalar, x vektor, tada je

(2) $$(c a) x = (c \lambda) x$$

(3) $$a^k x = \lambda^k x$$

(4) $$(c a^k + d a^l) x = (c \lambda^k + d \lambda^l) x$$

za proizvoljne skalare c, d i brojeve k, l.

Dokaz. (2) izlazi iz (1) množenjem sa c; pomnoži li se pak (1) sa a slijeva, dobije se $a^2 x = (a\lambda) x = (\lambda a) x = \lambda (a x) =$ (s obzirom na (1)) $= \lambda^2 a$. Analogno: ako (3) vrijedi za k, onda, množeći sa a proizlazi da vrijedi i za $k+1$, tj. (3) vrijedi za svaki prirodni broj k. No, iz $a^k x = \lambda^k x$ izlazi množenjem sa a^{-k}:

$$x = \lambda^k a^{-k} x, \quad \text{tj.} \quad \lambda^{-k} x = a^{-k} x,$$

što znači da (3) vrijedi za svaki cijeli broj uz uslov da je $\det a \neq 0$.

Jednakost (4) proizlazi iz analognih dviju jednakosti oblika (3).

Lema 5.1. može se izreći i kao

5.2. Lema. *Svaki svojstveni vektor matrice a također je svojstven i za matrice: $a a$, $c a^k$, gdje je c proizvoljan skalar, a k proizvoljan prirodni broj.* Simbolički: *ako je $\lambda \in S a$, onda je $c\lambda \in S(c a)$, $\lambda^k \in S(a^k)$.*

Na isti način dokazuje se ovo:

Ako je $p(a)$ bilo koji matrični polinom, sa skalarnim koeficijentima, tada su svojstveni vektori od a također svojstveni vektori od $p(a)$.

I ispravna kratnost je dobivena; imamo ovaj:

$\longrightarrow$ **5.3. Teorem o transformaciji spektra.** ***Pridružimo li kvadratnoj konačnoj matrici a reda n polinomnu matricu $p a$, tada se transformacijom***

$$\lambda \to p \lambda$$

preslikava spektar matrice a na spektar matrice $p a$ i to bilo da se radi o spektru S s ponavljanjem ili o spektru σ bez ponavljanja; simbolički:

$$a \to p a \;\Rightarrow\; S a \to S(p a) = p S a = \{p\lambda, \ \lambda \in S a\}$$

$$\sigma a \to \sigma p a \;\; = p \sigma a = \{p\lambda, \ \lambda \in \sigma a\}.$$

Drugim riječima, ako za polinom $p x$ i matricu a vrijedi

(5) $$p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_{s-1} x^{s-1} + p_s x^s = p_s \prod_{i=1}^{s} (x - x_i), \quad p_s \neq 0$$

(6) $$\det(\lambda - a) = \prod_{\nu=1}^{n} (\lambda - \lambda_\nu),$$

tada vrijedi

(7) $$\det(\lambda - p\,a) = \prod_{\nu=1}^{n} (\lambda - p\,\lambda_\nu)$$

(isp. također pogl. 24, § 2.4.5).

D o k a z. Najprije, uvrštavajući u identitet (5) $x \to \lambda_\nu$, a u identitet (6) $\lambda \to x_i$, izlazi

(8) $$p(\lambda_\nu) = p_s \prod_i (\lambda_\nu - x_i)$$

(9) $$\det(x_i - a) = \prod_\nu (x_i - \lambda_\nu).$$

Nadalje, supstitucija $x \to a$ u (5) daje

$$p\,a = p_s \prod_i (a - x_i),$$

dakle, prelazeći na determinante

$$\det p\,a = \det(p_s) \prod_i (\det(a - x_i) = (\text{prema } (9)) = p_s{}^n \prod_i (-1) \prod_\nu (x_i - \lambda_\nu) =$$

$$= \prod_\nu \prod_i p_s (\lambda_\nu - x_i) = (\text{prema } (8)) = \prod_\nu p(\lambda_\nu).$$

Dakle je

$$\det p\,a = \prod_\nu p(\lambda_\nu)$$

za svaki polinom p; specijalno, supstitucija $p \to \lambda - p\,a$ daje traženu formulu (7).

6. RASTAVLJANJE VEKTORSKOG PROSTORA U DIREKTNU SUMU POTPROSTORA. ORTOGONALNI KOMPLEMENT ZADANOG POTPROSTORA U UNITARNIM PROSTORIMA

Promotrimo proizvoljni vektorski prostor $V_n(K) = V$. Neka je $e = (e_{n'})$ jedna njegova *baza*. Tada to znači da je

(1) $$V = K\,e_1 + \cdots + K\,e_n,$$

pa čak i

($\dot{1}$) $$V = K\,e_1 \dot{+} K\,e_2 \dot{+} \cdots,$$

pri čemu (1) znači skup svih suma oblika $\sum_{n'} k_{n'} e_{n'}$, $k_{n'} \in K$; K znači neko algebarsko tijelo.

Kraće se kaže da je V direktna suma[1] svojih n potprostora $K\,e_{n'}$ jer osim (1) vrijedi i uslov ($\dot{1}$): *$K\,e_{n'}$ u sumi preostalih sumanada u* (1) *nema ništa osim* $\vec{0}$.

[1]) Važan primjer direktne sume upoznali smo u teoremu 13, § 4.7.2 te u teoriji grupa pogl. 17, § 14.5.

—→ 6.1. Teorem (isp. pogl. 13, § 4.7.2). *Ako je U potprostor, a e baza prostora $V_n(K)=V$ sa $\dim U$ članova u U, tada postoji jedan jedini minimalni potprostor U' sa svojstvom da je $U+U'=V$ i da baza od U' bude dio baze e. Svaki vektor može se na jedan jedini način predstaviti kao suma jednog vektora iz U i jednog vektora iz U'.*

Pogledajmo rastav 6. (1) i njegove sumande; svaki od tih sumanada ili je u potprostoru U ili, izuzev $\vec{0}$, izvan njega. Broj sumanada iz 6. (1) koji su u U iznosi upravo $m=\dim U$; znači da je broj preostalih sumanada $=n-m$; preostali sumandi u 6. (1) rađaju potpuno određen potprostor U', dimenzije $n-m$ i, naravno, $U+U'=V$. Uži potprostor od U' ne zadovoljava traženje, jer bi inače dimenzija prostora V bila $<m+\dim U'=n$—nemogućnost.

Iz jednoznačnosti rastava vektora v po bazi e izlazi i jednoznačna komponenta njegova v_U u U kao i komponenta v_U' u U'.

Iz dokaza se vidi da vrijedi

—→ 6.2. Teorem. *Ako je $e=(e_{n'})$ bilo koja baza prostora V, pa ako taj skup e razdijelimo bilo kako na disjunktne dijelove $X, Y, \ldots$, tada su time određeni potprostori $X_0, Y_0, \ldots$ što ih razapinju: X, odnosno $Y, \ldots$, a direktna suma tih potprostora je polazni prostor V.*

6.3. Slučaj hermitskih i euklidskih prostora. Ortogonalni komplement.

—→ Teorem. *Ako je V euklidski (ili hermitski) prostor, a U njegov potprostor, tada je jednoznačno određen prostor U' za koji je $U+U'=V$ i $U\perp U'$; piše se $U\oplus U'=V$ i kaže da je U' ortogonalni komplement potprostora U u odnosu na prostor V. Specijalno, $V\oplus\{0\}=V$.*[1]

Dokaz. Neka je e proizvoljna *ortonormirana* baza prostora V koja nastaje proširenjem neke baze e^0 od U; tada je time određen onaj dio $e'=e\setminus e^0$ izvan U (naime, ako je $U=V$, tada je e' prazno, jer nema nikojeg vektora izvan V, odnosno vektor $\vec{0}$ je jedini $\perp U=V$).

Po definiciji ortonormiranosti imamo $v^0\perp v^1$ za svako $v^0\in e^0$ i svako $v^1\in e^1$; no $v^1\perp U$; stvarno, ako je vektor v okomit na dva ili više vektora, $x_1, x_2, \ldots$, okomit je on i na prostoru što ga razapinju ti vektori, tj. na svakoj linearnoj kombinaciji $c_1x_1+c_2x_2+\cdots$ tih vektora. Naime:

$$(c_1x_1+c_2x_2+\cdots)\circ v=(\text{distributivnost skalarnog množenja vektora})=$$
$$=(c_1x_1)\circ v+(c_2x_2)\circ v+\cdots=(\text{izlučivanje skalara iz zagrade!})=$$
$$=c_1(x_1\circ v)+c_2(x_2\circ v)+\cdots=c_1\cdot 0+c_2\cdot 0+\cdots=0,$$

tj. v je okomit na prostoru što ga određuju promatrani vektori. Na taj je način, specijalno, svaki vektor baze e' okomit na čitavu prostoru U, jer podbaza e^0

[1]) Također se piše $U'=V\ominus U$.

razapinje U. Iz istog je razloga podbaza e^0 okomita na čitavu prostoru U' što ga određuje podbaza e'.

Još preostaje da se vidi da je $U \perp U'$ (naravno, $U \oplus U' = V$). No, za svako $u \in U$ i svako $u' \in U'$ postoje jednoznačni rastavi

$$u = \sum_x c_x x \, (x \in e^0) \quad \text{te} \quad u' = \sum_y c_y' y, \, (y \in e').$$

Tražeći njihov produkt $u \circ u'$ i znajući da je skalarno množenje distributivno prema zbrajanju, izlazi da je $u \circ u'$ suma izrazâ $(c_x c'_{x'})(x \circ x')$, što je $=0$, jer je $x \circ x' = 0$; naime, $x \in e^0$, $x' \in e'$ i $e^0 \perp e'$.

Time je ujedno dokazana i jednoznačna određenost potprostora U'; naime, za neku drugu ortonormiranu bazu f prostora V kojoj $f^0 = f \cap U$ razapinje U imali bismo analogno rastav baze f na f^0 i $f^1 = f \setminus f^0$; vektori iz e^1 generiraju U^1, a oni koji su iz f^1 neka generiraju U_1; tvrdimo da je $U^1 = U_1$. Najprije, $U^1 \subset U_1$: tj. $u^1 \in U^1 \Rightarrow u^1 \in U_1$. Naime, $u^1 \in V$, pa u bazi f imamo jednoznačan rastav $u^1 = \sum_x u_x^1 x \, (x \in f)$; no komponente od u^1 [po vektorima iz f^0 su $=0$, jer je $u^1 \perp U$; dakle je $u^1 = \sum_x u^1_x x$, $(x \in f^1)$, tj. $u^1 \in U_1$. Analogno se zaključuje da je, dualno, $U^1 \supset U_1$. Time je traženi teorem dokazan.

6.4. Ortogonalna projekcija vektora v na prostor U je onaj vektor v_u iz U koji zajedno s jednim vektorom iz ortogonalnog komplementa $V \ominus U$ daje v. Prelaz od $v \to v_U$ je tipičan linearni operator (naziva se i *projektor* P, tj. $Pv = v_U$). Naravno, $PP = P$; takvi hermitski operatori nazivaju se i *projektorima*.

6.5. Opće (koso) projiciranje. Neka je V bilo kakav vektorski prostor (može biti i bez metrike); neka je U jedan potprostor, a U' jedan njegov direktni komplement (npr. proširimo li bazu e^0 od U do baze e od V, onda $e \setminus e^0$ proizvodi U'). Neka je $x \in V$; tada znamo da je x jednoznačno rastavljivo po U, U'; onaj dio rastava koji je u U zove se *projekcija vektora x na potprostor U u smjeru U'* (odnosno u smjeru vektorâ baze e koji su izvan U, ukoliko $e \cap U$ generira U); može se označiti sa $P_{U'} x$.

Naravno, i taj prelaz od x na $P_{U'} x$ je homomorfija (linearni operator). Primijetili ste da projekcija zavisi ne samo od U nego i od „smjera" projiciranja što ga određuju vektori $v \setminus U$, odnosno potprostor U'.

$\longrightarrow$ **6.6. Osnovni teorem o spregnutim (konjugiranim) operatorima.** ***Ako je potprostor X nekog unitarnog prostora V invarijantan prema operatoru A, tada je njegov ortogonalni komplement $Y = V \ominus X$ invarijantan prema spregnutom ili konjugiranom operatoru $A^\star$. Posebno, ako je A unitarno, tada je i Y invarijantno prema A.***

Dokaz. Neka je, $x \in X$, $y \in Y$; tvrdimo da je $A^\star y \in Y$. No, $Ax \in X$, jer je X invarijantno prema A; dakle je $Ax \perp y$, tj. $0 = Ax \ominus y$ (po definiciji

$$A^\star :) = x \ominus A^\star y, \text{ tj. } x \ominus A^\star y = 0 \text{ za svako } x \in X;$$

to znači da je $A^\star y \in Y$, za čim smo i išli.

7. KOMUTATIVNI OPERATORI I NJIHOVI SVOJSTVENI VEKTORI

⟶ **7.1. Teorem.** *Ako su operatori A, B komutativni:*

$$AB = BA \tag{1}$$

te djeluju u kompleksnom prostoru $V_n(K)$ s konačno mnogo dimenzija, imaju oni bar jedan svojstven vektor zajednički.

7.2. Primjedba. Analogan teorem vrijedi i za svaki (konačni ili beskonačni) skup F komutativnih operatora u kompleksnom prostoru s konačnim brojem dimenzija jer u F nema beskonačno mnogo linearno nezavisnih operatora.

Naime, ako je $F_1, F_2, \ldots, F_f$ maksimalni broj linearno nezavisnih operatora u F (prema pretpostavci f je prirodan broj), pa ako bar jedan od njih npr. F_1 ima neku svojstvenu vrijednost λ, tada u pripadnom svojstvenom prostoru $P(F_1, \lambda)$ ima operator F_2 neki svojstveni vektor y_1; radeći sada sa y_1 i F_i $(i=1, 2)$ te sa $B=F_3$ daje prethodno razmatranje neki svojstveni zajednički vektor od F_1, F_2, F_3. Induktivno, stvar teče dalje pa se dolazi do nekog svojstvenog zajedničkog vektora y_f za operatore $F_1, \ldots, F_f$ a time i za sve njihove linearne kombinacije; to znači da je y_f svojstven vektor svakog člana od F.

7.3. Dokaz teorema 7.1. Neka je x neki svojstven vektor operatora A; dakle je

$$Ax = \lambda x, \quad x \neq \vec{0}. \tag{2}$$

Dakle je x svojstven vektor od A vezan za λ. (Ako je slučajno $Bx=0$, onda je x zajednički svojstven vektor).

$$B(Ax) = B(\lambda x)$$

$$(BA)x = (B\lambda)x \quad \text{zbog (1)}$$

$$(AB)x = \lambda Bx, \quad \text{tj.}$$

$$A(Bx) = \lambda(Bx), \quad x \neq \vec{0}. \tag{3}$$

Drugim riječima, za zadane operatore A, B relacija (2) ima za posljedicu relaciju (3). Iz istog razloga, množeći (3) sprijeda sa B, dolazimo najzad do relacije $A(B^2x) = \lambda(B^2x)$, pa odatle na $A(B^3 n) = \lambda(B^3 x)$, itd.

Induktivno zaključujući, relacija (2) uz pretpostavku (1) ima za posljedicu

$$A(B^m x) = \lambda(B^m x) \tag{4}$$

za svaki prirodni broj m.

No, u (4) se pojavljuje beskonačan niz vektorâ $B^k x$. Kako radimo u prostoru od n dimenzija, $n < \infty$, znači to da vektori (4) ne mogu biti nezavisni linearno. Pa neka je $m+1$ prvi prirodni broj, tako da vektor $B^{m+1}x$ bude linearna kombinacija vektorâ

$$B^k x \text{ za } k = 1, 2, \ldots, m \tag{5}$$

Neka je P prostor što ga razapinju ti vektori (5). Prostor P je invarijantan i prema matrici (operatoru) B, tj. $BP \subset P$. Naime, ako je $z \in P$, onda su određeni skalari $z_1, \ldots, z_m$ sa svojstvom

$$z = z_1 B x + z_2 B^2 x + \cdots + z_m B^m x.$$

Odatle

$$B z = z_1 B^2 x + z_2 B^3 x + \cdots + z_m B^{m+1} x; \tag{6}$$

no $B^{m+1} x$ je izrazivo linearno pomoću članova niza (5); to znači da zbog (6) to isto vrijedi i za $B z$, dakle je $B z \in P$. A to znači da je P invarijantan prostor u odnosu na operator B. To specijalno znači da prostor P sadržava jedan svojstven vektor y matrice B.

No, iz relacije (4) vidimo da je *svaki* član iz P ujedno svojstven vektor za matricu A. Dakle je i y svojstven za A, tj. vektor y je zajednički svojstven vektor od A i B. Q. E. D.

7.4. U općem slučaju operatori su nekomutativni. Komutativnost je znatno sužavanje slobode. Tako npr. već komutativnost tako bliskih operatora kao što su operatori A, A^* karakterizira vrlo važan i pravilan razred operatora — *normalne operatore*, odnosno *operatore »proste strukture«*.

7.5. *Ako je S skalarni operator, onda on komutira sa svakim operatorom.*

Lako se vidi da vrijedi i obratno: ako je: $S A = A S$ za *svaki* linearni operator S, onda je A konstantan skalar (raditi matrično!).

8. EKSPLICITAN (OTVOREN) OBLIK KARAKTERISTIČNOG POLINOMA

—→ **8.1. Teorem.**

$$\begin{vmatrix} \lambda - a_{11} & -a_{12} & -a_{1n} \\ \cdot & \cdots & \cdot \\ -a_{n1} & -a_{n2} & \lambda - a_{nn} \end{vmatrix} = (-1)^n \det a + A_{n-1} \lambda + A_{n-2} \lambda^2 + \cdots + A_{n-1} \lambda^{n-1} + \lambda^n,$$

pri čemu A_k za svako $k \leq n$ označuje sumu svih determinanata glavnih podmatrica reda k matrice a (*glavna podmatrica* je svaka koja je smještena u istoimenim recima i stupcima). Posebno, konstantan član je $(-1)^n \det a$; koeficijent od λ^{n-1} je suma članova na dijagonali matrice $-a$. To je tzv. trag $\mathrm{Tr}(-a)$ matrice $-n$.

Npr. za $n = 3$ koeficijent od λ glasi $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix}$ (na dijagonali dolaze samo dijagonalni članovi matrice a; zato je glavne minore pogodno ispisivati naznačujući najprije njihovu dijagonalu, a onda umetati ostale indekse).

—→ **8.1.1. Teorem o vrijednosti determinante.** $\det a = \lambda_1 \lambda_2 \ldots \lambda_n$, *tj. determinanta svake kvadratne matrice jednaka je produktu njenih svojstvenih vrijednosti, svaka uzeta s odgovarajućom kratnosti.*

Naime, u svakom algebarskom polinomu jedne varijable produkt članova njegova spektra i broja $(-1)^n$ jednak je konstantnom članu polinoma; u našem slučaju taj konstantni član je $\det -a = (-1)^n \det a$. Dakle

$$(-1)^n \Pi \lambda_i = (-1)^n \det a, \quad \text{dakle} \quad \Pi \lambda_i = \det a.$$

Dokaz teoreme 8.1. je pregledniji ako dokažemo ovaj teorem, koji je simetričniji:

8.2. Teorem o determinanti sume dviju matrica. *Ako su a, b dvije kvadratne matrice reda n, tada je*

$$\det [a+b] = \det [a_1 + b_1,\ a_2 + b_2,\ \ldots] = \Sigma \det [c_1,\ c_2,\ \ldots];$$

pri tom je $c_i \in \{a_i,\ b_i\}$ za svako *i; sumacija se proteže na sve matrice koje se mogu izgraditi uzimajući joj za svaki stupac odgovarajući stupac od a ili od b; izbor se vrši na svih* 2^n *načina.*

Dokaz teorema je direktna posljedica aditivnog svojstva determinanata. Tako npr. $\det (a+b) = \det [a_1,\ a_2 + b_2,\ \ldots] + \det [b_1,\ a_2 + b_2,\ \ldots]$. Analogan rastav stupca drugog doveo bi do nove dvije matrice, itd.

8.3. Leverrier-ove formule (1840).[1] Ako je

$\det (\lambda - a) = \lambda^n + A_1 \lambda^{n-1} + A_2 \lambda^{n-2} + \cdots + A_n$, $t_k = Tr_k\, a = \mathrm{Tr}\, a^k$, tada je

$$A_1 = -t_1,$$

$$A_2 = -\frac{1}{2}(A_1 t_1 + t_2)$$

$$A_3 = -\frac{1}{3}(A_2 t_1 + A_1 t_2 + t_2)$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$A_n = -\frac{1}{n}(A_{n-1} t_1 + A_{n-2} t_2 + \cdots + A_1 t_{n-1} + t_n).$$

Pri tom trag matrice X simbolički $\mathrm{Tr}\, X$, znači sumu članova na dijagonali. Dokaz formula nećemo izvoditi (isp. M. Bôcher, Introduction to Higher Algebra, New-York 1939, str. 243).

Njihova interesantnost proizlazi iz jednostavne građe veličina koje dolaze u formulama. Svaki koeficijent A_k je, prema tome, kombiniran od tragova potencija matrice a. Općenito: svaka polinomalna invarijanta od a je oblika

$$\Sigma\, \alpha_{k_1 \ldots k_p} \mathrm{Tr}\, a^{k_1} \mathrm{Tr}\, a^{k_2} \ldots \mathrm{Tr}\, a^{k_p}.$$

[1] U. J. J. Leverrier [Leverje] (1811—1877), francuski astronom koji je računom predskazao planet Neptun: istog dana 23. 9. 1846. kad je on svoje rezultate objavio, našao je teleskopom njemački astronom Galle na predskazanom mjestu novi planet nazvan Neptun.

⟶ **8.4. Teorem.** ***Transponirane matrice a, a^T imaju isti karakteristični polinom i iste svojstvene vrijednosti; međutim, svojstveni vektori ne moraju biti zajednički. Za svake dvije $\neq$ svojstvene vrijednosti pripadni prostori matrice a i matrice a^T međusobno su okomiti. (Riječ je o realnom a.)***

Najprije, prema teoremu 8.1 o građi koeficijenata u karakterističnim polinomima i znajući da svaka glavna podmatrica u a prelazi u odgovarajuću podmatricu u a^T, i da se pri tom determinanta ne mijenja, jasno je da $\varkappa(\lambda, a)$ i $\varkappa(a^T, \lambda)$ imaju iste odgovarajuće koeficijente i da su, dakle, ta dva polinoma identična. Time oni imaju iste svojstvene vrijednosti.

Dokažimo ono o ortogonalnosti.

No, iz

$$\begin{array}{r|l} a\,x_i = \lambda_i\,x_i & \cdot y_k \\ a^T\,y_k = \lambda_k y_k & x_i \end{array} \;-$$

izlazi:

$$y_k^T(a\,x_i) - x_i^T(a^T y_k) = y_k^T(\lambda_i\,x_i) - x_i^T(\lambda_k y_k)$$

$$y_k^T(a\,x_i) - (a\,x_i)^T y_k = \lambda_i\,x_i^T y_k - \lambda_k\,x_i^T y_k$$

$$0 = (\lambda_i - \lambda_k)\,x_i^T y_k, \quad \text{tj. zbog } \lambda_i \neq \lambda_k$$

$$x_i \perp y_k.$$

Time smo dokazali kako su stvarno matrice a, a^T međusobno povezane.

⟶ **8.5. Teorem.** ***Hermitski pridružene matrice a, $a^\star$ imaju spregnute (konjugirane) karakteristične polinome i spregnute svojstvene vrijednosti. Ako a, $a^\star$ imaju zajednički svojstven vektor, tada su pripadne svojstvene vrijednosti konjugirani kompleksni brojevi. Svojstveni vektori matrice a koji pripadaju svojstvenoj vrijednosti λ okomiti su na svojstvenim vektorima matrice a koji pripadaju svojstvenoj vrijednosti $\mu \neq \bar{\lambda}$.***

$$\begin{array}{ll} (1) & a\,x = \lambda\,x \\ (2) & a^\star\,x = \mu\,x \end{array} \left\{ x \neq 0 \right\} \Rightarrow \lambda = \bar{\mu}.$$

D o k a z. Početak teorema 8.5 dokazuje se slično kao početak teorema 8.4. Dokažimo (1), (2). Znamo da je identički

$$x^\star(a\,y) = \overline{y^\star(a^\star\,x)}$$

(pogl. 25, § 6.4.2); stavimo $y = x$:

$$x^\star(a\,x) = \overline{x^\star(a^\star\,x)};$$

zbog $(1)_1$:

$$x^\star(\lambda\,x) = \overline{(x^\star\,a^\star)}\,x = \overline{x^\star(a^\star\,x)} =$$

$=$ zbog $(2)_1 =$

$$= \overline{x^\star(\mu\,x)} = \overline{\mu\,x^\star\,x} = \bar{\mu}\,\overline{x^\star\,x} = \bar{\mu}\,x^\star\,x \qquad \text{(jer je } x^\star\,x \text{ realno).}$$

Dakle je $\lambda\,x^\star\,x = \bar{\mu}\,x^\star\,x$, odakle $\lambda = \bar{\mu}$.

Dokaz posljednje rečenice u teoremu provodi se slično kao i odgovarajući dokaz u prethodnom teoremu 8.4.

8.6. Navesti matricu kojoj je zadan karakteristični polinom. Matrica-pratilica ili suputnica zadanog normiranog polinoma (isp. § 2.17).

Teorem. Zadan je polinom

(1) $$p\,x = p_0 + p_1 x + \cdots + p_{n-1} x^{n-1} + x^n;$$

sagradimo pripadnu „matricu-pratilicu" ili suputnicu

(D) $$J_p = \begin{bmatrix} 0 & 0 & 0 & -p_0 \\ 1 & 0 & 0 & -p_1 \\ 0 & 1 & . & . \\ . & 0 & . & . \\ . & . & . & . \\ . & . & 1 & -p_{n-1} \end{bmatrix}.$$

(prva poddijagonala je konstanta 1).

Neka je A linearni operator kojem je u zadanoj bazi $e = e_1, \ldots, e_n$ matrični zapis upravo ta napisana matrica. Tada je polazni polinom (1) minimalni polinom operatora A, odnosno: p je normirani oblik karakterističnog polinoma operatora A.

Iz zapisa (D) očitavamo (kako?) da je $A e_1 = e_2$, tj. operator A prevodi prvi vektor e_1 baze u poziciju drugog vektora baze: isto tako, $A e_2 = e_3, \ldots,$

$$A e_{n-2} = e_{n-1}, \quad A e_{n-1} = e_n, \quad A e_n = \begin{bmatrix} -p_0 \\ -p_1 \\ . \\ . \\ -p_{n-1} \end{bmatrix}.$$

Drugim riječima, zapis (D) pokazuje da imamo stvarno posla s bazom vektorâ

$$e_1, \; A e_1 = e_2, \; (A e_2 =)\, A^2 e_1, \; (A e_3 =)\, A^3 e_1, \ldots, A^{n-1} e_1 = e_n,$$

za koju je

$$A^n e_1 = (-p_0 - p_1 A - p_2 A^2 - \cdots - p_{n-1} A^{n-1})\, e_1 \qquad (*)$$

Specijalno, posljednju jednakost možemo pisati i u ovom obliku:

(2) $$(p\,A)\, e_1 = \vec{0}.$$

Prema tome, za svaki vektor v imamo rastav u toj bazi:

(3) $$v = v_1 e_1 + v_2 A e_1 + v_3 A^2 e_1 + \cdots + v_n A^{n-1} e_1 =$$
$$= (v_1 + v_2 A + v_3 A^2 + \cdots + v_n A^{n-1})\, e_1 = f A\, e_1,$$

stavljajući

(4) $$f A = v_1 + v_2 A + v_3 A^2 + \cdots + v_n A^{n-1};$$

naravno, $\mathrm{st} f \leq n-1$.

No, pokažimo da relacija (3) ima za posljedicu $p\,A = 0$. Pokažimo, naime, da u (2) može umjesto e_1 stajati v.

Naime,

$$p\,A\,v = (\text{prema } (3)) = p\,A\,(f\,A\,e_1) = (p\,A\,f\,A)\,e_1 = (\text{matrični polinomi}$$
$$\text{istog } A \text{ komutiraju}) = f\,A\,(p\,A\,e_1) = \text{prema } (2) = f\,A\,0 = 0.$$

Drugim riječima, za svaki vektor v vrijedi $(p\,A)\,v = 0$; odatle nužno izlazi $p\,A = 0$. Dokažimo da je p upravo minimalni polinom operatora (matrice) A; stvarno, ako je $\mathrm{st} f \leq n-1$, tada je prema (3) svakako $f\,A\,e_1 = v \neq 0$. Dakle je $f\,A \neq 0$ i minimalni polinom od A je stupnja $> n-1$; a kako $p\,A = 0$, znači da je p minimalni polinom: stupanj mu je n, normiran je, a zadovoljava ga A.

Time je ujedno dokazano da je $p\,(A)$ karakteristični polinom operatora A, tj.

(5)
$$\det(\lambda - J) = \begin{bmatrix} \lambda & & & p_0 \\ -1 & \ddots & & \\ \vdots & \ddots & \ddots & \\ 0 & & -1 & \lambda + p_{n-1} \end{bmatrix} = p_0 + p_1\,\lambda + p_2\,\lambda^2 + \cdots + p_{n-1}\,\lambda^{n-1} + \lambda^n.$$

Relacija (5) može se provjeriti i direktno ovako (pokažimo na primjeru). Promatrajmo primjer matrice

$$J = \begin{bmatrix} 0 & 0 & -2 \\ 1 & 0 & -4 \\ 0 & 1 & -3 \end{bmatrix}, \qquad \lambda - J = \begin{bmatrix} \lambda & 0 & 2 \\ -1 & \lambda & 4 \\ 0 & -1 & \lambda + 3 \end{bmatrix};$$

dakle je

$$\det(\lambda - J) = \begin{vmatrix} \lambda & 0 & 2 \\ -1 & \lambda & 4 \\ 0 & -1 & \lambda + 3 \end{vmatrix} =$$

$=$ (posljednji redak množi sa λ i dodaj retku iznad njega) $=$

$$= \begin{vmatrix} \lambda & 0 & 2 \\ -1 & 0 & 4 + \lambda\,(\lambda + 3) \\ 0 & -1 & \lambda + 3 \end{vmatrix} =$$

$=$ (čini isto s retkom *drugim odozdo*) $=$

$$= \begin{vmatrix} 0 & 0 & p\,(\lambda) \\ -1 & 0 & 4 + \lambda^2 + 3\,\lambda \\ 0 & -1 & \lambda + 3 \end{vmatrix} = (\text{razvij po prvom retku}) =$$

$$= p\,(\lambda) \cdot (-1)^{3+1} \cdot (-1)^2 = p\,(\lambda) = \lambda^3 + 3\,\lambda^2 + 4\,\lambda + 2.$$

Dakle obrazac (5) stoji za naš primjer. U općem slučaju je postupak isti.

9. NORMALNI OPERATORI

Definicija. Operator (matrica A) je normalan, ako je $AA^\star = A^\star A$.

—→ **9.1. Osnovni teorem.** ***Ako je kvadratna matrica a normalna i reda $n < \infty$ i s kompleksnim vrijednostima, tada postoji ortonormirana baza $e = (e_1, e_2, \ldots, e_\nu, \ldots, e_n)$ od n svojstvenih vektora matrice a; ako su λ_ν svojstveni brojevi za koje je $a e_\nu = \lambda_\nu e_\nu$, tada je***

$$e^{-1}\, a\, e = \begin{bmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{bmatrix}.$$

U općem slučaju, $\lambda_1, \lambda_2, \ldots$ su kompleksni i nisu realni brojevi.

Dokaz. Kako su matrice $A^\star$, A komutativne, imaju one zajednički bar jedan karakterističan vektor $x_1 \neq 0$ (pogl. 27, § 7.1); time je određen potprostor $C x_1$ — pravulja —; taj je potprostor invarijantan prema a (prema $a^\star$); dakle (pogl. 27, § 6.6), ortogonalni komplement X_2 od $C x_1$ invarijantan je prema $a^\star$ (prema a), tj. X_2 je invarijantno i prema a i prema $a^\star$. Naravno, $\dim X_2 < \dim V$. Nalazeći se sada u prostoru X_2, možemo opet primijeniti činjenicu da su a, $a^\star$ komutativni i u prostoru X_2, pa u njemu imaju (§ 7.1) jedan zajednički svojstven vektor x_2; time se rađa potprostor $C x_2$, invarijantan i prema a i prema $a^\star$; i potprostor

(1) $$C x_1 + C x_2$$

je invarijantan prema a, $a^\star$, dakle i njegov ortogonalni komplement X_3, itd. Stvar teče dalje dok se ne dobije ortogonalna baza $x_1, \ldots, x_\nu, \ldots, x_n$ (svaki put x_{k+1} biramo među vektorima $\perp x_{k'}$) $(k' = 1, 2, \ldots, k)$. Uzimajući

$e_k = x_k \, | x_k |^{-1}$, dobije se potpuna ortogonalna baza $e = e_1, e_2, \ldots, e_n$.

Dokažimo da vrijedi obrat teorema 9.1:

9.2. Teorem. *Ako linearni operator A dopušta bazu ortonormiranih svojstvenih vektora, tada je on normalan.*

9.2.1. Pa neka je e jedna ortonormirana baza prostora C_n sastavljena od vektora s invarijantnih pravulja. Zapis A_e operatora A u toj bazi je dijagonalan (pogl. 27, § 2.2.2)

(1) $$A_e = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix},$$

gdje su λ_ν brojevi za koje je $A e_i = \lambda_i \cdot e_i$.

Očigledno, A_e je normalan operator:

(2) $$A_e A_e^\star = A_e^\star A_e.$$

No (pogl. 26, § 8.4), vrijedi

$$A_e = e^{-1} A e, \quad \text{dakle} \quad A = e A_e e^{-1}, \quad A^\star = (e^{-1})^\star A_e^\star e^\star.$$

Izvedimo iz (2) da je i A normalan operator, tj. da je $A A^\star = A^\star A$. No, vektori matrice e su ortonormirani; to znači da je

(3) $$e e^\star = 1,$$

dakle:

(4) $$e^\star = e^{-1}, \quad (e^{-1})^\star = e.$$

Iz obrazaca (2)—(4) proizlazi i normalnost operatora A. Naime:

$$A A^\star = (e A_e e^{-1}) (e A_e e^{-1})^\star = (e A_e e^{-1}) (e^{-1})^\star A_e^\star e^\star) \text{ (prema (4))} =$$
$$= e A_e (e^{-1} e) A_e^\star e^\star = e (A_e A_e^\star) e^\star = \text{(prema (2))} = e A_e^\star A_e e^\star =$$
$$= (e^{-1})^\star A_e^\star \underbrace{e^\star e}_{1} A_e e^{-1} = (e A_e e^{-1})^\star (e A_e e^{-1}) = A^\star A.$$

9.2.2. Direktno možemo teorem 9.2. i ovako dokazati. Prema pretpostavci vrijedi

$$A x_i = \lambda_i x_i, \quad x_i \ominus x_k = \delta_{ik} \text{ za } i, k = 1, \ldots, n.$$

Stavimo

$$y_j = A^\star x_j - \bar{\lambda}_j x_j.$$

Tada je

$$x_i \ominus y_j = x_i \ominus (A^\star x_j) - x \ominus (\bar{\lambda}_j x_j) = A x_i \ominus x_j - \lambda_j x_i \ominus x_j =$$
$$= \lambda_i x_i \ominus x_j - \lambda_j (x_i \ominus x_j) = (\lambda_i - \lambda_j)(x_i \ominus x_j) = 0, \quad \text{tj.}$$

(5) $$A^\star x_j = \bar{\lambda}_j x_j.$$

Prema tome, A, $A^\star$ imaju iste svojstvene vektore koji obrazuju bazu.

Odatle:

(6) $$A A^\star x_j = A \bar{\lambda}_j x_j = \bar{\lambda}_j (A x_j) = \bar{\lambda}_j \lambda_j x_j.$$

$$A^\star A x_j = A^\star \lambda_j x_j = \lambda_j A^\star x_j = \text{(prema (5) ima } A^\star \text{ iste svojstvene}$$
$$\text{vektore kao } A\text{; zato prema teoremu 8.5)} = \lambda_j \bar{\lambda}_j x_j, \quad \text{tj.}$$

$$A^\star A x_j = \lambda_j \bar{\lambda}_j x_j.$$

Iz (5) i (6) izlazi:

$$A^\star A x_\nu = A A^\star x_\nu \text{ za bazu } x = (x_1, \ldots, x_n);$$

prema teoremu o određenosti linearnih operatora (pogl. 24, § 4.2) znači to da je $A A^\star = A^\star A$. Q. E. D.

⟶ **9.3. Teorem (0).** ***Dimenzija svakog maksimalnog invarijantnog potprostora $(A; \lambda_k)$, što odgovara svojstvenoj vrijednosti λ_k normalnog operatora A, upravo je jednaka kratnosti n_k broja λ_k kao rješenja karakteristične jednadžbe $A(\lambda) = 0$, odnosno jednadžbe*** $\det(\lambda - A) = 0$, **tj.**

(00) *Defekt* $d(\lambda_k - A) = n_k$.

Dokaz. Defekt matrice $A - \lambda_k$ jednak je dimenziji d_k prostora što ga čine rješenja x za koja je $(A - \lambda_k)x = 0$ (isp. pogl. 13, § 8.3); no prema pogl. 27, § 2.15.

(1) $$d_k \leq n_k,$$

gdje n_k označuje kratnost svojstvene vrijednosti $\lambda_k \in \sigma_A$; to vrijedi za svako λ_ν iz spektra σ_A; kako je k tome $\Sigma n_k = n = \Sigma d_k$, znači to da je $n_k = d_k$ za svako $\lambda_k \in \sigma_A$.

Dakle je

$$n_k = \text{rang}(\lambda_k - A).$$

Spajajući prethodne rezultate, možemo u matričnom obliku izreći ovaj teorem (prevod na jezik linearnih operatora je očigledan).

⟶ **9.4. Glavni teorem o strukturi normalnih matrica.** ***Neka je a kvadratna matrica reda $n < \infty$ s vrijednostima u tijelu C kompleksnih brojeva; neka je***

$$\det[\lambda - A] = (\lambda - \lambda_1)(\lambda - \lambda_2) \cdots (\lambda - \lambda_n);$$

tada su ova dva svojstva međusobno ekvivalentna:

(1) ***$a a^\star = a^\star a$ (matrica a je normalna).***

(2) ***Postoji n ortonormiranih vektora $\vec{u^1}, \vec{u^2}, \ldots, \vec{u^n}$ koji zadovoljavaju jednadžbu $a x = \lambda x$; vrijedi***

$$u^{-1} a u = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix},$$

stupci matrice $u = [u^1, u^2, \ldots, u^n]$ ispunjeni su komponentama rješenja $\vec{u^1}, \ldots, \vec{u^n}$.

(3) ***Ako vrijedi (1) ili (2), tada kratnost ili frekvencija svakog λ_k jednaka je defektu matrice $\lambda_k - a$.***

Dokaz. (1) ⇒ (3) (§ 9.1); (3) ⇒ (1) (§ 9.2); (2) ⇒ (3) (§ 9.3).

9.4.1. Primjer koji pokazuje da (3) ne daje (1) ni (2).

Neka je $a = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$; tada je

$$\det(\lambda - a) = \begin{vmatrix} \lambda - 1 & -1 \\ 0 & \lambda - 2 \end{vmatrix} = (\lambda - 1)(\lambda - 2), \quad \text{tj.} \quad \lambda_1 = 1, \ \lambda_2 = 2$$

i defekt od $[\lambda_i - a]$ je 1; prema tome, matrica a zadovoljava uslovu (3).

Međutim, uslov (1) nije zadovoljen, jer je $a^\star = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$, $a a^\star = \begin{bmatrix} 2 & 2 \\ 2 & 4 \end{bmatrix}$, $a a^\star = \begin{bmatrix} 1 & 1 \\ 1 & 5 \end{bmatrix}$, dakle je $a a^\star \neq a^\star a$.

9.5. Defekt linearnog operatora. Primjetimo da se defekt matrice prenosi i na operator što ga ona predstavlja. Međutim, mnogo je bolje *defekt operatora direktno* ***definirati*** *kao dimenziju onog potprostora što ga sastavljaju rešenja x jednadžbe*

$$Ax=0 \quad \text{(isp. 13, § 8 i 25, § 4.3).}$$

10. GLAVNI TEOREM O UNUTRAŠNJOJ STRUKTURI HERMITSKIH MATRICA I HERMITSKIH OPERATORA

$\longrightarrow$ **10.1.** ***Neka je C_n n-dimenzionalni unitarni ili hermitski prostor; neka za linearni operator A: $C_n \to C_n$ bude***

$$\det(\lambda-A)=(\lambda-\lambda_1)(\lambda-\lambda_2)\cdots(\lambda-\lambda_n);$$

tada su ova dva svojstva (1), (2) međusobno ekvivalentna:

(1) ***$A^\star=A$ (operator je hermitski simetričan).***

(2) ***Operator A se može zapisati kao dijagonalna realna matrica u bar jednoj ortogonalnoj bazi.***

(3) ***Vrijedi li (1) ili (2), tada svojstvene vrijednosti operatora su realne, a kratnost je svake svojstvene vrijednosti λ_k jednaka defektu pripadnog operatora λ_k-A.***

Dokaz teorema sadržan je u dokazima odgovarajućih zaključaka za normalne matrice u prethodnom paragrafu; specijalno, u pogledu zaključka (3)$\Rightarrow$(1), v. § 9.4.1.

Na matričnom jeziku gornji teorem se iskazuje ovako.

$\longrightarrow$ **10.2. Teorem.** ***Za kompleksnu kvadratnu matricu a reda $n<\infty$ ova dva svojstva su međusobno ravnopravna:***

(1) ***Matrica je hermitska ($a=a^\star$).***

(2) ***Matrica je unitarno-slična s dijagonalnom realnom matricom, tj. postoji bar jedna unitarna matrica u za koju je $u^{-1}au$ dijagonalna realna matrica.***

(3) ***Vrijedi li (1) ili (2), tada svojstvene vrijednosti λ_k matrice sve su realne, a kratnost im je jednaka defektu matrice λ_k-a.***

10.3. Teoremi o antihermitskim matricama ($a^\star=-a$) dobiju se iz gornjih teorema zamjenjujući svuda riječ »*realan*« s »*čisto imaginaran*«.

11. UNUTRAŠNJA STRUKTURA SIMETRIČNIH I ANTISIMETRIČNIH LINEARNIH OPERATORA U EUKLIDSKIM PROSTORIMA

11.1. Teorem. Iskaz kao u § 10.1, samo što umjesto C treba pisati R (tijelo realnih brojeva); umjesto (1) treba čitati:

$$A=A^T \qquad \text{(operator je simetričan),}$$

Sasvim jednako iskazujemo ovdje i teoreme 9.2, 9.3 za simetrične matrice, odnosno za antisimetrične matrice i operatore.

12. UNITARNE MATRICE — UNITARNI OPERATORI

12.1. Kao korolar gornjeg osnovnog teorema 9.4. o normalnim matricama navedimo analogan teorem za tzv. unitarne matrice i operatore. Definiraju se kao oni za koje je (prostor konačno dimenzionalan!)

$$UU^{\star} = 1 = U^{*}U. \tag{1}$$

Sreli smo se s njima i u dokazu teorema 9.2 relacije (3), (4).

Očigledno, relacija (1) je ekvivalentna sa svakom od ovih relacija:

$$U^{\star} = U^{-1} \tag{2}$$

$$(U^{-1})^{\star} = U. \tag{3}$$

Duboko značenje imaju unitarne matrice jer im stupci predstavljaju ortonormiranu bazu (to je smisao definicije (1) u slučaju matrica), odnosno što hermitsko množenje vektorâ ostavljaju invarijantnim i čine grupu.

Naime, ako su x, y vektori, tada za vektore Ux, Uy imamo:

$$Ux \ominus Uy = (Uy)^{\star} \cdot Ux = y^{\star} U^{\star} Ux = y^{\star} x = x \ominus y.$$

I obratno, ako je neka transformacija U takva da je identički (prema vektorima)

$$(Uy)^{\star} \cdot Ux = y^{\star} \cdot x,$$

tada je

$$U^{\star} U = 1, \quad \text{tj.} \quad U \text{ je unitaran operator.}$$

—→ **12.2. Osnovni teorem o unitarnim operatorima i matricama.** ***Za linearni operator U u konačno-dimenzionalnom prostoru ova tri svojstva su ekvivalentna:***

(I) *Operator je unitaran, tj.* $UU^{\star} = \mathbf{1}$.

(II) *Sve su svojstvene vrijednosti unimodularne. tj. po modulu* $= \mathbf{1}$ *i kratnost svake je jednaka defektu odgovarajuće karakteristične matrice.*

(III) *Postoji niz* ***realnih*** *brojeva* $\mu_1, \mu_2, \ldots, \mu_n$ *i ortonormirana baza U sa svojstvom da zapis operatora A u toj bazi glasi:*

$$\begin{bmatrix} e^{i\mu_1} & & & \\ & e^{i\mu_2} & & \\ & & \ddots & \\ & & & e^{i\mu_n} \end{bmatrix} = \mathit{diag}\,[e^{i\mu_1}, e^{i\mu_2}, \ldots, e^{i\mu_n}]. \tag{$\star$}$$

12.3. Analogan teorem za matrice glasi slično; samo što iskaz (III) dobiva oblik da je $U^{-1}AU =$ napisana matrica ($\star$).

Dokažimo teorem 12.2. Čitav teorem je sličan onom o normalnim i hermitskim matricama. Samo se sada još radi o dodatku da je spektar operatora položen na jediničnoj kružnici. To treba dokazati.

(I) $\Rightarrow$ (II).

Treba dokazati da je $|\lambda_k|=1$. No, ako je

(4) $$U x_k = \lambda_k x_k,$$

tada je

(5) $$U^\star x_k = \bar{\lambda}_k x_k \quad (27, \S\ 8.5).$$

Iz (4) predmnoženje sa U^{-1} daje $x_k = \lambda_k U^{-1} x_k$, a ovo zbog

$$U U^\star = 1 \text{ postaje } x_k = \lambda_k U^\star x_k \Rightarrow \lambda_k^{-1} x_k = U^\star x_k;$$

ovo zajedno sa (5) daje

$$\lambda_k^{-1} x_k = \bar{\lambda}_k x_k; \quad (\text{jer je } x_k \neq 0) \Rightarrow \lambda_k \bar{\lambda}_k = 1,$$

tj.

(6) $$|\lambda_k| = 1.$$

Obrnuto, pokažimo da II $\Rightarrow$ (I). To stvarno znači da treba pokazati da iz (4), (5), (6) izlazi $U U^\star = 1$. No, iz (5) predmnoženje sa U daje

$$U U^\star x_k = \bar{\lambda}_k U x_k \quad (\text{zbog (4)}):$$

$$U U^\star x_k = \bar{\lambda}_k \lambda_k x_k; \quad (\text{zbog (6)}):$$

$$U U^\star x_k = x_k.$$

No, prema pretpostavci, x_k prolazi jednom bazom prostora. To znači da se identični operator 1 i operator $U U^\star$ podudaraju na jednoj bazi; oni su jednaki; a to baš i daje traženu jednakost.

12.4. Korolar. *Svaka svojstvena* ***realna*** *vrijednost unitarne matrice je oblika* 1 *ili* -1. *Specijalno, svaka svojstvena* ***realna*** *vrijednost* ***ortogonalnih*** *matrica je oblika* 1 *ili* -1.

12.5. *Još o spektru unitarne matrice.*

Evo još jednog dokaza da je *spektar svake unitarne* (*dakle i ortogonalne*) *matrice u položen na jediničnoj kružnici.*

U prvom redu, vrijednosti u_{ik} unitarne matrice u pripadaju jediničnom krugu, tj.

$$u_{ik} \bar{u}_{ik} = |u_{ik}|^2 \leq 1. \quad \text{To je jasno, jer je} \quad |u_{ik}| \leq u_i \bar{u}_i = 1.$$

U drugu ruku, neka je λ_0 svojstvena vrijednost za u. Tada je λ_0^m svojstvena vrijednost za u^m za svako cjelobrojno m. (isp. 27, § 5.1).

Odatle izlazi da postoji jedna majorizacija karakterističnog polinoma $\varkappa(\lambda; u)$ za svaku unitarnu matricu zadanog stupnja n i da ta majorizacija zavisi jedino od stupnja n, a ne od matrice u. K tome su prvi i posljednji koeficijent u $\varkappa(\lambda, u)$, po apsolutnoj vrijednosti jednaki broju 1. To znači da postoji broj M tako da za svako $\lambda_0 \in S u$ bude $|\lambda_0| < M$. U drugu ruku, mora biti također

(1) $$|\lambda_0^m| < M$$

za svako cjelobrojno m, jer iz $\lambda_0 \in S u$ izlazi $\lambda_0^m \in S(u^m)$ (pogl. 27. § 5.3), a u^m je također unitarna matrica.

No, relacija (1) je moguća jedino ako je $|\lambda_0|=1$, jer ako je npr.

$$|\lambda_0|>1, \text{ tada } |\lambda_0|^m \to \infty \text{ kad } m\to\infty, \text{ a ako je } |\lambda_0|<1,$$

$$\text{tada } |\lambda_0|^{-m} \to \infty \text{ kad } m\to\infty.$$

13. MEĐUVEZE UNITARNIH, HERMITSKIH I NORMALNIH OPERATORA

Neka U, H, N budu u ovom paragrafu oznake za unitarne, hermitske i normalne operatore A.

13.1. Znamo (pogl. 27, § 9.1) da N ima u ortonormiranoj bazi bar jedan matrični dijagonalni zapis:

$$N=\begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$

Stavimo li $\lambda_k=|\lambda_k|\,e^{i\alpha_k}$, tada je

$$N=\operatorname{diag}[|\lambda_k|]\cdot\operatorname{diag}[e^{i\alpha_k}]=H_d\,U=U\,H_d,$$

gdje je

$$H_d=\begin{bmatrix} |\lambda_1| & & \\ & \ddots & \\ & & |\lambda_n| \end{bmatrix},$$

$$U=\begin{bmatrix} e^{i\alpha_1} & & & \\ & e^{i\alpha_2} & & \\ & & \ddots & \\ & & & e^{i\alpha_n} \end{bmatrix}=e^{iH}; \quad H=\begin{bmatrix} \alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_n \end{bmatrix}.$$

Drugim riječima, svako N je oblika $H_d\,U=U\,H_d$, odnosno

(1) $$N=H_d\,e^{iH}=e^{iH}\,H_d;$$

pri tom su H, H_d dva hermitska operatora te

(2) $$U=e^{iH}.$$

13.1.1. Oblici (1) i (2) predstavljaju velika poopćenja onog što se dešava s kompleksnim brojevima kad svaki kompleksni broj u modula 1 pišemo u obliku

(3) $$u=e^{i\alpha},$$

a svaki kompleksni broj z pišemo kao produkt od $|z|$ i pripadnog jediničnog dijela $e^{i\arg z}$:

$$z=|z|\,e^{i\arg z}.$$

13.2. *U narednom paragrafu dokazat ćemo da se svaki linearni operator A može prikazati u obliku $A=HU$ i u obliku $U_1 H_1$. Operator je normalan onda i samo onda ako je također $UH=A$, tj. ako je $HU=A=UH$* (Gantmaher[1]) [1] str. 225 teorem 8).

13.3. S druge strane, umjesto transcendentne veze (3) među realnim brojevima α i kompleksnim brojevima λ možemo poći od veze

$$z=\frac{1+ix}{1-ix}, \text{ odnosno } x=i\frac{1-z}{1+z},$$

kojom se brojevna pravulja preslikava na jediničnu kompleksnu kružnicu bez $z=-1$. Postavlja se pitanje da li se među operatorima može naći slična veza — naime između operatora H (oni svi imaju realne spektre!) te između operatora U (jer svi oni imaju spektre na jediničnoj kružnici brojeva).

13.4. Cayley [Kejli] je pokazao da je to moguće i dokazao je veze

$$U=(1+iH)\ (1-iH)^{-1}$$
$$H=i(1-U)\ (1+U)^{-1};$$

pri tom je H proizvoljan hermitski operator, a U proizvoljan unitaran operator kojem broj -1 nije svojstvena vrijednost.

13.4.1. Analogna razmatranja vrijede i prilikom razmatranja opće razlomljene linearne funkcije koja pravulju preslikava na jediničnu kružnicu. (Isp. M. H. Stone [1].)

14. OPĆI OPERATOR KAO PRODUKT HERMITSKOG I UNITARNOG OPERATORA

→ **14.1. Teorem (Gantmaher-Krejn).** ***Za svaki linearni operator A u unitarnom prostoru postoji bar jedan pozitivan hermitski operator H_0 i jedan unitarni operator U sa svojstvom $A=H_0 U$. Analogno za rastav $A=U' H_0'$ (indeks 0 podsjeća da su svojstvene vrijednosti od H_0 sve ≥ 0).***

Ako je A regularno, rastavi su jednoznačni.

14.2. Teorem. Svaki linearni operator A u euklidskom prostoru moguće je napisati u obliku $A=S_0\omega=\omega' S_0'$, gdje su S_0, S_0' simetrični operatori ≥ 0; ω, ω' su ortogonalni operatori. Ako je A regularan operator, ti su rastavi jednoznačni.

Dovoljno je dokazati prvi teorem, jer je drugi specijalan slučaj prvoga.

Dokaz teorema 14.1. Neka je A proizvoljan operator; tada su

$A^* A$ i $A A^*$ hermitski operatori; npr. $(A^* A)^* = A^* A^{**} = A^* A$.

[1]) F. R. Gantmaher (1908—1964), ruski matematičar.

To znači da svaki od tih operatora dozvoljava dijagonalan realan zapis u svojstvenoj bazi. No, svojstvene vrijednosti operatorâ $A^\star A$, $A A^\star$ su ≥ 0, jer se one javljaju kao koeficijenti u skalarnom produktu

$$(A x)^\star \cdot (A x) = x^\star (A^\star A x).$$

Inače, $A^\star A$, $A A^\star$ imaju iste svojstvene polinome i isti spektar.

Prema tome, postoji posve određena matrica koja se iz dijagonalnog zapisa operatora $A A^\star$ dobije zamjenjujući svaki član $\check{c}$ na dijagonali s njegovim aritmetičkim antikvadratom $+\check{c}^{1/2}$. Neka je H operator s tako dobivenim zapisom.

Naravno, $$H^2 = A A^\star.$$

14.3. Ako je A regularan operator, tada u dijagonalnom zapisu nema na dijagonali nijedne 0; znači da je i H^{-1} regularan operator (dijagonalni zapis mu je supstitucija $\check{c} \to \check{c}^{-1}$ za svaki član na dijagonali).

Time je određen operator $H^{-1} A$. Isprobajmo ga s obzirom na unitarnost.

$$(H^{-1} A)(H^{-1} A)^\star = H^{-1} A (A^\star H^{-1\star}) = H^{-1} A A^\star H^{-1}$$

(jer je H^{-1} realan dijagonalan operator) $= H^{-1} H^2 H^{-1} = 1$.

Time smo dobili unitarni operator $U = H^{-1} A$, pa imamo željen rastav

(1) $$A = H U.$$

14.4. Preostaje slučaj kad je A singularan operator: $\det A = 0$.

Promatrajmo sad hermitski operator $A^\star A$ (umjesto $A A^\star$ od maloprije) i njegov aritmetički antikvadrat $H_1 = +(A^\star A)^{1/2}$; neka je dijagonala u zapisu za H_1, ispunjena sa λ_i; na taj način imamo svojstvene parove (λ_i, x_i), za koje je

(2) $$H_1 x_i = \lambda_i x_i,$$

x_i ortonormirani. Odatle;

$$H_1 H_1 x_i = \lambda_i H_1 x_i = \lambda_i^2 x_i \quad \text{tj.} \quad A^\star A x_i = \lambda_i^2 x_i.$$

Iz te jednadžbe, množeći sa x_k, izlazi:

$$A^\star A x_i \ominus x_k = \lambda_i^2 x_i \ominus x_k$$

$$A x_i \ominus A x_k = \lambda_i^2 \delta_i^k.$$

Drugim riječima, ortonormiranu bazu svojstvenih vektorâ x_i operatora $+(A^\star A)^{1/2}$ prevodi operator A u ortogonalan skup vektora, $A x_{n'}$ (ne moraju biti ortonormirani, niti čak nezavisni). Očigledno, tim vektorima $A x_i$ možemo pridružiti ortonormiranu n-članu bazu e vektora $\lambda_i e_i$ (na beskonačno mnogo načina u općem slučaju), tako da vrijedi:

(4) $$A x_i = \lambda_i e_i,$$

Uoči, da $A x_i = 0$ povlači $\lambda_i = 0$, pa i za takve λ_i vrijedi (4).

Time imamo dvije ortonormirane baze vektorâ: bazu vektorâ x_i i bazu e. Sada su potpuno određeni operatori H i U sa svojstvima

(5) $$H e_i = \lambda_i e_i, \quad U x_i = e_i.$$

Prvi je hermitski i ≥ 0, a drugi kao posrednik između dviju unitarnih baza, i sam je unitaran.

No, evo i zaključka:

$A x_i =$ (isp. (4)) $= \lambda_i e_i =$ (po (5)) $= H e_i =$ (po (5)) $= H(U x_i) = H U x_i$, tj.

(6) $$A x_i = H U x_i.$$

Operatori A, HU podudaraju se na jednoj bazi, dakle su isti: relacija (1) je dokazana i za slučaj $\det A = 0$. Pišući H_0 za H, dobije se prvi rastav, o kojem se govori u teoremu.

14.5. Iz relacije (1) proizlazi

$$A^\star = U^\star H^\star, \quad \text{tj. pišući} \quad A^\star = B:$$

(1) $$B = U^{-1} H.$$

To znači da svaki rastav operatora na produkt hermitskog i unitarnog daje ujedno i rastav konjugiranog operatora na rastav od unitarnog i hermitskog.

No, kad A prolazi svim operatorima, prolazi i $A^\star = B$ svim operatorima. Na taj je način zaista dokazano da je i relacija $A = U' H_0'$ moguća.

14.6. Pitanje jednoznačnosti. Iz teorema 14.1. imamo:

$$A \cdot A^\star = H_0 \cdot U U^\star \cdot H_0 = H_0^2.$$

To znači da „koeficijent“ H_0 u § 14.1. ima svoje značenje:

H_0 *u* § 14.1. *je antikvadrat od* $A A^\star$, *pa je on, kao pozitivan operator, određen jednoznačno.* Time je jednoznačno određeno i U ako je $\det A \neq 0$; tada je, naime, i H_0 regularno, pa je $U = H_0^{-1} A$. u općem slučaju

$$H_0' \neq H_0, \quad U' \neq U.$$

I u slučaju $H_0' = H_0$ može biti i $U' \neq U$.

Ako je A singularno, tada U, U' nisu određeni jednoznačno.

14.7. Analogija s realnim i s kompleksnim brojevima. Za slučaj prostora realnih, odnosno kompleksnih brojeva $\neq 0$, rastavi u teoremu 14.1. su jednoznačni: H_0 i H_0' predstavljaju apsolutnu vrijednost broja A; U predstavlja signum, tj. unimodularni broj $A/|A|$ (veličinu rotacije oko 0 broja 1 do broja $A/|A|$). Ako je A broj 0, tada U nije određeno.

14.8. Kao što kompleksni broj $A \neq 0$ određuje linearni operator $z \to Az$ u prostoru kompleksnih brojeva, koji — geometrijski govoreći — znači rotaciju za $\arg A$ i onda dilataciju za $|A|$, tako je analogna stvar s operatorom A u euklidskim prostorima. *Operator* $x \to Ax$ *sastoji se od rotacije* $x \to \omega x$ i onda od rastezanja $\omega x \to S \omega x$ (to je rastezanje linearno u smjeru ortonormirane svojstvene baze. Sličnu sliku imamo u unitarnim prostorima).

14.9. Polarni oblik gornjih veza. Spektar unitarnog operatora leži na jediničnoj kružnici; to znači da je u svojoj svojstvenoj bazi zapis od U oblika

$$\begin{bmatrix} e^{i\alpha_1} & & & \\ & e^{i\alpha_2} & & \\ & & \ddots & \\ & & & e^{i\alpha_n} \end{bmatrix} \text{—simbolički } U=e^{iH},$$

gdje je H neki hermitski operator. Gornji rastav $A=H_0 U$ prema tome, daje:

$$A=H_0\, e^{iH},$$

pri čemu je H hermitski, a H_0 k tome i ≥ 0. To je *polarni prikaz operatora A*. Slično za euklidske operatore:

$$A=w\, S_0\, e^S, \quad w^2=1$$

gdje je S_0 simetrični operator, sa svojstvenim vrijednostima ≥ 0, a S antisimetrični operator (antisimetrična matrica).

Za slučaj kompleksnih brojeva analogni „polarni" prikaz glasi:

$$z=|z|\, e^{i \operatorname{Arg} z};$$

$\operatorname{Arg} z$ je veličina kuta $\sphericalangle 1\, 0\, z$ mjerena u radijanima; broj $\operatorname{Arg} z$ nije određen jednoznačno; svi ti brojevi čine razred brojeva kojima je razlika djeljiva sa 2π; vrijednost $\operatorname{Arg} z$ iz $[0, 2\pi)$ označujemo sa $\arg z$.

15. FAKTORIZACIJA MINIMALNOG POLINOMA $\mu(\lambda; a)$ MATRICE a I INVARIJANTNI SVOJSTVENI POTPROSTORI MATRICE a

15.1. Minimalni polinom $\mu(\lambda; a)$. U pogl. 24, § 2.4.7. došli smo do određenog normalnog djelitelja $\mu(\lambda; a)$ karakterističnog polinoma $\varkappa(\lambda, a)$, koji poništava matrica a, tj. $\mu(a)=0$. Time, naravno, imamo $(\mu a)\, x=0$ za svaki vektor x, jer je μa nula-matrica, simbolički $\mu a=\boxed{0}$, da se stvar bolje istakne.

15.2. Slučaj kad je polinom μ produkt dvaju relativno prostih polinoma. Pretpostavimo sada da je polinom $\mu(\lambda)$ produkt dvaju relativno prostih polinoma f, g:

(1) $$\mu(\lambda)=f(\lambda)\, g(\lambda),\ f(\lambda)\, \mathrm{M}\, g(\lambda)=1.$$

Tada po Euklidovu algoritmu znamo odrediti polinome $\varphi(\lambda)$, $\gamma(\lambda)$ tako da bude

(2) $$\varphi(\lambda)\, f(\lambda)+\gamma(\lambda)\, g(\lambda)=1.$$

A sada dolazi primjena toga. Promatrajmo matrične polinome fA i gA (naprosto umjesto skalarne varijable λ pisati kvadratnu matricu A). Relacija (2) daje predočenje identičnog operatora I:

(3) $$\varphi\, \mathrm{A} f \mathrm{A}+\gamma\, \mathrm{A} g\, \mathrm{A}=\text{ident}.$$

Neka je F *nula-prostor operatora* fA, tj. F je skup svih vektora x za koje je $f(A)\,x=0$. Slično, neka G bude 0-prostor ili homomorfno jezgro operatora $g(A)$. Tada su F i G dva invarijantna potprostora i njihova direktna suma je čitav prostor V.

Dokaz da je F invarijantan prema A, tj. da iz $x\in F$ izlazi $A\,x\in F$.

Naime, $f(A)\,A\,x=A f(A)\,x=0$. Slično za $A\,G\subset G$. Neka je $v\in V$ proizvoljno. Tada iz (3) imamo, „množeći" (3) zdesna sa v:

$$\begin{cases} v_1+v_2=v, & \text{pri čemu je} \\ \varphi\,A f A\,v=v_1, & \gamma\,A\,g\,A\,v=v_2. \end{cases} \tag{4}$$

Dokažimo da je $v_1\in G$, $v_2\in F$.

$$g(A)\,v_1=g(A)\,(\varphi(A) f(A)\,v)=g(A)\,\varphi(A) f(A)\,v=$$
$$=\varphi(A)\,g(A) f(A)\,v=\varphi(A) f(A)\,g\,A\,v=0, \quad \text{tj. } v_1\in G.$$

Isto se tako dokazuje $v_2\in F$.

Na taj način $F\dot{+}G=V$. No, dokažimo da nema drugog rastava $v=v_1'+v_2'$ sa sličnim svojstvima.

Bilo bi, naime, $v_1+v_2=v_1'+v_2'$, pa bismo imali vektor

$$z=v_1-v_1'=v_2'-v_2,$$

koji je i u F i u G (kao razlika dvaju vektora iz F, odnosno dvaju vektora iz G).

Stavljajući z u identitet (3), imamo

$$\varphi\,A f A\,z+\gamma\,A\,g\,A\,z=z$$

$$0+0=z \quad \text{dakle} \quad v_1=v_1',\ v_2=v_2'.$$

Tako smo dokazali

15.3. Teorem. (priprava za prvi teorem o cijepanju prostora). *Ako je minimalni polinom operatora A produkt od dva relativno prosta polinoma $f(\lambda)$, $g(\lambda)$, tada nula-prostor F operatora $f\,A$ i nula-prostor G operatora $g\,A$ jesu dva invarijantna potprostora polaznog operatora A; i njihova direktna suma je sam prostor V. Polinom $f(\lambda)$ je minimalni polinom za podoperator $A\,|\,F$; slično, $g(\lambda)$ je minimalni polinom za podoperator $A\,|\,G$.*

Drugim riječima, $f(\lambda)$ *je najniži normirani polinom u* λ *sa svojstvom da je* $f(A)\,x=0$ *za svako* $x\in F$. Slično za $g(\lambda)$.

15.3.1. Zapravo, još preostaje da dokažemo da je $f(\lambda)$ *minimalni* polinom za $A\,|\,F$. U svakom slučaju, kako je $f(A)\,\dot{F}=0$, mora minimalni polinom $f_1(\lambda)$ od $A\colon F\to F$ biti određen djelitelj od $f(\lambda)$; isto tako mora minimalni polinom g_1 za $A\,|\,G$ biti neki djelitelj od $g(\lambda)$. No, rastav (4) pokazuje da mora vrijediti

$$f_1(A)\,g_1(A)\,v=f_1(A)\,g_1(A)\,\varphi\,A f A\,v+f_1(A)\,g_1(A)\,\gamma\,A\,g\,A\,v=$$
$$=g_1(A)\,f_1(A)\,v_1+f_1\,g_1\,v_2=0+0=0, \qquad \text{tj.}$$

polinom $f_1(\lambda)\cdot g_1(\lambda)$ je poništen operatorom A, što znači da je taj polinom djeljiv sa $\mu(\lambda, A)=f(\lambda)\,g(\lambda)$. Kako je $f_1|f$, $g_1|g$ i k tome $f\,\mathrm{M}\,g=1$, mora očigledno biti $f=f_1$, $g=g_1$. Q. E. D.

15.4. Analogan zaključak vrijedi ako je minimalni polinom produkt od 3, 4, ... relativno prostih polinoma. Tako se dobiva

$\longrightarrow$ **15.5. Prvi teorem o cijepanju prostora i faktorizaciji minimalnog mnogočlana ili Frobeniusov normalni oblik operatora.** *Neka je dat linearni operator $A: V_n \to V_n$ u vektorskom prostoru nad tijelom K; ako je minimalni mnogočlan $\mu(\lambda; A)$ prostora V produkt od relativno prostih polinoma $\mu_1(\lambda), \ldots, \mu_k(\lambda)$, tada faktorizaciji (cijepanju)*

(1) $$\mu(\lambda)=\mu_1(\lambda)\cdot\mu_2(\lambda)\cdots\mu_k(\lambda) \textit{ polinoma } \mu(\lambda) \textit{ odgovara cijepanje}$$

$$V=M_1\dot{+}M_2\dot{+}\cdots\dot{+}M_k$$

prostora V na invarijantne potprostore $M_1, M_2, \ldots, M_k$; pri tom je svako $M_{k'}$ skup svih rješenja jednadžbe $\mu_{k'}(A)\,x=0$; minimalni mnogočlan prostora $M_{k'}$ upravo je $\mu_{k'}(\lambda)$. Ako je podoperator od A u prostoru $M_{k'}$ zapisan matricom $A_{k'}$ u nekoj bazi $e^{k'}$ prostora $M_{k'}$, tada zapis čitava operatora A u prostoru V izgleda ovako:

(2) $$\begin{bmatrix} \boxed{A_1} & & & & \\ & \boxed{A_2} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \boxed{A_k} \end{bmatrix},$$

i to u bazi $e=(e^1, e^2, \ldots, e^k)$ koja je sastavljena od vektora koji sačinjavaju bazu e^1, bazu $e^2, \ldots, e^k$ (baza e^i je baza u potprostoru M_i i sastavljena je od nekog broja vektorâ $e_1^i, e_2^i, \ldots$).

Zapis (2) *moguć je u čisto dijagonalnom obliku onda i samo onda ako je minimalni mnogočlan* (1) *produkt linearnih binoma koji su međusobno prosti.*

15.6. Dokažimo eksplicitno posljednji dio teorema. Pretpostavimo da $\mu(\lambda)$ nema nula-tačaka kratnosti >1; to znači da za svako njegovo nula-mjesto λ_k imamo faktor $\lambda-\lambda_k$ i pripadni nula-prostor sastavljen od rješenjâ x, za koja je $(A-\lambda_k)\,x=0$, tj. $Ax=\lambda_k x$; uzimajući sa svake te pravulje po jedan vektor e_k, dobije se tražena baza u kojoj se operator A zapisuje dijagonalno.

Obratno, neka postoji jedan dijagonalan zapis; neka su $\lambda_1, \lambda_2, \lambda_3, \ldots$ vrijednosti s dijagonale koje su međusobno $\neq$; tada operator $f(A)=(A-\lambda_1)(A-\lambda_2)\ldots$ anulira svaki vektor baze, pa je, dakle, $fA=0$; zato je $f(\lambda)$ kratnik minimalnog polinoma μ, koji prema tome ne može imati višestrukih rješenja.

Na taj način vidimo da su struktura prostora i struktura minimalnog polinoma što pripada operatoru međusobno najtješnje povezani.

15.7. Korolar. Operatori proste strukture[1] imaju karakteristično svojstvo da im minimalni polinom ima proste faktore.

To je drukčije izrečen završni dio teorema 15.5.

To pravilo možemo provjeriti npr. na matrici

$$a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix};$$

njen je minimalni polinom $(\lambda - 1)^2$ i matrica nije proste strukture (§ 4.9). Isto vrijedi za Jordanove klijetke

$$J = \begin{bmatrix} \lambda_0 & 1 & & \\ & \lambda_0 & 1 & \\ & & \ddots & 1 \\ & & \ddots & \lambda_0 \end{bmatrix} \quad (\S\ 4.10).$$

15.8. Prostor kao direktna suma cikličkih potprostora. Kao što se svaka konačna komutativna grupa može predstaviti kao direktni rezultat stanovitih cikličkih podgrupa (pogl. 17, § 20.8), tako ćemo sada i svaki prostor moći predstaviti kao direktnu sumu stanovitih *cikličkih* potprostorâ. Dosad smo prema 15.5, prostor predstavili kao direktnu sumu prostorâ s minimalnim mnogočlanom oblika $(\lambda - \lambda_k)^{m_k}$. Sad ćemo dalje svaki ovakav prostor rastaviti na direktnu sumu *cikličkih* potprostora.

Pri tom ćemo primijeniti ovo:

15.8.1. Ako je I invarijantan prostor s obzirom na operator A, tada razni položaji $x \rightarrow x + I$ potprostora I određuju parcelaciju V/I; naime, suma od dva položaja ili razreda $x + I$, $x' + I$ definira se ovako:

$$(x + I) + (x' + I) = (x + x') + I;$$

produkt sa skalarom s definira se ovako:

$$s \cdot (x + I) = sx + I \text{ (jer je } sI = I).$$

Lema. *V/I je vektorski prostor; definiramo li*

$$A(x + I) = Ax + I \quad (x \in V),$$

dobije se određeno linearno preslikavanje prostora V/I u sama sebe.

U prostoru V/I ulogu nule ima sam potprostor I (to je upravo kao pri parcelaciji svake grupe G prema kakvoj invarijantnoj podgrupi I, isp. pogl. 17, § 10.3).

15.8.2. Lema. *Ako parcele $x_1 + I, \ldots, x_k + I$ čine bazu u V/I, tada ti vektori $x_1, \ldots, x_k$ zajedno s nekom bazom potprostora I čine određenu bazu u čitavu prostoru V.*

---

[1] To su operatori koji imaju *potpunu svojstvenu bazu*, tj. vektorsku bazu sastavljenu od *svojstvenih* vektora.

15.8.3. S obzirom na cijepanje prostora u potprostore M_i iz prvog teorema o cijepanju, možemo se ovdje ograničiti na slučaj da svaki taj potprostor M_i dalje pocijepamo u cikličke potprostore. Da ne pišemo indekse, možemo pretpostaviti da je i polazni prostor V takav da mu je minimalni mnogočlan $\mu(\lambda)$ oblika $\mu(\lambda)=p(\lambda)^r$, gdje je $p(\lambda)$ nerastavljiv u tijelu K; r je eksponent.

Evo prethodno nekoliko pojmova.

15.8.4. Minimalni polinom operatora A u odnosu na vektor x je najniži normirani polinom $p(\lambda)$ u λ sa svojstvom da operator $p(A)$ prevodi x u $\vec{0}$, tj. $p(A)x=\vec{0}$. Označivat ćemo ga sa

$$\mu(\lambda, A, x) \quad \text{ili kraće} \quad \mu(\lambda; x). \quad \text{Dakle je} \quad \mu(A, x)x=\vec{0}.$$

Kao primjena osnovnog teorema o dijeljenju polinoma neposredno se zaključuje ova

15.8.5. Osnovna lema. *Ako je za neki polinom* $p(\lambda)$ ispunjeno $p(A)x=0$, *tada je* $\mu(\lambda, x) \mid p(\lambda)$.

Dokaz je isti kao u pogl. 24, § 2.3, kad smo sličnu stvar dokazivali za minimalni polinom matrice, odnosno operatora.

15.8.6. Za bilo koji skup S vektora definiramo pripadni minimalni mnogočlan $\mu(\lambda; S)$ kao onaj koji je normiran, najnižeg stepena i za kojeg je

$$\mu(A; S)\dot{S}=\vec{0} \quad \text{za svako} \quad \dot{S}\in S.$$

15.8.7. Veza između polinoma $\mu(\lambda, S)$ i $\mu(\lambda, \dot{S})$ očituje se iz relacije

$$\mu(\lambda, S)=\mathrm{W}\,\mu(\lambda, \dot{S});$$

posebno, za čitav prostor V vrijedi:

$$\mu(\lambda; V)=\mu(\lambda, e)=(\text{za bilo koju bazu } e)=\mathrm{W}\,\mu(\lambda, \dot{e}). \tag{1}$$

Pri tom, kao što znamo, W označuje operator najmanjeg zajedničkog višekratnika. Specijalno,

$$\mu(\lambda, v'+v'') \,\Big|\, \frac{\mu(\lambda, v')\,\mu(\lambda, v'')}{\mu(\lambda, v')\,\mathrm{M}\,\mu(\lambda, v'')} \tag{2}$$

za bilo koja dva vektora v', v''.

Dokažimo relaciju (1). Prema osnovnoj lemi, polinom $\mu(\lambda, V)$ je kratnik od svakog polinoma $\mu(\lambda, \dot{e})$; obratno ako je $p(\lambda)$ kakav polinom koji je kratnik od svakog od n minimalnih polinoma $\mu(\lambda, \dot{e})$, tada $p(A)$ poništava $\dot{e}$. Stvarno, $p(A)\dot{e}=q(A)\mu(A, \dot{e})\dot{e}=(\text{gdje je } p(\lambda)=q(\lambda)\cdot\mu(\lambda, \dot{e}))=q(A)\cdot\vec{0}=\vec{0}$. Dakle je $p(A)\dot{e}=\vec{0}$; time je i $p(A)V=\{\vec{0}\}$, jer je $p(A)\dot{V}=\vec{0}$ (dovoljno je $\dot{V}$ izraziti pomoću vektorâ $\dot{e}$). Dakle je prema osnovnoj lemi $p(\lambda)$ djeljivo sa $\mu(\lambda, V)$. Prema tome je zaista $\mu(\lambda, V)=\mathrm{W}\,\mu(\lambda, \dot{e})$.

Dokažimo i (2). Neka je $\nu = \nu' + \nu''$. Imamo:

$$\mu(A, \nu') \cdot \mu(A, \nu)\, \nu'' = \mu(A, \nu')\, \mu(A, \nu)(\nu - \nu') = \mu(A, \nu')\, \mu(A, \nu) -$$

$$-\mu(A, \nu')\, \mu(A, \nu)\, \nu' = \mu(A, \nu)\, \vec{0} - \mu(A, \nu)\, \mu(A, \nu')\, \nu' = 0 - \mu(A, \nu)\, \vec{0} = \vec{0},$$

tj.

$$\mu(A, \nu')\, \mu(A, \nu)\, \nu'' = \vec{0}.$$

Odatle prema osnovnoj lemi

$$\mu(\lambda, \nu'') \mid \mu(\lambda, \nu') \cdot \mu(\lambda, \nu). \tag{3}$$

Slično

$$\mu(\lambda, \nu') \mid \mu(\lambda, \nu'') \cdot \mu(\lambda, \nu).$$

Ako su elementi u (3) nalijevo međusobno prosti, onda to znači da je $\mu(\lambda, \nu)$ djeljivo svakim od njih, dakle i njihovim produktom, pa je

$$\mu(\lambda, \nu) = \mu(\lambda, \nu') \cdot \mu(\lambda, \nu''),$$

jer se lako vidi da

$\mu(A, \nu') \cdot \mu(A, \nu'')$ poništava i ν' i ν'' (a time i $\nu = \nu' + \nu''$). Npr

$$\mu(A, \nu') \cdot \mu(A, \nu'') \cdot \nu' = \mu(A, \nu'')\,(\mu(A, \nu') \cdot \nu') = \mu(A, \nu'') \cdot \vec{0} = \vec{0}.$$

Ako je f=najveći zajednički faktor polinomâ, odnosno izrazâ na lijevim stranama u (3), tada su relacije (3) očigledno ekvivalentne s relacijama koje se iz njih dobiju dijeleći i lijevo i desno od znaka | sa f. Time se nalazimo u prethodnom slučaju, pa zaključujemo da je prvi član $(3)_1$ u (3) djeljiv drugim članom $(3)_2$.

Time je i relacija (2) dokazana.

Postavlja se pitanje da li je, obratno, drugi član u (2) djeljiv prvim članom, tj. da li matrični polinom $(2)_2$ poništava i ν' i ν''.

15.9. Ciklički zapis operatora A kojemu je minimalni polinom oblika $p(\lambda)^r$.

Teorem. ***Polazimo od prostora V kojemu je minimalni mnogočlan oblika***

$$\mu(\lambda, V) = p(\lambda)^{r_0}, \tag{1}$$

r_0 je prirodan broj; $p(\lambda)$ je polinom nerastavljiv na produkt drugih polinoma s koeficijentima u promatranom tijelu K.

Tada je moguće prostor V prikazati kao direktnu sumu

$$(e_0, V) \dot{+} (e_1, V) \dot{+} \cdots \dot{+} (e_{s-1}, V)$$

potpuno određena broja cikličkih prostorâ

$$(e_0, V), (e_1, V), \ldots, (e_{s-1}, V)$$

s potpuno određenim prirodnim minimalnim polinomima

$$p(x)^{r_0}, p(x)^{r_1}, \ldots, p(x)^{r_{s-1}}, \textit{ za koje je } r_0 \geq r_1 \geq r_2 \geq \cdots$$

Zapis operatora A u bazi e koja obuhvata cikličku bazu

$$e^i=(e_i,\ Ae_i,\ A^2 e_i, \ldots),\ \textit{svakog od tih potprostora}\ (e_i,\ V)$$

ima kvazidijagonalni oblik s klijetkom pridruženom polinomu $p(x)^{r_i}$: nastaje iz nula-matrice tako da se neposredno ispod glavne dijagonale stavlja **1**, *a u zadnji stupac se sastavljaju svi koeficijenti polinoma — $p(x)^{r_i}$ osim najstarijeg, i to po redu koeficijenti od* $\lambda^0, \lambda^1, \lambda^2, \lambda^3, \ldots$, (isp. § 15.9.6).

15.9.1. Svaki član $\dot{V}\in V$ ima minimalni polinom $\mu(\lambda, \dot{V})$ oblika $p(\lambda)^r$, jer je (1) zajednički kratnik svih $\mu(\lambda, \dot{V})$. *To specijalno znači da postoji jedan vektor $e_0\in V$ za koji je $\mu(\lambda, e_0)=\mu(\lambda, V)=p(\lambda)^{r_0}$:*

(2) $$\mu(\lambda, e_0)=p(\lambda)^{r_0}.$$

Obrazujmo pripadni ciklički invarijantni prostor $Z=(e_0;\ A)$ s bazom

(3) $$e_0,\ e_1=Ae_0,\ e_2=A^2 e_0, \ldots,\ e_{k-1}=A^{k-1} e_0,\ k=r_0\cdot \operatorname{st} p.$$

Ako je već $V=Z$, stvar je gotova: prostor je ciklički pa u bazi (3) operator A se zapisuje osebujnom matricom koja prati vezu

(3') $$e_k=-c_0 e_0-c_1 e_1+\cdots+c_{k-1} e_{k-1};$$

zapis je ovakav;

$$\begin{bmatrix} 0 & & & & -c_0 \\ 1 & 0 & & & -c_1 \\ 0 & 1 & \cdot & & -c_2 \\ 0 & \cdot & & & \cdot \\ 0 & & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & & -c_{k-2} \\ \cdot & & & 1 & -c_{k-1} \end{bmatrix}$$; ta matrica odražava upravo veze (3) i (3').

15.9.2. Ako je prostor V opsežniji nego Z, promatrat ćemo sve $Z+\dot{V}$ i od njih izgrađeni prostor V/Z. Njegova dimenzija je $\dim V-\dim Z$, dakle $<\dim V$. Pomoću

(4) $$A'(\dot{V}+Z)=A\dot{V}+Z$$

definiran je na V/Z određen operator A'. Učinimo sa V/Z i A' ono što smo učinili sa V, A i zapišimo prethodno da se svaki član f' iz Z prikazuje na potpuno određen način u bazi (3), odnosno u bazi $(e_0, \ldots, e_{k-1})$, tako da postoji polinom f stupnja $<k$ sa svojstvom da je

(4') $$f'=f(A)\cdot e_0.$$

Diobeni prostor V/Z ima svoj vlastiti minimalni polinom; on je oblika $p(\lambda)^{r_1}$ uz $r_1\leq r_0$; također, kao maloprije, postoji parcela $\gamma\in V/Z$ sa svojstvom da je

(5) $$\mu'(\lambda, \gamma)=p(\lambda)^{r_1},$$

pri čemu crticom u μ' želimo istaknuti da sada radimo u samostalnom prostoru V/Z i s minimalnim polinomom elemenata γ prema V/Z, A'. To znači da je (5) prvi normirani polinom sa svojstvom da je $\mu'(A', \gamma)\gamma = Z$ (jer u novom prostoru čitav bivši prostor Z igra ulogu nule); drugim riječima,

(6) $p(A)^{r_1}\dot{\gamma} \in Z$ za svako $\dot{\gamma}$ (kako je $\dot{\gamma} \in \gamma \subset V$, to je $\dot{\gamma} \in V$);

na taj način, prema onom što smo rekli u (4′), postoji zapis oblika (4) za element (6) označujući element iz (6) sa f'; drugim riječima, postoji polinom stepena $<k$ tako da je

(7) $$p(A)^{r_1}\dot{\gamma} = f(A)\, e_0.$$

No, zbog $\dot{\gamma} \in V$ vrijedi $0 = p(A)^{r_0}\dot{\gamma}$. Zato, množeći (7) sa $p(A)^{r_0-r_1}$, izlazi

(8) $$p(A)^{r_0}\dot{\gamma} = p(A)^{r_0-r_1} f(A)\, e_0, \quad \text{tj.} \quad 0 = p(A)^{r_0-r_1} f(A)\, e_0.$$

Baš ta jednakost iskazuje da polinom

(8′) $p(\lambda)^{r_0-r_1} f(x)$, koji pripada koeficijentu od e_0,

u (8), mora biti višekratnik od minimalnog polinoma

$$\mu(\lambda, e_0) = p(\lambda)^{r_0} \quad (\text{v. } (2));$$

drugim riječima, kvocijent polinoma (8′) i $p(\lambda)^{r_0}$ mora biti polinom, recimo $q(\lambda)$; to znači da postoji polinom $q(\lambda)$ sa svojstvom

(9) $$f(\lambda) = p(\lambda)^{r_1} q(\lambda).$$

S obzirom na (7) i (9) imamo

$$p(A)^{r_1}\dot{\gamma} = p(A)^{r_1} q(A)\, e_0$$

(10) $$p(A)^{r_1}(\dot{\gamma} - q(A)\, e_0) = 0.$$

No, $e_1 = \dot{\gamma} - q(A)\, e_0$ kao razlika člana $\dot{\gamma}$ iz γ i člana $q(A)\, e_0$ iz Z je opet u γ, tj. e_1 non$\in Z$. Tako imamo relacije

(11) $$e_1 \text{ non} \in Z \qquad p(A)^{r_1} e_1 = \vec{0}.$$

Ta druga relacija, interpretirana u polaznom prostoru V, znači da je $p(A)^{r_1}$ kratnik minimalnog polinoma $\mu(\lambda, e_1)$; kako je, s druge strane $\mu(\lambda, e_1)$ kratnik od $\mu'(\lambda, \gamma) = p(\lambda)^{r_1}$ prema (5), znači da je

(12) $$\mu(\lambda, e_1) = \mu'(\lambda, \gamma) = p(\lambda)^{r_1}.$$

15.9.3. Relacijom (12) uspostavljena je veza između polaznog prostora V i novog diobenog prostora V/Z: izvodnici γ, koja među parcelama ciklički rađa jedan ciklički prostor $(\gamma, V/Z)$, odgovara određen element e_1 i u polaznom prostoru V koji generira ciklički prostor $(e_1; V)$ u polaznom prostoru, i to iste dimenzije koju je imao i prostor $(\gamma; V/Z)$; time smo u polaznom prostoru V dobili već dva ciklička potprostora (e_0, V), (e_1, V), koji osim 0 nemaju ništa zajedničko.

Njihova direktna suma

(13) $$Z_1=(e_0,\ V)\dot{+}(e_1,\ V)$$

daje određen potprostor prostora V invarijantan u odnosu na A. Ako je time V iscrpeno, traženi ciklički prikaz je dobiven.

15.9.3.1. *Dokaz da iz* $v\in(e_0,\ V)\cap(e_1,\ V)$ *izlazi* $v=\vec{0}$. Naime v kao član iz $(e_0,\ V)$ bilo bi oblika $Q_0(A)\,e_0$, gdje je $Q_0(\lambda)$ polinom stupnja $<k$ $(=\dim(e_0,\ V))$; iz istog razloga je

$$v=Q_1(A)\,e_1,\ \operatorname{st} Q_1(\lambda)<k_1\ (=r_1 \operatorname{st} p),$$

jer vektori

$$e_1,\ e_2=A\,e_1,\ \ldots,\ e_{k_1}=A^{k_1-1}e_1$$

čine bazu u $(e_1,\ V)$. Dakle bi bilo

(*) $$Q_0(A)\,e_0=v=Q_1(A)\,e_1,\ \operatorname{st} Q_0<k,\ \operatorname{st} Q_1<k_1.$$

S druge strane, iz (4) izlazi

$$A'\,(e_1+Z)=A\,e_1+Z.$$

Odatle za polinom Q_1:

$$Q_1(A')\,(e_1+Z)=Q_1(A)\,e_1+Z=(\text{zbog }(*))=Q_0(A)\,e_0+Z=Q_0(e_0+Z)=Z.$$

Dakle je $Q_1(A')\,(e_1+Z)=Z$; to znači da je $Q_1(\lambda)$ djeljivo sa μ' što zbog (5) i $\operatorname{st} Q_1(\lambda)<\operatorname{st} p^{r_1}$ daje $Q_1(\lambda)\equiv 0$, tj. $v=\vec{0}$.

15.9.4. A ako je i (13) tek pravi dio od V, onda ćemo (13) uzeti kao novu „jedinicu" za razbijanje prostora V na parcele V/Z_1, pa zaključiti kao maloprije da postoji jedan član $e_2\in V/Z_1$ kojemu je $\mu(\lambda,\ e_2)$ oblika $p(\lambda)^{r_2}$ sa $r_2\leq r_1$ i koji rađa ciklički prostor $(e_2,\ V)$, koji sa (13) osim $\vec{0}$ nema ništa zajedničkog, tako da se može promatrati i direktna suma

(14) $$Z_2=Z_1\dot{+}(e_2,\ V)=(e_0,\ V)\dot{+}(e_1,\ V)\dot{+}(e_2,\ V);\ \text{itd.}$$

15.9.5. Proces se mora završiti, jer za dimenzije prostorâ vrijedi

$$\dim(e_i,\ V)=\operatorname{st}\mu(\lambda,\ e_i):$$

prvi razvoj daje potprostor $(e_0,\ V)$ dimenzije $r_0 \operatorname{st} p$;

drugi razvoj daje potprostor Z_1 dimenzije $(r_0+r_1) \operatorname{st} p$;

treći razvoj daje potprostor Z_2 dimenzije $(r_0+r_1+r_2) \operatorname{st} p,\ \ldots,$

tako da je razvijanje konačno-dimenzionalnog prostora V u cikličke potprostore osigurano i vodi sigurno do cilja.

15.9.6. Ujedno se vidi i ovo: kako su eksponenti $r_0,\ r_1,\ \ldots$ za $\mu(\lambda,\ e_0)$, $\mu(\lambda,\ e_1),\ \ldots$ imali svoje stvarno značenje u vezi sa samim prostorom V i njegovim podjelama, zaključujemo da su brojevi $r_0\geq r_1\geq\cdots$ jednoznačno određeni (inače zavise jedino od prostora V i operatora A).

15.9.7. Dokaz teorema 15.9. može se formalno provesti i induktivno prema broju $\dim V$. Prvi korak sastoji se u provođenju postupka iz § 15.9.1: formira se potprostor $(e_0, V)=Z_0$ dimenzije $p(\lambda)^{r_0}$; zatim se pretpostavi da je teorem ispravan za svaki prostor dimenzije $<n$ i kojemu minimalni polinom ima oblik (1). Onda se formira prostor V/Z_0 i operator A'; on udovoljava uslovima indukcije, pa je, dakle, direktna suma cikličkih potprostora Z_1', Z_2', ... s minimalnim polinomima oblika $p(\lambda)^{r_1}$, $p(\lambda)^{r_2}$ ..., gdje je $r_0 \geq r_1 \geq r_2 \geq \cdots$

Neka je γ_i onaj odabrani element u V/Z_0 koji ima svojstvo da $A\gamma_i$, $A^2\gamma_i$, ... služi kao baza u cikličkom potprostoru Z_i; tada prema razlaganju u § 15.9.2. postoji u γ_i bar jedan element e_i sa svojstvom (12); na taj način cikličkom potprostoru Z_i' u V/Z_0 dolazi o bok jednako-dimenzionalan ciklički potprostor $(e_i, V)=Z_i$ potprostora V; dolazi se do željenog rastava

$$V=Z_0 \dot{+} Z_1 \dot{+} Z_2 \dot{+} \cdots$$

$\longrightarrow$ **15.10. Opći teorem cijepanja prostora na cikličke potprostore i prosto-racionalni zapis linearnog operatora.** ***Ako je A linearni operator u V, pa ako je minimalni polinom*** $\mu(\lambda, A)$ ***operatora A produkt od relativno prostih polinoma oblika*** $p_i(\lambda)^{r_{i0}}$, ***pri čemu je*** $p_i(\lambda)$ ***nerastavljiv polinom u tijelu K, tada je V direktna suma potprostorâ*** V_i ***pri čemu je*** V_i ***prostor svih rješenja jednadžbe*** $p_i(A)^{r_{i0}}\,x=\vec{0}$; $\dim V_i = \mathrm{st}\, p_i(\lambda)^{r_{i0}}$ ***i minimalni polinom od*** V_i ***je*** $p_i(\lambda)^{r_{i0}}$; ***svaki od prostora*** V_i ***dalje se prikazuje kao direktna suma cikličkih potprostora prema teoremu* 15.9. *Na taj je način i sam prostor V direktna suma cikličkih potprostora kojima je narav opisana u* § 15.9.**

16. ELEMENTARNI DJELITELJI KARAKTERISTIČNIH MATRICA

Prema izlaganjima u prošlom paragrafu svaka matrica a dopušta osebujan ciklički zapis operatora što ga ona predstavlja. To znači da je matrica a slična s određenom prosto-racionalnom formom matrice u kojoj se pojavljuju nerastavljivi faktori minimalnog polinoma matrice.

Na taj način možemo zapisati da vrijedi ovaj

$\longrightarrow$ **16.1. Opći teorem o prosto-racionalnom kanonskom obliku matrice.** ***Neka je a matrica reda n nad tijelom K; tada je matrica a slična s kvazidijagonalnom matricom, i to jednom jedinom u kojoj su klijetke upravo matrice koje popraćuju polinome***

(1) $$p_i(\lambda)^{r_{i0}},\ p_i(\lambda)^{r_{i1}},\ \ldots,\ r_{i0} \geq r_{i1} \geq \cdots > 0;$$

pri tom za minimalni polinom $\mu(\lambda, a)$ ***matrice a vrijedi:***

$$\mu(\lambda, a)=p_1(\lambda)^{r_{10}} \cdot p_2(\lambda)^{r_{20}} \cdots$$

16.2. Definicija. Polinomi (1) koji se pojavljuju u gornjem rastavu zovu se *elementarni djelitelji ili elementarni divizori matrice* $\lambda - a$ (pa i matrice a); pri tom se svaki elementarni djelitelj računa sa svojom kratnošću, tj. onoliko puta u koliko se raznih klijetaka polinom oblika (1) pojavljuje.

16.3. Lema. Elementarni divizori i klijetke u kanonskom rastavu odgovaraju jedni drugima: svakoj klijetki kao matrici odgovara minimalni polinom i karakteristični polinom, koji se podudaraju i jednaki su određenom elementarnom djelitelju matrice; i obratno: svakom elementarnom djelitelju matrice odgovara jedna klijetka u kanonskom zapisu matrice.

16.4. Lema. Karakteristični polinom kvazidijagonalne matrice je produkt karakterističnih polinoma klijetaka.

Stvarno ako je npr.

$$a=\begin{bmatrix} b & \\ & c \end{bmatrix},$$

gdje su b, c, ... kvadratne matrice, tada je

$$\varkappa(\lambda, a)=\det(\lambda-a)=\begin{vmatrix} \lambda-b & \\ & \lambda-c \end{vmatrix}=(\text{za slučaj da je } b \text{ reda } 2)=$$

$$\begin{vmatrix} \lambda-b_{11} & -b_{12} & & \\ & \lambda-b_{22} & & 0 \\ & 0 & \lambda-c_{11} & \cdots \\ & & \cdot & \cdot\ \cdot\ \cdot \end{vmatrix}=$$

$$=(\text{po Laplaceovu pravilu razvijajući po recima u kojima je } \lambda-b)=$$

$$=\det[\lambda-b]\cdot\det[\lambda-c]=\varkappa(\lambda, b)\cdot\varkappa(\lambda, c).$$

Slično ako a ima 3, 4, ... klijetaka.

⟶ **16.5. Teorem.** ***Karakteristični polinom matrice je produkt elementarnih djelitelja te matrice.***

Naime, klijetke su u prosto-racionalnom kanonskom obliku zadane matrice a takve da im je pripadni karakteristični polinom jedan elementarni djelitelj matrice a. Prema prethodnoj tački karakteristični polinom matrice je upravo produkt karakterističnih polinoma tih klijetaka, dakle produkt elementarnih djelitelja matrice.

16.6. Lema. Elementarni djelitelji klijetaka kvazidijagonalne matrice tvore elementarne djelitelje same matrice; pri tom se svaki pojavljuje sa svojom kratnošću.

Npr. ako matrica a, odnosno b ima elementarne djelitelje

$$(\lambda-1)^2,\ (\lambda-1)^2,\ \text{odnosno}\ (\lambda-1)^2,\ (\lambda-1),\ (\lambda-1)^3,$$

tada matrica diag$[a, b]$ ima ove elementarne djelitelje:

$$(\lambda-1)^2,\ (\lambda-1)^2,\ (\lambda-1)^2,\ \lambda-1,\ (\lambda-1)^3;\ \text{format joj je } (10, 10).$$

17. JORDANOV OBLIK MATRICA I JORDANOV ZAPIS LINEARNOG OPERATORA

17.1. Neka je a kvadratna matrica s realnim ili kompleksnim vrijednostima; tada su nerastavljivi djelitelji karakterističnog polinoma $\varkappa(\lambda, a)$ nužno oblika $\lambda-\lambda_i$, gdje je λ_i kompleksni broj; prema tome, polinomi $p_i(\lambda)^{r_{ik}}$— elementarni djelitelji matrice — sad su oblika $(\lambda-\lambda_i)^{i'}$, gdje je i' cio broj; odgovarajuća klijetka u racionalnom kanonskom prikazu je kvadratna matrica reda i', u kojoj su posljednji stupac zauzeli prvih i' koeficijenata polinoma $-(\lambda-\lambda_i)^{i'}$; to je tako ako za bazu uzmemo vektore

(1) $$e_0,\ Ae_0,\ A^2e_0,\ \ldots,\ A^{i'-1}e_0;$$

pri tom je e_0 vektor kojemu je $(\lambda-\lambda_i)^{i'}$ minimalni mnogočlan. No, promatrajmo uz operator A također operator $A-\lambda_i$, koji pokazuje odstupanje skalarnog operatora λ_i od A. Uz taj operator pojavljuje se isto tako i' nezavisnih vektora

(2) $$e_0,\ (A-\lambda_i)e_0,\ (A-\lambda_i)^2e_0,\ \ldots,\ (A-\lambda_i)^{i'-1}e_0;$$

sagradimo iz njih novu bazu e' brojeći vektore (2) obrnutim redom, tj. stavimo

(3) $$e_0'=(A-\lambda_i)^{i'-1}e_0,\ e_1'=(A-\lambda_i)^{i'-2}e_0,\ \ldots,\ e'_{i'-2}=(A-\lambda_i)e_0,\ e'_{i'-1}=e_0,$$

Primijetimo da je

(4) $$(A-\lambda_i)e_0'=(A-\lambda_i)^{i'}e_0=0,$$

jer je $(\lambda-\lambda_i)^{i'}$ minimalni polinom vektora e_0 (čak i čitava cikličkog prostora što ga rađaju vektori (1)). Iz (4) izlazi:

$$Ae'_0=\lambda_i e'_0.$$

Analogno, množeći (3) sa $A-\lambda_i$, izlazi:

$$(A-\lambda_i)e'_{k+1}=e'_k, \quad \text{odakle} \quad Ae'_{k+1}=e'_k+\lambda_i e'_{k+1}.$$

Ukratko djelovanje operatora A na novoj bazi e' izgleda ovako:

$$Ae'_0=\lambda_i e'_0 \quad (\text{rastezanje duž } e'_0),$$
$$Ae_1'=e_0+\lambda_i e_1',\ \ldots,\ Ae'_{i'-1}=e'_{i'-2}+\lambda_i e'_{i-1},$$

odnosno zapisano tablično

$$J_i=\underbrace{\begin{bmatrix} \lambda_i & 1 & & \\ & \lambda_i & 1 & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix}}_{i}.$$

To je Jordanova klijetka, i to gornja Jordanova klijetka. Vidi se da ta matrica ima jedan jedini elementarni djelitelj, i to $(\lambda-\lambda_i)^i$ (isp. § 18.3.1). Time smo došli do

—→ **17.2. Teorema o Jordanovoj formi matrica, odnosno zapisa operatora.** ***Svaki linearni operator A koji djeluje u vektorskom prostoru može se zapisati kvazidijagonalno nizanjem Jordanovih klijetaka što pripadaju elementarnim divizorima operatora, odnosno pripadne matrice.***

Ako za minimalni polinom $\mu(\lambda, a)$ vrijedi

$$\mu(\lambda, a) = (\lambda - \lambda_0)^{r_{00}} (\lambda - \lambda_1)^{r_{10}} \dots$$

gdje su $\lambda_0, \lambda_1, \dots,$ međusobno $\neq$, tada se svako λ_i pojavljuje u Jordanovoj klijetki reda r_{i0}, ali se može pojaviti i u užim klijetkama reda

$$r_{i1} \geq r_{i2} \geq \dots$$

—→ **17.3. Teorem.** ***Ako je a kvadratna konačna matrica s kompleksnim vrijednostima, tada postoji nesingularna kompleksna matrica u sa svojstvom da matrica $u^{-1}au$ bude Jordanova oblika.***

18. MATRICE KOJIMA SU VRIJEDNOSTI POLINOMI (λ-MATRICE)

18.1. Neka je a proizvoljna matrica i neka je $a_{ik}(\lambda)$ stanovit algebarski polinom s obzirom na λ (običaj je pisati λ za varijablu ili neodređenicu). Na taj način matrica a zavisi od λ, pa se može govoriti o matrici $a(\lambda)$ da se istakne i veličina λ.

Npr. takve su matrice

$$\begin{bmatrix} 3-\lambda & \lambda^2+1 & \lambda^3-\lambda^2+1 \\ 2 & 5+\lambda & \lambda^4 \end{bmatrix}.$$

Sa λ-matricama možemo vršiti elementarne transformacije kao i s običnim matricama (pogl. 15, § 4). Samo što će se ovdje dopuštati da pojedini redak (stupac) smijemo množiti i polinomima u λ, ukoliko rezultate dodajemo nekom drugom retku (stupcu.).

18.2. Smithov normalni oblik matrice. Ideja je takvih transformacija da se zadana λ-matrica svede na što *prostiji dijagonalni oblik*, specijalno na takav da nenulti članovi na dijagonali budu normirani polinomi i da svaki dijeli naredni; to je tzv. *Smithov normalni oblik matrice* ili *normalni dijagonalni oblik matrice.* Kao u pogl. 15, § 6, tako se i za λ-matrice uvodi pojam ekvivalencije (λ-ekvivalencija λ-matrica). Rang $r(a(\lambda))$ se definira kao supremum duljinâ kvadratnih podmatrica c od $a(\lambda)$ kojima nije $\det c \equiv 0$. Npr. za svaku realnu (n, n)-matricu a je $r(\lambda - a) = n$.

18.3. Prvi korak. Zadanu λ-matricu $a(\lambda)$ *elementarno* preobraziti tako da u novoj matrici a' gornji lijevi ugao zauzima najveći zajednički djelitelj svih a_{ik}, tj. da bude

$$a'_{11}(\lambda) = \underset{i,k}{\mathrm{M}}\, a_{ik}(\lambda). \tag{1}$$

Upisivanje normiranog polinoma $\mathrm{M}\, a_{ik}(\lambda)$ kao a'_{11}, tj. njegovo dovođenje u polje (1, 1) teoretski je zanimljiv postupak i može se sastojati od dugog niza operacija (jer zasad još polinom (1) nije određen!).

18.3.1. Postupak je ovaj. U zadanoj matrici uoči se član $a_{ik}(\lambda)\neq 0$ s *minimalnim stepenom u* λ; ako ima više takvih članova, izaberimo onaj koji ima po modulu najmanji vodeći koeficijent. Permutacijom redaka i permutacijom stupaca može se uočeni član dovesti u gornji lijevi ugao. Dijeleći prvi stupac ili prvi redak vodećim koeficijentom novoga člana, možemo taj član normirati. Neka je $b(\lambda)$ tako dobivena matrica. A sad ćemo pokušati poništiti sve ostale komponente iz prvog stupca i prvog retka. Najprije dovedimo umjesto svakog $b_{i1}(\lambda)$ kojem je stepen $> \mathrm{st}\, b_{11}$, njegov ostatak pri dijeljenju sa $b_{11}(\lambda)$; to znači da treba odrediti kvocijent i ostatak prema $b_{i1}(\lambda)=b_{11}(\lambda)\, q_{i1}(\lambda)+r_{i1}(\lambda)$, pa redak $b_{1\cdot}$ pomnožiti sa $-q_{i1}(\lambda)$ i rezultat dodati retku $b_{i\cdot}$; tako će umjesto b_{i1} doći ostatak r_{i1}. Čim se tako pojavi koje $r_{i1}\neq 0$, dopremamo njega odnosno ono $r_{i1}\neq$koje ima najmanji stepen na čvorno mjesto $(1, 1)$ i s njim radimo kao s udarnim elementom. Jasno je da najzad mora izaći neka matrica koja u lijevom i gornjem rubu ima same 0, osim na polju $(1, 1)$, gdje stoji određen „top" $T(\lambda)$; ako ovaj top $T(\lambda)$ ne dijeli svaku preostalu komponentu momentane matrice c, onda se uoči jedna komponenta $c_{ik}(\lambda)$ nedjeljiva sa $T(\lambda)$, dotični stupac se doda prvom stupcu i na novoj matrici c vrši prethodni postupak. Nakon stanovitog broja koračaja moramo doći do matrice a' oblika

$$\begin{bmatrix} a'_{11}(\lambda) & 0 & 0 & \cdots & 0 \\ 0 & & & & \\ 0 & & & & \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ 0 & & & & \end{bmatrix}$$

i u kojoj $a'_{11}(\lambda)$ dijeli svaki član naznačenog pravokutnika; drugim riječima, cilj (1) je postignut.

To je bio prvi, dug korak.

18.3.2. Sada dolazi naredni korak; isti postupak od maloprije primjenjuje se na naznačeni pravokutnik. Time će se u polje $(2, 2)$ dovesti najveći zajednički djelitelj članova $a'_{ik}(\lambda)$ sa $i, k>1$, itd. Konačni rezultat bit će ovaj

$\longrightarrow$ **18.4. Teorem o svođenju matrice na Smithov normalni oblik.** ***Svaka matrica $a(\lambda)$ može se pomoću konačno mnogo elementarnih transformacija prevesti u kanonsku dijagonalnu matricu oblika***

$$\begin{bmatrix} I_1(a) & & & & 0 \\ & I_2(a) & & & \\ & & I_r(a) & & \\ & & & \ddots & \\ 0 & & & & I_n(a) \end{bmatrix}, \tag{2}$$

pri čemu svaki član na dijagonali dijeli naredni. Broj članova $\neq 0$ na dijagonali jednak je rangu r polazne matrice $a(\lambda)$; svi su oni određeni polinomi u λ (mogu biti $i=1$).

18.5. Definicija. **Invarijantni djelitelji vezani za λ-matricu** $\boldsymbol{a}(\lambda)$. Sami članovi $J_1(a), \ldots, J_r(a)$ u (2) zovu se *invarijantni »mnogočlani«* ili *»invarijantni« djelitelji* (*faktori*) vezani za polaznu λ-matricu $a(\lambda)$.

18.5.1. Primjer Jordanove klijetke:

$$J=\begin{bmatrix} \lambda_0 & 1 & 0 \\ 0 & \lambda_0 & 1 \\ 0 & 0 & \lambda_0 \end{bmatrix}$$

odnosno pripadne klijetke $\lambda - J =$

$$\begin{bmatrix} \lambda-\lambda_0 & \boxed{-1} & 0 \\ 0 & \lambda-\lambda_0 & -1 \\ 0 & 0 & \lambda-\lambda_0 \end{bmatrix} \to \begin{bmatrix} \boxed{-1} & \lambda-\lambda_0 & 0 \\ \lambda-\lambda_0 & 0 & -1 \\ 0 & 0 & \lambda-\lambda_0 \end{bmatrix} \to$$

(pomnoži prvi redak sa -1 radi normiranja; pomnoži 1. redak sa $(\lambda-\lambda_0)$ i dodaj drugom retku)

$$\begin{bmatrix} 1 & -(\lambda-\lambda_0) & 0 \\ 0 & (\lambda-\lambda_0)^2 & -1 \\ 0 & 0 & \lambda=\lambda_0 \end{bmatrix} \to$$

(prvi stupac pomnožen sa $(\lambda-\lambda_0)$ i dodan drugom)

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & (\lambda-\lambda_0)^2 & -1 \\ 0 & 0 & (\lambda-\lambda_0 \end{bmatrix}.$$

Sad se proces ponavlja na kofaktoru od 1; imamo po redu:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & (\lambda-\lambda_0)^2 \\ 0 & \lambda-\lambda_0 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -(\lambda-\lambda_0)^2 \\ 0 & 0 & (\lambda-\lambda_0)^3 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (\lambda-\lambda_0)^2 \end{bmatrix}.$$

To je traženi Smithov oblik matrice $\lambda - J$, pa očitavamo:

$$I_1 = 1, \quad I_2 = 1, \quad I_3 = (\lambda-\lambda_0)^3.$$

Dakle se pojavljuje jedan jedini invarijantni faktor $\neq 1$, i to $I_3 = (\lambda-\lambda_0)^3$.

18.6. Kao i kod matrica s konstantnim (postojanim) vrijednostima, tako se i ovdje vidi da se prelaz od zadane matrice $a(\lambda)$ na normirani njen oblik

$I(a)$ može izvršiti određenim predmnoženjem matricom $p(\lambda)$ i zamnoženjem matricom $q(\lambda)$, tako da je

$$p(\lambda)\, a\, q(\lambda) = \begin{bmatrix} I_1(a) & & & & & & 0 \\ & I_2(a) & & & & & \\ & & \ddots & & & & \\ & & & I_r(a) & & & \\ & & & & 0 & & \\ & 0 & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}; \tag{2}$$

pri tom $\det p(\lambda)$ i $\det q(\lambda)$ ne zavise od λ i obje su $\neq 0$ (isp. poglavlje 15 § 7.3).

18.6.1. Matrice $e(i, j)$. Pri tom znajmo ovo: ako $e(i, j)$ označuje kvadratnu matricu kojoj je vrijednost $=1$ u (i, j) a inače su joj vrijednosti $=0$, onda se za svako $i \neq j$ i svako λ matrica $(1 + \alpha e(i, j))\, a$ (odnosno matrica $a(1 + \alpha e(i, j)))$ dobije iz matrice a tako da se retku $a_{i\cdot}$ (stupcu $a_{\cdot i}$) doda $\alpha a_{\cdot j}$ (odnosno $\alpha a_{\cdot j}$).

18.6.2. Teorem 18.4. s dodacima 18.6—18.6.1. prenosi se neposredno na svaku matricu konačnog formata (n, n) s vrijednostima u bilo kojem asocijativnom prstenu $(A+, \cdot)$ s jedinicom i u kojem je svaki ideal glavni ideal (tj. oblika Ax za neko $x \in A$) (isp. poglavlje 6, § 12 nota[1]); takav je npr. prsten $(D, +, \cdot)$ cijelih racionalnih brojeva (pogl. 6, § 12.2). Na taj način imamo

18.6.3. Teorem. *Svaka kvadratna konačna matrica a s vrijednostima a_{ij} u D može se pomoću unimodularnih matrica p, q s komponentama iz D prevesti u oblik*

$$p\, a\, q = \begin{bmatrix} I_1(a) & & & & & & 0 \\ & I_2(a) & & & & & \\ & & \ddots & & & & \\ & & & I_r(a) & & & \\ & & & & 0 & & \\ & 0 & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

pri čemu je $I_\rho(a) > 0$ $(\rho = 1, 2, \ldots, r = \text{rang od } a)$ te $I_\rho \mid I_{\rho+1}$ *za svako* $\rho < r$.

18.7. Najveći zajednički djelitelj svih minora zadanog formata (determinantni divizori). Označimo sa $\mathrm{M}_k(a)$ ili $\mathrm{M}_k(a; \lambda)$ tzv. *determinantni faktor*: najveći zajednički djelitelj determinanata svih kvadratnih podmatrica reda k izvađenih iz matrice $a(\lambda)$. To vrijedi za $k = 1, 2, \ldots, n$.

To posebno znači da $\mathrm{M}_1(a) = \underset{i,k}{\mathrm{M}}\, a_{ik}(\lambda)$; nadalje, za kvadratnu matricu $a(\lambda)$ reda n znači to da je $\mathrm{M}_n(a) = \det a(\lambda)$. Također je jasno da svako $\mathrm{M}_k(a)$

dijeli svako $M_l(a)$ za $k<l$; to je posljedica Laplacova teorema o determinantama. Nadalje, po dogovoru: $M_k(a)=0$ za svako $k>r$.

Pri tom se držimo konvencije da je $M(0, 0, 0, \ldots)=0$ i da za svaki niz $n_1, n_2, \ldots$ vrijedi $M(n_1, n_2, \ldots)=M(n_1', n_2', \ldots)$, gdje je $n_1', n_2', \ldots$ maksimalni parcijalni podniz sa članovima $\neq 0$. Specijalno, svakom nizu brojeva među kojima ima bar jedan koji nije cio pridjeljujemo $M=1$. To je korisna konvencija.

18.7.1. Teorem. *Ako su matrice a, b ekvivalentne, tada je $M_i(a)=M_i(b)$, tj. λ-ekvivalentne matrice imaju jednake najveće zajedničke djelitelje determinanata svih kvadratnih podmatrica odgovarajućeg reda.*

Neka je

$$b(\lambda)=p\cdot a(\lambda)\cdot q.$$

Pogledajmo kako se izražava podmatrica c poretka s matrice $b(\lambda)$.

Dokaz. Neka je

$$c=b\begin{bmatrix}\alpha_1 & \alpha_2 \cdots \alpha_s\\ \beta_1 & \beta_2 \cdots \beta_s\end{bmatrix},$$

tj. neka c stoji u recima $b_{\alpha_1}\, b_{\alpha_2}, \ldots, b_{\alpha_s}$ i stupcima $b_{\cdot\beta_1}, b_{\cdot\beta_2}, \ldots, b_{\cdot\beta_s}$ matrice b. Opći član b_k^i je oblika

$$b_k^i=\sum_{j,l} p_j^i\, a_l^j\, q_k^l;$$

prelazeći na determinante, vidi se da je, po Binet-Cauchyjevoj formuli:

$$\det b\begin{bmatrix}\alpha_1 \cdots \alpha_s\\ \beta_1 \cdots \beta_s\end{bmatrix}=\sum \det p\begin{bmatrix}\alpha_1 \cdots \alpha_s\\ \gamma_1 \cdots \gamma_s\end{bmatrix}\det a\begin{bmatrix}\gamma_1 \cdots \gamma_s\\ \varphi_1 \cdots \varphi_s\end{bmatrix}\det q\begin{bmatrix}\varphi_1 \cdots \varphi_s\\ \beta_1 \cdots \beta_s\end{bmatrix};$$

pri tom se zbrajanje Σ vrši po svim strogo uzlaznim nizovima po s članova $\gamma_1<\gamma_2<\cdots<\gamma_s$ te $\varphi_1<\varphi_2<\cdots<\varphi_s$ u skladu sa širinom i visinom matrice a.

Gornja relacija kaže da je svaka zajednička mjera (dakle i najveća zajednička mjera $M_s(a)$) svih $\det a\begin{bmatrix}\gamma_1 \cdots \gamma_s\\ \varphi_1 \cdots \varphi_s\end{bmatrix}$ ujedno mjera svih determinanata kvadratnih matrica poretka s u b, pa je zato $M_s(a) \mid M_s(b)$. No, vrijedi i obrat; naime, ako je b λ-ekvivalentno sa a, tada je λ-ekvivalentno i a sa b; to znači da je također

$$M_s(b) \mid M_s(a), \text{ pa dakle } M_s(a)=M_s(b),$$

jer su polinomi $M_s(a)$, $M_s(b)$ normirani i istog stepena.

18.7.2. Prema teoremu 18.7.1. imamo, dakle:

$$\mathrm{M}_k(a) = \mathrm{M}_k \begin{bmatrix} I_1(a) & & & & & & \\ & I_2(a) & & & & & \\ & & \ddots & & & & \\ & & & I_r(a) & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}. \tag{3}$$

No, izraz na desnoj strani lako je odrediti, jer svaki član na dijagonali dijeli naredni; imamo $\mathrm{M}_1(a) = I_1(a)$, $\mathrm{M}_2(a) = I_1(a)\, I_2(a)$, ...

$$\mathrm{M}_k(a) = I_1(a)\, I_2(a) \cdots I_k(a) \quad \text{za } k = 1, 2, \ldots, n. \tag{4}$$

Odatle izlaze osnovne formule:

$$\begin{gathered} I_1(a) = \mathrm{M}_1(a) \\ \mathrm{M}_1(a)\, I_2(a) = \mathrm{M}_2(a) \ldots \\ \mathrm{M}_{k-1}(a)\, I_k(a) = \mathrm{M}_k(a), \quad I_k(a) = \frac{\mathrm{M}_k(a)}{\mathrm{M}_{k-1}(a)}. \end{gathered} \tag{5}$$

Time smo dobili stvarno značenje niza invarijantnih mnogočlana

$$I_1(a),\ I_2(a),\ \ldots,\ I_r(a).$$

⟶ **18.8. Osnovni teorem o λ-matricama.** ***Svaka λ-matrica a(λ), tj. svaka matrica kojoj su komponente a_{ik} algebarski polinomi $a_{ik}(\lambda)$ prema λ jest λ — ekvivalentna s pripadnom matricom***

$$\boldsymbol{Ia} = \begin{bmatrix} I_1(a) & & & & & \\ & \ddots & & & & \\ & & I_r(a) & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}, \tag{6}$$

pri čemu vrijedi (3), (4) i (5).

$M_k(a)$ znači najveći djelitelj determinanata svih kvadratnih podmatrica iz a poretka k. Broj r je rang matrice a.

18.9. Primjer Jordanove klijetke. Neka je zadan normiran polinom

$$c(\lambda) = c_0 + c_1\lambda + \cdots + c_{n-1}\lambda^{n-1} + \lambda^n;$$

pripadna Jordanova klijetka je suputnica polinoma $c(\lambda)$, tj.

$$J_c = \begin{bmatrix} 0 & & & & -c_0 \\ 1 & 0 & & & -c_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & & \\ & & & 1 & -c_{n-1} \end{bmatrix}$$

i ima karakterističnu matricu $\lambda - J_c$, za koju se lako vidi da je $\det(\lambda - J_c) = c(\lambda)$ (pomnoži n-ti redak sa λ i dodaj retku pred njim; u novoj determinanti $\det(\lambda - J_c)$ pomnoži redak $n-1$ sa λ i dodaj retku iznad, itd. dok se ne dođe do množenja drugog retka sa λ i dodavanja prvom; u dobivenoj matrici m je $m_{1n} = c(\lambda)$, svi ostali elementi u $m_{1\cdot}$ su 0, a komplement od m_{1n} je $(-1)^{n-1}$; dakle je

$$\det(\lambda - J_c) = \det m = (-1)^{n-1} \cdot (-1)^{n+1} \cdot c(\lambda) = c(\lambda)).$$

S druge strane, $M_{n-1} = 1$, jer je algebarski komplement od c_0 jednak 1 ili -1. Prema tome, invarijantni djelitelji su svi $=1$ osim posljednjeg:

$$M_n = \det(\lambda - J_c) = c(\lambda).$$

To ujedno znači da je $c(\lambda)$ minimalni polinom i svojstven polinom matrice J_c.

$\longrightarrow$ **18.10. Teorem.** *Da dvije λ-matrice budu λ-ekvivalentne, potrebno je i dovoljno da imaju isti format i iste invarijantne mnogočlane.*

Naime, matrica a je ekvivalentna s normalnim oblikom 18.8 (6); u njemu može najprije doći stanovit broj puta 1, a onda rastući polinomi; to znači da je $p\,a\,q = I(a)$ za neke regularne matrice p, q, pri čemu $\det p$, $\det q$ ne zavise od λ; no isti oblik ima i $I(b)$, pa je, dakle, za neke matrice P, Q također $P\,b\,Q = I(b) = I(a) = p\,a\,q$, tj. $P\,b\,Q = p\,a\,q$. Odatle se zaključuje da su a i b ekvivalentne; tako npr. odatle izlazi $b = P^{-1}\,p\,a\,q\,Q^{-1}$ pri tom determinante matricâ p, q, P, Q ne zavisi od λ. Obratno, ako su a, b λ-ekvivalentne, imaju one iste invarijantne djelitelje. To je posljedica teorema 18.6. i formula 18.7.2 (5).

18.11. Elementarni djelitelj matrice $a(\lambda)$. — **18.11.1.** Definicija. Pod *elementarnim djeliteljem* λ-matrice $a(\lambda)$ razumijevamo svaki polinom oblika $p(\lambda)^s$; pri tom je $p(\lambda)$ bilo koji *nerastavljiv* djelitelj kojeg invarijantnog djelitelja $I_\rho(a)$, i to tako da je $p(\lambda)^s \mid I_\rho$ ali nije $p(\lambda)^{s+1} \mid I_\rho$ ukoliko je $s > 0$ (isp. § 18.4).

Drugim riječima, provedimo faktorizaciju invarijantnih mnogočlana

$$I_1(a),\ I_2(a),\ \ldots,\ I_r(a) \text{ matrice } a \text{ (isp. § 18.5).}$$

18.11.2. Neka je $I(\lambda)$ bilo koji invarijantni djeljitelj matrice a koji nije konstantan (isp. § 18.4 i § 18.5); ako je $I(\lambda) \neq 1$, tada postoji rastav oblika

$$I(\lambda) = p_1(\lambda)^{s_1}\, p_2(\lambda)^{s_2} \cdots$$

pri čemu su $p_1(\lambda)$, $p_2(\lambda)$, ... nesvodljivi (ireducibilni) polinomi s glavnim koeficijentom $=1$; brojevi s_1, s_2, ... su >0. Polinomi $p_1(\lambda)^{s_1}$, $p_2(\lambda)^{s_2}$, ... zovu se *elementarni divizori invarijantnog djelitelja* $I(\lambda)$ matrice a.

18.11.3. Definicija. *Elementarnim divizorima matrice a nazivamo svaki elementarni divizor svakog invarijantnog nekonstantnog djelitelja matrice a.* Skup elementarnih divizora od a je sastavljen od elementarnih divizora d invarijantnih divizora od a, *pri čemu se d računa onoliko puta koliko se puta on ubraja kao elementarni divizor u nizu* $I_1(\lambda)$, $I_2(\lambda)$, ... *invarijantnih divizora od a* (Weierstrass [Vajerštras] 1868).

Z **18.11.4.** Skup svih elementarnih divizora od a je ***skup s ponavljanjem.***

18.11.5. Primjer. Matrici s invarijantnim divizorima

$$(\lambda+1)^3(\lambda-1)^2,\ (\lambda+1)^3(\lambda-1),\ (\lambda+1)(\lambda-1),\ \lambda+1 \tag{1}$$

pripada ovaj *skup s ponavljanjem* elementarnih divizora:

$$(\lambda+1)^3,\ (\lambda+1)^3,\ (\lambda+1),\ \lambda+1,\ (\lambda-1)^2,\ (\lambda-1),\ (\lambda-1). \tag{2}$$

Iz niza (2) može se rekonstruirati (1): najprije se izgrađuje produkt najviših potencija u (2) svih faktorâ koji su međusobno prosti (dobije se 1. član u (1)), zatim se s preostalim članovima niza (2) proces iterira: dobije se $(\lambda+1)^3\cdot(\lambda-1)$, tj. 2. član u (1), itd.

18.11.6. Primjedba. Ono što smo u § 16.2. zvali elementarnim djeliteljima obične matrice a (koja nije λ-matrica) jesu elementarni djelitelji λ-matrice

$$\lambda-a=\begin{bmatrix} \lambda-a_{11} & -a_{12}\cdot\cdot\cdot-a_{1n} \\ \cdot\cdot\cdot\cdot\cdot\cdot & \cdot\cdot\cdot\cdot\cdot\cdot \\ -a_{n1}\cdot\cdot\cdot & \cdot\lambda-a_{nn} \end{bmatrix}$$ (isp. § 16.2); rang joj je n.

$\longrightarrow$ **18.11.7. Teorem.** ***Dvije λ-matrice su ekvivalentne onda i samo onda ako imaju: iste elementarne djelitelje, isti rang i isti format.***

Naime, elementarni djelitelji određuju na jednoznačan način invarijantne djelitelje, i to ovako: produkt najviših potencija među elementarnim divizorima daje najviši invarijantni faktor; produkt narednog sloja elementarnih divizora daje naredni niži invarijantni polinom, itd. Na taj se način dobiju svi invarijantni faktori $\neq 1$, a onda se još na početak dijagonale pripiše onoliko puta broj 1 za koliko je rang r viši od broja invarijantnih faktora $\neq 1$, tj. onoliko puta koliko se puta i broj 1 pojavljuje kao invarijantan faktor.

Tako npr. ako je poredak λ-matrice a jednak 8, rang 4, a elementarni djelitelji $\neq 1$ jesu

$$(\lambda-1)^3,\ (\lambda+1)^2,\ (\lambda-1)^3,\ (\lambda+1),$$

tada imamo ove invarijantne faktore $\neq 1$:

$$(\lambda-1)^3(\lambda+1)^2,\ (\lambda-1)^3(\lambda+1).$$

Ima ih 2; zbog $r=4$, i brojevi 1, 1 su invarijantni faktori.

Smithov oblik matrice bio bi:

$$\operatorname{diag}[1,\ 1,\ (\lambda-1)^3(\lambda+1),\ (\lambda-1)^3(\lambda+1)^2,\ 0,\ 0,\ 0,\ 0].$$

18.11.8. *Skup elementarnih divizora i Jordanov oblik.* Ako su zadani elementarni divizori od a tada prema 18.5.1 možemo odmah svakom elementarnom divizoru $(\lambda-\lambda_0)^i$ pridijeliti pripadnu Jordanovu klijetku, a onda iz ovih klijetaka obrazovati kvazidijagonalnu matricu; najzad se pripiše preostali broj jedinica 1 i onda ostalo ispuni sa 0 (onoliko koliko traži produkt: dužina $\times$ širina matrice).

Time se dobije Jordanov zapis promatrane matrice.

Tako npr. ako elementarni djelitelji matrice reda 8 glase $(\lambda-2)^3$, $(\lambda-2)^3$, $(\lambda+1)$, tada je Jordanov oblik promatrane matrice a ovakav:

$$J=\begin{bmatrix} 2 & 1 & & & & & & \\ & 2 & 1 & & & & & \\ & & 2 & & & & & \\ & & & 2 & 1 & & & \\ & & & & 2 & 1 & & \\ & & & & & 2 & & \\ & & & & & & -1 & \\ & & & & & & & 0 \end{bmatrix}.$$

18.12. Specijalni slučaj λ-matrica. Pramen matrica. To je slučaj kad je svaki član matrice $a(\lambda)$ stepena ≤ 1 u odnosu na λ; pišemo li

$$a_{ik}(\lambda)=b_{ik}+c_{ik}\cdot\lambda,$$

znači to da za λ-matrice a, b, c vrijedi

$$a=b+c\cdot\lambda.$$

Prevođenje λ-matrice a praćeno je prevođenjem obiju matrica b i c.

Pa ako je λ-matrica a ekvivalentna nekoj matrici a', znači to da je

$$a'=paq=p\,(b+c\cdot\lambda)\,q=pbq+(pcq)\,\lambda,$$

tj. matrica a' je slične strukture: eksplicitno linearna s obzirom na λ, no koeficijenti p, q su λ-matrice. No, tim postupkom prevodimo zapravo dvije matrice b i c u jednostavniji oblik $b'=pbq$, $c'=pcq$, i to služeći se *istim* λ-transformacijama p, q. I obrnuto, želimo li dvije matrice b, c s istim domenom istodobno dijagonalizirati pomoću istih λ-transformacija, dovoljno je promatrati pripadni pramen matricâ $a(\lambda)=b+c\lambda$, pa raditi sa λ-matricom $a(\lambda)$ onako kako smo radili u ovom paragrafu.

18.13. Parovi bilinearnih forama. Pramenovi matrica dolaze i kad želimo da dvije kvadratne ili bilinearne forme prevedemo obje na normalni oblik: dovoljno je promatrati pramen matrica $a+\lambda b$ što pripada matricama a, b formi i onda λ-matricu $a+\lambda b$ dijagonalizirati, ukoliko je dijagonalizacija moguća. Dijagonalizacija je moguća ako je npr. b pozitivno definitivna kvadratna matrica (isp. GANTMAHER [1], 254, teor. 9).

Dodajmo i ovo. Ako su $a(\lambda)=a_0+a_1(\lambda)$, $b(\lambda)=b_0+b_1(\lambda)$ dva regularna matrična dvočlana (prema tome su a_0, a_1, b_0, b_1 matrice za koje je $\det a_1 \neq 0 \neq \det b_1$), pa ako su matrice $a(\lambda)$, $b(\lambda)$ λ-ekvivalentne matrice u smislu da je $b(\lambda)=p(\lambda)\,a(\lambda)\,q(\lambda)$ pvi čemu $\det p(\lambda)$ i $\det q(\lambda)$ ne zavise od λ, tada su matrice $b(\lambda)$, $a(\lambda)$ naprosto ekvivalentne (postoje konstantne regularne matrice p, q za koje je $b(\lambda)=paq$) (v. GANTMAHER [1], 122—124).

19. KORIJENSKI PROSTORI. JORDANOVE BAZE

19.1. Vidjeli smo da svakoj matrici a (odnosno linearnom operatoru A) u prostoru V_n odgovara Jordanov oblik A_J i da postoji regularan operator X sa svojstvom $X^{-1}AX=A_J$ (§ 18).

Kako odrediti bazu — zove se *Jordanova baza* — pa da u njoj operatoru A pripada upravo Jordanov zapis A_J?

Naravno, ako su svojstvene vrijednosti $\lambda_i \in \sigma_A$ sve međusobno različite i da ih ima n, tada je dovoljno za svako λ_i izabrati neki svojstven vektor e_i (dakle $ae_i = \lambda_i e_i$, $e_i \neq 0$), pa da dobijemo bazu $e = [e_1, e_2, \ldots, e_n]$ u kojoj je A zapisano dijagonalno. I u slučaju kad je A normalan operator ($AA^* = A^* A$) može se baza e izgraditi iz svojstvenih vektora (27, § 9.1). No, to nije moguće učiniti za operatore koji nisu normalni i imaju svojstvene vrednosti koji višestruko zadovoljavaju minimalni polinom $\mu(\lambda, a)$. Tada svojstvene vektore zamjenjuju »*korijenski vektori*«.

19.2. Korijenski prostor. Neka je $\lambda_i \in \sigma a$ (dakle $ax = \lambda_i x$, $x \neq 0$); skup svih vektora prostora V od kojih svaki zadovoljava jednadžbu

$$(a - \lambda_i)^k x = 0 \tag{1}$$

za bar jedan prirodni broj k (zavisan od x) zove se *korijenski prostor operatora* (*matrice*) *a pridružen svojstvenoj vrijednosti* λ_i. Označuje se sa

$$P_i = P(\lambda_i, a).$$

Neka je P_{ik} skup svih rješenja x jednadžbe (1); tada je naravno

$$P_{i1} \subset P_{i2} \subset P_{i3} \subset \cdots$$

$$P_i = P_{i1} \cup P_{i2} \cup P_{i3} \cup \cdots$$

Specijalno, P_{i1} je svojstveni prostor matrice a što pripada vrijednosti λ_i (27, § 2.4.4).

19.2.1. Korijenski vektor. Rješenje jednadžbe (1) u § 19.2 zove se *korijenski vektor matrice a* pridružen svojstvenoj vrijednosti λ_i i *pokazatelju k*.

19.3. Izborom pogodne vektorske baze u P_i i ulažući tu bazu u traženu bazu samog prostora V dobije se i sama tražena Jordanova baza u kojoj se operator a zapisuje kao a_J. Izbor prikladnih baza u P_i vrši se na osnovu činjenice da je $P_i = P_{ik}$ za neko k; naime, kako su P_{ik} potprostori od V koji, po pretpostavci, imaju konačno mnogo dimenzija, to ne može biti

$$P_{i1} \subsetneq P_{i2} \subsetneq \cdots \subsetneq P_{ik} \subsetneq P_{ik+1} \quad \text{za svako} \quad h = 1, 2, \ldots,$$

nego za neko k mora biti $P_{ik} = P_{ik+1}$; neka je n_i prvi takav broj k. Onda to znači da je

$$(a - \lambda_i)^{n_i} x = 0 \quad \text{za svako} \quad x \in P_i;$$

$$(a - \lambda_i)^{n_i - 1} x \neq 0$$

bar za jedno $x \in P_i$.

Drugim riječima, matrica $(a - \lambda_i)^{n_i}$ djeluje na P_i kao nula-matrica pa se i piše

$$(a - \lambda_i)^{n_i} \,|\, P_i = 0.$$

Kaže se također da je $(a - \lambda_i) \,|\, P_i$ nilpotentan operator i da mu je stepen nilpotentnosti jednak n_i (isp. 15, § 17.7.8).

19.4. Nilpotentni operatori.

19.4.1. Operator je *nilpotentan* ako mu je neka potencija jednaka nula-operatoru 0; prvi prirodni broj k za koji je $a^k=0$ zove se *stepen nilpotentnosti operatora a.*

19.4.2. Lema. ***Ako je m stepen nilpotentnosti operatora*** $a:V_n \to V_n$, ***tada je*** $m \leq n$ ***i*** λ^m ***je minimalni mnogočlan*** $\mu(\lambda)$ ***toga operatora.***

Kako naime $a^m=0$, mora, prema 24, § 2.4.7. polinom λ^m biti djeljiv sa $\mu(\lambda)$; zato je nužno $\mu(\lambda)=\lambda^k$; dakle je $k=m$ jer zbog $0=\mu(\lambda)=a^k$ ne može biti $k<m$.

$\longrightarrow$ **19.4.3. Teorem.** ***Ako je a nilpotentan stepena m, tada za svaki vektor*** $v \in V$ ***za koji je*** $a^{m-1}v \neq 0$ ***imamo m linearno nezavisnih vektora***

$$a^{m-1}v, \; a^{m-2}v, \ldots, a^2v, \; av, \; v \tag{1}$$

koji određuju određen potprostor $V_{(1)}$ ***sa svojstvom*** $aV_{(1)} \subset V_{(1)}$. ***Ako je*** $V_{(1)}=V$, ***tada zapis operatora a u bazi (1) glasi upravo***

$H(m)$=gornja nilpotentna Jordanova klijetka sa nulama na dijagonali.

Dokaz. Neka je

$$c_{m-1}a^{m-1}v+c_{m-2}a^{m-2}v+\cdots+c_1av+c_0v=0; \tag{2}$$

pri čemu su $c_{m-1}, \ldots, c_0$ skalari. Djelujemo li na (2) s lijeve strane sa a^{m-1}, tada zbog linearnosti izlazi (pišimo obratnim redom!):

$$c_0a^{m-1}v+a^m(c_1v+c_2av+\cdots+c_{m-1}a^{m-2}v)=0;$$

no, za taj drugi sastojak je $a^m(\quad)=0$ po definiciji broja m; zato prethodna jednakost postaje

$$c_0a^{m-1}v=0; \quad \text{odatle zbog} \quad a^{m-1}v \neq 0 \quad \text{izlazi} \quad c_0=0.$$

Imajući na umu nađenu relaciju $c_0=0$ dobije se, djelujući na (2) sa a^{m-2}, relaciju $c_1=0$; itd.: djelujući dalje sa a^{m-3} pa sa $a^{m-4}, \ldots$, sa a, dobije se redom $c_2=0$, $c_3=0, \ldots, c_{m-1}=0$. A to znači da su vektori (1) linearno nezavisni.

Očigledno je $V_{(1)}$ invarijantan potprostor. Djelujemo li operatorom a na vektore (1), prelaze oni u vektore:

$$0, \; a^{m-1}v, \; a^{m-2}v, \ldots, a^2v, \; av.$$

Ovi vektori, prema bazi (1), imaju upravo stupce matrice $H(m)$ kao svoje komponente.

19.4.4. Ako ciklički prostor $V_{(1)}$ što ga proizvode vektori (1) ne iscrpljuje prostor V, može se pokazati da postoji invarijantni potprostor $V_{(1)}'$ sa svojstvom da V bude direktna suma prostora $V_{(1)}$ i prostora $V_{(1)}'$ (dovoljno je s $V_{(1)}'$ označit invarijantni potprostor *maksimalne* dimenzije i sa svojstvom da je $V_{(1)} \cap V_{(1)}'=\{0\}$). Dakle je $V=V_{(1)} \oplus V_{(1)}'$.

Radeći dalje sa $V_{(1)}'$ kao maloprije sa V, dobije se ciklički potprostor $V_{(2)}$ i potprostor V_2' tako da bude $V_1' = V_2 \oplus V_2'$, dakle

$$V = V_1 \oplus V_2 \oplus V_2'.$$

Ako V_2' nije ciklički, možemo proces nastaviti i time nakon konačno mnogo koračaja doći do rastava

$$V = V_1 \oplus V_2 \oplus V_3 \oplus \cdots \oplus V_k,$$

pri čemu su sumandi ciklički prostori. Birajući u svakom sumandu cikličku bazu na način kao u V_1, zapisuje se podoperator $a \mid V_i$ kao Jordanova klijetka; unija tih podbaza daje bazu samog prostora V, pa se u njoj operator a zapisuje kvazidijagonalno nižući Jordanove klijetke po dijagonali.

19.4.5. Uloga nilpotentnog operatora. *Tako dakle svaki nilpotentni operator u $V_n = V$ daje povoda da se V prikaže kao direktna suma cikličkih potprostora i da se sam operator prikaže kvazidijagonalno nizanjem Jordanovih klijetaka.*

19.5. Određivanje Jordanove baze u korijenskom prostoru P_i.

19.5.1. Znajući da linearni operator $A \mid V$ dopušta Jordanov oblik a_J možemo korijenski prostor P_i iz § 19.2. direktno odrediti. Neka naime svojstvenoj vrijednosti λ_i kratnosti φ_i odgovaraju ovi elementarni divizori oblika $(\lambda - \lambda_i)^k$:

$$(\lambda - \lambda_i)^{e_{i1}},\ (\lambda - \lambda_i)^{e_{i2}},\ \ldots,\ (\lambda - \lambda_i)^{e_{ij_i}}$$

Tim elementarnim djeliteljima (ima ih j_i) odgovara isto toliko pripadnih Jordanovih klijetaka

$$\lambda_i + H(e_{i1}),\ \ldots,\ \lambda_i + H(e_{ij_i})$$

nanizanih po dijagonali matrice a_J, i u kojima su na dijagonali smješteni λ_i i ništa drugo. Zato u matrici

$$(1) \qquad a_J - \lambda_i$$

u odgovarajućih j_i klijetaka stoje same nule na glavnoj dijagonali; svaka od tih klijetaka je singularna matrica s defektom 1; zato je defekt matrice (1) jednak j_i. To znači (isp. pogl. 13, § 8.3) da rješenja jednadžbe

$$(a_J - \lambda_i)\, x = 0$$

daju određen prostor P_{i1} dimenzije j_i.

19.5.2. I matrica

$$(2) \qquad (a_J - \lambda_i)^2$$

je kvazidijagonalna, a vidi se da iz $a_J - \lambda_i$ izlazi kvadrirajući joj svaku klijetku. No, tim kvadriranjem pomiče se dijagonala za 1 i gubi jedno 1 u svakoj od uočenih j_i klijetaka dužine > 1; time se rang matrice (1) umanjuje za toliko izgubljenih jedinica, odnosno za isti broj jedinica povećava se defekt matrice (2). To znači da ćemo rješavajući jednadžbu

(3) $$(a_J-\lambda_i)^2 x=0$$

doći i do novih rješenja $x^{(2)}$ koja nisu u P_{i1}.

No jednadžba (3) *upravo znači da je*

(4) $$(a-\lambda_i)\, x^{(2)}=x^{(1)}, \quad \textit{gdje je} \quad x^{(1)}\in P_{i1}.$$

19.5.3. Isto bismo dalje zaključili da za svako eventualno $x^{(3)}$ iz $P_{i3}\setminus P_{i2}$ vrijedi

(5) $$(a-\lambda_i)\, x^{(3)}=x^{(2)}$$

za određeno $x^{(2)}\in P_{i2}$, itd. (pri tom $x^{(2)}$ iz (5) ne mora biti ono isto $x^{(2)}$ iz (4)).

Među vektorima $x^{(1)}$ ima upravo j_i linearno nezavisnih:

(6) $$\operatorname{def}(a_J-\lambda_i)=j_i;$$

neka su to vektori

$$x_{i1}{}^{(1)},\ x_{i2}{}^{(1)},\ \ldots,\ x_{ij_i}{}^{(1)}.$$

Među vektorima $x^{(2)}$ ima određen maksimalan broj linearno nezavisnih; itd. slično za vektore oblika $x^{(3)}$, $x^{(4)}$ ukoliko postoje.

Ispišimo sve te linearno nezavisne vektore tako da one koji su pridruženi istoj Jordanovoj klijetki pišemo jedne do drugih; time se dobija željena baza $e(i)$ korijenskog prostora P_i vezanog za λ_i.

Učinimo li odgovarajuću stvar za svako $\lambda_i\in\sigma_a$, dobit će se željena baza

(7) $$x=e(1),\ e(2),\ \ldots$$

samog prostora V. Nije teško pokazati da matrica (7) — stupci su joj: stupci matrice $e(1)$, matrice $e(2)$, itd. ima svojstvo da je

$$a\,x=x\,a_J,$$

dakle

$$x^{-1}\,a\,x=a_J.$$

To znači da *izborom stupaca matrice x kao nove baze, matrica (odnosno operator) a dobiva upravo Jordanov zapis a_J.*

Posebno je pitanje kako će se odrediti korijenski vektor $x^{(2)}$, $x^{(3)}$, ... (korijenske vektore $x^{(1)}$ znamo određivati jer su to svojstveni vektori pridruženi vrijednosti λ_i).

Naime za razliku od jednadžbe $(a-\lambda_i)\,x=0$ koja je homogena, preostale jednadžbe (4), (5), nisu homogene, pa za njihovo postojanje imamo određene kriterije (pogl. 14, § 0.3). Posebno, zbog singularnosti matrica

$$(a-\lambda_i)^2,\ (a-\lambda_i)^3,\ \ldots,$$

bit će redići svake od tih matrica međusobno vezani linearno. Specijalno će postojati konstante $y_1, y_2, \ldots$ (ne sve $=0$) za koje će vrijediti

(8) $$y_1(a-\lambda_i)_{1\cdot}+y_2(a-\lambda_i)_{2\cdot}+\cdots=0.$$

Za iste te konstante y_k prema Capelli-Kroneckerovu teoremu (v. 14, § 0.3) primenjenom na (4) vektor $x^{(1)}=[x_1^{(1)}, x_2^{(1)}, \ldots]$ ispunjava uslov

(9) $$y_1 x_1^{(1)}+y_2 x_2^{(1)}+\cdots=0; \qquad \text{tj.}$$

$$(a-\lambda)^T\vec{y}=0, \quad \text{gdje je} \quad y=[y_1, y_2 \cdots]^T; \quad \text{dakle je}$$

(10) $$(a^T-\lambda_i)\,y=0.$$

19.5.4. Drugim riječima, vektor y koji se pojavljuje u uslovnoj jednadžbi (8) odnosno (9) jest svojstven λ_i-vektor transponata a^T zadane matrice a (isp. pogl. 27, § 8.4); pomoću y i veze (9) suzuje se sloboda ulaženja vektora $x^{(1)}$ iz P_{i1} u jednadžbu (4); prikazujući $x^{(1)}$ kao linearnu kombinaciju osnovnih vektora neke baze e prostora P_{i1}, dobiju se neke relacije među koeficijentima te linearne veze, pa to doprinosi izboru članova baze.

19.5.5. Inače sam prostor P_i možemo odrediti direktno rješavajući homogeni sistem $(a-\lambda_i)^{k_i}x=0$, pri čemu je k_i kratnost od λ_i za svojstveni polinom $\varkappa(\lambda, a)$ matrice a.

Naime iz osnovnog teorema 15.10 izlazi posebno ovaj

⟶ **19.6. Teorem. (0)** ***Dimenzija korijenskog prostora P_i koji je pridružen svojstvenoj vrijednosti λ_i matrice a jednaka je kratnosti k_i vrijednosti λ_i u odnosu na svojstveni polinom $\varkappa(\lambda, a)$ matrice a.***

(0 0) ***Čitav prostor V_n od konačno mnogo dimenzija je direktna suma korijenskih prostora koji su pridruženi bilo kojem linearnom operatoru a koji djeluje iz V u V.***

19.7. Slučaj normalnih operatora. Za normalne matrice $(aa^*=a^*a)$ znamo da već svojstveni prostor P_{i1} ima dimenziju k_i jer je defekt matrice $a-\lambda_i$ jednak kratnosti od λ_i (pogl. 27, § 9.4); dakle je $P_{i1}=P_i$; odatle izlazi da matrice $a-\lambda_i$, $(a-\lambda_i)^2$ imaju isti defekt pa sve Jordanove klijetke moraju biti jednočlane: Jordanov oblik prelazi u dijagonalni oblik. Odatle izlazi posebno

19.7.1. Korolar. Elementarni djelitelji svake kompleksne kvadratne normalne matrice jesu linearni i oblika $\lambda-\lambda_i$; posebno to vrijedi za hermitske operatore.

⟶ **19.8. Teorem.** ***Ako je matrica slična dijagonalnoj matrici, onda su njeni elementarni divizori linearni; i obrnuto. Odnosno: ako se linearan operator u V_n može zapisati dijagonalno, onda su njegovi elementarni divizori linearni; i obrnuto.***

20. Zadaci o svojstvenim vrijednostima i oblicima matrica.

1. Odredi spektar matrice a iz pogl. 16, § 2.9.4.
2. Isto pitanje za pogl. 15, § 2.5.4.
3. Odredi: 1) elementarne djelitelje;
   2) Jordanov oblik matricâ A, B, C iz pogl. 10, § 4.7.9.

4. Isto pitanje za matrice iz pogl. 10, § 4.7.10.

5. Isto pitanje za matrice iz pogl. 10, § 4.7.11.

6. Isto pitanje za matricu $1'(n)$ = sporedna diag. [1 1 1 · · · 1]; npr.

$$1'(3)=\begin{bmatrix} & & 1 \\ & 1 & \\ 1 & & \end{bmatrix}.$$

7. Naći elementarne divizore matrice

$$a=\begin{bmatrix} \lambda^2+2 & \lambda^2+1 & \lambda^2+1 \\ 3 & \lambda^2+1 & 3 \\ \lambda^2+1 & \lambda^2+1 & \lambda^2+1 \end{bmatrix}$$

nad tijelom 1) racionalnih, 2) realnih, 3) kompleksnih brojeva.

8. Odredi korijenske prostore za svaku matricu iz zadataka 3—6 kao i vektorsku bazu u kojoj se matrica zapisuje kao Jordanov oblik.

9. Neka je V skup svih realnih izvodljivih (derivabilnih) funkcija s oblasti R; neka je D operator deriviranja; dokaži da je svako $c \in R$ svojstvena vrijednost od D i da je e^{ct} pripadni svojstveni vektor, a

$$(c_0+c_1 t+c_2 t^2+\cdots+c_k t^k)\, e^{ct}$$

jesu pripadni korijenski vektori.

10. Ako konačna trokutna matrica ◺ (odnosno ◹) na dijagonali nema jednakih vrijednosti, tada n svojstvenih vektora koji odgovaraju vrijednostima na dijagonali obrazuju opet trokutnu matricu istog oblika.

11. 1) Za kvadradne matrice a, b matrice ab, ba imaju isti stojstveni polinom i isti spektar;

 2) za nekvadratne matrice a, b za koje postoji ab, ba vrijedi $\varkappa(\lambda, ba)=$ $=\lambda^{n-m}\varkappa(\lambda, ab)$, pri čemu je $\operatorname{Dom} a=(m, n)$, $m<n$.

12. Kako izgleda Jordanov oblik 1) idempotentne matrice $(a^2=a)$;

 2) involutivne matrice $(a^2=1)$;

 3) periodičke matrice $(a^m=1)$ za neki prirodni broj m)?

13. Odredi 1) svojstveni polinom $\varkappa$, 2) minimalni polinom μ, 3) invarijantne divizore, 4) determinantne faktore matrice kojoj su red i elementarni djelitelji:

 1) $n=3$, $(\lambda-2)^3$; 2) $n=3$, $(\lambda-2)^2$, $(\lambda-2)$;

 3) $n=3$, $\lambda-2$, $\lambda-2$, $\lambda-2$; 4) $n=3$, $\lambda-2$, $\lambda+2, \lambda+2$;

 5) $n=3$ $(\lambda-2)^2$, $\lambda+2$; 6) $n=5$, $(\lambda+2)^5$; 7) $(\lambda+2)^4$, $\lambda+3$;

 8) $(\lambda+2)^2$, $(\lambda+2)^2$, $\lambda+2$; 9) $(\lambda+2)^3$, $(\lambda-3)^2$;

 10) $n=6$, $(\lambda+2)^4$, $(\lambda-2)^2$; 11) $(\lambda+2)^3$, $(\lambda+2)^2$, $(\lambda+2)$.

14. Neka je spektar σ_a matrice a jednak $\sigma_a = \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$; neka vrijednosti λ_i odgovara u Jordanovu obliku j_i klijetaka u kojima je λ_i na dijagonali i to širine $\sigma_{i1}, \sigma_{i2}, \ldots, \sigma_{ij_i}$; tada se pod *Segreovom karakteristikom od a* podrazumijeva niz

$$[(\sigma_{11}, \sigma_{12}, \ldots, \sigma_{1j_1})\,(\sigma_{21} \ldots \sigma_{2j_2}) \ldots (\sigma_{m1} \ldots \sigma_{mj_m})];$$

odredi matricu kojoj je Segreova karakteristika: 1) (2); 2) [(3) (1)]; 3) [(3) (1) (1)], [(2, 2), 1] a spektar joj je {5}, odnosno {5, 2}, odnosno {5, 2, 4} odnosno {5, 4}.

15. *Weyrova karakteristika matrice.* Neka je k_i kratnost svojstvene vrijednosti λ_i matrice a; tada se niz brojeva

$$\alpha_{i1} = \mathrm{Def}\,(a-\lambda_i),\ \alpha_{i2} = \mathrm{Def}\,(a-\lambda_i)^2 - \alpha_{i1}, \ldots, \alpha_{ik_i} =$$
$$= \mathrm{Def}\,(a-\lambda_i)^{k_i} - \alpha_{ik_{i-1}}$$

(Def = defekt) zove Weyrova karakteristika matrice a u vezi sa λ_i; označuje se sa $[\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ik_i}]$; pustimo λ_i varirati u σ_a.

Niz $[[\alpha_{11} \cdots \alpha_{1k_1}], [\alpha_{21} \cdots \alpha_{2k_2}] \cdots]$ zove se *Weyrova karakteristika matrice a.* Tako npr. Weyrova karakteristika od

$$a = \begin{bmatrix} 3 & 1 & & & \\ & 3 & & & \\ & & 3 & 1 & \\ & & & 3 & \\ & & & & 2 \end{bmatrix}$$

glasi [[2 2], [1]]. Odredi Weyrovu karakteristiku

1) matrica iz zad. 13, odnosno ovih matrica;

$$2) \begin{bmatrix} 2 & 1 & & \\ & 2 & & \\ & & 3 & 1 \\ & & & 3 \end{bmatrix}, \quad 3) \begin{bmatrix} 2 & & & & \\ & 2 & 1 & & \\ & & 2 & & \\ & & & 3 & 1 \\ & & & & 3 \end{bmatrix}, \quad 4) \begin{bmatrix} 2 & 1 & & \\ & 2 & 1 & \\ & & 2 & 1 \\ & & & 2 \end{bmatrix}.$$

16. Dokaži da se svaki invarijantni potprostor u odnosu na operator A može prikazati kao direktna suma presjeka toga potprostora s korijenskim potprostorima operatora A.

17. Neka je $P_{in_i} = P_{in_i+1}$ (oznake su kao u § 19.3); neka je e^{n_i} baza u P_{in_i} u odnosu na potprostor P_{in_i-1} (tj. e^{n_i} je maksimalan niz linearno nezavisnih vektora sa svojstvom da se pomoću njih i pomoću vektorâ iz P_{in_i-1} može prikazati svaki član u P_{in_i}); i niz $(a-\lambda_i)\,e^{n_i}$ koji se dobije iz e^{n_i} djelovanjem operatora $a-\lambda_i$ je sastavljen od linearno nezavisnih članova (ima ih $\dim P_{in_i} - \dim P_{in_i-1}$); pomoću e^{n_i-1} nadopunimo ga do neke baze potprostora P_{in_i-1} u odnosu na P_{in_i-2}; itd.

Induktivno, dobije se tako ovakav dvostruki niz

e^{n_i} (baza od P_{in_i} u odnosu na P_{in_i-1})

$(a-\lambda_i)\, e^{n_i} \quad e^{n_i-1}$ (baza od P_{in_i-1} u odnosu P_{in_i-2}).

$(a-\lambda_i)^2\, e^{n_i} \quad (a-\lambda_i)\, e^{n_i-1}$

. . . .

$(a-\lambda_i)^{n_i}\, e^{n_i-1}\ (a-\lambda_i)^{n_i-2}\, e^{n_i-1},\ (a-\lambda_i)^{n_i-3}\, e^{n_i-2}, \ldots$

(baza od P_{i2} prema P_{i1}).

Čitajući tako dobiven dvostruki niz vektora po stupcima odozdo prema gore dobije se Jordanova baza u korijenskom prostoru P_i. Radeći to za svako $\lambda_i \in \sigma_a$, dobije se Jordanova baza samog prostora V.

18. Dokaži da je svaka λ-matrica konačnog formata oblika

$$a_0 + a_1 \lambda + a_2 \lambda^2 + \cdots + a_n \lambda^n,$$

pri čemu su $a_0, a_1, \ldots, a_n$ matrice.

L i t e r a t u r a: Vidi literaturu za poglavlje 23.

POGLAVLJE 28.

ORTONORMIRANE MATRICE

Uloga je *ortogonalnih* ili bolje: *ortonormiranih matrica* da služe kao matematički aparat za prikazivanje *rotacija u prostoru*, odnosno za opisivanje prelaza iz jedne ortonormirane baze vektorâ u drugu ortonormiranu vektorsku bazu (radimo u euklidskim prostorima; analogon u unitarnim ili hermitskim prostorima su *unitarne matrice*).

1. OSNOVNI PROBLEM I DEFINICIJA ORTONORMIRANIH MATRICA

1.1. Osnovni problem. Zadan je skalarni produkt

(1) $$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

Pišemo ga matrično

(2) $$y^T x, \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \end{bmatrix}, \quad y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \end{bmatrix}.$$

Provedimo promjenu:

(3) $$x = bx', \quad y = cy'.$$

Time (1), odnosno (2) prelaze u

$$(cy')^T (bx') = y'^T c^T bx' = y'^T (c^T b) x'.$$

Dakle: $$y^T x = y'^T (c^T b) x'.$$

Ovaj će izraz imati oblik kao i polazni, tj. bit će

(*) $$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = x_1' y_1' + \cdots + x_n' y_n'$$

onda i samo onda ako je

$$c^T b = 1.$$

Specijalno, ako je $b = c$, dolazi se do uslova $c^T c = 1$, koji se piše i ovako: $c^{-1} = c^T$. To je definicija ortogonalne matrice.

1.2. Definicija. Kvadratna matrica ω je *ortogonalna* ili *ortonormirana* ako joj je transponat jednak s inverzom, tj. ako je

$$(1) \qquad \omega^T = \omega^{-1}.$$

Ortogonalnu matricu označivat ćemo obično sa ω (da nas podsjeti na rotaciju).

1.2.1. Primjedba. Imajući na umu kako je *teško sprovesti inverziju opće matrice*, uočimo da se *inverzija ortogonalne matrice sprovodi naprosto transponiranjem!*

1.3. Kontragredijent matrice. Ako u definicionoj jednakosti (1) uzmemo operator T, izlazi

$$(2) \qquad \omega = (\omega^{-1})^T = \omega^{\sim} = (\omega^T)^{-1}.$$

Matrica $(c^{-1})^T$, odnosno $(c^T)^{-1}$ zove se *kontragredijent matrice* c. Relacija (2) pokazuje *da je matrica ortogonalna onda i samo onda ako se podudara sa svojim kontragredijentom.*

Ovo svojstvo je bliže svrsi nego formalna definicija (1) jer bolje odražava osnovnu jednakost (*): promjene što doživljuju veličine x_i neutraliziraju se promjenama veličinâ y_k.

1.4. No, znamo (v. 12 § 5.2) da je za svaku regularnu matricu c

$$(c^{-1})_{ik} = \frac{f c_{ki}}{\det c};$$

$$(c^{-1})^T_{ik} = \frac{f c_{ik}}{\det c},$$

tj. za ortogonalne matrice imamo

$$(3) \qquad \omega_{ik} = \frac{f \omega_{ik}}{\det \omega}$$

(pazi! isti redoslijed indeksa lijevo i desno); pri tom $f\omega_{ik}$ označuje *algebarski kofaktor* elementa ω_{ik} u matrici ω.

Relacija (3) je vrlo pogodna za rad s ortogonalnim matricama.

Npr. matrica

$$\omega = \begin{bmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{bmatrix}$$

je ortogonalna; tako npr. $f \sin\varphi = -\sin\varphi \cdot (-1)^3 = \sin\varphi$.

Matrica $$d = \begin{bmatrix} 2 & 1 \\ 4 & 0 \end{bmatrix}$$

nije ortogonalna jer je njen kontragredijent

$$d^{\sim} = -\frac{1}{4} \begin{bmatrix} 0 & -4 \\ -1 & 2 \end{bmatrix}$$

dakle $\neq d$. Jedinična matrica je ortogonalna. Ortogonalna je i svaka matrica koja iz jedinične matrice 1_n nastaje permutacijom stupaca (redaka). Tako npr. permutacija 4 3 1 2 stupaca u matrici 1 (4) daje ovu ortogonalnu matricu:

$$[(1_4)_{\cdot 4}\ (1_4)_{\cdot 3}\ (1_4)_{\cdot 1}\ (1_4)_{\cdot 2}] = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

1.5. Teorem. *Determinanta svake ortogonalne realne matrice je* 1 *ili* -1.

Iz definicije (1) izlazi $\omega^T \omega = 1$; odatle

$$\det(\omega^T \omega) = 1 \Rightarrow \det \omega^T \det \omega = 1 \Rightarrow \det \omega \det \omega = 1 \Rightarrow \det \omega = \pm 1.$$

2. GLAVNI ILI DUGI TEOREM O ORTOGONALNIM MATRICAMA

2.1. ***Za svaku kvadratnu konačnu realnu matricu*** ω ***ovih* 10 *svojstava međusobno je ravnopravno*:**

(I) $$\omega^T = \omega^{-1}.$$

(II) $$\omega = \omega^{\sim}, \quad \textit{gdje je} \quad \omega^{\sim} = (\omega^{-1})^T.$$

(III) $$\omega^T \omega = \mathbf{1},$$

tj. stupci matrice čine ortonormiran niz vektora.

(IV) $$\omega\, \omega^T = \mathbf{1}.$$

tj. reci matrice čine ortonormiran niz vektora.

(V) ***Za svaki niz realnih brojeva*** $x^T = [x_1, x_2, \ldots, x_n]$ ***i supstituciju*** $x = \omega x'$ ***vrijedi*** $x_1^2 + x_2^2 + \cdots + x_n^2 = x_1'^2 + x_2'^2 + \cdots + x_n'^2$.

(VI) ***Skalarni kvadrat svakog vektora je invarijantan pri prelazu iz jedne ortonormirane baze e u drugu*** $e' = e\,\omega$.

(VII) $x_1 y_1 + \cdots + x_n y_n = x_1' y_1' + \cdots + x_n' y_n'$, ***ako je*** $x = \omega x'$, $y = \omega y'$.

(VIII) ***Skalarni produkt bilo kojih dvaju vektora ne mijenja se pri prelazu iz ortonormirane baze e u bazu*** $e' = e\,\omega$.

(IX) ***Ako je vektorska baza e ortonormirana, onda je to i*** $e\,\omega$.

(X) ***Preslikavanje*** $x \rightarrow \omega x$ ***je realno i pripada mu potpuna ortonormirana rotacija čitava prostora oko* 0 *u smislu da je*** $|x| = |\omega x|$. ***(stavljamo*** $|x| = +(x^T x)^{1/2} = +(N x)^{1/2}$, ***(tačke*** x ***i*** ωx ***jednako su daleko od* 0). *Veličina kutova se ne mijenja; orijentacija kutova je ista ili suprotna, već prema tome da li je*** $\det \omega = \mathbf{1}$ ***ili*** $\det \omega = -\mathbf{1}$.

Svako to svojstvo pripada ortogonalnoj matrici i izvire iz svakog drugog od tih nabrojenih svojstava.

2.2. D o k a z **2.2.1.** (I) $\Leftrightarrow$ (II) (uzmi operator T u (I), odnosno u (II)): simbolički $(\mathrm{I})^T \Leftrightarrow$ (II), $\mathrm{II}^T = \mathrm{I}$.

2.2.2. $(\mathrm{I})\,\omega = \mathrm{III}$ (značenje je jasno: (I) pomnoži zdesna sa ω).

2.2.3. $\mathrm{I} = \mathrm{III}\,\omega^{-1}$.

2.2.4. $\omega\,\mathrm{I} = \mathrm{IV}$ (predmnoži I sa ω, tj. ω pomnoži sa $\omega^T = \omega^{-1}$).

2.2.5. $\mathrm{I} = \omega^{-1}\,\mathrm{IV}$.

2.2.6. III $\Rightarrow$ V. Supstitucijom $x = \omega\,x'$ prelazi zadani izraz $\sum x_i^2 = x^T x$ u

$$(\omega\,x')^T(\omega\,x') = x'^T(\omega^T\omega)\,x' = x'^T x' = \sum x_i'^2.$$

2.2.7. V $\Rightarrow$ III: čitaj unatrag gornji dokaz III $\Rightarrow$ V.

2.2.8. V $\Rightarrow$ VI. Pa neka je $e' = e\,\omega$. Prema osnovnoj relaciji $e v_e = e' v_{e'}$ (pogl. 21, § 3.8) za zapise $v_e, v_{e'}$ istog vektora v znači to da je $e v_e = e\,\omega\,v_{e'}$, tj. $v_e = \omega\,v_{e'}$.

Zato prema pretpostavci V izlazi odatle da je $v_e^T v_e = v_{e'}^T v_{e'}$, što se i traži izrekom VI.

2.2.9. Na isti način se dokazuje VII $\Rightarrow$ VIII.

2.2.10. III $\Rightarrow$ VII. Dokaz isti kao III $\Rightarrow$ VI.

2.2.11. I $\Rightarrow$ IX. Treba dokazati da I $\Rightarrow (e\,\omega)^T(e\,\omega) = 1$. No, to se odmah vidi pišući $(e\,\omega)^T = \omega^T e^T$ i znajući da je $e^T e = 1$.

2.2.12. IX $\Rightarrow$ III. Dovoljno je za e uzeti jediničnu matricu.

2.2.13. Najprije III $\Rightarrow$ X.

Naime,

$$|\,\omega\,x\,| = +((\omega\,x)^T\,\omega\,x)^{1/2} = (x^T\,\omega^T\,\omega\,x)^{1/2} = (x^T x)^{1/2} = |\,x\,|.$$

Nadalje, za svaki par vektora $x, y \neq \vec{0}$ imamo:

$$\cos(x, y) = \frac{y^T x}{(N x)^{1/2}(N y)^{1/2}} = (\text{stavlja se } z' = \omega\,z,\ \omega^{-1} z' = z \text{ za } z = x, y) =$$

$$= \frac{(\omega^{-1} y')^T(\omega^{-1} x')}{(N\,\omega^{-1} x')(N\,\omega^{-1} y')^{1/2}} = \frac{y'^T(\omega^{-1})^T\omega^{-1} x'}{((\omega^{-1} x')^T(\omega^{-1} x')(\omega^{-1} y')^T\omega^{-1} y')^{1/2}} =$$

$$= (\text{prelazeći u III na inverze}) = \frac{y'^T x'}{x'^T x' \cdot y'^T y'} = \cos(x', y').$$

2.2.14. X $\Rightarrow$ III. Dokaz se razabire iz dokaza 2.2.13.

2.3. Time je dokazan gornji teorem koji zapravo obuhvata $10 \cdot 9 = 90$ teoremâ.

Zanimljivo je preispitati koji je najkraći dokaz svakog od tih 90 teorema. Provjerite da nije ništa ispušteno: svaki od sudova I — X upotrijebljen je i kao pretpostavka i kao zaključak.

Posebno ukazujemo na ekvivalenciju $\omega^T \omega = 1 \Leftrightarrow \omega\omega^T = 1$ (ta ekvivalencija ne stoji za beskonačne matrice). Iz te ekvivalencije proizlazi, između ostaloga, da je ω normalno ($\omega^T \omega = \omega\omega^T$).

3. TIPIČAN SLUČAJ KAKO NASTAJU ORTONORMIRANE MATRICE

⟶ **3.1. Teorem.** ***Ako je e jedna ortonormirana baza, a e' druga, tada je prelaz od prve u drugu: $e' = e \cdot c$ izvršen potpuno određenom matricom c, koja je nužno ortonormirana; pri tom je***

(1) $$c_{ik} = \cos(e_i, e_k') \text{ ili tabelarno:}$$

$$e' = e \cdot c \qquad e'_{ik} = \sum_j e_{ij} c_{jk} \qquad \begin{array}{c|ccccc} & e_1' & e_2' & \cdot & e_k' & e_n' \\ \hline e_1 & & & & \cdot & \\ e_2 & & & & \cdot & \\ \vdots & & & & \cdot & \\ e_i & \cdot & \cdot & \cdot & c_{ik} = \cos(e_i, e_k') & \\ e_n & & & & & \end{array}$$

(*lako se pamti mnemotehnički*: $c \to \cos \quad c_{ik} \to \cos(e_i, e_k')$)

Tabela: osnovna veza među ortonormiranim bazama.

D o k a z. Relacija $e' = ec$ znači da je

$$e'_k := e_1 c_{1k} + e_2 c_{2k} + \cdots + e_i c_{ik} + \cdots + e_n c_{nk}.$$

Odatle

$$e_i^T e'_k = e_i^T e_1 c_{1k} + e_i^T e_2 c_{2k} + \cdots + \underbrace{e_i^T e_i}_{1} c_{ik} + \cdots + \underbrace{e_i^T e_n}_{=0} c_{nk}$$

$$e_i^T e'_k = c_{ik}, \text{ tj. } c_{ik} = e_i^T e'_k =$$

$$\underbrace{(N e_i)^{1/2}}_{1} \underbrace{N(e'_k)^{1/2}}_{1} \cos(e_i, e_k') = \cos(e_i, e'_k);$$

dakle je zaista (1) na snazi.

⟶ **3.2. Teorem (cos-zapis ortogonalnih matrica).** *Svakoj ortogonalnoj matrici ω reda n pripada jedna jedina kvadratna matrica $[\alpha_{ik}]$ istog reda n sa svojstvom da je $\omega_{ik} = \cos \alpha_{ik}$, $0 \leq \alpha_{ik} \leq \pi$.*

Teorem se očitava s gornje tabele. No, ipak, dokažimo ga! Neka je, dakle, ω ortogonalna matrica: neka je, nadalje, $e = e_1, \ldots, e_n$ proizvoljna ortonormirana baza; nađimo $e' = e\,\omega$; e' je opet baza, i to ortonormirana; e' je jednoznačno određeno kao produkt matrica e i ω; no time ω kao prevodna matrica baze e u bazu e' ima oblik c_{ik} iz gornjeg teorema, tj. $\omega_{ik} = \cos(e_i, e'_k)$; time je $\sphericalangle(e_i, e'_k)$ jednoznačno određen zahtjevom da mu veličina bude u zatvorenom intervalu $R[0, \pi]$. Q. E. D.

4. GRUPA ORTONORMIRANIH MATRICA

Sva su gornja razmatranja mala posljedica izreke:

⟶ **4.1. Teorem.** ***Ortonormirane matrice reda n čine množidbenu grupu (tzv. ortogonalnu grupu O_n od n varijabli). Specijalno, u tročlanoj relaciji***

$$\omega\omega' = \omega'' \tag{1}$$

pretpostavka da je bilo koji dvočlan podniz od $\omega, \omega', \omega''$ sastavljen od ortonormiranih matrica ima za posljedicu da je i preostali član ortonormirana matrica.

Time je ukratko, na jeziku teorije grupa, iskazano mnogo toga u vezi s promjenama koordinatnih baza i koordinata.

4.2. Lema. *Ako su a, b ortonormirane matrice (s determinantom 1 svaka), tada je to i ab.*

Naime, iz $a^T = a^{-1}$, $b^T = b^{-1}$ izlazi $b^T a^T = b^{-1} a^{-1}$, tj. $(ab)^T = (ab)^{-1}$, što se i tvrdilo, (ono o determinanti je očigledno jer je $\det ab = \det a \det b = \pm 1 \cdot \pm 1 = \pm 1$). Dakle imamo posla s grupoidom. Zakon asocijacije je na snazi.

Jedinična matrica je očigledno ortonormirana.

Još treba da pokažemo da je i ω^{-1} ortonormirano kad je to ω.

No, iz $\omega^T = \omega^{-1}$ izlazi $(\omega^T)^{-1} = (\omega^{-1})^{-1}$, što zbog $(\omega^T)^{-1} = (\omega^{-1})^T$ daje traženu relaciju $(\omega^{-1})^T = (\omega^{-1})^{-1}$, koja kaže da je ω^{-1} ortonormirano.

Time je na jednostavan način dokazana jedna osnovna stvar koja se neprestano javlja u matematici.

Ono o međuzavisnosti u tročlanoj relaciji (1) neposredna je posljedica činjenice da je (O_n) grupa. Inače, najčešće se u primjenama javlja baš relacija (1).

5. ORTOGONALNE MATRICE REDA 2

5.1. Teorem. *Svaka ortogonalna matrica ω reda 2 je oblika*

$$\text{I} \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \quad \text{ili} \quad \text{II} \begin{bmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{bmatrix},$$

pri čemu je α jednoznačno određeno u $0 \le \alpha < 2\pi$.

U prvom slučaju prikazuje ω *rotaciju početne baze za kut* α *u pozitivnom smislu; u drugom slučaju: istu rotaciju kombiniranu s promjenom orijentacije.*

Neka je
$$\omega=\begin{bmatrix} p & q \\ r & s \end{bmatrix}.$$

Zbog $p^2+r^2=1$ možemo uvijek staviti

$$p=\cos\alpha; \quad \text{time je} \quad r=(-1)^f \sin\alpha;$$

isto tako zbog

$$p^2+q^2=1 \quad \text{izlazi} \quad q=(-1)^e \sin\alpha;$$

najzad je

$$s=(-1)^g \cos\alpha;$$

pri tom su brojevi $e, f, g \in \{0, 1\}$ i $\alpha \in [0, 2\pi)$.

Dakle nužno

$$(1) \qquad \omega=\begin{bmatrix} \cos\alpha & (-1)^e \sin\alpha \\ (-1)^f \sin\alpha & (-1)^g \cos\alpha \end{bmatrix}; \ e, f, g \in \{0, 1\}.$$

Pregled svih mogućih slučajeva vidi se iz ove tabele (*početi sa g*):

	e	f	g
a	1	0	0
b	0	1	0
c	0	0	1
d	1	1	1

Prva su dva oblika međusobno simetrična, a jedan iz drugoga izlazi kad se α prevede u $-\alpha$, tj. u $2\pi-\alpha$. Zato slučaj b ne daje ništa novo što ne bi obuhvatio i slučaj a. Slučaj d izlazi iz slučaja c istom supstitucijom:

$$\alpha \to 2\pi-\alpha.$$

Dakle zaista dolaze samo slučajevi a i c.

Sad dolazi pitanje jednoznačnosti. Za danu matricu ω jednoznačno je određen broj $\alpha \in [0, 2\pi)$ i jedna jedina od matrica (1) koja je jednaka sa ω.

Neka je $\mathbf{I}=\mathbf{I}'$, tj.

$$\cos\alpha=\cos\alpha', \qquad \alpha=\alpha' \quad \text{ili} \quad \alpha+\alpha'=2\pi$$

$$\sin\alpha=\sin\alpha' \quad \text{tj.} \quad \alpha=\alpha' \quad \text{ili} \quad \alpha+\alpha' \in \{\pi, 3\pi\},$$

$$\text{tj.} \quad \alpha=\alpha'.$$

Isto tako za drugi tip II = II'. Najzad dolazi slučaj I = II', tj.

$$\begin{aligned} \cos\alpha &= \cos\alpha' \\ -\sin\alpha &= \sin\alpha' \\ \cos\alpha &= -\cos\alpha'. \end{aligned}$$

To nije moguće. Naime, iz prve i treće relacije izlazilo bi

$$\cos\alpha' = -\cos\alpha', \quad \text{tj.} \quad \alpha' \in \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\};$$

isto tako

$$\alpha \in \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}.$$

Dolazi još relacija $-\sin\alpha = \sin\alpha'$. Nju ne zadovoljava ni slučaj $\alpha = \alpha'$ ni slučaj $\alpha \neq \alpha'$. Time je sve dokazano.

6. ORTONORMIRANE MATRICE REDA 3

$\longrightarrow$ **6.1. Teorem.** ***Svaka ortogonalna matrica ω reda 3 s determinantom 1 predočuje potpuno određenu rotaciju prostora, tj. određuje jednu os u i broj α tako da preslikavanje $x \to \omega x$ znači rotaciju tačke x oko osi u u pozitivnom smislu za kut veličine α*** (isp. svojstvo (X) u § 2.1).

Naime, promatrajmo karakterističnu jednadžbu

$$\det(\lambda - \omega) = 0 \tag{1}$$

matrice ω. Njena su rješenja po apsolutnoj vrijednosti $= 1$ (svaka ortogonalna matrica je unitarna, a spektar unitarnih matrica smješten je na jediničnoj kružnici). No, kako su koeficijenti jednadžbe (1) realni, to uz rješenje z dolazi i konjugirano $\bar{z}$; znači da je bar jedno rješenje i realno, dakle $= 1$ ili -1. Ako su sva tri rješenja realna, slučaj $\lambda_1 = \lambda_2 = \lambda_3 = -1$ ne može nastupiti, jer je $\det\omega = \lambda_1 \cdot \lambda_2 \cdot \lambda_3$, dakle prema pretpostavci $= 1$; dakle je jedno $\lambda_i = 1$. Ako je bar jedno λ_i nerealno, onda je i $\bar{\lambda}_i$ u spektru i k tome $\bar{\lambda}_i \neq \lambda_i$ pa treće rješenje mora biti 1 (a ne -1 iz razloga $\det\omega = 1$). Dakle je broj 1 takav da je $\det(\omega - 1) = 0$. No, odredimo tada jedinični vektor e_3 tako da bude

$$[\omega - 1]\, e_3 = 0. \tag{2}$$

To je, naravno, moguće jer se radi o homogenoj matričnoj jednadžbi sa singularnom determinantom $\det(\omega - 1)$. K tome su komponente od e_3 realne jer je matrica $\omega - 1$ realna. Odredimo sada ortonormiranu bazu $e = (e_1, e_2, e_3)$ služeći se nađenim vektorom e_3 kao trećim koordinatnim vektorom.

Gornja jednakost (2) iskazuje da je

$$\omega e_3 = e_3$$

i da pri transformaciji $x \to \omega x$ čitava pravulja e_3 ostaje na miru.

Radi se, dakle, o rotaciji oko e_3, pa je njen zapis u bazi e oblika

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & 0 \\ \alpha_{21} & \alpha_{22} & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

no matrica $\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{12} \end{bmatrix}$ je ortogonalna i reda 2, i s determinantom $=1$; to prema teoremu 5.1, znači, da je ona nužno oblika I s jednoznačno određenim kutom $\alpha \in [0, 2\pi)$. Time je dokazano da u bazi e polazna matrica ω ima zapis

$$\begin{bmatrix} \cos\alpha & \sin\alpha & 0 \\ -\sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

i da se transformacija $x \to \omega x$ u toj bazi e prikazuje kao rotacija za α oko osi e_3.

7. DRUGI DOKAZ TEOREMA. ORTONORMIRANE MATRICE REDA N.

7.1. Evo još jednog dokaza gornjeg teorema 6.1. Dokaz je tako priređen da se iz njega može odmah preći na euklidske prostore od više dimenzija i u njima predočiti ortonormirane matrice odgovarajućeg reda.

Neka je, dakle, ω ortonormirana realna matrica (reda 3); time je potpuno određen spektar brojeva $\lambda_1, \lambda_2, \lambda_3$, za koje je

$$(1) \qquad \det[\lambda - \omega] = (\lambda - \lambda_1)(\lambda - \lambda_2)(\lambda - \lambda_3).$$

Prema teoremu 4.1. iz poglavlja 27. možemo sagraditi hermitski ortonormiranu bazu $e = (e_1, e_2, e_3)$ vektora, tj. $e_i e_k = \delta_i^k$ (za koje je $\omega e_k = \lambda_k e_k$). A sad dolazi pitanje realnosti. Ako je λ_k realno, tada je i vektor e_k realan, tj. komponente su mu realne. Ako broj λ_k nije realan, nego je $\lambda_k = \alpha_k + i\beta_k$, $\beta_k \neq 0$, tada se u spektru matrice ω pojavljuje i član $\overline{\lambda}_k = \alpha_k - i\beta_k$ (naravno, $\overline{\lambda}_k, \lambda_k \in S_1 =$ jedinična kružnica). Ako operator ω pustimo da djeluje i u kompleksnom, unitarnom prostoru, tada brojevima $\lambda_k, \overline{\lambda}_k$ odgovaraju posve određene dvije „invarijantne pravulje" (kao dvije kompleksne ravnine) u kompleksnom prostoru; one mogu biti generirane od dva ortonormirana kompleksna vektora $w_k, \overline{w}_k$, koji su konjugirani (spregnuti). No, očigledno, vektori $w_k, \overline{w}_k$ određuju istu „ravninu“ C_2 (to je 4-dimenzionalni prostor iz perspektive R), koju određuju i vektori

$$x_k = \frac{1}{2}(w_k + \overline{w}_k), \; y_k = \frac{1}{2i}(w_k - \overline{w}_k).$$

Ortonormiranost vektora $w_k, \overline{w}_k$ ima za posljedicu ortonormiranost vektora x_k, y_k. No, vektori x_k, y_k su realni; pripadna kompleksna „pravulja“ Cx sadrži euklidsku pravulju Rx; isto tako kompleksna pravulja Cy (zapravo ravnina u našoj perspektivi iz tijela R) sadrži euklidsku pravulju Ry. Operator ω, koji je u kompleksnom prostoru djelovao po obrascu $\omega w = \omega(x+iy) = \omega x + i\omega y$, djeluje sada opet u euklidskom prostoru. Nadalje, iz

$$\omega x_k + i\omega y_k = w z_k = \lambda_k z_k = (\alpha_k + i\beta_k)(x_k + i y_k)$$

izlazi

$$\omega x_k = \alpha_k x_k - \beta_k y_k, \quad \omega_k y_k = \beta_k x_k + \alpha_k y_k.$$

Na taj se način vidi kako operator ω djeluje na nezavisne vektore x_k, y_k; pripadni podoperator u ravnini tih dvaju vektora ima, dakle, matrični zapis u bazi (x_k, y_k) ovakav:

(1) $$\begin{bmatrix} \alpha_k & \beta_k \\ -\beta_k & \alpha_k \end{bmatrix};$$

pri tom je bilo

$$\alpha_k + i\beta_k \in S_1$$

$$\alpha_k + i\beta_k = e^{i\varphi_k} = \cos\varphi_k + i\sin\varphi_k,$$

dakle

$$\alpha_k = \cos\varphi_k, \; \beta_k = \sin\varphi_k.$$

7.2. Dakle smo došli do rezultata: *svakom kompleksnom i nerealnom članu* $\alpha_k + i\beta_k = e^{i\varphi_k}$ *spektra ortogonalne matrice* ω *odgovara invarijantna ravnina u kojoj se podoperator operatora* ω *zapisuje u obliku* (1).

7.3. Ako spektar rješenjâ λ_k jednadžbe $\det[\lambda - \omega] = 0$ ima i drugih nerealnih rješenja, onda je pripadna invarijantna ravnina ortogonalna na prethodnu, pa se u njoj nezavisno pojavljuje analogan zapis podoperatora ω.

7.4. No, realni članovi među λ_k su oblika ± 1; njima odgovaraju invarijantne pravulje s lokalnim zapisom

$$\begin{bmatrix} & 0 & \\ & 0 & \\ \cdots & 1 & \cdots \\ & \cdot & \\ & \cdot & \\ & \cdot & \end{bmatrix}, \text{ odnosno } \begin{bmatrix} & 0 & \\ & \vdots & \\ \cdots & -1 & \cdots \\ & 0 & \\ & \cdot & \\ & \cdot & \\ & \cdot & \end{bmatrix}.$$

7.5. Kako je čitav prostor direktna suma invarijantnih ravnina, odnosno pravuljâ tipa kakvu promatrasmo, izlazi odatle da će operator ω u ortonormiranoj bazi e, kojoj članovi e_k leže na spomenutim prostorima, biti zapisan nizanjem po dijagonali stanovitog broja blokova tipa I, pa tipa -1 (iza dijagonale se metne nekoliko marki -1), pa tipa 1 (marke 1).

Npr. matrica

$$\begin{bmatrix}
\cos 30^\circ & \sin 30^\circ & & & & & & & & \\
-\sin 30^\circ & \cos 30^\circ & & & & & & & & \\
& & \cos 30^\circ & \sin 30^\circ & & & & & & \\
& & -\sin 30^\circ & \cos 30^\circ & & & & & & \\
& & & & -1 & & & & & \\
& & & & & -1 & & & & \\
& & & & & & -1 & & & \\
& & & & & & & -1 & & \\
& & & & & & & & 1 & \\
& & & & & & & & & 1
\end{bmatrix}$$

je ortogonalna i predstavlja određenu rotaciju u euklidskom prostoru R^{10} od 10 dimenzija.

8. PRIKAZ BILO KOJEG OPERATORA PROSTE STRUKTURE U PROSTORU R_n

Neka je sada A bilo koji operator proste strukture u prostoru R_n. To naprosto znači da spektru $\lambda_1, \ldots, \lambda_n$ rješenjâ jednadžbe $\det[\lambda - A] = 0$ odgovara baza e svojstvenih vektora koji su općenito kompleksni. Ponavljajući od riječi do riječi gornja razmatranja, dolazi se do kvazidijagonalnog zapisa kao maloprije — s jedinom razlikom što sada članovi spektra ne moraju ležati na jediničnoj kružnici.

Konačni zapis operatora A bit će oblika:

$$\begin{bmatrix} \square & & \\ & \square & \ldots \end{bmatrix}, \tag{1}$$

pri čemu je svaki dijagonalni blok $\square$ jednog od ovih tipova:

$$\begin{bmatrix} \alpha_k & \beta_k \\ -\beta_k & \alpha_k \end{bmatrix} \tag{2}$$

pri čemu je $\lambda_k = \alpha_k + i\beta_k$, odnosno

$$[\lambda_k], \qquad \text{ako je } \lambda_k \text{ realno.} \tag{2'}$$

No, operator A na svakoj pravulji $e_k R$ vrši rastezanje s koeficijentom λ_k; specijalno, ako je $\lambda_k = 0$, znači to da operator A vrši i projiciranje u smjeru te pravulje. Nadalje, u ravnini što pripada svojstvenim vektorima uz blok (2) predstavlja operator rotaciju kombiniranu sa stezanjem — to je preslikavanje izomorfno onom što ga vrši kompleksni broj

$$\lambda_k = \alpha_k + i\beta_k, \text{ tj. } (z \to \alpha_k + i\beta_k) \cdot z.$$

Na taj način, sveukupno operiranje $x \to Ax$ sastavlja se od određenog broja elementarnih rotacija u vezi s matricom (2), zatim od eventualnih rastezanja u vezi sa (2) te rastezanje tipa $x \to \lambda_k x$ u vezi s realnim članovima spektra promatranog operatora.

No, rezultat (rastezanja) rotacija opet je (rastezanje) rotacija; a rastezanja su definirana hermitskim operatorom. Na taj smo način ponovo dokazali mogućnost faktorizacije $A = S\omega$ svakog linearnog operatora A u euklidskim prostorima (pri tom je S simetričan; isp. pogl. 27, § 14.2).

Npr. $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Tu $\omega = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ prikazuje rotaciju ravnine za $\pi/2$; $S = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ prikazuje projiciranje na drugi koordinatni vektor; konačni rezultat $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ slaže se matrično od ta dva procesa. Npr. vektor $\begin{bmatrix} 2 \\ 3 \end{bmatrix}$ prelazi najzad u $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \end{bmatrix}$.

Uzmimo ovu rotaciju $\omega = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ (ciklička rotacija osi) i projiciranje $p = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ u smjeru prve osi. Rezultat $p\omega = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$; to se provjeri i izmnažanjem i geometrijskim gledanjem. Isto tako:

$$\omega p = (\text{najprije projicirati pa rotirati za } \pi/2) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

9. SIMETRIČNE MATRICE I ORTOGONALNE MATRICE

$\longrightarrow$ **9.1. Teorem.** *Ako je a simetrična (nesimetrična) matrica, tada je za svaku ortogonalnu matricu ω matrica $\omega^{-1} a \omega$ simetrična (nesimetrična). Drugim riječima, matrica koja je ortogonalno-slična sa simetričnom (nesimetričnom) matricom i sama je simetrična (nesimetrična).*

Dokažimo stvar za simetriju, tj. ako je

$$a^T = a, \quad \text{onda je i} \quad (\omega^{-1} a \omega) = (\omega^{-1} a \omega)^T.$$

Naime, po preokrenutoj distributivnosti operatora T imamo:

$$(\omega^{-1} a \omega)^T = \omega^T a^T (\omega^{-1})^T; \tag{1}$$

no $\omega^T = \omega^{-1}$, jer je ω ortogonalna matrica; znamo da je $(\omega^{-1})^T = (\omega^T)^{-1}$, pa je to $= (\omega^{-1})^{-1} = \omega$; kako je zbog simetrije $a^T = a$, to vidimo da $(1)_2$ postaje zaista $\omega^{-1} a \omega$, što se i traži.

Analogno za nesimetriju. Ako je a nesimetrično, onda $\omega^{-1} a \omega = b$ ne može biti simetrično, jer bismo inače obrnutim putem imali $a = \omega b \omega^{-1}$, tj. $a = d^{-1} b d$, gdje je $d = \omega^{-1}$ opet ortogonalna matrica; to znači da bismo iz simetrije matrice b zaključili i na simetriju polazne matrice a protivno pretpostavci.

Interpretiramo li ortogonalnu matricu ω kao prelaz od jedne ortonormirane koordinatne baze na drugu, možemo sadržinu gornjeg teorema izreći i ovako:

$\longrightarrow$ 9.2. **Teorem.** ***Ako je matrica simetrična (nesimetrična) s obzirom na jednu ortonormiranu koordinatnu bazu, onda je ona takva i s obzirom na svaku drugu ortonormiranu bazu koja iz prve izlazi pomoću ortogonalne transformacije.***

9.3. **Zrcaljenje.** Zrcaljenju koordinatnog prostora R_3 od 3 dimenzije prema ravnini xy odgovara matrični zapis

$$\begin{bmatrix} 1 & & \\ & 1 & \\ & & -1 \end{bmatrix};$$

slično se dešava u euklidskom prostoru R_n, pa zato neka vrijedi ovo:

9.3.1. **Definicija zrcalne matrice.** Svaka dijagonalna matrica kojoj je dijagonala sastavljena od jednog primjerka broja -1 i određenog broja jedinicâ 1 zove se *zrcalna matrica.*

Odmah se vidi da je *svaka zrcalna matrica ortogonalna* i da *produkt dviju zrcalnih matrica ne mora opet biti zrcalna matrica.* Međutim, svaka ortogonalna matrica može se prikazati kao produkt dviju ili više zrcalnih matrica, kao što to tvrdi

9.3.2. **Teorem.** ***Svaka realna ortogonalna matrica ω formata $n \times n$ produkt je od n ili manjeg broja zrcalnih matrica.***

Dokažimo stvar induktivno; teorem je očigledan ako je $n = 1$ (tada je naime $\omega = [\pm 1]$); pretpostavimo da je teorem ispravan za $n \leq k$; dokažimo ga i za slučaj $n = k + 1$.

Razlikujemo dva slučaja, već prema tome da li je broj 1 svojstvena vrijednost ili nije svojstvena vrijednost od ω. Ako je 1 svojstvena vrijednost matrice ω, tada postoji jedinični vektor x_0 za koje je $\omega x_0 = 1 \cdot x_0 = x_0$; ortogonalni komplement U pravulje $R x_0$ ima n-1 dimenzija i invarijantan je prema ω; zato je prema pretpostavci operator-matrica $\omega \mid U$ produkt od $\leq n-1$ simetrijâ $s_1, s_2, \ldots$ prostora U; svakoj toj simetriji s_i odgovara određena simetrija S_i čitavog prostora R_n za koju je $S_i \mid U = s_i$, $S_i \mid R_i x_0 =$ identitet. Tada je $\omega = S_1 S_2 \ldots$ jer je $\omega \mid U = s_1 s_2 \ldots$

Drugi slučaj: broj 1 nije u spektru σ_ω pa je $\omega x \neq x$ za svako $x \neq 0$.

Neka je specijalno $x_0 \in R_n$, $x \neq 0$.

Možemo uzeti da je $(x_0, x_0)=1$.

Odaberimo vektor y tako da bude $(y, y)=1$ i da za simetriju:

(1) $$S(x)=x-2(x, y)y$$

vrijedi:

(2) $$S\,\omega\, x_0=x_0.$$

Mora biti:

$$\omega\, x_0-2(\omega\, x_0, y)y=x_0, \quad \text{tj.} \quad \omega\, x_0-x_0=2(\omega\, x_0, y)y.$$

No, to znači da je

(3) $$y=\lambda(\omega\, x_0-x_0).$$

Iz $(y, y)=1$, dobija se

(4) $$\lambda=\pm(\omega\, x_0-x_0,\ \omega\, x_0-x_0)^{1/2}.$$

Iz (3) i (4) slijedi (2).

Kako je S, pa dakle i $S\,\omega$, ortogonalna transformacija, a potprostor $x_0{}^{\perp}$ invarijantan u odnosu na $S\,\omega$, može se prema pretpostavki indukcije $S\,\omega\,|\,x_0{}^{\perp}$ prikazati u obliku proizvoda od najviše $\dim x_0{}^{\perp}=n-1$ simetrija $s_1, \ldots, s_k$ prostora x_0. Ako stavimo

$$S_i\, x_0=x_0, \quad S_i\,|\,x_0{}^{\perp}=s_i \quad (i=1, 2, \ldots, k),$$

bit će očigledno S_i simetrije prostora X te $S\,\omega=S_1\cdot S_2\ldots S_k$.

Odatle je

$$\omega=S\cdot S_1\cdot S_2\ldots S_k$$

proizvod od $k+1\leq n$ simetrijâ prostora X.

10. Zadaci o ortogonalnim matricama

1. Koje su od ovih matrica ortogonalne:

$$1)\begin{bmatrix} 0{,}5 & -(0{,}75)^{1/2} \\ 0{,}75 & 0{,}5 \end{bmatrix}; \quad 2)\begin{bmatrix} 1/2, & 0 \\ 1/3, & 1 \end{bmatrix};$$

$$3)\begin{bmatrix} 0{,}5 & 0{,}01 & 0 \\ 0{,}2 & 2 & 0 \\ 0{,}1 & 1 & 1 \end{bmatrix}; \quad 4)\begin{bmatrix} 0{,}5 & -0{,}75^{1/2} & 0 \\ 0{,}75^{1/2} & 0{,}5 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \cos x & 0 & \sin x \\ 0 & 1 & 0 \\ \sin x & 0 & \cos x \end{bmatrix};$$

$$5)\begin{bmatrix} \cos x & \sin x & 0 \\ -\sin x & \cos x & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos y & \sin y \\ 0 & -\sin y & \cos y \end{bmatrix}\begin{bmatrix} \cos z & 0 & \sin z \\ 0 & 1 & 0 \\ -\sin z & 0 & \cos z \end{bmatrix}?$$

2. Permutacijom stupaca izvedi iz zadane matrice druge matrice. One su sve ortogonalne ili nijedna. Dokaži!

3. Može li produkt neortogonalnih matrica biti ortogonalan?
4. Ako su matrice a, b ortogonalne, onda su ortogonalne i matrice

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix}$$

5. Promatraj određenu ortogonalnu matricu a stupnja $n=2, 3 \ldots$; odredi nekoliko ortogonalnih nadmatrica stupnja $n+1$. Koliko ima takvih nadmatrica ako su preostale vrijednosti nadmatrice $0, \pm 1$?
6. Ako su a, b ortogonalne matrice, odredi ortogonalne nadmatrice najnižeg stupnja (isp. zadatak 4).
7. Odredi ortonormiranu bazu u prostoru što ga određuju vektori:

   1) $(2, 5)^T$, $(-4, 7)^T$; 2) $(1, 2, 3)^T$, $(2, 0, 0)^T$, $(5, 3, 4)^T$;

   3) $(1, 1, 1, 1)^T$, $(2, 3, -2, 4)$, $(-1, -2, 3, 5)$, $(3, 7, 10, 3)^T$.
8. Neparne i parne ortogonalne matrice jesu one ortogonalne matrice kojima je determinanta jednaka -1, odnosno 1. Skup svih ortogonalnih matrica zadanog formata $n \times n$ čini multiplikativnu grupu u kojoj sve parne matrice čine invarijantnu podgrupu P indeksa 2.
9. Ako je $\vec{v}^T v = 1$ (vektor $\vec{v}$ je veličine 1), tada je $S(v) = 1(n) - 2vv^T$ neparna ortogonalna matrica; dokaži da za jedinične vektore v, w vrijedi $v \perp w \Leftrightarrow S(v)S(w) = S(w)S(v)$.
10. Svako kretanje u prostoru R_3 pri kojem je jedna tačka na miru predstavlja rotaciju oko neke pravulje (Euler, D'Alembert).

Literatura

Anđelić [3]; Birkhoff—Maclane [1]; Bourbaki [1]; Dubreil—Jacotin [1]; Gantmaher [2]; Kurepa S. [1]; Lichnerowicz [1]; Proskurjakov [1]; Zurmühl [1].

POGLAVLJE 29.

RJEŠENJA ZADANE JEDNADŽBE PREMA ZADANOJ OBLASTI BROJEVA

0. UVOD

Imamo dva osnovna problema:

0.1. Prvi problem. Zadan je polinom $p(x)$ i neki skup O kompleksnih brojeva (npr. $O = C =$ skup svih kompleksnih brojeva, $O = R$, iR, $O =$ jedinična kružnica, desna poluravnina itd.). Odredi da li p ima rješenja koja su u O; odredi $rp \cap O$, tj. odredi sva nula-mjesta (ništišta) polinoma p koja su u O.

0.2. Drugi problem. *Odredi karakteristična svojstva onih polinoma kojima sva nula-mjesta leže u O.*

Ta dva fundamentalna problema rješena su u nekim specijalnim slučajevima.

0.3. U mnogo blažoj formi problemi se rješavaju da se nađe broj nula-mjesta (a ne sama nula-mjesta) koja leže u O.

0.4. Čini se da su začetnici te problematike bili Diofant i Descartes nastojeći da odrede koliko zadana jednadžba ima *cjelobrojnih*, odnosno *realnih* rješenja. Specijalno je Descartes iz fenomenološkog gledanja kako se predznaci u polinomu nižu — da li variraju ili ne variraju — našao teorem o broju pozitivnih i o broju negativnih nula-mjesta polinoma p. Njegova nastojanja dotjerali su Budan, Fourier i dr. Sturmov teorem stvar i rješava potpuno, dajući sredstvo kako da se odredi broj nula-mjestâ u zadanom intervalu. Isto tako teorija kompleksnih funkcija daje odgovor na slično pitanje za svaki prilično jednostavno građeni skup $O \subset C$ (v. § 6.3).

0.5. Matrični zapis algebarskih polinoma pokazuje se u problematici koja nas zanima vanredno plodan. Naime, smatrajući svaku kvadratnu matricu a kao izvor za pripadni karakteristični polinom $\det(\lambda - a)$, dolazimo na zaista plodno matematičko rasuđivanje. Ukazujemo pri tom npr. na potpunu karakterizaciju karakterističnih polinoma kojima je spektar realan (dakle je $O \subset R$), čisto imaginaran ($O \subset iR$) ili smješten na jediničnoj kružnici, itd.

0.6. U ovom poglavlju upoznat ćemo se s daljim rezultatima u tom pogledu. Tako ćemo dokazati Hurwitz-Routhov teorem da se vidi kojim polinomima leže nula-mjesta u lijevoj otvorenoj poluravnini-to su tzv. Hurwitzovi polinomi (pitanje je u tijesnoj vezi sa stabilnosti pri izučavanju mehanizma, kretanja itd.) (v. § 13.6.6—13.9.9).

0.7. Spominjemo i Perron (1907)—Frobeniusov (1912) teorem o tome da svaka realna nerazloživa[1] kvadratna matrica s neodrečnim koordinatama ≥ 0 ima prostu svojstvenu vrijednost koja je pozitivna, jednaka ili veća nego apsolutna vrijednost svake druge svojstvene vrijednosti (taj teorem ima primjenâ u računu vjerojatnosti i statistici u vezi sa stohatističkim (slučajnim) procesima i lancima Markova te u ispitivanju malih titranja elastičnih sistema). Dokaz teorema je vrlo dug (isp. npr. Gantmaher, str. 321—330).

0.8. Napomenimo da ćemo u § 6.5 opet (isp. 7 § 13) vidjeti da svaki algebarski polinom $p(x)$ nad R ili C ima svoja nula-mjesta u C i opet dokazati tzv. „fundamentalni teorem algebre", koji je strogo dokazao prvi put Gauss (uglavnom u svojoj doktorskoj disertaciji). Mnogi bi današnji matematičari rekli da ti polinomi $p(x)$ imaju svoja nula-mjesta *na žalost* već u C, tako da otpada užitak da se zajednica C proširuje rođacima koje rađa polinom $p(x)$ (kao što već moramo proširivati zajednicu R zbog čak tako jednostavnog polinoma kao što je x^2+1 nad R, koji rađa nula-mjesta $-i$ i $+i$, kojih nema u R i time dolazimo do oblasti svih kompleksnih brojeva).

1. GORNJA MEĐA POZITIVNIH KORIJENA

1.1. Oznaka polinoma. Radimo s polinomom $a(x)$ s realnim koeficijentima. Izvedimo nekoliko pravila kako da odredimo broj $L>0$ iznad kojeg jednadžba nema nijednog pozitivnog rješenja. Polinom ćemo zapisati ovako:

$$a(x) \equiv a_0 x^0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n,\ a_n > 0. \tag{1}$$

Primijetite također da smo u (1) dodali uslov $a_n>0$. Naravno, to nije nikakvo ograničenje.

1.2. Brojevi: L, l, L', l'. Pod L ćemo razumijevati bilo koji broj *iznad kojeg* promatrana jednadžba nema realnih rješenja; prema tome: ako je $x>L$, onda je $a(x) \neq 0$. Od interesa će biti da se odredi *što manji takav broj* L za zadanu jednadžbu.

1.2.1. Broj l za jednadžbu je takav pozitivan broj *ispod kojeg* jednadžba nema nikojeg pozitivnog rješenja.

Ukratko, l, L je uređena dvojka pozitivnih brojeva sa svojstvom da svaka pozitivna nula-tačka polinoma leži u zatvorenom odresku

$$[l, L]; \quad \text{pri tom je} \quad l \leq L.$$

---

[1] Kaže se da je matrica (nerazloživa) razloživa ako se permutiranjem redaka međusobno i stupaca međusobno matrica (ne) može svesti na oblik

$$\begin{bmatrix} X & 0 \\ Y & Z \end{bmatrix}, \text{ gdje su } X, Z \text{ kvadratne matrice.}$$

Ako je $l=L$, onda to znači da je L jedini pozitivni korijen jednadžbe $a(x)=0$.

Ako se radi o polinomu a, onda se brojevi l, L mogu označiti i sa l_a, L_a.

Analogno se definiraju negativni brojevi L', l' tako da bude $L' \leq l' < 0$ i da zatvoreni segment $[L', l']$ obuhvata svaki negativni korijen jednadžbe o kojoj govorimo.

1.2.2. Primjer. Promatrajmo funkciju

$$f(x)=x^4+x^3-3x^2+x-100.$$

$$\text{Ona je } =x^4+x^2(x-3)+x-100.$$

Odatle se vidi da je za $x>5$ svakako $f(x)>0$. Dakle je $L=5$. Vidi se također da je $f(3)<0$, dakle je $L>3$.

1.3. Funkcija $\operatorname{sgn} x$; $\operatorname{sgn} a(x)$. Podsjetimo se da je

$$\operatorname{sgn} x = \ \ 1 \text{ za } x>0,$$

$$\operatorname{sgn} x = -1 \text{ za } x<0 \text{ te } \operatorname{sgn} 0 = 0.$$

1.3.1. Teorem. Ako je $x>L$, onda je $\operatorname{sgn} a(x)=\operatorname{sgn} a_n$.

Naime, jasno je da za dani polinom $a(x)$ možemo x uzeti tako veliko da $a_k x^{k-n}$ bude proizvoljno maleno. No,

$$a(x)=x^n(a_0x^{-n}+a_1x^{1-n}+a_2x^{2-n}+\cdots+a_n).$$

To znači da svaki član u toj zagradi, osim posljednjeg, može biti učinjen proizvoljno malenim, recimo $<\varepsilon$, gdje je $\varepsilon>0$; dovoljno je zato promatrati veliko x, tako da svaki od onih n članova u zagradi bude $<\varepsilon n^{-1}$.

Time svih n članova u zagradi daju zajedno, po apsolutnoj vrijednosti, doprinos $<n\cdot\varepsilon n^{-1}=\varepsilon$, tako da zagrada ima znak $\operatorname{sgn} a_n$. Kako je $x^n>0$, znači da je $\operatorname{sgn} a(x)=\operatorname{sgn} a_n$. No, to je za dovoljno velike x-ove. A kako je $a(x)$ istog znaka poslije L, tj. za sve $x>L$, znači da je $\operatorname{sgn} a(x)=\operatorname{sgn} a_n=1$ za svako $x>L$.

Međutim, u dokazu se više nalazi nego što je izrečeno u teoremu 1.3.1.

Naime, stvarno je dokazano da je

$$|a(x)|=|x^n|\cdot a_n+I| \geq |x^n||a_n|-|a_{n-1}x^{-1}+$$
$$+a_{n-2}x^{-2}+\cdots+a_1x^{n-1}+a_0x^{-n}|),$$

tj. drugim riječima imamo:

—→ Teorem. *Ako je $|x|$ dovoljno veliko, tada je $|a(x)|$ automatski dovoljno veliko; to znači, specijalno, da vanjštinu dovoljno velikog kruga oko ishodišta* 0 *polinom $a(x)$ preslikava u vanjštinu dovoljno velikog kruga oko* 0. *Formalno: za svaki broj $r>0$ (tj. za svaki krug $K(O;r)$) postoji broj $r'>0$ (tj. krug*

$K(0; r')$) sa svojstvom da iz $|x|>r'$ izlazi $|a(x)|>r$, tj. da polinom $a(x)$ prebacuje cijeli dio ravnine izvan kruga $K(O, r')$, negdje izvan kruga $K(O, r)$[1].

1.4. Lagrangeov teorem. *Ako a_k za polinom $a(x)=\sum_{\nu=0}^{n} a_\nu x^\nu$ znači negativni koeficijent*[2] *u nizu $a_0, a_1, a_2 \ldots$ s najvećim indeksom, tada je*

$$L = 1 + \left(\frac{M}{a_n}\right)^{\frac{1}{n-k}}$$

pri tom je M = supremum apsolutnih vrijednosti negativnih koeficijenata.

1.4.1. Npr. za jednadžbu

$$x^4 + x^3 - 3x^2 + x - 100 = 0 \quad \text{je} \quad k=2, \; M=100,$$

pa je

$$L = 1 + \sqrt{\frac{100}{1}} = 11.$$

To znači da promatrana jednadžba iznad 11 nema nijednog rješenja, nego je $a(x)>0$ za $x>11$. Taj je rezultat lošiji od rezultata $L=5$, što smo ga dobili direktno (§ 1.2.1). No, stvar je u tom da u 1.4. imamo *pravilo* koje dovodi do cilja za svaki polinom.

Dokaz gornjeg teorema 1.4. Treba pokazati da

$$x > L \Rightarrow a(x) > 0.$$

Za $x>0$ je svakako

$$(*) \qquad a_{k+1}x^{k+1} + a_{k+2}x^{k+2} + \cdots + a_n x^n \geq a_n x^n,$$

jer su svi napisani koeficijenti ≥ 0.

Svakako je

$$a_0 + a_1 x + \cdots + a_k x^k \geq -M(1 + x + x^2 \cdots + x^k) = -M\frac{x^{k+1}-1}{x-1}.$$

Zbrajanjem te relacije i (*) izlazi

$$(2) \qquad a(x) \geq a_n x^n - M\frac{x^{k+1}-1}{x-1}.$$

Promatrajmo slučaj $x>1$, tj. $x-1>0$. Treba se osigurati veza $a(x)>0$.

To će prema (2) sigurno biti za one $x>1$ za koje je

$$a_n x^n (x-1) > M(x^{k+1}-1),$$

[1] Posebno je dublje pitanje kako izgleda skup svih brojeva $a(x)$ sa koje je $|x|>r$.

[2] Ako uopće nema negativnih koeficijenata, onda je jasno da nema ni jednog pozitivnog korijena, pa je $L=0$.

pa to prije ako je

(3) $$a_n x^n (x-1) > M\, x^{k+1}.$$

No iz (3) izlazi

$$a_n x^{n-k-1} (x-1) \geq M, \quad \text{što će zbog} \quad x^{k-1} > (x-1)^{k-1}$$

sigurno vrijediti ako je

$$a_n (x-1)^{n-k-1} (x-1) \geq M, \quad \text{tj.} \quad a_n (x-1)^{n-k} \geq M,$$

odatle $$(x-1)^{n-k} \geq a_n^{-1} M \Rightarrow x-1 \geq (a_n^{-1} M)^{1/(n-k)}, \qquad \text{odatle i (1).}$$

Dakle je istina: ako je $x > L$ iz (1), tada je $a(x) > 0$, To je bilo za slučaj $x > 1$. Međutim, nama je dovoljno i taj slučaj promatrati, jer se kod broja L ne radi o tome da se pronađe *najmanji* mogući broj L s traženim svojstvom. Na to se treba naviknuti i u daljim razlaganjima.

1.5. Teorem (Cauchy). *Neka je*

$$a(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n, \quad (a_0 > 0)$$

(pazi na indekse!); *neka je* $a_{\nu_0}, a_{\nu_1}, \ldots, a_{\nu_{k-1}}$ *podniz svih negativnih koeficijenata; neka je*

(4) $$\alpha = \sup_r \left| k \frac{a_{\nu_r}}{a_0} \right|^{\frac{1}{\nu_r}};$$

tada je $\alpha = L$ (*može se desiti da bude i* $a(\alpha) = 0$; *tada je* α *najveći pozitivni korijen*).

Treba pokazati da iz $x > \alpha$ izlazi $a(x) > 0$.

$$x > \alpha \;\Rightarrow\; x^{\nu_r} > \alpha^{\nu_r} \geq (\text{prema (4)}) \geqq k \cdot \frac{|a_{\nu_r}|}{a_0}.$$

Odatle, množeći sa $a_0 > 0$:

$$a_0 x^{\nu_r} > a_0 \alpha^{\nu_r} \geqq k\, |a_{\nu_r}|. \text{ Množeći sa } x^{n-\nu_r}:$$

$$a_0 x^n > a_0 \alpha^{\nu_r} x^{n-\nu_r} \geqq k\, |a_{\nu_r}|\, x^{n-\nu_r}, \qquad \text{tj.}$$

(5) $$a_0 x^n > k |a_{\nu_r}|\, x^{n-\nu_r} \text{ za } r = 0, 1, \ldots, k-1.$$

Sabirući tih k nejednakosti (5), pojavljuje se i na lijevoj strani faktor k, pa skraćujući s njim:

$$a_0 x^n > \sum_r |a_{\nu_r}|\, x^{n-\nu_r},$$

(6) $$a_0 x^n + \sum_r^{k-1} a_{\nu_r} x^{n-\nu_r} > 0.$$

Dakle, $x > \alpha \;\Rightarrow\;$ (6), pa će pogotovu $x > \alpha \;\Rightarrow\; a(x) > 0$, jer nenapisani članovi $a_i x^i$ su svi sa $a_i > 0$. Time je i Cauchyjevo pravilo dokazano.

1.5.1. Za gornji primjer iz 1.4.1:

$$x^4+x^3-3x^2+x-100=0 \qquad \text{imamo}$$

$a_3=-3$, $a_4=-100$, $k=2$; posmatrajmo, prema (4), brojeve $\left(2\cdot\frac{3}{1}\right)^{1/2}$,

$$\left(2\cdot\frac{100}{1}\right)^{1/4}=(10\cdot 2^{1/2})^{1/2}; \text{ drugi je veći.}$$

Dakle je $\alpha=\sqrt{10\sqrt{2}}$; specijalno je $L=4$: za $x>4$ već je $a(x)>0$ (Lagrangeovo pravilo je dalo $L=11$), a direktno rasuđivanje $L=5$; § 1.2.1).

1.6. Teorem (Newton-Rolle [Njutn-Rol]). *Ako je neki pozitivan broj* β *takav da je* $a(\beta)>0$, $a'(\beta)>0, \ldots, a^{(r-1)}(\beta)>0$, $a^{(r)}(x)>0$ *pri* $x\geq\beta$, $(r\leq n-1)$ *tada je* $a(x)>0$ *za* $x\geqq\beta$, *dakle je* $\beta=L$.

Stvarno, iz $a^{(r-1)}(\beta)>0$ i $a^{(r)}(x)>0$ za $x\geqq\beta$ izlazi da je funkcija $a^{(r-1)}(x)$ uzlazna za $x>\beta$, dakle je ona >0, jer je $a^{(r-1)}(\beta)>0$; iz istog je razloga $a^{(r-2)}(x)>0$ i uzlazna, itd., dok se ne dođe na $a^{(0)}(x)=a(x)$, koje je isto tako pozitivna i uzlazna za $x>\beta$. A to znači da je $\beta=L$.

1.6.1. Za

$$a(x)=x^4+x^3-3x^2+x-100 \tag{7}$$

imamo

$$a'(x)=4x^3+3x^2-6x+1$$

$$a''(x)=12x^2+6x-6$$

$$a'''(x)=24x+6.$$

Sve je to >0 za $x=5$; zato je $L=5$.

Na taj način vidimo kako smo na četiri načina određivali L-broj za polinom (7) i da je vrijednost za L u ovom slučaju izašla 5 kao i u direktnom sagledanju iz § 1.2.1; našli smo također $L=11$ i $L=4$ (§ (2.5.1).

1.7. Brojevi l, L' l'. Promatrajmo funkciju

$$f(x)=a(x^{-1}).$$

Tada je

$$a(x^{-1})=a_n x^{-n}+a_{n-1}x^{-n+1}+\cdots+a_n x^{-1}+a_0 x^0=$$

$$=x^{-n}(a_n x^0+a_{n-1}x^1+a_{n-2}x^2+\cdots+a_0 x^n).$$

U zagradi se pojavljuje određeni polinom — *dual polaznog*; označimo ga sa a^T.

Prema tome je $a(x^{-1})=x^{-n}a^T(x)$. Vidi se da je L-broj za a^T ujedno L-broj za $x^{-n}a^T(x)$, tj. za $a(x^{-1})$. Drugim riječima, znamo odrediti *L-broj funkcije* $a(x^{-1})$. No, *recipročna vrijednost* L^{-1} *toga L-broja jest l-broj za funkciju* $a(x)$.

Naime, $x>L_a(x^{-1})$ znači da je $a(x^{-1})\neq 0$. Stavimo $y=x^{-1}$. To znači:

$$y^{-1}>L^{-1}{}_{aT} \text{ ima za posljedicu } a(y)\neq 0,$$

tj.

$$0<y<L^{-1}{}_{aT} \text{ ima za posljedicu } a(y)\neq 0.$$

A to znači da je $$(L_{a^T})^{-1} = l_a.$$

Time znamo odrediti l-broj i L-broj za svaki polinom.

Isto se tako vidi ovo: L-broj polinoma $a(-x)$ jest $-L'$-broj polinoma $a(x)$. Dakle,

$$L'_{a(x)} = -L_{a(-x)}.$$

Slično tako

$$l'_{a(x)} = -l_{a(-x)}.$$

Na taj se način određivanje brojeva l, L, l', L' svodi na određivanje L-brojeva za polinome $a(x)$, $a^T(x)$, $a(-x)$.

2. PREDZNAK FUNKCIJE

Izložit ćemo nekoliko jednostavnih, ali osnovnih stvari o predznacima. U ovom razmatranju leži korijen o prebrojavanju nula-tačaka ili ništišta polinoma.

2.1. Definicija sgn x. Za svaki realni broj x definira se

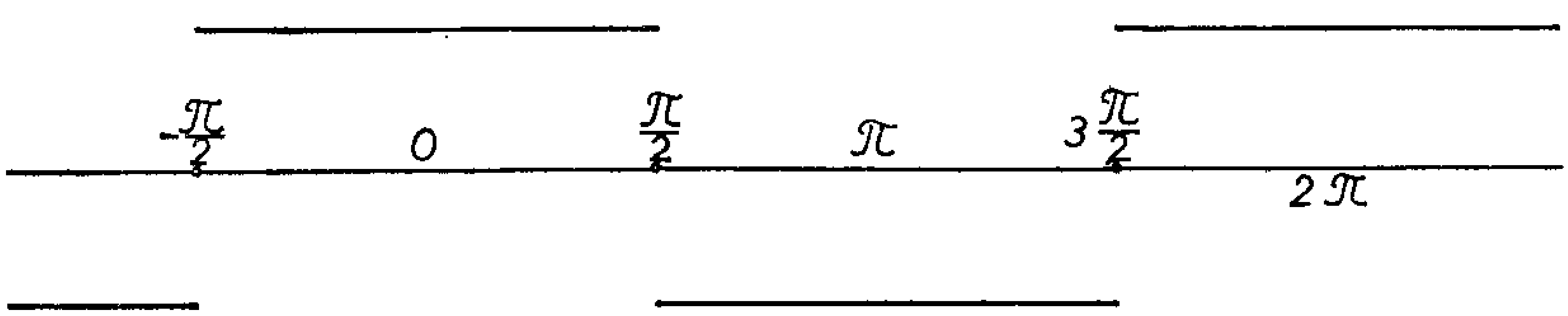
$$\operatorname{sgn} 0 = 0$$
$$\operatorname{sgn} x = 1 \quad \text{za} \quad x > 0$$
$$\operatorname{sgn} x = -1 \quad \text{za} \quad x < 0.$$

$$\operatorname{sgn} x = \frac{x}{|x|}$$

(stvarno bi se ovom jednakošću trebalo definirati $\operatorname{sgn} x$ za svaki *kompleksni* broj $x \neq 0$). Prema tome, funkcija $x \to \operatorname{sgn} x$ je prekidna u tijelu R realnih brojeva: prekida se u 0, skačući s -1 na 1 kad varijabla x skoči s negativnih na pozitivne brojeve.

2.2. Za svaku funkciju f s *realnim vrijednostima* imamo i funkciju $\operatorname{sgn} f$.

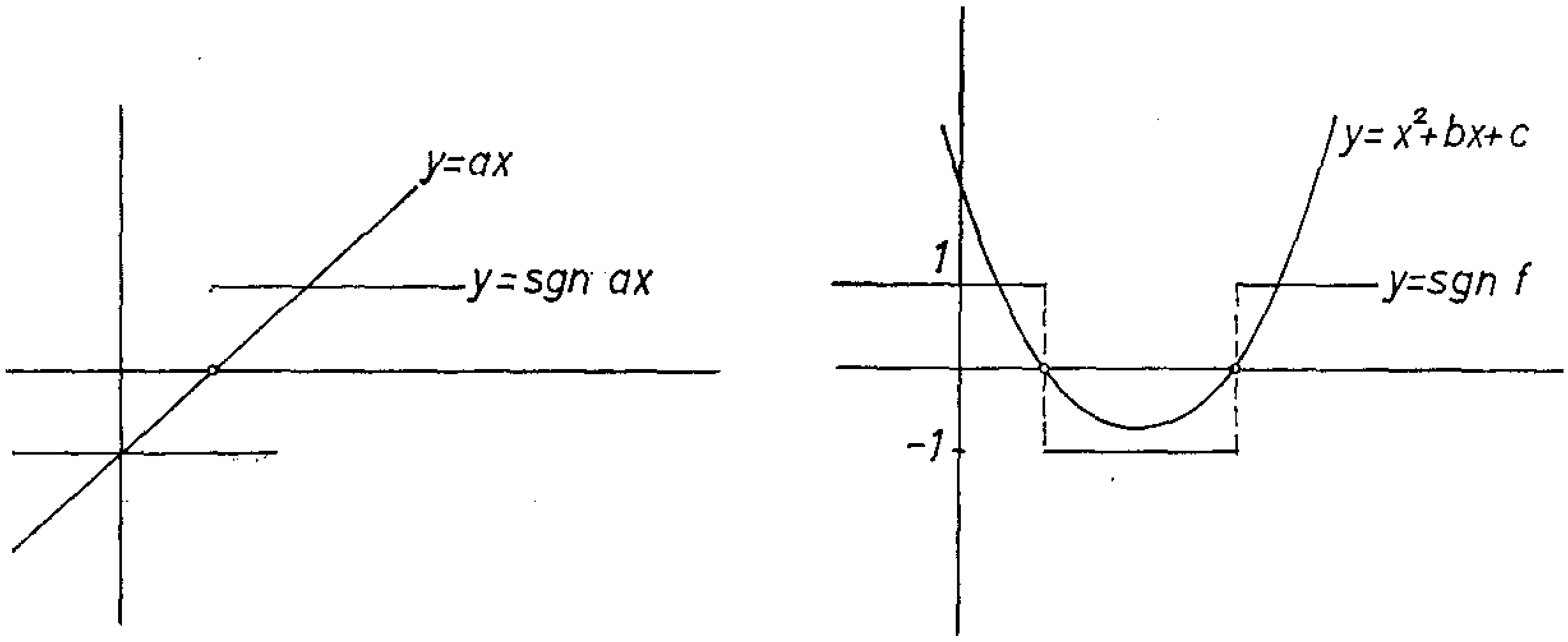
Tako npr. $\operatorname{sgn} \cos x$ *ima ovakvu* sliku:



Sl. 29. 2.2.

Iz te slike vidimo gdje se sgn cos prekida: prekida se tamo gdje je $\cos x = 0$. Pa ako se gornja slika uporedi sa slikom za $\cos x$, vidi se u kojoj mjeri funkcija $y = \operatorname{sgn} \cos x$ *odražava* funkciju $y = \cos x$.

2.3. Funkcija sgn f je dragocjeno sredstvo za ispitivanje nula-mjesta funkcije f: *ona upravo na drastičan način pokazuje sva mjesta gdje se neprekidna funkcija f poništava.* Gledaj dobro ove dvije slike: na svakoj je prikazano f i sgn f.



Sl. 2.3.

2.4. Iz funkcije sgn $f(x)$ vide se odmah tri množine:

prvo: skup $[f=0]$ realnih nula-mjestâ funkcije $f(x)$,

drugo: skup $[f>0]$ realnih mjestâ gdje je funkcija >0 i

treće: skup $[f<0]$ realnih mjestâ gdje je funkcija <0.

⟶ Specijalno, *skup rješenja algebarske jednadžbe $f(x)=0$ u zadanom intervalu I podudara se sa skupom brojeva iz I u kojima se funkcija* sgn f *prekida.*

Eto, ta *jednostavna i očigledna činjenica osnov je svih drugih razmatranja* u narednim paragrafima. Samo će još biti potrebno da nađemo kako da na lakši način odredimo gdje se sgn f prekida! Tzv. *Sturmov niz vezan za polinom* $f(x)$ bit će pogodan alat za tu svrhu! (v. § 5; § 13.2—13.4).

⟶ **2.5. Bolzanov [Bolcano] teorem.** *Ako je funkcija f neprekidna u kakvu intervalu $R[a, b]$ realnih brojeva pa ako u krajevima a, b toga intervala funkcija f uzima protivno označene vrijednosti, tj. $f(a)\cdot f(b)<0$, tada je $f(x_0)=0$ za bar jedno $x_0 \in R(a, b)$.*

Govoreći geometrijski, znači to ovo: *ako za neprekidni luk AB ravninske krivulje koji se projicira na interval I znamo da krajevi luka leže jedan u jednoj, a drugi u drugoj otvorenoj poluravnini pravulje I, tada se luk i interval I sijeku bar u jednoj tački.*

Dokaz Bolzanova teorema. Polazimo od zatvorenog intervala $I=R[a, b]$; po pretpostavci u njemu funkcija sgn f ima bar dvije vrijednosti protivnog znaka. Podijelimo I na dva jednaka zatvorena odreska: lijevi I_0 i desni I_1; neka je I_{k_0} prvi od njih — dakle po mogućnosti I_0 — u kojem funkcija f uzima i pozitivnih i negativnih vrijednosti; neka $I_{k_0 k_1}$ nastaje iz I_{k_0} kao što je I_{k_0} nastao iz I;

neka isto tako $I_{k_0 k_1 k_2}$ nastaje iz segmenta $I_{k_0 k_1}$, itd. Dobivamo strogo silazan beskonačan niz

(1) $$I_{k_0} \supset I_{k_0 k_1} \supset I_{k_0 k_1 k_2} \cdots$$

zatvorenih odrezaka; u svakom od njih funkcija je negdje pozitivna i negdje negativna. No, dužine su tih odrezaka po redu

$$d = |b-a|,\ 2^{-1} d,\ 2^{-2} d, \ldots, \text{ dakle} \to 0.$$

Time se svi odresci niza (1) stežu na jednu tačku z, koju možemo zapisati kao

(2) $$I_{k_0 k_1 k_2} \cdots$$

U tački (2) funkcija je 0, jer u svakoj okolini $O(z)$ te tačke z uzima funkcija f i negativnih i pozitivnih vrijednosti. A jedina vrijednost neprekidne funkcije s tim svojstvom je 0.

Naime, po definiciji neprekidnosti funkcije f u tački z znači to da za svaku okolinu $Of(z)$ od $f(z)$ — a ne od z — postoji jedna okolina $O(z)$ koju f prevodi u $Of(z)$; no $O(z)$ sadrži bar jedan od intervala (1), pa dakle skup fOz, a time i njegov nadskup Ofz, ima i pozitivnih i negativnih brojeva, a to znači da je $f(z) = 0$.

Ujedno je gornji dokaz dao i dijadski zapis traženog rješenja z; u dijadskom sistemu glasi z

(3) $$z = a + \frac{0, k_0 k_1 \ldots}{b-a},$$

pri čemu su i brojevi a, b zapisani dijadski.

U decimalnom sistemu zapis bi glasio isto, (3), samo bi onda podjela svakog intervala bila ne u 2, nego u 10 jednakih dijelova i svaki put bismo odabrali *prvi* interval, idući s lijeve strane na desnu, u kojem funkcija f postaje što pozitivna što negativna.

2.6. Jednadžbe neparnog stupnja. Teorem. *Svaka algebarska jednadžba neparnog stupnja i s realnim koeficijentima ima bar jedan realan korijen.* (v .§ 6.5).

Stvarno, prema teoremu 1.3.1, ako polinom $a(x) = \Sigma a_k x^k$ ima realne koeficijente te ako je $n = \operatorname{st} a$, postoji broj L sa svojstvom da je $\operatorname{sgn} a(x) = \operatorname{sgn} a_n$ za $x > L$; isto tako postoji broj $L' < 0$ sa svojstvom da je $\operatorname{sgn} a(x) = -\operatorname{sgn} a_n$ ako je $x < L'$; to znači da će za $x > \sup\{L, |L'|\}$ polinom $a(x)$ imati u $x, -x$ protivne znakove, tj.

$$a(x) \cdot a(-x) < 0.$$

Zato prema Bolzanovu teoremu postoji jedan broj z između x i $-x$ sa svojstvom $f(z) = 0$.

2.7. Predznak izraza $p(x) = (x - x_0)^r$. Taj izraz ima isti znak (i to $(-1)^r$ lijevo od x_0 i isti znak (i to $+1$) desno od x_0; kad x preskoči slijeva nadesno preko x_0, tada se $\operatorname{sgn} p$ množi sa $(-1)^r$; prema tome, ako je $x' < x_0 < x''$, tada je $\operatorname{sgn}(x''-x_0)=(-1)^r \operatorname{sgn}(x'-x_0)$. Ako je r neparno, onda prelaskom varijable x preko x_0 izlaz $(x-x_0)^r$ *mijenja* znak, a inače, ako je r parno, znak od $p(x)$ je isti lijevo od x_0 i desno od x_0.

Često ćemo se služiti gornjom činjenicom, i to zbog ovog rezultata:

$\longrightarrow$ **2.7.1** Lema. *Ako je x_0 ništište realne funkcije $f(x)$, i to kratnosti r, tada se u neposrednoj okolini O broja x_0 predznak broja fO_0 na lijevom kraju O_0 i broja fO_1 na desnom kraju O_1 okoline O razlikuju multiplikativno za* $(-1)^r$:

$$\operatorname{sgn} f O_1=(-1)^r \operatorname{sgn} f O_0. \tag{1}$$

Dokaz. Najprije znamo da to što je x_0 ništište kratnosti r za funkcije $f(x)$ znači (pogl 5, § 4.2.7) da je $f(x)=(x-x_0)^r g(x)$, pri čemu je $g(x_0)\neq 0$; no iz toga što je $g(x_0)\neq 0$ izlazi da je $\operatorname{sgn} g(x)$ konstanta u nekoj okolini O broja x_0. Zato iz

$$\operatorname{sgn} f(x)=\operatorname{sgn}(x-x_0)^r\cdot \operatorname{sgn} g(x) \tag{2}$$

izlazi specijalno za krajeve O_0 i O_1 okoline O:

$$\frac{\operatorname{sgn} fO_1}{\operatorname{sgn} fO_0}=\frac{\operatorname{sgn}(O_1-x_0)^r}{\operatorname{sgn}(O_0-x_0)^r}=(\text{prema } 1.3.3)=(-1)^r.$$

Odatle izlazi obrazac (1).

$\longrightarrow$ **2.8. Teorem (princip supstitucije).** *Neka je I kakav interval tijela R realnih brojeva; neka je f neprekidna funkcija koja se ne poništava ni u jednom od krajeva I_0, I_1 intervala I; ako se f poništava u konačno mnogo, svega m tačaka $x_{m'}\in I$ s odgovarajućim kratnostima $k_{m'}$, $(m'=1,2,\ldots,m)$, tada je*

$$\operatorname{sgn} f I_1=(-1)^{\Sigma k_{m'}} \operatorname{sgn} I_0, \qquad \text{tj.} \tag{3}$$

$$\operatorname{sgn} f I_0\cdot f I_1=(-1)^{\nu I}, \tag{4}$$

$$\text{gdje} \quad \nu I=\sum_{m'=1}^{m} k_{m'}$$

kazuje na koliko se mjesta u I funkcija f poništava; pri tom se svaka nula-tačka računa prema svojoj kratnosti.

Naime, putujući od lijevoga kraja I_0, broj $\operatorname{sgn} f(x)$ se ne mijenja sve dok ne naiđemo na prvo ništište x_1; u samom broju x_1 funkcija $\operatorname{sgn} f$ je $=0$, a odmah desno (prema § 1.3.4) jednak je $(-1)^{k_1} \operatorname{sgn} I_0$; idući sada dalje $\operatorname{sgn} f(x)$ je neprestano isto i $=(-1)^{k_1} \operatorname{sgn} I_0$, dok ne naiđemo na naredno ništište x_2; kad varijabla x skoči preko x_2 na drugu stranu, znači to za $\operatorname{sgn} f$ množenje sa $(-1)^{k_2}$, gdje je k_2 kratnost od x_2 kao ništište za f. Prema tome, neposredno desno od x_2 je $\operatorname{sgn} f x=(-1)^{k_1+k_2} \operatorname{sgn} I_0$, itd., dok ne dođemo na drugi desni kraj I_1 intervala I; postupno vidimo da u I_1 stižemo s vezom (3). Iz (3), množeći sa $\operatorname{sgn} f I_0$, izlazi (4), jer je očigledno sgn produkta produkt signumâ faktorâ; nadalje je $\Sigma k_{m'}=\nu I$.

⟶ **2.9.** Teorem. *U neposrednoj okolini O ništišta x_0 funkcije f vrijedi:*

(1)
$$\operatorname{sgn}(x-x_0)=\operatorname{sgn}\frac{f(x)}{f'(x)}.$$

Drugim riječima, neposredno lijevo od x_0 predznak je -1, a neposredno desno od x_0 predznak je $+1$.

Promotrimo slučaj da je x_0 prosto ništište, tj.

$$f(x_0)=0,\quad f'(x_0)\neq 0.$$

Iz definicije

$$f'(x_0)=\lim_{x\to x_0}\frac{f(x)-f(x_0)}{x-x_0},\ \text{zbog } f(x_0)=0,$$

izlazi:

$$f'(x_0)=\lim_{x\to x_0}\frac{f(x)}{x-x_0},$$

odnosno

(2)
$$f'(x_0)=\frac{f(x)}{x-x_0}+\varepsilon;\ \text{pri tom } \varepsilon\to 0 \text{ kad } x\to x_0.$$

Za slučaj $f'(x_0)\neq 0$ izlazi iz (2):

(3)
$$\operatorname{sgn} f'(x_0)=\operatorname{sgn}\frac{f(x)}{x-x_0}=\frac{\operatorname{sgn} f(x)}{\operatorname{sgn}(x-x_0)},$$

jer aditivna veličina od ε za predznak desne strane u (2) ne odlučuje. No, zbog neprekidnosti ima f isti predznak u nekoj okolini od x_0; to znači da u (3) možemo umjesto $f'(x)$ pisati $f(x_0)$; a time se dobije upravo tražena formula (1).

Dokažimo sada (1) općenito i strogo. Služimo se Taylorovim obrascem (pogl. 7, § 12.4); prema tome osnovnom teoremu:

$$f(x)=f(x_0)+\frac{f'(x_0)}{1!}(x-x_0)+\cdots+\frac{f^{(k)}(x_0)}{k!}(x-x_0)^k+\cdots$$

Ako je x_0 k-kratno ništište, onda je tu prvih k članova $=0$, pa imamo:

(3)
$$f(x)=\left(\frac{f^k(x_0)}{k!}+\frac{f^{(k+1)}(x_0)}{(k+1)!}\cdot(x-x_0)+\cdots\right)\cdot\left(x-x_0\right)^k.$$

Pri tom se x može uzeti tako blizu broja x_0 da zbroj u zagradi ima predznak svojeg prvog dijela.

Radeći sličan posao s funkcijom f', imamo analogno

(3′)
$$f'(x)=\left(\frac{f^k(x_0)}{(k-1)!}+\frac{f^{(k+1)}(x_0)}{k!}\cdot(x-x_0)+\ldots\right)\cdot\left(x-x_0\right)^{k-1}.$$

I opet se x može uzeti tako blizu do x_0 da predznak sadržine duge zagrade bude predznak prvog člana u toj zagradi; naime, taj član ne zavisi od razlike $x-x_0$, a svi drugi članovi zavise množidbeno od $x-x_0$.

Podijelimo li (3) sa (3') i skratimo li sa $(x-x_0)^{k-1}$, izlazi:

$$\frac{f(x)}{f'(x)}=(x-x_0)\cdot\frac{\mathrm{I}}{\mathrm{II}}, \tag{4}$$

gdje I, odnosno II označuje izraz iz dugačke zagrade u (3), odnosno (3'). Iz (4) izlazi:

$$\operatorname{sgn}\frac{f(x)}{f'(x)}=\operatorname{sgn}(x-x_0)\cdot\operatorname{sgn}\frac{\mathrm{I}}{\mathrm{II}}. \tag{5}$$

No,
$$\operatorname{sgn}\frac{\mathrm{I}}{\mathrm{II}}=\frac{\operatorname{sgn}\mathrm{I}}{\operatorname{sgn}\mathrm{II}}=\frac{\operatorname{sgn}\dfrac{f^{(k)}(x_0)}{k!}}{\operatorname{sgn}\dfrac{f^{(k)}(x_0)}{(k-1)!}}=\operatorname{sgn}\frac{1}{k}=1.$$

Time (5) daje traženu jednakost (1).

2.10. Formulu (1) možemo pisati i ovako:

$$\operatorname{sgn} f'(x)=\operatorname{sgn}\frac{f(x)}{x-x_0} \tag{6}$$

za x u blizini broja x_0, gdje je $f(x_0)=0$.

Odatle se odmah vidi vladanje funkcije f u okolini $O(x_0)$ od x_0 u zavisnosti od funkcije $\operatorname{sgn} f'$. Možemo simbolički sa x_0+0 označiti svaki broj $>x_0$ vrlo blizak broju x_0; slično x_0-0 neka bude oznaka za svaki broj oblika x_0-h za dovoljno male brojeve $h>0$.

Tada prema (6), imamo, ovu tablicu:

		x_0-h	x_0+h	
	$\operatorname{sgn}(x-x_0)$	-1	1	
1. slučaj:	$\operatorname{sgn} f'$	1	1	
	$\operatorname{sgn} f$	-1	1	
	f	<0	>0	f raste
2. slučaj:	$\operatorname{sgn} f'$	1	-1	
	$\operatorname{sgn} f$	-1	-1	
	f	<0	<0	
3. slučaj:	$\operatorname{sgn} f'$	-1	1	
	$\operatorname{sgn} f$	1	1	
	f	>0	>0	
4. slučaj:	$\operatorname{sgn} f'$	-1	-1	
	$\operatorname{sgn} f$	1	-1	
	f	>0	<0	f pada

Na taj način, promatrajući f' u okolini ništišta x_0 od f, dobije se uvid u vladanje same funkcije f u okolini $O(x_0)$.

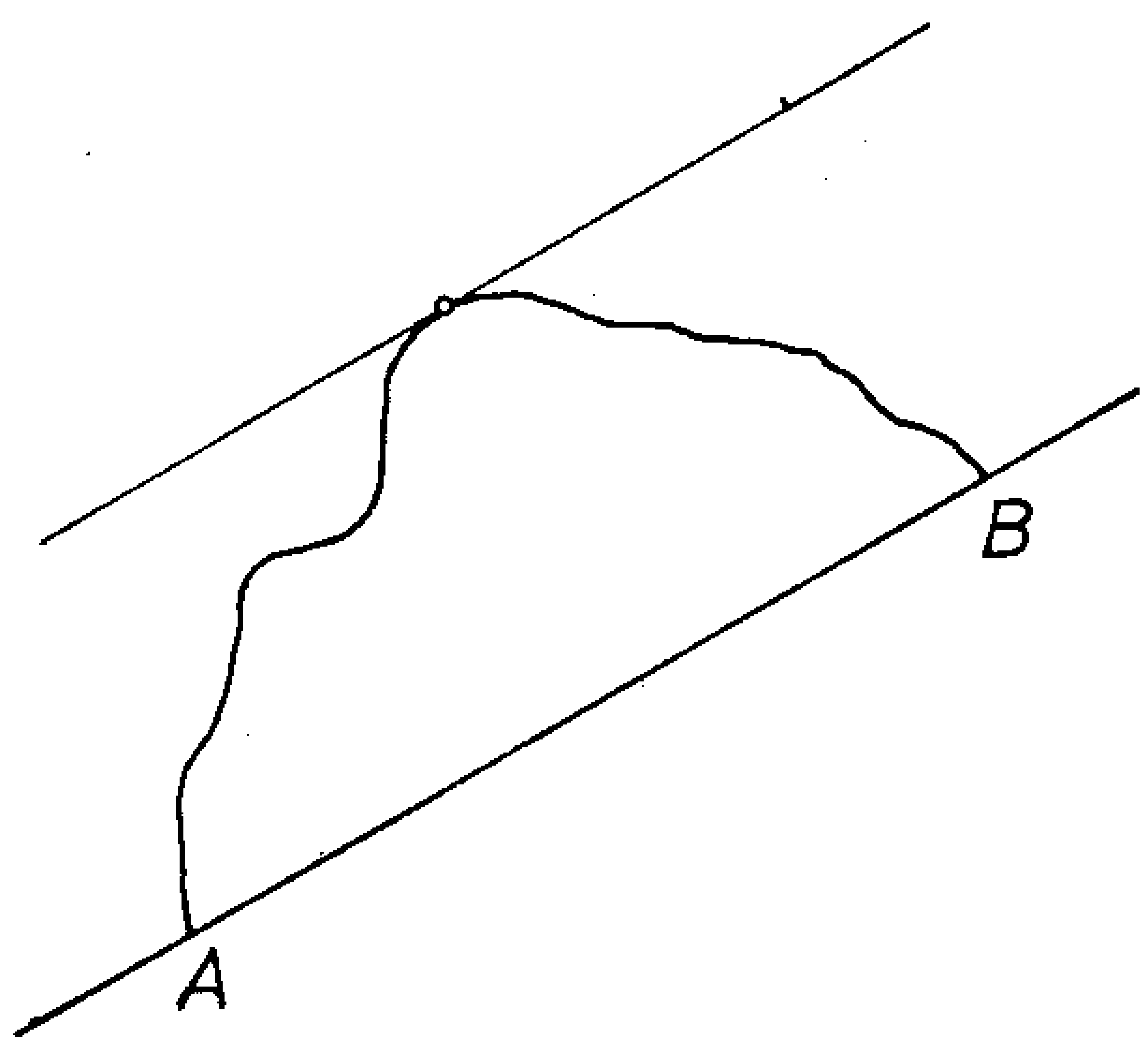
Primjedba. Slični zaključci o rastenju ili padanju funkcije f lijevo ili desno od x_0 vrijede i onda ako nije nužno $f(x_0)=0$.

3. OKO ROLLEOVA TEOREMA[1]

Jedan od središnjih teorema u diferencijalnom računu iz kojega izviru ostali teoremi te matematičke oblasti je ovaj

—→ **3.1.** Teorem. (*M. Rolle*). *Ako je realna funkcija f jednoznačna i neprekidna u zatvorenom intervalu I, a k tome izvodljiva u unutrašnjosti intervala I, tada iz pretpostavke da se f poništava na krajevima intervala I izlazi da se derivat f' poništava bar u jednoj tački u nutrini tog intervala realnih brojeva.*

Mnogo je jednostavnija geometrijska formulacija. Grubo govoreći: *za svaki luk $\widehat{AB}$ krivulje koja je »prilično pravilna« postoji jedna tangenta otvorenog luka AB koja je paralelna s tetivom AB.*



Sl. 3.1.

Tako jednostavna, a tako dalekosežna činjenica! Psihološki ukazujemo pri tom na ovu činjenicu: čitajući tu geometrijsku formulaciju (to je zapravo već tzv. *teorem o srednjoj vrijednosti*), mi obično imamo na umu vrlo jednostavne, svakidašnje lukove i krivulje; dobro je da tako radimo, da se bolje zagleda ideja. No, naknadno treba dobro ispitati doseg pojmova s kojima radimo. Naime, npr. u konkretnom slučaju, u ono doba kad je Rolle našao svoj teorem ni izdaleka se nije moglo *definirati* što je to luk, krivulja itd. pa da te riječi pokriju odgovarajuće pojmove današnje matematike! Danas se npr. zna da ima „krivulja" koje ispune čitav kvadrat, čitavu kocku, hiperkocku itd. (to je otkrio G. Peano (1858—1932); v. Đ. Kurepa [1] § 29.7.3.). Naravno da za takve „divlje" krivulje neće vrijediti gornja formulacija Rolleova teorema.

3.2. Za *algebarske polinome* može se Rolleov *pooštriti* ovako:

—→ **Teorem. (Rolle).**[1] ***Ako su c, d, dva uzastopna (susjedna) ništišta algebarskog polinoma $f(x)$, tada derivat f' ima u otvorenom intervalu $R(c, d)$ neparan broj ništišta (u gornjoj formulaciji* 3.1. *moglo se zaključiti da f' ima bar jedno ništište položeno negdje između c i d.).***

---

[1] Michel Rolle [Mišél Rol] (1652—1719), francuski matematičar; teorem je objavio u poznatom djelu *Traité d' Algèbre*, 1690.

D o k a z. Prema principu supstitucije 2.8. dovoljno je da vidimo da je

$$f'(I_0) \cdot f'(I_1) < 0,$$

pa da zaključimo da f' u $R(c,d)$ ima *neparno* mnogo ništišta, pri čemu se svako ništište računa sa svojom kratnosti. Pri tom I označuje interval unutar $R(c,d)$ proizvoljno blizak samom intervalu $R(c,d)$; dalje je I_0 lijevi, a I_1 desni kraj intervala I. Treba, dakle, dokazati da je

$$\operatorname{sgn} f'(c+h) \cdot f'(d-h) = -1 \tag{1}$$

za vrlo male brojeve $h > 0$.

No, promatrajmo

$$\operatorname{sgn} \frac{f}{f'} = \frac{\operatorname{sgn} f}{\operatorname{sgn} f'} \text{ u nutrini intervala } [c,d]. \tag{2}$$

U blizini broja c teorem 2.9. kaže da je funkcija (2) $= \operatorname{sgn}(x-c) = 1$; isti teorem osigurava da je funkcija (2) u blizini desnog kraja d jednaka $\operatorname{sgn}(-d) = -1$ (nas ne zanima zasad što se zbiva izvan $R(a,b)$). To znači da funkcija (2) nije konstanta u (c,d), jer specijalno u blizini krajeva a i b uzima *suprotne* vrijednosti. No, u intervalu (c,d) funkcija $\operatorname{sgn} f$ jest konstanta: u obratnom slučaju bile bi bar dvije tačke c', d' položene unutar (c,d), tako da bude

$$\operatorname{sgn} f(c') \neq \operatorname{sgn} f(d'), \quad \text{tj.} \quad f(c') f(d') < 0,$$

pa bi prema Bolzanovu teoremu bilo bar jedno $x_0 \in R(c',d')$ sa svojstvom $f(x_0) = 0$; dakle bi bilo $f(x_0) = 0$ i $c < x_0 < d$, protivno pretpostavci da su c, d bila *susjedna* ništišta funkcije f. Dakle je zaista funkcija $\operatorname{sgn} f$ konstantna u $R(c,d)$. No, to znači da onda funkcija $\operatorname{sgn} f'$ nije konstanta u $R(c,d)$ i da kao kvocijent $\dfrac{\operatorname{sgn} f}{\operatorname{sgn} f'}$ konstante $\operatorname{sgn} f$ i funkcije $\operatorname{sgn} f'$ uzima u blizini krajeva c, d protivne vrijednosti Q. E. D.

Izvedimo neke posljedice iz Rolleova teorema.

3.3. T e o r e m. **(Realnost nula-tačke polinoma).** *Između dva susjedna ništišta derivata f' polinoma f nalazi se najviše jedno ništište samog polinoma f* (pri tom to ništište ne može biti višestruko).

Kad bi se, naime, između dva uzastopna ništišta x_1, x_2 od f' nalazila dva različita ništišta a, b polinoma f nalazila bi se unutar $R(a,b)$, dakle i unutar $R(x_1,x_2)$ bar jedno ξ, za koje je $f'(\xi) = 0$, protivno pretpostavci da su x_1, x_2 *susjedne* nula-tačke za f'. Iz posljednjeg razloga ne može nijedno ništište polinoma f koje leži između x_1, x_2 imati kratnost > 1.

3.4. T e o r e m. Ako funkcija f u intervalu I ima k realnih ništišta, tada derivat f' u I ima bar $k-1$ ništište (svako ništište se broji sa svojim stepenom kratnosti), tj. $\nu(I,f') \geqq \nu(I,f) - 1$ pri čemu $\nu(I,g)$ označuje koliko g u I ima ništišta.

Stvarno, neka su

$$x_1, \ldots, x_s \tag{3}$$

različita uzlazna ništišta polinoma f u I, i to kratnosti $k_1, k_2, \ldots, k_s$; dakle je $k_1 + k_2 + \cdots + k_s = \nu(I;f)$. No, ti isti brojevi (3) su ništišta kratnosti $k_1 - 1, \ldots, k_s - 1, \ldots$ polinoma f', tako da je $\nu(I, f')$ jednako bar sumi tih brojeva; u drugu ruku, između svaka dva uzastopna člana niza (3) leži prema Rolleovu teoremu bar jedno ništište polinoma f', što daje ukupno bar $s-1$ novih ništišta koja nisu u (3); ukupno je, dakle,

$$\nu(I, f') \geqq \sum_{i=1}^{s} (k_i - 1) + (s-1) = \sum_{i=1}^{s} k_i - 1 = \nu(I;f) - 1.$$

Dakle, zaista $\nu(I, f') \geqq \nu(If) - 1$; a to je trebalo da se dokaže.

3.5. Teorem. *Ako polinom p ima sva ništišta realna, tada to vrijedi i za p', p'' itd.*

Naravno, dovoljno je stvar pokazati za p'. Najprije, prema 3.4, ima f' bar $n-1$ realno ništište. No, prema osnovnom teoremu algebre ima p' kao polinom stepena $n-1$ baš $n-1$ rješenje. Time je sve dokazano.

4. DESCARTESOV TEOREM. BUDAN-FOURIEROV TEOREM

Ako su svi koeficijenti algebarskog polinoma istog predznaka, jasno je da on ne može imati nijednog *pozitivnog* ništišta. Zato naslućujemo da će postojati neka veza između broja *pozitivnih ništišta* polinoma $p(x)$ i pojave raznih preznaka njegovih koeficijenata. Descartes je u tom pogledu našao teorem kojim se došlo najdalje dokle se moglo doći u ono doba, bez upotrebe pojmova derivata funkcije.

→ **4.1. Teorem. (Descartes)**[1]. *Broj pozitivnih ništišta algebarskog polinoma $f(x)$, svako brojeno svojom kratnošću, za paran broj je manji nego što niz koeficijenata sređenog polinoma $f(x)$ pokazuje promjena predznaka idući od člana na član (broj negativnih ništišta polinoma $f(x)$ jednak je broju pozitivnih ništišta polinoma $f(-x)$, koji nastaje iz zadana polinoma pišući $-x$ umjesto argumenta x).*

4.1.1. Bugarski matematičar *Nikola Obreškov* (1896—1963) poopćio je Descartesov teorem ovako:

Neka je $a(x)$ cijela racionalna funkcija stepena n i s realnim koeficijentima; ako je V broj promjena predznaka niza $a_0, a_1, \ldots, a_n$, tada je broj ništišta od $a(x)$ kojima je argument u intervalu $R\left(\frac{\pi}{n-V}, \frac{\pi}{n-V}\right)$ jednak V ili je za paran broj manji. (v. Н. Обрешков, Доклады Ак. Н. СССР, 85 (1952) 489—492; također N. Obreškov [2] str. 82).

[1] *René Descartes* (č. Rene Dekart) (1596—1650), veliki francuski filozof i matematičar; poznat je pod latinskim imenom *Cartesius* (č. Kartezijus).

Uvedimo odmah ova dva pojma.

4.2. Definicija. **Promjena ili varijacija predznaka.** Neka je

$$x_0, x_1, \ldots, x_k \tag{1}$$

niz realnih brojeva $\neq 0$; kaže se da svaki par *susjednih* članova niza (1) sa *suprotnim* predznacima daje ili prikazuje jednu *promjenu ili varijaciju predznaka* u nizu (1). Broj svih tih varijacija zove se *broj varijacija predznaka niza* (1). Ako u nekom nizu dolazi i 0 kao član, onda se broj varijacija takva niza definira kao broj varijacija niza dobivenog ispuštanjem svih članova koji su $=0$.

Analogno se definira pojam *permanencije, postojanosti ili istrajnosti* predznaka: tu se radi o svakom paru *susjednih* članova s *istim predznakom.*

Tako npr. trinom

$$-6x+1+3x^2$$

sređen uzlazno daje ove koeficijente:

$$1, \quad -6, \quad 3.$$

Tu imamo dvije promene predznaka: prelaz od 1 na -6 i prelaz od -6 na 3. Znači da pozitivnih realnih ništišta može biti ili 2 ili 0. A to znamo i inače.

4.3. Primjer. Polinom

$$5x^4-x^3+4x^2-1+x^7 \tag{1}$$

ima ovaj niz koeficijenata:

$$-1, \quad 0, \quad 4, \quad -1, \quad 5, \quad 0, \quad 0, \quad 1.$$

Promjene ili varijacije predznaka jesu: -1, 4 (broj 0 ispuštamo) 4, -1, -1, 5; dakle, za broj v promjena ili varijacija predznaka imamo $v=3$. Prema tome, gornji polinom (1) ima ili 3 ili 1 pozitivno ništište, dakle ima bar jedno pozitivno ništište. Riješimo slično pitanje za *negativne* korijene. No, negativna ništišta funkcije f jesu $-x_0$, gdje je x_0 proizvoljno pozitivno ništište funkcije $f(-x)$. Prema tome, dovoljno je naći broj pozitivnih korijena polinoma $f(-x)$, koji za (1) glasi:

$$5x^4+x^3+4x^2-1-x^7.$$

Koeficijenti su

$$-1 \quad 4, \quad 1, \quad 5, \quad -1, \quad \text{tj.} \quad v=2.$$

Dakle: polinom (1) ili je bez negativnih ništišta ili ima dva negativna ništišta (može biti i jedno, ali je ono onda kratnosti 2).

Ostaje još broj 0: broj 0 nije ništište za (1). Dakle: polinom (1) može imati najviše pet realnih ništišta: to znači da ima sigurno bar jedan par nerealnih (i konjugiranih) ništišta.

Descartesov teorem je specijalan slučaj Budan-Fourierova teorema (§ 4.5).

4.4. Budan-Fourierov niz za zadani polinom. — 4.4.1. Definicija. Uz polinom f stepena n promatrajmo niz njegovih derivatâ:

$$f(x), \quad f'(x), \quad f''(x), \ldots, f^{(n)}(x).$$

Taj se niz zove *Budan-Fourierov niz zadanog polinoma.* Gledajmo kako se mijenja broj varijacija $V(x)$ niza (1) kad x putuje po brojevnoj crti. Naravno da se $V(x)$ eventualno mijenja jedino kad x prolazi preko kojeg ništišta z kojeg člana u (1).

4.4.2. Prvi slučaj. Uzmimo najprije slučaj da je $f(z)=0$, pa neka je z k-struko ništište; to znači da je

$$f(z)=f_1'(z)=\ldots=f^{(k-1)}(z)=0,\ f^{(k)}(z)\neq 0.$$

No, u neposrednoj blizini ništišta z imaju funkcije

$$x-z, \frac{f^{(i)}(z)}{f^{(i+1)}(z)}\ (i=0, 1, \_, \ldots, k-1)$$

isti znak (§ 2.9). To znači da u lijevom susjedstvu od z prvih $1+k$ članova niza (1) pokazuje k-varijacija, dok neposredno desno od z te funkcije uopće ne pokazuju varijacija u predznaku. Drugim riječima, prelazom preko svakog ništišta z od $f(x)$ gubi se k varijacija koje proizlaze iz promatranja početnog odlomka niza (1) od prvih $1+k$ članova. Odmah ćemo vidjeti kako se to očituje ako je to isto z ništište i kojeg daljeg člana niza (1), poslije člana $f^{(k)}$, za kojega znamo da je $f^{(k)}(z)\neq 0$. Dolazimo, dakle, na

4.4.3. Drugi slučaj. z je ništište nekog srednjeg člana, recimo

(2) $$f^{(\alpha-1)}(z)\neq 0,\ f^{(\alpha)}(z)=0,\ f^{(\alpha+1)}(z)=0,\ldots,f^{(\alpha+r-1)}(z)=0,$$
$$f^{\alpha+r}(z)\neq 0.$$

To znači da je z ništište za $f^{(\alpha)}$ kratnosti r. Rasuđivanje iz prethodnog slučaja kazuje da prelaskom varijable preko broja z komad

(3) $$f^{(\alpha)}(x),\ f^{(\alpha+1)}(x),\ldots,f^{(\alpha+r-1)}(x),\ f^{(\alpha+r)}(x)$$

niza (1) *gubi* upravo r promjenâ. Još treba ispitati što je s komadom

(4) $$f^{(\alpha-1)}(x),\ f^{(\alpha)}(x)$$

kad varijabla x preskoči s lijeve strane na desnu stranu od z.

No, prema teoremu 2.7. za dovoljno malu okolinu O broja z imamo:

(5) $$\operatorname{sgn} f^{(\alpha)}(O_0)=(-1)^r f^{(\alpha)}(O_1),$$

gdje je O_0 lijevi, a O_1 desni kraj intervala O.

Imamo dva podslučaja.

Prvi podslučaj: *r je parno.* Tada iz (5) izlazi da je $\operatorname{sgn} f^{(\alpha)}$ konstanta u $O(z)$, pa zato niz (4) ne doživljuje nikakve promjene predznaka. To znači da duži niz (3) gubi upravo paran broj r promjena predznaka.

Drugi podslučaj: *r je neparno.* Tada (5) kazuje da $f^{(\alpha)}$ u O_0 i O_1 ima suprotne predznake; to znači da u nizu (4) prelaskom sa niza

$$f^{(\alpha-1)}O_0,\ f^{\alpha}O_0 \quad \text{na} \quad f^{(\alpha-1)}O_1,\ f^{(\alpha)}O_1$$

imamo jednu promjenu predznaka; to može biti gubitak varijacije ili dobitak jedne promjene (recimo prelaz sa 1,1 na 1 —1 ili obratno); no to znači da niz (2) u O_0 i O_1 gubi $r \pm 1$ promjenâ predznaka, tj. gubi paran broj promjena predznaka (parno zato jer je r neparan broj).

Dakle, drugi slučaj kaže da se prelaskom preko nulišta z nekog srednjeg člana gubi paran broj promjena predznaka u komadu (2) niza (1). Radeći tako i u eventualnom duljem komadu niza (1), došli bismo do analognog zaključka, pa smo time dokazali[1] ovaj

—→ **4.5. Budan-Fourierov teorem**[2]. *Ako je $f(x)$ algebarski polinom stupnja n, tada se u nizu*

$$f(x),\ f'(x),\ f''(x), \ldots, f^{(n)}(x) \tag{1}$$

prelaskom od $x=a$ na veći broj $x=b$ broj varijacija $V(x)$ u tom nizu (1) *ne povećava, nego ostaje bez promjena ili se umanjuje*, tj. $V(a) \geqslant V(b)$. *Razlika $V(a)-V(b)$ je jednaka broju ν korijena jednadžbe $f(x)=0$, koji su u $R(a, b)$, ili je za paran broj veća od broja ν*; dakle je $Va-Vb-\nu$ paran broj ≥ 0.

4.5.1. Primjer. Za polinom

$$f(x)=x^4+x^3-3x^2+x-100 \tag{6}$$

iz § 1.2.1. glasi Budan-Fourierov niz ovako:

(7) $x^4+x^3-3x^2+x-100,\ 4x^3-3x^2-6x+1,\ 12x^2+6x-6,\ 24x+6,\ 24.$

Nađimo V_1; dovoljno je gledati predznake u (7); oni su:

$$-1,\ 1,\ 1,\ 1,\ 1, \quad \text{tj. } V_1=1. \quad \text{Slično } V_0=3,\ V_2=1.$$

To znači da je za $2<x$, $V_2-V_x=1$, tj. postoji jedan jedini korijen >2. Nađimo V_3; pripadna je sekvencija predznaka: $-1, 1, 1, 1, 1$ itd. Dakle $V_3=1$; dalje $V_4=0$, tj.

$$V_3-V_4=1;$$

to znači da polinom (6) ima jedno jedino pozitivno ništište $z>2$ i ono je smješteno između 4 i 3; dakle $z=3,\ldots$

Nastaje problem daljeg određivanja. Treba sada odrediti koji od intervala

$$(3;\ 3{,}1],\quad (3{,}1;\ 3{,}2], \ldots (3{,}9;\ 4]$$

sadrži to ništište. Treba tražiti V_x za te brojeve

$$x=3{,}1;\quad 3{,}2;\quad 3{,}3; \ldots;\ 3{,}9 \quad \text{itd.}$$

4.6. Dokaz Descartesova teorema. Primijenimo Budan-Fourierov teorem na interval $R(0, \infty)$ svih pozitivnih realnih brojeva. Broj varijacija V_0 Budan-Fourierova niza za polinom

$$f(x)=f_0+f_1x+\cdots+f_nx^n$$

[1] Preporučuje se čitav gornji dokaz ponoviti za slučaj da su ništišta z jednostruka!

[2] Čini se da je teorem otkrio Fourier [Furje] (1768—1830) god. 1796, a Budan god. 1811; izašao je u Fourierovu djelu *Analyse des équations*, 1831. (Ispitivanje jednadžbi).

za $x=0$ je broj varijacija niza

$$f(0)=f_0, f'(0)=f_1, f''(0)=2!\,f_2, f'''(0)=3!\,f_3, \ldots,$$
$$f^{(n-1)}(0)=(n-1)!\,f_{n-1}, f^{(n)}(0)=n!\,f_n \text{ (isp. pogl. 5, § 11. 3).}$$

Drugim riječima, V_0 je broj varijacija koeficijenata $f_0, f_1 \ldots, f_{n-1}, f_n$ polinoma f. Svi pak članovi Budan-Fourierova niza imaju za $x=\infty$ znak kao i f_n, $n=\operatorname{st} f$, pa niz uopće ne pokazuje varijacija (§ 1.3.1); tj. $V_\infty=0$. Dakle je $V_0-V_\infty=V_0-0=$ broj pozitivnih korijena + paran broj, tj.

$$\nu(0,\infty)_f=V_0-\text{paran broj};$$

a to je Descartesov teorem.

4.6.1. Inače, najjednostavniji dokaz Descartesova teorema dao je 1756. god. Segner, a osniva se na činjenici da produkt $g(x)\cdot(x\pm c)$ ima jednu varijaciju više predznaka nego što ih ima polinom $g(x)$.

5. STURMOV TEOREM[1)]

5.1. Sturmov lanac. Sturmov teorem daje odgovor na pitanje *koliko polinom f u intervalu $R(a,b)$ ima korijena.* Pretpostavit ćemo da polinom f nema višestrukih nula-mjesta, tako da su, dakle, f i f' relativno prosti polinomi. Primijenivši na f, f' Euklidov algoritam (pogl. 7, § 5), to znači da će posljednji divizor pri diobi biti konstantan; iz naročitih razloga ostatke ćemo snabdjeti znakovima —; radi pregleda stavimo

$$f=v_0, f'=v_1; \tag{1}$$

pa neka je

$$\begin{aligned} v_0&=v_1 q_1-v_2\\ v_1&=v_2 q_2-v_3\\ &\cdots\cdots\\ v_{k-1}&=v_k q_k-v_{k+1}\\ &\cdots\cdots\\ v_{s-2}&=v_{s-1} q_{s-1}-v_s\\ v_{s-1}&=v_s q_s. \end{aligned} \tag{E}$$

Prema pretpostavci, v_s je konstanta, odnosno izraz koji ne mijenja znaka.

Napose

$$v_s(x)\neq 0, \quad (x\in R). \tag{2}$$

Tako dobivamo niz polinoma

$$v_0, v_1, v_2, \ldots, v_k, \ldots, v_{s-1}, v_s, \tag{S}$$

koji se zove *Sturmov lanac ili Sturmov niz koji pripada polinomu $f=v_0$.*

[1)] J.C. F. Sturm (1803—1855), švicarski matematičar; teorem je dokazao 1829.

5.2. Kvadratni trinom. Kubni polinom. — 5.2.1. Sturmov lanac kvadratnog trinoma ax^2+bx+c. Prva dva člana lanca su

$$ax^2+bx+c,\ 2ax+b.$$

Treći ćemo naći dijeljenjem:

$$\begin{array}{l} 2a^2(ax^2+bx+c):(2ax+b)=a^2x+\dfrac{ab}{2} \\ \underline{-2a^3x^2 \pm a^2bx} \\ \qquad a^2bx+2a^2c \\ \qquad \underline{-a^2bx \pm \dfrac{a^2b}{2}} \\ \qquad\qquad -\dfrac{a}{2}(b^2-4ac)=-\dfrac{a}{2}D; \end{array}$$

treći je član dakle

$$-\left(-\frac{a}{2}D\right),\ \text{tj.}\ \frac{a}{2}D\ \text{ili}\ aD.$$

Prema tome, Sturmov lanac glasi:

$$ax^2+bx+c,\ 2ax+b,\ aD.$$

Usporedi taj lanac s Budan-Fourierovim lancem:

(3) $$ax^2+bx+c,\ 2ax+b,\ 2a.$$

5.2.2. Sturmov lanac polinoma x^3+px+q.

$$\begin{array}{l} 3(x^3+px+q):(3x^2+p)=x \\ \underline{-3x^3 \pm px} \\ \quad 2px+q=-(-2px-3q) \\ \quad 2p^2(3x^2+p):(-2px-3q)=-3px+\dfrac{9}{2}q \\ \quad \underline{-6p^2x^2 \pm 9pqx} \\ \qquad -9pqx+2p^3 \\ \qquad \underline{\mp 9pqx \mp \dfrac{27}{2}q^2} \\ \qquad\qquad \dfrac{27}{2}q^2+2p^3=\dfrac{1}{2}\overbrace{(27q^2+4p^3)}^{-D}=\dfrac{1}{2}\cdot -D. \end{array}$$

Niz glazi:

(4) $$x^3+px+q,\ 3x^2+p,\ -2px-3q,\ -27q^2-4p^3=D.$$

5.3. Svojstva Sturmova lanca. Sturmov niz ima nekoliko jednostavnih svojstava, koja ćemo sada nabrojiti.

5.3.1. Lema. *Dva uzastopna člana u Sturmovu nizu nemaju nijedno zajedničko ništište.*

Naime, *prema* (E) iz $v_{k-1}(x)=v_k(x)=0$ izlazilo bi i $v_{k+1}(x)=0$, pa dakle i $v_{k+2}=0$, a nakon nekoliko koraka zaključili bismo da i posljednji član v_s iščezava: $v_s(x)=0$, protivno pretpostavci (2).

5.3.2. Lema. *Ako je*

$$v_k(a)=0,\ 0<k<s,$$

tada je

$$v_{k-1}(a)=-v_{k+1}(a),$$

tj. *ako je a nula-tačka kojeg srednjeg člana Sturmova lanca, tada susjedni članovi lanca u a poprimaju suprotne brojeve.*

Lema neposredno izlazi iz k-te jednakosti sistema (E).

5.3.3. Lema. *Ako u zatvorenom odresku* $R[x_1, x_2]$ *ne iščezava nijedanput nijedan član Sturmova lanca* (S), *tada je*

$$\operatorname{sgn} v_\sigma(x_1)=\operatorname{sgn} v_\sigma(x_2) \quad za\ \sigma\leq s. \tag{4}$$

U obrnutom slučaju, brojevi $v_\sigma(x_1)$, $v_\sigma(x_2)$ bili bi suprotno označeni, pa bi prema Bolzanovu teoremu postojalo bar jedno ništište polinoma u $[x_1, x_2]$, protivno pretpostavci.

—→ **5.4. Sturmov teorem.** ***Zadan je polinom $f(x)$ i broj a; označimo sa***

$$V(f;a) \quad \textit{ili kraće} \quad V(a)$$

broj varijacija niza što se iz Sturmova niza (S) dobije uvrštavanjem vrijednosti a za nezavisnu varijablu. Ako polinom f nema višestrukih ništišta (nulamjesta), tj. ako je $M(f,f')=1$, tada je broj ništišta polinoma f u otvorenom intervalu $R(a,b)$ jednak razlici

$$V(f;a)-V(f;b)$$

varijacija što ih Sturmov niz pokazuje na početku a i na svršetku b promatranog intervala.

Dokaz. Najprije je jasno da se broj varijacija u nizu (S) može promijeniti jedino onda kad varijabla prolazi preko ništišta bar jednog člana niza (S). Pa neka je z broj u kojem se poništava bar jedan član niza (S).

Razlikujemo dva moguća slučaja (isp. dokaz Budan-Fourierova teorema, § 4.5).

5.4.1. Prvi slučaj: $v_k(z)=0$ za neko $k>0$. Prema lemi 5.3.2. brojevi $v_{k-1}(z)$, $v_{k+1}(z)$ su suprotno označeni te $\neq 0$; radi neprekidnosti, može se odrediti tako mala okolina $O(z)$ oko z da u njoj funkcije v_{k-1}, v_{k+1} ne mijenjaju znaka, tako dakle da u nizu v_{k-1}, v_{k+1} broj varijacija ostaje isti kad varijabla putuje slijeva nadesno u $O(z)$. To isto vrijedi i za niz

$$v_{k-1},\ v_k,\ v_{k+1},$$

kao što se odmah utvrđuje. Naime, krajnji članovi daju za predznake ili

$$+1, \quad -1 \quad \text{ili} \quad -1, \quad +1;$$

uklopi li se između njih bilo kakav broj, broj se varijacija ne mijenja, jer npr.

$$V(1, \ -1) = V(1, \ 1, \ -1) = V(1, \ -1, \ -1).$$

5.4.2. Drugi slučaj: $v_0(z)=0$, tj. $f(z)=0$; z je ništište zadanog polinoma f. Prema teoremu 2.9. u dovoljno maloj okolini O broja z imaju funkcije $x-z$ i $\frac{f(x)}{f'(x)}$ isti predznak; to znači da su u lijevom susjedstvu broja z funkcije f i f' protivno označene, a neposredno desno od z one su istog predznaka. Drugim riječima, kad varijabla x pređe preko z, *gubi niz* f, f' (to je dvočlani početak lanca (S)) jednu promjenu predznaka. Dokažimo da to vrijedi i za čitav niz (S). Razlikujemo dvije mogućnosti:

(*a*) Broj z je ništište još nekog f_k, $k \neq 0$; tada kao i u slučaju 5.4.1. zaključujemo da niz (1) $f_1, f_2, \ldots, f_s$ ima isti broj promjena predznaka u čitavom intervalu $O(z)$ koji osim z ne obuhvata nikoje drugo ništište nijedne od funkcija (1).

(*b*) $f_k(z) \neq 0$ $(k=1, 2, \ldots, s)$. Tada nijedna od funkcija u (1) ne mijenja svoj predznak u spomenutom Oz.

Ukratko, kad varijabla raste i prijeđe preko jednog korijena jednadžbe $f(x)=0$, tada Sturmov lanac (S) izgubi jednu jedinu varijaciju predznaka. Tih je gubitaka u $R(a, b)$ toliko koliko se puta f poništava unutar $R(a, b)$. Time je Sturmov teorem dokazan.

5.5.1. Primjedba. Ako se usporedi dokaz Sturmova teorema i dokaz Budan-Fourierova teorema, vidi se da su dokazi slični. Prividno je dokaz Fourierova teorema zamršeniji; to proizlazi odatle što se tamo ispituju i prelazi preko ništišta svake funkcije $f^{(\alpha)}$ pri $\alpha \geq 1$.

5.5.2. Napomena. Pri određivanju broja korijena u $R(a, b)$ nije potrebno za posljednji član Sturmova niza uzeti baš najveću zajedničku mjeru $M(f, f')$; dovoljno je ići do jednog člana u Sturmovu nizu koji u $R(a, b)$ nema ništišta. Npr. neka je

$$f = x^4 - 2x^2 + x - 1 = 0.$$

Dakle

$$f' = 4x^3 - 4x + 1$$

$$4(x^4 - 2x^2 + x - 1) : (4x^3 - 4x + 1) = x$$

$$\frac{-4x^4 \mp 4x^2 \pm x}{-4x^2 + 3x - 4 = r(x).}$$

No, Diskr. $r(x) < 0$, što znači da je $r(x) < 0$ za svaki broj x, pa je dovoljno promatrati niz $f, f', -r$, tj. niz

$$\underset{x^4-2x^2+x-1,}{f} \quad \underset{4x^3-4x+1,}{f'} \quad \underset{4x^2-3x+4.}{-r}$$

5.6. Slučaj višestrukih ništišta (nula-tačaka) polinoma $f(x)$. Neka je $f M f' = M$ najveća zajednička mjera polinomâ f, f'. Tada polinom $\frac{f}{M}$ ima samo jednostruka ništišta, a sva su ništišta zajednička s onima od f. Uistinu, ako je z k-struko ništište od f, tada je $f(x)$ djeljivo sa $(x-z)^k$, a f' sa $(x-z)^{k-1}$; dakle je $M(x)$ djeljivo sa $(x-z)^{k-1}$, pa je z jednostavno ništište od $\frac{f}{M}$.

Dakle polinomi f i $\frac{f}{M}$ imaju ista ništišta. Posljednji polinom ima samo jednostruka ništišta.

⟶ **5.6.1. Teorem.** ***Neka je $f(x)$ algebarski polinom s realnim koeficijentima, a α, β dva realna broja za koje je $\alpha<\beta$; broj ništišta polinoma $f(x)$ koja su smještena između α, β a svako računato kao prosto ništište, jednak je broju gubitaka varijacija predznaka Sturmova niza polinoma f pri prelazu varijable x s α na β.***

Naime, dijeleći svaki član Sturmova niza (S) funkcije f najvećom zajedničkom mjerom M od f, f' dobije se Sturmov niz (S') polinoma $\frac{f}{M}$. To neposredno izlazi iz definicije nizova (S), (S') jer M zapravo nastaje normiranjem posljednjeg člana niza (S). Kako nizovi (S), (S') imaju isti broj varijacija predznaka to primjenom teorema 5.4. na niz (S') izlazi i teorem 5.6.1.

5.7. Sturmov teorem i ispitivanje kvadratne jednadžbe. Sturmov lanac za kvadratni polinom $f \equiv ax^2+bx+c$ glasi (§ 5.2.1):

(S) $$ax^2+bx+c, \quad 2ax+b, \quad aD, \quad \text{gdje je} \quad D=b^2-4ac.$$

5.7.1. Nađimo uslov da oba korijena budu stvarna (realna). To znači da treba biti

$$V(f,-\infty)-V(f;+\infty)=2, \text{ dakle } V(f;\infty)=0, \ V(f,-\infty)=2.$$

Specijalno, dakle, mora biti $V(f,\infty)=0$. No, za $x=\infty$, niz (S) ima znakove:

$$\operatorname{sgn} a, \ \operatorname{sgn} a, \ \operatorname{sgn} aD, \text{ dakle mora biti i } \operatorname{sgn} aD = \operatorname{sgn} a, \text{ tj. } D \geqq 0,$$

5.7.2. Lema. Da oba korijena budu $<\alpha$, treba da niz

$$f(\alpha), \quad f'(\alpha), \quad a \quad \text{(ovaj niz je Budan-Fourierov)}$$

pokazuje dvije promjene predznaka, dakle su krajnji članovi istog znaka, susjedni različita znaka:

(1) $$af(\alpha)>0, \quad af'(\alpha)<0, \text{ naravno, uz } D \geqq 0.$$

5.7.3. Lema. *Da oba korijena budu $<\beta$, treba da je $D \geqq 0$ i da niz*

$$f(\beta), \quad f'(\beta)$$

ne pokazuje promjena predznaka, što je ekvivalentno sa sistemom:

(2) $$af(\beta)>0,\ af'(\beta)>0.$$

⟶ **5.7.4.** Teorem. *Da korijeni kvadratna polinoma*

$$f(x)\equiv ax^2+bx+c$$

budu u $R(\alpha,\beta)$ *treba a i dosta je da je* $D\geqq 0$ *te* (1) *i* (2). *Specijalno, uslov* $af(\alpha)>0$ *znači da broj* α *ne leži između korijena* (stvarno, za svaki broj x između korijena vrijedi $af(x)<0$).

Nejednakost

$$af'(\alpha)<0,\ tj.\ a(2a\alpha+b)<0\ daje\ \alpha<-\frac{ab}{2a^2}=-\frac{b}{2a}.$$

Isto tako

$$af'(\beta)>0,\quad tj.\quad \beta>-\frac{b}{2a}$$

(to je jasno, jer $-\frac{b}{2a}$ znači polovinu zbroja korijena).

Nužnost teorema je dokazana; dokažimo i dovoljnost: ako je $D\geq 0$ te ako vrijedi (1), (2), tada brojevi x_1, x_2 leže u $R(\alpha,\beta)$. Kako je $D\geq 0$, korijeni su realni; zbog $af(\alpha)>0$, odnosno zbog $af(\beta)>0$ ne leži ni α ni β u intervalu $R[x_1,x_2]$; to znači da $R(\alpha,\beta)$ obuhvata $R[x_1,x_2]$; zbog

$$af'(\alpha)<0>af'(\beta),$$

polusuma $-\frac{b}{2a}$ korijenâ je veća od α, a manja od β; dakle je zaista $\alpha<\{x_1,x_2\}<\beta$.

5.7.5. Specijalno se često traži da korijen bude u $[-1, 1]$, pa da se može prikazati u obliku sinusa, odnosno kosinusa.

5.8. Kubna jednadžba i Sturmov teorem. Za kubnu jednadžbu $x^3+px+q=0$ glasi Sturmov niz (§ 5.2.2):

(S) $$x^3+px+q,\ 3x^2+p,\ -2px-3q,\ D:=-(27q^2+4p^3).$$

Gledajmo broj promjenâ znaka članova niza (S) za pojedino x, odnosno pripadnih predznaka.

1. *Slučaj* $D<0$, tj. $27q^2+4p^3>0$. Imamo ovu tablicu signuma niza (S):

x	$\operatorname{sgn} fx$	$\operatorname{sgn} f'x$	$\operatorname{sgn}(-2px-3q)$	$\operatorname{sgn} D$	broj varijacija predznaka
$-\infty$	-1	$+1$	$\operatorname{sgn} p$,	-1	2
$+\infty$	1	1	$-\operatorname{sgn} p$,	-1	1
				gubitak varijacija:	$\triangle V=2-1=1.$

To znači da jednadžba ima jedan realan korijen; ostala dva su nerealna.

2. *Slučaj* $D>0$, tj. $-(27q^2+4p^3)>0 \Rightarrow 27q^2+4p^3<0 \Rightarrow p<0$:

x	$\operatorname{sgn} fx$	$\operatorname{sgn} f'x$	$\operatorname{sgn}(-2px-3q)$	$\operatorname{sgn} D$	$V(x)$
$-\infty$	-1	1	$\operatorname{sgn} p=-1$	1	3
$+\infty$	1	1	1	1	0
					$\triangle V=3$

Ako je $D>0$, *sva tri korijena su realna. To je bio nesvodljivi slučaj* (*casus irreducibilis*, pogl, 5, § 6.4.3).

3. *Slučaj.* $D=0$, $q\neq 0$; dakle je $p<0$. Znamo da tada jednadžba ima i nejednostavno rješenje. Sturmov teorem nije dokazan za taj slučaj. Ipak, pogledajmo što daje niz (S):

x	$\operatorname{sgn} f(x)$	$\operatorname{sgn} f'(x)$	$\operatorname{sgn}(-2px-3q)$	$\operatorname{sgn} D$	$V(x)$
$-\infty$	-1	1	-1	0	2
∞	1	1	1	0	0
					$\triangle V=2$,

tj. izlaze dva realna rješenja. To i stoji tako, samo što samu kratnost teorem ne daje.

4. Pogledajmo slučaj jednadžbe $x^3=0$ (0 je 3-struko rješenje).

Gornja razmatranja daju ovu tablicu:

x	$\operatorname{sgn} f(x)$	$\operatorname{sgn} f'(x)$	$\operatorname{sgn}(-2px-3q)$	$\operatorname{sgn} D$	$V(x)$
$-\infty$	-1	1	0	0	1
∞	1	1	0	0	0
					$\triangle V=1$,

tj. jedno je rješenje realno. A ostala dva?

No, znajući da je broj 0 rješenje, treba ispitati kratnost toga rješenja; vidi se da je 0 trostruko rješenje!

6. BROJ NIŠTIŠTA POLINOMA $a(x)$ U ZADANOJ OBLASTI KOMPLEKSNIH BROJEVA

6.0. Neka je C zatvorena krivulja u ravnini kompleksnih brojeva: uzimat ćemo da C nema dvostrukih tačaka; sa C_i označit ćemo *unutrašnju* a sa C_e *vanjsku* oblast ravnine kojima je C zajedničko omeđenje; sam skup C nećemo ubrajati ni u C_i ni u C_e, tako da se čitava ravnina cijepa na *disjunktne* skupove C_i, C, C_e.

Ispitat *ćemo koliko zadan polinom* $a(z)$ *ima ništišta u skupu* C_i (svako ništište broji se svojom kratnošću).

6.1. Lema. *Neka je* z_0 *zadana tačka kompleksne ravnine; za svaki kompleksni broj* $z\neq z_0$ *razlika* $z-z_0$ *je jednaka vektoru* $\overrightarrow{z_0 z}$; *specijalno,* $\operatorname{Arg}(z-z_0)$ *je* *mjerni broj kuta što ga s apscisnom osi čini vektor* $\overrightarrow{z_0 z}$; *kad* z *proputuje kružnicom ili kakvom jednostavnom zatvorenom krivuljom* C *kompleksnih brojeva na kojoj leži* z_0, *tada se* $\operatorname{Arg}(z-z_0)$ *vrati na svoju polaznu vrijednost ili se promjeni za* 2π, *već prema tome da li* z_0 *leži u* C_e *ili u* C_i.

Dokaz leme je očigledan.

6.2. Lema. *Neka je polinom* $p(x) \neq 0$ *za svaku tačku* x *krivulje* C *kao i za svaku tačku oblasti* C_i; *kad* z *proputuje krivuljom* C *počev od proizvoljne tačke* $z' \in C$, *tada se broj* $\operatorname{Arg} p(z)$ *vrati na svoju polaznu vrijednost* $\operatorname{Arg} p(z')$.

Dokaz je jasan jer $\operatorname{Arg} p(z)$ znači mjerni broj kuta između apscisne osi i vektora $\overrightarrow{Op(z)}$, a polinom p preslikava skup $C \cup C_i$ u skup kome je ishodište vanjska tačka.

⟶ **6.3. Teorem. (tzv. princip o argumentu).** ***Broj ništišta polinoma*** $p(x)$ ***koja se nalaze u unutrašnjosti oblasti*** C_i ***zatvorene krivulje*** C ***dobije se tako da se sa*** 2π ***podijeli povećanje broja*** $\operatorname{Arg} p(z)$ ***kad*** z ***proputuje krivuljom*** C ***u pozitivnom smislu; pri tom se pretpostavlja da je*** $p(z) \neq 0$ ***za svako*** $z \in C$.

Dokaz. Neka je $z_1, z_2, \ldots, z_\nu \in C_i$ te

$$p(z) = (z-z_1)(z-z_2)\ldots(z-z_\nu)\,q(z) \tag{1}$$

te $q(z) \neq 0$ za svako $z \in C_i$. Iz (1) izlazi

$$\operatorname{Arg} p(z) = \operatorname{Arg}(z-z_1) + \operatorname{Arg}(z-z_2) + \ldots + \operatorname{Arg}(z-z_\nu) + \operatorname{Arg} q(z). \tag{2}$$

Kad z proputuje C u pozitivnom smislu, broj $\operatorname{Arg} q(z)$ se vrati na svoju polaznu vrijednost (§ 6.2); naprotiv, svaki od preostalih sumanada u $(2)_1$ poveća se za 2π; to znači da se $\operatorname{Arg} p(z)$ poveća upravo za $2\pi \cdot \nu$; a međutim ν je upravo broj ništišta od $p(z)$ unutar C_i. Specijalno, ako $p(z)$ nema nikoje ništište u C_i, tada je $p(z) = q(z)$, pa je uvećanje broja $\operatorname{Arg} p(z)$ jednako 0 pri svakom jednokratnom proputovanju tačke z po C.

6.4. Rouché-ov teorem [č. Ruše-ov teorem]. *Neka je* C *jednostavna zatvorena krivulja u ravnini kompleksnih brojeva, a* $p(z), q(z)$ *polinomi sa svojstvom* $|p(z)| < |q(z)|$ *za svako* $z \in C$; *tada polinom*

$$a(z) = p(z) + q(z)$$

ima unutar C_i *upravo onoliko ništišta koliko ih ima i* $q(z)$ (*naravno, da su općenito ništišta od* $q(z)$ *različita od ništišta polinoma* $a(z)$).

Dokaz. Imamo

$$a(z) = p(z) + q(z) = q(z) \cdot u(z),\; u(z) = 1 + \frac{p(z)}{q(z)}.$$

Dakle je
$$\operatorname{Arg} a(z) = \operatorname{Arg} q(z) + \operatorname{Arg} u(z).$$

Zato treba pratiti mijenjanje brojeva $\operatorname{Arg} a(z)$, $\operatorname{Arg} p(z)$, $\operatorname{Arg} q(z)$ pri kretanju broja z po C. Radi $|p(z)| < |q(z)|$ za $z \in C$ leži, za svako $z \in C$, tačka $\frac{p(z)}{q(z)}$ unutar jediničnog kruga oko O; to znači da za svako $z \in C$ tačka $u(z) = 1 + \frac{p(z)}{q(z)}$ leži u unutrašnjosti jediničnog kruga sa središtem u 1; zato kad z opisuje C opisivat će $u(z)$ određenu krivulju C' a O leži u vanjskoj oblasti C_e' te krivulje C'; prema tome, pri ophodu tačke T po C' vraća se broj $\operatorname{Arg} u$ na svoju polaznu vrijednost. To drugim riječima znači da pri ophodu tačke z po C izrazi $\operatorname{Arg} a(z)$, $\operatorname{Arg} q(z)$ dožive isto povećanje; a to prema principu o argumentu iz § 6.3. znači da funkcije $q(z)$, $a(z)$ imaju u C_i jednak broj ništišta.

Primijenimo Rouché-ov teorem i izvedimo iz njega

—→ **6.5. Osnovni teorem algebre (v. 7, § 13.1. (iii))** ***Svakom algebarskom polinomu $a(z)$ s kompleksnim koeficijentima pridružen je bar jedan kompleksni broj u kojem taj polinom uzima vrijednost 0. Tačnije: svaki algebarski polinom $a(x)$ s koeficijentima iz tijela $R(i)$ kompleksnih brojeva ima u $R(i)$ upravo $n(=\operatorname{st} a)$ ništišta; pri tom se svako ništište broji svojom kratnošću.***

D o k a z. Neka je

$$a(z) = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n, \quad a_n \neq 0; \qquad \text{tada je}$$

(1) $$a(z) = a_n z^n \left(\frac{a_0}{a_n} z^{-n} + \frac{a_1}{a_n} z^{-n+1} + \ldots + \frac{a_{n-1}}{a_n} z^{-1} + 1 \right).$$

No, kad $|z| \to \infty$, onda $z^{-1} \to 0$ i uopće $z^{-k} \to 0$ za svaki prirodni broj k. Zato se svaki član $\neq 1$ iz zagrade u (1) može po apsolutnoj vrijednosti učiniti proizvoljno malim za dovoljno veliko $|z|$; specijalno će za neko $r > 0$ i svako $|z| > r$ suma modulâ n članova u zagradi od (1) biti < 1; zato će pri $|z| > r$ pogotovo biti

$$\left| \frac{a_0}{a_n} z^{-n} + \frac{a_1}{a_n} z^{-n+1} + \ldots + \frac{a_{n-1}}{a_n} z^{-1} \right| < 1, \text{ tj. } \left| \frac{a(z) - a_n z^n}{a_n z^n} \right| < 1.$$

Dakle je

(2) $$|a(z) - a_n z^n| < |a_n z^n| \text{ za } |z| < r.$$

Posebno će za svaku kružnicu $C(O, R)$ sa $R > r$ vrijediti (2); prema Rouché-ovu teoremu ima tada $a(z)$ kao suma od $(a(z) - a_n z^n)$ i $a_n z^n$ upravo onoliko ništišta u $C(O, R)$ koliko ih ima $a_n z^n$ — dakle ih ima n.

6.6. Teorem o neprekidnoj zavisnosti ništišta od koeficijenata. *Ako se koeficijenti polinoma $a(z)$ mijenjaju neprekidno (kontinuirano), tada se i ništišta polinoma $a(x)$ mijenjaju na neprekidan način. Ako je polinom $a(z)$ limes niza $p_1(z), p_2(z), \ldots$ polinomâ kojima su ništišta na nekoj krivulji C, tada su i ništišta od $a(z)$ na C.*

D o k a z. Neka je $a(z_0) = 0$; neka je K kružnica sa središtem z_0 tako da je z_0 jedino ništište od a koje se nalazi u krugu K; naravno da takvo K postoji jer $a(z)$ ima konačno mnogo ništišta. Neka ništište z_0 ima kratnost ν. Promijenimo koeficijente polinoma $a(z)$ tako da nastane polinom $b(z)$ sa svojstvom

(3) $$|b(z) - a(z)| < |a(z)| \text{ za } z \in K.$$

Takav polinom $b(z)$ postoji; naime, ako je $m = \inf_z |a(z)|$, $z \in K$ tada je $m > 0$ jer je $a(z) \neq 0$ pri $z \in K$; ako tada koeficijente od a promijenimo tako da nastane polinom $b(z)$ sa svojstvom $|b(z) - a(z)| < \varepsilon < m$ za $z \in K$, tada će automatski vrijediti i (3). Zato prema Rouché-ovu teoremu funkcija $b(z)$ $(= (b-a) + a)$ ima unutar K upravo onoliko ništišta koliko ih ima $a(z)$ — dakle ima upravo ν ništišta unutar K.

Dokažimo i drugi dio teorema 6.6. Neka su $z_1, z_2, \ldots, z_n$ sva ništišta od $a(z)$; tada se oko z_ν može opisati kružnica koja ne obuhvata nikoje drugo ništište od $a(z)$ i na kojoj je $|p_k(z) - a(z)| < |a(z)|$ za svaki indeks $k > k_0$, gdje je k_0 neki prirodni broj. Kad ne bi bilo $z_\nu \in C$, mogla bi se oko z_ν opisati neka kružnica K_ν kojoj krug nema nijedne zajedničke tačke sa skupom C: k tome se K_ν može uzeti tako malim da na K_ν vrijedi $|a(z) - p_k(z)| < |p_k(z)|$; zato bi prema § 6.4. funkcija $p_k(z)$ i funkcija $a = (a - p_k(z)) + p_k(z)$ imale jednak broj ništišta unutar K_ν, što je nemoguće jer prema pretpostavci sva ništišta od $p_k(z)$ leže u skupu C koji je disjunktan prema K_ν.

7. BROJ RJEŠENJA UNUTAR JEDINIČNOG KRUGA[1]

7.1. Teorem. (*I. Schur*, 1918) (č. *Šur*). *Polinom*

$$a(z) = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n, \quad a_n \neq 0$$

ima sva svoja ništišta u unutrašnjosti jediničnog kruga onda i samo onda ako i polinom nižeg stupnja

$$a^{(1)}(z) \equiv z^{-1}(\bar{a}_n \cdot a(z) - a_0 a^\star(z)) \tag{1}$$

ima sva svoja ništišta u unutrašnjosti jediničnog kruga te ako vrijedi

$$|a_0| < |a_n|. \tag{2}$$

Pri tom se stavlja

$$\bar{a}(z) = \bar{a}_0 + \bar{a}_1 z + \ldots + \bar{a}_n z^n \quad \text{i}$$

$$a^\star(z) = z^n \bar{a}(z^{-1}) = \bar{a}_0 z^n + \bar{a}_1 z^{n-1} + \ldots + \overline{a_{n-1}} z + \bar{a}_n. \tag{3}$$

Dokaz. Pretpostavimo da su sva ništišta od $a(z)$ po modulu < 1; tada je i njihov produkt po modulu < 1; no taj produkt je upravo $|a_0/a_n|$; dakle je $|a_0/a_n| < 1$ (2) vrijedi.

Dokažimo nadalje

$$|z| = 1 \Rightarrow a^\star(z) = \bar{a}(z). \tag{4}$$

---

[1] Pogledati članke: I. Schur (Journal für Math. 148 (1918), 125—145), A. Cohn (Math. Zeitschrift, 14 (1922) 110—138), Herglotz (Math. Z. 19 (1924), Liénard—Chipart (Journal de Math. 10 (1914) 271—346), M. Fujiwara (Math. Zeitschrift, 24 (1925), 161—169).

Naime, $|z|=1$ daje $\bar{z}=z^{-1}$ pa je

$$a^{\star}(z)=z^n\overline{a(z^{-1})}=z^n\overline{a(\bar{z})}=(\text{prema (3)})=$$

$$=z^n\bar{a}(z)=\bar{a}_0 z^n+\bar{a}_1 z^{n-1}+\ldots+\bar{a}_{n-1}\bar{z}+\bar{a}_n=$$

$$=\overline{a_0 z^n}+\overline{a_1 z^{n-1}}+\ldots+\overline{a_{n-1} z}+\overline{a_n}=\overline{a(z)}.$$

Dakle, (4) vrijedi. Specijalno je dakle $|a^{\star}(z)|=|a(z)|$ za svako $|z|=1$; ta jednakost i nejednakost (2) daju

(5) $$|a_0 a^{\star}(z)|<|\bar{a}_n a(z)| \text{ po jediničnoj kružnici } |z|=1.$$

Zato prema Rouché-ovu teoremu 6.4. funkcije

(6) $$\bar{a}_n a(z),\ \bar{a}_n a(z)-a_0 a^{\star}(z)$$

imaju jednak broj ništišta u unutrašnjosti jediničnog kruga; kako je posljednji izraz u (6) upravo $za^{(1)}(z)$ (isp. (1)), znači to da zaista sva nulišta od (1) imaju modul <1.

Dokažimo obrat: ako (1) ima nulišta modula <1 te ako vrijedi(2), onda su i moduli nulišta od $a(z)$ manji od 1. Zbog (4) i (2) vrijedi (5) pa prema § 6.4. funkcije (6) imaju jednak broj ništišta kojima je modul <1. No prema pretpostavci sva ništišta funkcije (1) su po modulu <1; naravno da to vrijedi i za ništišta funkcije $z a^{(1)}(z)$; to znači da zaista $a(z)$ ima n ništišta — jednakih ili nejednakih — kojima je modul <1.

Time je Schurov teorem dokazan. Analogno se dokazuje

7.2. Teorem. (I. Schur, 1918). *Ništišta polinoma $a(z)$ leže na jediničnoj kružnici onda i samo onda ako za neki unimodularni broj ε (dakle $|\varepsilon|=1$) vrijedi*

$$a_\nu=\varepsilon\,\bar{a}_{n-\nu}\ (\nu=0,1,2,\ldots n)$$

te ako sva ništišta od $a'(z)$ leže u zatvorenom jediničnom krugu.

—→ **7.3.** Teorem. *Ako je $a(x)=a_0+a_1x+\ldots+a_{n-1}a^{n-1}+x^n$ normiran polinom s bar dva koeficijenta $\neq 0$, tada svako njegovo ništište leži u krugu $K(O,\leq r)$, gdje r označuje jedino pozitivno ništište normiranog polinoma*

$$A(x)=-|a_0|-|a_1|x-\ldots-|a_{n-1}|x^{n-1}|+z^n;\quad \textit{dakle je}$$

$$(\text{spektar od } a)\quad \sigma_a\subset K(O,\leq r)\ A(r)=0,\ r>0.$$

Dokaz. Polinom $A(x)$ (kao i $a(x)$) ima bar dva koeficijenta $\neq 0$; koeficijenti su mu realni i pokazuju upravo jednu promjenu predznaka; zato prema Descartesovu teoremu iz § 4.1. postoji jedno jedino pozitivno realno ništište r polinoma $A(x)$. Dokažimo da iz $a(\zeta)=0$ nužno izlazi $|\zeta|\leq r$. Pretpostavimo naprotiv da je $|\zeta|>r$ za neko ništište ζ od $a(x)$. Ne može biti $A(|\zeta|)=0$, jer bi to značilo da bi $A(x)$ imalo dva pozitivna ništišta r, $|\zeta|$; ne može biti ni $A(|\zeta|)<0$; naime, kako je vodeći koeficijent od $A(x)$ pozitivan, to za dovoljno veliki broj $R>r$ nužno je $A(R)>0$; zato bi prema Bolzanovu teoremu iz § 2.5. postojao neki realan broj x_0 između $|\zeta|$ i R u kojemu bi bilo $A(x_0)=0$; dakle bi $A(x)$ imalo bar dva pozitivna ništišta

r, x_0, protivno činjenici da je r jedino pozitivno ništište od $A(x)$. Dakle ne bi bilo niti $A(|\zeta|) \leq 0$; međutim, posljednja relacija je ispravna i izlazi iz jednakosti $a(\zeta) = 0$ primjenom obrasca o stranicama u trokutu, odnosno obrasca

$$x + y = z \Rightarrow |x| - |y| \leq |z|.$$

⟶ **7.4. T e o r e m.** ***Za svaki normiran polinom***

$$a(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$$

i svaki pozitivni realni broj $\rho > 0$ ***relacija*** $a(\zeta) = 0$ ***daje*** $|\zeta| \leq R$, ***gdje je***

$$R = \mathrm{Sup}\,\{\rho^{-1}, |a_0|\,\rho^{n-1} + |a_1|\,\rho^{n-2} + \ldots + |a_{n-2}|\,\rho + |a_{n-1}|\};$$

specijalno je spektar σ_a ***polinoma a sadržan u krugu*** $K(O, \leq R)$ ***za***

$$R = \sup\{1, |a_0| + |a_1| + \ldots + |a_{n-1}|\} \quad (\textit{slučaj } \rho = 1).$$

Teorem je ispravan ako je

$$a_0 = a_1 = \ldots = a_{n-1} = 0.$$

Ako sve te relacije ne stoje, onda polinom $a(x)$ ima bar dva koeficijenta $\neq 0$ da prema teoremu 7.3. postoji jedini korijen r jednadžbe $A(x) = 0$ koji je pozitivan. Preostaje da dokažemo da je nužno $R \geq r$. Kad bi naime bilo $R < r$, bilo bi specijalno $\rho^{-1} < r$. No iz $A(r) = 0$, tj. iz

$$r^n = |a_0| + |a_1|\,r + \ldots + |a_{n-1}|\,r^{n-1}$$

izlazi dijeleći sa r^{n-1}:

$$r = |a_0|\,r^{-(n-1)} + |a_1|\,r^{-(n-2)} + \ldots + |a_{n-1}|$$

što bi prema $\rho^{-1} < r$ dalo

$$r \leq |a_0|\,\rho^{n-1} + |a_1|\,\rho^{n-2} + \ldots + |a_{n-1}| \leq R,$$

dakle $r \leq R$, protivno pretpostavci.

8. NEKOLIKO ČINJENICA O NULIŠTIMA POLINOMA S REALNIM KOEFICIJENTIMA[1]

8.1. T e o r e m. *Ako su koeficijenti polinoma* $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ *pozitivni realni uzlazni brojevi, tada je apsolutna vrijednost svakog rješenja jednadžbe* $a(x) = 0$ *manja od* 1, *tj. spektar* σ_a *leži u unutrašnjosti* $K(0, < 1)$ *jedinične kružnice; ako je* $a_0 > a_1 > \ldots a_n > 0$, *tada spektar* σ_a *leži u spoljašnosti* $K(0, > 1)$, *jedinične kružnice; drugim riječima* $a(\zeta) = 0 \Rightarrow |\zeta| > 1$.

Prema tome, koeficijenti polinoma $a(x)$ su pozitivni realni brojevi i niz im je strogo uzlazan, odnosno strogo silazan. Oslobodimo li se ovog posljednjeg uslova dobit ćemo naredni teorem koji neposredno ima za posljedicu teorem 8.1.

---

[1] Pogledati članke: Kakeya (Tôhoku Math. J., 2 (1922), G. Eneström (isti časopis 18 (1920), L. Berwald (Math. Z. 37 (1933) 61—76.

—→ **8.2. Teorem.** *Ako su koeficijenti polinoma $a(x)$ realni pozitivni brojevi, tada iz $a(\zeta)=0$ izlazi*

$$m \leq |\zeta| \leq M,$$

tj.

$$\sigma_a \subset K(0, \leqq M) \setminus K(0, <m);$$

pri tom m, odnosno M znači najmanji odnosno najveći član niza

$$\frac{a_0}{a_1}, \frac{a_1}{a_2}, \ldots, \frac{a_{n-1}}{a_n}.$$

Dokažimo teorem 8.2. Najprije je jasno da će biti

$$M \geq \frac{a_{\nu-1}}{a_\nu} \qquad (\rho = 1, 2, \ldots, n), \qquad \text{dakle također}$$

(1) $$M a_\nu - a_{\nu-1} \geq 0 \qquad (\nu = 1, 2, \ldots . n).$$

No, ovi se brojevi pojavljuju kao faktori koeficijenata polinoma

$$a_n^{-1}(x-M)\,a(x)$$

jer je

$$a_n^{-1}(x-M)\,a(x) = -\frac{a_0}{a_1} M - \frac{a_1 M - a_0}{a_n} x - \frac{a_2 M - a_1}{a_n} x^2 - \ldots -$$
$$-\frac{a_n M - a_{n-1}}{a_n} x^n + x^{n+1}.$$

Primijenimo, na taj polinom, teorem 7.4, i to za posebni slučaj $\rho = M^{-1}$; tada je dakle

(*) $$|\zeta| \leq \sup\{M, P\},$$

gdje je

$$P = \left| -\frac{a_n M - a_{n-1}}{a_n} \right| + \left| -\frac{a_{n-1} M - a_{n-2}}{a_n} \right| M^{-1} + \ldots +$$
$$+ \left| -\frac{a_1 M - a_0}{a_n} \right| M^{-(n-2)} + \left| -\frac{a_0}{a_n} \right| M^{-(n-1)}.$$

No, zbog (1) dalje je

$$P = \frac{a_n M - a_{n-1}}{a_n} + \frac{a_{n-1} - a_{n-2} M^{-1}}{a_n} + \frac{a_{n-2} M^{-1} - a_{n-3} M^{-2}}{a_n} + \ldots +$$
$$+ \frac{a_1 M^{-(n-2)} - a_0 M^{-(n-1)}}{a_n} + \frac{a_0 M^{-(n-1)}}{a_n}.$$

$$P = M; \quad \text{dakle je} \quad \sup\{M, P\} = \sup\{M, M\} = M,$$

pa relacija (*) pokazuje da je zaista $|\zeta| \leq M$.

Ako u polinomu $a(x)$ napravimo zamjenu $y = x^{-1}$, tada se analogno dokazuje da je $|\zeta| \geq m$. Time je teorem potpuno dokazan.

9. GAUSS-LUCASOV TEOREM[1]

Neka je $a(z)$ proizvoljan algebarski polinom s kompleksnim koeficijentima; svaki konveksni skup koji obuhvata spektar σ_a od a obuhvata i spektar $\sigma_{a'}$ derivata a', spektar $\sigma_{a''}, \ldots, \sigma_{a^{(n-1)}}$.

Sam teorem je posljedica ove činjenice:

9.1. Lema. *Ako neka zatvorena poluravnina P kompleksnih brojeva obuhvata σ_a, obuhvata ona i $\sigma_{a'}$.*

Naime, svaki konveksni skup S koji sadrži $\sigma_{a'}$ sadrži i minimalni konveksni poligon p u kojem leži σ_a; zato je dovoljno pokazati da $p \supset \sigma_a$; no poligon p je presjek određena broja zatvorenih poluravnina $P_1, P_2, \ldots, P_k$:

$$p = P_1 \cap P_2 \cap P_3 \cap \ldots P_k.$$

Kako u svakoj od tih poluravnina leži (prema lemi 9.1) $\sigma_{a'}$, ležat će $\sigma_{a'}$ i u p. Iz istog razloga ležat će u p i skup $\sigma_{a''}$ pa spektar od a''', itd. Time je teorem 9 izveden iz 9.1.

Dokažimo 9.1, i to najprije za slučaj da se P podudara s gornjom zatvorenom poluravninom P_0 kompleksnih brojeva $x+iy$ za koje je $y \geq 0$. Neka su ništišta od $a(z)$ upravo brojevi

(1) $$z_\nu = \alpha_\nu + i\beta_\nu \quad (\nu = 1, 2, \ldots, n);$$ prema pretpostavci je

(2) $$\beta_\nu \geq 0 \qquad (\nu = 1, 2, \ldots, n).$$

Ako je $f'(z) = 0$, $f(z) \neq 0$, tada će naravno biti $\dfrac{f'(z)}{f(a)} = 0$, što zbog

$$f(x) = a_n (x - z_1)(x - z_2) \ldots (x - z_n)$$

daje

(3) $$\frac{1}{z - z_1} + \frac{1}{z - z_2} + \cdots \frac{1}{z - z_n} = 0.$$

Stavimo li

(4) $$z = \alpha + i\beta,$$

tada (3) povlači

(5) $$\sum_{\nu=1}^{n} \frac{\beta - \beta_\nu}{(\alpha - \alpha_\nu)^2 + (\beta + \beta_\nu)^2} = 0.$$

Zbog (2) ne može biti $\beta < 0$ jer za $\beta < 0$ izraz na lijevoj strani (5) postaje < 0; dakle je nužno $\beta \geq 0$, a to upravo znači da je $\sigma_{a'} \subset P_0$.

Ako zadana poluravnina P nije P_0, može se ona afinom transformacijom $x \to kx + l$ prevesti u P_0. No, pri afinoj transformaciji $x = kx_1 + l$ (nova je varijabla x_1) prelazi $a(x)$ u $a(x) = a(kx_1 + l) = b(x_1)$, pa je

$$b'(x_1) = ka'(x).$$

[1] Isporediti: Gauss, Werke Bd 3 str. 112, Bd 8 str. 32 tc Lucas (č. Lüka), Comptes rendus Acad. Paris 89 (1879).

Kako $\sigma_{b'(x_1)}$ leži u P_0 znači da će $\sigma_{a'(x)}$ ležati u odgovarajućoj poluravnini P. Time je lema 9.1. dokazana. Pri tom za proizvoljan polinom $c(x)$ označujemo sa σ_c skup svih nulišta od $c(x)$.

9.2. Posljedice. *Ako σ_a leži na pravulji ili na odresku pravulje, tada na njemu leži i $\sigma_{a'}$ (isp. § 3.5. za slučaj kad je pravulja u pitanju upravo realna os).*

10. PELLETOV TEOREM[1]

Neka je

(1) $$a(x) = a_0 + a_1 x^{e_1} + \cdots + a_n x^{e_n} \quad (e_1 < e_2 < \cdots < e_n)$$

cijela racionalna funkcija s kompleksnim koeficijentima sa svojstvom

(2) $$a_\nu \neq 0 \quad (\nu = 0, 1, \ldots, n);$$

tada postoji bar jedan kompleksni broj ζ za koji je $a(\zeta) = 0$ i

(3) $$|\zeta|^{e_1} \leq n \cdot \left|\frac{a_0}{a_1}\right|.$$

Drugim riječima, krug $K(0, \leq p)$ kojemu je polumjer

(4) $$p \geq \left| n a_0 a_1^{-1})^{\frac{1}{e_1}}\right.$$

obuhvata bar jedno ništište polinoma (1). U pojedinom slučaju znak $\leq$ u (3) odnosno (4) može biti i znak $=$.

10.1. Dokaz ćemo provesti induktivno i to s obzirom na broj $l\,(= 1 + n)$ članova polinoma (1). Ako je $l = 2$ (tj. $n = 1$), teorem je očigledan. Pretpostavimo da je teorem istinit za svaki polinom od n ili manje članova; dokažimo tada da je teorem istinit za svaki polinom oblika (1) od $1 + n$ članova. Neka niz

(5) $$\zeta_1, \zeta_2, \ldots \zeta_{e_n}$$

predstavlja svih e_n ništišta polinoma (1) i pretpostavimo da je nizanje (5) provedeno tako da bude

(6) $$|\zeta_1| \leq |\zeta_2| \leq \cdots \leq |\zeta_{e_n}|.$$

10.2. Brojevi $a_0 a_n^{-1}, a_1 a_n^{-1}, \ldots, a_{n-1} a_n^{-1}$ spadaju među osnovne simetrične funkcije veličina (5) (isp. 19 § 1.2.2); znamo za veze između koeficijenata polinoma i funkcija $s_k = \zeta_1^k + \zeta_2^k + \ldots$ za $k = 0, 1, 2, \ldots$ (pogl. 19. § 2.2). Međutim, analogni izrazi postoje i za s_k za $k = -1, -2, \ldots$ ($a_0 \neq 0$!); dovoljno je provesti supstituciju $x_\nu = y_\nu^{-1}$ i promatrati ne funkciju

$$f(t) = (t - x_1)(t - x_2) \ldots$$

[1] v. Pellet (č. Pele), Bulletin des Sciences math. 59 (1924).

kao u pogl. 19, § 2.2. nego funkciju

$$f_1(t)=(t-y_1)(t-y_2)\dots(t-y_n)=(t-x_1^{-1})(t-x_2^{-1})\dots(x-x_n^{-1})$$
$$=\frac{(-1)^n}{x_1\dots x_n}t^n(t^{-1}-x_1)(t^{-1}-x_2)\dots(t^{-1}-x_n)$$
$$=\frac{1}{\sigma_n}t^n f(t^{-1})=t^n+\frac{\sigma_{n-1}}{\sigma_n}t^{n-1}+\dots+\frac{\sigma_1}{\sigma_n}t+\frac{1}{\sigma_n}.$$

To znači da u pogl. 19, § 2.2. dolazi do supstitucije $s_k\to s_{k-1}$ i

$$\begin{array}{cccc} \sigma_1, & \sigma_2, & \dots, & \sigma_n \\ \downarrow & & & \\ \dfrac{\sigma_{n-1}}{\sigma_n}, & \dfrac{\sigma_{n-2}}{\sigma_n}, & \dots, & \dfrac{1}{\sigma_n} \end{array}$$

pa Newtonove formule (7) iz pogl. 19, § 2.2. prelaze u nove formule

$$s_{-1}=-\frac{\sigma_{n-1}}{\sigma_n}$$

(7)
$$n\frac{\sigma_{n-\nu}}{\sigma_n}+\frac{\sigma_{n-(\nu-1)}}{\sigma_n}s_{-1}+\frac{\sigma_{n-(\nu-2)}}{\sigma_n}s_{-2}+\dots+\frac{\sigma_{n-1}}{\sigma_n}s_{-(\nu-1)}+s_{-\nu}=$$
$$=(n-\nu)\frac{\sigma_{n-\nu}}{\sigma_n}\quad(\nu=0,1,\dots,n-1).$$

Primijenimo li obrasce (7) na polinom (1) tada zbog $s_\nu=0$ za $\nu=1,2,\dots e_1-1$ imamo $s_{-\nu}=0$ za $\nu=1,2,\dots,e_1-1$ dok je

$$s_{-e_1}+e_1\frac{a_1}{a_0}=0,\quad \text{tj.}\quad s_{-e_1}=-e_1\frac{a_1}{a_0}.$$

Napišemo li eksplicitno izraz sa s_{-e_1} veličinâ (5) i prijeđemo na apsolutne vrijednosti, daje prethodna jednakost relaciju

$$\sum_{\nu=1}^{e_n}\left|\frac{1}{\zeta_\nu^{e_1}}\right|\geq e_1\left|\frac{a_1}{a_0}\right|$$ koja zbog (6) daje

$$e_n\frac{1}{|\zeta_1|^{e_1}}\geq e_1\left|\frac{a_1}{a_0}\right|,$$

odnosno

(8)
$$|\zeta_1|^{e_1}\leq\frac{e_n}{e_1}\left|\frac{a_0}{a_1}\right|.$$

Time smo se približili cilju (3) — cilj je čak dostignut ukoliko je $e_n\leq ne_1$. Zato još preostaje izvesti (3) uz pretpostavku $e_n>ne_1$, tj.

(9)
$$\frac{e_n}{e_n-e_1}<\frac{n}{n-1}.$$

10.3. Polinom $b(x) = x^{e_n} a(x^{-1})$ ima kao ništišta reciproke brojeva (5). Vidi se da je

$$b'(x) = e_n a_0 x^{e_n - 1} + (e_n - e_1) a_1 x^{e_n - e_1 - 1} + \ldots + (e_n - e_{n-1}) a_{n-1} x^{e_n - e_{n-1}}.$$

Zbog uslova uzlaznosti (6) bit će $|\zeta_\nu^{-1}| \leq |\zeta_1^{-1}|$; zatim će prema Gauss-Lucasovu teoremu 9. krug $K(0, \leq |\zeta_1|^{-1})$ obuhvatiti spektar $\sigma(b')$ derivata b'. No, uz izraz $b'(x)$ vezan je i izraz

$$c(x) = x^{e_n - 1} b'(x^{-1}) = e_n a_0 + (e_n - e_1) a_1 x^{e_1} + \ldots + (e_n - e_{n-1}) a_{n-1} x^{e_{n-1}}$$

jer c i b' imaju međusobno recipročna ništišta koja su $\neq 0$; specijalno će zato svako $\zeta \in \sigma_c$ zadovoljavati $|\zeta|^{-1} \leq |\zeta_1|^{-1}$, tj.

$$|\zeta_1| \leq |\zeta|. \tag{10}$$

No, prema indukcionoj hipotezi teorem 10. vrijedi za n-člani polinom $c(x)$. Dakle za bar jedno ništište $\zeta \in \sigma_c$ vrijedi

$$|\zeta|^{e_1} \leq (n-1) \frac{e_n a_0}{(e_n - e_1) a_1} \tag{11}$$

što radi (10) daje

$$|\zeta_1|^{e_1} \leq (n-1) \left| \frac{e_n a_0}{(e_n - e_1) a_1} \right|;$$

odatle zbog (9) izlazi

$$|\zeta_1|^{e_1} \leq (n-1) \left| \frac{n}{n-1} \frac{a_0}{a_1} \right| = n \left| \frac{a_0}{a_1} \right|. \qquad \text{Q. E. D.}$$

10.4. Slučaj polinoma

$$a_0 \left(1 + \frac{a_1}{n a_0} x^{e_1} \right)^n = a_0 + a_1 x^{e_1} + \frac{(n-1) a_1^2}{2 n a_0} x^{2 e_1} + \ldots + \frac{a_1^n}{n^n a_0^{n-1}} x^{n e_1}$$

pokazuje da svako njegovo ništište ζ zadovoljava jednadžbu (3) a ne samo nejednadžbu (3).

10.5. Primjedba o Pelletovu teoremu. Važno je uočiti da u ocjeni kruga u Pelletovu teoremu dolaze samo: broj članova polinoma a ne stupanj polinoma, koeficijenti a_0, a_1 i eksponent e_1 (isp. § 11.); s tim u vezi, poučno je Pelletov teorem usporediti s poznatim Landauovim teoremom o redovima potencija.

11. LAGUERRE-OV TEOREM[1]

Neka je $a(x)$ cijela racionalna funkcija s kompleksnim koeficijentima i stepena $n \geq 1$; neka je α bilo kakav kompleksan broj za koji je

$$a(\alpha) \neq 0 \neq a'(\alpha);$$

[1] E. Laguerre (č. Lager) (1834—1886); v. Laguerre [1], str. 56—60.

neka je K bilo kakva kompleksna kružnica na kojoj leže brojevi

$$\alpha, \ \alpha - n\frac{a(\alpha)}{a'(\alpha)}.$$

Tada pripadni zatvoreni krug od K obuhvata bar jedno ništište od a (x). *Ako cio spektar σ_a ne leži na kružnici K, tada σ_a zadire u unutrašnjost i u spoljašnost kruga K.*

Teorem će biti posljedica narednih dviju činjenica 11.1, 11.2.

11.1. Teorem. Zadan je polinom $a(x) \equiv a_0 + a_1 x + \ldots + a_n x^n$ stepena n (dakle je $a_n \neq 0$, $n \geq 1$); svaka pravulja p koja prolazi tačkom

$$\zeta = -\frac{1}{n}\frac{a_{n-1}}{a_n} \tag{1}$$

ima svojstvo da obuhvata čitav skup $\sigma(a)$ ništišta od a ili pak da $\sigma(a)$ zadire i u jednu i u drugu otvorenu poluravninu koje p omeđuje. U prvom slučaju je ili $\sigma(a) = \{\zeta\}$ ili $\sigma(a)$ zadire u obje otvorene zrake pravulje p kojima je ζ međašnja tačka.

Neka je naime $\zeta_1, \zeta_2, \ldots, \zeta_n$ spektar s ponavljanjem polinoma a; tada je

$$\zeta_1 + \zeta_2 + \ldots + \zeta_n = -\frac{a_{n-1}}{a_n}$$

(Viète; isp. poglavlje 19, § 1.2.1).

Zato (1) daje

$$\zeta = \frac{1}{n}(\zeta_1 + \zeta_2 + \ldots + \zeta_n).$$

To znači da je ζ težište množine $\sigma_a = \{\zeta_1, \ldots, \zeta_n\}$, pri čemu se svakom $x \in \sigma(a)$ pridjeljuje kratnost $k(x)$ od x kao težina. Zato ζ leži u minimalnom konveksnom skupu C koji obuhvata $\sigma(a)$; iz istog razloga ne može ζ biti na rubu od C, osim ako je $\sigma(a) = \{\zeta\}$. A to se upravo i iskazuje teoremom 11.1.

11.2. Transformacijom $x = y^{-1}$ imamo

$$a(x) = (y^{-1}) = y^n (a_n + a_{n-1} y + \ldots + a_1 y^{n-1} + a_0) \equiv y^n a^T(y).$$

Ako je $a_0 \neq 0$, i novi polinom a^T je stepena n; težište njegova spektra s ponavljanjem je $-\frac{1}{n}\frac{a_1}{a_0} = \zeta$ pa svaka pravulja p tim težištem ima svojstva iz teorema 11.1. u odnosu na polinom a^T. No, transformacijom $x = y^{-1}$ prelazi p u određenu kružnicu K tačkama 0, $\zeta^{-1} = -n\frac{a_0}{a_1}$ (zato pretpostavljamo da je $a_1 \neq 0$); dvjema otvorenim poluravninama u vezi sa p odgovaraju sada unutrašnjost i spoljašnost kruga od K. Time je dokazan

11.3. Teorem. Ako u polinomu $a_0 + a_1 y + \ldots + a_n y^n$, $n \geq 1$ vrijedi $a_0 \neq 0 \neq a_1$, tada svaka kružnica K koja prolazi tačkama 0, $-n\frac{a_0}{a_1}$ obuhvata čitav spektar $\sigma(a)$ ili $\sigma(a)$ zadire i u unutrašnjost i u spoljašnost kruga K; u prvom slučaju je ili $\sigma(a)=\left\{-n\frac{a_0}{a_1}\right\}$ ili $\sigma(a)$ zadire u oba otvorena luka kružnice K kojima su 0, $-n\frac{a_0}{a_1}$ zajednički krajevi.

11.4. Dokaz Laguerre-ova teorema. Neka je $a(\alpha)\neq 0\neq a'(\alpha)$; supstitucija $x=y+\alpha$ daje

$$a(x)=a(y+\alpha)=(\text{prema } 7,\ \S\ 12.4)=a(\alpha)+a'(\alpha)\,y+\frac{a''(\alpha)}{2!}y^2+\ldots$$

Primjenom teorema 11.3 na $b(x)$ izlazi upravo Laguerre-ov teorem, jer tačkama $0, -n\frac{a_0}{a_1}$ odgovaraju sada pomaknute tačke α, $\alpha-n\frac{a_0}{a_1}$.

12. KOMPOZICIONI TEOREMI O SPEKTRIMA POLINOMA

Ima niz teorema o spektrima, odnosno ništištima polinoma kojima koeficijenti zadovoljavaju razne uslove. Jedan od najpoznatijih takvih teorema je naredni teorem

—→ **12.1. Teorem.** **(Grace, 1902)**[1]. ***Neka je K proizvoljna kružnica ili pravulja kompleksne ravnine, a K_0 bilo jedan bilo drugi zatvoreni odlomak ravnine kojemu je K omeđenje (prema tome $K\subset K_0$)***[2]***. Neka je***

(1) $$z_1, z_2, \ldots, z_n$$

bilo kakav konačan niz tačaka iz K_0.

Neka su $\sigma_1, \sigma_2, \ldots, \sigma_n$ osnovne simetrične funkcije veličinâ (1) (pogl. 19, § 1.2.2); stavimo $\sigma_0=1$. Ako niz kompleksnih brojeva $a_0, a_1, \ldots, a_n$ zadovoljava

(2) $$a_0\sigma_0+a_1\sigma_1+\ldots+a_n\sigma_n=0.$$

tada polinom

(3) $$a_0+\binom{n}{1}a_1x+\binom{n}{2}a_2x^2+\ldots+\binom{n}{n}a_nx^n$$

ima bar jedno ništište u K_0.

Dokaz ćemo provesti induktivno prema prirodnom broju n uz pomoć Laguerre-ova teorema 11. Najprije, teorem je očigledan za $n=1$. Pretpostavimo da je teorem već dokazan za prirodne brojeve n koji su $<s$; dokažimo ga i za $n=s$. Promatrajmo pomoćni polinom

(4) $$c(x)=a_0+\binom{s}{1}a_1x+\binom{s}{2}a_2x^2+\ldots+\binom{s}{s}a_sx^s.$$

---

[1] J. H. Grace (č. Grejs), On the zeros of a polynominal (Proc. Cambridge Phil. Soc. 11 (1902) 352—356).

[2] Ako je K pravulja, tada je K_0 porubljena poluravnina. Prema analogiji kada je K pravulja, može se K_0 zvati *zatvorena kružna poluravnina*; komplement od K_0 je *otvorena kružna poluravnina*.

Lako se provjeri da je

$$xc'-sc=-s\left[a_0+\binom{s-1}{1}a_1x+\ldots+\binom{s-1}{s-1}a_{s-1}x^{s-1}\right]. \tag{5}$$

Zato za izraz

$$x_s=x-s\frac{c(x)}{c'(x)} \tag{6}$$

vrijedi

$$x_s=\frac{a_0+\binom{s-1}{1}a_1x+\ldots+a_{s-1}x^{s-1}}{a_1+\binom{s-1}{1}a_2x+\ldots+a_sx^{s-1}}. \tag{7}$$

Odatle izlazi

$$\left(a_0+a_1x_s\right)+\binom{s-1}{1}\left(a_1+a_2x_s\right)x+\ldots+\left(a_{s-1}+a_sx_s\right)x^{s-1}=0. \tag{8}$$

Lijeva strana jednadžbe (8) je oblika (3) i nastaje iz (3) supstitucijama:

$$n\to s-1,\quad a_\nu\to a_\nu+a_{\nu-1}x_s \quad \text{za} \quad \nu=0,1,\ldots,s-1.$$

Za osnovne simetrične funkcije $\sigma'_0=1, \sigma_1', \ldots, \sigma'_{s-1}$ veličina $a_\nu+a_{\nu+1}x_s$ imamo

$$x_s\sigma'_{s-1}=\sigma_s,\ \sigma'_\nu+x_s\sigma'_{\nu-1}=\sigma_\nu \quad (\nu=1,2,\ldots,s-1)$$

pa je

$$(a_0+a_1x_s)\sigma'_0+(a_1+a_2x_s)\sigma'_1+\ldots+(a_{s-1}+a_sx_s)\sigma'_{s-1}= \tag{9}$$
$$a_0\sigma_0+a_1\sigma_1+\ldots+a_s\sigma_s=(\text{po uslovu (2)})=0.$$

Iz te jednakosti razabiremo da se na polinom (8) može, prema indukcionoj hipotezi, primijeniti teorem 12.1: polinom (8) ima bar jedno ništište ζ u K_0. Pripadni broj ζ je također u K_0.

Ako je $\zeta=\zeta_s$, tada $x_s=x=\zeta$ zadovoljava (8); a to uvrštenje pokazuje da je upravo $c(\zeta)=0$ pa bi stvar bila dokazana jer $\zeta\in K_0$. Ako je $\zeta\neq\zeta_s$, tada relacije $0\neq\zeta-\zeta_s=s\dfrac{c(\zeta)}{c'(\zeta)}$ pokazuju da je $c(\zeta)\neq0\neq c'(\zeta)$. Zato na polinom $c(x)$ i broj $\alpha=\zeta$ možemo primijeniti Laguerre-ov teorem 11: svaki zatvoreni krug C tačkama $\zeta, \zeta_s=\zeta-\dfrac{c(\zeta)}{c'(\zeta)}$ ima svojstvo da sadrži tačku iz σ_c, a ujedno σ_c zadire u uniju od vanjštine kruga C i omeđenja kruga C. No, izabere li se C specijalno tako da C dodiruje ishodnu kružnicu (pravulju) K, znači to da će skup K_0 sadržavati puni skup $K\cap\sigma_c$. Q. E.D.

Navedimo bez dokaza ovu posljedicu teorema 12.1:

12.2. Teorem (I. Schur, 1914). *Ako spektar polinoma*

$$a_0+\binom{n}{1}a_1x+\binom{n}{2}a_2x^2+\ldots+\binom{n}{n}a_nx^n$$

leži u nekom konveksnom skupu $S \ni 0$, *a spektar polinoma*

$$b_0 + \binom{n}{1} b_1 x + \binom{n}{2} b_2 x^2 + \ldots + \binom{n}{n} b_n x^n$$

u realnom intervalu $R(-1,\ 0)$, *tada i spektar kompozicionog polinoma*

$$a_0 b_0 + \binom{n}{1} a_1 b_1 x + \binom{n}{2} a_2 b_2 x^2 + \ldots + \binom{n}{n} a_n b_n x^n$$

leži u S (isp. Obreškov [4] str. 26).

Tipičan kompozicioni teorem je ovo:

⟶ **12.3 Teorem.** *Ako za izraze*

$$a(x) \equiv \sum_{\nu=0}^{n} a_\nu x^\nu, \quad b(x) = \sum_{\nu=0}^{n} b_\nu x^\nu$$

vrijedi

$$\sum_{\nu=0}^{n} (-1)^\nu \frac{a_\nu b_\nu}{\binom{n}{\nu}} = 0 \ (\textit{uslov apolarnosti}),$$

tada svaka zatvorena kružna poluravnina K_0 koja obuhvata $\sigma(a)$ sadrži bar jednu tačku od $\sigma(b)$, odnosno: sadrži li K_0 skup $\sigma(b)$, tada K_0 sadrži bar jednu tačku iz $\sigma(a)$. Drugim riječima, skupovi $\sigma(a)$, $\sigma(b)$ ne mogu se odijeliti nijednom kružnicom K u smislu da bi odgovarajuća jedna zatvorena poluravnina sadržavala $\sigma(a)$ (odnosno $\sigma(b)$) a bila disjunktna sa $\sigma(b)$ (odnosno $\sigma(a)$).

Primijenimo 12.3 i dokažimo naredno poopćenje Laguerre-ova teorema 11.

⟶ **12.4. Teorem (Dragoljub Marković)[1].** *Neka je*

$$a(x) = a_0 + a_1 x + \cdots + a_n x^n$$

polinom, ν jedan od brojeva $1, 2, \ldots, n-1$ te α bilo koji kompleksni broj za koji je

(1) $$a(\alpha) \neq 0 \neq a^{(\nu)}(\alpha);$$

tada svaki zatvoreni krug koji obuhvata α i tačke

(2) $$\beta_k = \alpha - e^{\frac{2k\pi i}{\nu}} \left[\frac{n!}{(n-\nu)!} \frac{a(\alpha)}{a^{(\nu)}(\alpha)} \right]^{\frac{1}{\nu}} \quad (k = 0,\ 1, \ldots, \nu-1)$$

obuhvata bar jedno ništište polinoma $a(x)$.

Slučaj $\nu = 1$ daje teorem 11.

[1] D. Markovič: *O teoremi Grace-a* (Prvi kongres matematičara i fizičara Jugoslavije Bled, 1949; *Izvještaji, Beograd* 1951 Sv. II, str. 67—71).

D o k a z. Translacijom

(3) $$x = \alpha + y \qquad \text{prelazi } a(x) \text{ u}$$

(4) $$b(y) \equiv \sum_{\nu=0}^{n} b_\nu y^\nu = \sum_{\nu=0}^{n} \frac{a^{(\nu)}(\alpha)}{\nu!} y^\nu \, (= a(\alpha + y)).$$

Simetrične funkcije $\sigma_1, \sigma_2, \ldots, \sigma_n$ spektra $y_1, y_2, \ldots, y_n$ polinoma $b(y)$ zadovoljavaju Viète-ovim jednadžbama (19, § 1.2.1)

$$\sigma_n = \frac{b_0}{b_n}$$

$$\sigma_{n-\nu} = \frac{b_\nu}{b_n} \quad (\nu = 0, 1, 2, \ldots, n)$$

odakle izlazi

(5) $$b_0 \sigma_{n-\nu} - b_\nu \sigma_n = 0 \quad (\nu = 0, 1, 2, \ldots, n).$$

Po uzoru $(5)_1$ sagradimo polinom

(6) $$\beta\, b_0 y^{n-\nu} - b_\nu y^n.$$

Zasad je β neodređeno, a odredit ćemo ga iz uslova apolarnosti: primjenom teorema 12.3. na polinome (6), $b(y)$ uslov apolarnosti postaje

$$(-1)^\nu \cdot \frac{(\beta\, b_0)\, b_\nu}{\binom{n}{n-\nu}} + (-1)^n \cdot \frac{-b_\nu b_0}{\binom{n}{n}} = 0$$

odakle izlazi

(7) $$\beta = -(-1)^\nu \binom{n}{n-\nu}.$$

S obzirom na $b_\nu = \dfrac{a^{(\nu)}(\alpha)}{\nu!}$ glasi dakle polinom (6)

(8) $$\left[-(-1)^\nu \binom{n}{n-\nu} a(\alpha) + \frac{a^{(\nu)}(\alpha)}{\nu!} y^\nu\right] y^{n-\nu}.$$

Ništišta polinoma (8) jesu: 0 (računata $n-\nu$ puta) i brojevi

(9) $$-e^{k \cdot \frac{2\pi i}{\nu}} \left[\frac{n!}{(n-\nu)!} \frac{a(\alpha)}{a^{(\nu)}(\alpha)}\right]^{\frac{1}{\nu}} \quad (k = 0, 1, 2, \ldots, \nu - 1).$$

Prema 12.3. svaki zatvoreni krug K koji obuhvata 0 i brojeve (9) obuhvata i bar jedno ništište polinoma $b(y)$, tj. polinoma $a(\alpha + y)$.

Eliminirajmo y prema (3) i prijeđimo na x: 0 prelazi u α, brojevi (9) prelaze u brojeve (2), $a(\alpha + y)$ prelazi u $a(x)$ a krug K u krug $K + \alpha$; ovaj krug obuhvata dakle brojeve (2) i broj α; no mijenjajući K tako da K obuhvata 0 i (9), krug $K + \alpha$ zauzme položaj svakog kruga koji sadrži α i brojeve (2). Time je teorem 12.4. potpuno dokazan.

13. OKO PROBLEMA STABILNOSTI, NESTABILNOSTI I REZONANCIJE

13.0. Razna pitanja dinamičkih sistema traže da se zna odrediti da li zadani polinom $p(z)$ ima sva svoja ništišta u lijevoj otvorenoj poluravnini $Rez<0$ (*pitanje stabilnosti*), u poluravnini $Rez>0$ (*pitanje nestabilnosti*), ili na pravulji $Rez=0$ i da ništišta budu višekratna (*pitanje rezonancije*). Služeći se *Cauchy-evim indeksima* i *Sturmovim lancima* Routh je 1877. našao put kako da se odredi broj članova spektra σ_p u $Rez>0$; Hurwitz je 1895. našao kriterij za relaciju $\sigma_p \subset (Rez>0)$. Iznijet ćemo te rezultate.

13.1. Cauchy-evi indeksi. Neka a znači realan broj, $-\infty$ ili ∞; neka također bude $b \in R \cup \{-\infty, \infty\}$.

13.1.1. Definicija. Indeks $\overset{b}{\underset{a}{I}}$ *racionalne realne* funkcije $f(x)$ kazuje razliku broja skokova od $-\infty$ do $+\infty$ i broja padanja od $+\infty$ do $-\infty$ što ih pokazuje funkcija $f(x)$ *kad varijabla* x *putuje od* a *do* b (isključuje se i a i b); takav indeks se označuje $\overset{b}{\underset{a}{I}} f(x)$.

$$\text{Npr.}\quad \overset{\infty}{\underset{-\infty}{I}} \frac{1}{x}=1,\quad \overset{\infty}{\underset{-\infty}{I}} \frac{3}{x}=1,\quad \overset{\infty}{\underset{-\infty}{I}} \frac{-2}{x}=-1,\quad \overset{\infty}{\underset{-\infty}{I}} \frac{c}{x}=\operatorname{sgn} c,$$

$$\overset{\infty}{\underset{-\infty}{I}} \left(\frac{3}{x-1}+\frac{5}{x-3}\right)=\overset{\infty}{\underset{-\infty}{I}} \frac{3}{x-1}+\overset{\infty}{\underset{-\infty}{I}} \frac{5}{x-3}=2.$$

Ako racionalna realna funkcija $g(x)$ nema realnih polova, tada je

$$\overset{\infty}{\underset{-\infty}{I}} g(x)=0;$$

ako cijela racionalna realna funkcija p ima jedino r-člani skup $\{x_1, x_2, \ldots, x_r\}$ kao svoj realni spektar, tada je

$$p(x)=(x-x_1)^{k_1}(x-x_2)^{k_2}\cdots(x-x_r)^{k_r} q(x)$$

pri čemu su $k_1, k_2, \ldots, k_r$ određeni prirodni brojevi a funkcija $\operatorname{sgn} q(x)$ konstanta na skupu R; tada je

$$\frac{p'(x)}{p(x)}=\frac{k_1}{x-x_1}+\cdots+\frac{k_r}{x-x_r}+\frac{q'(x)}{q(x)}$$

pa je

$$\overset{\infty}{\underset{-\infty}{I}} \frac{p'(x)}{p(x)}=r;\qquad \overset{b}{\underset{a}{I}} \frac{p'(x)}{p(x)}$$

je, po modulu, broj ništišta u realnom intervalu $R(a, b)$.

No, taj broj članova skupa $\sigma_p \cap R(a, b)$ znamo odrediti pomoću Sturmova teorema, odnosno pomoću Sturmova niza za polinom $p(z)$ (§ 5).

13.2. Sturmovi lanci polinoma. Niz realnih polinoma

(S) $$v_0(x),\ v_1(x), \ldots, v_s(x)$$

zove se *Sturmov niz (lanac)* u intervalu $R(a, b)$ ako su ispunjena ova dva uslova:

(S_1) Ako je $x \in R(a, b),\quad 0<j<s,\quad v_j(x)=0,$ onda je

$$v_{j-1}(x)\, v_{j+1}(x)<0 \quad \text{(isp. § 5.3.2)}$$

(S_2) $$\operatorname{sgn} v_s(x) = \text{konstanta u } R(a, b).$$

Na osnovu ta dva svojstva dokazuje se

⟶**13.3. Teorem (Sturm).** *Neka je*

(1) $$v_0(x),\ v_1(x), \ldots, v_s(x)$$

Sturmov niz realnih polinoma u intervalu $R(a, b)$ sa $a<b$; neka $V(x)$ označuje koliko niz brojeva (1) pokazuje promjena znakova; tada je

$$\mathop{I}_a^b \frac{v_1(x)}{v_0(x)} = V(a) - V(b).$$

Dokaz je sličan s dokazom teorema 5.4.

13.4. Kako se izgrađuje Sturmov lanac? Jednostavan način kako se dobije Sturmov lanac (S) kojemu su zadani prvi član $v_0(x)$ i drugi član $v_1(x)$ opisan je u § 5.1. kao postupak (E). Isto tako, množeći članove Sturmova niza (S), u odnosu na interval $R(a, b)$, nekim polinomom $d(x)$ koji u $R(a, b)$ ima konstantan predznak dobije se opet Sturmov niz polinomâ.

13.5. Indeks racionalne funkcije $\frac{p(x)}{q(x)}$ ($p(x)$, $q(x)$ su relativno prosti realni polinomi); najprije se odredi ostatak $r(x)$ pri dijeljenju polinoma $p(x)$ sa $q(x)$; tada je

$$\mathop{I}_b^a \frac{p(x)}{q(x)} = \mathop{I}_b^a \frac{r(x)}{q(x)}.$$

Zatim se formira Sturmov niz (S) uzimajući da su $q(x)$, $r(x)$ prva dva člana niza (S) (primjena algoritma — postupka (E) iz § 5.1).

13.6. Broj d ništišta u poluravnini $Re\, z>0$. Promatrat ćemo slučaj da je $p(z)$ *bez čisto imaginarnih ništišta* (dakle: $t \in R \Rightarrow p(it) \neq 0$).

13.6.1. *Promjena $\arg p(z)$ po omeđenju polukruga.* Prema teoremu o argumentu (§ 6.3) broj $\arg p(z)$, pri ophodu varijable z (u smjeru kretanja obrnuto satnim kazaljkama) i to kad z proputuje omeđenje dosta velikog desnog polukruga sa središtem u O doživi povećanje

$$\Delta \arg p(z) = 2\pi d, \tag{1}$$

pri čemu je d broj ništišta polinoma $p(z)$ u desnoj poluravnini $Re\, z > 0$. No, pri tom proputovanju samom polukružnicom imamo

$$\Delta \arg p(z) = \Delta \arg p_n z^n; \tag{2}$$

pri tom je $p_n z^n$ glavni član od $p(z)$). To izlazi iz činjenice da je na svakom takvom dovoljno velikom kružnom luku

$$\frac{p(z)}{p_n z^n} = 1 + \eta(z)$$

gdje je $|\eta(z)|$ proizvoljno mala veličina. Kako je $\Delta \arg p_n z^n = n\pi$, pri ophodu polukružnicom u pozitivnom smjeru, znači prema (1) i (2) da će biti

$$\Delta_{+ir}^{-ir} p(z) + n\pi = 2d\pi,$$

odnosno

$$-\Delta_{-ir}^{ir} p(z) + n\pi = 2d\pi$$

$$-\Delta_{-r}^{r} p(it) + n\pi = 2d\pi,$$

t realno. Dakle vrijedi

13.6.2. Teorem. *Ako polinom $p(z)$ na imaginarnoj osi nema ništišta, tada je*

$$\Delta_{-\infty}^{\infty} \arg p(it) = (n - 2d)\pi, \quad n = \operatorname{st} p; \tag{1}$$

d je broj ništišta sa pozitivnim realnim dijelom.

13.6.3. *Intervencija Cauchy-evih indeksa.* Broj na lijevoj strani od (1) možemo odrediti pomoću Cauchy-evih indeksa. Neka je za realno t

$$p(it) = u(t) + i\,v(t).$$

Tada je

$$\arg p(it) = \operatorname{arc\,tg} \frac{v(t)}{u(t)}$$

pa se lako dokazuje ovo:

ako je n parno, tada je

$$u(t) = (-1)^{\frac{n}{2}} (p_n t^n - p_{n-2} t^{n-2} + - \cdots)$$

$$v(t) = (-1)^{\frac{n}{2}-1} (p_{n-1} t^{n-1} - p_{n-3} t^{n-3} + - \cdots);$$

ako je n neparno, tada je

$$u(t)=(-1)^{\frac{n-1}{2}}(p_{n-1}t^{n-1}-p_{n-3}t^{n-3}+\cdots)$$

$$v(t)=(-1)^{\frac{n-1}{2}}(p_n t^n-p_{n-2}t^{n-2}+-\cdots).$$

Zato će vrijediti

$$\frac{1}{\pi}\overset{\infty}{\underset{-\infty}{\Delta}}\arg p(it)=\begin{cases}\displaystyle\int_{-\infty}^{\infty}\frac{u(t)}{v(t)} & \text{za neparno } n\\[2ex] \displaystyle\int_{-\infty}^{\infty}\frac{v(t)}{u(t)} & \text{za parno } n.\end{cases}$$

Odatle izlazi

13.6.4. Teorem. Ako je $p(it)\neq 0$ za svako realno t, tada je

$$\int_{-\infty}^{\infty}\frac{p_{n-1}t^{n-1}-p_{n-3}t^{n-3}+-\cdots}{p_n t^n-p_{n-2}t^{n-2}+-\cdots}=n-2d. \tag{1}$$

13.6.5. *Određivanje prethodnog indeksa u regularnom slučaju.* Napisani indeks u 13.6.4. (1) može se odrediti na osnovu Sturmova teorema: formira se Sturmov lanac

$$v_0(t),\ v_1(t),\ \ldots,\ v_s(t) \tag{1}$$

primjenom postupka (E) iz § 5.1. na funkcije

$$\begin{aligned} v_0(t)&=p_n t^n-p_{n-2}t^{n-2}+-\cdots\\ v_1(t)&=p_{n-1}t^{n-1}-p_{n-3}t^{n-3}+-\cdots \end{aligned} \tag{2}$$

Obradimo tzv. *regularni slučaj:* za nj je, po definiciji

$$s=n+1. \tag{3}$$

Kako je $\operatorname{st} v_0\,(=n)>\operatorname{st} v_1>\cdots>\operatorname{st} v_s$, $s=n+1$, znači da je $\operatorname{st} v_j=\operatorname{st} v_{j-1}+1$ i $\operatorname{st} v_s(x)=0$; no v_s je najveći zajednički divizor od $v_0(t)$, $v_1(t)$; to znači da $v_0(x)$, $v_1(x)$ nemaju zajedničkog ništišta pa zato za realno t vrijedi $v_0(t)+iv_1(t)\neq 0$ tj. $p(it)\neq 0$. Prema tome, za *regularni slučaj vrijedi* 13.6.4. No, u *regularnom* slučaju vrlo je lako odrediti najstariji koeficijent od $v_2(t)$ jer je on jednak

$$p_{n-2}-\frac{p_n}{p_{n-1}}p_{n-3}=\frac{p_{n-2}p_{n-1}-p_{n-3}p_n}{p_{n-1}}.$$

Slično vrijedi za ostale funkcije $v_3(t)$, $v_4(t)$, ...

Stvar se pregledno prikazuje pomoću tzv. Routhove sheme.

13.6.6. Routhova shema polinoma $p(x)$. Pravi se ovako:

$$\begin{array}{lllll} & p_n & p_{n-2} & p_{n-4}\cdots & \text{(prvi redak)} \\ & p_{n-1} & p_{n-3} & p_{n-5}\cdots & \text{(drugi redak)} \\ \text{shema množenja } \nearrow\!-\!\searrow & \dfrac{p_{n-1}p_{n-2}-p_n p_{n-3}}{p_{n-1}}, & \dfrac{p_{n-1}p_{n-4}-p_n p_{n-5}}{p_{n-1}}, & \cdots & \text{(treći redak)} \\ & \cdots & \cdots & \cdots & \end{array}$$

Novi redak dobije se iz posljednjeg i pretposljednjeg tako da se njihov ***prvi*** stupac pomnoži *unakrst* redom s ostalim stupcima i rezultat podijeli prvim članom posljednjeg retka.

Drugim riječima, novi redak se dobije dijeleći s protivno označenim prvim članom posljednjeg retka niz determinanata podmatricâ dužine 2 kojima je prvi stupac dvočlani završetak već izgrađenog prvog stupca sheme.

13.6.6.1. Primjer. Routhova tablica polinoma $12+22x+18x^2+7x^3+x^4$ izgleda ovako

$$\begin{array}{lllllll} 1 & 18 & 12 & & 1 & 18 & 12 \\ 7 & 22 & & & 7 & 22 & \\ \left(\dfrac{7\cdot 18-1\cdot 22}{7}=18-\dfrac{22}{7}\doteq\right)15 & \left(\dfrac{7\cdot 12-1\cdot 0}{7}=\right)12 & & \text{dakle} & 15 & 12 & \\ \left(\dfrac{15\cdot 22-7\cdot 12}{15}=22-\dfrac{7\cdot 15}{15}\doteq\right)16 & & & & 16 & & \\ 12 & & & & 12 & & \end{array}$$

Broj promjenâ predznaka prvog stupca je $V=0$.

13.6.6.2. Routhova tablica polinoma $12+2x-2x^2-3x^3+x^4$ glasi

$$\begin{array}{lll} 1 & -2 & 12 \\ -3 & 2 & \\ -\frac{4}{3} & 12 & \\ -25 & & \\ 12 & & \end{array}$$

Tu je $V(1, -3, -\frac{4}{3}, -15, 12)=2$.

13.6.7. *Prvi stupac Routhove sheme.* Posebno je važan prvi stupac Routhove sheme jer je on sastavljen od vodećih koeficijenata Sturmova niza. Prema Sturmovu teoremu 13.3. indeks u teoremu 13.6.4. je jednak promjeni

$$V(-\infty)-V(+\infty)$$

varijacija predznaka Sturmova niza 13.6.5. (1); zato teorem 13.6.4. postaje

(1) $$V(-\infty)-V(+\infty)=n-2\,d.$$

No, za svaki realni polinom $f(x)$ je $\operatorname{sgn} f(+\infty)=\operatorname{sgn} f_n$, $n=\operatorname{st} f$; kako je prvi stupac $R_{\cdot 1}$ Routhove sheme sastavljen od najstarijih koeficijenata Sturmova lanca bit će

(2) $$V(+\infty)=V(R_{\cdot 1}).$$

Isto je tako

(3) $$V(-\infty)=V(R_{11}, -R_{21}, R_{31}, -+\ldots)=n-V(+\infty).$$

Zato (1) postaje
$$(n-V(+\infty))-V(+\infty)=n-2\,d.$$
Tako smo dokazali

—→ **13.7. Teorem. (Routh, 1877).** ***$V(R_{\cdot 1})=d$, tj. ako realni polinom $p(x)$ ima svojstvo da se Sturmov lanac koji počinje sa***

$$v_0(x)=p_n\,x^n-p_{n-2}\,x^{n-2}+-\ldots$$
$$v_1(x)=p_{n-1}\,x^{n-1}-p_{n-3}\,x^{n-3}+-\ldots$$

sastoji od $1+n$ članova ($n=\operatorname{st} p$), tada je broj ništišta polinoma $p(x)$ kojima je realni dio pozitivan jednak broju V promjena predznaka članova prvog stupca Routhove tablice koja je pridružena polinomu p.

Tako npr. za polinom p iz § 13.6.6.1 je $V=0$ dakle i $d=0$; stvarno je $\sigma_p=\{-2, -3, -1\pm i\}$. Isto tako za polinom $p(x)$ iz § 13.6.6.2 je $V=2=d$. Stvarno je $\sigma_p=\{2, 3, -1\pm i\}$; ništišta 2, 3 su u desnoj poluravnini.

—→ **13.8. Teorem. (Routh).** ***Ako polinom p s realnim koeficijentima ima sva svoja ništišta u lijevoj otvorenoj poluravnini $\operatorname{Re} z<0$, onda svi članovi prvog Routhova stupca imaju predznak $\operatorname{sgn} p_n$; i obrnuto.***

Direktni dio teorema. Prema pretpostavci, $\sigma_p\subset(\operatorname{Re} z<0)$; zato na imaginarnoj osi nema nikojeg ništišta od $p(z)$; zato formula 13.6.7. (1) vrijedi sa značenjem $d=0$; dakle je

(1) $$V(-\infty)-V(+\infty)=n.$$

Kako su $V(-\infty)$, $V(+\infty)$ članovi u $\{0, 1,\ldots s-1\}$, $s-1\leq n$, to iz (1) izlazi da je $s=n+1$, $V(+\infty)=0$, $V(-\infty)=s-1=n$; specijalno je dakle $V(+\infty)=0$, što prema 15.6.7 (2) znači da svi članovi Routhova prvog stupca $R_{\cdot 1}$ imaju predznak $\operatorname{sgn} p_n$.

Obratni dio teorema. Kako svi članovi stupca $R_{\cdot 1}$ imaju isti predznak kao $p_n\,(=R_{11})$, znači da su oni svi $\neq 0$, pa ih zato ima maksimalno mnogo, dakle $1+n$. A to kao što smo vidjeli u § 15.6.5. znači da vrijedi 13.6.7. (1); zbog $V(+\infty)=V(R_{\cdot 1})=0$, bit će prema 13.6.7. (3) $V(-\infty)=n$, pa obrazac 13.6.7. (1) daje
$$n-0=n-2\,d$$
dakle $d=0$. Kako niti na imaginarnoj osi nema nikojeg ništišta polinoma p znači da je zaista spektar σ_p u lijevoj otvorenoj poluravnini.

Takav je polinom $p(z)=12+22\,x+18\,x^2+7\,x^3+x^4$ iz § 13.6.6.1. jer je bilo $V=0$; stvarno je $\sigma_p=\{-2, -3, -1+i, -1-i\}$.

13.9. Hurwitz-ova matrica polinoma p.[1] Gornje Routhove teoreme izrazio je Hurwitz 1895. jezikom determinanata, pri čemu dolazi do izražaja ova:

13.9.1. Definicija. *Hurwitzova matrica H polinoma*

$$p(z)=p_n z^n+p_{n-1}z^{n-1}+\cdots+p_1 z+p_0$$

je formata (n, n) i glasi

$$\underset{(n,\,n)}{H=H(p)}=\begin{bmatrix} p_{n-1} & p_{n-3} & p_{n-5}\cdots p_{n-(2n-1)} \\ p_n & p_{n-2}\cdots & \\ p_{n+1}\cdots\cdots & & \\ \vdots & & \\ p_{2n-2} & & \end{bmatrix}$$

pri čemu se stavlja

$$p_k=0 \text{ za } k \text{ non}\in\{0, 1, 2, \ldots, n\}; \text{ tu je } n=\operatorname{st} p, \quad \text{dakle} \quad p_n\neq 0.$$

13.9.2. Uočimo da je $H_{11}=p_{n-1}$ (a ne $H_{11}=p_n$); indeksi u redićima padaju za 2 a u stupcima rastu za 1.

Npr. $H(4x+2+x^3)=H(x^3+0x^2+4x+2)=\begin{bmatrix} 0 & 2 & 0 \\ 1 & 4 & 0 \\ 0 & 0 & 2 \end{bmatrix}$.

Vidimo da je prvi redak $H_1.$ drugi redak Routhove sheme; $H_2.$ je prvi redak Routhove sheme, na koji se nadovezuje određen broj 0.

13.9.3. Mi ovdje obrađujemo tzv. regularni slučaj (isp. § 12.6.5). Prevedimo matricu H u gornje-trokutni oblik. Najprije nadomjestimo redak $H_2.$ retkom $H_2.-\dfrac{H_{21}}{H_{11}}H_1.$; uopće, neka je $H^{(1)}$ matrica formata (n, n) za koju je

$$H^{(1)}_{k.}=H_{k.} \quad (k=1, 3, \ldots)$$

$$H^{(1)}_{k.}=H_{k.}-\frac{H_{21}}{H_{11}}H_{(k-1)}. \quad (k=2, 4, \ldots).$$

Sada $H^{(1)}_{2}.$ počinje sa 0 i trećim retkom Routhove sheme. Izvedimo analogno $H^{(2)}$ iz $H^{(1)}$ stavljajući

$$H^{(2)}_{k.}=H^{(1)}_{k.}-\frac{H^{(1)}_{32}}{H^{(1)}_{22}}H^{(1)}_{(k-1)}. \quad (k=3, 5, \ldots), \text{ inače } H^{(2)}_{k.}=H^{(1)}_{k.}.$$

$$H^{(3)}_{k.}=H^{(2)}_{k.}-\frac{H^{(2)}_{43}}{H^{(2)}_{33}}H^{(2)}_{(k-1)}, \quad (k=4, 6, \ldots), \text{ inače } H^{(3)}_{k.}=H^{(2)}_{k.}$$

. . . .

[1] Adolf Hurwitz (1859—1919), njemački matematičar; uglavnom, djelovao je u Zürichu.

13.9.4. *Routhova matrica* Δ. Neka je Δ tako dobivena trokutna matrica; ona se zove *Routhova matrica*; nastaje iz Routhove sheme R iz § 13.6.6. tako da se spusti prvi redak od R a preostali redići pomaknu se tako udesno da prvi član dođe na dijagonalu; u preostale pretince matrice stavi se 0.

13.9.5. *Minori* Δ_ν. Na osnovu elementarnih svojstava determinanata zaključujemo da *Hurwitzova matrica* H *i Routhova matrica* Δ *imaju jednake odgovarajuće glavne početne minore*. Obično se stavlja

$$\Delta_\nu = \det H\binom{1\,2\ldots\nu}{1\,2\ldots\nu} = \text{determinanta početnog glavnog minora reda } \nu \text{ od } H.$$

No, odgovarajući glavni minor u Δ je

$$R_{21}\; R_{31}\cdots R_{1+\nu\,1},$$

tako da je

$$\Delta_\nu = R_{21}\; R_{31}\cdots R_{1+\nu\,1} \quad (\nu = 1,\, 2, \ldots\, n) \tag{1}$$

(pri regularnom slučaju, Routhov stupac $R_{\cdot 1}$ ima $1+n$ članova i to $R_{11} = p_n$ i članove dijagonale matrice Δ).

Iz formulâ (1) izlazi

$$R_{21} = \Delta_1,\; R_{31} = \frac{\Delta_2}{\Delta_1},\; \ldots,\; R_{\nu 1} = \frac{\Delta_\nu}{\Delta_{\nu-1}} \quad (\nu = 1,\, 2, \ldots,\, n+1). \tag{2}$$

Time Routhov stupac $R_{\cdot 1} = R_{11},\, R_{21}, \ldots,\, R_{n+1\,1}$ postaje (pišući ga kao redak)

$$R_{\cdot 1} = R_{11},\; \frac{\Delta_2}{\Delta_1},\; \frac{\Delta_3}{\Delta_2}, \ldots,\; \frac{\Delta_n}{\Delta_{n-1}}. \tag{3}$$

Time obrazac za broj d ništišta u desnoj poluravnini postaje

$$d = VR_{\cdot 1} = V\left(p_n,\; \frac{\Delta_2}{\Delta_1},\; \frac{\Delta_3}{\Delta_2}, \ldots,\; \frac{\Delta_n}{\Delta_{n-1}}\right) \quad \text{(isp. 13.7).}$$

Na taj način Routhov teorem 13.7. daje

—→ **13.9.6. Teorem. (Hurwitz, 1895).** ***Za broj d ništišta realnog polinoma***

$$p(x) = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_1 x + p_0,\; p_n \neq 0$$

vrijedi

$$d = V\left(p_n,\; \frac{\Delta_2}{\Delta_1},\; \frac{\Delta_3}{\Delta_2}, \ldots,\; \frac{\Delta_n}{\Delta_{n-1}}\right)$$

pri čemu Δ_ν ***označuje glavni početni minor*** ν***-tog reda Hurwitzove matrice H koja je pridružena polinomu p.***

Routhov teorem 13.8. postaje

—→ **13.9.7. Teorem. (Hurwitz, 1895).** ***Ako realni polinom***

$$p(z) = p_n z^n + p_{n-1} z^{n-1} + \cdots + p_1 z + p_0,\; p_n \neq 0$$

ima sva svoja ništišta u lijevoj otvorenoj poluravnini (dakle je d = 0), tada svi članovi niza

$$p_n,\; \Delta_1,\; \frac{\Delta_2}{\Delta_1}, \ldots,\; \frac{\Delta_n}{\Delta_{n-1}}$$

imaju predznak* sgn p_n*; dakle je

$$p_n \Delta_\nu > 0 \quad \textit{za} \quad \nu = 1, 3, \ldots$$

$$\Delta_\nu > 0 \quad \textit{za} \quad \nu = 2, 4, \ldots; \ \textit{i obrnuto}.$$

Odatle posebno izlazi

—→ **13.9.8. Teorem. (Hurwitzov kriterij stabilnosti).** ***Ako je najstariji koeficijent realnog polinom $p(x)$ pozitivan, tada sva ništišta od $p(x)$ imaju negativan realni dio onda i samo onda ako su svi početni glavni minori Hurwitzove matrice H pozitivni.***

Znatna je redukcija toga kriterija sadržana u narednom

13.9.9. Teorem (kriterij stabilnosti; Liénard i Chipart[1], 1914):

Realni polinom $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, $a_n > 0$ ima sva svoja ništišta u lijevoj otvorenoj poluravnini onda i samo onda ako je ispunjen jedan od ova 4 uslova:

1. $a_0 > 0, \ a_2 > 0, \ a_4 > 0, \ldots, \ \Delta_1 > 0, \ \Delta_3 > \cdots$
2. $a_0 > 0, \ a_2 > 0, \ a_4 > 0, \ldots, \ \Delta_2 > 0, \ \Delta_4 > 0, \ldots$
3. $a_0 > 0, \ a_1 > 0, \ a_3 > 0, \ldots, \ \Delta_1 > 0, \ \Delta_3 > 0, \ldots$
4. $a_0 > 0, \ a_1 > 0, \ a_3 > 0, \ldots, \ \Delta_2 > 0, \ \Delta_4 > 0, \ldots$

(isp. Gantmaher [1], st. 457).

Prema tome uslovi 1—4 međusobno su ekvivalentni.

13.9.9.1. Posljedica. (A. Stodola[2]). *Ako je realni polinom s pozitivnim najstarijim koeficijentom Hurwitzov polinom, onda su svi koeficijenti polinoma pozitivni.*

Stodolin rezultat se lako dokazuje i direktno.

14. Zadaci o polinomu $a(x) = a_0 + a_1 x + \cdots + a_n x^n$ stepena n.

1. Nađi brojeve L, l, L', l' služeći se teoremom 1.4, odnosno teoremom 1.5 i to za ove polinome: 1) $2x - 4x^2 + x^4$; 2) $x - x^3 - x^5$; 3) $3 \cdot 5 + 4 \cdot 2x^3 - x^5$; 4) $x^2 - x^3 + 5x^4 - 3x^6$.

2. Dokaži: $a(x) = 0 \Rightarrow$ 1) $|x| \leq 1 + \sup\limits_{\nu < n} \left| \dfrac{a_\nu}{a_n} \right|$

$$2)\ |x| \leq r + \sup_{\nu < n} \left| \frac{a_\nu}{a_n r^{\nu - 1}} \right|$$

[1] Liénard et M. H. Chipart, Sur le signe de la partie réelle des racines d'une équation algébrique (J. Math. Paris, (6), 10 (1914) 291—346).

[2] A. Stodola bio je čehoslovački inženjer, konstruktor parnih turbina.

$$3)\ |x| \leq 2 + \sup_{\nu<n} \left| \left(\frac{a_\nu}{a_n}\right)^{\frac{1}{n-\nu}} \right|$$

$$4)\ |x| \leq \left| \frac{a_{n-1}}{a_n} \right| + \sup_{\nu} \left| \left(\frac{a_{n-\nu}}{a_{n-1}}\right)^{\frac{1}{\nu-1}} \right|.$$

3. Ako je $a(x) = (x-2)^3 (x^2-5x+6)(x-3)$ odredi $\operatorname{sgn} f(x)$ funkcije:

   1) $a(x)$, 2) $\dfrac{x^2-5x+4}{a(x)}$, 3) $(x^2-5x-4)\,a(x)$.

4. Zadan je polinom $a(x) = -4+3x-5x^2+x^4$; odredi broj $V(a)$ promjena predznaka toga polinoma kao i svakog polinoma stupnja 4 kojemu se skup koeficijenata podudara sa skupom koeficijenata polinoma a. Koliko članova ima skup svih $V(a)$?

5. Odredi Budan-Fourierov niz polinoma iz zad. 4.

6. Odredi Sturmov niz pridružen polinomu: 1) $-4+3x-5x^2+x^4$; 2) $3-4x-5x^2+x^4$; 3) $-5+3x-4x^2-4x^4$. Koliko pojedini od tih polinoma ima ništišta u $R(0, 1)$, odnosno u $R(0, 10)$?

7. Odredi Sturmov niz polinoma 1) $T_n(x)$, 2) $L_n(x)$, 3) H_n, 4) $E_n(x) = 1 + \dfrac{x}{1} + \dfrac{x^2}{2!} + \cdots + \dfrac{x^n}{n!}$ kao i njegov broj ništišta u $R(-1, 1)$; pogledati 7, § 12.8. k za $k=6, 7, 8$.

8. Koliko realnih ništišta ima trinom $x^n + px + q$?

9. Dokaži da Legendre-ov polinom $X_n(x)$ ima n-člani spektar iz $R(-1, 1)$ i da između svaka dva susjedna člana iz $\sigma(X_{n-1})$ ima jedan jedini član spektra σX_n (v. 7, § 12.8.5).

10. Dokaži: ako spektar polinoma $p(x)$ leži u otvorenoj donjoj ili gornjoj poluravnini, tada realni polinomi $f(x)$, $g(x)$ za koje je $p(x) = f(x) + ig(x)$ nemaju višestrukih nulišta (Hermite, 1856; Biehler, 1879).

11. Nađi nuždan i dovoljan uslov da bi spektar realna polinoma $p(x)$ stepena 3 bio sastavljen od 1) pozitivnih; 2) negativnih brojeva.

12. Ako su spektri polinomâ $p(x)-a$, $p(x)-b$ realni, tada je i spektar od $p(x)-c$ realan za svako $c \in R(a, b)$; pri tom su a, b realni brojevi; $p(x)$ je realan polinom.

13. Na osnovu Pelletova teorema 10. odredi neki krug oko ishodišta u kojem leži bar jedno ništište ovog polinoma: 1) $3-5x-6x^2$;

    2) $3-5x^2-6x^3$; 3) $3-5x^2-6x^4$; 4) $3-5x^5-6x^{11}$;

    5) $3-5x^n-6x^{2n+1}$.

14. Izvesti Laguerre-ov teorem 11. iz kompozicionog teorema 12.3.

15. Odredi Cauchy-ev indeks $\int\limits_{-\infty}^{\infty} \frac{p(x)}{q(x)}$ za ove parove funkcija $p(x)$, $q(x)$;

1) $x-2$, $x+2$; 2) x^2-9, $x+2$; 3) x^3-2x+4, x^2-5;
4) x^2-5, x^3-2x+4.

16. Odredi: 1) Routhovu shemu; 2) Hurwitzovu matricu; 3) Routhovu matricu polinoma T_n za $n=2, 4, 6$ iz pogl. 7, § 12.8.6.

17. Može li koji polinom Čebiševa imati spektar u otvorenoj: 1) lijevoj; 2) desnoj; 3) donjoj; 4) gornjoj poluravnini?

18. Isto pitanje za polinom $E_n(x) = 1 + \frac{x}{1} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$.

19. Ispitaj da li je koji od ovih polinoma Hurwitzov: 1) $1+x+x^2+2x^3$; 2) $1+x+2x^2+x^3$; 3) $1+2x+x^2+x^3$; 4) $2+x+x^2+x^3$?

20. Isto pitanje za polinom koji se iz prethodnoga primjera iz zad. 19. dobije tako da umjesto koeficijenata 2 pišemo 3, 4, 5, ..., n, ...

21. Ima li koji Hurwitzov polinom oblika $k+x+x^2+\cdots+x^n$, pri čemu je k cio broj.

22. Ako su sva nulišta realnog normiranog polinoma negativna, tada su koeficijenti toga polinoma pozitivni; i obratno.

23. Ima li
    1) polinom $x^4-2x^3-5x^2-2x+24$;
    2) koji polinom dobiven iz prethodnoga pišući umjesto nekog p_k broj $-p_k$ ikoje cjelobrojno ništište?

Literatura

Obreškov [1]—[4]; Perron [1]; Serret [1]; Sierpiński [1]; Simonart [1]; Smirnov [1]; Weber [1].

POGLAVLJE 30.

LINEARNO PROGRAMIRANJE

0. UVODNA RAZMATRANJA

U vremenu 1935—1955 izrasla je nova matematička disciplina koja se zove *Linearno programiranje*, odnosno *Matematičko programiranje* (linearno, nelinearno, dinamičko). Disciplina je izrasla iz planskih razmatranja privrednih, proizvodnih i prevoznih problema. Izgleda da su prvu ideju o linearnom programiranju dali J. von Neumann (1936) i L. V. Kantorović (1939), i to Neumann u vezi s *modelima ekonomije* u razvoju a L. V. Kantorović u vezi s *planiranom proizvodnjom i prevoženjem*. G. B. Dantzig je 1947. formulirao *opći problem linearnog programiranja* i razvio tzv. *simpleksnu metodu* za rješavanje toga problema.

Uz tu novu disciplinu vezana su, osim gornjih imena, još specijalno imena: W. W. Leontief, F. L. Hitchcock, T. C. Koopmans, E. Stiefel, A. Charnes i dr.

Kod linearnog programiranja traži se optimalno rješenje pojedinog zadatka koji se može izraziti pomoću linearnih funkcija, linearnih jednadžbi i linearnih nejednadžbi. Naziv *programiranje* dolazi odatle što u praksi i proizvodnji treba planirati i koordinirati više faktora kako bi se došlo do traženog *optimalnog* rješenja.

Matrice su vrlo pogodno oruđe u teoriji i praksi linearnog programiranja.

Primjene linearnog programiranja a pogotovo matematičkog programiranja uopće vrlo su brojne i raznovrsne i to u ekonomskim, tehničkim naukama, u proizvodnji, biologiji itd.

1. PRIMJERI LINEARNOG PROGRAMIRANJA

1.1. Primjer. Tvornica proizvodi dva modela M_1, M_2 neke robe i to pomoću strojeva S_1, S_2; za model M_1 strojevi rade 2^h i 4^h; za model M_2 radno vrijeme je 4^h i 2^h. Ako je zarada 300,00 d po modelu M_1, a 500,00 d po modelu M_2, treba odrediti kako treba organizirati rad strojevima pa da zarada bude što veća.

Neka je x_1 broj izrađenih jedinica modela M_1 na dan.

Neka je x_2 broj izrađenih jedinica modela M_2 na dan.

To znači da je zarada

(1) $$300\,x_1 + 500\,x.$$

K tome treba da bude:

(2) $$\begin{cases} 2\,x_1 + 4\,x_2 \leq 24 \\ 4\,x_1 + 2\,x_2 \leq 24 \\ x_1 \geq 0 \\ x_2 \geq 0. \end{cases}$$

Rješenja svake od nejednadžbi (2) je zatvorena poluravnina (nacrtajte ih!); rješenja od svih četiriju nejednadžbi daju konveksni 4-kut

(3) $$(0,\ 0),\quad (6,\ 0),\quad (4,\ 4),\quad (0,\ 6)$$

kao presjek tih poluravnina. Lako je dokazati da su ekstremalne vrijednosti poprimljene na vrhovima (isp. § 2.9). Za same vrhove (3) funkcija (1) ima vrijednosti; 0, 1800, 3200, 3000. Dakle je optimum postignut u (4, 4).

To znači da će zarada biti maksimalna kad se na stroju S_1 dnevno izradi 4 primjerka robe M_1 a na stroju S_2 4 primjerka robe M_2. Zarada je dnevno 3200 d.

1.2. Problem prevoženja ili transporta tereta. Na zadanih m stovarišta $S_1, S_2, \ldots, S_m$ nalazi se teret i to po $a_{m'}$ jedinica (npr. u $S_{m'}$ nalazi se $a_{m'}$ tona žita) za $m' = 1, 2, \ldots, m$. Čitav teret treba razdijeliti na n odredišta $O_1, O_2, \ldots, O_n$ tako da u $O_{n'}$ dođe $b_{n'}$ jedinica tereta.

Ako je c_{ik} cijena prevoza jedinice tereta iz S_i u O_k, tad se pita za broj x_{ik} jedinicâ tereta koje se iz stovarišta (skladišta) S_i imaju prevesti u odredište O_k tako da svota-izdatak

(1) $$I = \sum_{i,k} c_{ik}\, x_{ik}$$

bude minimalna.

Prema uslovima zadatka vrijedi:

(2) $$\sum_{\nu=1}^{n} x_{i\nu} = a_i, \qquad \sum_{i=1}^{m} x_{ik} = b_k.$$

Tablično se podaci ispisuju ovako:

	O_1	O_2	$\cdots$	O_n	
S_1	$c_{11};\ x_{11}$	$c_{12};\ x_{12}$	$\cdots$	$c_{1n};\ x_{1n}$	a_1
S_2	$c_{21};\ x_{21}$	$c_{22};\ x_{22}$	$\cdots$	$c_{2n};\ x_{2n}$	a_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_m	$c_{m1};\ x_{m1}$	$c_{m2};\ x_{m2}$	$\cdots$	$c_{mn};\ x_{mn}$	a_m
	b_1	b_2		b_n	

Traži se matrica x formata (m, n) tako da funkcija (1) *bude minimalna na skupu rješenja relacija* (2).

Shema sadrži i zadanu matricu c cijenâ $c_{i\nu}$ kao i traženu matricu x o raspodjeli robe.

1.3. Problem radnog učinka i cijene proizvoda. Na svakom od m zadanih mjesta $S_1, S_2, \ldots, S_m$ može se proizvoditi svaki od potrebnih n proizvoda $H_1, H_2, \ldots, H_n$; zna se za broj a_{ik} jedinicâ (vremena, sirovine, ...) (norma!) koje su potrebne za proizvodnju jedne jedinice proizvoda H_k. Poznat je potencijal s_i mjesta S_i (npr. s_i označuje maksimalan broj časova ili kilograma sirovine, s kojom se mjesečno raspolaže pri mjestu, stroju, S_i).

Zadana je minimalna količina h_k proizvoda H_k koju treba proizvesti.

c_{ik} je cijena proizvodnje po jedinici na S_i od H_k.

Neka je x_{ik} količina jedinicâ proizvoda H_k na radnom mjestu S_i.

Treba x_{ik} odrediti tako da cijena

$$C = \sum_{i,k} c_{ik}\, x_{ik} \tag{1}$$

bude najmanja i da vrijedi

$$(2)\qquad \sum_i x_{ik} \geq h_k, \qquad \sum_k a_{ik}\, x_{ik} \leq s_i \qquad (3)$$

Na taj način imamo $m \cdot n$ neodređenih nepoznatih veličina

$$x_{m'n'} \geq 0 \tag{4}$$

za koje vrijedi (2), (3), (4) i da (1) treba biti minimalno.

Shematski, zadatak se može zadati ovako:

	H_1	H_2	$\cdots$	H_n	
S_1	$c_{11};\ x_{11}$	$c_{12};\ x_{12}$	$\vdots$	$c_{1n};\ x_{1n}$	s_1
S_2	$c_{21};\ x_{21}$	$c_{22};\ x_{22}$	$\vdots$	$c_{2n};\ x_{2n}$	s_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_m	$c_{m1};\ x_{m1}$	$c_{m2};\ x_{m2}$	$\vdots$	$c_{mn};\ x_{mn}$	s_m
	h_1	h_2	$\cdots$	h_n	

1.4. Problem ishrane i kalorija. Riječ je o tome da se za pojedine sastavne dijelove hrane nađu najmanje potrebne količine potrebne dnevno i da cijena hrane bude minimalna.

Zadane su ove veličine:

m broj sastavnih dijelova hrane (nutrienti),

n broj jelâ,

a_{ik} kazuje broj miligrama i-tog sastojka u 1 dg k-ovog jela,

b_i minimalan broj miligrama i-og sastojka,

c_k cijena po dg k-te hrane,

x_k broj u dg k-te hrane koja se ima nabaviti.

Svota-izdatak u dinarima je

(1) $$S = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n.$$

Ta svota treba biti minimalna uz uslove

(2) $$\begin{cases} x_{n'} \geq 0 \\ a_{11} x_1 + a_{12} x_2 + \cdots + a_{1n} x_n \geq b_1 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_{m1} x_1 + \cdots + a_{mn} x_n \geq b_n. \end{cases}$$

Treba dakle riješiti linearni sistem (2) i da (1) bude minimalno.

1.5. Problem razvoženja tereta u najkraće vrijeme. Iz zadanih spremišta

$$S_1,\ S_2, \ldots, S_m$$

s teretom po redu

$$a_1,\ a_2, \ldots, a_m$$

treba robu prevesti na odredišta $O_1, \ldots, O_n$ u količini

$$b_1, \ldots, b_n$$

pri čemu prevoz iz S_i do O_k traje t_{ik}. Odredi količinu x_{ik} koja se iz S_i ima prevesti u O_k tako da prevoženje traje što kraće vrijeme.

Problem je od osobite važnosti kod prevoženja brzo pokvarljive robe.

U obliku tablice problem se ispisuje kao i u prethodnim slučajevima.

Radi se o linearnim jednadžbama:

$$\sum_k x_{ik} = a_i$$

$$\sum_i x_{ik} = b_k, \qquad \sum_i a_i = \sum_k b_k. \tag{1}$$

Svakom rješenju $x \geq 0$ tih jednadžbi odgovara određena matrica $t(x)$ koja se podudara sa t na mjestima gdje je $x > 0$, a na ostalim mjestima je $=0$. Time je određen i $\sup\limits_{i,k} t_{i,k}(x) = t(x)$. Traži se *optimalno* rješenje $x = x_{opt}$ u smislu da bude

$$\sup_{i,k} t(x_{opt}) = \inf_x \sup_{i,k} t_{i,k}(x),$$

pri čemu je $x \geq 0$ i x zadovoljava zadanim jednadžbama (1).

1.5.1. Prema tome, zadaća (2) koju imamo da riješimo je jedna »*minimaks*«-*zadaća* (*inf sup-zadaća*).

Na primjerima se lako vidi da se rješenje gornjeg zadatka ne dobije *ekstremaliziranjem linearne funkcije* $\sum_{i,k} t_{ik} x_{ik}$, jer takva rješenja u pravilu nisu optimalna s obzirom na vrijeme.

2. MATEMATIČKA FORMULACIJA PROBLEMA LINEARNOG PROGRAMIRANJA

2.1. *Prva formulacija.* Zadana je linearna forma

(1) $$f = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n \quad \text{tj.} \quad f = c^T x$$

i sistem linearnih relacija

(2) $$a_{i1} x_1 + \cdots + a_{in} x_n \overset{\le}{\underset{\ge}{=}} b_i \quad (i = 1, 2, \ldots, k);$$

$$\text{ili kraće } a \cdot x \overset{\le}{\underset{\ge}{=}} b_i; \text{ te}$$

(N) $$x_\nu \ge 0;$$

treba naći ekstrem funkcije (1) uz uslove (2), tj. treba naći ona rješenja relacijâ (2) za koje funkcija (1) postaje najmanja (najveća). Podaci $a_{i\nu}$, b_i u (1) i (2) su realni (stvarni) brojevi.

2.2. *Redukcije problema linearnog programiranja.*

2.2.1. *Može se pretpostaviti* $b_i \ge 0$.

Stvarno, ako koje b_i nije ≥ 0 dovoljno je i-tu relaciju u (2) pomnožiti sa -1.

2.2.2. *Može se pretpostaviti da su sve linearne relacije* (2) *jednadžbe.*

Ako i-ta relacija (2_i) u (2) nije jednadžba, dovoljno je uvesti novu *neodrečnu veličinu*

(3)
$y_i = b_i - a_i x$ ako u (2_i) stoji znak $<$ (y_i se zove *varijabla viška*)

$y_i = a_i x - b_i$ ako u (2_i) stoji znak $>$ (y_i se zove *varijabla manjka*).

Ako tada uz nepoznanice x promatramo i te dodatne relacije $y_i \ge 0$ (ukoliko ih ima) nejednadžba (2_i) postaje jednadžbom

$(2_i')$ $$a_i x + y_i = 0$$

u kojoj je desna strana $= 0$.

Zamjenjujući svaku nejednadžbu u sistemu (2) odgovarajućom jednadžbom oblika $(2_i')$ dobije se određen sistem (2') linearnih jednadžbi.

Primijetimo da je broj nepoznanica sistema (2') veći od broja n nepoznanica u (2) i to za broj koji kazuje koliko u (2) ima nejednadžbi.

Iz svakog rješenja

(3) $$(x_1^0, x_2^0, \ldots, x_n^0 \ldots y_i^0 \ldots)$$

sistema (2') *očitava se neposredno i odgovarajuće rješenje* $(x_1^0 \cdots x_n^0)$ *zadanog sistema* (2) *i to kao n-člani početni dio od* (3). *Zato se i možemo ograničiti na slučaj da već u* (2) *imamo samo jednadžbe. Tako nastaje*

2.3. *Formulacija problema linearnog programiranja pomoću jednadžbi.* Zadanu linearnu funkciju

(1) $$c^T x = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n$$

učiniti ekstremalnom (maksimalnom, minimalnom) uz uslov da vrijede jednadžbe

(2) $$a_{i1} x_1 + a_{i2} x_2 + \cdots + a_{in} x_n = b_i \quad (i = 1, 2, \ldots k)$$

te nejednadžbe

(3) $$x_\nu \geq 0 \quad (\nu = 1, 2, \ldots, k).$$

Pri tom su a_i zadani brojevi isto kao i brojevi b_i; pretpostavlja se da je

(4) $$b_i \geq 0 \quad (i = 1, 2, \ldots k).$$

Uvodeći matricu $\underset{(k,\, n)}{a} = [a_{i\nu}]_{i,\nu}$ kao i matrice (stupce) $x = [x_1, \ldots, x_n]^T$, $b = [b_1, \ldots b_k]^T$, tada nastaje

2.4. *Matrična formulacija linearnog programiranja. Zadan je redak*

$$\underset{(1,\, n)}{c^T} = [c_i, \ldots, c_n] \text{ i neodrečan stupac } \underset{(k,\, 1)}{b} \geq 0 \text{ te matrica } \underset{(k,\, n)}{a};$$

naći sve neodrečne stupce $\underset{(n,\, 1)}{x} \geq 0$ *za koje vrijedi*

$$ax = b$$

tako da vrijednost izraza $c^T x$ — *vrijednost programa* — *bude ekstremalna.*

2.5. *Optimalno rješenje.* Svako rješenje x koje ispunjava tražene uslove iz § 2.3. odnosno iz § 2.4. zove se *optimalnim rješenjem ishodnog problema.*

Prema tome, govoreći geometrijski, optimalno rješenje je jedan vektor u prostoru R_n od n dimenzija.

Zato je zgodno služiti se geometrijskim predodžbama i geometrijskom terminologijom.

2.6. Teorem. *Skup svih rješenja x za koje vrijedi*

(L) $$\begin{cases} ax = b \\ x \geq 0 \end{cases}$$

je konveksan i zatvoren (i prazan skup smatramo da je konveksan i zatvoren).

Neka su naime x', x'' bilo koja dva rješenja relacija (L).

Treba dokazati da i njihova tzv. *konveksna* kombinacija

$$x_\theta = \theta\, x' + (1-\theta)\, x''$$

za svaki realni broj $0 \leq \theta \leq 1$ zadovoljava uslovima (L) tj.

(5) $$a x_\theta = b$$

(6) $$x_\theta \geq 0.$$

No, $$a x_\theta = a\,(\theta\, x' + (1-\theta)\, x'') = a\,(\theta\, x') + a\,((1-\theta)\, x'') =$$

$$= \theta\, a x' + (1-\theta)\, a x'' = \theta\, b + (1-\theta)\, b = b;$$

dakle zaista vrijedi (3).

Dokažimo da vrijedi (6). No,

$$x_{\theta i} = \theta\, x_i' + (1-\theta)\, x_i'';$$

po pretpostavci je

$$x_i' \geq 0,\ x_i'' \geq 0, \quad \text{dakle je i } x_{\theta i} \geq 0.$$

Također se neposredno vidi da je skup rješenja od (L) *zatvoren*, tj. da *svaki limes rješenjâ od* (L) *opet je rješenje od* (L).

Na osnovu prethodnog teorema problem linearnog programiranja svodi se na ovaj *problem o ekstremima* (isp. primjer 1.1).

2.7. *Formulacija problema linearnog programiranja pomoću konveksnih skupova.*

Zadan je ***zatvoren konveksan*** *skup C u Euklidovu prostoru R_n s ravnim rubom i linearna forma $c^T x = c_1 x_1 + \cdots + c_n x_n$;* odredi ekstremalne vrijednosti funkcije *$c^T x$ na C i mjesta u C (ako postoje) u kojima je ekstremum postignut.*

2.8. *Idejno rješenje.* Idejno, rješenje posljednjeg problema je vrlo lako provesti. Naime, za svaki broj k, jednadžba

(1) $$c^T x = k$$

predstavlja (»*hiperravninu*«) paralelnu s prostorom R_{n-1} koji je $\perp \vec{c}$; nejednakim vrijednostima k odgovaraju *paralelne* ravnine koje su $\perp \vec{c}$; ujedno vektor $\vec{c}$ pokazuje smjer raštenja funkcije (1).

Projekcija množine C na $\vec{c}$ je određen *konveksan zatvoren skup* $C_{\vec{c}} = [m, M]$ realnih brojeva; *m je minimum a M* je maksimum funkcije (1). Odgovarajuće ravnine $\perp \vec{c}$ zovu se *upirne* (*potporne*) *ravnine množine C za smjer* $\perp \vec{c}$ i to *donja i gornja ravnina. Zajedničke tačke svakih od tih upirnih ravnina sa C daju mjesta na kojima će biti poprimljen ekstrem.*

Na donjoj upirnoj ravnini hvata zadana forma svoj minimum a na gornjoj svoj maksimum.

Naravno, može se desiti da koja od upirnih ravnina ne postoji, tj. ode u beskonačnost.

2.9. No, ako upirna ravnina postoji, sadrži ona bar jedan vrh zatvorenog konveksnog skupa C, pa zato taj vrh množine C možemo smatrati kao pravo rješenje problema linearnog programiranja.

Lako se vidi da pri omeđenom C upirna ravnina sigurno postoji.

3. KAKO SE RJEŠAVA ZADANI LINEARNI PROGRAM?

3.1. Osnovni tip linearnog programiranja. *Zadan je sistem linearnih jednadžbi (pisan matrično vektorski)*

(1) $$\underset{(n,k)}{a}\ \underset{(n,1)}{x} = \underset{(k,1)}{b}$$

uz uslov

(2) $$b \geq 0;$$

treba naći neodrečno rješenje

(3) $$x \geq 0$$

za koje će linearna forma $c^T x$ biti maksimalna.

Matričnu smo jednadžbu (1) obradili u poglavlju 14 § 3; ona dopušta rješenje onda i samo onda ako vektori-stupci $a_{\cdot\nu}$ matrice a generiraju i stupac b; to se kaže još i drukčije da matrica a i matrica $[a, b]$ imaju isti rang r. Prema teoremu 14 § 3.5 možemo se ograničiti na rješavanje bilo kojih r linearno nezavisnih jednadžbi (1). Pretpostavljat ćemo da je upravo prvih r linearnih jednadžbi u (1) linearno nezavisno i da je specijalno »*sjeverozapadna*« matrica

(4) $$A = [a_{ij}] \quad (i, j = 1, 2, \ldots, r)$$

regularna (u 14 § 4.1 matrica A je označivana sa c).

3.2. Bazično rješenje. Stupac x za koji je

(1) $$\begin{bmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_r \end{bmatrix} = A^{-1} \begin{bmatrix} b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_r \end{bmatrix}, \quad \begin{bmatrix} x_{r+1} \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}$$

zadovoljava sistem 3.1. (1) (isp. 14 § 4.2, posljednji obrazac). Rješenje (1) zove se *bazično rješenja sistema* (3.1). (1); kod njega je važno da su jednake nuli sve *nebazične nepoznanice*, tj. nepoznanice kojima stupac koeficijenata nije stupac matrice 3.1. (4).

3.2.1. D e f i n i c i j a. **Bazično rješenje** konsistentne jednadžbe $a\vec{x} = \vec{b}$ jest svako rješenje $\xi = [\xi_1, \xi_2, \ldots, \xi_n]^T$ koje ima svojstvo da za neku regularnu (r, r)-podmatricu A od a bude $\xi_\nu = 0$ za svaki stupac $a_{\cdot\nu}$ koji nije stupac od A (inače, za pojedino $a_{\cdot\nu}$ koje je stupac od A može no ne mora biti $\xi_\nu = 0$).

U vezi sa M-podmatricom $A = [a_{\cdot\nu_1} a_{\cdot\nu_2} \cdots a_{\nu_r}]$ od a govori se o *bazičnim nepoznanicama* $x_{\nu_1}, x_{\nu_2} \cdots, x_{\nu_r}$ i preostalim *nepoznanicama* koje se zovu *nebazične* (isp. 15, § 1.0).

3.3. Nedegenerirana bazična rješenja jesu ona kod kojih su *bazične* nepoznanice $\neq 0$; ako se među bazičnim nepoznanicama rješenja nalazi bar jedna s vrijednosti 0, govori se o *degeneriranom bazičnom rješenju.*

3.4. Bazično neodrečno rješenje. *Problem je naći neodrečno bazično rješenje ukoliko postoji, odnosno dokazati da takvo rješenje ne postoji.* Rješenje se traži jednom iteracionom metodom koja se zove *simpleksna metoda*, jer se geometrijska interpretacija metode svodi na razmatranja o konveksnim skupovima iz § 2.7 koji su u jednostavnijim slučajevima simpleksi[1].

3.5. Pripravni korak pri rješavanju. Rješavanje postavljenog problema 3.1 sastoji se u traženju bazičnog rješenja koje je neodrečno (ostvarljivo); a zatim ćemo dobiveno rješenje nastojati poboljšati da dobijemo *optimalno* rješenje.

Matričnu jednadžbu 3.1. (1), odnosno odgovarajuće linearne jednadžbe rješavat ćemo ovako (držeći na umu uslove (2) (3), iz § 3.1).

3.5.1. *Odvajanje nekih nepoznanica.* Pogledati da li koji stupac $a_{\cdot\nu}$ ima jedan jedini koeficijent $\neq 0$, koji je k tome i pozitivan. *Svaku ćemo takvu nepoznanicu odvojiti rješavajući odgovarajuću jednadžbu i tako riješene jednadžbe stavljati na prva mjesta*; neka takvih nepoznanica, odnosno jednadžbi ima e; njihova matrica je jedinična, ostale jednadžbe (ima ih k-e) *svedimo na nula-oblik*, s tim da 0 dođe na lijevu stranu. Na taj način, provodeći po potrebi promjenu oznaka koeficijenata i nepoznanica dolazimo do *ekvivalentnog sistema*:

$$
(1)\qquad
\begin{aligned}
x_1 &= b_1 - \sum_{\nu=e+1}^{n} a_{1\nu} x_\nu \\
&\dots\dots\dots \\
x_e &= b_e - \sum_{\nu} a_{e\nu} x_\nu \\
&\dots\dots\dots \\
0 &= b_{e+1} - \sum_{\nu} a_{e+1\,\nu} x_\nu \\
&\dots\dots\dots \\
0 &= b_k - \sum_{\nu} a_{k\nu} x_\nu .
\end{aligned}
$$

Sad ćemo na sistemu (1) izvršiti tzv. *simpleksnu transformaciju.*

3.6. Simpleksna metoda rješavanja linearnog sistema.

3.6.1. Pogledati slobodne članove b_i nula-jednadžbi $j_i\,(i = e+1, \dots, k)$; ako su oni svi $=0$, tada se dobije neodrečno rješenje time da sve neodijeljene nepoznanice budu $=0$.

3.6.2. Neka zato bude $b_{e_1} > 0$; promatrajmo odgovarajuću jednadžbu j_{e_1}.

[1] *Najmanji konveksni* skupovi koji obuhvataju zadanih $1+n$ geometrijskih tačaka prostora R_n od n dimenzija zovu se *simpleksi* u R_n. Tako npr. svaki trokut (tetraedar) je simpleks u $\boldsymbol{R}_2$ (odnosno $\boldsymbol{R}_3$).

3.6.2.1. Ako su svi koeficijenti $-a_{e_1\nu}$ pozitivni, tada sistem nema neodrečna rješenja.

3.6.2.2. Ako svi koeficijenti $-a_{e_1\nu}$ nisu >0, neka je npr. koeficijent uz x_{ν_1} negativan tj. $-a_{e_1\nu_1}<0$; taj ćemo član jednadžbe j_1 *markirati tako da ga dvaput podcrtamo.* Učinit ćemo x_{ν_1} *bazičnim,* tj. odijelit ćemo x_{ν_1} *i to iz one jednadžbe* j_{e_1*} za koju je

$$\frac{b_{e_1*}}{a_{e_1*\nu_1}} = \min_{i=1,2,\ldots k}\left\{\frac{b_i}{a_{i\nu_1}}\right\}, \quad a_{i\nu_1}>0. \tag{2}$$

Koeficijent $a_{e_1*\nu_1}$ je *masno štampan ili uokviren* (zbog preglednosti).

3.6.2.3. Time se dobije *ekvivalentni linearan sistem; i pri njemu su slobodni koeficijenti neodrečni.* Odabiranje stožernog člana po uslovu (2) izvrši se zato da se ne pokvari neodrečnost slobodnih koeficijenata. Naime, iz jednadžbe j_{e_1*} sistema (1) posebno izlazi

$$x_{\nu_1} = \frac{b_{e_1*}}{a_{e_1*\nu_1}} - \sum_{\nu_1\neq\nu=e+1}^{n} \frac{a_{e_1*\nu}}{a_{e_1*\nu_1}} x_\nu, \tag{3}$$

pa slobodni koeficijenti postaju

$$b_i' = b_i - a_{i\nu_1}\frac{b_{e_1*}}{a_{e_1*\nu_1}} \tag{4}$$

$$b_i^* = b_i \quad \text{za } i = e_i^*.$$

Odatle izlazi $b_i'\geq 0$; kad bi naime bilo $a_{i\nu_1}<0$, onda je svakako $b_i'>b_i\geq 0$. Ako je $a_{i\nu_1}\leq 0$, tada je

$$b_i' = a_{i\nu_1}\left(\frac{b_i}{a_{i\nu_1}} - \frac{b_{e_1*}}{a_{e_1*\nu_1}}\right)$$

pa je kao produkt neodrečnih brojeva i b_i neodrečno (drugi faktor je neodrečan zbog (2)).

3.6.2.4. Uočenu jednadžbu j_{e_1} obrađivat ćemo tako dugo dok koji njen član ne postane stožernim (koeficijent je i dvaput podcrtan i uokviren), tj. dok se 0-jednadžba j_{e_1} ne svede na razriješeni oblik $\neq 0$ ili dok se ne uvidi da je takvu redukciju nemoguće dobiti na opisani način (*pojava kruženja*!).

3.6.2.5. Ako se stožerni (uokvireni) član nalazi u jednadžbi kojoj je slobodni član $=0$, tada će prema (4) i novi stožerni član biti $=0$.

3.6.2.6. Ako smo završili sa 0-jednadžbom j_{e_1}, onda se prelazi na narednu 0-jednadžbu j_{e_2} itd. dok se ne dobije sistem od r odvojenih nepoznanica ($r=$rang od a), odnosno dok se ne uvidi da sistem nije moguć.

3.7. Shema računanja za računanja na matematičkim strojevima.

3.7.1. Zadan je sistem linearnih jednadžbi oblika

$$0=b_i-\sum_{\nu=1}^{n} a_{i\nu}x_\nu,\ b_i\geq 0 \quad (i=1,2,\ldots,k).$$

3.7.2. Ima li koje $a_{i\nu}>0$?

Nema! Zadatak je nemoguć!

Ima! Tada iz prve moguće 0-jednadžbe j_i izaberemo prvi koeficijent $a_{i\nu_1}$ koji je >0; slobodni član b_i podijeliti sa odgovarajućim članom $a_{i\nu_1}$ iz stupca $a_{\cdot\nu_1}$, ukoliko je $a_{i\nu_1}>0$; zatim naći minimum $\frac{b_{e_1}}{a_{e_1\nu_1}}$ tih kvocijenata.

3.7.3. Riješiti jednadžbu j_{e_1} po x_{ν_1}.

3.7.4. Zapisati tu jednadžbu kao prvu u novom sistemu.

3.7.5. Iz preostalih jednadžbi sistema eliminirati nepoznanicu x_{ν_1} s lijeve strane prve jednadžbe.

3.7.6. Odstraniti eventualne identitete $0\equiv 0$.

3.7.7. Provjeriti da li ima koja 0-jednadžba.

3.7.8. Ako nema više nijedne nula-jednadžbe, tada se *očitava neodrečno bazično rješenje* time, što je svaka bazična nepoznanica jednaka svojem slobodnom koeficijentu a svaka nebazična nepoznanica je $=0$.

3.7.9. Tada se prelazi na traženje optimalnog rješenja.

3.8.1. Primjer. *Naći bazično neodrečno rješenje jednadžbi*

$$\begin{aligned} x_1+x_2+5x_3+2x_4-x_5&=13\\ 3x_1-2x_2+4x_3-5x_4+6x_5&=24\\ -x_1\qquad -3x_3+5x_4+5x_5&=1 \end{aligned} \tag{1}$$

nula-oblik:

$$\begin{array}{ll} 0=13-\underline{\underline{x_1}}-x_2-5x_3+2x_4+x_5 & 13:1=13\\ 0=24-\boxed{3x_1}+2x_2-4x_3+5x_4-6x_5 & 24:3=\boxed{8}\\ 0=1+x_1\qquad +3x_3-5x_4-5x_5 & \\ \hline x_1=8+\frac{2}{3}x_2-\underline{\underline{\frac{4}{3}}}x_3+\frac{5}{3}x_4-2x_5 & 8:\frac{4}{3}=6\\ 0=5-\frac{5}{3}x_2-\boxed{\frac{11}{3}x_3}-\frac{11}{3}x_4+3x_5 & 5:\frac{11}{3}=\boxed{\frac{15}{11}}\\ 0=9+\frac{2}{3}x_2+\frac{5}{3}x_3-\frac{10}{3}x_4-7x_5 & 9:\frac{5}{3}=\frac{27}{5}\\ \hline \end{array}$$

$$x_3 = \frac{15}{11} - \frac{5}{11} x_2 - \boxed{x_4} + \frac{9}{11} x_5 \qquad \frac{15}{11} : 1 = \boxed{\frac{15}{11}}$$

$$x_1 = \frac{68}{11} + \frac{42}{33} x_2 + 3\, x_4 - \frac{34}{11} x_5$$

$$0 = \frac{124}{11} - \frac{1}{11} x_2 - 5\, x_4 - \frac{62}{11} x_5 \qquad \frac{124}{11} : 5 > 2$$

$$x_4 = \frac{15}{11} - \frac{5}{11} x_2 - x_3 + \frac{9}{11} x_5$$

$$x_1 = \frac{113}{11} - \frac{1}{11} x_2 - 3\, x_3 - \frac{7}{11} x_5$$

$$0 = \frac{49}{11} + \frac{24}{11} x_2 + 5\, x_3 - \boxed{\frac{107}{11}} x_5$$

$$x_5 = \frac{49}{107} + \frac{24}{107} x_2 + \frac{55}{107} x_3$$

$$x_4 = \frac{2046 - 319\, x_2 - 682\, x_3}{1177}$$

$$x_1 = \frac{1}{1177} (11638 - 275\, x_2 - 3916\, x_3).$$

Odatle očitavamo jedno neodrečno (ostvarljivo) rješenje:

(2) $$x_1 = \frac{11638}{1177} = \frac{1058}{107}, \quad x_2 = 0, \quad x_3 = 0, \quad x_4 = \frac{2046}{1777} = \frac{186}{107}, \quad x_5 = \frac{49}{107}.$$

Brojevi (2) su dosta nespretni. Inače evo još jednog baričnog rješenja:

(3) $$0, \qquad 0, \qquad 3, \qquad 0, \qquad 2.$$

Rješenje (2) je bazično, jer stupci nepoznanicâ x_1, x_4, x_5 daju matricu A sa $\det A \neq 0$ $(\det A = -107)$ pa je $r \geq 3 = k$ dakle $r = 3 = k$.

3.8.2. Primjer. (*slučaj kruženja*) (v. A. S. Barsov [1], str. 43).

$$x_1 = 0 - \boxed{x_4} + x_5 + x_6 - 3\, x_7 \qquad 0 : 1 = \boxed{0}$$

$$x_2 = 0 - 2\, x_4 + x_5 + \frac{1}{2} x_6 - x_7 \qquad 0 : 2 = 0$$

$$x_3 = 1 - x_4 - x_5 - 3\, x_6 + 8\, x_7 \qquad 1 : 1 = 1$$

Odatle odmah očitavamo neodrečno rješenje:

$$x_1=0,\quad x_2=0,\quad x_3=1,\quad x_4=0,\quad x_5=0,\quad x_6=0,\quad x_7=0.$$

Primijenimo simpleksnu metodu s ciljem da desno u razrješenom obliku ne bude neslobodnih koeficijenata <0. Izlazi

$$\begin{array}{ll}
x_4=0-x_1+x_5-x_6-3x_7 & 0:1=0\\
x_2=0+2x_1-\boxed{x_5}-\frac{3}{2}x_6+5x_7 & 0:1=\boxed{0}\\
x_3=1+x_1-\underline{\underline{2x_5}}-4x_6+11x_7 & 1:2=0{,}5
\end{array}$$

$$\begin{array}{ll}
x_5=0+2x_1-x_2-\frac{3}{2}x_6+5x_7 & 0\\
x_4=0+x_1-x_2-\boxed{\frac{1}{2}x_6}+2x_7 & \boxed{0}\\
x_3=1+3x_1+2x_2-\underline{\underline{x_6}}+x_7 & 1:1=1
\end{array}$$

$$\begin{array}{l}
x_6=0+2x_1-2x_2-2x_4+4x_7\\
x_5=0-x_1+2x_2+3x_4-\boxed{x_7}\\
x_3=1-5x_1+4x_2+2x_4-\underline{\underline{3x_7}}
\end{array}$$

$$\begin{array}{l}
x_7=0-x_1+2x_2+3x_4-x_5\\
x_6=0-\boxed{2x_1}+6x_2+10x_4-4x_5\\
x_3=1-\underline{\underline{2x_1}}-2x_2-7x_4+3x_5
\end{array}$$

$$\begin{array}{l}
x_1=0+3x_2+5x_4-2x_5-\frac{1}{2}x_6\\
x_7=0-\boxed{x_2}-2x_4+x_5+\frac{1}{2}x_6\\
x_3=1-\underline{\underline{8x_2}}-17x_4+7x_5+x_6
\end{array}$$

$$\begin{array}{l}
x_1=0-x_4+x_5+x_6-3x_7\\
x_2=0-2x_4+x_5+\frac{1}{2}x_6-x_7\\
x_3=1-x_4-x_5-3x_6+8x_7
\end{array}$$

A to je ishodni sistem, pa se proces nastavlja kružno.

3.9. Bazična neodrečna rješenja i vrhovi konveksnog skupa C. U § 2.6. dokazali smo da *sva neodrečna* rješenja x jednadžbe $ax=b$ čine određen zatvoren *konveksan skup* C (koji može biti i prazan). Sada ćemo dokazati kako postoji *organska povezanost između bazičnih neodrečnih rješenja s jedne strane i vrhova od C s druge strane.*

3.9.1. Definicija vrha. Svaka tačka C_0 od C sa svojstvom da iz

$$C_0=\lambda x+(1-\lambda)y, \quad \{x, y\}\subset C, \quad 0<\lambda<1$$

izlazi

$$C_0=x=y$$

zove se *vrh od C.*

⟶ **3.9.2. Teorem.** ***Svako bazično neodrečno rješenje x_A jednadžbe $ax=b$ određuje vrh konveksnog skupa C svih neodrečnih rješenja.***

Zbog jednostavnijeg pisanja možemo pretpostaviti da je prvih m koordinata od x_A pozitivno, a da su preostale koordinate (nepoznanice) $=0$, tj.

$$x_A=[x_{A1}\, x_{A2} \ldots x_{Am}\, 0,\, 0, \ldots, 0]^T.$$

Kada element $x_A\in C$ ne bi bio vrh od C, postojala bi dva druga *različna* elementa y i t iz C sa svojstvom da x_A bude *konveksna kombinacija* od y i t, dakle

$$x_A=\lambda y+(1-\lambda)t \text{ za neki broj } \lambda\in R(0, 1) \text{ (isp. § 2.6).}$$

Kako su koordinate od x_A, x, t neodrečne, to relacije

$$x_{A\nu}=0\ (\nu=m+1, \ldots, n)$$

odnosno relacije

$$\lambda y_\nu+(1-\lambda)t_\nu=0 \quad \text{daju} \quad y_\nu=0=t_\nu \quad \text{za } \nu=m+1, m+2, \ldots, n$$

pa je

$$y=[y_1, y_2, \ldots, y_m, 0, 0, \ldots, 0]^T, \quad t=[t_1, t_2, \ldots, t_m, 0, 0, \ldots, 0]^T.$$

To znači da bi vektori y, t kao rješenja od $ax=b$ dali

$$y_1 a_{\cdot 1}+\cdots+y_m a_{\cdot m}=b$$

$$t_1 a_{\cdot 1}+\cdots+t_m a_{\cdot m}=b;$$

odakle

$$y_1 a_{\cdot 1}+\cdots+y_m a_{\cdot m}=t_1 a_{\cdot 1}+\cdots+t_m a_{\cdot m}.$$

No, vektori-stupci $a_{\cdot 1}, \ldots, a_{\cdot m}$ su linearno nezavisni; zato iz poslednje jednakosti izlazi $y_\mu=t_\mu$ ($\mu=1, 2, \ldots, m$) dakle $y=t$, protivno pretpostavci da je $y\neq t$.

⟶ **3.9.3. Teorem.** ***Svaki vrh $\xi=[\xi_1, \ldots \xi_n]^T$ konveksnog skupa C svih neodrečnih rješenja jednadžbe $ax=b$ daje određeno bazično rješenje te jednadžbe pa je zato b odgovarajuća linearna kombinacija vektorâ $a_{\cdot\nu}$:***

$$\xi_1 a_{\cdot 1}+\cdots+\xi_n a_{\cdot n}=b.$$

Posebno, pretpostavimo li da je prvih m koordinata vrha pozitivno, a da su preostale koordinate $=0$, tada je

$$\xi_1 a_{\cdot 1}+\cdots+\xi_m a_{\cdot m}=b. \tag{1}$$

Obradimo poslednji slučaj

$$\xi_\mu > 0 \ (\mu = 1, 2, \ldots, m), \quad \text{te} \quad \xi_i = 0 \quad \text{za } i = m+1, \ldots, n.$$

Tada vrijedi (1). Tvrdimo da su stupci-vektori $a_{\cdot 1}, \ldots, a_{\cdot m}$ linearno nezavisni. U obratnom slučaju postojao bi vektor $y = [y_1, \ldots, y_m]^T \neq 0$ sa svojstvom

$$y_1 a_{\cdot 1} + \cdots + y_m a_{\cdot m} = \vec{0} \tag{2}$$

pa bi za *svaki* realni broj $\lambda > 0$ iz (1) i (2) izlazilo

$$\begin{aligned} (\xi_1 + \lambda y_1) a_{\cdot 1} + \cdots + (\xi_m + \lambda y_m) a_{\cdot m} &= b \\ (\xi_1 - \lambda y_1) a_{\cdot 1} + \cdots + (\xi_m - \lambda y_m) a_{\cdot m} &= b \end{aligned} \tag{3}$$

(dovoljno je (2) pomnožiti sa λ i dodati k (1) odnosno oduzeti od (1)).

Posebno bi se zbog pretpostavke $y \neq \vec{0}$ broj λ mogao odrediti tako malim da *svi koeficijenti* u (3) *budu* > 0 (jer je $\xi_\mu > 0$). To znači da bi $\xi + \lambda y$, $\xi - \lambda y$ bila *dva različna neodrečna rješenja* od $ax = b$, a ξ bi bila njihova polusuma; drugim riječima, ξ ne bi bio vrh od C, protivno pretpostavci.

3.10. Put od neodrečnog osnovnog rješenja k mogućem optimalnom rješenju. — 3.10.1. *Problem je ovaj: uz zadani vektor* $b \geq 0$ *i zadanu matricu* a *formata* (r, n) *naći vektor* x *tako da bude*

$$\begin{aligned} ax &= b \\ x &\geq 0 \end{aligned} \tag{1}$$

te da zadana linearna forma $z = c^T x$ *bude maksimalna* (isp. § 2).

Pretpostavimo da jednadžbe

$$ax = b, \quad \text{uz uslov } b \geq 0$$

dopuštaju *bar jedno neodrečno rješenje* x'; rješenje x' ima

$$r \ (= \operatorname{rang} a = \operatorname{rang} [a, b])$$

bazičnih nepoznanica 0 ili $\neq 0$; ostalih n-r nepoznanica vektora x' imaju vrijednost 0. Označimo sa A podmatricu od a kojoj su stupci upravo a_s, pri čemu x_s označuje opću *bazičnu* nepoznanicu u spomenutom rješenju x'. Tada samo bazično rješenje x' možemo u zavisnosti od A označiti sa

$$x_A = \begin{bmatrix} x_{A1} \\ \cdot \\ \cdot \\ \cdot \\ x_{An} \end{bmatrix} = [x_{A1}, \ldots, x_{An}]^T. \tag{2}$$

Zbog iščezavanja nebazičnih nepoznanica u rješenju x_A jednadžba $ax_A = b$ poprima također ovaj posebni oblik

$$\sum_{\rho=1}^{r} x_{A\rho} A_{\cdot\rho} \quad (\rho = 1, 2, \ldots, r). \tag{3}$$

I vrijednost programa $c^T x$ poprima sada specijalniji oblik

$$c_A^T x_A \tag{4}$$

pri čemu je c_A onaj podniz od niza $c = [c_1, \ldots, c_n]^T$ koji odgovara nizu *baričnih* nepoznanica u nizu $x_1, \ldots, x_n$ svih nepoznanica problema (isp. § 3.2).

Mijenjajući svojstvenu bazu A mijenja se bazično rješenje x_A i vrijednost (4) programa. Može li se A tako odabrati da (4) bude maksimalno?

3.10.2. Kako je A regularna podmatrica od a reda koji je jednak rangu r od a, znači to da će svaki stupac $a_{\cdot\nu}$ od a biti linearna kombinacija stupaca $A_{\cdot\rho}\,(\rho = 1, 2, \ldots, r)$ matrice A. Pa neka je $a_{\cdot\nu}(A)$ zapis vektora-stupca $a_{\cdot\nu}$ u bazi A; dakle

$$a_{\cdot\nu} = \sum_\rho a_{\rho\nu}(A)\, A_{\cdot\rho}\,(\rho = 1, 2, \ldots, r). \tag{1}$$

Pokušajmo neki stupac $A_{\cdot e}$ baze A nadomjestiti kojim stupcem $a_{\cdot\nu}$ van A time da dobijemo opet jednu vektorsku bazu

$$A' = [A_{\cdot 1}, \ldots, A_{\cdot e-1}, a_{\cdot\nu}, A_{e+1} \ldots A_r]$$

i da odgovarajuće bazično rješenje $x_{A'}$ daje veću vrijednost

$$c_{A'}^T x_{A'}, \tag{2}$$

programa od one vrijednosti koja odgovara bazi A.

U relaciji (1) za $\rho = e$ mora biti $a_{e\nu}(A) \neq 0$, jer će se samo tada $A_{\cdot e}$ moći izraziti u bazi A'; bit će

$$A_{\cdot e} = \frac{a_{\cdot\nu}}{a_{e\nu}(A)} - \sum_{\rho \neq e} \frac{a_{\rho\nu}(A)}{a_{e\nu}(A)} A_{\cdot\rho}.$$

Time jednadžba (3) iz § 3.10.1. postaje

$$\sum_{\rho \neq e} x_{A\rho} A_{\cdot\rho} + x_{Ae}\left(\frac{a_{\cdot\nu}}{a_{e\nu}(A)} - \sum_{\rho \neq e} \frac{a_{\rho\nu}(A)}{a_{e\nu}(A)} A_{\cdot\rho}\right) = b,$$

tj.

$$\sum_{\rho \neq e}\left(x_{A\rho} - x_{Ae}\frac{a_{\rho\nu}(A)}{a_{e\nu}(A)}\right) A_{\cdot\rho} + \frac{x_{Ae}}{a_{e\nu}(A)} a_{\cdot\nu} = b. \tag{3}$$

Kako tražimo da i novo bazično rješenje, $x_{A'}$, bude neodrečno, znači da u (3) koeficijenti uz stupce baze A' moraju biti ≥ 0, tj.

$$x_{A'\rho} \equiv x_{A\rho} - x_{Ae}\frac{a_{\rho\nu}(A)}{a_{e\nu}(A)} \geq 0 \quad \rho \neq e, \tag{4}$$

$$x_{A'e} \equiv \frac{x_{Ae}}{a_{e\nu}(A)} \geq 0. \tag{5}$$

Kako je $x_A \geq 0$, to za neodrečnost od $x_{A'}$ mora biti

$$a_{e\nu}(A) > 0,$$

ukoliko želimo dobiti neodrečno rješenje $x_{A'}$. No, bit će $x_{A'} \geq 0$, ukoliko stupac $A_{\cdot e}$ koji uklanjamo izaberemo tako da vrijedi

(6) $$\frac{x_{Ae}}{a_{e\nu}(A)} = \inf_{\rho} \frac{x_{A\rho}}{a_{\rho\nu}(A)}$$

uz uslov

(7) $$a_{\rho\nu}(A) > 0.$$

Naime, uz (7) relacija (4) je ekvivalentna s relacijom

(4') $$\frac{x_{A\rho}}{a_{\rho\nu}(A)} - \frac{x_{Ae}}{a_{e\nu}(A)} \geq 0.$$

No, relacija (4') je sigurno ispunjena ako smo indeks e odredili na osnovu (6) i (7).

3.10.3. Usporedimo vrijednost z' linearnog programa za bazično rješenje $x_{A'}$ i vrijednost z za bazično rješenje x_A:

$$z' = c_{A'}^T x_{A'} = c_{A'1} x_{A'1} + \cdots + c_{A'r} x_{A'r} = (\text{zbog relacija (4), (5)}) =$$

(8) $$z' = \sum_{\rho \neq e} c_{A\rho} \left(x_{A\rho} - x_{Ae} \frac{a_{\rho\nu}(A)}{a_{e\nu}(A)} \right) + c_\nu \cdot \frac{x_{Ae}}{a_{e\nu}(A)}$$

(naime $c_{A'e} = c_\nu$, $c_{A'\rho} = c_{A\rho}$ za $\rho \neq e$).

Tu se sumacija može protegnuti i na slučaj $\rho = e$ jer je odgovarajući član jednak 0; na taj način izraz sa z' postaje

(9) $$z' = \sum_{\rho=1}^{r} c_{A\rho} x_{A\rho} - \frac{x_{Ae}}{a_{e\nu}(A)} \sum_{\rho=1}^{r} c_{A\rho} a_{\rho\nu}(A) + \frac{x_{Ae}}{a_{e\nu}(A)} c_\nu .$$

Stavimo li

(10) $$z_\nu = \sum_{\rho=1}^{r} c_{A\rho} a_{\rho\nu}(A),$$

postaje (9) oblika

(11) $$z' = z + \mu (c_\nu - z_\nu), \quad \mu = \frac{x_{Ae}}{a_{e\nu}(A)} .$$

Za danu bazu A i dani stupac $a_{\cdot\nu}$ brojevi c_ν, z_ν kao i broj $c_\nu - z_\nu$ potpuno su određeni. No,

(12) $$\mu \geq 0,$$

pa imamo dva slučaja: $\mu = 0$, odnosno $\mu > 0$. Ako je $\mu > 0$, tada je $\operatorname{sgn}(z' - z) = \operatorname{sgn}(c_\nu - z_\nu)$; specijalno, ako je $z_\nu < c_\nu$, bit će stvarno $z' > z$ pa je novo bazično rješenje $x_{A'}$ bolje od prethodnog.

Pretpostavimo da je

(13) $$z_\nu \geq c_\nu \text{ za svako } \nu = 1, 2, \ldots n.$$

Dokažimo da će odgovarajuće bazično rješenje x_A biti optimalno, tj. pripadajuća vrijednost z_0 *programa je maksimalna.* Drugim riječima, za svako neodrečno rješenje x jednadžbe $ax=b$ bit će

$$\sum_{\rho=1}^{r} x_{A\rho}\, c_{A\rho}=z_0\geq z=\sum_{\nu=1}^{n} c_\nu x_\nu. \tag{14}$$

To znači da iz $x\geq 0$ i

$$\sum_\nu x_\nu a_{\cdot\nu}=b \text{ izlazi (14).} \tag{15}$$

Da to dokažemo, sjetimo se relacije 3.10.2 (1); zato (15) postaje

$$\sum_\nu x_\nu \sum_\rho a_{\rho\nu}(A)\cdot A_{\cdot\rho}=b,$$

što zajedno sa $b=\sum\limits_\rho x_{A\rho} A_{\cdot\rho}$ daje

$$x_{A\rho}=\sum_\nu x_\nu\, a_{\rho\nu}(A). \tag{16}$$

U drugu ruku, za svako ρ koje odgovara bazičnoj nepoznanici vrijedi $z_\rho=c_\rho$; kako za ostale nepoznanice po hipotezi vrijedi (13) znači da je $z_\nu\geq c_\nu$ za svako ν iz niza $1, 2, \ldots, n$. Kako je $x\geq 0$, bit će $z_\nu x_\nu\geq c_\nu x_\nu$ dakle

$$\sum_\nu z_\nu x_\nu\geq\sum c_\nu x_\nu\equiv z. \tag{17}$$

No, po definiciji (10) daje (17) relaciju

$$\sum_\nu\sum_\rho c_{A\rho}\, a_{\rho\nu}(A)\, x_\nu\geq z,$$

tj.

$$\sum_\rho\Big(\sum_\nu a_{\rho\nu}(A)\, x_\nu\Big)\, c_{A\rho}\geq z. \tag{18}$$

Relacija (16) i relacija (18) daju

$$\sum_\rho x_{A\rho}\, c_{A\rho}\geq z.$$

Na osnovu (14) znači to da je zaista $z_0\geq z$.

3.10.4. Kad bi u (13) umjesto znaka $\geq$ stajalo $\leq$, tada bi na analogan način zakjučili da je z_0 minimalna vrijednost linearnog programa. Na taj smo način dokazali

⟶ **3.10.5. Teorem (i).** ***Ako linearni program***

$$\boldsymbol{ax=b,\quad x\geq 0,\quad \max c^T x}$$

ima u nekoj bazi A rješenje $x_A=A^{-1}b$, pa ako u toj bazi vrijedi

$$z_\nu\geq c_\nu\ (\nu=1, 2, \ldots, n),$$

tada je x_A optimalno rješenje; dakle je pripadna vrijednost z_0 programa maksimalna.

(ii) *Ako linearni program*

$$ax = b, \quad x \geq 0, \quad \min c^T x$$

u nekoj bazi A ima rješenje $x_A = A^{-1} b$ *pa ako u toj bazi stupaca vrijedi*

$$z_\nu \leq c_\nu \; (\nu = 1, 2, \ldots, n),$$

tada rješenje x_A *daje minimalnu vrijednost linearnog programa.*

3.10.6. Primjer. Obradimo primjer iz § 1.1. uvodeći pomoćne nepoznanice

$$x_3 = 24 - 2x_1 - 4x_2, \quad x_4 = 24 - 4x_1 - 2x_2:$$

riješiti linearni program:

(1)
$$\begin{aligned} 2x_1 + 4x_2 + x_3 \quad\quad &= 24 \\ 4x_1 + 2x_2 \quad\quad + x_4 &= 24 \end{aligned}$$

(2)
$$\max z = 300x_1 + 500x_2 + 0 \cdot x_3 + 0 \cdot x_4.$$

Tu je

$$a = \begin{bmatrix} 2 & 4 & 1 & 0 \\ 4 & 2 & 0 & 1 \end{bmatrix}, \quad c = [300, 500, 0,0]^T.$$

Jedno neodrečno rješenje prvih dviju jednadžbi je npr. 3, 3, 6, 6; pripadno je $z = 2\,400$. Tražimo li da bude $x_3 = x_4 = 0$, tada jednadžbe (1) daju $x_1 = x_2 = 4$ pa imamo bazično neodrečno rješenje

$$x_A = [4, 4, 0, 0]^T \text{ za bazu } A = a._1, a._2 = \begin{bmatrix} 2 & 4 \\ 4 & 2 \end{bmatrix}.$$

Za stupac $a._3 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ imamo

$$a._3 = \lambda_1 \begin{bmatrix} 2 \\ 4 \end{bmatrix} + \lambda_2 \begin{bmatrix} 4 \\ 2 \end{bmatrix}, \text{ tj.}$$

$$2\lambda_1 + 4\lambda_2 = 1 \quad 4\lambda_1 + 2\lambda_2 = 0$$

odakle

$$\lambda_1 = -\frac{1}{6}, \quad \lambda_2 = \frac{1}{3}.$$

Dakle je $a._3(A) = \begin{bmatrix} -1/6 \\ 1/3 \end{bmatrix}$; pripadno z_3 je

$$z_3 = c_1 \cdot -1/6 + c_2 \cdot 1/3 = -50{,}00 + 166{,}66 > 0,$$

što zbog $c_3 = 0$ znači da je $z_3 \geq c_3$.

Isto tako za stupac $a._4 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ imamo prikaz $a._4(A) = \begin{bmatrix} 1/3 \\ -1/6 \end{bmatrix}$ u bazi A pa se vidi da je također $z_4 \geq c_4 \; (= 0)$. Zato prema teoremu 3.10.5. (i) rješenje $x_A = 4, 4, 0, 0$ daje traženo optimalno rješenje. Stvarno je $z_0 = 3200$.

3.11. Još oko traženja neodrečnog rješenja. Poteškoća u rješavanju problema linearnog programiranja sastoji se specijalno u nalaženju *neodrečnog* ili tzv. *ostvarljivog* (engl. *feasible*) rješenja, odnosno u dokazu da neodrečnog rješenja nema. Naime, ako poznamo neko neodrečno rješenje, može se iz njega dobiti (npr. na način opisan u § 3.10.3) i *bazično neodrečno rješenje.*

No, u zadanom sistemu jednadžbi (k jednadžbi sa n nepoznanicâ) *može se dodati određen broj vještačkih ili artificijelnih nepoznanicâ* $y_1, y_2, \ldots$ tako da u novonastaloj matrici bude ipak jedna jedinična podmatrica duljine $r = \operatorname{rang} a$; u najnepovoljnijem slučaju može se umjesto jednadžbe $ax = b$ promatrati jednadžba

(1) $$a^\circ x + 1_r y = b \quad \text{tj.} \quad [a\, 1_r]\begin{bmatrix} x \\ y \end{bmatrix} = b;$$

pri tom je a° podmatrica od a sastavljena od r linearno nezavisnih redaka matrice a; 1_r je jedinična matrica reda r; za jednadžbu (1) možemo odmah navesti bazično neodrečno rješenje, npr. ovo

(2) $$x = \vec{0}, \quad y = \vec{b}.$$

Naravno, rješenje (2) nije bazično za polazni problem $ax = b$, no bazično rješenje (2) možemo poboljšavati na način opisan u § 3.10.3. i dobiti bazično neodrečno rješenje same jednadžbe $ax = b$, ukoliko ono postoji; pri tom *vještačkim varijablama* $y_1, y_2, \ldots$ *pridružujemo pripadne koeficijente cijenâ* $c_{n+1} = c_{n+2} = \cdots = -M$ *gdje je* M ***veliki pozitivan broj***; ovakav izbor brojeva $c_{n+1}, c_{n+2}, \ldots$ ima za cilj da eventualno optimalno maksimalno rješenje proširenog problema (1) poništi svaku vještačku varijablu i da se iz toga rješenja odmah čita rješenje i zadanog problema.

Naime, ako je neka vještačka nepoznanica y_i pozitivna, tada se možemo nadati da to rješenje poboljšamo u smislu da vrijednost z programa bude još veća.

4. DUAL ZADANOG LINEARNOG PROGRAMA

4.0. Promatrajmo opet linearni program, ali ovaj put u *obliku nejednadžbi* (svaku jednadžbu $e = f$ možemo nadomjestiti sa $e \geq f$, $e \leq f$); također možemo pretpostaviti da su sve nejednadžbe ili tipa $\leq$ ili tipa $\geq$ (jedan tip prelazi u drugi množeći sa -1; zato pri linearnom programu s nejednadžbama vektor b ne mora biti ≥ 0).

Promatrajmo ovaj

4.1. Tip I linearnog programa: *Zadani su: matrica a, vektori b, c; traži se vektor x tako da funkcija*

(1) $$z = c^T x$$

bude maksimalna uz uslove da vrijedi

(2) $$ax \leq b,$$
$$x \geq 0.$$

Međutim, uz matricu a vezana je i transponirana matrica a^T pa iz matrice a^T i vektorâ b, c možemo formulirati

4.2. Dual linearnog programa I: *Naći vektor X tako da funkcija*

(3) $$Z = b^T X$$

poprimi minimalnu vrijednost za sva neodrečna rješenja X nejednadžbe

(4) $$a^T X \geq c.$$

Neposredno se vidi da dužina i širina matricâ a, x, b, c odnosno dužine matrica a^T, X, c, b dopuštaju gornju dualnu formulaciju. Kaže se da je I dual svojeg duala.

Dokazat ćemo da između linearnog programa (4.1.) i njegova duala (4.2.) postoje vrlo uske veze.

4.3. Teorem. *Vrijednost z programa I i vrijednost Z njegova duala zadovoljavaju $z \leq Z$ tj. $c^T x \leq b^T X$ za svako neodrečno rješenje x nejednadžbe* (2) *i svako neodrečno rješenje X nejednadžbe* (4).

Naime, zbog $X \geq 0$ daje relacija (2) skalarnim množenjem sa X ovu relaciju

(5) $$X^T ax \leqq X^T b = b^T X = Z.$$

Iz istog razloga množeći (4) skalarno vektorom $x \geq 0$ dobijemo

$$x^T (a^T X) \geq x^T c$$

odakle (zbog vektorskog identiteta $x^T y = y^T x$)

(6) $$(a^T X)^T x \geq c^T x$$

$$X^T ax \geq c^T x = z.$$

Iz (5), (6) izlazi tražena relacija $z \leq Z$.

⟶ **4.4. Teorem.** ***Neka je $\overset{\circ}{x}$ neodrečno rješenje programa $ax \leq b$,*** **$\max z = c^T x$*****; neka je $\overset{\circ}{X}$ neodrečno rješenje dualnog problema $a^T X \geq c$,*** **$\min Z = b^T X$*****; tada jednakost***

(7) $$c^T \overset{\circ}{x} = b^T \overset{\circ}{X}$$

ima za posljedicu da su $\overset{\circ}{x}$, $\overset{\circ}{X}$ optimalna rješenja problema I, odnosno dualnog problema **I^d** ***(naravno da je općenito $\overset{\circ}{x} \neq \overset{\circ}{X}$).***

Naime, prema § 4.3. za svako neodrečno rješenje x relacije (2) vrijedi $c^T x \leq b^T \overset{\circ}{X}$; ta relacija zajedno sa (7) daje $c^T x \leq c^T \overset{\circ}{x}$; to znači da je $\overset{\circ}{x}$ traženo optimalno (dakle ovdje maksimalno) rješenje.

$\longrightarrow$ **4.5. Osnovni teorem o dualitetu.** ***Linearni program*** $ax \leq b$, $\max z = c^T x$ ***dopušta optimalno rješenje onda i samo onda ako dualni linearni program*** $a^T X \geq c$, $\min Z = b^T X$ ***dopušta optimalno rješenje; tada je vrijednost programa jednaka vrijednosti dualnog programa.***

4.5.1. Dokažimo nužni (prvi) dio teorema. Pa neka je x_A optimalno rješenje primarnog programa (1), (2). Napišimo relaciju $ax \leq b$ kao *jednadžbu*

(8) $$a^\circ x + 1_r y = b \quad \text{tj.} \quad [a^\circ, 1_r]\begin{bmatrix} x \\ y \end{bmatrix} = b \quad (v. \ § \ 3. \ 11 \text{ za } a^\circ).$$

Pri tom je $x \geq 0$, $y \geq 0$; naravno

$$y_\rho = b_\rho - (ax)_\rho \quad (\rho = 1, \ldots r);$$

koeficijent cijene c_{n+k} koji odgovara varijablama y jednak je 0. Za svaki vektor $a'_{\cdot j}$ matrice $a' = [a, 1_r]$ za odgovarajuću veličinu $z_j = \sum\limits_\rho c_{A\rho} a'_{\rho j}(A)$ (vidi § 3.10.3. (10)) zbog optimalnosti rješenja x_A vrijedi

$$\sum_\rho c_{A\rho} a_{\rho j}(A) \geq c_j,$$

tj.

(9) $$c_A^T a_{\cdot j}(A) \geq c_j.$$

Pri tom vrijedi jednakost 3.10.2. (1) iz koje izlazi

$$a_{\cdot j}(A) = A^{-1} a_{\cdot j};$$

uvrstimo li taj izraz u (9) izlazi

(10) $$c_A^T A^{-1} a_{\cdot j} \geq c_j \quad (j = 1, 2, \ldots);$$

dakle je

(11) $$c_A^T A^{-1} a \geq c \quad \text{odnosno} \quad a^T (A^{-1})^T c_A \geq c.$$

Drugim riječima, stavimo li

(12) $$X = (A^{-1})^T c_A,$$

tada to X zadovoljava (4).

Dokažimo da je $X \geq 0$. Naime, ima li u (10) indeks j vrijednost koja odgovara dodatnoj varijabli y_{n+i}, tada je $c_{n+i} = 0$ pa (10) postaje

(13) $$c_A^T A^{-1} a_{\cdot n+\rho} \geq 0 \quad (\rho = 1, 2, \ldots r);$$

no $a_{\cdot n+\rho}$ je stupac sastavljen od nula i jedne jedinice na ρ-tom mjestu; zato iz (13) izlazi

$$c_A^T A^{-1} 1_r \geq 0$$

tj.

$$c_A^T A^{-1} \geq 0,$$

dakle (transponiraj!) također $X \geq 0$.

Dokažimo da je X i optimalno rješenje dualnog problema 4.2. Naime,

$$Z = b^T X = X^T b = c_A{}^T A^{-1} b = c_A{}^T X_A = \max z.$$

Prema tome, x_A, odnosno X su neodrečna rješenja programa 4.1, odnosno programa 4.2. i daju istu vrijednost z odnosno Z tim programima; prema teoremu 4.4. zaključujemo da su x_A, X zaista optimalna rješenja.

4.5.2. Dovoljni dio teorema: ako dualni problem

(1) $$a^T X \geq c, \quad X \geq 0, \quad \min Z = b^T X$$

ima optimalno rješenje, onda i ishodni linearni program dopušta optimalno rješenje. Naime, problem (1) možemo ekvivalentno izraziti kao „primarni" linearni program:

(2) $$(-a^T) X \leq -c, \; X \geq 0, \; \max z' = -b^T X, \; \min Z = -\max z'.$$

No, po pretpostavci taj „primarni" linearni program dopušta optimalno rješenje; zato po dokazanom prvom dijelu teorema dopušta optimalno rješenje i dual od (2).

A dual od (2) glasi

$$-ax \geq -b, \; x \geq 0, \; \min y = -c^T x$$

odnosno u ekvivalentnom obliku

(3) $$ax \leq b, \; x \geq 0, \; \max z = c^T x,$$

pri čemu je $\min y = -\max z$ (naime $\min t = -\max(-t)$).

No, (3) je upravo ishodni primarni linearni program.

Dokažimo još da vrijedi

(4) $$c^T \overset{\circ}{x} = b^T \overset{\circ}{X}.$$

Prema § 4.3. ispravno je u (4) znak $=$ čitati $\leq$. S druge strane, pođemo li od programa 4.5.2. (2), tada je ishodni program dual od 4.5.2. (2) pa primjena istog teorema 4.3. daje $b^T \overset{\circ}{X} \leq c^T \overset{\circ}{x}$. Dakle u (4) znak $=$ možemo zamijeniti i sa $\leq$ i sa $\geq$, a to znači da (4) stoji.

Može se dokazati i

$\longrightarrow$ **4.6. Teorem o postojanju.** ***Linearni program* 4.1. *odnosno program* 4.2. *dopušta optimalno rješenje onda i samo onda ako oba problema dopuštaju neodrečna rješenja.***

4.7. Teorem. ***Optimalno rješenje x primarnog linearnog programa* 4.1. *i optimalno rješenje X dualnog programa* 4.2. *zadovoljavaju***

$$(a^T X - c)_\nu = 0 \vee x_\nu = 0 \quad (\nu = 1, 2, \ldots, n) \; (\textit{znak } \vee \textit{ čitati »ili«});$$

specijalno

$$x_\nu > 0 \Rightarrow (a^T X)_\nu = c_\nu; \; \textit{isto tako } (a^T X)_\nu > c_\nu \Rightarrow x_\nu = 0.$$

Naime, iz $a^T X \geq c$, odnosno iz $X^T a \geq c^T$ skalarno množenje sa x daje

(1) $$X^T ax \geq c^T x. \quad \text{Slično} \quad X^T ax \leq b^T X.$$

No zbog optimalnosti je

$$c^T x = b^T X \text{ (isp. § 4.4.)}$$

što s (1) daje $X^T ax = c^T x$, odnosno $x^T a^T X = x^T c$, i dalje

$$x^T (a^T X - c) = 0 \quad \text{tj.} \quad \sum_{\nu=1}^{n} x_\nu (a^T X - c)_\nu = 0,$$

odnosno

(2) $$\sum_{\nu=1}^{n} x_\nu ((a^T X)_\nu - c_\nu) = 0,$$

odakle zbog

$$x_\nu \geq 0, \ (a^T X)_\nu - c_\nu \geq 0$$

izlazi da je svaki sumand u (2) jednak 0; iz te činjenice izlazi i tvrdnja u teoremu.

Znajući da je dual duala linearnog programa L sam program L i da je prema tome L dual svojeg duala možemo teorem 4.7. izreći i kao

—→ **4.8. Teorem. (I)** ***Svakoj bazičnoj nepoznanici x_ν optimalnog rješenja primarnog linearnog problema pridružena ν-ta relacija u dualnom problemu je jednadžba, tj. ν-ta dodatna ili oduzetna varijabla je $= 0$ (isp. § 2.2.2).***

(II). ***Ako u optimalnom bazičnom rješenju primarnog linearnog programa dolazi koja dodatna ili oduzetna varijabla, tada je odgovarajuća nepoznanica u optimalnom rješenju dualnog programa jednaka 0 (isp. § 2.2.2).***

4.9. Ekonomska interpretacija dualnosti. — 4.9.1. Tipični linearni program tipa I iz § 4.1. možemo interpretirati i ovako (isp. § 1.1): *Poduzeće (tvornica, grad, država, ...) raspolaže sa k vrsta sirovina, materije, u ograničenim količinama $b_1, b_2, \ldots, b_k$, i želi da iz njih proizvodi n vrsta robe $M_1, \ldots, M_n$, kojima je cijena po komadu $c_1, \ldots, c_n$.*

Kako treba sirovine kombinirati pa da novčani prinos (zarada) bude maksimalan?

Ako je x_ν broj komada, odnosno količina ν-tog proizvoda, onda je zarada upravo $\sum c_\nu x_\nu = c^T x$; $a_{i\nu}$ je količina i-te sirovine koja ulazi u svaku jedinicu ν-tog proizvoda; $c_\nu - z_\nu$ (isp. (10) u § 3.10.3) označuje uvećanje zarade pri proizvođenju jedne jedinice više ν-tog proizvoda usklađujući količine ostalih bazičnih proizvođenja tako da se dobije neodrečno rješenje.

4.9.2. Međutim, možemo zamisliti da *proizvodnju organiziramo i tako da se pitamo za* ***najmanje*** *troškove, tako da cijena proizvodnje bude minimalna!*

U toj »*dualnoj*« interpretaciji odgovara i-toj sirovini određena vrijednost cijena, X_i po jedinici i-te sirovine. Tada je

$$Z = b_1 X_1 + \cdots + b_k X_k$$

vrijednost ili cijena svih sirovina zajedno. Izraz

$$\sum_{i=1}^{k} a_{i\nu} X_i$$

je vrijednost sirovina potrebnih za proizvodnju svake jedinice ν-tog proizvoda; ta vrijednost je bar onolika kolika je zarada po komadu pri prodaji ν-tog proizvoda. Odatle i proizlazi uslov

$$\sum_{i=1}^{k} a_{i\nu} X_i \geq c_\nu .$$

4.9.3. Slično se i pri ostalim linearnim programima (npr. pri problemu prevoženja u § 1.2, određivanje radnog učinka u § 1.3, problem ishrane u § 1.4, razvoženje tereta u § 1.5, itd.) može od zadanog linearnog programa preći na interpretaciju njegova duala; formalno se radi ovako: *matrica a aktivnosti se transponira, svaka nejednadžba* $\leq$ *(odnosno* $\geq$*) prelazi u* $\geq$ *(odnosno* $\leq$*), vektor b i vektor c zamijene svoje uloge, maksimalizacija (problem maksimuma) i minimalizacija također zamijene svoje uloge.*

Na taj način vidimo kako ekonomska i industrijska razmatranja dovode do dualnog problema i kako ona mogu osvijetliti problem dualnosti.

4.10. Nelinearna programiranja. Dinamička programiranja. Linearni programi, u ekonomskoj interpretaciji, pretpostavljaju da je zarada proporcionalna količini prodanih proizvoda, da se cijena ne mijenja tokom nekog vremena, itd; međutim, u mnogim problemima takve pretpostavke nisu opravdane, pa će zato tada umjesto linearnih jednadžbi i funkcija dolaziti nelinearne jednadžbe i funkije koje će zavisiti i o vremenu. Tako se dolazi do *nelinearnih* kao i do *dinamičkih i ekonomskih programiranja.* Ta se pitanja danas mnogo obrađuju u matematičkoj ekonomici.

5. LINEARNO PROGRAMIRANJE I MATEMATIČKA TEORIJA IGARA

U posljednjih tridesetak godina razvila se još jedna matematička disciplina: *matematička teorija igara*; ona ima mnogobrojne primjene u ekonomskim naukama, u vojnim naukama, itd; u vrlo je uskoj vezi s teorijom programiranja i specijalno s linearnim programima.

Objasnimo stvar na slučaju tzv. *igre sa dva igrača (duel).*

5.1. Matrica plaćanja. Neka se igrači I i II takmiče na ovaj način: zadana je određena matrica $a=[a_{i\nu}]$ formata (k, n): $a_{i\nu}$ je realan broj za svako $i=1, 2, \ldots, k$ i svako $\nu=1, 2, \ldots, n$. Takmičenje ili igra između I i II sastoji se u ovome: pri svakom „potezu" (koraku) igrač I bira neki broj $i \in \{1, 2, \ldots, k\}$, a igrač II bira istodobno neki broj $\nu \in \{1, 2, \ldots, n\}$; time je pri svakom koraku određena uređena dvojka (i, ν) kao i broj-komponenta $a_{i\nu}$ matrice a; prema pravilima igre, na tom potezu igrač I dobije $a_{i\nu}$ d koje daje II; to znači: ako je $a_{i\nu} \leq 0$, tada na tom koraku igrač I gubi (plaća) $|a_{i\nu}|$ d koje dobije igrač II. Ako je $a_{i\nu}=0$, smatra se kao da potez nije učinjen pa se igra nastavlja.

Matrica a se zove matrica plaćanja odnosno matrica primanja igrača I, II; I bira retke a II bira stupce matrice a; biranje retka $a_{i\cdot}$ zove se *i-ta taktika ili i-ta čista strategija igrača* I; biranje broja ν, odnosno stupca $a_{\cdot\nu}$ zove se *ν-ta taktika ili ν-ta čista strategija igrača* II. *Nijedan igrač ne zna šta bira njegov suigrač ali zna da mu suigrač igra znalački i da želi igru dobiti.*

Kako treba igrati I *odnosno* II *pa da što više dobije ili bar da što manje izgubi?*

5.1.1. Primjer. Neka je $a=\begin{bmatrix}-1 & 2\\ 4 & -7\end{bmatrix}$ matrica plaćanja. I bi želio dobiti 4, no boji se da bira pripadni drugi redak jer bi igrač II mogao izabrati 2. stupac, pa bi time I izgubio 7 bodova. Zato I računa da je bolje igrati strategiju br. 1 (prvi redak) jer u najgorem slučaju gubi 1, ukoliko II igra najbolje tj. na strategiju (stupac) 1. Analogno, II zaključuje ovako: Želim dobiti 7 dakle ću igrati na strategiju br. 2. jer u najgorem slučaju mogu izgubiti 2; to je bolje nego da igram na 1. stupac jer u tom slučaju mogu izgubiti 4 „uloga".

5.2. Čista strategija (taktika) igrača I i igrača II.

5.2.1. Igrač I će u *svakom* retku $a_{i\cdot}$ tražiti *najmanji* član

$$\inf_{\nu=1,\ldots,n} a_{i\nu} \tag{1}$$

znajući da će primjenjujući i-tu strategiju dobiti bar (1) ako je $(1)>0$, odnosno izgubiti ne više od $|(1)|$ ako je broj u (1) negativan; zato je u interesu igrača I da svoj dobitak (1) učini što većim i da traži veličinu

$$\sup_i \inf_\nu a_{i\nu}. \tag{2}$$

Birajući redak u kojem je smješten broj (2) igrač I provodi *svoju optimalnu čistu strategiju.*

5.2.2. Igrač II će promatrati *supremum* članova svakog stupca $a_{\cdot\nu}$ dakle brojeve

$$\sup_i a_{i\nu} \tag{1'}$$

a onda promatrati infimum tih brojeva, tj.

$$\inf_\nu \sup_i a_{i\nu}. \tag{2'}$$

Stupac u kojem je taj infimum zove se *optimalna čista strategija igrača* II. Tako dolazimo do brojeva

$$\sup_i \inf_\nu a_{i\nu}, \quad \inf_\nu \sup_i a_{i\nu}. \tag{3}$$

5.2.3. Uvijek je

(4) $$\sup_i \inf_\nu a_{i\nu} \leq \inf_\nu \sup_i a_{i\nu}.$$

5.2.4. Međutim, može se desiti da bude

(5) $$\sup_i \inf_\nu a_{i\nu} = \inf_\nu \sup_i a_{i\nu} \; [= v = \text{„vrijednost igre"}].$$

5.2.5. Pretinac ili polje (k_0, n_0) matrice a u kojem leži v zove se prevojni ili sedlasti pretinac ili položaj ravnoteže.

5.2.6. Ako matrica a ima prevojni ili sedlasti pretinac (k_0, n_0), tj. ako vrijedi jednakost (5) te ako su brojevi u (5) jednaki $a_{k_0 n_0}$, onda je za igrače I, II najbolje da biraju svoje optimalne čiste strategije, tj. taj redak $a_{k_0 \cdot}$, odnosno stupac $a_{\cdot n_0}$.

5.2.7. Primjer. U igri kojoj je matrica

$$\begin{array}{rc|c} & & \inf\limits_\nu a_{i\nu} \\ & a = \begin{bmatrix} 2 & -4 & 3 \\ -3 & 1 & -1 \end{bmatrix} & \begin{array}{c} -4 \\ \boxed{-3} \end{array} \\ \sup\limits_i a_{i\nu} & \begin{array}{ccc} 2 & \boxed{1} & 3 \end{array} & \end{array}$$

nema optimalne čiste strategije jer uokvireni elementi nisu jednaki (pripisani stupac, odnosno redak, predstavlja brojeve (1), odnosno brojeve (1') za

$$i = 1, 2, \ldots, k \text{ odnosno za } \nu = 1, 2, \ldots, n.$$

Brojevi (3) su uokvireni.

5.2.8. Primjer

$$\begin{array}{c|c} \begin{bmatrix} -3 & -3 & 4 \\ 8 & \boxed{7} & 9 \end{bmatrix} & \begin{array}{c} -3 \\ \boxed{7} \end{array} \\ \begin{array}{ccc} 8 & \boxed{7} & 9 \end{array} & \end{array}$$

Optimalna strategija postoji — to je (2, 2), a vrijednost igre je $=7$.

5.3. Mješovita strategija. Ako igra ne dopušta optimalne čiste strategije, tada će se igrač I odlučiti s nekom vjerojatnosti $x_i \geq 0$ da igra na i-tu čistu strategiju (bira i-ti redak); dakle je

$$x_i \geq 0 \quad \text{te} \quad \sum_{i=1}^{k} x_i = 1.$$

Vektor $x = [x_1, \ldots, x_k]^T$ zove se *mješovita strategija igrača* I. Isto tako svaki neodrečni vektor $y = [y_1, \ldots, y_n]^T$ za koji je $y_1 + \cdots y_n = 1$ zove se *mješovita* *strategija igrača* II. Te će strategije imati uticaja na igru jer će svaki igrač z na osnovu njih birati pojedinu svoju čistu strategiju s određenom frekvencijom, ali tako da protivnik ne dokuči kako z bira redoslijed svojih čistih strategija ili taktikâ.

5.4. Optimalna mješovita strategija. Služi li se I mješovitom strategijom $[X_1, \ldots, X_k]^T$, tada on očekuje da će protiv ν-te čiste strategije igrača II dobiti bar iznos

$$a_{1\nu} X_1 + a_{2\nu} X_2 + \cdots + a_{k\nu} X_k. \tag{1}$$

To znači da se I nada da će u igri dobiti bar svotu

$$v' = \inf_{\nu=1,\ldots n} \sum_{i=1}^{k} a_{i\nu} X_i \tag{2}$$

računajući pri tom na svih n taktika igrača II. Igrač I će nastojati da traži takvu strategiju X kojom će njegova iščekivanja (2) biti maksimalna; neka je

$$v_1 = \sup_X v' = \sup_X \inf_{\nu=1,\ldots n} \sum_{i=1}^{k} a_{i\nu} X_i. \tag{3}$$

5.4.1. Broj v_1 zove se *vrijednost igre u odnosu na igrača* I. Svaka strategija X tj. svaki niz brojeva

$$X_1, X_2, \ldots, X_k \quad \text{za koji je } X_1 + X_2 + \cdots + X_k = 1, \tag{4}$$

$$X_i \geq 0 \quad (i = 1, 2, \ldots, k)$$

i pri kojem v' poprima vrijednost v_1 zove se *optimalna mješovita strategija* igrača I.

Ako je $v_1 = 0$, kaže se da je igra *pravedna, ravnopravna* ili *fair.*[1]

5.4.2. Veze s linearnim programiranjem. Na taj način (isp. (2)) imamo

$$\sum_{i=1}^{k} a_{i\nu} X_i \geq v', \quad X_i \geq 0, \quad \sum_{i=1}^{k} X_i = 1. \tag{5}$$

U zavisnosti od matricâ a, X može $v' = v'(a, X)$ biti <0, 0 ili >0.

5.4.2.1. *Slučaj* $v' > 0$. Podijelimo li relacije (5) sa v' i stavljajući

$$\frac{X_i}{v'} = y_i \quad \text{izlazi}$$

$$\sum_{i=1}^{k} a_{i\nu} y_i \geq 1, \quad y_i \geq 0, \tag{6}$$

$$\sum_{i=1}^{k} y_i = \frac{1}{v'}. \tag{7}$$

[1] Engleski *fair play* (lijepa, časna igra).

Ove relacije imaju oblik linearnog programa pri kojem se traži neodrečni vektor y za koji će vrijediti (6) i koji funkciju (7) čini minimalnom. *Dakle je problem igre sveden na problem linearnog programiranja.*

5.4.2.2. *Slučaj* $v' \leq 0$. Ako umjesto matrice a promatramo matricu $a+\lambda=a'$ za neki pozitivan broj λ za koji je $a_{i\nu}+\lambda>0$ za svako i, ν, tada je pripadni broj $v'(a')>0$ pa se problem igre s matricom a' obrađuje kao u 5.4.2.1.

No, neposredno se vidi da je

$$v'(a+\lambda)=v'(a)+v'(\lambda) \quad \text{i da je} \quad v'(\lambda)=\lambda.$$

Isto tako je

$$v_1(a+\lambda)=v_1(a)+\lambda;$$

nadalje su vrijednosti igara koje odgovaraju matricama a, $a+\lambda$ poprimljene pri *istoj optimalnoj strategiji igrača* I. Prema tome je određena optimalna strategija $\overset{\circ}{X}$ igre a; određena je i vrijednost $v_1(a)$ ishodne igre i to po obrascu

$$v_1(a)=v_1(a+\lambda)-\lambda.$$

5.5. Optimalna mješovita strategija igrača II. Služi li se II mješovitom strategijom $x=[x_1, \ldots, x_n]^T$, tada on strahuje da će suočen s i-tom taktikom od I izgubiti bar svotu $a_{i1}x_1+\cdots+a_{in}x_n$; kako je $i=1, 2, \ldots, k$, znači to da uz strategiju x najveći gubitak koji igrača II može zadesiti iznosi

$$v''=\sup_{i=1,2,\ldots,k}\sum_{\nu=1}^{n} a_{i\nu}x_\nu. \tag{1}$$

5.5.1. Prirodno je da II strategiju x podesi tako da taj *maksimalni* teoretski gubitak učini *minimalnim* i da on bude

$$v_2=\inf_x v''(x)=\inf_x \sup_{i=1,\ldots,k}\sum_{\nu=1}^{n} a_{i\nu}x_\nu; \tag{2}$$

v_2 zavisi od a i zove se *vrijednost igre* a o kojoj je riječ, *i to u odnosu na* II; svaka mješovita strategija $\overset{\circ}{x}$ za koju je $v''(\overset{\circ}{x})=v_2$ zove se *optimalna mješovita strategija igrača* II.

5.5.2. Kao i u slučaju igrača I tako se i sada određivanje od $\overset{\circ}{x}$ svodi na slučaj kada je $v''>0$; no u ovom slučaju razmatranja poput onih u § 5.4. dovode do redukcije problema igre na ovaj linearni program:

Odrediti neodrečni vektor $x'=[x_1', \ldots, x_n']^T$ *za koji je*

$$\sum a_{i\nu}x_\nu' \leq 1 \quad (i=1, 2, \ldots, k)$$

i za koju je funkcija $\frac{1}{v''}=\sum_{\nu=1}^{n} x_\nu'$ *maksimalna.*

5.6. Primjer (*igra glava-pismo*). Igra se prema matrici

$$a=\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

ili simbolično

	G	P
G	1	−1
P	−1	1

Takmičari I, II bacaju nasumce istodobno po jedan primjerak jednakog novčića; pokažu li oba novčića jednake (nejednake) strane, dobiva I (odnosno II).

Kolika je vrijednost v_1 igre i kolika je optimalna strategija igrača I?

Igra nema položaja ravnoteže jer je infimum (supremum) svakog retka (stupca) jednak -1 (odnosno 1). Pri strategiji $X=[X_1, X_2]^T$ igrač I očekuje dobitak bar svote:

$$1\,X_1+(-1)\,X_2 \quad \text{tj.} \quad (\text{zbog } X_1+X_2=1) \text{ svote } 2\,X_1-1$$

pri taktici br. 1 igrača II, odnosno

$$-1\,X_1+1\,X_2 \quad \text{tj.} \quad -2\,X_1+1$$

pri taktici br. 2 igrača II; pri tom je $0 \leq X_1 \leq 1$.

To znači da će I dobiti na osnovu svoje strategije bar svotu

$$\inf\{2\,X_1-1,\ -2\,X_1+1\}. \tag{1}$$

No ta će svota biti maksimalna upravo za $X_1=1/2$, tj. za strategiju $X=[1/2,\ 1/2]$.

Prema tome, vrijednost igre u odnosu na I glasi

$$v_1=\sup(1)=\sup\{2\cdot 1/2-1,\ -2\cdot 1/2+1\}=0, \quad \text{tj.} \quad v_1=0.$$

Prema tome je igra ravnopravna.

Isto se tako dokazuje da je optimalna strategija igrača II jednaka $[1/2,\ 1/2]^T$ i da je $v_2=0$.

5.7. Oko osnovnog teorema teorije dvoboja. U § 5.4. i § 5.5. vidjeli smo kako se takmičenje između I, II koje je određeno matricom a svodi na dva linearna programa koji su međusobno dualni. No, prema osnovnom teoremu 4.5. vrijednost linearnog programa i vrijednost njegova duala su međusobno jednake. To specijalno za linearne programe iz § 5.4. i § 5.5. znači da je

$$\frac{1}{v_1}=\frac{1}{v_2} \quad \text{dakle} \quad v_1=v_2;$$

zaključak je ispravan bar za slučaj $v_1>0$, $v_2>0$, a kao što smo vidjeli, na taj slučaj se svodi opći slučaj kad i nije $v_1>0$. Na taj način, osnovni teorem o dualitetu iz § 4.5. ima za posljedicu

—→ **5.8. Osnovni teorem o dvotakmičenju (J. von. Neumann 1928)**[1]. *Neka je a realna matrica konačnog formata (k, n); kad X prolazi skupom svih strategija*

$$(X_1, X_2, \ldots, X_k)^T, \; (\textit{dakle je } X_1 \geq 0, \ldots, X_k \geq 0, \; X_1 + \cdots + X_k = 1)$$

igrača I, *a x skupom svih strategija*

$$(x_1, x_2, \ldots, x_n)^T \; (\textit{dakle je } x_\nu \geq 0, \; x_1 + \cdots + x_n = 1)$$

igrača II, *tada je vrijednost igre*

$$v_1 = \sup_X \inf_\nu \sum_{i=1}^{k} a_{i\nu} X_i$$

u odnosu na igrača I *jednaka vrijednosti igre*

$$v_2 = \inf_x \sup_{i=1\cdots k} \sum_{\nu=1}^{n} a_{i\nu} x_\nu$$

u odnosu na igrača II; *postoji »optimalna strategija«* $\overset{\circ}{X}$ *od I i optimalna strategija* $\overset{\circ}{x}$ *igrača* II *tako da bude*

$$v_1 \equiv \inf_{\nu=1\cdots n} \sum_{i=1}^{k} a_{i\nu} \overset{\circ}{X}_i = \sup_{i=1\cdots k} \sum_{\nu=1}^{n} a_{i\nu} \overset{\circ}{x}_\nu \equiv v_2.$$

Teorem je otkriven 1928. dakle desetak godina prije no što se počela izrađivati nauka o linearnom programiranju. Ima više direktnih dokaza Neumannova teorema (isp. Vajda [1], str. 26—35).

5.9. Pojam rješenja zadane igre. Vidjeli smo kako je *matrica* usko vezana sa *dvotakmičenjem*; zato se umjesto o *matrici a* može govoriti o pripadnom *takmičenju ili o pripadnoj igri a.* U vezi s gornjim razmatranjima o strategiji igrača I i igrača II u igri *a* postavlja se

5.9.1. Definicija rješenja zadane igre *a.* Neka je *a* zadana realna matrica konačna formata (k, n); pod *rješenjem igre a* razumijeva se svaka uređena dvojka (X, x) optimalne mješovite strategije X igrača I i optimalne mješovite strategije x igrača II. Drugim riječima, rješenje igre *a* je svaka uređena dvojka (X, x) neodrečnog realnog niza $X = (X_1, \ldots, X_k)$ i neodrečnog realnog niza $x = (x_1, \ldots, x_n)$ sa svojstvom

$$X_1 + \cdots + X_k = 1, \; x_1 + \cdots + x_n = 1$$

za koje je

$$v_1 = \inf_{\nu=1,\ldots,n} \sum_{i=1}^{k} a_{i\nu} X_i, \quad v_2 = \sup_{i=1,\ldots,k} \sum_{\nu=1}^{n} a_{i\nu} x_\nu.$$

Na osnovu teorema 5.8. dobiva se

[1] J. von Neumann: Zur Theorie der Gesellschaftsspiele, Math. Annalen 100 (1928) 295—320.

J. von Neumann (Nojman) (28.12. 1903—08.02. 1957) je vrlo veliki mađarsko-američki matematičar.

—→ **5.9.2. Teorem (kriterij o rješenju igre).** *Uređena dvojka neodrečnih nizova*

$$X=(X_1, X_2, \ldots, X_k), \quad x=(x_1, \ldots, x_n)$$

stvarnih brojeva X_i, x_ν *za koje je*

$$\sum_{i=1}^{k} X_i=1, \quad \sum_{\nu=1}^{n} x_\nu=1$$

predstavlja jedno rješenje realne igre a formata (k, n) *onda i samo onda ako vrijedi*

$$\inf_{\nu=1,\ldots,n} \sum_{i=1}^{k} a_{i\nu} X_i = \sup_{i=1,\ldots,k} \sum_{\nu=1}^{n} a_{i\nu} x_\nu;$$

svaka takva igra dopušta bar jedno rješenje.

6. Zadaci o linearnom programiranju.

1. Naći bar jedno neodrečno rješenje jednadžbi

$$\begin{aligned} 2x-3y+4z&=16 \\ 5x+4y-z&=8. \end{aligned}$$

2. Naći najveću vrijednost funkcije $z=3x+5y$ uz uslove

$$0\leq x\leq 4, \quad 0\leq y\leq 5.$$

3. 1) Naći najveću vrijednost funkcije $z=x+y$, ako brojevi x, y zadovoljavaju uslovima $x\geq 0$, $y\geq 0$, $2x+y\leq 3$, $x-2y\leq 1$;

   2) naći najmanju vrijednost funkcije $z=3x+y$ pri čemu je $x\geq 0$, $y\geq 0$, $2x+y\geq 1$, $x-2y\geq 1$.

4. Naći $\max z=5x_1-4x_2$ uz uslove $x_1\geq 0$, $x_2\geq 0$, $x_2-5x_1\geq -10$, $2x+5y\leq 31$, $y-5x\leq 3$.

5. Izraziti zadatak 4. u matričnom obliku i naći dualni linearni program.

6. Naći sva 1) bazična, 2) bazična neodrečna rješenja jednadžbi u zad. 1.

7. Naći skup svih bazičnih neodrečnih rješenja jednadžbi

$$\begin{aligned} 2x_1+3x_2+4x_3+5x_4&=6 \\ 3x_1+4x_2+5x_3+6x_4&=8. \end{aligned}$$

8. Zadane su tačke $A=(1, 0)$, $B=(2, 3)$, $C=(0, 4)$, $D=\left(\frac{1}{2}, \frac{1}{2}\right)$;

   1) odrediti najmanji konveksni skup K u kojemu leže tačke A, B, C, D. 2) Leži li u K tačka 1) $E=(3/2, 2)$, $F=(3/2, 3)$? 3) Postoje li neodrečni brojevi x_1, x_2, x_3, x_4 tako da bude $x_1A+x_2B+x_3C+x_4D=F$?

9. Dakazati: ako postoji neodrečni vektor x za koji je $ax=b$, tada postoji i bazično neodrečno rješenje. Dokaži da je taj iskaz ekvivalentan s ovim: ako je skup svih neodrečnih rješenja neprazan, onda on ima određen vrh.

10. Simpleksnom metodom riješiti linearni program

$$8x_1+3x_2+4x_3+x_4\le 7$$
$$2x_1+6x_2+x_3+5x_4\le 3$$
$$x_1+4x_2+5x_3+2x_4\le 8$$
$$x_v\ge 0$$
$$\max z=3x_1+4x_2+x_3+7x_4.$$

Kako glasi dualan program?

11. Naći dualan program linearnog programa

$$2x_1+3x_2+4x_3\le 5$$
$$5x_1-2x_2+x_3\le 0$$
$$x_i\ge 0$$
$$\max z=3x_1+4x_2.$$

12. Zadatak 4 riješiti služeći se dualnim programom.
13. Navesti jedan linearan program sa svojstvom da ni on ni njegov dual nemaju rješenja.
14. Poduzeće proizvodi dva tipa M_1, M_2 neke robe i to pomoću 3 stroja S_1, S_2, S_3; broj časova potrebnih za proizvodnju te robe na strojevima S_1, S_2, S_3 očitava se iz tablice

	S_1	S_2	S_3
M_1	1	2	0,5
M_2	2	1/4	1

Ako strojevi sedmično rade ne više od 42^h, pa ako je zarada po komadu robe M_1, odnosno M_2 jednako 2 000 d, odnosno 3 000 d, koliko treba sedmično proizvoditi robe M_1, a koliko robe M_2 pa da zarada bude maksimalna? (isp. § 1.1).

15. Poduzeće ima na skladištu S_1 30 tona i na skladištu S_2 18 tona robe; roba se treba prevesti u odredišta O_1, O_2, O_3, O_4 i to 10, 8, 16, 14 tona; neka je cijena prevoza data matricom

	O_1	O_2	O_3	O_4	
S_1	4	3	15	8	30
S_2	6	5	1	6	18
	10	8	16	14	

Kako treba izvršiti prevoz uz uslov da troškovi budu minimalni?

16. Kako bi glasile linearne relacije i linearna funkcija za prevozni problem dat ovom tablicom:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	
1		13				12			8						33
2							11							7	18
3	2														2
4	11		20						7						38
5	1			7							6				14
6										9	14				23
7			1					30							31
8	1				18							8	11		38
9	3														3
	18	13	21	7	18	12	11	30	15	9	20	8	11	7	

Uvjeriti se da je rješenje dato tablicom optimalno.
Zadatak je bio rješavan na matematičkom stroju Strijela, i to u vremenu od 1^m (isp. Barsov, str. 89).

17. Kako glasi problem ishrane (isp. § 1.4) za koji je

$$a=\begin{bmatrix}3 & 2\\ 1 & 4\\ 5 & 1\end{bmatrix},\quad b=\begin{bmatrix}4\\ 2\\ 6\end{bmatrix},\quad c=\begin{bmatrix}1\\ 2\\ 3\end{bmatrix}?$$

18. Objasniti značenje dvotakmičenja koje je definirano matricom:

$$1)\ \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix};\quad 2)\ \begin{bmatrix}1/2 & 0\\ 0 & 0\end{bmatrix};\quad 3)\ \begin{bmatrix}1 & 2 & 4\\ 4 & 2 & 1\end{bmatrix};\quad 4)\ \begin{bmatrix}2 & 3 & -3\\ 4 & -5 & 1\end{bmatrix};$$

$$6)\ \begin{bmatrix}-3 & 4 & 3\\ 0 & 3 & 0\\ 3 & -1 & 1\end{bmatrix};\quad 6)\ \begin{bmatrix}2 & 3 & 4 & -5\\ 3 & -4 & 5 & 2\\ -4 & 5 & 2 & 3\end{bmatrix};\quad 7)\ \begin{bmatrix}0 & 2 & -3 & 0\\ -2 & 0 & 0 & 3\\ 3 & 0 & 0 & -4\\ 0 & -3 & 4 & 4\end{bmatrix}.$$

Postoji li element ravnoteže?

19. Ako osobe I, II igraju prema matrici plaćanja $a=\begin{bmatrix}4 & -2\\ -5 & 3\end{bmatrix}$, objasniti što to znači; naći vrijednost igre u odnosu na I, odnosno u odnosu na II kao i optimalne mješovite strategije tih igrača.

20. (*Igra s 2 prsta*). I igrač I i igrač II ispruže i lijevom i desnom rukom 1 ili 2 prsta, pri čemu broj ispruženih prstiju na lijevoj ruci treba da znači da je suigrač toliko prstiju ispružio na svojoj desnoj ruci. Ako oba

igrača pogode ili ako nijedan ne pogodi, potez je neriješen: 0; ako pogodi samo jedan od njih, onda onaj koji nije pogodio plaća onoliko jedinica koliko su prstiju oba igrača ispružila na desnoj ruci. 1) Kako izgleda platežna matrica? 3) Postoji li element ravnoteže? 3) Odrediti vrijednost igre u odnosu na I, odnosno u odnosu na II. 4) Odrediti optimalnu strategiju od I, odnosno od II.

21. Ako u dvotakmičenju između igrača I i II koje je određeno matricom a formata $k \times n$ igrači I, II igraju potez strategijom X odnosno strategijom x, treba dokazati da broj $Xax = \sum_{\substack{i=1,\ldots,k \\ \nu=1,\ldots,n}} X_i a_{i\nu} x_\nu$ predstavlja svotu za koju se igrač I nada će je dobiti pri tom potezu.

22. Kako glasi linearni program koji odgovara igraču I, odnosno igraču II u igri koja je definirana matricom plaćanja a iz zad. 18?

23. Naći rješenje igre iz zadatka 18. Posebno, dokazati da igra

$$\begin{bmatrix} 1 & 2 & 4 \\ 4 & 2 & 1 \end{bmatrix}$$

dopušta ova rješenja:

$$\left[\frac{1}{3}t+\frac{2}{3}(1-t),\ \frac{2}{3}t+\frac{1}{3}(1-t)\right]^T,\ [0,\ 1,\ 0]$$

za svaki broj $0 \leq t \leq 1$.

Literatura

Barsov [1], Hadley [1]; Karlin [1]; Vajda [1], [2].

POGLAVLJE 31.

NUMERIČKO ILI PRIBLIŽNO RJEŠAVANJE JEDNADŽBI I NEJEDNADŽBI

Jedna od najvažnijih primjena matematike sastoji se u tom da se zadane relacije (jednadžbe, nejednadžbe, itd.) riješe *numerički*, tj. *na određen broj decimalnih mjesta*. S *teorijskog* gledišta je važno znati naći *skup svih rješenja*, posebno vidjeti da li je taj skup možda prazan, no s *praktičkog gledišta* i s *gledišta veza matematike s drugim* oblastima mnogo je važnije naći *približno* rješenje, čak i onda kad potpuno tačno rješenje ni ne postoji. U današnje doba kad su nam na usluzi brzometni računski strojevi ta *numerička problematika matematike* postala je od goleme važnosti i na bitan način se splela s onim naučno-tehničkim istraživanjima i primjenama koje na najefikasniji način vode čovječanstvo u nove i nepoznate oblasti. Govori se o *kvalitativnom rješavanju* pri čemu se strojem iznalaze *komparativne* (*uporedne*) *jednačine*.

Jedna od osnovnih crta numeričkog približnog rješavanja problema sastoji se u postupnom približavanju ka željenom cilju; to približavanje se odražava u povećavanju broja decimalnih poznatih mjesta, odnosno broja elemenata traženog skupa. Posebno, metoda iteracije je od velike važnosti.

0. PRIPREMNI KORAK: SEPARACIJA NULIŠTA

0.1. *Separirati* (*odvojiti*) nulišta funkcije fx znači odrediti oblasti (intervale) sa po jednim jedinim nulištem funkcije f i da razdaljina svakog para tačaka u svakoj oblasti bude $<d$, gdje je d zadan pozitivni broj (npr. $d=1$). Ako se radi o *realnim* nulištima x funkcije f onda se za zadano $d<1$ separiranjem svih nulišta odredi bar najveće cijelo, Ex, svakog nulišta x.

0.2. Separiranje *realnih* nulišta realna polinoma $a(x)$ vrši se pomoću Sturmova teorema (isp. pogl. 29. § 5.4). Pri tom brojevi l_a, L_a (isp. pogl. 29 § 1.2) mogu biti od koristi, jer su sva pozitivna realna nulišta polinoma $a(x)$ smještena u zatvorenom intervalu $[l_a, L_a]$; podijelimo li taj interval na dva dijela, može se dalje odrediti koliko nulišta ima u prvom a koliko u drugom dijelu; daljom subdivizijom intervala može se doći do manjih intervala duljine <1 s nikojim ili s po jednim jedinim nulištem, i da je time obuhvaćeno svako eventualno pozitivno nulište. Daljim dijeljenjem dobivenih intervala mogu se nulišta još bolje odrediti i to na onoliko decimalnih mjesta koliko pojedina situacija traži (isp. pogl. 31 § 3. o Ruffini-Hornerovoj metodi).

0.3. Dobro je prethodno dati bar približnu sliku (grafikon) funkcije $y=fx$ da se po prilici vidi gdje krivulja $y=fx$ presijeca apscisnu os, tj. da se bar približno vidi kolika su rješenja jednadžbe $fx=0$.

Tako nagoviještena rješenja određuju se dalje na željen broj decimalnih mjesta; pri tom se služimo raznim postupcima koje ćemo opisati u ovom poglavlju.

0.4. Kako pri rješavanju jednadžbe $fx=0$ nađeno približno rješenje treba provjeriti, dobro je znati pojedine postupke kako se za zadano x_0 vrijednost fx_0 nađe brzo i pregledno. U tom pogledu Ruffini-Hornerov postupak sintetičke divizije (pogl. 21, § 2.4.4) vrlo je pogodan ukoliko je x_0 realan broj, a fx_0 cijela racionalna funkcija.

0.5. *Ruffini-Hornerov postupak u kompleksnom području* (isp. pogl. 21, § 2.4).

Riječ je o polinomu $a(x)=a_0+a_1x+\cdots+a_nx^n$ i o (približnoj) vrijednosti $x_0=u+iv$; ako su koeficijenti a_ν realni, tada je prema Collatzu (Zeitschrift für angewandte Math. (20/1940) 235—236) zgodno polinom $a(x)$ podijeliti sa $(x-x_0)(x-\bar{x}_0)=x^2-2ux+u^2+v^2=x^2-2px-q$, gdje je $2p=2u$, $q=-u^2-v^2$, naći kvocijent $b(x)$ i ostatak $r(x)$; ostatak $r(x)$ je 0 ili dvočlan oblika $a_1'x+a'_0$; vrijedi $a(x_0)=\text{ostatak}=r(x_0)=a'_1x_0+a'_0$.

Označimo kvocijent $b(x)$ sa $a'_2+a'_3x+\cdots+a'_nx^{n-2}$; tada imamo identitet

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=(a'_nx^{n-2}+a'_{n-1}x^{n-3}+\cdots+$$
$$+a'_3x+a'_2)(x^2-2px-q)+(a'_1x+a'_0).$$

Izmnažanjem na desnoj strani i izjednačavanjem koeficijenata na lijevoj i desnoj strani dobiva se:

$$a_n=a'_n,\ a_{n-1}+2pa'_n=a'_{n-1},\ a_{n-2}+qa_n+2pa'_{n-1}=$$
$$=a'_{n-2},\ldots,\ a_1+qa'_3+2pa'_2=a'_1,\ a_0+qa'_2=a'_0;$$

odnosno u obliku sheme:

	a_n	a_{n-1}	a_{n-2}	a_{n-3}	$\cdots$	$a_\nu\cdot\cdots$	a_2	a_1	a_0
+			qa_n	qa'_{n-1}	$\cdots$	$qa'_{\nu+2}\cdot$	qa_4'	qa'_3	qa'_2
		$2pa_n$	$2pa'_{n-1}$	$2pa'_{n-2}$	$\cdots$	$2pa'_{\nu+1}\cdot$	$2pa_3'$	$2pa'_2$	
	a_n	a'_{n-1}	a'_{n-2}	a'_{n-3}	$\cdots$	a_ν',	a'_2	a'_1	a'_0
			koeficijenti kvocijenta					koeficijenti ostatka	

Dakle je $a(x_0)=a'_1x_0+a'_0$, pa se tako i nalazi vrijednost $a(x_0)$.

1. METODA ITERACIJE ILI PONAVLJANJA

Metoda se sastoji u tom da se rješavanje započne i onda nastavi na osnovu dobivenih djelomičnih rezultata i onda provjeri kolika je eventualna greška.

1.1. Primjer. Naći bar jedno rješenje jednadžbe

(1) $$f(x) \equiv x^8 - 15x^5 + 24x - 5 = 0.$$

Kako je $f(0) = -5 < 0$, $f(1) = 5 > 0$, znači da postoji bar jedno rješenje između 0 i 1; pokušat ćemo ga naći najprostijom metodom: napisati

$$x = \frac{1}{24}(5 + 15x^5 - x^8) = \varphi(x),$$

započeti s nekom početnom vrijednosti $x = x_0$ i računati po propisu:

$$\begin{aligned} x_1 &= \varphi(x_0) \\ x_2 &= \varphi(x_1) \\ &\cdots\cdots \\ x_{n+1} &= \varphi(x_n) \\ &\cdots\cdots \end{aligned}$$

i pogledati da li taj proces vodi bar približno do cilja.

Uzmimo neki broj x_0 između 0 i 1 npr. $x_0 = 0{,}3$. Tada imamo

(2) $$x_1 = \frac{1}{24}(5 + 15 \cdot 0{,}3^5 - 0{,}3^8)$$

$$15 \cdot 0{,}3^5 = 0{,}03645$$

$$0{,}3^8 \doteq 0 \text{ (zanemarujemo).}$$

Tako je

(3) $$x_1 = \frac{1}{24} \cdot 5{,}03645 \doteq 0{,}2099 \doteq 0{,}21.$$ Izračunavamo

$$x_2 = \varphi(x_1) = \frac{1}{24}(5 + 15 \cdot 0{,}21^5 - 0{,}21^8)$$

$$\log 15 \cdot 0{,}21^5 = 1{,}17609 + 5 \cdot (0{,}32222 - 1) =$$
$$= 1{,}17609 + (1{,}61110 - 5) = 0{,}78719 - 3$$

$15 \cdot 0{,}21^5 \doteq 0{,}006126.$ Slično

$0{,}21^8 \doteq 0{,}000004.$ Zato je

$$x_2 \doteq 0{,}2086$$

$$x_3 \doteq \varphi(x_2) \doteq 0{,}2086$$

$$x_4 \doteq \varphi(x_3) \doteq 0{,}2086.$$

Prema tome, i dalje su vrijednosti

$$=x_4=x_5=x_6=\cdots$$

pa se na osnovu upotrebljenih tablica rezultat ne može popraviti.

Nađimo $f(x_3)$, tj. $f(0{,}2086)=0{,}2086^8-15\cdot 0{,}2086^5+24\cdot 0{,}2086-5$.

$$\log 0{,}2086^8=8\,(0{,}31931-1)=0{,}55448-6$$

$$0{,}2086^8\doteq 0{,}0000036$$

$$15\cdot 0{,}2086^5\doteq 0{,}005924$$

$$24\,x=5{,}0064.$$

$$f(x_3)\doteq 0{,}00048.$$

Kad bi x_3 bilo tačno nulište polinoma f, bilo bi $f(x_3)=0$, a stvarno je $f(x_3)\doteq 0{,}00048$; dakle se dobije 0,00048 umjesto 0; to znači da traženo nulište i nađeni broj x_3 daju na 3 decimalna mjesta zajedničku vrijednost funkcije f. U mnogim primjenama takav rezultat posve zadovoljava.

Međutim, to još ne znači da je i x_3 dovoljno blizu traženom korijenu ξ. Međutim, brzo se provjeri da je $f(0{,}208)<0$, što s $f(0{,}2086)>0$ znači da je $0{,}208<\xi<0{,}2086$; to znači da je $\xi\doteq 0{,}208$ dobra približna vrijednost traženog rješenja.

1.2. O dovoljnim uslovima konvergencije pri iteriranju.

Riječ je o rješavanju jednadžbe oblika

(1) $$x=\varphi(x)$$

metodom iteracije: pođe se od nekog broja x_0, stavlja

(2) $$x_{n+1}=\varphi(x_n)\quad (n=0,\,1,\,2,\ldots)$$

i ispituje da li postoji

(3) $$\lim x_n=\xi$$

i da li je

(4) $$\xi=\varphi(\xi).$$

Ako je limes (3) određen broj te ako je funkcija φ neprekidna u ξ, tada naravno (4) stoji.

1.2.1. *Lipschitzov uslov.*[1] Kaže se da realna funkcija f definirana u realnom skupu S zadovoljava Lipschitzovu uslovu s faktorom M ako iz $x', x''\in S$ izlazi

$$|fx'-fx''|\leq M\,|x'-x''|.$$

Posebno je od interesa slučaj $0<M<1$.

1.2.2. Teorem. Neka je I interval realnih brojeva, a φ realna funkcija iz I u I koja u I zadovoljava Lipschitzovu uslovu sa $0<M<1$, tj. postoji realan broj M tako da vrijedi $0<M<1$ i

(1) $$|\varphi(x')-\varphi(x'')|\leq M\,|x'-x''|$$

---

[1] Rudolf Lipschitz (1832—1903, njemački matematičar.

za bilo koje x', $x'' \in I$; tada za svako $x_0 \in I$ niz

(2) $$x_0,\ x_1 = \varphi x_0,\ x_2 = \varphi x_1, \ldots,\ x_{n+1} = \varphi(x_n), \ldots$$

konvergira i iz $\lim\limits_{n\to\infty} \varphi x_n = \xi$ izlazi $\xi = \varphi \xi$.

D o k a z. Treba dokazati da se gotovo svi članovi niza (2) nalaze u proizvoljno kratkim intervalima, tj. da je $|x_n - x_s|$ proizvoljno mala veličina čim su n, s vrlo veliki brojevi. No

$$|x_n - x_s| = |\varphi x_{n-1} - \varphi x_{s-1}| \leq M \cdot |x_{n-1} - x_{s-1}|, \text{ tj.}$$

$$|x_n - x_s| \leq M |x_{n-1} - x_{s-1}|.$$

Iz istog je razloga to dalje

$$\leq M \cdot M |x_{n-2} - x_{s-2}|, \text{ itd.}$$

(3) $$|x_n - x_s| \leq M^n |x_0 - x_{s-n}|$$

Kako je

$$|x_0 - x_{s-n}| \leq |x_0 - x_1| + |x_1 - x_2| + \cdots + |x_{s-n-1} - x_{s-n}| \leq |x_0 - x_1| +$$
$$+ M |x_0 - x_1| + M^2 |x_0 - x_1| + \cdots + M^{s-n-1} |x_0 - x_1| \leq$$
$$\leq |x_0 - x_1| (1 + M + M^2 + \cdots) = \frac{1}{1-M} |x_0 - x_1|,$$

to (3) daje

(4) $$|x_n - x_s| \leq \frac{M^n}{1-M} |x_0 - x_1|.$$

Kako je $\lim M^n = 0$ znači, prema (4), da zaista za svako $\varepsilon > 0$ postoji neki indeks n_0 tako da iz $n, s > n_0$ izlazi $|x_n - x_s| < \varepsilon$. Dakle je niz x_n Cauchyjev pa zato postoji $\xi = \lim\limits_{n\to\infty} x_n$.

Za element $\xi = \lim x_n$ imamo

$$|\varphi x_n - \varphi \xi| \leq M |x_n - \xi|, \text{ što zbog } |x_n - \xi| \to 0 \text{ znači da je}$$
$$\lim |\varphi x_n - \varphi \xi| = 0, \text{ tj. } |\xi - \varphi \xi| = 0, \text{ dakle je } \xi = \varphi \xi.$$

Dokažimo da je ξ jedinstveno i da ne zavisi od x_0. Ako umjesto x_0 uzmemo u I element $x_0' \neq x_0$, tada istim postupkom dolazimo do određena niza $x'_{n+1} = \varphi(x'_n)$, $(n = 0, 1, \ldots)$ i do elementa $\xi' = \lim x_n'$ za koji je $\xi' = \varphi \xi'$.

Pretpostavka

$$0 \neq |\xi' - \xi| = |\varphi \xi' - \varphi \xi|$$

u protivnosti je s relacijom

$$|\varphi \xi' - \varphi \xi| \leq M |\xi' - \xi| < |\xi' - \xi|.$$

Dakle je ξ jedina nepomična tačka funkcije φ.

$\longrightarrow$ **1.2.3. T e o r e m o kontrakciji ili stezanju i o nepomičnoj tački.**

Ako je E bilo koji metrički potpuni prostor, a φ bilo koje neprekidno stezanje (kontrakcija) prostora E u sama sebe, tada postoji jedan jedini član

ξ u prostoru E za koji je $\xi = \varphi\xi$. Taj nepomični element ξ je limes niza x_0, $x_1 = \varphi x_0, \ldots, x_{n+1} = \varphi x_n, \ldots$ pri čemu početni član x_0 može značiti proizvoljan element prostora E.

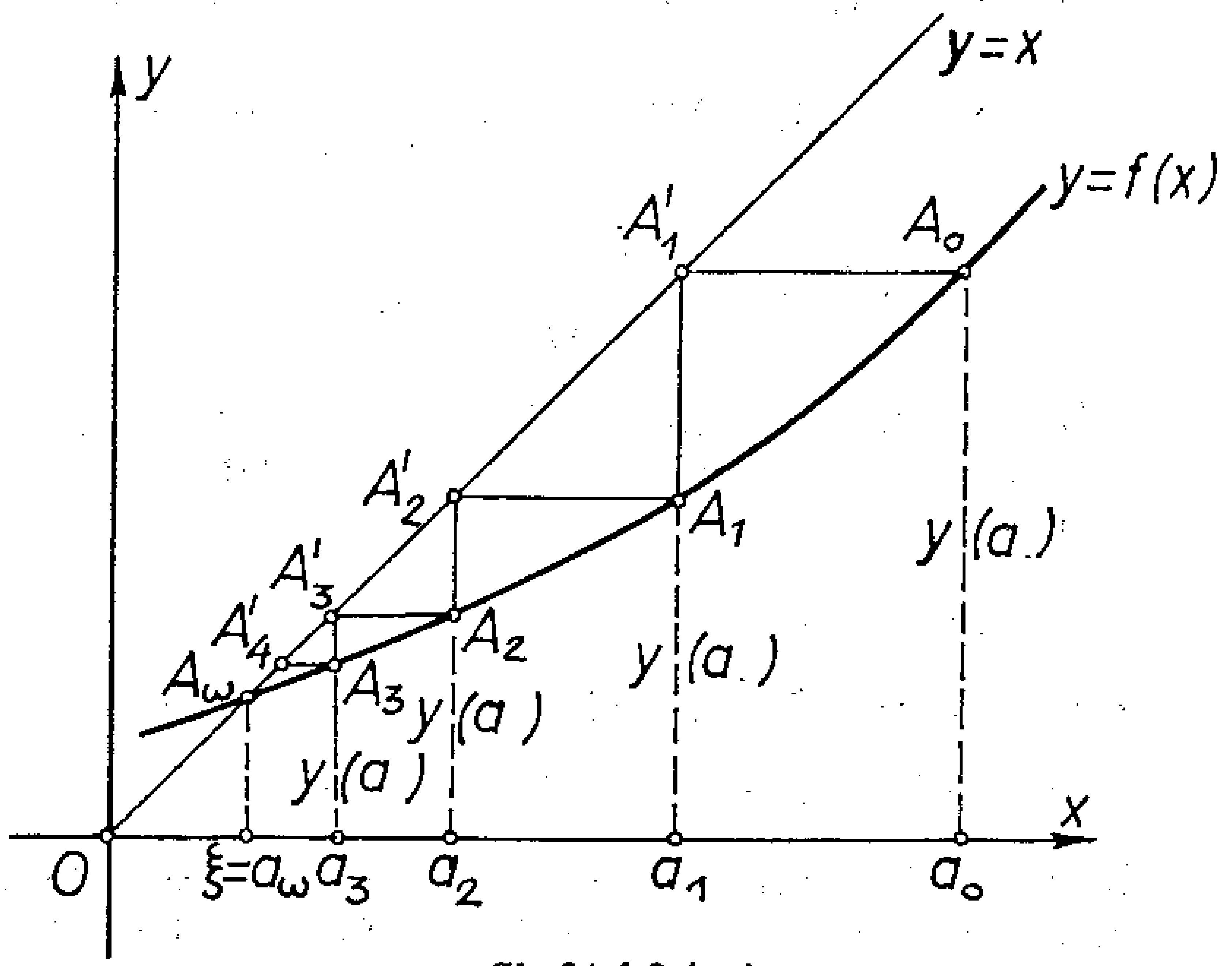
Specijalno, to vrijedi za svaki euklidski prostor (dakle i za skup kompleksnih brojeva) (o terminologiji v. npr. Đ. Kurepa [1] (§ 30).

Dokaz je potpuno sličan s dokazom teorema 1.2.2: dovoljno je umjesto $|x-y|$ u 1.2.2 pisati $\rho(x, y)$ = razdaljina elemenata $x, y \in E$. Pri tom vrijedi

1.2.3.1. *Definicija stezanja* (*kontrakcije*). Preslikavanje φ metričkog prostora E u sama sebe zove se *stezanje* (*kontrakcija*) ako postoji neki realni broj $0 < M < 1$ sa svojstvom $\rho(\varphi x, \varphi y) \leq M \rho(x, y)$ za svako $x, y \in E$.

U slučaju kad promatramo prostor R realnih brojeva ili koji njegov omeđeni zatvoreni interval I, tada je Lipschitzov uslov posljedica pojedinog vladanja izvedene funkcije φ'. Posebno imamo

⟶ **1.2.4. Teorem.** ***Ako je I zatvoren omeđen interval realnih brojeva, a φ neko preslikavanje od I u I sa svojstvom da derivat φ' postoji i da je*** **sup** $|\varphi'| = M < 1$, ***tada jednadžba $x = \varphi x$ ima jedno jedino rješenje $\xi \in I$, a dobije se kao limes iteracionog postupka; kao početni član se može uzeti bilo koji element*** $x_0 \in I$ (isp. sliku 31.1.2.4 *a*))[1].



Sl. 31.1.2.4. *a*)

Naime, za $x', x'' \in I$ imamo prema teoremu o srednjoj vrijednosti

$$\varphi(x') - \varphi(x'') = (x' - x'')\,\varphi(c) \text{ za neko } c \in R(x', x'').$$

Odatle prelazeći na apsolutne vrijednosti izlazi zaista

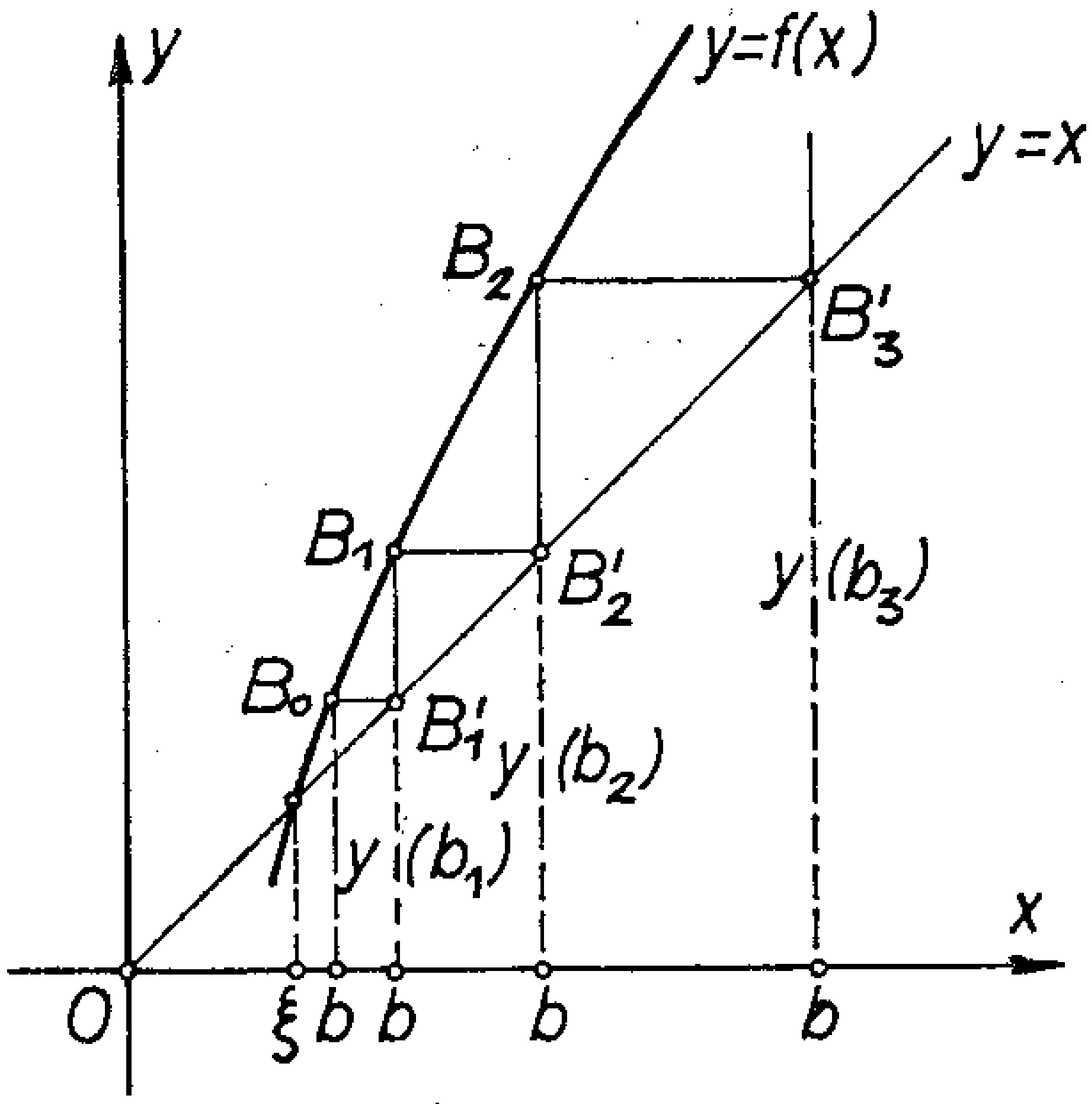
$$|\varphi x' - \varphi x''| \leq |x' - x''|\,M \text{ jer je } M \geq \varphi'(c).$$

Primjenom teorema 1.2.3. odnosno teorema 1.2.2. izlazi i sam iskaz 1.2.4.

---

[1] Izgleda da je naš primjenjeni matematičar Milanković Milutin (1879—1958) prvi, 1909. godine na primjeru geometrijskih redova, na geometrijski način, očigledno prikazao konvergenciju (v. Orlov Konstantin, *Geometriska teorija redova M. Milankovića*, Vesnik Društva mat. fiz., Beograd, IV_{1-2} (1952) 61—68).

Treba imati na umu da se radilo o *preslikavanju omeđena zatvorenog intervala I u sama sebe*, tj. da je $\varphi I \subset I$. Međutim, taj uslov možemo osigurati i na drugi način kao što se vidi iz teorema 1.2.5.



Sl. 31.1.2.4. *b*)

1.2.5. Teorem. ***Neka je $K=K(C, r)$ zatvorena kugla u potpunom razdaljinskom prostoru E sa središtem C i radijusom r. Ako je $x \to \varphi x$ neprekidno preslikavanje kugle K u prostor E koje zadovoljava Lipschitzovu uslovu sa $0<M<1$, pa ako je $\rho(\varphi C, C) \leq (1-M)r$, tada jednadžba $x=\varphi x$ ima jedno jedino rješenje ξ u K, a dobije se kao $\xi = \lim\limits_{n\to\infty} x_n$, gdje je $x_{n+1}=\varphi x_n$, s proizvoljnim elementom $x_0 \in K$.***

Dokažimo da je $\varphi K \subset K$ pa je time teorem 1.2.5. sveden na 1.2.3. No, neka je $x \in K$; tada je

(1) $$\rho(\varphi x, C) \leq \rho(\varphi x, \varphi C_1) + \rho(\varphi C, C).$$

Prvi sumand je $\leq M\rho(x, x_0)$, dakle $\leq Mr$; drugi sumand je po pretpostavci $\leq (1-M)r$. Zato (1) daje $\rho(\varphi x, C) \leq Mr + (1-M)r$, tj. $\rho(\varphi x, C) \leq r$, dakle zaista $\varphi x \in K$.

1.2.6. Prelaz na obratnu funkciju. Ako u okolini O ništišta ξ funkcije

$$x-\varphi x \text{ vrijedi } |\varphi'| \geq M > 1 \quad (\text{v. sl. } 31.1.2.4.\ b),$$

tada opisani proces iteriranja ne konvergira pa se ξ ne može dobiti kao limes veličina φx_n. Međutim promatramo li inverznu funkciju $\varphi^{-1}(x) = \psi(x)$ (geometrijski: zrcaljenje na simetrali prvog kvadranta!), tada je

$$|\psi'(x)| = \left|\frac{1}{\varphi'(x)}\right| \leq M^{-1} < 1,$$

pa se umjesto jednadžbe $x=\varphi x$ može promatrati jednadžba

(2) $$\varphi^{-1} x = x$$

jer pripadni iteracioni proces konvergira; jednadžbe (1), (2) imaju u okolini O jedno te isto rješenje ξ.

1.2.6.1. Primjer. $fx \equiv x^3 - x - 14{,}976 = 0$; odrediti bar jedno pozitivno rješenje ξ (ukoliko postoji).

Kako je $f(2)<0$, $f(3)>0$, postoji $\xi \in R(2, 3)$ za koje je $f\xi = 0$. Jednadžba $fx = 0$ je ekvivalentna sa jednadžbom

$$x = \varphi x, \quad \varphi x = x^3 - 14{,}976.$$

Međutim, $\varphi' x = 3x^2 \geq 12$; zato ćemo umjesto φx promatrati $\varphi^{-1} x$, odnosno zadanu jednadžbu ćemo pisati u obliku $x^3 = x + 14{,}976$, tj.

$$x = \psi x, \quad \psi x = (x + 14{,}976)^{1/3}.$$

Sada je $\psi' x = \frac{1}{3}(x + 14{,}976)^{-\frac{2}{3}} \leq \frac{1}{3}$ za $x \in R(2, 3)$ pa proces iteriranja konvergira. Poći ćemo od približne vrijednosti $x_0 = 3$ pa ćemo imati

$$x_{n+1} = (x_n + 14{,}976)^{\frac{1}{3}}, \text{ odnosno pripadnu tabelu}$$

n	0	1	2	3
x_n	3	2,615	2,607	2,6005

Sam korijen je $\xi = 2{,}6$.

1.2.7. Teoremi 1.2.2—1.2.5. jesu podloga pri dokazima konvergencije pojedinih iteracionih procesa; navedimo sada tri načina: *metoda sekante*, *metoda tangente i mješovita metoda*. Radit ćemo s funkcijama fx kojima su *i varijabla* x *i vrijednost* fx *realni*. Pretpostavit ćemo da f promatramo u nekom intervalu $R[a, b]$ sa svojstvima:

(i) $fa \cdot fb < 0$;

(ii) Postoje derivat f' i derivat f'' pa su $\operatorname{sgn} f'$, $\operatorname{sgn} f''$ konstante u $R[a, b]$; to geometrijski znači da je skup $\widehat{AB}\,\overline{BA}$ konveksan; pri tom je

$$A = (a, fa), \quad B = (b, fb);$$

(iii) $|b - a| \leq 1$.

Specijalno, radi li se o algebarskom polinomu f, tada se npr. na osnovu Sturmova teorema 5.4 iz poglavlja 29 uvijek može naći interval I realnih brojeva u kojem f ima jedno jedino ništište i da duljina od I bude <1.

U svakom slučaju će uz funkciju fx biti zgodno promatrati i funkciju

$$\varphi x = x - f(x)\,\lambda(x)$$

gdje je $\lambda(x)$ još neodređena funkcija, no koja se bira tako da iteracioni proces konvergira (pri metodi sekante je $\lambda(x) = \frac{x - b}{fx - fb}$; pri metodi tangente je $\lambda(x) = \frac{1}{f' x}$; geometrijsko značenje funkcije $\lambda(x)$ je tu očigledno!).

1.3. Metoda sekante (metoda tetive, metoda linearne interpolacije, regula falsi). — **1.3.1.** Ako je realna funkcija f definirana u zatvorenom segmentu $R[a, b]$, pa ako je $f(a)\cdot f(b)<0$, *tada se metoda sekante sastoji u tom da se odrezak* $\overline{AB}$ *smatra aproksimacijom luka* $\widehat{AB}$; *sjecište* x_1 *odreska* $\overline{AB}$ *i x-osi* smatra se približnom vrijednosti korijena $\xi\in R(a, b)$.

No, jednačina pravulje AB glasi

$$y-fb=\frac{f(b)-f(a)}{b-a}(x-b)$$

odakle za $y=0$ izlazi

$$(b_1=)\; x=b-\frac{b-a}{fb-fa}fb.$$

Stavimo li $b=b_0$, imamo

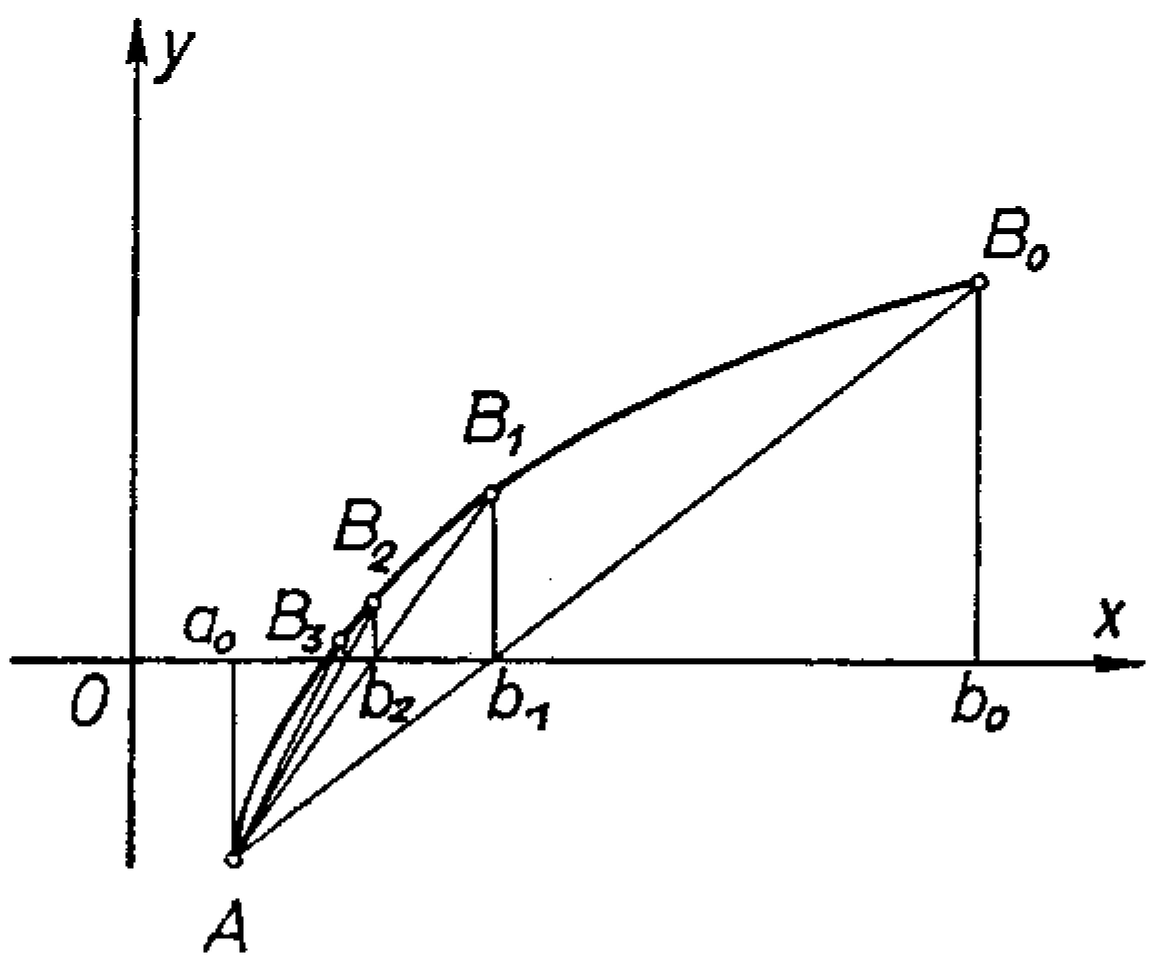
$$b_1 \;=b_0-\frac{b_0-a}{fb_0-fa}f(b_0).$$

Iteracijom se dobije

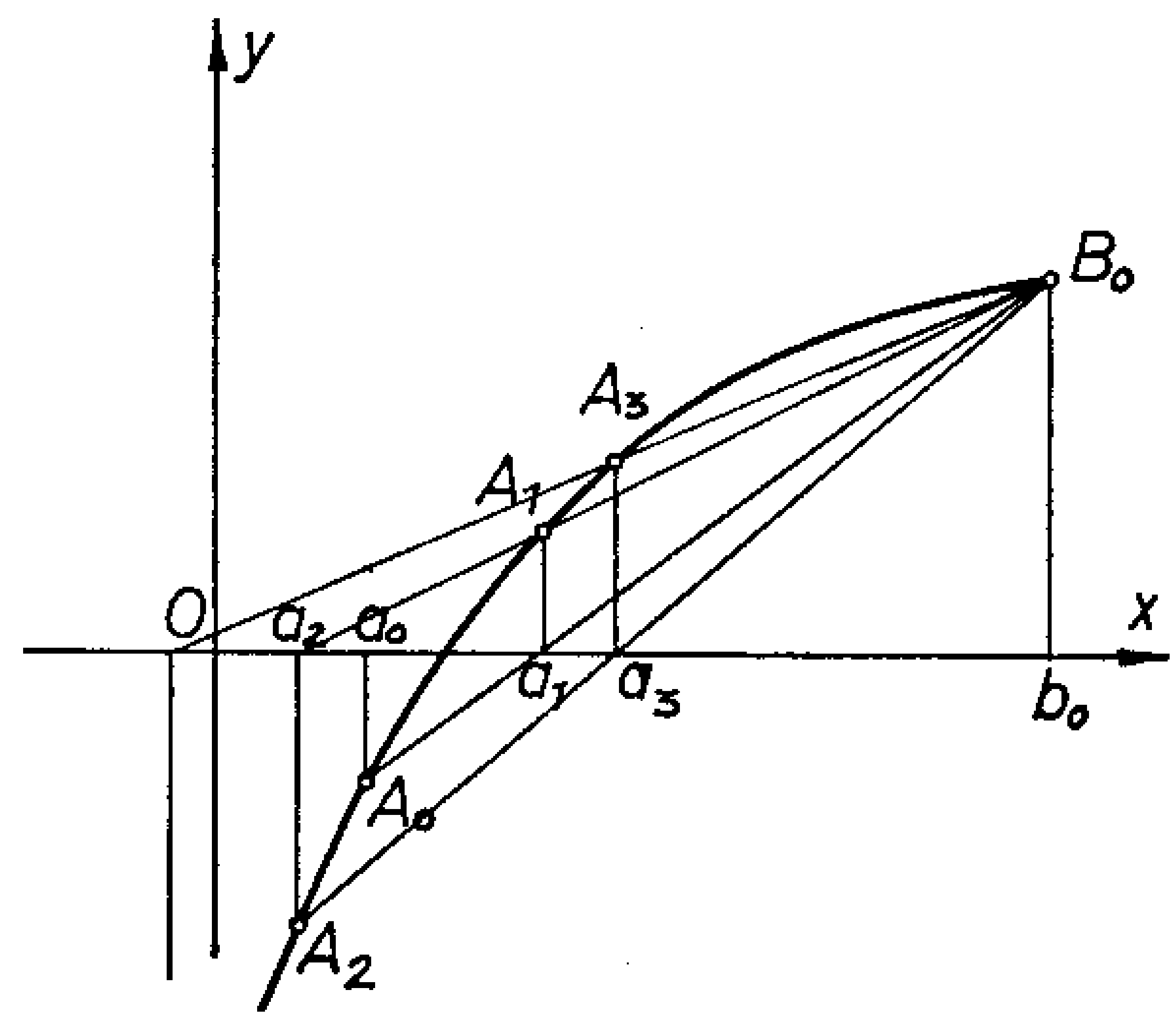
$$b_2 \;=b_1-\frac{b_1-a}{fb_1-fa}f(b_1)$$

(1) $$b_{n+1}=b_n-\frac{b_n-a}{fb_n-fa}f(b_n) \qquad (n=1, 2, 3, \ldots).$$

Nastaje pitanje o konvergenciji niza b_n.



Sl. 31.1.3. *a*)



Sl. 31.1.3. *b*)

⟶ **1.3.2. Teorem.** ***Uz pretpostavku da u*** $R(a, b)$ ***postoje neprekidne izvedene funkcije*** f', f'' ***i da su funkcije***

$$\operatorname{sgn} f', \quad \operatorname{sgn} f''$$

konstante u $R(a, b)$, ***gornji niz*** b_n ***konvergira prema određenom ništištu*** ξ ***funkcije*** f ***i leži između*** a, b.

Svakako, ako $\lim b_n$ postoji (neka je $=\xi$), tada je naravno $f\xi \neq fa$ pa relacija (1) daje

$$\xi = \xi - \frac{\xi - a}{f\xi - fa} f(\xi).$$

Kako je $a \neq \xi$, izlazi da je zaista $f\xi = 0$.

Dokažimo da $\xi = \lim b_n$ postoji. U vezi s (1) imamo funkciju

$$\varphi(x) = x - \frac{x-a}{fx - fa} fx = \frac{afx - fa \cdot x}{fx - fa}, \tag{2}$$

na kojoj je proveden iteracioni proces (1).

Deriviranje relacije (2) daje

$$\varphi' x = \frac{(af' x - fa)(fx - fa) - f' x (afx - xfa)}{(fx - fa)^2}. \tag{3}$$

Posebno, za ništište ξ koje po Bolzanovu teoremu postoji u $R(a, b)$ daje (3) zbog $f\xi = 0$:

$$\varphi' \xi = \frac{fa + (\xi - a) f' \xi}{fa}. \tag{4}$$

Po Taylorovoj formuli imamo

$$fx = f\xi + f'\xi \cdot (x - \xi) + \frac{f'' c}{2} (x - \xi)^2,$$

gdje je $c \in R(\xi, x)$; no $f\xi = 0$ pa specijalno za $x = a$ izlazi odatle

$$fa = -f'\xi (\xi - a) + \frac{1}{2} f''(c) (a - \xi)^2$$

pa zato (4) postaje

$$\varphi' \xi = \frac{(a - \xi)^2}{2} \frac{f'' c}{fa}. \tag{5}$$

Prema pretpostavci, funkcija f'' je neprekidna u $R(a, b)$; zato je f'' omeđeno oko ξ pa je broj $\varphi'\xi$ malen po apsolutnoj vrijednosti.

Dakle će bar u maloj okolini oko ξ biti $|\varphi'| < M < 1$. Prema teoremu 1.2.4. znači to da će niz $b_0, b_1, b_2, \ldots$ zaista konvergirati prema ništištu ξ funkcije f; pa je dakle ξ ništište same ishodne funkcije f.

1.3.3. Ocjena greške. Možemo ocijeniti i brzinu konvergiranja $b_n \to \xi$; stavimo li $m = \inf |f' x|$ za $x \in R[b_0, b_1]$, tada iz $fb_n - f\xi = f'(c) \cdot (b_n - \xi)$ izlazi

$$\left| b_n - \xi \right| \leq \frac{1}{m} \left| fb_n \right|. \tag{6}$$

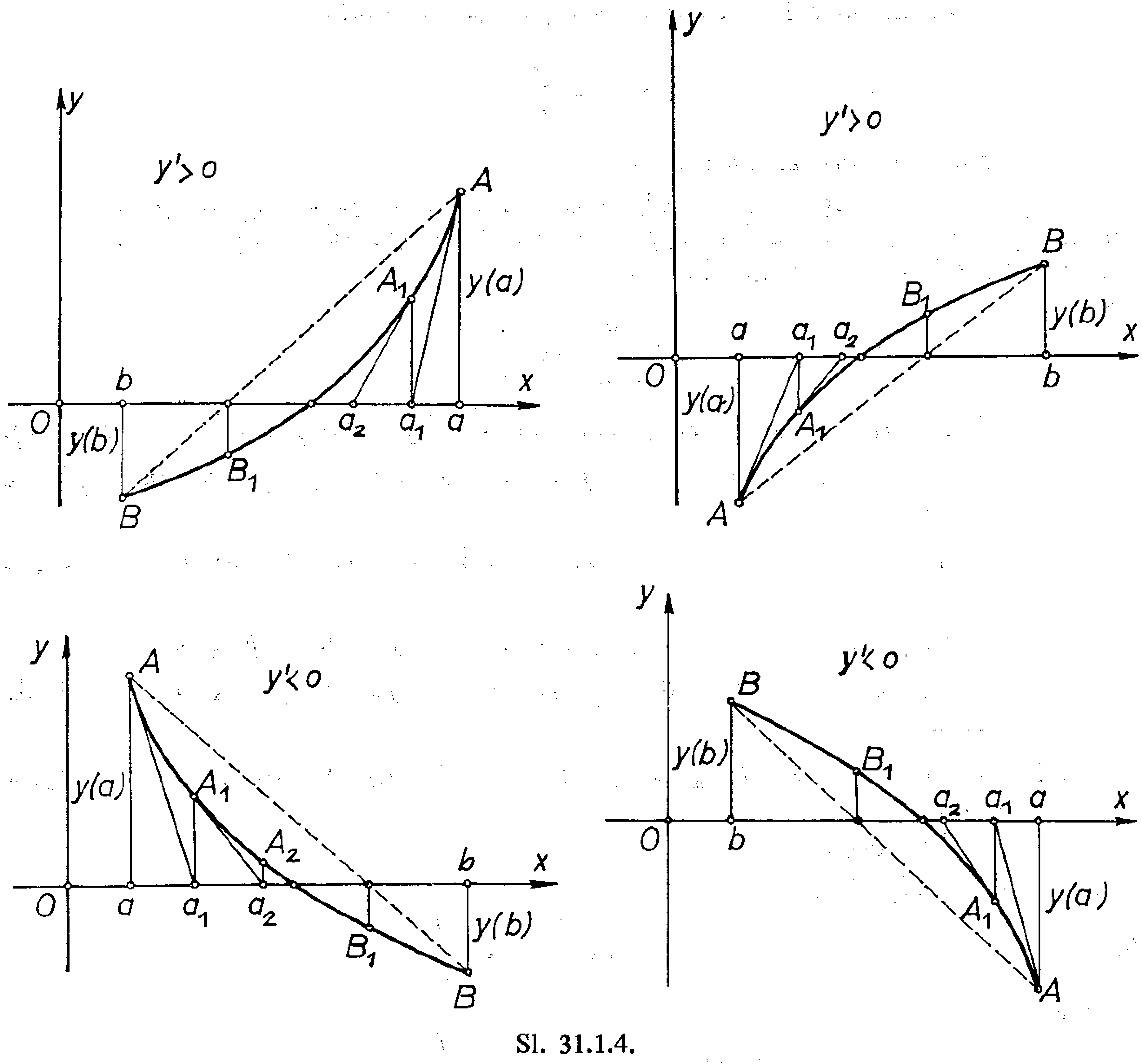
1.3.4. Primjedba. Metoda sekante je specijalan slučaj iteracione metode izvršene za funkciju (2).

1.4. Metoda tangente ili dirke (I. Newton 1669, J. Raphson 1697[1]). Metoda se sastoji u tom da se luk $\overset{\frown}{AB}$ krivulje $y=fx$ koji se projicira u $R[a, b]$ nadomjesti tangentom u $(a, fa)=A$ pri čemu pretpostavljamo da je ispunjen ovaj tzv. *Fourierov uslov*

(1) $$f(a)\cdot f''(a)>0$$

(isp. pretpostavke (i), (ii), (iii) iz § 1.2.7).

Uz taj uslov (1) ne mora biti nužno $a<b$; po dogovoru, onaj kraj intervala $I=R[a, b]$ za koji vrijedi (1) označujemo sa a (isp. sliku).



Sl. 31.1.4.

1.4.1. Ako sada broj $a_0=a$ smatramo približnom vrijednosti korijena ξ iz $R(a, b)$, tada tangenta u A

$$y-fa=f'(a)(x-a)$$

[1] I. Newton u djelu *Analysis per aequationum numerorum infinitas* (1669) tiskano 1711; J. Raphson u djelu *Analysis aequationum universalis* (Opća analiza jednadžbi), London 1697.

daje bolju aproksimaciju a_1 korijena ξ; a_1 se dobije iz (2) stavljajući $y=0$; tako da se radi o sjecištu $(a_1, 0)$ tangente (2) i x-osi; dakle je

(2) $$a_1 = a_0 - \frac{fa_0}{f' a_0}.$$

Iteracija dalje daje

(3) $$a_{n+1} = a_n - \frac{fa_n}{f' a_n} \text{ za } n=0, 1, 2, \ldots$$

1.4.2. Vidi se da ta iteracija izlazi kao granični slučaj metode sekante iz § 1.3. kada $b \to a$; inače iz (3) se vidi da metoda tangente izlazi kao poseban slučaj iteracione metode kad se ova primjenjuje na funkciju

(4) $$\varphi x = x - \frac{fx}{f' x}.$$

Dokažimo da proces konvergira.

Kako su a_n iz $R[a, b]$, dovoljno je dokazati da je niz a_n ili strogo uzlazan: $a_0 < a_1 < a_2 < \cdots$ (slučaj $f'(a)f''(a) < 0$) ili strogo silazan: $a_0 > a_1 > a_2 > \cdots$ (slučaj $f'(a)f''(a) > 0$). Dokažimo da je

(5) $$\operatorname{sgn} \frac{fa}{f' a} = \operatorname{sgn} \frac{f'}{f''}.$$

Prvi slučaj: $fa<0$. Tada zbog (1) imamo $f'' a<0$ dakle $f''<0$ u $R(a, b)$.

Ako je $a<b$, onda je $f'>0$ jer f raste od $fa (<0)$ do $fb>0$; dakle je $f'f''<0>faf'a$.

Ako je $a>b$, onda je $f'<0$, jer f pada od $fb>0$ do $fa<0$; dakle $f'f''>0<faf'a$.

Drugi slučaj: $fa>0$ dakle zbog (1) $f''a>0$ i $f''>0$ u $R(a, b)$.

Ako je $a<b$, onda f pada od $fa>0$ do $fb<0$ pa je $f'<0$; dakle $f'f''<0>faf'a$.

Ako je $a>b$, onda f raste od $fb<0$, do $fa>0$, pa je $f'>0$; dakle $f'f''>0>faf'a$.

Time je (5) dokazano.

No (5) i (2) daju

(6_0) $$\operatorname{sgn}(a_1 - a_0) = -\operatorname{sgn} \frac{f'}{f''}.$$

Analogno

(6_n) $$\operatorname{sgn}(a_{n+1} - a_n) = -\operatorname{sgn} \frac{f'}{f''}.$$

A iz relacija (5), (6) se neposredno zaključuje da je ili $a_0 < a_1 < a_3 < \cdots$ (slučaj $f'af''a<0$) ili $a_0 > a_1 > a_2 > \cdots$ (slučaj $f'af''a>0$).

1.4.3. Procjena greške. Za korijen ξ zbog (2) imamo

(7) $$\xi - a_1 = (\xi - a_0) + \frac{fa_0}{f' a_0}.$$

Prema Taylorovoj formuli je

$$f\xi = fa + f'a\cdot(\xi - a) + \frac{f''c_0}{2}(\xi - a)^2 \text{ za neko } c_0 \in R(a, b);$$

to zbog $f\xi = 0$ daje dijeleći sa $f'a$ i stavljajući $a_0 = a$:

$$0 = \frac{fa_0}{f'a_0} + (\xi - a_0) + \frac{1}{2}\frac{f'c_0}{f''a_0}(\xi - a)^2.$$

Ta relacija zajedno sa (7) daje

(8) $$\xi - a_1 = -\frac{1}{2}\frac{f''c_0}{f'a_0}(\xi - a_0)^2 \text{ za neko } c_0 \in R(a, b).$$

Zamijenimo li u (8) indeks 0 sa n izlazi formula poput (8) i glasi

(9) $$\xi - a_{n+1} = -\frac{1}{2}\frac{f''(c_n)}{f'(a_n)}(\xi - a_n)^2$$

za neko $c_n \in R(a, b)$; ako je

$$m = \inf|f'| \text{ u intervalu } I,$$

$$M = \sup|f''| \text{ u intervalu } I,$$

daje (9) procjenu:

(10) $$\left|\xi - a_{n+1}\right| \leq \frac{M}{2m}\left|a_n - \xi\right|.$$

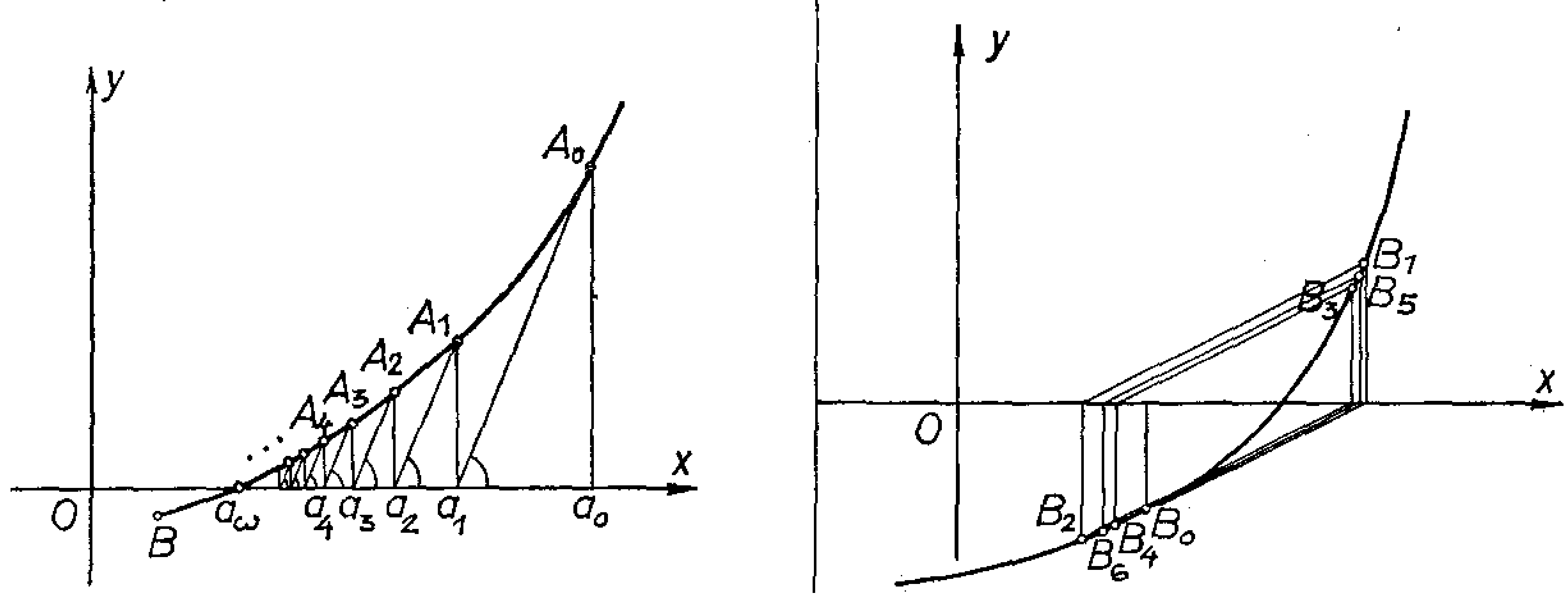
1.4.4. Preinačena Newtonova metoda. Ako je približno

(11) $$f'a_n \doteq f'a_0,$$

tada umjesto relacija (3) možemo promatrati relacije

(12) $$a_{n+1} = a_n - \frac{fa_n}{f'a_0}.$$

To znači da su pravulje a_2A_1, $a_3A_2, \ldots$ paralelne s tangentom A_0a_1 (gl. sliku!); može se dokazati da i niz (12) konvergira prema rješenju ξ za koje je $f\xi = 0$ i $\xi \in R(a, b)$.



Sl. 31.1.4.4.

1.4.5. Kombinacija metode sekante i tangente (*Dandelin*, 1826). Pođe se od intervala $I_0 = R[a, b]$ sa svojstvom

(1) $$f(a)f''(a) > 0$$

i stavi $a_0 = a$, $b = b_0$, metodom tangente odredi

$$a_1 = a_0 - \frac{f(a_0)}{f' a_0},$$

a metodom sekante odredi broj

$$b_1 = \frac{a_0 f(b_0) - b_0 f(a_0)}{f(b_0) - f(a_0)};$$

proces se iterira s intervalom

$$I_1 = R(a_1, b_1),$$

čime dobijemo interval

$$I_2 = R(a_2, b_2)$$

pa

$$I_3 = R(a_3, b_3),$$

itd. stavljajući

(2) $$a_{n+1} = a_n - \frac{f a_n}{f' a_n}$$

(3) $$b_{n+1} = b_n - \frac{f a_n - f b_n}{a_n - b_n} f b_n = \frac{b_n f a_n - a_n f b_n}{f a_n - f b_n} \quad (n = 1, 2, \ldots).$$

Postupno se vidi da relacija (1) vrijedi za svako a_n (a ne samo $a_0 = a$).

Prednost metode sastoji se u tom što uzastopne približne vrijednosti $a_0, b_0, a_1, b_1, \ldots$ leže na raznim stranama ispitivanog nulišta pa zato na svakom koraku imamo uvid u postignutu aproksimaciju broja ξ.

1.5. Određivanje kompleksnih korijena Newtonovom metodom. Ako znamo da funkcija $f(z)$ ima kompleksni korijen $\zeta = \xi + i\eta$, tada se polazeći od neke približne vrijednosti $z_0 = x_0 + iy_0$ može odrediti bolja približna vrijednost na način sličan Newtonovom. Naime, po Taylorovoj formuli je

(1) $$f(\zeta) = f(z_0) + f'(z_0)(\zeta - z_0) + \frac{f''(c)}{2}(\zeta - z_0)^2,$$

za neko c na dužini između z_0, ζ.

Ako je $\zeta - z_0$ dovoljno malo, može se onaj član sa $\Delta z_0{}^2 = (\zeta - z_0)^2$ zanemariti pa zbog $f(\zeta) = 0$ imamo

(2) $$0 = f z_0 + f'(z_0)(\zeta - z_0)$$

dakle

(3) $$z_1 = z_0 - \frac{f z_0}{f' z_0}.$$

Pri tom smo sa z_1 označili rješenje jednadžbe (2). Proces se može iterirati pa dobivamo niz

(4) $$z_{n+1}=z_n-\frac{f(z_n)}{f'(z_n)}.$$

U jednostavnijim slučajevima niz z_n konvergira prema određenom broju ζ pa se tako dođe do nulišta ζ funkcije fz.

Posebno, ako u nekoj okolini O u kojoj se nalazi niz z_n vrijedi

$$|f'|\geq m>1,$$

tada se može pokazati da je

(5) $$|z_n-\zeta|\leq m^{-1}|fz_n|$$

(isp. *Demidovič-Maron* [1] str. 155).

1.5.1. Primjer. Naći na dvije decimale nulište kompleksne funkcije $fz=e^z-0{,}2z+1$ kojem je apsolutna vrijednost minimalna.

Po realnoj osi funkcija f je >0 jer je

$$e^z=1+\frac{z}{1}+\frac{z^2}{2!}+\ldots \text{ dakle } fz=2+0{,}8z+\frac{z^2}{2!}+\frac{z^3}{3!}+\ldots$$

Za približnu vrijednost nulišta ζ uzmimo $z_0=\pi i$; tada je $fz_0=e^{\pi i}+1-$ $-0{,}2\pi i=-0{,}2\pi i$, jer je $e^{\pi i}+1=0$; nadalje je $f'\pi i=e^{\pi i}-0{,}2=-1{,}2$. Prema (3) možemo izračunati z_1 pa se dobije $z_1=\frac{5}{6}\pi i=2{,}618i$. Izračunamo li dalje z_2, $z_3,\ldots$ prema (4) dobiju se rezultati ove tablice:

n	z_n	e^{z_n}	$f(z_n)$	$f'(z_n)$
0	$3{,}142i$	-1	$-0{,}628i$	$-1{,}2$
1	$2{,}618i$	$-0{,}868+0{,}5i$	$0{,}132-0{,}024i$	$-1{,}068+0{,}5i$
2	$0{,}153+2{,}658i$	$-1{,}030+0{,}541i$	$-0{,}061+0{,}009i$	$-1{,}230+0{,}541i$
3	$0{,}109+2{,}646i$	$-0{,}978+0{,}535i$	$0+0{,}006i$	$-1{,}178+0{,}535i$
4	$0{,}107+2{,}650i$	$-0{,}981+0{,}525i$	$-0{,}002-0{,}005i$	$-1{,}181+0{,}525i$
5	$0{,}107+2{,}646i$	$-0{,}997+0{,}534i$	$+0{,}002+0{,}005i$	$-1{,}177+0{,}534i$

Kako je približno

$$|f'(\zeta)|=1{,}3\leq|f'|,$$

to je prema (5)

$$|z_5-\zeta|\leq\frac{0{,}001\cdot 20^{\frac{1}{2}}}{1{,}3}\doteq 0{,}004,$$

tako da je

$$z_5=0{,}107+2{,}646i\doteq\zeta \text{ na 2 decimalna mjesta.}$$

1.6. Rješavanje jednadžbi s dvije i više nepoznanica Newtonovom metodom. Recimo da treba riješiti jednadžbe

$$F(x, y)=0, \quad G(x, y)=0 \tag{1}$$

i da za rješenje (ξ, η) znamo neke približne vrijednosti (x_0, y_0); primjenom Taylorove formule na funkcije F, G imamo

$$\begin{aligned} F(\xi, \eta) &= F(x_0, y_0)+\frac{\partial F(x_0, y_0)}{\partial x}(\xi-x_0)+\frac{\partial F(x_0, y_0)}{\partial y}(\eta-y_0)+\varepsilon_1 \\ G(\xi, \eta) &= G(x_0, y_0)+\frac{\partial G(x_0, y_0)}{\partial x}(\xi-x_0)+\frac{\partial G(x_0, y_0)}{\partial y}(\eta-y_0)+\varepsilon_2. \end{aligned} \tag{2}$$

Ako su veličine $\xi-x_0$, $\eta-y_0$ dosta male, mogu se veličine ε_1, ε_2 zanemariti pa zbog $F(\xi, \eta)=0=G(\xi, \eta)$ nalazimo rješenje (x_1, y_1) odgovarajućih jednadžbi koje nastaju iz (2) stavljajući

$$\varepsilon_1=0=\varepsilon_2, \quad F(\xi, \eta)=0=G(\xi, \eta).$$

Izlazi

$$\begin{aligned} x_1 &= x_0-\frac{1}{J(x_0, y_0)}\begin{vmatrix} F(x_0, y_0) & F_y'(x_0, y_0) \\ G(x_0, y_0) & G_y'(x_0, y_0) \end{vmatrix} \\ y_1 &= y_0-\frac{1}{J(x_0, y_0)}\begin{vmatrix} F_x'(x_0, y_0) & F(x_0, y_0) \\ G_x'(x_0, y_0) & G(x_0, y_0) \end{vmatrix}, \end{aligned} \tag{3}$$

$$J(x_0, y_0)=\begin{vmatrix} F_x'(x_0, y_0) & F_y'(x_0, y_0) \\ G_x'(x_0, y_0) & G_y'(x_0, y_0) \end{vmatrix}.$$

Iteracijom postupka dobije se

$$\begin{aligned} x_{n+1} &= x_n-\frac{1}{J(x_n, y_n)}\begin{vmatrix} F(x_n, y_n) & F_y'(x_n, y_n) \\ G(x_n, y_n) & G_y'(x_n, y_n) \end{vmatrix} \\ y_{n+1} &= y_n-\frac{1}{J(x_n, y_n)}\begin{vmatrix} F_x'(x_n, y_n) & F(x_n, y_n) \\ G_x'(x_n, y_n) & G(x_n, y_n) \end{vmatrix} \quad (n=0, 1, 2\ldots) \end{aligned} \tag{4}$$

U jednostavnijim slučajevima proces konvergira prema traženom rješenju (ξ, η) jednadžbi (1).

1.6.1. Primjer.

$$\begin{aligned} x^2+y-3{,}61 &= 0 \\ x+y^2-6{,}86 &= 0. \end{aligned} \tag{5}$$

Nacrtamo li krivulje (5) na milimetarskom papiru vidimo da se one sijeku u 4 tačke, po jedna tačka u svakom kvadrantu; za tačku I iz prvog kvadranta vidimo da je približno $I=(1;\ 2{,}5)=(x_0, y_0)$; za tu je tačku

$$J(x_0, y_0)=\begin{vmatrix} 2 & 1 \\ 1 & 5 \end{vmatrix}=9.$$

Nadalje je

$$F(x_0, y_0) = 1 + 2{,}5 - 3{,}61 = -0{,}11$$
$$G(x_0, y_0) = 1 + 6{,}25 - 6{,}86 = 0{,}39.$$

Zato formule (3) daju naredno približenje

$$x_1 = 1{,}1$$
$$y_1 = 2{,}41.$$ Dalje bi se našlo x_2, y_2.

Tačno rješenje je

$$(\xi, \eta) = (1{,}1;\ 2{,}4), \quad \text{tj.} \quad \xi = 1{,}1, \ \eta = 2{,}4.$$

1.6.2. *Na sličan način rješavaju se jednadžbe s* 3 *i više nepoznanica.*

1.7. Rješavanje sistema jednadžbi iteracionim postupkom.

1.7.1. Imamo li riješiti jednadžbe

$$F(x, y) = 0, \quad G(x, y) = 0,$$

tada se one napišu u obliku

$$x = f(x, y), \quad y = g(x, y);$$

pođe li se od *približna rješenja* (x_0, y_0), tada se radi po ovom *iteracionom postupku*:

$$x_{n+1} = f(x_n, y_n), \ y_{n+1} = g(x_n, y_n), \quad (n = 0, 1, 2, \ldots)$$

i gleda da li niz x_{n+1}, odnosno niz y_{n+1} konvergira; njihovi eventualni limesi ξ, η daju traženo rješenje (ξ, η). Posebno se može dokazati ovo:

⟶ **1.7.2. Teorem.** ***Ako u nekoj oblasti O u kojoj leže tačke*** (x_n, y_n) ***vrijedi***

$$|f_x'| + |f_y'| \le M < 1$$
$$|g_x'| + |g_y'| \le M < 1,$$

tada niz (x_n, y_n) ***konvergira prema određenom rješenju*** $(\xi, \eta) \in O$ ***jednadžbi* (1).**

Dokažimo još općenitiji teorem.

⟶ **1.7.3. Teorem.** ***Zadan je sistem jednadžbi***

(1) $$x_\nu = \varphi_\nu(x_1, \ldots x_n) \qquad (\nu = 1, 2, \ldots, n),$$

tj. u vektorskom obliku

(2) $$\vec{x} = \varphi(\vec{x}) = [\varphi_1(\vec{x}), \ \varphi_2(\vec{x}), \ldots, \varphi_n(\vec{x})]^T;$$

neka su funkcije φ_ν ***kao i njihovi derivati***

$$\frac{\partial \varphi_\nu}{\partial x_i}$$

neprekidne funkcije u nekoj konveksnoj oblasti O euklidskog prostora R_n; ako tačka $\vec{x}^{(0)}=[x_1^{(0)}, x_2^{(0)}, \ldots, x_n^{(0)}]$ kao i tačke

$$\vec{x}^{(k+1)}=\varphi(\vec{x}^{(k)}) \quad (k=0, 1, 2, \ldots)$$

leže u O pa ako za neki broj $0<M<1$ vrijedi

$$\sup_{\nu=1,\ldots,n} \sum_{i=1}^{n} \left|\frac{\partial \varphi_\nu(x)}{\partial x_i}\right| \leq M<1 \text{ za svako } x\in O, \tag{3}$$

tada postoji $\vec{\xi}=\lim_{k\to\infty} \vec{x}^{(k)}$ i vrijedi $\vec{\xi}=\varphi(\vec{\xi})$.

Dokaz ćemo svesti na teorem 1.2.3; u tu svrhu je zgodno u koordinatnom Euklidskom prostoru R_n od n dimenzija uvesti ovakvu metriku.

1.7.4. Definicija. Tački

$$(x_1, \ldots, x_n), \text{ odnosno vektoru } \vec{x}=[x_1, x_2, \ldots, x_n]^T$$

pridružiti broj

$$\|\vec{x}\|=\sup_\nu |x_\nu| \quad (\nu=1, 2, \ldots, n)$$

kao normu; udaljenost tačaka x, y definira se tada kao $\|x-y\|$.

Lako se vidi da time prostor R_n postaje *potpun metrički prostor.*

U (3) se pojavljuje kvadratna matrica širine n; zove se *Ostrogradski-Jacobijeva matrica,* a može se označiti sa $\varphi'(\vec{x})$, da nas oznaka podsjeti na deriviranje; dakle je

$$(\varphi'(x))_{\nu i}=\frac{\partial \varphi_\nu(x)}{\partial x_i}, \quad (i, \nu=1, 2, \ldots, n).$$

Suprem u (3) označuje se $\|\varphi'(x)\|_{\mathrm{I}}$ i zove se prva norma matrice $\varphi'(x)$ i to u smislu ove definicije:

1.7.5. Definicija. *Prva norma matrice a formata* (k, n) jest

$$\|a\|_{\mathrm{I}}=\sup_{i=1,\ldots,k} \sum_{s=1}^{n} |a_{is}|.$$

Na taj način uslov (3) se ispisuje $\|\varphi' x\|_{\mathrm{I}}<M$ za svako $x\in O$.

1.7.6. Dokaz teorema 1.7.3. Dokažimo da za funkcije $\varphi_\nu(x)$ iz iskaza 1.7.3. preslikavanje $\vec{y}=\varphi(\vec{x})$, pri čemu je

$$\varphi(\vec{x})=\begin{bmatrix} \varphi_1(x_1\cdots x_n) \\ \cdots\cdots \\ \varphi_n(x_1\cdots x_n) \end{bmatrix}$$

jest određeno *stezanje* (*kontrakcija*) *oblasti O* iz teorema i da je *koeficijent stezanja* $\leq M < 1$, tj. vrijedi

$$\| y^{(2)} - y^{(1)} \|_{\mathrm{I}} \leq M \| x^{(2)} - x^{(1)} \|_{\mathrm{I}} \text{ za bilo koje } x^{(1)}, x^{(2)} \in O.$$

No,
$$\| y^{(2)} - y^{(1)} \|_{\mathrm{I}} = \sup_{\nu} | \varphi_\nu x^{(2)} - \varphi_\nu x^{(1)} |.$$

Po teoremu o srednjoj vrijednosti za funkciju φ_ν imamo stavljajući $x^{(2)} = x^{(1)} + \Delta x^{(1)}$;

$$\varphi_\nu (x^{(1)} + \Delta x^{(1)}) = \varphi_\nu x^{(1)} + \sum_{i=1}^{n} \frac{\partial \varphi_\nu c_\nu}{\partial x_i} \Delta x_i$$

gdje je $c_\nu = x^{(1)} + \theta_\nu \Delta x^{(1)}$ za neko $0 < \theta_\nu < 1$.

Dakle je $c_\nu \in O$, jer je tačka c_ν na otvorenom odresku kojem su krajevi tačke

$$x^{(1)} = (x_1^{(1)}, \ldots, x_n^{(1)}), \quad x^{(2)} = (x_1^{(2)}, \ldots, x_n^{(2)}).$$

Dakle je

$$| \varphi_\nu (x^{(2)}) - \varphi_\nu (x^{(1)}) | \leq \sum_i \left| \frac{\partial \varphi_\nu c_\nu}{\partial x_i} \right| \cdot | \Delta x_i |.$$

Zato je

$$\| y^{(2)} - y^{(1)} \|_{\mathrm{I}} \leq \sup_{\nu \in \{1, 2, \ldots n\}} \sum_i \left| \frac{\partial \varphi_\nu c_\nu}{\partial x_i} \right| \cdot | \Delta x_i | \leq \| x^{(2)} - x^{(1)} \|_{\mathrm{I}} \sup_{\nu} \sum \left| \frac{\partial \varphi_\nu c_\nu}{\partial x_i} \right|,$$

gdje je

$$\| x^{(2)} - x^{(1)} \|_{\mathrm{I}} = \sup_{\nu \in \{1, 2, \ldots n\}} | \Delta x_\nu^{(1)} |.$$

No, kako ν prolazi konačnim skupom svakako postoji broj $k \in \{1, 2, \ldots, n\}$ za koji je

$$\sup_{\nu} \sum_i \left| \frac{\partial \varphi_\nu c_\nu}{\partial x_i} \right| = \sum_i \left| \frac{\varphi_k c_k}{\partial x_i} \right|; \text{ ovo je dalje očigledno } \leq \sup_{\nu} \sum_i \left| \frac{\partial \varphi_k (c_k)}{\partial x_i} \right|;$$

kako je posljednji izraz po definiciji upravo $\| \varphi' (c_k) \|_{\mathrm{I}}$, bit će

$$\| y^{(2)} - y^{(1)} \|_{\mathrm{I}} \leq \| x^{(2)} - x^{(1)} \|_{\mathrm{I}} \cdot \| \varphi' (c_k) \|_{\mathrm{I}}.$$

No, po pretpostavci, u O je $\| \varphi' \|_{\mathrm{I}} \leq M < 1$ dakle je specijalno zbog $c_k \in O$ ispunjeno $\| \varphi' (c_k) \|_{\mathrm{I}} \leq M < 1$ pa je dakle

$$\| y^{(2)} - y^{(1)} \|_{\mathrm{I}} \leq M \| x^{(2)} - x^{(1)} \|_{\mathrm{I}} \text{ za svako } x^{(1)}, x^{(2)} \in O.$$

A to znači da se zaista može primijeniti teorem 1.2.3. o stezanju. Time je teorem 1.7.3. dokazan.

1.7.7. Ocjena greške pri približavanju. Kao što smo dokazali obrazac (4) iz § 1.2.2. tako se i sada dokazuje da je

$$\| \xi - x^{(k)} \|_{\mathrm{I}} \leq \frac{M^k}{1-M} \| x^{(1)} - x^{(0)} \|_{\mathrm{I}} \qquad \text{za } k=1, 2, \ldots$$

Primijenimo teorem 1.7.3. na slučaj linearnih algebarskih jednadžbi, odnosno na matričnu jednadžbu oblika

$$\vec{x} = c\vec{x} + d.$$

—→ **1.7.7.1. Teorem.** *Zadana je kvadratna realna matrica c duljine n kao i n-djelni vektor d; neka je* $\|c\|_{\mathrm{I}} \leq M < 1$, *tj. neka postoji neki broj* $0 \leq M < 1$ *za koji je* $\sum_{s=1}^{n} |c_{is}| \leq M$ *za* $i=1, 2, \ldots, n$; *tada matrična jednadžba* $\vec{x} = c\vec{x} + \vec{d}$ *ima posve određeno rješenje* ξ; *ono se dobije iteracionim postupkom* $x^{(0)} = d$, $x^{(n+1)} = cx^{(n)} + d$ $(n=0, 1, 2, \ldots)$ *i vrijedi* $\vec{\xi} = \lim \vec{x}^{(k)}$, *tj.* $\xi_\nu = \lim x_\nu^{(k)}$ *za* $\nu = 1, 2, \ldots, n$.

1.7.7.2. Naravno, teorem 1.7.7. može se i direktno dokazati: zbog $\det|c-1| \neq 0$, (isp. § 1.7.8.) matrična jednadžba

(1)
$$\vec{x} = c\vec{x} + d$$

ima određeno rješenje ξ; stavi li se $\sup\limits_{\nu=1,\ldots,n} |\xi_\nu - d_\nu| = K$, tada iz

$$\xi_\nu = \sum_{s=1}^{n} c_{\nu s} \xi_s + d_\nu$$

izlazi

$$\xi_\nu - x_\nu^{(n+1)} = \sum_{s=1}^{n} c_{\nu s} \xi_s + d_\nu - \sum_{s=1}^{n} (c_{\nu s} x_s^{(n)} + d_\nu);$$

dakle

$$|\xi_\nu - x_\nu^{(n+1)}| \leq \sum_{s=1}^{n} |c_{\nu s}| \cdot |\xi_s - x_s^{(n)}|.$$

Specijalno, za $x^{(1)} = d$ daje to

$$|\xi_\nu - x_\nu^{(1)}| \leq \sum |c_{\nu s}| \cdot |\xi_s - d_s| \leq K \cdot \sum_{s=1}^{n} |c_{\nu s}|, \text{ gdje je } K = \sup_s |\xi_s - d_s|.$$

Dakle je $|\xi_\nu - x_\nu^{(1)}| \leq KM$. Induktivno se vidi da je

$$|\xi_\nu - x_\nu^{(k)}| \leq KM^k \text{ za } k=1, 2, \ldots$$

Kako je $0 < M < 1$, znači da zaista $|\xi_\nu - x_\nu^{(k)}|$ teži prema 0 sa $k \to \infty$. Dakle je $\lim x_\nu^{(k)} = \xi_\nu$, tj. $x^{(k)} \to \xi$ kad $k \to \infty$.

1.7.7.3. Matrične jednadžbe oblika (1) mnogo su ispitivane (isp. *D. K. Faddeev-V. N. Faddeeva* [1]) Zanimljiv je dokaz teorema 1.7.7. *metodom Monte Carlo* jer je u vezi s teorijom slučajnih procesa (v. *Demidovič-Maron* [1], str. 650—656; riječ je o posljednjem paragrafu te knjige).

1.7.8. Jedan dovoljan uslov za regularnost matrice. Usporedimo li teorem 1.7.7. s činjenicom da matrična jednadžba $ax=b$ (a je kvadratna matrica konačna formata) ima jedno jedino rješenje onda i samo onda ako je $\det a \neq 0$, tada se vidi da vrijedi

$\longrightarrow$ Teorem. *Ako kvadratna realna ili kompleksna matrica a konačna formata zadovoljava* $\|1-a\|_{\mathrm{I}}<1$, *tada je* $\det a \neq 0$.

Naime jednadžba $ax=b$ ekvivalentna je s jednadžbom

$$x=(1-a)x+b; \quad \text{ako je} \quad \|1-a\|_{\mathrm{I}}<1,$$

tada posljednja jednadžba ima jedno jedino rješenje (teorem 1.7.7.), pa je zato $\det a \neq 0$ (posljedica teorema 8.4. iz pogl. 13. i teorema 2.0.2. iz pogl. 14).

1.8. Napomena. Izložena razmatranja u ovom §-u o rješavanjima jednačina vrijede i za algebarske i za nealgebarske jednačine.

1.9. Prešićev način istovremenog nalaženja svih ništišta algebarskog višečlana.[1]

1.9.1. Pođimo od višečlana

$$p(x) \equiv x^n + p_{n-1}x^{n-1} + \cdots + p_1 x + p_0 \equiv (x-x_1)(x-x_2)\cdots(x-x_n) \tag{1}$$

s nejednakim još nepoznatim ništištima $x_1, \ldots, x_n$. Ako je $(a, b, \ldots, l)$ uređen niz od $1+s$ sabiraka prirodnih brojeva za koje je (2) $a+b+\cdots+l=n$, tada postoji niz algebarskih višečlana $A, B, \ldots, L$ za koje je

$$p=AB\cdots L, \text{ st } A=a, \text{ st } B=b, \ldots, \text{ st } L=l. \tag{3}$$

Ti polinomi $A, B, \ldots, L$ mogu se dobiti graničnim postupkom

$$A=\lim_{k\to\infty} A(k), \ldots, L=\lim_{k\to\infty} L(k) \tag{4}$$

polazeći od nekih izrazâ $A(0), B(0), \ldots, L(0)$ i tražeći da bude

$$\begin{cases} A(k)=x^a+\alpha_{a-1}(k)x^{a-1}+\cdots+\alpha_0(k), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ L(k)=x^l+\lambda_{l-1}(k)x^{l-1}+\cdots+\lambda_0(k) \end{cases} \tag{4'}$$

te da vrijedi npr. ovakva veza među funkcijama pri koraku $k+1$ i pri koraku k:

$$\begin{aligned} &A(k+1)B(k)\cdots L(k)+A(k)B(k+1)\cdots L(k)+\cdots+ \\ &+A(k)B(k)\cdots L(k+1)-sA(k)B(k)\cdots L(k)=p \; (k=0, 1, 2, \ldots). \end{aligned} \tag{C_k}$$

Ako se u (C_k) izjednače koeficijenti odgovarajućih stepenâ od x, dobije se veza između koeficijenata pri koraku $k+1$ i onih pri koraku k. To omogućava da se pusti da k teži u $+\infty$ i da se dođe do izrazâ (4) i rastava (3).

1.9.2. U posebnom slučaju $a=b=\cdots=l=1$ može se uvesti oznaka (5) $A(k)\equiv x-a_1(k), \ldots, L(k)\equiv x-a_n(k)$; ako pretpostavimo da među veličinama $a_1(k), \ldots, a_n(k)$ nema jednakih, pa ako u odgovarajuću jednačinu (C_k) stavimo $x=a_\nu(k)$ i odatle izračunamo $a_\nu(k+1)$, izlazi

$$a_\nu(k+1)=a_\nu(k)-\frac{p(a_\nu(k))}{Q_k'(a_\nu(k))} \quad (\nu=1, 2, \ldots, n) \text{ pri čemu je} \tag{6}$$

$$Q_k(x)=(x-a_1(k))(x-a_2(k))\cdots(x-a_n(k)).$$

[1] Slaviša B. Prešić, *Jedan interativan postupak za faktorizaciju polinoma* (Matem. Vesnik Beograd 5 (20) (1968) 205-216.

Prešićeva postupna veza (6) odgovara Newtonovoj postupnoj vezi

$$(7)\qquad a_\nu(k+1)=a_\nu(k)-\frac{p(a_\nu(k))}{p'(a_\nu(k))}\ \text{(isp. (3) u t. 1.4.1)}$$

za izračunavanje jednog (inače bilo kojeg) nistišta polinoma $p(x)$.

1.9.3. Primjer (v. isti Prešićev članak, s. 211). Neka je zadan višečlan

$$p(x)\equiv x^4-18x^3+104x^2-222x+135.$$

Pođe li se od niza (05; 2,6; 4,2; 8,1) kao približnog niza za niz (x_1, x_2, x_3, x_4) traženih nulišta toga višečlana, tada izračunavanja daju slijedeću tablicu:

	x_1	x_2	x_3	x_4
0	0,5	2,6	4,2	8,1
1	1,309668	3,131948	4,838669	8,719715
2	0,997929	2,954510	5,041347	9,006184
3	1,000025	2,999006	5,000985	8,999984
4	1,000000	3,000000	5,000000	9,000000
5	1,000000	3,000000	5,000000	9,000000

Dakle je $(x_1;\ x_2;\ x_3;\ x_4)=(1;\ 3;\ 5;\ 9)$.

1.9.4. Slučaj od više nepoznanica. Sličan postupak za istovremeno određivanje svih rješenja sistema jednačina također je ispitivan[1].

2. NUMERIČKO RJEŠAVANJE ALGEBARSKIH JEDNADŽBI METODOM DANDELIN-LOBAČEVSKI-GRAEFFE[2]

2.0. Ideja vodilja. — **2.0.0.** Riječ je o tome da se algebarska jednadžba

$$a(x)\equiv\sum_{\nu=0}^{n} a_\nu x^\nu \equiv a_n\prod_{i=1}^{n}(x-x_i)=0$$

sa zadanim *numeričkim* koeficijentima riješi na *određen broj decimala* i to specijalno da se *nađu rješenja kojima je apsolutna vrijednost maksimalna.*

2.0.1. Ideja počiva na D. Bernoullievoj zamisli da se formiraju simetrične funkcije $s_k=\sum_{i=1}^{n} x_i^k$; ako je ξ član u spektru $\sigma(a)$ maksimalnog modula pa ako je α kratnost od ξ, tada je

$$s_k=\alpha\xi^k+x_{\alpha+1}{}^k+\cdots+x^k{}_n;$$

za dosta veliko k bilo bi približno

$$\frac{s_k}{s_{k-1}}\doteq\xi.$$

[1] Vidjeti: Jovan P. Petrić—Slaviša V. Prešić, *Algoritam za rešavanje jednog sistema nelinearnih jednačina.* (Naučno-tehnički pregled, Beograd, 20 (1970) br. 9-10, 63-73).

[2] *G. Dandelin* 1826, Bull. Ac. Bruxelles 3 (1826) 48; *N. I. Lobačevski* 1834, Algebra, Kazan § 257; *C. H. Graeffe,* Auflösung der höheren numerischen Gleichungen, Zürich 1837. (v. Н. И. Лобачевский, Полное собрание сочинений, 4 (1948) str. 472).

Ako je $|\xi|$ mnogo veće od apsolutnih vrijednosti ostalih korijena, tada je $s_k \doteq \alpha\xi^k$ pa se odatle nađe ξ i vrši proba, da se od k vrijednosti

$$(\alpha^{-1} s_k)^{\frac{1}{k}}$$

izabere ona koja približno zadovoljava $a(x)=0$.

2.0.2. Izrazi s_k $(k=1, 2, \ldots)$ mogu se odrediti *iz koeficijenata* a_ν *i bez poznavanja rješenjâ* x_k (isp. pogl. 19, § 2.2.2); specijalno je $s_1=-a_{n-1}a_n^{-1}$. Prema tome, odredimo li polinom $(x+x_1^2)(x+x_2^2)\cdots(x+x_n^2)$, bit će u *njemu* s_2 *upravo koeficijent od* $(x^2)^{n-1}$; *i taj polinom i taj koeficijent, tj.* s_2 *brzo se nađu.* Iteracijom, moći će se tako odrediti $s_{2^2}, s_{2^3}, s_{2^4}, \ldots$ dakle s_k za dovoljno visoko k.

2.0.3. Pretpostavljat ćemo $a_0 \neq 0$, tj. $a(0) \neq 0$; inače je dovoljno odrediti $b(x)$ i m tako da bude $a(x) \equiv x^m b(x)$, $b(0) \neq 0$ (m prirodni broj), pa umjesto $a(x)$ promatrati $b(x)$.

2.0.4. U *praktičnom pogledu* bolje da $a(x)$ ima *što više koeficijenata* $=0$. U *teoretskim* obrazloženjima pretpostavljat ćemo da su svi koeficijenti $\neq 0$. Naime, kako mi sada tražimo približna rješenja, može se svako $a_\nu=0$ zamijeniti tako malim brojem $a_\nu' \neq 0$ pa da nova jednadžba i stara jednadžba budu *ekvivalentne s obzirom na traženi broj decimala.*

2.0.5. Od bitnog su značenja Vièteove formule.

2.1. Uloga Vièteovih formula (isp. pogl. 19, § 1.2.1).

2.1.1. Neka je

$$a(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n=a_n(x-x_1)(x-x_2)\cdots(x-x_n)$$

algebarski polinom n-og stepena (dakle je $a_n \neq 0$); tada Vièteove formule glase (isp. pogl. 19, § 1.2.1; u 7. retku teorema treba očigledno umjesto $(-1)^k$ biti $(-1)^\nu$):

$$\begin{aligned} &\sigma_1(x_1,\ldots,x_n)=-(x_1+x_2+\cdots+x_n)=a_{n-1}a_n^{-1},\\ \text{(V)}\quad &\sigma_2(x_1,\ldots,x_n)=\quad \Sigma x_{i_1}x_{i_2}=a_{n-2}a_n^{-1}\quad (i_1, i_2=1, 2, \ldots, n;\ i_1<i_2),\\ &\sigma_\nu(x_1,\ldots,x_n)=(-1)^\nu\,\Sigma x_{i_1}x_{i_2}\cdots x_{i_\nu}=a_{n-\nu}a_n^{-1}\,(i_1, i_2, \ldots, i_\nu=1, 2, \ldots, n \end{aligned}$$

uz uslov

$$i_1<i_2<\cdots<i_\nu),\quad (\nu=1, 2, \ldots, n).$$

2.1.2. *Slučaj kad se nulišta polinoma međusobno mnogo razlikuju.* Ako su nulišta polinoma $a(x)$ međusobno nejednaka pa ako ih numeriramo uzlazno po apsolutnoj veličini dakle

$$|x_1| \leq |x_2| \leq \cdots \leq |x_n|, \tag{1}$$

pa ako je svaki član niza (1) (osim posljednjega) mnogo manji od svojeg sljedbenika, tada iz Vièteovih formula (V) zaključujemo da približno vrijede ove jednakosti

$$\begin{aligned} x_n &= -a_{n-1}a_n^{-1},\\ x_{n-1}x_n &= a_{n-2}a_n^{-1} \\ &\cdots\cdots\cdots\\ x_{n-\nu+1}x_{n-\nu+2}\cdots x_n &= (-1)^\nu a_{n-\nu}a_n^{-1}\quad (\nu=1, 2, \ldots, n) \end{aligned} \tag{2}$$

Naime u izrazima (V) na lijevoj strani dominiraju završni članovi, pa preostale članove zanemarujemo.

⟶ **2.1.3. Teorem.** *Ako polinom*

$$a(x)=\sum_{i=0}^{n} a_i x^i \quad \textit{stepena } n$$

ima n različitih korijena $x_1, x_2, \ldots, x_n$ *pa je pri tom*

(3) $$|x_1| \ll |x_2| \ll \cdots \ll |x_n|,$$

tada približno vrijedi obrazac (2); *znak* $x \ll y$ *iskazuje da je x znatno manje od y. Specijalno, ako su koeficijenti* $a_\nu \neq 0$, *tada je*

(4) $$x_\nu \doteq -a_{\nu-1} a_\nu^{-1} \qquad (\nu=1, 2, \ldots, n).$$

Primjedba. U (2), odnosno (4) pojavljuju se sama nulišta a ne apsolutne vrijednosti nulištâ; u tome je znatna prednost obrazaca (2), odnosno (4).

2.1.4. Ako nulišta polinoma nemaju vrlo razmaknute svoje apsolutne vrijednosti, tada ih postupnim kvadriranjem možemo sve više razmicati; pogotovo ako je koje ništište dominantno, ta će se dominantnost još više povećati kvadriranjem svih ništišta. Na tome se i zasniva metoda Lobačevskog.

⟶ **2.1.5. Osnovni teorem o približnom razbijanju.**

(i) *Ako se skup s ponavljanjem* $x_1, x_2, \ldots, x_n$ *(označimo ga sa* $S=S_{a(x)}$*)*[1] *za koji je* $a(x) \equiv a_n \prod_{\nu=1}^{n}(x-x_\nu)$ *može razbiti na dva dijela* $S(1)$, $S(2)$ *tako da za svako* $y_1 \in S(1)$ *i svako* $y_2 \in S(2)$ *bude* $|y_1| \ll |y_2|$, *tada je približno*

(1) $$S(a_0+a_1 x+\cdots+a_{k_1} x^{k_1}) \doteq S(1)$$

(2) $$S(a_{k_1}+a_{k_1+1} x+\cdots a_n x^{n-k_2}) \doteq S(2),$$

pri čemu je k_i *broj članova u* $S(i)$, $(i=1,2)$.

Specijalno se $S(2)$ *vlada gotovo kao da zadana jednadžba glasi*

$$\sum_{\nu=n-k_2}^{n} a_\nu x^\nu = 0.$$

(ii) *Ako je* $$S(a)=S(1) \cup S(2) \cup \cdots \cup S(r)$$

i pri tom

$$|y_1| \ll |y_2| \ll \cdots \ll |y_r| \quad \textit{za } y_1 \in S(1),\ y_2 \in S(2), \ldots, y_r \in S(r),$$

tada je približno

(3)
$$\begin{aligned}
&S(a_0+a_1 x+\cdots+a_{k_1} x^{k_1}) \doteq S(1)\\
&S(a_{k_1}+a_{k_1+1} x+\cdots+a_{k_1+k_2} x^{k_2}) \doteq S(2)\\
&\quad\cdots\cdots\cdots\cdots\cdots\cdots\\
&S\left(\sum_{\nu=0}^{k_r} a_{k_1+k_2+\cdots+k_{r-1}+\nu}\, x^\nu\right) \doteq S(r),
\end{aligned}$$

[1] $S(a(x))$ je spektar s ponavljanjem polinoma $a(x)$; odmah ćemo taj skup rastavljati na dijelove, npr, $S(1)$, $S(2)$.

pa je rješenje jednadžbe $a(x)=0$ približno ekvivalentno rješavanju faktorske ili rascijepne jednadžbe

$$\left(\sum_{e_1=0}^{k_1} a_{e_1} x^{e_1}\right)\left(\sum_{e_2=0}^{k_2} a_{k_1+e_2} x^{e_2}\right)\left(\sum_{e_3=0}^{k_3} a_{k_1+k_2+e_3} x^{e_3}\right)\cdots\left(\sum_{e_r=0}^{k_r} a_{k_1+k_2+\cdots+k_{r-1}+e_r} x^{e_r}\right)=0;$$

pri tom k_ρ za $\rho=1, 2, \ldots, r$ znači broj članova u $S(\rho)$; kratnost se uračunava.

Primjedba. U slučaju $r=n$, daje teorem 2.1.5. upravo teorem 2.1.3. Obradimo slučaj $r=2$. Promatrajmo osnovne simetrične funkcije

$\sigma_\nu(x_1, x_2, \ldots, x_n)$ i pišimo kraće $\sigma_\nu(Sa)$, odnosno $\sigma_\nu(S)$;

isto tako se razumije da je npr.

$\sigma_\nu S(\rho)=\sigma_\nu(z_1, z_2, \ldots, z_k)$ ako je $S(\rho)=z_1, z_2, \ldots, z_k$.

Prema Vièteovim formulama imamo

$$a_n^{-1} a_{n-1}=\sigma_1 S=\sum_{\nu=1}^{n} -x_\nu=\sigma_1(S(1))+\sigma_1(S(2))=(\text{približno})\ \sigma_1 S(2),$$

$$\text{jer } |\sigma_1 S(1)| \ll |\sigma_1 S(2)|.$$

Isto tako $a_n^{-1} a_{n-2}=\sigma_2 S=\sigma_2 S(2)+\sum_{i_1<i_2} x_{i_1} x_{i_2}$, pri čemu je bar jedan od brojeva x_{i_1}, x_{i_2} iz $S(1)$. Dakle se to $\Sigma\, x_{i_1} x_{i_2}$ može zanemariti pa je

$$a_n^{-1} a_{n-2} \doteq \sigma_2(S(2)).$$

Isto se tako zaključuje da je približno

(5) $$a_n^{-1} a_{n-\nu} \doteq \sigma_\nu(S(2)) \quad \text{za } \nu=1, 2, \ldots, k_2.$$

A to, zbog identiteta

$$\prod_{\alpha \in S(2)} (x-\alpha)=\sum_{\nu=0}^{k_2} \sigma_\nu S(2)\, x^{k_2-\nu}$$

upravo znači da približno vrijedi relacija (2).

Promatrajmo obrasce

(6) $$a_n^{-1} a_{n-\nu}=\sigma_\nu S \quad \text{i za preostale } \nu=k_2+1,\ k_2+2, \ldots, \ldots, n.$$

U svakom članu toga $\sigma_\nu S$ pojavljuje se bar jedan element iz $S(1)$; zbog $S(1) \ll S(2)$, možemo zanemariti svaki član u $\sigma_\nu S$ u kojem se pojavljuje bar $\nu-k_2+1$ varijabla iz $S(1)$; time svaki zadržani član od $\sigma_\nu S$ sadržava kao faktor produkt od svih k_2 članova iz $S(2)$ kao i produkt od $\nu-k_2$ elemenata iz $S(1)$; to znači da je približno

$$\sigma_\nu S \doteq \sigma_{k_2} S(2) \cdot \sigma_{\nu-k_2} S(1).$$

Prema (5) i (6) postaje to

$$a_n^{-1} a_{n-\nu} \doteq a_n^{-1} a_{k_2} \sigma_{\nu-k_2} S(1)$$

(7) $$\sigma_{\nu-k_2}(S(1)) = a_{k_2}^{-1} a_{n-\nu} \text{ za } \nu = k_2+1, \ldots, n.$$

Stavimo li $k = \nu - k_2$, znači to da će biti

$$\sigma_k S(1) = a_{k_2}^{-1} a_{n+k_2-k} \text{ za } k = 1, 2, \ldots, n-k_2 (=k_1).$$

Identitet

$$\prod_{\alpha \in S(1)} (x-\alpha) = \sum_{k=0}^{k_1} \sigma_k S(1) x^{k_1-k}$$

postaje time

$$\prod_{\alpha \in S(1)} (x-\alpha) = a_{k_2}^{-1} \sum_{k=0}^{k_1} a_{k_1-k} x^{k_1-k}$$

što znači da je ispravna relacija (1).

Dakle je teorem istinit za $r=2$; analogno bi se teorem dokazao za $r = 3, 4, \ldots$

2.2. Jednadžba veličinâ — x_ν^2.[1] — **2.2.1.** Teorem o operatoru $a \to a^\square$. *Ako je* $a(x) = a_n (x-x_1)(x-x_2) \cdots (x-x_n)$, $a_n \neq 0$, tada stavljajući $a_n^2 (x+x_1^2)(x+x_2^2) \cdots (x+x_n^2) = a^\square(x) = a_0^\square + a_1^\square x + a_2^\square x^2 + \cdots + a_n^\square x^n$ izlazi

(1)
$$\begin{aligned}
a_0^\square &= a_0^2 \\
a_1^\square &= a_1^2 - 2a_0 a_2 \\
&\cdots\cdots\cdots\cdots \\
a_\nu^\square &= a_\nu^2 - 2\sum_{e=1}^{\nu} (-1)^e a_{\nu-e} a_{\nu+e} \quad (\nu = 1, 2, \ldots, n-1) \\
a_n^\square &= a_n^2.
\end{aligned}$$

Shematski:

Polinom a	a_0	a_1	a_2	$a_3 \cdots$
	a_0^2	a_1^2	a_2^2	$a_3^2 \cdots$
		$-2a_0a_2$	$-2a_1a_3$	$-2a_2a_4 \cdots$
+			$2a_0a_4$	$2a_1a_5 \cdots$
				$-2a_0a_6 \cdots$
				$\cdots\cdots$
Polinom $a^\square$	$a_0^\square$	$a_1^\square$	$a_2^\square$	$a_4^\square \cdots$

[1] Predznak — uzima se iz razloga da veza među novim koeficijentima $a_i^\square$ i starim koeficijentima a_k bude što preglednija (isp. § 2.0.2).

Dokaz. Očigledno, polinom $a^{\square}(x)$ izlazi iz

$$b(x^2)=a_n^2(-x^2+x_1^2)(-x^2+x_2^2)\cdots(-x^2+x_n^2)\,(=a(x)\,a(-x))$$

pišući x umjesto $-x^2$. No,

$$b(x^2)=a(x)\,a(-x)=\sum_{\nu=0}^{n}[a_0\cdot a_{2\nu}-a_1a_{2\nu-1}+ \tag{2}$$

$$+a_2a_{2\nu-2}+-\cdots+(-1)^\nu a_\nu^2+(-1)^{\nu-1}a_{\nu+1}a_{\nu-1}+\cdots+a_{2\nu}a_0]\,x^{2\nu}.$$

U [ ] su jednaki oni članovi koji su jednako daleko od krajeva; pišemo li $-x$ umjesto x^2 dakle $(-1)^\nu x^\nu$ umjesto $x^{2\nu}$, prelazi (2) u jednakost

$$b(-x)=\sum_{\nu=0}^{n}\left[a_\nu^2-2a_{\nu+1}a_{\nu-1}+2a_{\nu+2}a_{\nu-2}-+\cdots+(-1)^\nu 2a_{2n}a_0\right]x^\nu,\text{ tj.}$$

$$a^{\square}(x)=\sum_{\nu=0}^{n}\left[a_\nu^2-2(a_{\nu-1}a_{\nu+1}-a_{\nu-2}a_{\nu+2}+-\cdots+(-1)^\nu a_0a_{2n}\right]x^\nu; \tag{3}$$

(desnu polovinu od [ ] smo množili sa 2, jer smo lijevu polovinu ispustili).

Izjednačujući u (3) koeficijente na lijevoj i desnoj strani, dobiju se upravo traženi obrasci (1).

2.2.2. Primjedba. Ako jednadžba $a(x)=0$ s *realnim* koeficijentima ima samo *realne* korijene, tada jednadžba $a^{\square}(x)=0$ ima samo *negativne* korijene; zato prema Descartesovu teoremu koeficijenti od $a^{\square}$ ne mogu biti <0. Prema tome, ako polinom $a^{\square}$ ili $a^{\square\square},\ldots$ ima koji koeficijent <0, onda je to siguran znak da $a(x)$ ima bar jedno *nerealno nulište*.

N. I. Lobačevski
01. 12. 1792—24. 02. 1856,
veliki ruski matematičar.

2.2.3. Metoda Dandelin-Lobačevski-Graeffeova (D. L. G.-metoda).

2.2.3.1. Pri toj metodi polazeći od numeričke jednadžbe

$$a(x)\equiv a_0+a_1x+a_2x^2+\cdots+a_nx^n=0 \tag{1}$$

odredi se jednadžba $a^{\square}(x)=0$ na način opisan u § 2.2; izračunavanja se vrše pomoću tablica ili raznih računskih pribora. Zatim se proces iterira i odredi

$$a^{\square^2}(x)=(a^{\square}(x))^{\square},\ a^{\square^3}(x)=(a^{\square^2}(x))^{\square},\ldots,\ a^{\square^k}=(a^{\square^{k-1}}(x))^{\square};$$

pišimo kraće

$$A(x)\equiv a^{\square^k}(x).$$

To znači da se $\square$-proces iterira k puta i time iz jednadžbe $a(x)=0$ dobije jednadžba $A(x)=0$ stepena n za veličine

$$y_\nu=-x_\nu^s,\ (\nu=1,2,\ldots,n); \tag{2}$$

stavili smo $2^k = s$; dakle je

$$A(y) \equiv a_n^s (y + x_1^s)(y + x_2^s) \cdots (y + x_n^s) = 0, \quad s = 2^k. \tag{3}$$

Iteriranje $\square$-procesa vrši se tako dugo dok glavni koeficijenti ne postanu skoro neosjetljivi na $\square$-proces; pri tom treba imati na umu da se izračunavanja vrše na određen broj decimala.

Vièteove formule vezane za jednadžbu (3) glase

$$\begin{aligned} &A_n^{-1} A_{n-1} = -(y_1 + y_1 + \cdots + y_n) = x_1^s + x_2^s + \cdots + x_n^s \\ &A_n^{-1} A_{n-2} = \Sigma\, y_{i_1} y_{i_2} = \Sigma\, x_{i_1}^s x_{i_2}^s \\ &\cdots\cdots\cdots\cdots \\ &A_n^{-1} A_{n-\nu} = (-1)^\nu \Sigma\, y_{i_1} \cdots y_{i_\nu} = \Sigma\, x_{i_1}^s \cdots x_{i}^s; \quad (\nu = 1, 2, \ldots, n); \end{aligned} \tag{4}$$

pri tom je $i_1 < i_2 < \cdots < i_\nu$ te $i_\nu \in \{1, 2, \ldots, n\}$.

—→ **2.3.2. Teorem.** ***Ako nulišta $x_1, x_2, \ldots, x_n$ polinoma $a(x)$ zadovoljavaju $|x_1| \leq |x_2| \leq \cdots \leq |x_n|$, tada za povelik broj $s = 2^k$ vrijedit će približno***

$$x_\nu^s = A_{\nu-1} A_\nu^{-1}; \tag{5}$$

pri tom $A(y) = A_0 + A_1 y + A_2 y^2 + \cdots + A_n y^n$ označuje polinom koji se iz polinoma $a(x)$ dobije iteriranim $\square$-postupkom izvedenim uzastopno k puta (isp § 2.2).

Naime, teorem je drukčije napisan teorem 2.1.3.

2.3.2.1. Primjedba o normiranju ishodne jednadžbe. Prije no što se prijeđe na traženje jednadžbe $a^\square(x) = 0$, dobro je zadanu jednadžbu $a(x) = 0$ normirati (podijeliti sa a_n), odnosno preobraziti u takvu jednadžbu kojoj je najstariji koeficijent $= 1$.

2.3.3. Povratak na x. Kad se približno našlo $y = -x^s$, treba odrediti i samo ništište x od $a(x)$; svakako je

$$x_\nu = (-y_\nu)^{1/s}; \tag{6}$$

samo se radi o tome koju od s vrijednosti (6) uzeti u obzir; stvarno, treba provjeriti za svaku vrijednost $(-y_\nu)^{1/s}$ da li bar približno zadovoljavaju relaciju $a(x) = 0$. Time se dakle dobiju približne vrijednosti traženih rješenja x_ν.

2.3.4. Slučaj da je spektar σ_a realan. Ako znamo unaprijed da x mora biti realno pa i sa određenim predznakom, onda je prelaz od y na x lak i brz.

2.3.5. Primjer.

$$a(x) \equiv x^3 - 4x + 1 = 0.$$

Prema Descartesovu teoremu jednadžba ima jedno jedino negativno rješenje; kako $a(0)\, a(1) < 0$, znači da je jedno nulište između 0 i 1; zato su dva rješenja pozitivna.

Postupak $\square$ izvest ćemo po ovoj shemi radeći na način prikazan u § 2.2:

	Korak	a_0	a_1	a_2	a_3
$a(x)$	0	1	-4	0	1
$a^{\square}(x)$	1	1	16	8	1
$a^{\square^2}(x)$	2	1	240	32	1
			57600 $-$ 64	1024 -480	
	3	1	57536	544	1
			3310391296 $-$ 1938	180864	1
	4	1	3310390208 $\doteq 3{,}31 \cdot 10^9$	$\doteq 1{,}8 \cdot 10^5$	1
	5	1	$1{,}09587 \cdot 10^{19}$	$2{,}6 \cdot 10^{10}$	1
$A(x)$	6	1	$1{,}20 \cdot 10^{38}$	$6{,}59 \cdot 10^{20}$	1

$$s = 2^6 = 64.$$

$$x_1^s = A_0 : A_1; \quad \log|x_1| = 0{,}40501 - 1$$
$$|x_1| = 0{,}2541.$$
$$x_2^s = A_1 : A_2; \quad \log|x_2| = 0{,}2696992$$
$$|x_2| = 1{,}8608.$$
$$x_3^s = A_2 : A_3; \quad \log|x_3| = 0{,}32529$$
$$|x_3| = 2{,}1149.$$

Kako je $x_1 + x_3 + x_2 \doteq 0$ mora biti $x_3 < 0$, dakle $x_1 > 0$, $x_2 > 0$, pa je

$$x_1 \doteq 0{,}2541 \qquad x_2 \doteq 1{,}8608 \qquad x_3 \doteq -2{,}1149.$$

Pokus daje zaista $x_1 + x_2 + x_3 \doteq 0$.

2.3.6. D L G-metoda i prisustvo dvaju konjugirano kompleksnih nerealnih rješenja.

$\longrightarrow$ **Teorem.** ***Ako spektar $x_1, x_2, \ldots, x_n$ realna polinoma $a(x)$ stepena n ima jedan jedini par x_e, $\bar{x}_e$ nerealnih nulišta[1], pa ako je***

(1) $$|x_1| \leqslant |x_2| \leqslant \cdots |x_\alpha| = r = |\bar{x}_{\alpha+1} \leqslant |x_{\alpha+2}| \leqslant \cdots |x_n|,$$

[1] Kako su koeficijenti polinoma $a(x)$ realni, to iz $a(z) = 0$ za konjugirani broj $\bar{z}$ izlazi $a(\bar{z}) = 0$ (pogl. 5, § 3.2.3).

tada se iz pripadne diskriminantne jednadžbe $A(y)=0$ *gdje je* $A=a^{\square k}$ (isp. § 2.3.2) *realna nulišta* x_ν *određuju kao i prije pomoću realnih brojeva*

(2) $$y_\nu = -x_\nu^s,\quad s=2^k;$$

približno je

(3) $$A_{\nu-1} + A_\nu y_\nu \doteq 0;$$

kompleksni brojevi

$$y_\alpha = -x_\alpha^s,\quad y_{\alpha+1} = -x_{\alpha+1}^s$$

zadovoljavaju približno jednadžbu

(4) $$A_{\alpha-1} + A_\alpha y + A_{\alpha+1} y^2 = 0;$$

apsolutna vrijednost $r=|x_\alpha|=|x_{\alpha+1}|$ *izračunava se iz*

(5) $$r = +(A_{\alpha-1} A_{\alpha+1}^{-1})^{1/2s};$$

argument φ *nulišta* $x_\alpha = r(\cos\varphi + i\sin\varphi)$ *izračunava se iz*

(6) $$2r\cos\varphi = -a_{n-1} a_n^{-1} - \sum_\nu x_\nu,$$

pri tom je $\nu = 1, 2, \ldots, n$ *te* $\alpha \neq \nu \neq \alpha+1$.

Naime, za poveće $s=2^k$ brojevi (2) zadovoljavat će

$$|y_1| \ll |y_2| \ll \cdots \leq |y_\alpha| = r^s = |\overline{y_{\alpha+1}}|^s \leq |y_{\alpha+2}| \ll \cdots \ll |y_n|$$

pa relacije (3), (4) izlaze iz osnovnog teorema 2.1.5; obrazac (5) izlazi iz činjenice da je $y\bar{y} = A_{\alpha-1} A_{\alpha+1}^{-1}$ (produkt korijena kvadratne jednadžbe!).

Obrazac (6) je posljedica Vièteove formule

$$\sum_{\nu=1}^{n} x_\nu = -a_{n-1} a_n^{-1}$$

i činjenice da je $x_\alpha + \overline{x_{\alpha+1}} = 2r\cos\varphi$.

2.3.7. D L G-metoda i prisustvo dvaju parova konjugirano kompleksnih nerealnih rješenja.

—→ **Teorem.** *Ako spektar* $x_1, x_2, \ldots, x_n$ *realna polinoma* $a(x)$ *stepena* n *ima* $n-4$ *realna člana i konjugirano kompleksne članove*

$$x_{\alpha_1},\ x_{\alpha_1+1} \quad \textit{odnosno} \quad x_{\alpha_2},\ x_{\alpha_2+1}$$

pri čemu vrijedi

(1) $$|x_1| \ll |x_2| \ll \cdots \leq |x_{\alpha_1}| = |x_{\alpha_1+1}| \leq \cdots \leq |x_{\alpha_2}| = |x_{\alpha_2+1}| \leq \cdots \leq |x_n|,$$

tada se realni članovi x_ρ *izračunavaju kao i u* § 2.3.5.

Ako je $x_{\alpha_p} = r_p(\cos\varphi_p + i\sin\varphi_p)$ $(p=1, 2)$, *te* $r_1 < r_2$, *tada se* r_p *izračuna iz*

(2) $$r_p = (A_{\alpha_p-1}^{-1} A_{\alpha_p+1}^{-1})^{\frac{1}{2s}};$$

argumenti φ_p *izračunavaju se iz*

(3) $$2r_1\cos\varphi_1 + 2r_2\cos\varphi_2 = -a_{n-1} a_n^{-1} - \sum_\nu x_\nu^{-1}$$

(3^T) $$2r_1^{-1}\cos\varphi_1 + 2r_2^{-1}\cos\varphi_2 = -a_1 a_0^{-1} - \sum_\nu x_\nu^{-1};$$

pri tom* ν *prolazi brojevima* 1, 2, ..., *n izostavljajući

$$\alpha_1,\ \alpha_1+1,\ \alpha_2,\ \alpha_2+1.$$

Dokaz je sličan kao u § 2.3.5; jedino u vezi s relacijom (3^T) treba napomenuti da ona izlazi promatrajući dualni polinom

$$a^T(x) = a_n + a_{n-1}x + \cdots + a_2 x^{n-2} + a_1 x^{n-1} + a_0 x^n$$

kojemu je spektar $= S^{-1} = x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}$; zato relacija ($3^T$) znači isto što i relacija (3) primjenjena na polinom $a^T(x)$ (umjesto na polinom $a(x)$).

2.3.8. Ako realni polinom $a(x)$ ima 3 para nerealnih nulišta

$$x_{\alpha_p} = r_p(\cos\varphi_p + i\sin\varphi_p),\ (p=1,\ 2,\ 3),$$

tada se r_p izračunava kao i maloprije; argumente φ_p u sklopu

$$z_p = 2r_p\cos\varphi_p = x_{\alpha_p} + \bar{x}_{\alpha_p} \quad \text{izračunavamo iz jednadžbi}$$

$$\sigma_1(x_1, \ldots, x_n) = -a_{n-1}a_n^{-1},\ \sigma_{n-1} = a_1 a_n^{-1};$$

iz tih jednadžbi izrazimo z_1, z_2 linearno pomoću z_3 što uvršteno u

$$\sigma_2 = a_{n-2}a_n^{-1},\ \sigma_{n-2} = a_2 a_n^{-1}$$

daje 2 kvadratne jednadžbe za z_3; iz njihove najveće zajedničke mjere izračunava se z_3.

2.3.9. Modifikacija D L M-metode.[1]

Provedimo za zadanu jednadžbu $a(x)=0$ supstituciju $x=z+h$ pretpostavljajući da je broj h tako mali da u računima možemo zanemariti $h^2, h^3, \ldots$ Time $a(x)=0$ prelazi približno u jednadžbu

$$b(z) \equiv a(z) + a'(z)h = 0.$$

Provede li se s ovom jednadžbom $\square$-postupak uzastopce k puta, dobit će se određene jednadžbe oblika

$$b^{\square}(z) = a^{\square}(z) = 2hp^{[1]}(z) = 0$$

$$b^{\square^2}(z) = a^{\square^2}(z) + 2^2 hp^{[2]}(z) = 0$$

$$\cdots\cdots\cdots\cdots$$

$$B(z) = A(z) + shp^{[k]}(z) = 0;$$

stavili smo $a^{\square^k} = A$, $b^{\square^k} = B$; $s = 2^k$.

Za realno nulište $-x_\nu^s$ od $A(x)$ odnosno nulište $-z_\nu^s$ od $B(z)$ približno je

(1) $$x_\nu^s = A_{\nu-1}A_\nu^{-1}$$

odnosno

$$z_\nu^s = \frac{A_{\nu-1} + hsp_{\nu-1}^{[k]}}{A_\nu + hsp_\nu^{[k]}} = \frac{A_{\nu-1}}{A_\nu}\cdot\frac{1+hsP_{\nu-1}}{1+hsP_\nu} \quad \text{pri čemu je} \quad P_\nu = \frac{p_\nu^{[k]}}{A_\nu},\quad p_n^{[k]} = 0.$$

[1] S. Brodetsky—G. Smeal, On Graeffe's method for complex roots of algebraic equations, Proc. Cambridge Phil. Soc. 22 (1924), 83—87.

Približno je

$$z_\nu^s \doteq \frac{A_{\nu-1}}{A_\nu}[1 + hs(P_{\nu-1} - P_\nu)]$$

jer

$$(1 + hsP_{\nu-1})(1 - hsP_\nu + h^2 s^2 P_\nu^2 - + \cdots) \doteq 1 + hs(P_{\nu-1} - P_\nu);$$

pri tom smo izraz $(1 + hsP_\nu)^{-1}$ razvili u geometrijski red.

S druge strane je

$$z_\nu^s = (x_\nu - h)^s \doteq x_\nu^s - hsx_\nu^{s-1} = x_\nu^s(1 - hsx_\nu^{-1}) = A_{\nu-1} A_\nu^{-1}(1 - hsx_\nu^{-1}).$$

Dakle je

$$A_{\nu-1} A_\nu^{-1}(1 - hsx_\nu^{-1}) = z_\nu^s = A_{\nu-1} A_\nu [1 + hs(P_{\nu-1} - P_\nu)];$$

odatle izlazi približna vrijednost x_ν a ne samo približna vrijednost $|x_\nu|$:

$$x_\nu = -(P_{\nu-1} - P_\nu)^{-1}.$$

To je tako za realno rješenje x_ν. Za kompleksno rješenje

$$x_\nu = r(\cos\varphi + i\sin\varphi)$$

dobije se analogno

$$r = +(A_{\nu-1} A_{\nu+1}{}^{-1})^{\frac{1}{2s}}, \quad \cos\varphi = -\frac{r}{2}(P_{\nu-1} - P_{\nu+1}).$$

2.3.10. Primjer[1]. DLG-metodom riješiti

$$1 + 2x - 3x^2 + 6x^3 - 4x^4 + x^5 = 0.$$

Shema računanja

korak k	a_0	a_1	a_2	a_3	a_4	a_5
0	1	2	-3	6	-4	1
1	1	10	-23	16	4	1
2	1	146	217	460	-16	1
3	1	20 882	$-87\,263$	218 836	-664	1
4	1	$4{,}36232 \cdot 10^{8}$	$-1{,}52464 \cdot 10^{9}$	$4{,}77734 \cdot 10^{10}$	3 224	1
5	1	$1{,}90298 \cdot 10^{17}$	$-3{,}93560 \cdot 10^{19}$	$2{,}28230 \cdot 10^{21}$	$-9{,}55364 \cdot 10^{10}$	1
6	1	$3{,}62133 \cdot 10^{34}$	$6{,}84261 \cdot 10^{38}$	$5{,}20889 \cdot 10^{42}$	$4{,}56260 \cdot 10^{21}$	1
7	1	$1{,}31140 \cdot 10^{69}$	$0{,}85493 \cdot 10^{77}$	$2{,}71325 \cdot 10^{85}$	$1{,}03995 \cdot 10^{43}$	1
8	1	$1{,}71977 \cdot 10^{138}$	$-6{,}38541 \cdot 10^{154}$	$7{,}36173 \cdot 10^{170}$	$0{,}53885 \cdot 10^{86}$	1
9	1	$2{,}95761 \cdot 10^{276}$	$1{,}54525 \cdot 10^{309}$	$5{,}41951 \cdot 10^{341}$	$1{,}43124 \cdot 10^{171}$	1

[1] Primjer je uzet iz djela И. С. Березин—М. П. Жидков, Методы вычислений II, Москва 1962, 670 (str. 112—114).

$$x_1{}^{512} = \frac{1}{2{,}95761} \cdot 10^{-276}; \qquad 512 \lg |x_1| = -276{,}47094;$$

$$\rho_2{}^{1024} = 5{,}41951 \cdot 10^{341}; \qquad 1024 \lg \rho_2 = 341{,}73396;$$

$$\rho_1{}^{1024} = \frac{2{,}95761}{5{,}41951} \cdot 10^{-65}; \qquad 1024 \lg \rho_1 = -65{,}263019;$$

$\lg |x_1| = -0{,}53998$; dakle (primjenom Descartesova teorema) $x_1 = -0{,}28841$;

$\lg \rho_2 = 0{,}33372$; $\qquad \rho_2 = 2{,}15637$;

$\lg \rho_1 = 1{,}93627$ $\qquad \rho_1 = 0{,}86351$;

$$-0{,}28841 + 4{,}31274 \cos \varphi_2 + 1{,}72702 \cos \varphi_1 = 4;$$

$$\frac{-1}{0{,}28841} + \frac{2 \cos \varphi_2}{2{,}15637} + \frac{2 \cos \varphi_1}{0{,}86351} = -2;$$

$\cos \varphi_2 = 0{,}88213$; $\quad \cos \varphi_1 = 0{,}28927$; $\quad \sin \varphi_2 = 0{,}47101$; $\quad \sin \varphi_1 = 0{,}95992$;

$$x_{1,2} = 0{,}24201 \pm 0{,}82890\,i \qquad x_{3,4} = 1{,}90219 \pm 1{,}01568\,i;$$

3. OKO NULIŠTA KOJEMU JE APSOLUTNA VRIJEDNOST MAKSIMALNA. MAKSIMALNA SVOJSTVENA VRIJEDNOST MATRICE

3.1. Označimo sa x_n nulište polinoma $a(x)$ stepena n sa svojstvom da za svako drugo nulište x_ν od $a(x)$ vrijedi $|x_\nu| \leq |x_n|$. Korijen x_n znamo odrediti. Ako je $|x_\nu| \ll |x_n|$ i ako je x_n realno, tada x_n približno zadovoljava jednadžbu $a_{n-1}x + a_n = 0$ (§ 2.3.1).

Ako $|x_n|$ nije znatno veće od ostalih brojeva $|x_\nu|$, tada se metodom Lobačevskog iz § 2 tvore polinomi $a^\square$, $a^{\square 2}, \ldots$ pa se onda nađe x_n. Slično je ako x_n nije realan broj.

3.2. Dominantna svojstvena vrijednost matrice.

3.2.1. Specijalno se na taj način može za zadanu kvadratnu matricu a obrađivati svojstvena jednadžba

$$\det(\lambda - a) = 0 \text{ i naći njen spektar } S_a = (\lambda_1, \lambda_2, \ldots, \lambda_n).$$

Međutim, u nekim slučajevima može se do λ_n doći direktno i brzo. Vrijedi

⟶ 3.2.2. T e o r e m[1]. *Ako kvadratna realna matrica a konačna formata* (n, n) *dopušta svojstvenu bazu* $e=(e_1, \dots e_n)$, *tj. bazu od s v o j s t v e n i h vektora* e_ν, $(\nu = 1, 2, \dots, n)$, *pa ako je svojstvena dominantna vrijednost* λ_n *realna i prosta, tada za proizvoljan vektor* v *sa svim komponentama* $\neq 0$ (*npr. za* $v = e_1 + e_2 + \cdots + e_n$) *niz smjerova vektorâ*

$$v, \; v^{(1)} = av, \dots, \; v^{(k+1)} = av^{(k)}, \dots$$

konvergira prema jediničnom svojstvenom vektoru e_n *koji je pridružen dominantnoj svojstvenoj vrijednosti* λ_n; *drugim riječima, niz jediničnih vektora*

$$\operatorname{sgn} a^k v \overset{\text{def}}{=} \frac{1}{|a^k v|} a^k v$$

konvergira prema određenom jediničnom svojstvenom vektoru e_n *matrice* a; *pripadna svojstvena vrijednost* λ_n *je dominantna. Približno je*

$$a^{k+1} v \doteq \lambda_n a^k v \tag{1}$$

za svako dosta veliko k, *što znači da je približno* $a^k v$ *svojstven vektor vezan za svojstvenu vrijednost* λ_n *matrice* a.

Praktički se svojstven par $(\lambda_n, v^{[n]})$ *traži ovako: pođe se od konstantnog vektora*

$$v = [1, \dots, 1]^T; \quad \textit{nađe se} \quad v^{(1)} = av; \tag{2}$$

„normalizira“ se $v^{(1)}$ *i nađe*

$$w_1^{(1)} = (v_{n'}^{(1)})^{-1} v^{(1)},$$

tj. $v^{(1)}$ *se dijeli svojom određenom* n' *komponentom; traži se*

$$v^{(2)} = aw^{(1)}, \; w^{(2)} = (v_{n'}^{(2)})^{-1} v^{(2)}, \; v^{(k+1)} = aw^{(k)}, \; w^{(k+1)} = (v_{n'}^{(k+1)})^{-1} v^{(k+1)}, \dots$$

Prvi put kad je, približno, vektor $v^{(k+1)}$ *proporcionalan s vektorom* $v^{(k)}$, *tj. kad je približno*

$$w^{(k+1)} \doteq w^{(k)}, \tag{3}$$

bit će $v^{(k)}$ *približno svojstveni vektor, a broj* $v_{n'}^{(k)}$ *je približno tražena dominantna svojstvena vrijednost* λ_n, *tj.*

$$v_{n'}^{(k)} \doteq \lambda_n. \tag{4}$$

Pri tom je n' *fiksan broj u nizu* $1, 2, \dots, n$; *npr.* $n' = n$.

D o k a z. Iz (2), tj. iz $v = \sum_{\nu=1}^{n} e_\nu$ za neku *svojstvenu* bazu $(e_1, \dots e_n)$ izlazi

$$av = \Sigma\, ae_\nu = \Sigma\, \lambda_\nu e_\nu$$

---

[1] Richard von Mises—Hilda Geisinger, Zeitschrift f. angewandte Math. u. Mechanik 9 (1929) 58—77, 152—164.

pri čemu je λ_ν svojstvena vrijednost, a e_ν pripadni svojstveni vektor matrice a; isto tako za svako k vrijedi

$$a^k v = \sum_\nu \lambda_\nu^k e_\nu.$$

Dakle je

$$\operatorname{sgn} a^k v = \sum_{\nu=1}^{n} b_{\nu k} e_\nu,$$

gdje je

$$b_{\nu k} = \frac{\lambda_\nu^k}{(\sum_i \lambda_i^{2k})^{1/2}} = \frac{(\lambda_\nu \lambda_n^{-1})^k}{(\sum_i [\lambda_i \lambda_n^{-1}]^{2k})^{1/2}}.$$

Odatle zbog

$$|\lambda_\nu \lambda_n^{-1}| < 1 \text{ za } \nu \neq n \text{ izlazi } \lim_{k\to\infty} b_{\nu k} = 0 \quad \text{za} \quad \nu \neq n$$
$$= 1 \quad \text{za} \quad \nu = n.$$

Prema tome,

$$\lim_{k\to\infty} \operatorname{sgn} a^k v = \sum_{\nu=1} (\lim_{k\to\infty} b_{\nu k})\, e_\nu = e_n.$$

Dokažimo da za dosta visoko k vrijedi približno

$$a^{k+1} v \doteq \lambda_n a^k v, \quad \text{tj.}$$

$$(a^{k+1} v)_\nu = \lambda_n (a^k v)_\nu \quad (\nu = 1, 2, \ldots, n).$$

Naime,

$$a^k v = \sum_{\nu=1}^{n} \lambda_\nu^k e_\nu = \lambda_n^k [e_n + \sum_{\nu=1}^{n-1} (\lambda_\nu \lambda_n^{-1})^k];$$

kako $[\,.\,] \to e_n$ kad $k \to \infty$, znači da je približno $a^k v \doteq \lambda_n^k e_n$ za svako dovoljno visoko k. Specijalno,

$$a^{k+1} v \doteq \lambda_n^{k+1} e_n = \lambda_n (\lambda_n^k e_n) = \lambda_n a^k v.$$

Time je (1) dokazano.

Dokažimo relaciju (4). No, broj $(v^k)_{n'} = c_{n'}$ jer faktor proporcionalnosti pri prelazu od vektora v^k na vektor $v^{k+1} = a\left(\frac{v^k}{c_{n'}}\right) = aw^k$; taj faktor je isti kao i pri prelazu od $a^k v$ na $a^{k+1} v$ koji je prema (1) jednak λ_n; dakle je zaista $c_{n'} = \lambda_n$. tj. (4) vrijedi.

Time je teorem potpuno dokazan.

3.2.3. O daljim rezultatima o spektru matrice v. npr. D. K. Faddeev-V. N. Faddejeva [1], 348—676 kao i E. Bodewig [1] 267—439.

3.2.4. Kako se svaki algebarski polinom $p(x)$ može shvatiti i kao karakteristična jednadžba određene kvadratne matrice „svoje pratilice“ (27, § 8.6), mogu se gornji rezultati primijeniti i na pojedine algebarske polinome.

3.2.5. Primjer[1]. Za narednu matricu a naći približno λ_n i $v^{[n]}$, tj. naći dominantni svojstveni par $(\lambda_n, v^{[n]})$.

Zadana matrica $a=$					$\lambda\max = \lambda_n$
	5	6	5	4	
	6	10	12	11	
	5	12	15	14	
	4	11	13	16	
v	1	1	1	1	—
$v^{(1)}$	20	39	46	45	—
$w^{(1)}$	0,444444	0,866667	1,022222	1	45
$v^{(2)}$	16,533338	34,599998	41,955554	41,622221	—
$w^{(2)}$	0,397224	0,831287	1,008009	1	41,622221
$v^{(3)}$	16,013887	33,792322	41,081699	40,845179	—
$w^{(3)}$	0,392063	0,827327	1,005791	1	40,845179
$v^{(4)}$	15,953232	33,695140	40,975104	40,749923	—
$w^{(4)}$	0,391491	0,826876	1,005526	1	40,749923
$v^{(5)}$	15,946341	33,684018	40,962857	40,738964	—
$w^{(5)}$	0,391427	0,826826	1,005496	1	40,738964
$v^{(6)}$	15,945571	33,682774	40,961487	40,737738	—
$w^{(6)}$	0,391420	0,826820	1,005492	1	40,737738
$v^{(7)}$	15,945480	33,682624	40,961320	40,737588	—
$w^{(7)}$	0,391419	0,826819	1,005492	1	40,737588
$v^{(8)}$	15,945469	33,682608	40,961303	40,737573	—
$w^{(8)}$	0,391419	0,826819	1,005492	1	40,737573

Dakle je $\lambda_n \doteq 40{,}737573$, $\quad v^{[n]} = v^{(8)}$

3.3. Slučaj pozitivno definitnih matrica (spektar $0 < x_1 < x_2 < \cdots < x_n$). Za takve matrice može se λ_n ocijeniti na razne načine pomoću tragova matrice.

3.3.1. Teorem. *Ako je kvadratna matrica pozitivno definitna, tada je*

$$\lambda_n = \lim_{k\to\infty} \operatorname{Tr}(a^k)^{1/k}; \text{ pri tom je } \operatorname{Tr} a = \sum_{\nu=1}^{n} a_{\nu\nu} \qquad \text{(isp. 27 § 8.1).}$$

Kako je naime

$$\operatorname{Tr} a = \lambda_1 + \lambda_2 + \cdots + \lambda_n \qquad \text{(isp. pogl. 27. § 8,1),}$$

$$\operatorname{Tr} a^k = \lambda_1^k + \lambda_2^k + \cdots + \lambda_n^k \qquad \text{(isp. pogl. 27, § 5.3),}$$

bit će

$$\lambda_n^k \leq \operatorname{Tr} a^k = \lambda_n^k \left[1 + \sum_{\nu=1}^{n-1} (\lambda_\nu \lambda_n^{-1})^k\right]; \qquad \text{dakle je}$$

$$\lambda_n \leq (\operatorname{Tr} a^k)^{1/k} = \lambda_n \left[1 + \sum_{\nu=1}^{n-1} ((\lambda_\nu \lambda_n)^{-1})^k\right]^{1/k}.$$

Kako izraz $[\ ] \to 1$ za $k \to \infty$ znači da $[\ ]^{1/k} \to 1$ za $k \to \infty$, pa je teorem dokazan.

3.3.2. Teorem (S. N. Bernštajn, 1939). *Za pozitivno definitne realne (n, n)-matrice vrijedi*

$$2^{-\frac{1}{k}} \left\{ \operatorname{Tr} a^k \left[1 + \left(2 \frac{\operatorname{Tr} a^{2k}}{\operatorname{Tr} a^k} - 1 \right)^{\frac{1}{2}} \right] \right\}^{\frac{1}{k}} < \lambda_{\max} < + \left(\operatorname{Tr} a^k \right)^{\frac{1}{k}}.$$

[1] Primjer je uzet iz knjige: А. Ф. Смирнов, Устойчивость и колебания сооружений, Москва, 1958, 572; str. 104—105.

Dokaz se može pogledati na str. 100—103 knjige citirane u prethodnoj bilješki.

3.4. Slučaj bilo kakvih kompleksnih ili realnih matrica. Navedimo nekoliko činjenica o spektru σ_a matrice a formata (n, n); inače vrijednosti a_{ij} mogu biti i kompleksne. Specijalno vrijedi 3.4.1.

—→ **3.4.1. Teorem (Geršgorin, 1931).**[1] *Svaka svojstvena vrijednost kvadratne matrice a s kompleksnim komponentama a_{ij} leži u uniji Ga zatvorenih krugova $K(a_{ii}; \leq R_i)$, gdje je*

$$R_i = \sum_{i \neq j=1}^{n} |a_{ij}|.$$

Dokaz. Neka je λ određena svojstvena vrijednost od a; neka je x pripadni svojstveni vektor, dakle $x \neq \vec{0}$ te $ax = \lambda x$; dakle je

$$\sum_j a_{ij} x_j = \lambda x_i, \quad \text{odnosno} \quad \sum_{i \neq j=1}^{n} a_{ij} x_j = (\lambda - a_{ii}) x_i \quad (i = 1, 2, \ldots, n).$$

Neka je $\sup |x_i| = |x_m|$; dakle je $m \in \{1, 2, \ldots, n\}$. Tada gornja jednadžba za $i = m$ podijeljena sa x_m daje

$$\lambda - a_{mm} = \sum_{m \neq j=1}^{n} a_{mj} \frac{x_j}{x_m}. \qquad \text{Odatle}$$

$$|\lambda - a_{mm}| \leq \Sigma |a_{mj}| \cdot \left|\frac{x_j}{x_m}\right| \leq \left(\text{zbog} \left|\frac{x_j}{x_m}\right| \leq 1\right) \leq \sum_{j \neq m} |a_{mj}| = R_m.$$

Dakle zaista $\lambda \in K(a_{mm}; \leq R_m)$; pri tom $m = m(\lambda)$ zavisi od λ; kad λ_ν prolazi spektrom σ_a, dobivamo krugove $K(\lambda_\nu)$, pa je zato $\sigma_a \subset \bigcup_\nu K(\lambda_\nu)$.

3.4.2. Teorem. *Najmanji zatvoreni krug oko 0 koji obuhvata Geršgorinov skup Ga pridružen matrici a jest $K(0, \leq \|a\|_{\mathrm{I}})$ pri čemu je*

$$\|a\|_{\mathrm{I}} = \sup_{i=1,2,\ldots,n} \sum_{j=1}^{n} |a_{ij}|.$$

Naime iz

$$|z - a_{mm}| \leq R_m \text{ izlazi } |z| \leq |a_{mm}| + R_m, \qquad \text{dakle}$$

$|z| \leq \sup_m \{|a_{mm}| + R_m\} = \|a\|_{\mathrm{I}}$; pri tom je $\|a\|_{\mathrm{I}} = |a_{ii}| + R_i$ za neko $i \in \{1, \ldots, n\}$, pa se kružnica $K(O, \|a\|_{\mathrm{I}})$ i skup G_a dodiruju.

—→ **3.4.3. Teorem.** *Svaka svojstvena vrijednost kvadratne konačne matrice a je po apsolutnoj vrijednosti*

$$\leq \|a\|_{\mathrm{I}}; \quad \textit{specijalno je} \quad |\lambda_m| \leq \|a\|_{\mathrm{I}}.$$

[1] S. A Geršgorin, Über die Abgrenzung der Eigenwerte einer Matrix, Izvestia A. N. S. S. S. R., ser. mat. 7 (1931) 749—754; isp. Faddeev—Faddeeva [1] str. 139.

4. GRAFIČKO RJEŠAVANJE JEDNADŽBI

Osim *numeričkog i algebarskog* rješavanja jednadžbi često se služimo i *grafičkim* rješavanjem. Pri tom je važno da se *crtanjem* iskoriste podaci jednadžbe i onda *crtanjem* pokažu tražena rješenja.

4.1. Rješenja jednadžbi $a(x,y)=0$, $b(x,y)=0$ jesu koordinate sjecištâ tih dviju krivulja; tako npr. $|x|+|y|-1=0$

$$|x|-|y|=0$$

imaju 4 rješenja i to su tačke u kojima simetrale $y=x$ odnosno $y=-x$ sijeku omeđenje kvadrata s vrhovima $(0, \pm 1)$, $(\pm 1, 0)$; rješenja su oblika

$$\left(\pm\frac{1}{2}2^{\frac{1}{2}},\quad \pm\frac{1}{2}2^{\frac{1}{2}}\right).$$

4.2.1. Realna rješenja jednadžbe $a(x)=0$ jesu apscise sjecišta krivulje $y=a(x)$ i apscisne osi; pri tom funkcija $a(x)$ može biti i nealgebarska, dakle transcendentna.

4.2.2. Realna rješenja jednadžbe $a(x)=b(x)$ jesu apscise sjecišta krivulje $y=a(x)$ i krivulje $y=b(x)$.

4.2.3. Tako npr. realna rješenja kvadratne jednadžbe $x^2+px+q=0$ jesu apscise sjecišta parabole $y=x^2$ i pravulje $y=-px-q$.

4.2.3.1. Ako je

$$A=(0,\ 1),\qquad B=\left(-\frac{b}{a},\ \frac{c}{a}\right),$$

tada tačke $(x_1,\ 0)$, $(x_2,\ 0)$ kružnice k kojoj je $\overline{AB}$ prečnik jesu nulišta trinoma ax^2+bx+c; naime, jednadžba kružnice k glasi

$$\left(x+\frac{b}{2a}\right)^2+\left(y-\frac{a+c}{2a}\right)^2=\frac{b^2+(a-c)^2}{4a^2}$$

odakle za $y=0$ izlaze rješenja x_1, x_2.

4.2.4. Isto tako, realna rješenja jednadžbe $x^n+px+q=0$ dobiju se grafički kao apscise sjecišta parabole $y=x^n$ i pravulje $y=-px-q$.

4.2.5. Kubnu jednadžbu

(1) $$a_3x^3+a_2x^2+a_1x+a_0=0,$$

tj. jednadžbu

$$x(a_3x^2+a_2x+a_1)+a_0=0$$

možemo *grafički* rješavati kao sistem

(2) $$y=a_3x^2+a_2x+a_1 \quad \text{(parabola)}$$

$$xy+a_0=0 \qquad \text{(hiperbola).}$$

Dakle, apscisa svakog sjecišta parabole (2) i hiperbole (3) daje realno rješenje jednadžbe (1).

4.2.6. Normirana jednadžba 4. stepena. Jednadžbu

(1) $$x^4 + a_2 x^2 + a_1 x + a_0 = 0$$

možemo riješiti stavljajući

(2) $$y = x^2$$

(3) $$y^2 = a_2 y + a_1 x + a_0 = 0,$$

Prema tome se radi o apscisi svakog sjecišta parabole (2) i parabole (3). Iz (2), (3) također izlazi zbrajanjem

(4) $$x^2 + y^2 + (a_2 - 1) y + a_1 x + a_0 = 0.$$

To je jednadžba kružnice; nju je relativno lako nacrtati. *Apscise sjecišta parabole* (2) *i kružnice* (4) *jesu realna rješenja jednadžbe* (1).

4.3. Kako se crta krivulja $y = a(x)$? Radimo u Descartesovoj koordinatnoj ravnini i neka su e_1, e_2 osnovni radijus-vektori (obično je $e_1 \perp e_2$; vektori e_1, e_2 ne moraju biti jednake duljine).

4.3.1. Obradimo slučaj da je u pitanju polinom

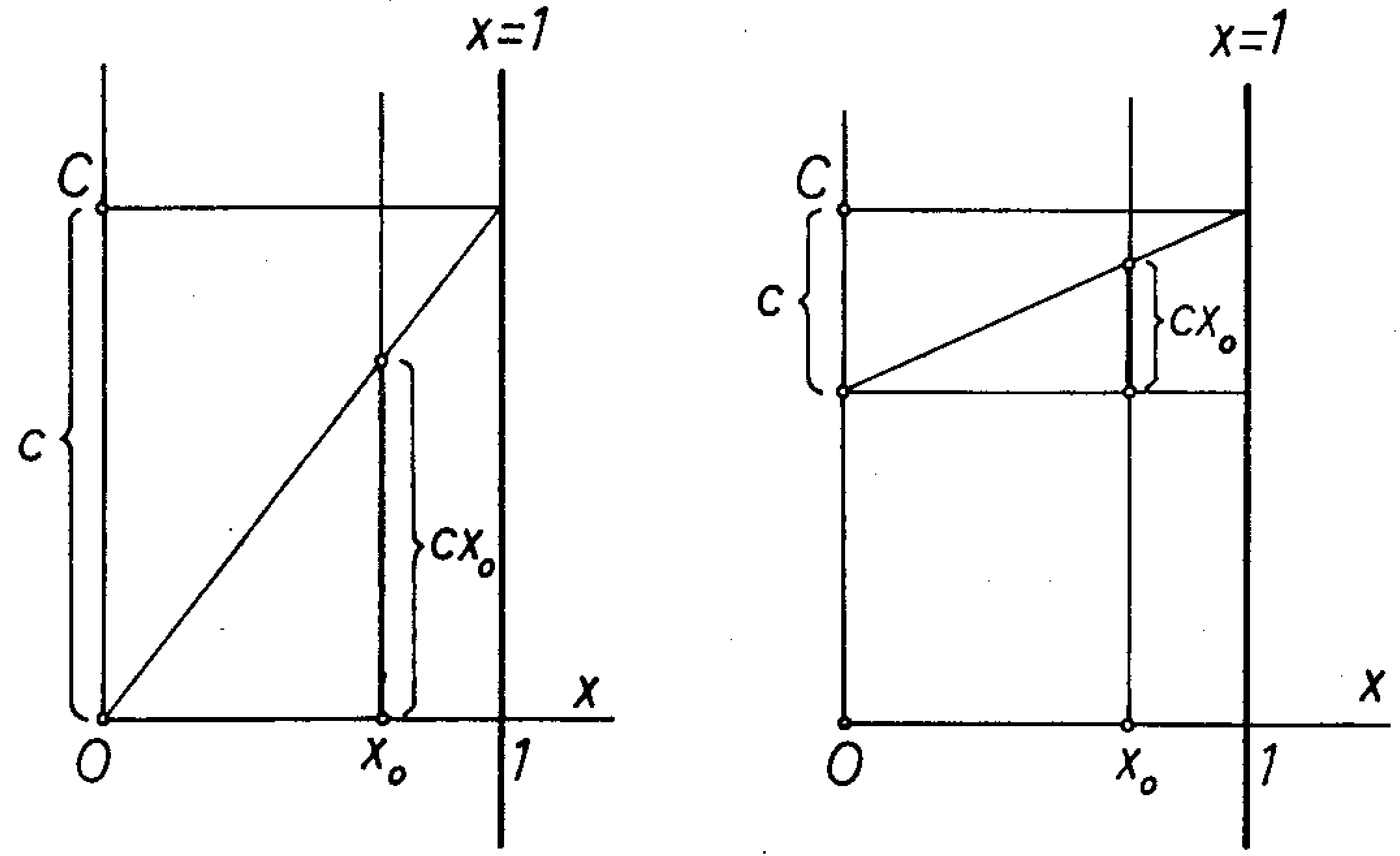
(1) $$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n, \quad a_n \neq 0.$$

4.3.2. Tada se vidi da je

(2) $$a(x) = a_n x + a_{n-1})_1 x + a_{n-2})_2 x + \cdots + a_2)_{n-2} x + a_1)_{n-1} x + a_0$$

(sprijeda nismo zagrade ni stavljali; inače smo ih numerirali). Prema tome, $a(x)$ se dobije množenjem i zbrajanjem; i to onim redom kako je navedeno u (2).

4.3.3. Jasno je kako se zbraja grafički. Grafičko množenje brojeva c, x_0 vrši se prema slici 4.3.3. (bilo na jedan ili na drugi način).



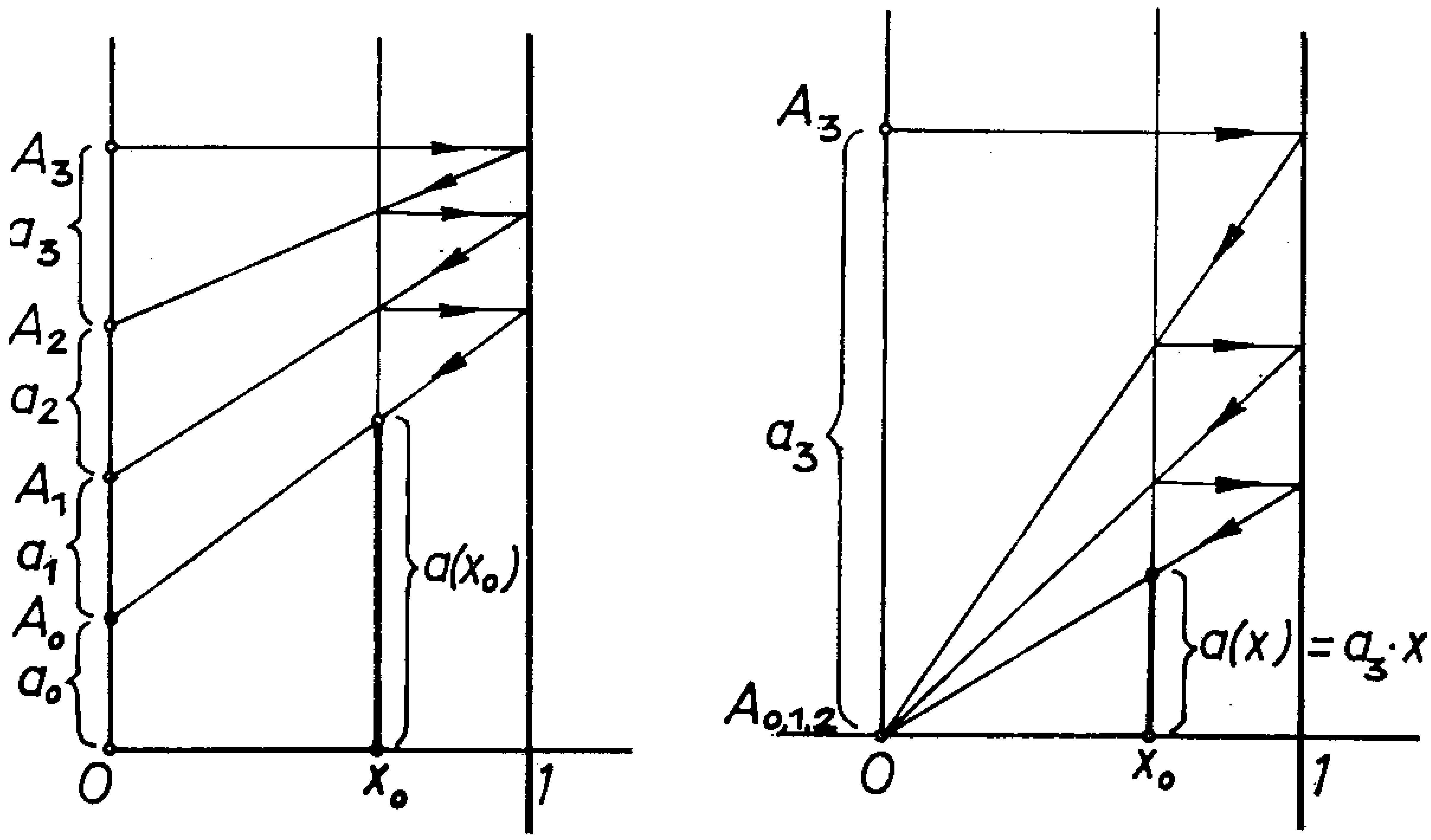
Sl. 31.4.3.3.
Kako se grafički nalazi produkt cx_0?

4.3.3.1. Pravulja $x=1$, tj. paralela s vektorom e_2 završnom tačkom radijus-vektora e_1 ima važnu ulogu u konstrukciji (na slici ta je paralela podebljana).

4.3.3.2. Veličina $a(x_0)$ za danu vrijednost x_0 crta se na osnovu jednakosti (2) tako da su u koordinatnoj ravnini najprije na ordinatnoj osi nosiocu -vektora e_2 određene tačke $A_0, A_1 \ldots, A_n$ pomoću jednakosti:

$$\overrightarrow{OA_0}=a_0 \vec{e}_2, \ \overrightarrow{A_{\nu-1} A_\nu}=a_\nu \vec{e}_2 \quad \text{za } \nu=1, 2, \ldots, n.$$

Naravno, ako je $a_\nu=0$, onda je $A_{\nu-1}=A_\nu$; tako npr. za polinom $a(x)=x^n$ je $A_\nu=0$ za $\nu=0, 1, 2, \ldots, n-1$.



Sl. 31.4.3.4.
Grafičko određivanje vrijednosti $a(x_0)$.

Zatim se po redu provode konstrukcije koje odgovaraju operacijama na desnoj strani jednadžbe (2). Rezultat je ovaj:

4.3.4. Teorem. U opisanoj konstrukciji pri danom broju x_0 nacrtana pravulja tačkom A_0 siječe pravulju $x=x_0$ u tački kojoj je ordinata tražena vrijednost $a(x_0)$ polinoma:

$$\overrightarrow{(x_0)(a(x_0))}=a(x_0)\vec{e}_2,$$

tj. ordinata tačke $(x_0, a(x_0))$ je upravo vrijednost $a(x_0)$ polinoma $a(x)$ za danu vrijednost x_0 argumenta x.

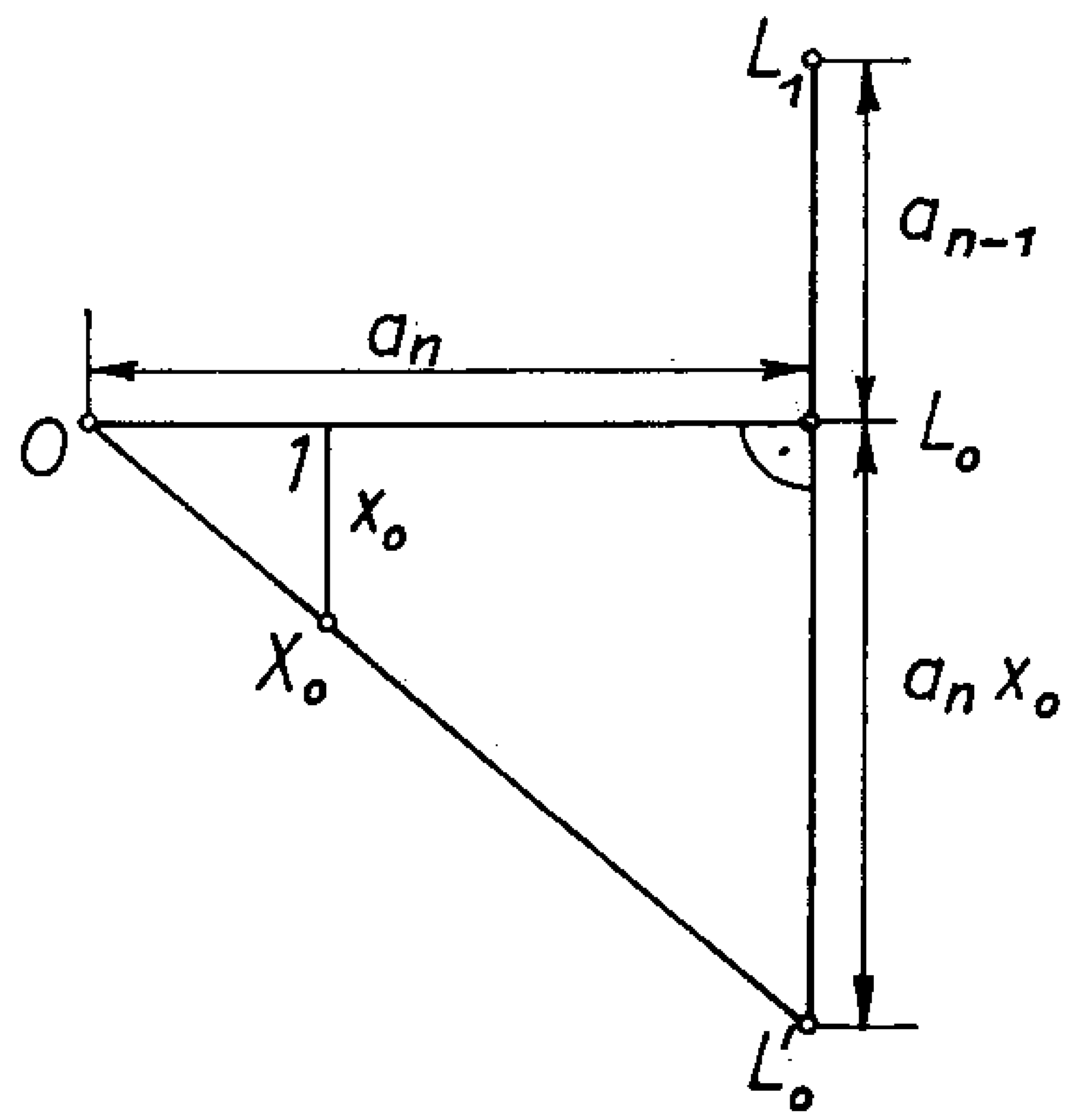
Dobro je to sagledati za $0<x_0<1$ (kao na slici), $x_0=1$ (tada je $\overrightarrow{0A_n}=a(1)\cdot\vec{e}$), za $1<x_0$, $x_0=-1$ itd.

4.3.5. Primjedba. Pri konstrukciji vrijednosti $a(x_0)$ i inače važnu ulogu, osim koordinatnih osa, igraju ove 3 pravulje:

pravulja $x=x_0$, pravulja $x=1$ i pravulja $y=x$ (spojnica tačaka $(0,0)$, $(1,1)$).

Prva pravulja se mijenja promjenom argumenta x; *preostale dvije pravulje su fiksne za čitavu sliku* $y=a(x)$, *odnosno za čitavu funkciju* $a(x)$.

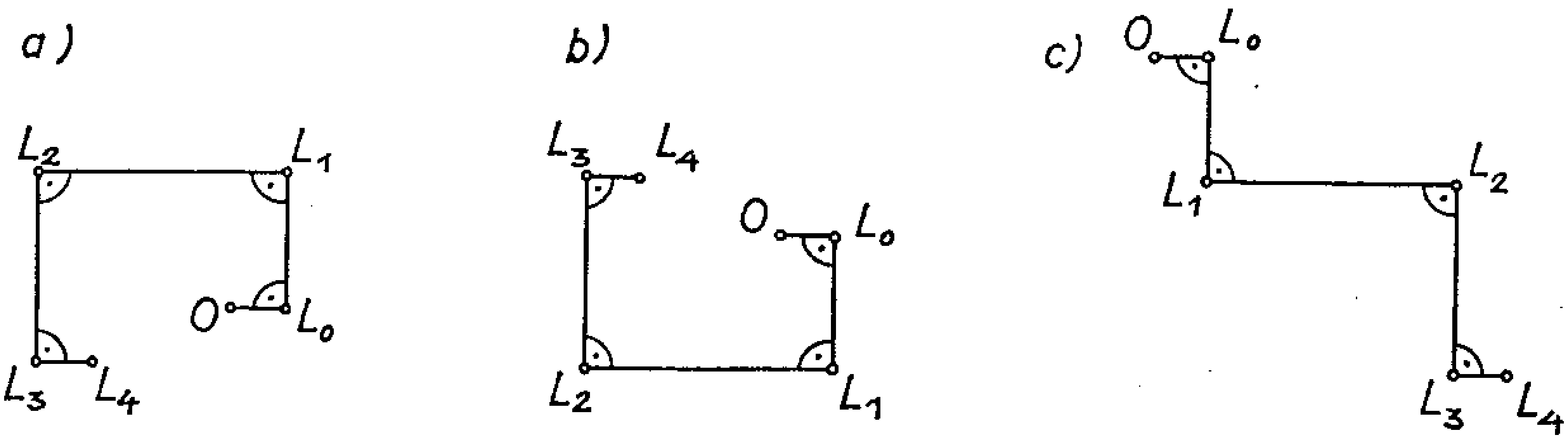
4.4. Lillova konstrukcija[1] broja $a(x_0)$ i traženje približne vrijednosti nulišta polinoma $a(x)$. Oslanja se na ovu konstrukciju početnih dvaju koraka u operacijama (2) kao na sl. 4.4.



Sl. 31.4.4.

4.4.1. Odabiranje koordinatne baze u ravnini. Polazimo od radijus-vektora j koji uzimamo jediničnim; drugi vektor ćemo dobiti iz j rotirajući j za $+\pi/2$ te ga formalno označiti sa ij (i je imaginarna jedinica); uopće za neki radijus-vektor v neka iv označuje onaj radijus-vektor koji iz v nastaje rotacijom oko 0 za $\pi/2$ radijana. Tako imamo vektore $j, ij, i^2j=-j, i^3j=-ij, i^4j=j$, tj.

$$\begin{array}{c|c|c} & \overleftarrow{\quad\quad} & \\ \downarrow & i^3 i \quad i^2 j & \uparrow \\ & \overrightarrow{\quad\quad} & \\ & j=i^4 j & \end{array} \quad ij;$$ dalje se vektori obnavljaju.



$x^4+2x^3+4x^2+3x+1$ $\qquad$ $x^4-2x^3+4x^2-3x+1$ $\qquad$ $x^4-2x^3-4x^2+3x+1$

Sl. 31.4.4.2.
Lillov potez napisanih polinoma.

4.4.2. Lillov potez u odnosu na polinom $a(x)=a_0+a_1x+a_2x^2+\dots+a_nx^n$, $a_n \neq 0$, jest slomljena *pravokutna crta* $L_nL_{n-1}L_{n-2}\dots L_2L_1L_0$ kojoj se niz vrhova $L_n, L_{n-1}, \dots, L_1, L_0$ određuje iz ovih jednakosti:

$$\overrightarrow{OL_0}=a_nj$$

$$\overrightarrow{L_0L_1}=a_{n-1}(ij)$$

$$\cdots\cdots$$

$$\overrightarrow{L_{\nu-1}L_\nu}=a_{n-\nu}(i^\nu j), \quad (\nu=1, 2, \dots, n).$$

[1] Našao je francuski inženjer Lill (1867).

Naravno, ako je $a_{n-1}=0$, tada je $L_{\nu-1}=L_\nu$; ako je $a_\nu<0$, tada je $a_{n-\nu}(i^\nu j)=(-a_{n-\nu})(-i^\nu j)$.

4.4.3. Određivanje veličine $a(x_0)$ za zadan broj x_0.

4.4.3.1. Prvi korak (gl. sliku 31.4.4). Odredi se orijentirani kut

$$\alpha_0=\sphericalangle(X_0\,O\,1) \text{ za koji je } -\pi/2<\alpha_0<\pi/2 \text{ te } \operatorname{tg}\alpha_0=x_0 \text{ (gl. sliku);}$$

drugi krak kuta α_0 je vektor j. U pravokutnom $\Delta\ O\,1\,X_0$ katete su 1 i $x_0=1\,X_0$. Tačka X_0 je ispod j-osi za $x_0>0$, iznad j-osi za $x_0<0$. Neka je L_0' sjecište zrake $O\,X_0$ te (ij)-osi; tada je

$$\overrightarrow{L'_0 L_0}=a_n x_0(ij), \text{ odnosno } \overrightarrow{L'_0 L_1}=(a_n x_0+a_{n-1})(ij).$$

4.4.3.2. Tačka L_0' je potpuno određena uređenom trojkom O, L_0, x_0[1]. Pa se može pisati

$$L_0'=f(O, L_0, x_0).$$

Dalje se određuju tačke $L_1', L_2', \ldots$ po propisu

$$L'_1=f(L'_0, L_1, x_0) \text{ i uopće}$$

$$L'_\nu=f(L'_{\nu-1}, L_\nu, x_0) \quad \text{za } \nu=1,2,\ldots,n-1.$$

Specijalno je za $\nu=n-1$:

$$L'_{n-1}=f(L'_{n-2}, L_{n-1}, x_0).$$

Sama vrijednost je $a(x_0)=L'_{n-1}L_n$; s obzirom na predznak vrijedi

$\longrightarrow$ **4.4.3.3. Teorem** $\overrightarrow{L'_{n-1}L_n}=a(x_0)(i^n j)$.

Teorem je posljedica relacijâ

$$L'_{n-\nu}L_{n-\nu+1}=\{a_n x_0+a_{n-1}(x_0+\cdots)x_0+a_{\nu-1}\}\cdot(i^{n-\nu}j)$$

($\nu=n, n-1, \ldots, 1$) *koje se dokazuju induktivno.*

4.4.4. Približno rješavanje jednadžbe $a(x)=0$. Kad se jednom za polinom $a(x)$ ima Lillov niz $O, L_0, L_1, \ldots, L_{n-2}, L_{n-1}, L_n$, tada su za zadani broj x_0 tačke niza

$$(x_0) \qquad L'_0, L'_1, L'_2, \ldots, L'_{n-1},$$

potpuno određene; mijenja li se x_0, mijenja se i niz (x_0); specijalno se nastoji tačka X_0 tako odabrati da veličina $L'_{n-1}L_n$ bude što manja.

Vrlo je zgodno raditi s *prozirnim milimetarskim papirom* koji se u O pričvrsti na papir na kojem je nacrtan potez $O\,L_0\,L_1\cdots L_{n-1}\,L_n$; okrećući milimetarski papir oko O i crtajući ravnalom ili prateći pogledom potez

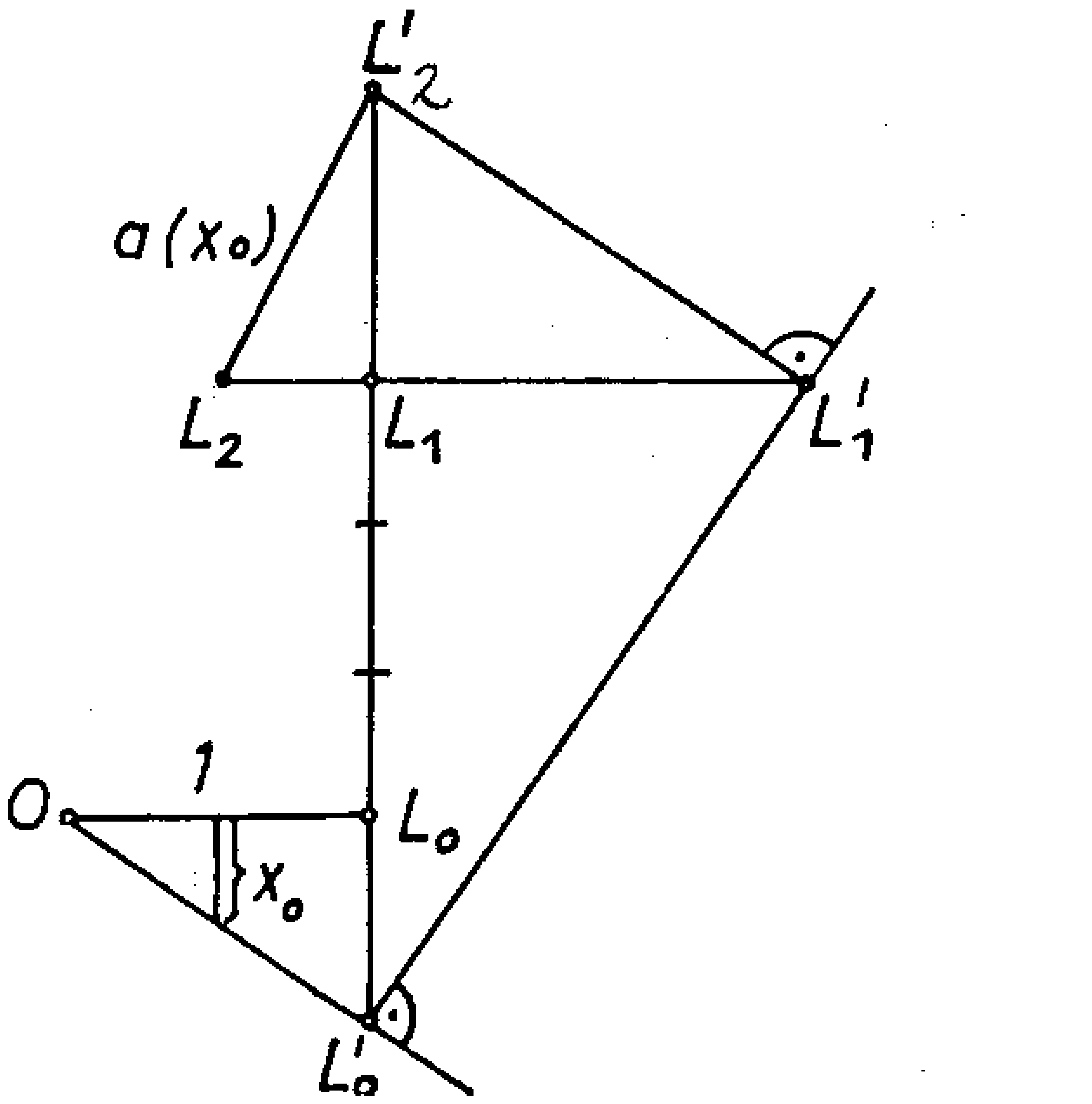
$$O\,L'_0\,L'_1,\ \ldots\ L'_{n-2}, L'_{n-1}$$

[1] Umjesto broja x_0 moglo bi se promatrati tačku X_0.

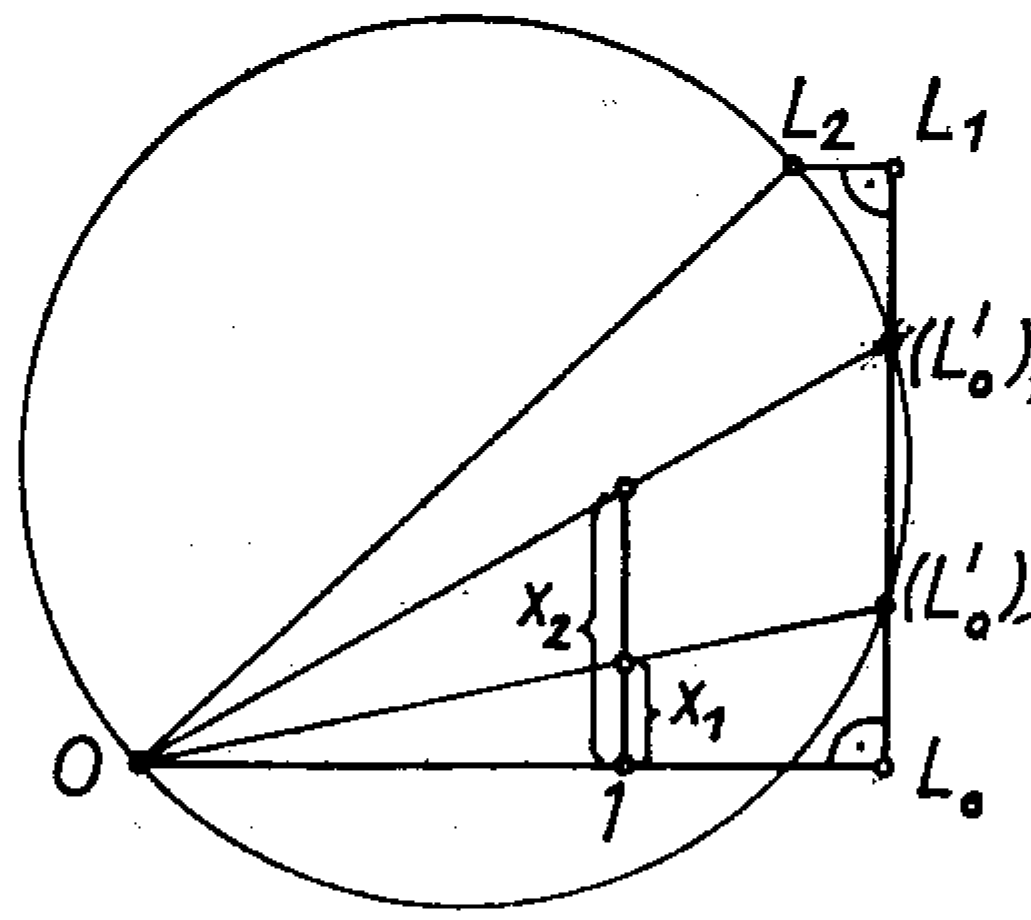
dobije se — pokušavanjem — traženi položaj tačke X_0 za koju je pripadno $L'_{n-1} L_n$ dovoljno malo, odnosno $L'_{n-1} = L_n$.

4.4.5. Slučaj kvadratnog polinoma $a_0 + a_1 x + a_2 x^2$. U slučaju kvadratnog polinoma može se tačka L'_0 odmah nacrtati kao sjecište pravulje $p = p(L_0 L_1)$ i kružnice k kojoj su O, L_2 dijametralne tačke.

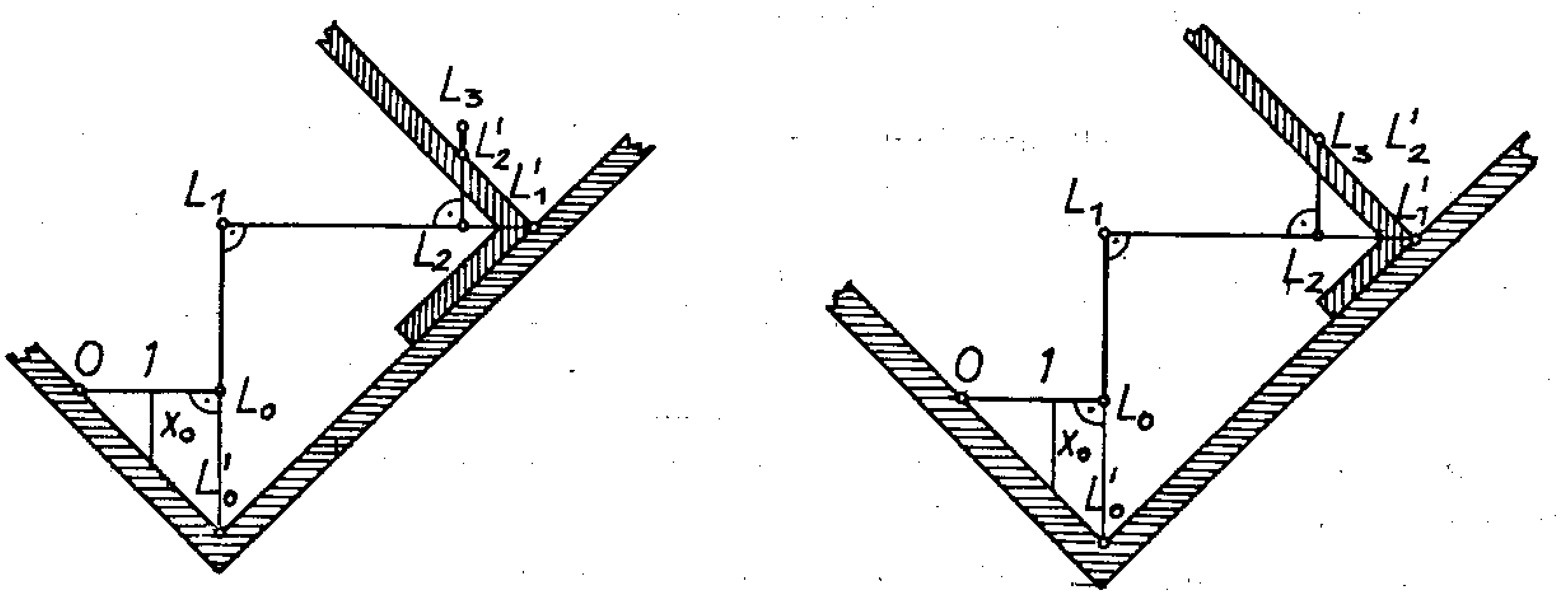
Time je naravno određena i tačka X_1 te je pripadni argument x_1 traženo nulište (primjena Talesova poučka!); na slici je $x_1 < 0$. Drugim sjecištem od k i p određeno je i drugo nulište x_2 trinoma $a(x)$. Ako su k, p bez zajedničke tačke, nulišta od $a(x)$ su nerealna. Ako se k, p dodiruju, nulište x_1 je realno i dvostruko (gl. crtež!).



Sl. 31.4.4.5. *a*) Slučaj polinoma $a(x)$ stepena 2.



Sl. 31.4.4.5. *b*)



Sl. 31.4.4.6. Slučaj kubnog polinoma $a(x)$

4.4.6. Slučaj kubne jednadžbe. Rješavanje pomoću dva prava kuta. Imamo li kubni polinom

$$a(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3, \quad a_3 \neq 0,$$

i nacrtan Lillov potez $O L_0 L_1 L_2 L_3$, tada se potez $O L'_0 L'_1 L'_2$ može odrediti *pokusno* pomoću dva *prava kuta* P, P'; mijenjajući položaj od P (tj. mijenjajući vrh L'_0 po pravulji $L_0 L_1$), mijenja se položaj drugog kuta P'; posebno se može položaj L'_0 tako udesiti da krak od P' prolazi tačkom L_3; tada je $L'_0 L_0$ traženo rješenje ukoliko je $O L_3 = 1$ (inače je broj $L'_0 L_0 : O L_0$ nulište od $a(x)$).

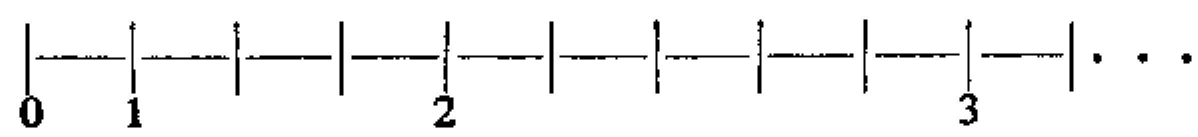
5. NOMOGRAFSKE METODE. RJEŠAVANJE POMOĆU STROJEVA

5.0. Osim *numeričkih, algebarskih i grafičkih* načina rješavanja jednadžbe imamo i *mješovite metode*, posebno *nomografske metode* rješavanja; one su zapravo *numeričko-grafičke*.

Kod *nomografskih metoda*[1] bitnu ulogu imaju funkcijske skale.

5.1. Skala zadane funkcije. — 5.1.1. Skala zadane funkcije fx nastaje tako da za zadani jedinični radijus-vektor $\overrightarrow{OE}$ nanosimo vektor $\overrightarrow{OA(x)} = f(x) \cdot \overrightarrow{OE}$, no na kraju toga vektora ***upisujemo ne vrijednost funkcije $f(x)$ nego vrijednost x argumenta.***

Tako npr. za funkciju $y = x^2$ imamo skalu kvadrata.



Pojam funkcijske skale proširuje pojam brojevne pravulje koja je zapravo funkcijska skala identične funkcije $y = x$.

5.1.2. *Funkcijska skala za prikazivanje funkcije i pripadne antifunkcije.*

Ako je na istom segmentu B naznačena ne samo skala F zadane funkcije $f(x)$ nego i obična brojevna skala B, tada se neposredno za argument x sa F očitava na B pripadno $y = f(x)$; i obratno: broju y sa B očitava se na F ono x za koje je $fx = y$. Prema tome, takva dvostruka skala služi za predočivanje funkcije f i inverzne funkcije f^{-1}.

Posebno se na logaritamskom mjerilu očitava veza $x \to \log x$ kao i obratna veza $y \to 10^y$.

5.2. Nomogram ili grafička tablica je skup određenih funkcijskih skala i crteža pomoću kojeg se iz zadanih veličina određuju na poseban način druge veličine. Prema tome, nomogram je poseban numeričko-geometrijski način prikazivanja funkcionalnih veza. Tako npr. postoji nomogram za zbrajanje, za množenje, za potenciranje, nomogram za rješavanje kvadratne jednadžbe, nomogram za rješavanje jednadžbe zadanog tipa, itd. Razvila se čitava i vrlo opsežna matematička nauka. *Nauka o nomogramima* zove se *nomografija*; nomografiju je znatno unaprijedio francuski inženjer — matematičar M. d'Ocagne (č. d'Okanj) 19/20. st.).

5.2.1. Primjer: *nomogram u vezi s relacijom*

(1) $$b^a = c,$$

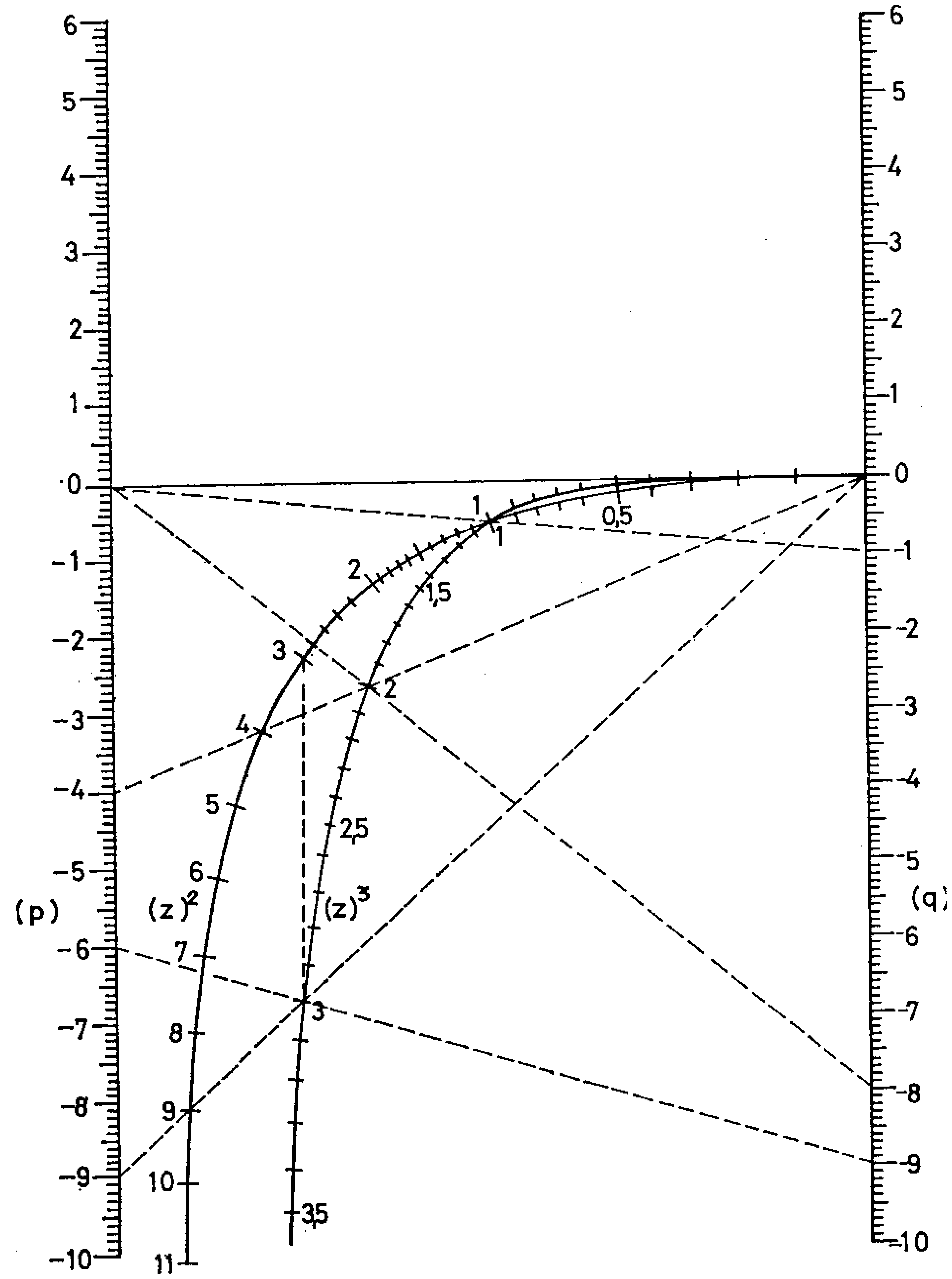
odnosno

(2) $$a \log b = \log c.$$

---

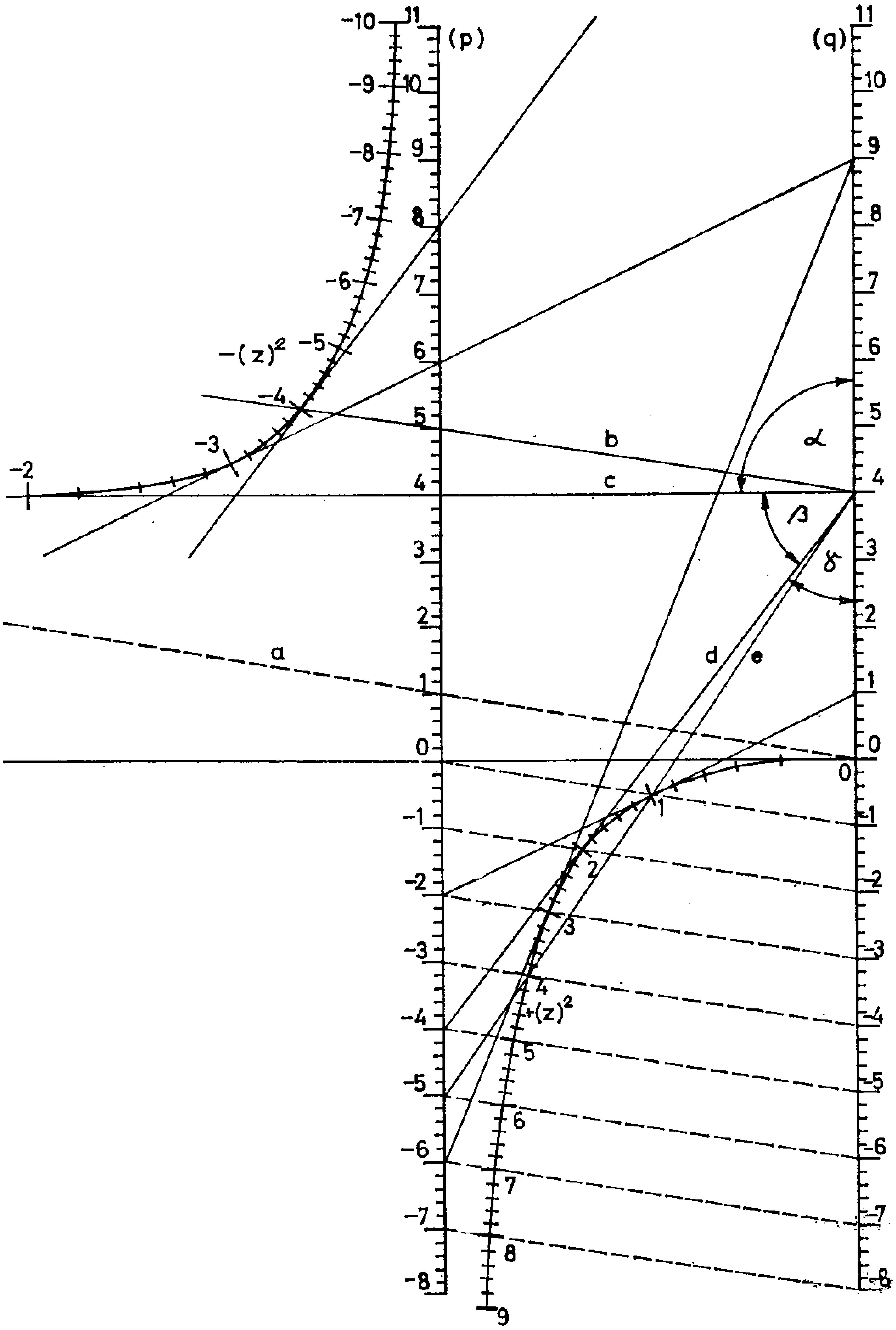
[1] Grčki *nomos* (νομος) = zakon; treba razlikovati *nomogram* od *monograma, nomografiju* od *monografije.*

U toj relaciji uređenu trojku a, b, c određujemo pomoću bilo koja njena dva člana, tako da imamo: *potenciranje* (traži se c), *antipotenciranje* (traži se b) i *logaritmiranje* (traži se a).



Sl. 31.5.2.4. *a*)

Nomogram $(z)^2$, odnosno $(z)^3$ jednadžbe $t^n + pt + q = 0$ za $n = 2$, odnosno $n = 3$.



Sl. 31.5.2.4. *b)*

Nomogram $+(z)^2$ za pozitivno i $-(z)^2$ za negativno rješenje kvadratne jednadžbe

$$t^2+px+q=0.$$

Ako na običnu brojevnu skalu ili brojevnu pravulju (skala A) u ishodištu (O) i jediničnoj tački (1) nanesemo okomito po jednu logaritamsku skalu i to skalu C u (O) i skalu B u (1), tada za kolinearne brojeve $a \in A$, $b \in B$, $c \in C$ vrijedi relacija (2), odnosno relacija (1). Specijalno se na taj način dobije nomogram jednadžbe $b^x = c$ (podaci b, c jednadžbi očitavaju se na skali B, odnosno C; rezultat x kao realni broj očitava se na skali A). Pri tom obadvije logaritamske skale B, C imaju jednu te istu jedinicu mjere za mjerenje.

5.2.2. *Krivocrtna brojevna skala.* Ako u koordinatnoj ravnini tačka $T = (x, y)$ krivulje K zavisi od nekog broja t preko vezâ

(3) $$x = f(t), \quad y = g(t),$$

tada se tačka T može markirati naprosto sa t.

Time *krivulja K postaje nosiocem odgovarajućih brojeva t* pa se zove *krivocrtna ili krivuljna skala!*

Npr. ako je $x = \cos t$, $y = \sin t$, tada su tačke jedinične kružnice k sa središtem (0, 0) markirane brojevima t za koje je $0 \leq t < 2\pi$; time je k određena *brojevna skala.*

5.2.3. *Krivocrtna skala i jednadžbe.* Ako promatramo tačke

$$A = (0, a), \quad B = (b, 0),$$

tada pravulja AB siječe krivocrtnu skalu K u određenim tačkama koje nose svoje marke $t_1, t_2, t_3; \ldots$; time se između brojeva $a, b, t_1, t_2, t_3, \ldots$ *uspostavlja* određena veza, *koja može poslužiti pri rješavanju jednadžbi.*

5.2.4. Trinomne jednadžbe i krivocrtna skala. Zadana je trinomna jednadžba

(1) $$t^n + pt + q = 0;$$

dovoljno je promatrati krivuljnu skalu koja odgovara krivulji K

(2) $$x = (1 + t)^{-1}, \quad y = -t^n (1 + t)^{-1}$$

i u koordinatnoj ravnini uzeti pravulju $x = 1$ kao nosioca veličinâ q u obliku tačke $(1, q)$ a y-os uzeti kao nosioca veličinâ p u obliku $(0, p)$; naime tačke

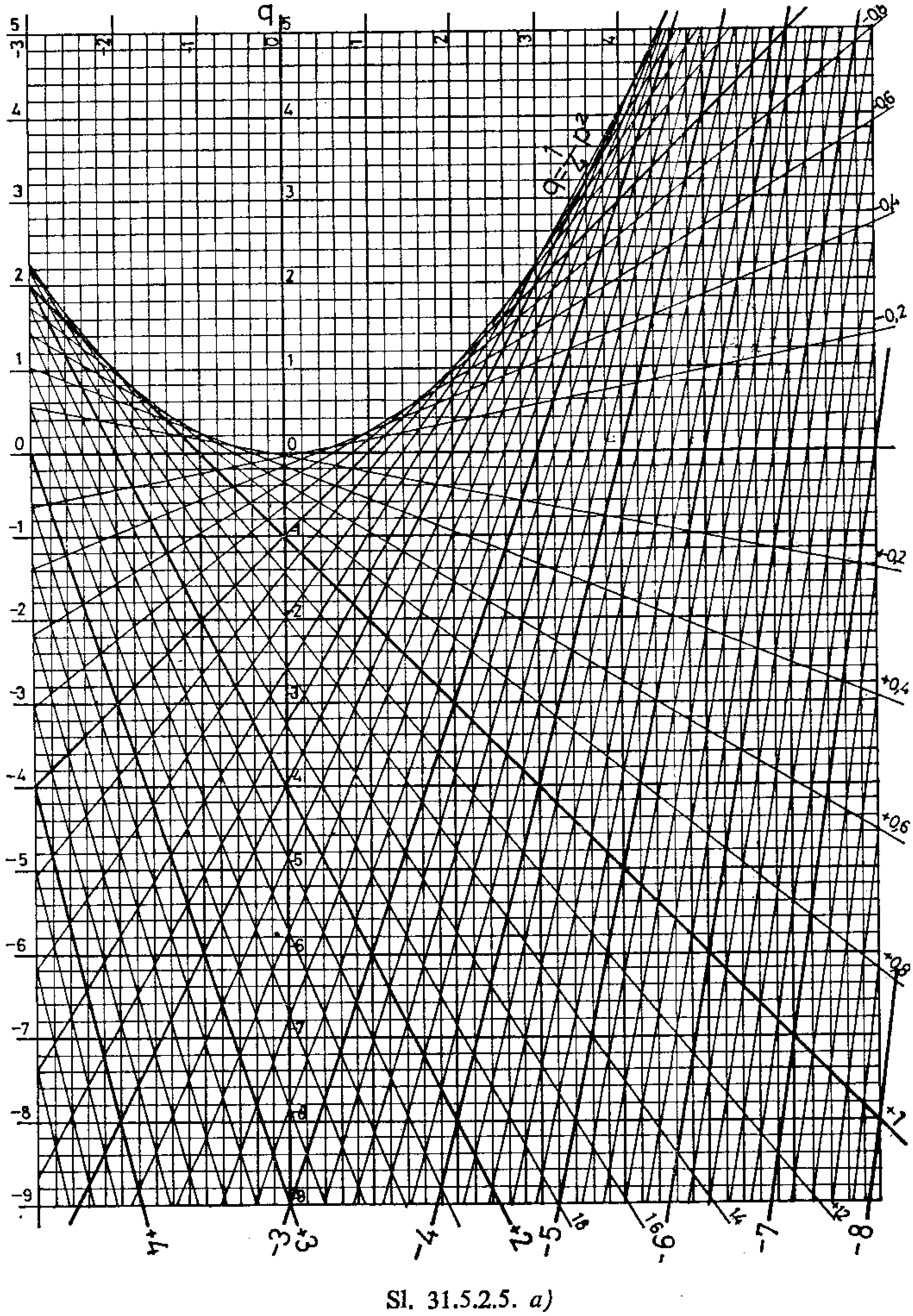
(3) $$(0, p), \ (1, q), \ ((1 + t)^{-1}, \ -t^n (1 + t)^{-1}$$

leže na istoj pravulji onda i samo onda ako vrijedi (1). No uklonimo li iz (2) parametar t, dobije se veza

(4) $$y = -(1 - x)^n x^{-n+1}.$$

U slučaju $n = 2$ krivulja (4) je hiperbola $xy = -(1 - x)^2$.

Prema tome, krivuljna skala određena parametrizacijom (2) leži na krivulji (4); ta krivulja K postaje nosilac odgovarajućih brojeva t kao rješenjâ jednadžbe (1). (isp. sl. 31.5.2.4. a) i b)).



Sl. 31.5.2.5. *a)*

Mrežni nomogram za rješavanje jednadžbe

$$x^2+px+q=0$$

Prema tome, *nomogram jednadžbe* (1) *sastoji se od ove tri skale:*

Prva skala: *pravulja* $x = 1$ *kao nosilac brojeva* q

Druga skala: *ordinatna os kao nosilac brojeva* p;

Treća skala: *krivulja* (2), *odnosno* (4) *na kojoj se upisuju brojevi* t; ova krivuljna skala se nacrta što tačnije, tj. odredi se što više vrijednosti t i pripadnih tačaka (2); izračunavanja (2) mogu se vršiti pomoću logaritamskih tablica, logaritmara i sl.

Prema tome, krivuljna skala (2) omogućuje da bar približno odredimo bar neko rješenje jednadžbe (1) uz zadano p i zadano q. Naravno, u praksi se broj p kreće u određenom skupu, broj q također, jer u praksi nije potrebno rješavati (1) za *svako* p i *svako* q.

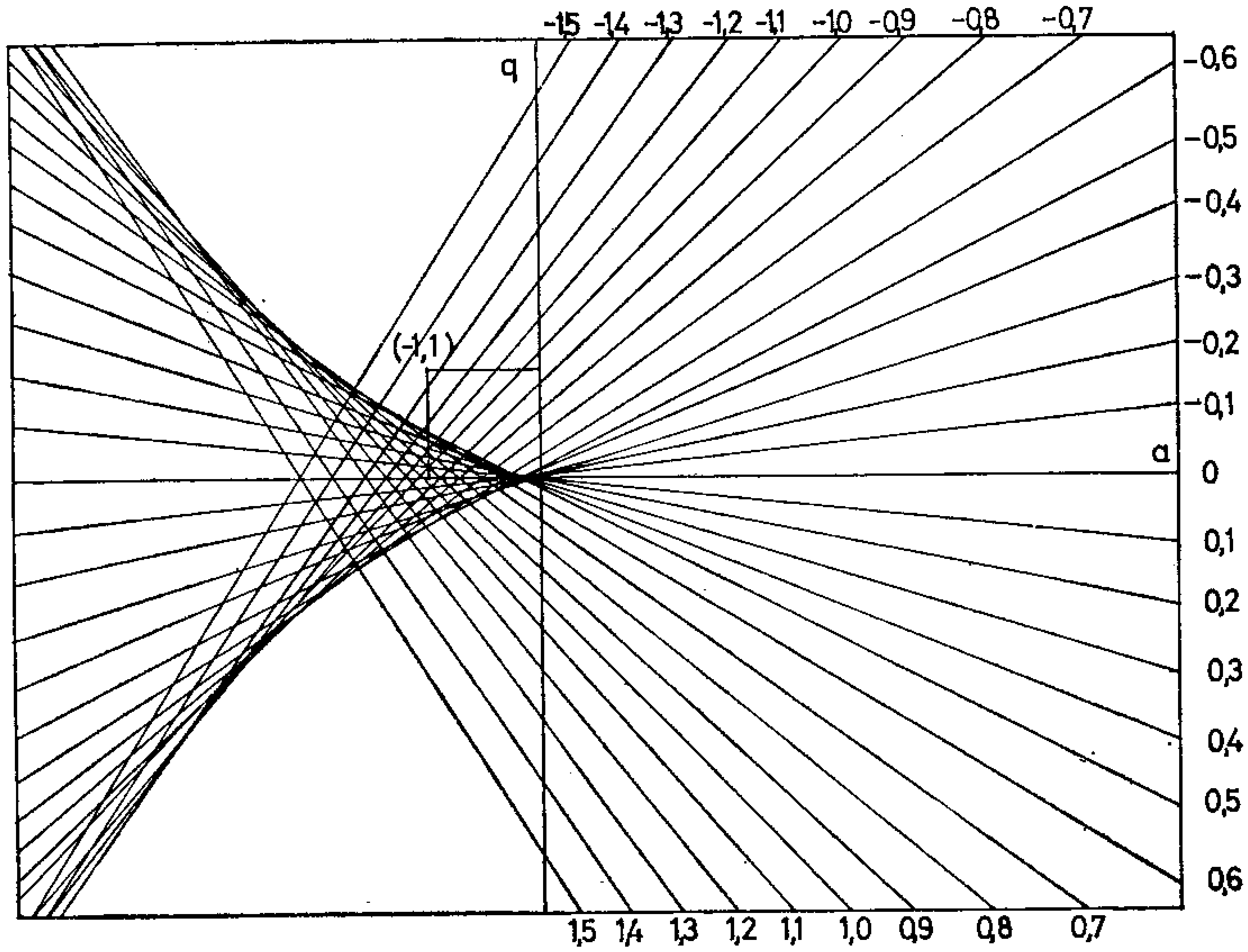
Inače, ako koeficijenti p, q padaju izvan dosega nomograma, možemo se poslužiti supstitucijom $t = kz$; za novu nepoznanicu z, daje (1) dijeleći sa k^n

$$z^n + \frac{p}{k^{n-1}} z + \frac{q}{k^n} = 0,$$

pa se k može odrediti tako da *novi koeficijenti dođu u okvir nomograma.*

5.2.5. Mrežni nomogram kubne jednadžbe

$$x^3 + px + q = 0. \tag{1}$$



Sl. 31.5.2.5. *b)*

Mrežni nomogram za rješavanje jednadžbe $x^3 + ax + q = 0$.

Za svaki broj $x=c$ daje (1) određenu pravulju; nacrtamo li u koordinatnoj (p, q)-ravnini pravulju (1) za poveći izbor vrijednosti parametra x pa na nacrtanoj pravulji

$$c^3+pc+q=0 \tag{2}$$

ucrtamo broj c kao marku te pravulje, tada se dobije *mrežni nomogram jednadžbe* (1); druge dvije obitelji krivulja mreže su koordinatne crte $p=$ konst., $q=$ konst.

5.2.5.1. Rješavanje jednadžbe pomoću nomograma. Jednadžba (1) rješava se pomoću nomograma tako da se ucči tačka (p, q) ravnine nomograma i gleda ona crta $x=c$ nomograma koja prolazi tačkom (p, q) ili se dovoljno blizu nalazi do tačke (p, q); odgovarajući broj c na crti $x=c$ je *rješenje jednadžbe* (1). Tako npr. za tačku $(p, q)=(-1, 1)$ jednadžba $x^3-x+1=0$ ima, prema slici 31.5.2.5 *a*), približno rješenje $x=-1{,}34$.

5.2.5.2. Na slici se ne može neposredno očitati rješenje jednadžbe sa npr. $(p, q)=(100, 150)$; no, provedemo li supstituciju $x=kz$, tada (1) prelazi nakon dijeljenja sa k^3 u jednadžbu

$$z^3+100\,k^{-2}\,z+150\,k^{-3}=0$$

pa npr. za $k=5$ tačka $(100\,k^{-2}, 150\,k^{-3})$, tj. $(p=4;\ q=2{,}3)$ leži u dosegu crtnje; pripadna marka je približno $z \doteq -0{,}29$, tj.

$$x \doteq 5\cdot -0{,}29 \doteq -1{,}45.$$

5.2.5.3. Uslov $D=0$ i Neilova parabola. Na slici 31.5.2.5 *b*) se vidi kako pravulje (1) (x je parametar; p, q su tekuće koordinate na svakoj pravulji) *obmataju određenu krivulju*; za svaku tačku (p, q) te krivulje ima jednadžba (1) *neprosto* rješenje x. Inače se jednadžba krivulje dobije uklanjanjem parametra x iz (1) i jednadžbe

$$3\,x^2+p=0 \tag{3}$$

dobivene iz (1) deriviranjem po x. Pomnožimo li (1) sa 3 a (3) s $-x$ i zbrojimo izlazi

$$2\,p\,x=-3\,q, \quad \text{tj.} \quad x=-\frac{3q}{2p}. \tag{4}$$

Iz (3) i (4) izlazi

$$\left(-\frac{p}{3}\right)^{\frac{1}{2}}=x=-\frac{3q}{2p}$$

odakle kvadriranjem

$$-\frac{p}{3}=\frac{9\,q^2}{4p^2} \quad \text{tj.}$$

$$-27\,q^2-4\,p^3=0, \tag{5}$$

odnosno

$$D=0 \quad (\text{isp. } 5,\ \S\ 6.2.2). \tag{6}$$

Krivulja (5) zove se *Neilova parabola*[1]. Tako vidimo kako je Neilova parabola vezana uz uslov (6), pri čemu je D diskriminanta jednadžbe (1).

---

[1] Krivulju su u 17. stoljeću našli N. W. Neil i P. Fermat; ona je uz kružnicu prva algebarska krivulja kojoj se umjelo odrediti duljinu lukova.

5.2.6. Mrežni nomogram trinomne jednadžbe $x^n + px^m + q = 0$, odnosno jednadžbe oblika $a(x) + p\,b(x) + q\,c(x) = 0$ konstruiraju se na isti način kao i u slučaju jednadžbe (1); pri tom su $a(x)$, $b(x)$, $c(x)$ zadane funkcije (algebarske ili nealgebarske). Inače, naziv mrežni nomogram dolazi otuda što krivulje $p = c_1$, $q = c_2$, $x = c_3$ pri mijenjanju brojeva c_1, c_2, c_3 čine 3 obitelji crtâ koje u ravnini čine isprepletenu mrežu (na slici su nacrtane samo pravulje $x = c_3$; ostali skupovi $p = c_1$, odnosno $q = c_2$ nisu nacrtani no njih čine crte milimetarskog papira na kojem se nomogram obično crta).

5.3. Mehaničko i fizikalno rješavanje jednadžbi. Pojedini *mehanički* i *fizikalni* pojavi i sredstva mogu poslužiti pri rješavanju jednadžbi. Tako npr. pojav o *spojenim posudama* može poslužiti za hidrostatično rješavanje jednadžbi;[1] npr. u sl. 31.5.3. a) znači visina v stupca vode u desnom valjku rješenje jednadžbe $x^3 + x = c$, pri čemu smo raspodijelili količinu c cm³ vode u valjak (volumen $1 \cdot x$ cm³) i stožac (volumena x^3 cm³); presjek valjka je 1 cm²: visina v cm stošca i promjer $2r$ cm baze u vezi su

$$r^2 \pi v = 3 v^3, \quad \text{tj.} \quad v = \left(\frac{\pi}{3}\right)^{1/2} r \doteq 1{,}0234\, r.$$

U slučaju jednačine $x^3 - x = c$ imamo uređaj kao na sl. 31.5.3 b): *pun* valjak stavlja se u stožac.

5.4. Jednačine $x^3 \pm x = c$ poseban su slučaj *tročlanih jednačina* oblika

$$x^m \pm x^n = c;$$

i ove se mogu rešavati pomoću napravâ građenih poput onih na sl. 31.5.3 (Demanet, 1898).

5.5. G. Meslin[2] je 1900, našao postupak da na osnovu vage i hidrodinamike rješava jednačine oblika $a_1 x^{n_1} + a_2 x^{n_2} + \cdots + a_k^{n_k} = c$.

5.6. A. Emch[3] je 1901. sagradio takav hidraulički aparat pomoću kojega se korijen jednačine određuje mjerenjem vremena za koje se sudovi posebna oblika isprazne kroz mali otvor na dnu sprave.

5.7. Posebno se s uspjehom koriste pojedini pojavi *nauke o elektricitetu* pri rješavanju algebarskih jednadžbi, posebno sistema linearnih jednadžbi s mnogo nepoznanica, obrtanju (inverziji) matricâ velikog formata, itd.

5.8. Mašinsko i automatsko rješavanje raznih oblika jednadžbi (algebarskih, nealgebarskih, diferencijalnih itd.) bazirano na pojedinim fizikalnim pojavima danas se mnogo upotrebljava i jedan je od oslonaca današnjeg snažnog tehničkog razvoja i mnogobrojnih primjena matematike u nauci, tehnici i proizvodnji.

---

[1] v. M. Petrović, *Sur l'intégration hydraulique des équations différentielles*, Amer. J. Math. 20 (1897), 293—300.

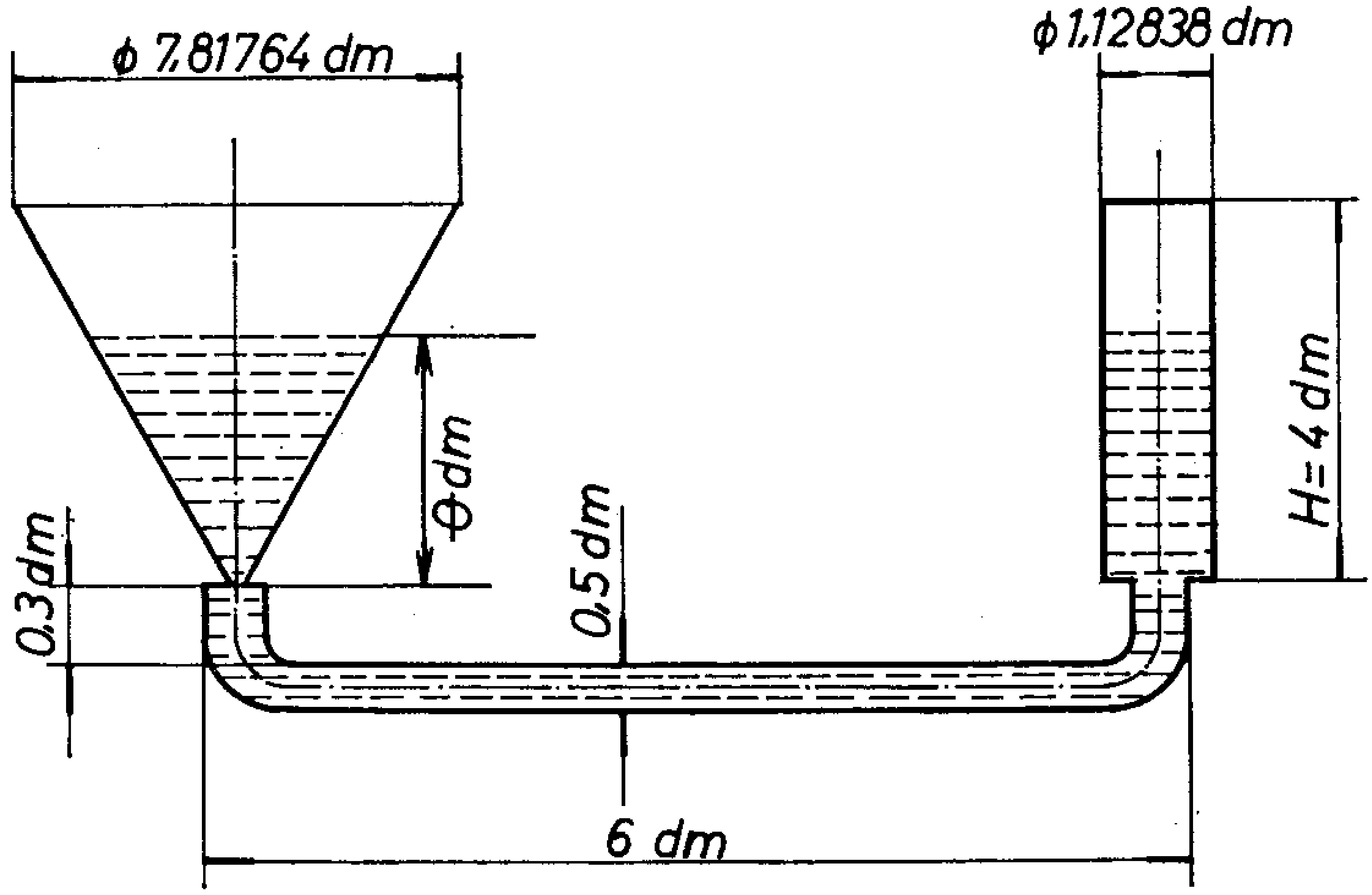
Demanet (Mathesis (2) 8 (1898)) se je koristio idejom Thomson-Tait-a (Treatise on natural philosophy, part I, 3, 1887, str. 70—88) i M. Petrovića o primeni hidrostatike u matematičkom modeliranju.

v. također: Brujevič. N. G., *Mašini dl'a rešenija algebraičeskih uravnenij*, Vestnik metalopromišlenosti, 1 (1938), 54—71,

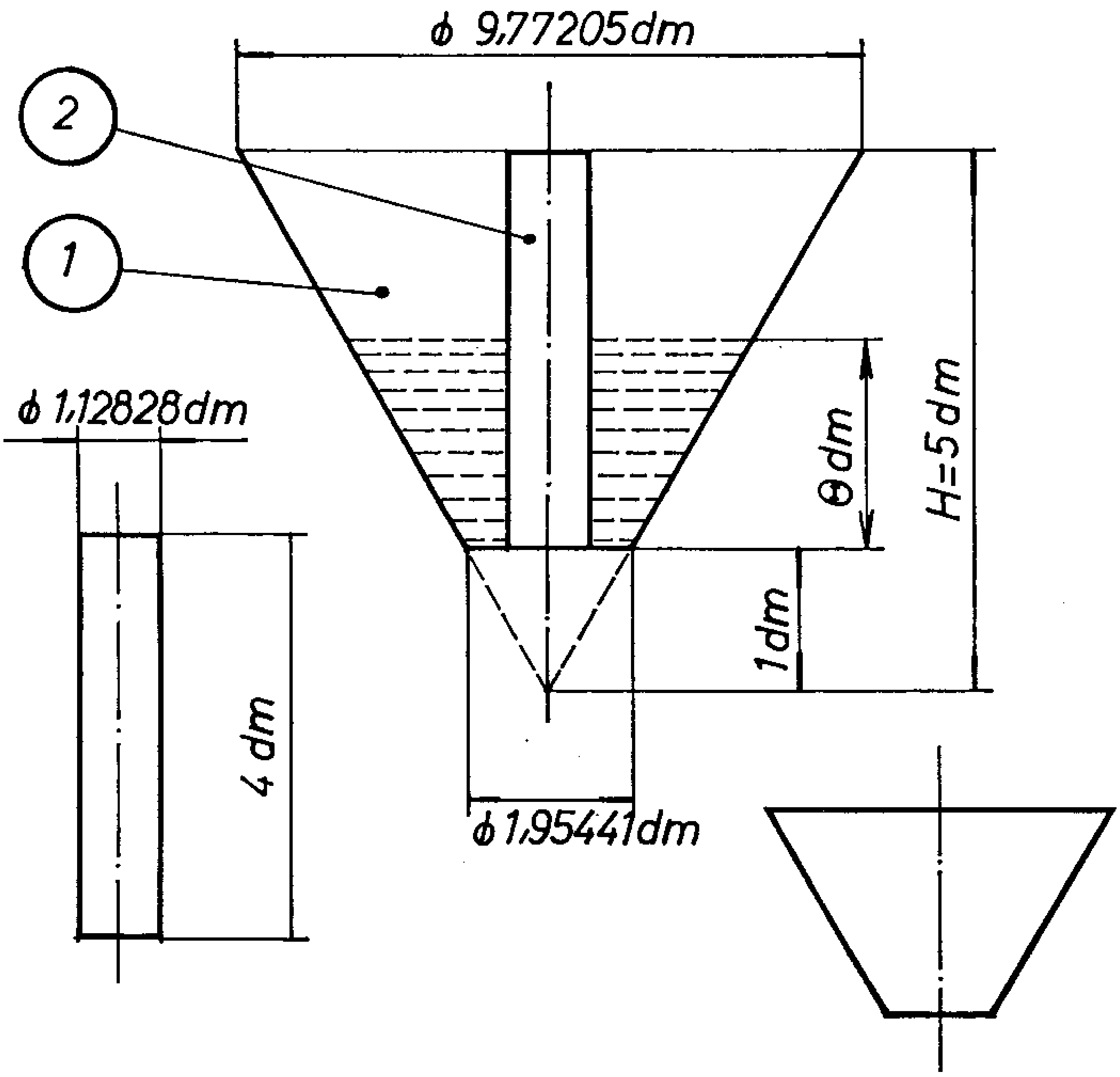
Weltmann W., Zeitschr. für Instrumentenkunde 4 (1884), str. 338.

[2] G. Meslin, C. R. Paris 130 (1900) str. 888.

[3] A. Emch, Amer. Math. Monthly 8 (1901), s. 58.



Sl. 31.5.3. a) Rješavanje jedn. $\theta^3+\theta=c$.



Sl. 31.5.3. b) Rješavanje jedn. $\theta^3-\theta=c$.

6. PRIBLIŽNO RJEŠAVANJE NEJEDNADŽBI

6.1. Nejednadžba s nepoznanicom x je jednog od oblika

(1) $$f x<0, \quad f x\leq 0, \quad f x\geq 0, \quad f x>0, \quad f x\neq 0.$$

6.2. Kako su nejednadžbe $f x<0$, $-f x>0$, ekvivalentne, isto kao i $f x\leq 0$, $-f x\geq 0$, možemo se ograničiti na nejednadžbu $f x<0$.

6.3. Nejednadžba $f x\neq 0$ je zadovoljena za svako x koje nije nulište od f. Skup

(2) $$R\setminus\sigma_f$$

je sastavljen upravo od svih realnih brojeva x za koje je $f x\neq 0$. Ako je $f x$ *neprekidna* funkcija, skup (2) se sastoji od određenog broja otvorenih intervala (među kojima je nužno jedna lijeva poluzraka i jedna desna poluzraka ako je $f(x)$ cijela racionalna funkcija s realnim koeficijentima); u tom slučaju bit će $\operatorname{sgn} f$ konstanta u svakom maksimalnom intervalu množine (2). Zato je bitno odrediti spektar σ_f tj. riješiti $f x=0$, jer je onda lako dalje naći rješenja pojedinih nejednadžbi iz (1).

6.4. Nejednadžbe sa 2 i više nepoznanica. I one su vezane s odgovarajućim *jednadžbama.* Ako se npr. radi o nejednadžbi $a(x, y)<0$, onda treba znati da odgovarajuća jednadžba $a(x, y)=0$ znači, općenito, neku „krivulju" K; preostatak $R_2\setminus K$ ravnine R_2 raspada se u određen skup svezanih *maksimalnih* oblasti kojima omeđenje leži u K; u svakoj od tih oblasti funkcija $\operatorname{sgn} a(x, y)$ je konstanta; dvije takve oblasti O, O_1 sa zajedničkim lukom kao pregradom imaju svojstvo da u njima $\operatorname{sgn} f$ poprima vrijednosti $+1$ i -1. Tako npr. ako je K hiperbola $a(x, y)\equiv x^2-y^2-1=0$, tada se $R_2\setminus K$ raspada u 3 oblasti, $O(F_1)$, $O(F_2)$, $O(O)$ u kojima je fokus F_1, odnosno fokus F_2, odnosno ishodište O; funkcija $\operatorname{sgn} a(x, y)$ je u njima $+1$, $+1$, odnosno -1.

6.4.1. Primjedba. Zanimljivo je da se $R_2\setminus K$ može sastojati i od beskonačno mnogo oblasti i da one sve imaju K kao svoje zajedničko omeđenje! (isp. P. S. Aleksandrov, Kombinatornaja topologija, Moskva 1947, 660, posebno str. 68; fenomen je pronašao nizozemski matematičar Brouwer 1909. godine).

7. ZADACI O PRIBLIŽNOM RJEŠAVANJU JEDNADŽBI I NEJEDNADŽBI

1. Naći $a(x)\equiv 4x^3-5x^2+6$ za 1) $x=1+2i$; 2) $x=-5+4i$; 3) $x=7-3{,}2i$; 4) $x=-7{,}5+4{,}2i$.

2. *Separirati* realna ništišta ovih polinoma (isp. 31, § 0):
   1) $x^3-15{,}6x^2+74{,}28x-111{,}52$; 2) $x^3-7{,}6x^2-18{,}52x+111{,}52$;
   3) $x^4-11x^3+26{,}88x^2+11x-27{,}88$; 4) $x^4-20x^3+120x^2+20x-101$;
   5) $x^5-x^4+4x^3+4x^2+3x+5$;
   6) $x^6-4x^5-6{,}01x^4-2{,}02x^3-4{,}99x^2+6{,}02x-2{,}02$.

3. *Ruffini-Hornerova metoda rješavanja.* Neka polinom $a(x)$ ima nulište ξ kojemu je c cijeli dio (dakle je $c \leq \xi < c+1$); naći polinom $a^{(1)}(y) = a(y+c)$ metodom iz pogl. 21 § 2.4.4 i znamenku desetina d_1 njegova nulišta $\eta = \xi - c$ metodom pokušavanja $\eta = 0,1$; $0,2, \ldots$; $0,9$; proces ponoviti i odrediti $a^{(2)}(z) = a^{(1)}(z + d_1 10^{-1})$, pa odrediti znamenku d_2 stotnina nulišta $0,0 d_2 \cdots$ polinoma $a^{(2)}(z)$ itd. Odrediti Ruffini-Hornerovim postupkom na tačnost 10^{-2}:
   1) najmanje pozitivno nulište $\frac{x}{r}$ od $x^3 - 3rx + r^3$ i odrediti njegovo geometrijsko značenje;
   2) pozitivno nulište od $x^4 + 4x^3 + 2x^2 - 12x - 15$;
   3) negatino nulište od $x^4 - 2x^3 - 3x^2 - 2x - 4$;
   4) veći pravi razlomak za koji je $-x^4 + x - 0,2 = 0$;
   5) realna nulišta na 10^{-1} od $x^4 + 45x^3 + 214x^2 + 1492x + 595$ (zadatak je u vezi s preračunavanjima o stabilnosti aviona).
4. Ruffini-Hornerovim postupkom odrediti (riješiti) na tačnost 10^{-3};
   1) najveće realno nulište od $x^4 - 4x^3 + 2x^2 - 4x + 1$;
   2) najmanje pozitivno nulište od $x^4 - 7x^3 + 4x^2 + 3x + 11$;
   3) $x^4 - 6x^3 + 8x^2 + 2x - 1 > 0$; 4) $-x^4 + x - 2 < 0$.
5. Zadana je pravokutna limena pločica P veličine 30 cm, 20 cm; od P treba napraviti pravokutnu posudicu p zapremine 400 cm³ tako da se p dobije iz P presavijanjem nakon što su na vrhovima pločice P isječeni jednaki kvadrati.
6. Metodom iteracije (31, § 1) naći na 10^{-2} najveće ništište funkcije:
   1) $x^3 + 2x - 1$; 2) $x^4 - 2x^3 + x - 1$; 3) $x - \cos x$, $0 < x < \pi/2$;
   4) $2x - \cos x$, $0 < x < \pi/2$; 5) $x - \operatorname{tg} x$, $0 < x < \pi/2$;
   6) $2x - \operatorname{tg} x$; 7) $x - \cos 2x$.

6'. Metodom iteracije naći na 10^{-2} nulište minimalne apsolutne vrijednosti funkcije 1) $e^z + 0,1z + 2$; 2) $e^{2z} - 0,2z + 3$.

7. Primjenom metode sekante (21, § 1.3) ili tangente (31, § 1.4) riješiti
   1) $x^4 - 6,2x^3 + 8,2x^2 + 2,2x - 1,2 = 0$;
   2) $x^4 - 6,03x^3 + 8,01x^2 + 2,02x - 1,01 = 0$;
   3) $2x^4 - x + 1 = 0$; 4) $2x^4 + x - 1 = 0$; 5) $x^2 - \sin \pi x = 0$ na 10^{-5}.
8. Metodom iteracije ili metodom dodira odrediti na 10^{-2} rješenje jednadžbi: 1) $2x^3 - y^2 - 1 = 0$, $xy^3 - y - 4 = 0$ polazeći od približnog rješenja $(x_0, y_0) = (1,2;\ 1,7)$; 2) $x + 3 \log x - y^2 = 0$, $2x^2 - xy - 5x + 1$; $(x_0, y_0) = (1,4;\ -1,5)$.

8'. Metodom ponavljanja (iteracije) naći ništišta mnogočlana $x^8 - 15x^5 + 24x - 5 \equiv a(x)$ sa $x_0 = 0,3$ kao početnom vrijednosti.

9. Na tačnost od 10^{-3} riješiti: 1) $x^2 + 2y = 30$, $y^2 + 2x = 20$;
   2) $x = \operatorname{tg} x$, $y = \operatorname{tg} x$ pri čemu je $(x_0, y_0) \doteq (1,3;\ 4,0)$.
10. Naći $a^{\square}(x)$ (isp. 31 § 2.2.1) ako $a(x)$ znači: 1) $x^3 + 4x^2 + 5x + 1$;
   2) $-x^3 + 4x^2 + 5x + 1$; 2) $x^3 - 4x^2 + 5x + 1$;
   4) $x^3 + 4x^2 - 5x + 1$; 5) $x^3 + 4x^2 + 5x - 1$.

11. Naći $a^{\square 2}(x)$ ako $a(x)$ znači:
1) $1+5x+4x^4+6x^5$; 2) $1-5x+4x^4-6x^5$;
3) $-1+5x+4x^4-6x^5$; 4) $1+5x-4x^4-6x^5$.

12. Metodom Dandelin-Lobačevski-Graeffe-a iz § 2.3 riješiti jednadžbu:
1) $x^3+5x-3=0$; 2) $-x^4+x-c=0$ za $c=0{,}1$; $0{,}2$; $0{,}3$; $0{,}4$; ... ; $0{,}9$;
3) $x^4+3x^3-4x-1=0$; 4) $x^4-4x^3-4x^2+16x-8=0$;
5) $-8x^4-16x^3-4x^2+4x+4$;
6) $x^5-3x^4-7x^3-5x^2+1=0$ (primjer Lobačevskoga; rez. 4,70968);
7) $x^8-\frac{3}{2}x^6+\frac{27}{40}x^4-\frac{57}{560}x^2+\frac{55}{22400}=0$.

13. Babilonci su približno stavljali $+(a^2+b^2)^{1/2} \doteq a+\frac{b}{2a}$ pri $0<b<a$; da li se tu radi o metodi tangente?

14. Isto pitanje za približnu jednakost
1) $(a^2+r)^{1/2} \doteq a+\frac{r}{2a+1}$ (arapski matematičari iz 11. stoljeća);
2) $(a^3+r)^{1/3}=a+r(3a^2+3a+1)^{-1}$ (Leonardo iz Pize; 1202).

15. Riješiti $a(x)<0$, ako $a(x)$ označuje funkciju iz zad. 2.

16. Riješiti $a(x)>0$, ako $a(x)$ označuje funkciju iz zad. 4.

17. Riješiti $\frac{a(x)}{b(x)}>0$, ako $a(x)$ označuje funkciju iz zad. 2; $b(x)$ označuje funkciju iz zad. 3.

18. Isto pitanje za $\frac{1+a(x)}{1+b(x)}>0$, odnosno za $\frac{2+a(x)}{2+b(x)}>0$.

19. Lillovom metodom iz § 4.4. odrediti grafički vrijednost $a(x_0)$ ako $a(x)$, odnosno x_0 znače: 1) $2x^2+3x+4$; 1; 2) $-2x^2+3x+4$; $-0{,}5$;
3) $x^3-5x+2x-1$; 2; 4) x^3-5x^2-2x+1; 2.

20. Lillovom metodom riješiti približno: 1) $x^3-2x^2+x-1=0$;
2) $x^3=2$; 3) $4x^3-3x=c$ za pojedino $c\in\{1/2,\ 1/3, \ldots, 1/10\}$.

21. Isti zadatak riješiti metodom dvaju kutova (isp. § 4.4.6).

22. Odredi pravocrtne skale ovih funkcija (isp. § 5.1.):
1) x^2+3x+1; 2) x^3+2x+3; 3) x^3-2x-3 za $0\leq x\leq 3$; neka se nacrtane susjedne vrijednosti argumenta razlikuju za 10^{-1}.

23. Odredi nomogram za rješavanje 1) kvadratne jednadžbe; 2) kubne jednadžbe bez kvadratnog člana (isp. § 5.2.4).

24. Odredi mrežni nomogram jednadžbi 1) $x^2+px+q=0$;
2) $x^4+px+q=0$; 3) $x^4+px^3+q=0$; 4) $3x^3+px^2+q=0$.

25. Odredi dominantnu svojstvenu vrijednost i pripadni svojstven vektor ovih matrica (isp. § 3.2.2):

$$1)\begin{bmatrix}4 & 2 & 0\\1 & 6 & 0\\0 & 0 & 1\end{bmatrix};\quad 2)\begin{bmatrix}4 & 2 & 0\\1 & 6 & 0\\3 & 1 & 0\end{bmatrix};\quad 3)\begin{bmatrix}1 & 0{,}1 & 0{,}2\\0{,}1 & 1 & 0{,}4\\0{,}2 & 0{,}4 & 1\end{bmatrix};$$

$$4)\begin{bmatrix}1 & -0{,}1 & 0{,}2\\-0{,}1 & 1 & 0{,}4\\0{,}2 & 0{,}4 & 1\end{bmatrix};\quad 5)\begin{bmatrix}1 & 0{,}1 & -0{,}2\\0{,}1 & 1 & 0{,}4\\-0{,}2 & 0{,}4 & 1\end{bmatrix};$$

$$6)\begin{bmatrix}1 & 0{,}1 & 0{,}2\\0{,}1 & 1 & -0{,}4\\0{,}2 & -0{,}4 & 1\end{bmatrix};\quad 7)\begin{bmatrix}1 & 0{,}1 & -0{,}2\\0{,}1 & 1 & -0{,}4\\-0{,}2 & -0{,}4 & 1\end{bmatrix};$$

$$8)\begin{bmatrix}1 & -0{,}1 & 0{,}2\\-0{,}1 & 1 & -0{,}4\\0{,}2 & -0{,}4 & 1\end{bmatrix};\quad 9)\begin{bmatrix}1 & -0{,}1 & -0{,}2\\-0{,}1 & 1 & 0{,}4\\-0{,}2 & 0{,}4 & 1\end{bmatrix};$$

$$10)\begin{bmatrix}1 & -0{,}1 & -0{,}2\\-0{,}1 & 1 & -0{,}4\\-0{,}2 & -0{,}4 & 1\end{bmatrix}.$$

26. Metodom iteracije iz § 1.7. riješiti jednadžbu $a\vec{x}=\vec{c}$; $\vec{c}=[1,\ 0,\ 0]^T$; pri tom je a matrica iz zadatka 25.

27. Isto pitanje za vektor $c=1_2=[0,\ 1,\ 0]^T$.

28. Isto pitanje za vektor $c=1_3=[0,\ 0,\ 1]^T$.

29. Isto pitanje za vektor $c=[2,\ 3,\ -4]^T$.

30. Odrediti normu $\|a\|_{\mathrm{I}}$ za matrice iz zadatka 25; odrediti također Geršgorinov skup $\mathbf{G}a$ matrice a (isp. § 3.4.1).

Literatura:

Berezin-Židkov [1];
Demidovič-Maron [1]; Faddejev-Faddejeva [1]; Faddejev-Sominski [1]; Obreškov [1]-[4]; Ostrowski [1].

POGLAVLJE 32.

NEKE ALGEBARSKE STRUKTURE

Naučili smo naći bar približna rješenja zadane algebarske jednadžbe; ako je stepen polinoma $p(x)$ veći od 4, onda se nulišta od $p(x)$ ne mogu više dobiti pomoću konačnog broja prvih 5 računskih operacija (zbrajanje, oduzimanje, množenje, dijeljenje, antipotenciranje) (Ruffini-Abel). Galois je skrenuo rješavanje algebarskih jednadžbi na sasvim nov put našavši da su grupe i tijela adekvatna sredstva za prikazivanje prave situacije (v. § 6).

Upoznat ćemo se s nekojim osnovnim pojmovima toga novog pravca u algebri.

1. NEŠTO O ALGEBARSKIM BROJEVIMA

1.1. Definicija. *Algebarski brojevi* jesu rješenja algebarske jednadžbe $a_0 + a_1 x + \cdots + a_n x^n = 0$ s racionalnim koeficijentima $a_0, a_1, \ldots, a_n$; pri tom n prolazi skupom prirodnih brojeva.

Brojevi koji nisu algebarski zovu se transcendentni brojevi.

Skup svih algebarskih brojeva označit ćemo sa A.

Na pr. -3, $2/5$, $3^{1/2}$, $5^{7/100}$ su algebarski brojevi. Zna se da brojevi e, π e^{π}, $e+\pi$, $2^{(2^{1/2})}$ nisu algebarski. Ne zna se da li su brojevi 2^{π}, 2^{e}, π^{e}, $C = \lim\limits_{n\to\infty}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{n} - ln\right)$ racionalni ili iracionalni.

1.1.1. Jasno je da svaki algebarski broj zadovoljava i jednadžbu s *cijelim* racionalnim koeficijentima — reći ćemo kraće: zadovoljava jednadžbu nad D. Dovoljno je jednadžbu nad Q koju zadovoljava neki algebarski broj a pomnožiti sa najmanjim zajedničkim kratnikom nazivnikâ svih koeficijenata pa da se dobije jedna jednadžba nad D koju zadovoljava broj a.

Također se vidi da baš ta jednadžba ima dalje ovo svojstvo: najveći zajednički faktor svih koeficijenata jednadžbe je $=1$.

Prema tome dobili smo

1.1.2. Teorem. *Svaki algebarski broj zadovoljava određenoj algebarskoj jednadžbi nad D i s koeficijentima čiji je najveći zajednički kratnik jednak* 1.

1.2. Cijeli algebarski brojevi. Množina EA.

1.2.1. Definicija. Svaki broj koji je rješenje *normirane* algebarske jednadžbe s cijelim racionalnim koeficijentima zove se *cio algebarski broj.* Skup svih cijelih algebarskih brojeva označivat ćemo sa EA.

Naravno, obični racionalni cijeli brojevi su cijeli i kao algebarski brojevi.

1.2.2. Primjedba. U definiciji *cijelih* algebarskih brojeva naglasak je na tome da je jednadžba *normirana,* tj. da je koeficijent najviše potencije nepoznanice $=1$ i da su ostali koeficijenti uzeti u D (a ne u Q).

Tako npr. $2^{1/2}$ je cio algebarski broj jer zadovoljava $x^2-2=0$. Drugim riječima iracionalni realni broj $2^{1/2}$ je *cio* algebarski broj. Naravno, svaki cio racionalni broj je cio i kao algebarski broj; ujedno, drugih racionalnih brojeva koji bi bili cijeli algebarski brojevi niti nema, jer je na snazi

1.2.2.1. Lema. *Ako je q racionalan broj i ujedno cio algebarski broj, onda je q cio racionalan broj; drugim riječima*

$$Q \cap EA = D.$$

Dokaz leme! Neka je $q=\frac{a}{b}$, pri čemu su a, b međusobno prosti cijeli racionalni brojevi. Kako je $q \in EA$, zadovoljava $\frac{a}{b}$ svoju minimalnu jednadžbu

$$c(x) := x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0,$$

pri čemu su $c_0, c_1, \ldots, c_{n-1}$ cijeli racionalni brojevi (koeficijent od x^n je 1).

To znači da je $c\left(\frac{a}{b}\right)=0$; pomnožimo li ovu jednadžbu sa b^n i iz dobivene jednadžbe nađemo a, dobije se

$$a^n = -b\,(a^{n-1} c_{n-1} + a^{n-2} b c_{n-2} + \cdots + a b^{n-1} c_1 + b^n c_0). \tag{2}$$

Tvrdimo da je $b \in \{1, -1\}$. U obrnutom slučaju postojao bi prost djelilac p od b; prema (2) bi bilo $p \mid a^n$ dakle i $p \mid a$; to znači da bi p dijelilo i a i b, protivno pretpostavci da su a, b međusobno prosti. Dakle je zaista $b \in \{1, 1\}$, dakle $q=\frac{a}{\pm 1} \in D$.

1.3. Stupanj ili stepen algebarskog broja *a* je ***najmanji*** stupanj normirane algebarske jednadžbe s koeficijentima u Q, koju broj a zadovoljava.

1.4. Matični ili minimalni polinom $M(a)$ vezan za broj a. Na taj način, svakom algebarskom broju a pripada određen stupanj, označen $\operatorname{st} a$.

To je jasno. Međutim, ne samo da broju a pripada određen stupanj $\operatorname{st} a$, nego njemu pripada i jedan jedini *normiran polinom* $M(a)$ stupnja $= \operatorname{st} a$ kojeg broj a zadovoljava; označimo taj polinom sa $M(a)$, odnosno $M(a)(x)$. To znači da je

$$M(a)(a)=0, \quad \operatorname{st} M(a) = \operatorname{st} a \quad \text{i} \quad M(a)_{\operatorname{st} a} = 1; \tag{1}$$

naime koeficijente polinoma $M(a)$ označujemo po redu

$$M(a)_0,\ M(a)_1,\ M(a)_2,\ \ldots;$$

ako su dalje $p(x)$, $q(x)$ normirani i stupnja $s = \operatorname{st} a$ pa ako je

$$p(a) = q(a), \text{ tada je i } p(a) - q(a) = 0;$$

no polinom $p-q$ je stupnja $<s$ pa zato on identički iščezava tj. $p=q$. Kad bi naime $p-q$ imalo bar jedan koeficijent $\neq 0$, mogli bismo polinom $p-q$ normirati i promatrati njega; jasno je da bi broj a poništavao taj polinom, kojemu je stupanj $<\operatorname{st} a$, protivno definiciji broja $\operatorname{st} a$.

Poseban je problem da se za svako $a \in A$ odredi broj $\operatorname{st} a$ i polinom $M(a)$.

1.4.1. Primjer. Neka je $a = 2^{1/2} + 3^{1/2}$. Odredi broj $\operatorname{st} a$ i polinom $M(a)$.

Postupak je tipičan: naprave se nove jednadžbe promatrajući a^2, a^3, ... pa se onda a ukloni.

Kvadriramo li, imamo

$$a^2 = 2 + 2 \cdot 6^{1/2} + 3,$$

odatle

$$(a^2-5)^2 = 24 \quad \text{tj. } a \text{ zadovoljava} \quad x^4 - 10x^2 + 1 = 0.$$

To je tražena jednadžba za broj a. Prema tome polinom $M(a)$ glasi $x^4 - 10x^2 + 1$. Vidi se da je $\operatorname{st} a = \operatorname{st} M(a) = 4$.

1.4.2. Tu je postupak eliminacije bio kraći zbog pojednostanjenja izraza a^2.

Korisno je pogledati recimo broj $b = 3^{1/3} + 5^{1/4}$ pa gledati kako da se dođe do polinoma $M(b)$. Rezultat je: polinom 12 stupnja! A najteže pitanje koje se tu postavlja jest: da li je dobiveni polinom *najnižeg* mogućeg stupnja!

1.4.3. Za svaki prirodni broj n postoji bar jedan cio algebarski broj stupnja n; takav je npr. broj

$$\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = e^{i\frac{2\pi}{n}} \quad \text{ili npr.} \quad +2^{\frac{1}{n}}.$$

1.5. Konjugirani ili spregnuti brojevi algebarska broja.

Spregnuti ili konjugirani brojevi zadana algebarska a broja jesu brojevi koji zadovoljavaju matičnu jednadžbu $M(a)(x) = 0$ koja pripada broju a. (v. t. 1.4).

Tako npr. broju $+3^{1/2}$ pripada jednadžba $x^2 = 3$; zato konjugirani broj od $+3^{1/2}$ glasi $-3^{1/2}$.

Konjugirani broj od $b = 2 + 3^{1/2}$ glasi $a' = 2 - 3^{1/2}$; stvarno, jednadžba za a glasi $(a-2)^2 = 3$; njena rješenja glase $2 \pm 3^{1/2}$.

Konjugirani broj od $3-4i$ $(i = (-1)^{1/2})$, glasi $3+4i$ iz istog razloga.

Nađimo spregnut broj od $a = 2^{1/2} + 3^{1/2}$. U 1.4.1 smo vidjeli da matična jednadžba broja a glasi $x^4 - 10x^2 + 1 = 0$; njena rješenja glase:

$$x = \pm(5 \pm 24^{1/2})^{1/2};$$

tu se osim zadana broja a pojavljuju još 3 s njim spregnuta broja.

1.6. Norma i trag zadana algebarska broja.

1.6.1. *Norma algebarskog broja a* jest *umnožak* svih nulišta matičnog polinoma $M(a)(x)$ broja a; svako nulište se računa svojom kratnošću. Norma broja a označuje se sa $N(a)$ ili Na.

1.6.2. *Trag algebarskog broja a* jest suma svih nulišta matičnog polinoma $M(a)(x)$ broja a; označuje se sa $\operatorname{Tr} a$ ili $\operatorname{Tr}(a)$.

Npr. za kompleksni broj $a = 2 - 3i$, pripadna jednadžba izlazi iz $(a-2)^2 = (-3i)^2 = -9$; glasi $x^2 - 4x + 13 = 0$ kojoj su rješenja $2 \pm 3i$; dakle je $Na = (2-3i)(2+3i) = 4+9 = 13$.

Trag je $\operatorname{Tr} a = (2-3i) + (2+3i) = 4 =$ dvostruki realni dio od a.

1.6.3. Teorem. *Norma broja a jest produkt konstantnog člana polinoma $M(a)$ i broja $(-1)^s$ tj. $Na = M(a)_0 \cdot (-1)^s$.*

Trag broja a jest $-M(a)_{s-1}$ tj. produkt od -1 i koeficijenta od x^{s-1}; pri tom je $s = \operatorname{st} a$.

Na osnovu ovog teorema nalaze se $N(a)$ i $\operatorname{Tr}(a)$, a da se i ne traže brojevi koji su sa a konjugirani.

Npr. $N\,2^{1/3} = ?$ No polinom koji pripada algebarskom broju $2^{1/3}$ je $x^3 - 2$; stepen je $s = 3$, konstantni član je -2; treba ga množiti sa (-1) dakle je $N\,2^{1/3} = (-1) \cdot (-2) = 2$.

1.7. Tijelo A algebarskih brojeva. Kolo EA — 1.7.1. Možemo se pitati ovo: ako je a ***(cio) algebarski*** broj, da li je onda $-a$ također (cio) algebarski broj pa a^{-1} (ako je $a \neq 0$), da li je suma, odnosno produkt dvaju (cijelih) algebarskih brojeva također algebarski broj? Potvrdan odgovor na to pitanje u suštini iscrpljuje sadržinu naslova ovog paragrafa jer ostali uslovi za tijelo, odnosno kolo (zakon združivanja ili asocijacije, pa raspodjele ili distribucije itd.) automatski su ispunjeni jer se ipak ovdje radi o brojevima.

1.7.2. Dokažimo npr. da iz

$$a \in A \text{ izlazi } -a \in A \text{ i } a^{-1} \in A \text{ (ako je } a \neq 0).$$

No ako je f polinom nad Q za koji je

$$f(a) = 0 \text{ tj. } f_0 + f_1 a + f_2 a^2 + \cdots = 0,$$

tada je očigledno

$$f_0 - f_1(-a) + f_2(-a)^2 - f_3(-a)^3 + \cdots = 0 \quad \text{tj.}$$

$$\sum_k (-1)^k f_k (-a)^k = 0; \quad \text{a ovo je opet jedan polinom nad } Q.$$

1.7.3. Također se vidi da je

$$f(a^{-1}) = a^{-n} \sum_{k=0}^{n} f_{n-k} a^k \quad \text{tj.} \quad f^T(a^{-1}) = 0,$$

gdje je f^T daul polinoma f (f i f^T imaju ovakve koeficijente: $f_i^T = f_{n-i}$, $n = \operatorname{st} f$)

Prema tome, recipročna vrijednost algebarskog broja $\neq 0$ opet je algebarski broj.

Da li je suma algebarskih brojeva algebarski broj, tj. da li je $(A, +)$ grupoid? Da li je $(A; \cdot)$ grupoid? Jest, kao što se vidi iz ovog

$\longrightarrow$ **1.7.4. Teorema.** ***Ako su b, c algebarski brojevi, a $p(x, y)$ kakav god algebarski polinom nad Q, tada je i broj***

(1) $$\lambda = p(b, c) \qquad \textbf{\textit{algebarski broj.}}$$

Dokaz nije tako jednostavan. Dobro je promozgati kako da čovjek stvar dokaže za poseban slučaj $p(x, y) = x + y$, odnosno $p(x, y) = x \cdot y$.

Neka je $\operatorname{st} b = m$, $\operatorname{st} c = n$; neka je $f(x) = 0$, odnosno $g(x) = 0$ normirana jednadžba stupnja m, odnosno n koju zadovoljava broj b, odnosno broj c i koje imaju minimalan stupanj.

Te su jednadžbe jednoznačno određene (§ 1.4), imamo

(2) $$\begin{aligned} b^m &= -f_0 - f_1 b - f_2 b^2 - \cdots - f_{m-1} b^{m-1}, \quad \text{gdje } \operatorname{st} b = m \\ c^n &= -g_0 - g_0 c - g_2 c^2 - \cdots - g_{n-1} c^{n-1}, \quad \operatorname{st} c = n. \end{aligned}$$

Na taj način vidimo da se broj b^m može izraziti kao spoj brojeva $b^{m\cdot}$, a broj c^n kao spoj brojeva $c^{n\cdot}$ s racionalnim koeficijentima $f_{m\cdot}$ odnosno $g_{n\cdot}$. To opet znači da se produkt $b^r c^s$ može izraziti kao spoj brojeva

(3) $$b^{m'} c^{n'}, \; (m' = 0, 1, \ldots, m-1, \quad n' = 0, 1, \ldots, n-1),$$

njih mn na broju koje možemo numerirati i svrstati u niz

(4) $$z_1, z_2, \ldots, z_{k-1}, z_k \quad \text{gdje je} \quad k = mn.$$

Specijalno, možemo produkte $z_i \lambda$, gdje je $\lambda = p(b, c)$ iz (1) izraziti homogeno-linearno pomoću k brojeva iz (4); pa neka je

(5) $$z_i \lambda = \sum_{j=1}^{k} q_{ij} z_j.$$

Pri tom su koeficijenti q_{ij} naravno racionalni. Sistem od k jednadžbi (5) pišemo i ovako:

(5) $$\begin{aligned} (\lambda - q_{11}) z_1 - q_{12} z_2 - \cdots - q_{1k} z_k &= 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ -q_{k1} z_1 - q_{k2} z_2 + \cdots + (\lambda - q_{kk}) z_k &= 0. \end{aligned}$$

Time se dobije k jednadžbi za veličine (4). Kako te veličine nisu sve $= 0$, znamo (poglavlje 11, § 10.7) da mora biti

(7) $$\det [\lambda - q] = 0$$

gdje $[\lambda - q]$ označuje razliku skalarne matrice $\lambda(k) = \operatorname{diag}[\lambda, \lambda, \ldots, \lambda]$ i matrice $q = [q_{ij}]$.

No, jednadžba (7) je, za veličinu λ, algebarska jednadžba stupnja $k = mn$; koeficijenti su joj u pravilnoj zavisnosti od matrice q. Jednadžbe oblika (7) od znatne su važnosti (isp. 27, § 8). Jednadžba (7) je normirana i koeficijenti su joj racionalni.

1.7.4.1. Primjer.

$$b = 2^{1/2},\quad c = 3^{1/2},\quad \lambda = b + c.$$

Jednažba za b je

$$x^2 - 2 = 0 \text{ tj. } (2^{1/2})^2 = 2 + 0 \cdot 2^{1/2}.$$

Slično

$$(3^{1/2})^2 = 3 + 0 \cdot 3^{1/2}.$$

Niz (4) glasi ovdje ovako:

	1	$3^{1/2}$
$b^0 = 1$	1	$3^{1/2}$
$b = 2^{1/2}$	$2^{1/2}$	$6^{1/2}$

tj. $z_1 = 1,\ z_2 = 2^{1/2},\ z_3 = 3^{1/2},\ z_4 = 6^{1/2}$.

Množimo $\lambda = b + c$ sa članovima toga niza; izlazi;

$$\begin{aligned} z_1\lambda &= 0 \cdot z_1 + z_2 + z_3 + 0 \cdot z_4 \\ z_2\lambda &= 2 \cdot z_1 + 1 \cdot z_4 \\ z_3\lambda &= 3\, z_1 + z_4 \\ z_4\lambda &= 3\, z_2 + 2\, z_3; \end{aligned}$$

to znači da je matrica

$$q = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 1 \\ 0 & 3 & 2 & 0 \end{bmatrix};\ \text{jednadžba (7) glasi}$$

$$\begin{vmatrix} \lambda & -1 & -1 & 0 \\ -2 & \lambda & 0 & -1 \\ -3 & 0 & \lambda & -1 \\ 0 & -3 & -2 & \lambda \end{vmatrix} = 0, \text{ odnosno } \lambda^4 - 10\,\lambda^2 + 1 = 0$$

Dokaz teorema 1.7.4. ujedno pokazuje da vrijedi i

⟶ **1.7.5. Teorem.** ***Ako su b, c dva cijela algebarska broja a $f(x, y)$ kakav god polinom s koeficijentima iz D, tada je i broj $f(b, c)$ cio algebarski broj.***

Ujedno je sadržinom teorema 1.7.4. i 1.7.5. prebrođena glavna poteškoća da se dokaže

⟶ **1.7.6. Glavni teorem.** ***Skup A svih algebarskih brojeva je jedno tijelo; skup EA svih cijelih algebarskih brojeva je prsten ili kolo.***

1.8. Primjeri dijelova tijela *A* koji su i sami tijela.

1.8.1. Vidjeli smo da je množina A algebarskih brojeva tijelo. No, A je dio opsežnijeg tijela ili korporacije, npr. tijela K kompleksnih brojeva. Sa svoje strane, tijelo A obuhvata npr. skup Q racionalnih brojeva kao svoje *podtijelo.* Da li u A ima i drugih podtijela osim tijela Q? Jasno je da ima! Npr. tijelo $Q(2^{1/2})$ svih »*racionalnih izraza u odnosu na* $2^{1/2}$ *nad* Q« (kao rezervom za koeficijente).

Uopće, za svaki npr. prost broj p imamo tijelo $Q(p^{1/2})$; ono obuhvata tijelo Q a obuhvaćeno je u tijelu ili organizaciji A.

1.8.2. Sva su ta tijela ne samo nejednaka nego i *neizomorfna*: tj. ne može se udesiti između njih tolikovanje t pri čemu bi suma prešla u sumu a produkt u produkt.[1]

1.8.3. Uopće, ako je r proizvoljan racionalan, a n prirodan broj, možemo promatrati skup $Q(r^{1/n})$ vrijednosti svih racionalnih funkcija u odnosu na $r^{1/n}$ — taj je skup tijelo, kao što se brzo provjeri. Specijalno se tijela $Q(r^{1/2})$ zovu *kvadratna tijela.* Takva su tijela npr. $Q(2^{1/2})$, $Q(i)$, $i=(-1)^{1/2}$; to je Gaussovo tijelo; $Q((-5)^{1/2})$, itd.

1.8.4. *Primjer tijela* $Q(2^{1/3})$. Tu osnovni zakon kaže da je

(1) $$x^3-2=0 \quad \text{a} \quad x=2^{1/3}=\rho,$$

i sve se eventualne redukcije imaju toga pravila pridržavati. Nerastavljivost od x^3-2 nad Q izlazi iz 5 § 8.4. Inače se radi po pravilima kao da je ρ iz Q. Zato će npr. biti

$$\rho^4=\rho^3\,\rho=2\,\rho;\ \rho^{14}=\rho^{3\cdot 4+2}=\rho^{3\cdot 4}\cdot\rho^2=(\rho^3)^4\cdot\rho^2=2^4\,\rho^2.$$

$$\rho^{-1}=1\cdot\rho^{-1}=(\rho^2\cdot\rho^{-2})\cdot\rho^{-1}=\rho^2\,(\rho^{-2}\,\rho^{-1})=\rho^2\cdot(\rho^3)^{-1}=2^{-1}\cdot\rho^2.$$

Na taj način, u $Q(\rho)$ pojavljuje se uz ρ i ρ^2 te $\frac{\rho}{\rho}=1$ te $1+\rho+\rho^2$ te

(2) $$a_0+a_1\,\rho+a_2\,\rho^2,$$

za proizvoljne racionalne brojeve a_0, a_1, a_2.

1.8.4.1. *I baš svi ti izrazi* (2) *upravo i čine zgodan prikaz svih članova korporacije* $Q(\rho)$.

1.8.4.2. Naime, u prvom redu dva izraza q, q' oblika (2) jednaka su onda i samo onda, ako su koeficijenti po redu jednaki:

$$a_0=a'_0,\quad a_1=a'_1,\ a_2=a'_2.$$

1.8.4.3. Zbrajanje i množenje se vrši na očigledan način. Najzanimljivije je sa dijeljenjem, odnosno s recipročnom vrijednosti.

[1] Inače, bez ovih dodatnih zahtjeva, tolikovanje je moguće: sva su ta tijela jednakobrojna kao i skup N prirodnih brojeva, odnosno tijelo A svih algebarskih brojeva.

1.8.4.4. Nađimo a^{-1}, ako je

(3) $$a = a_0 + a_1 \rho + a_2 \rho^2 \text{ i } a \neq 0.$$

Postupak je tipičan: Prvi korak. Uz izraz, odnosno broj (3) promatra se pripadni *polinom*

(4) $$a(x) = a_0 + a_1 x + a_2 x^2;$$

(5) $$a(\rho) = a.$$

Drugi korak. Njegov stupanj je manji nego stupanj broja ρ, odnosno polinoma $M(\rho)(x) = x^3 - 2$ iz osnovne veze (1).

Treći korak. Kako je polinom $M(\rho)$ množidbeno nerastavljiv, polinomi $a(x)$ i $M(\rho)(x)$ su prosti međusobno, tj.

(6) $$M(a(x), M(\rho)(x)) = 1.$$

Četvrti korak. Relacija (6) prema Euklid-Bézoutovu teoremu (7 § 5.5) ima za posljedicu, da se broj 1 može pomoću njih izraziti ovako

(7) $$a(x) \cdot A(x) + M(\rho)(x) B(x) = 1,$$

pri čemu su A i B polinomi s koeficijentima iz tijela Q.

Peti korak. Uvrstimo li sada u Bézoutovu vezu $x = \rho$ izlazi

$$a(\rho) \cdot A(\rho) + M(\rho)(\rho) B(\rho) = 1.$$

što zbog

(8) $$M(\rho)(\rho) = 0$$ daje

$$a(\rho) A(\rho) = 1 \quad \text{tj.} \quad \text{(gledaj (5))}$$

$$a \cdot A(\rho) = 1. \quad \text{Dakle} \quad A(\rho) = a^{-1}.$$

I to je tražena recipročna vrijednost broja a.

Na posve isti način dokazuje se ovaj

→ **1.8.5. Osnovni teorem o algebarskim tijelima.**

Ako je ρ bilo koji algebarski broj, tada skup $Q(\rho)$ svih vrijednosti racionalnih funkcija u odnosu na ρ i s koeficijentima iz Q jest određeno tijelo. Svi cijeli algebarski brojevi koji su u $Q(\rho)$ čine kolo (prsten) brojeva, pa čak i oblast cijelih (Isp. § 2). Svaki element $a \in Q(\rho)$ ima jedan jedini zapis oblika

$$a = a_0 + a_1 \rho + a_2 \rho^2 + \ldots + a_{s-1} \rho^{s-1},$$

gdje je $s = \operatorname{st} \rho$ i $a_k \in Q$, $k = 0, 1, \ldots, s-1$.

1.9. Zadaci. 1. Zadani su algebarski brojevi: $2^{1/2}$, $2^{1/3}$, $2^{1/4}$, $2^{1/5}$, $\frac{1}{2}(-13 + \sqrt{-115})$; odredi stupanj i polinom što pripada svakom od tih brojeva.

2. Isto pitanje za algebarski broj $2^{1/2} + 2^{1/3}$, odnosno $2^{1/2} \cdot 2^{1/3}$.

3. Koji je od ovih brojeva cio algebarski broj a koji nije cio:
1) $2^{1/3}$, 2) $\frac{1}{3}\cdot 2^{1/3}$, 3) $2^{1/2}+3^{1/2}$.

4. Odredi trag, normu i konjugat (e) broja iz 3. zadatka.

5. Dokaži da su cijeli brojevi iz $Q(i)$ oblika $d+d'i$, $(d, d'\in D)$.

6. Cio algebarski broj iz $Q(\sqrt{-2}), Q(\sqrt{-3}), Q(\sqrt{-7}), Q(\sqrt{-11})$ je oblika $c=d+d'\omega$, pri čemu je $\{d, d'\}\subset D$ te po redu:

$$\omega=\sqrt{-2},\ \omega=\frac{1}{2}(1+\sqrt{-n}) \text{ za } n=3,\ 7,\ 11.$$

Norma od c je po redu:

$$d^2+2d'^2,\quad d^2+d'^2+dd',\quad d^2+dd'+2d'^2,\quad d^2+dd'+3d'^2.$$

7. Dokaži da je $N(xy)=N(x)\,N(y)$, $T_r(xy)=T_r(x)+T_r(y)$.

2. OBLAST CIJELIH ILI INTEGRITETNO PODRUČJE

2.1. Definicija. *Oblast cijelih ili integritetno područje* je svako asocijativno kolo ili prsten s neutralnim jediničnim elementom i u kojem nema nula-divizora (tj. produkt dvaju članova je 0 onda i samo onda ako je bar jedan faktor $=0$). Oblast cijelih obično se označuje sa I.

2.2. Djeljivost u oblasti cijelih. — 2.2.1. Promatrajmo jednostavan slučaj tijela $Q(m^{1/2})$ gdje je m cio broj bez kvadratnih cijelih faktora $\neq 1$.

Pripadna oblast cijelih je zapravo skup

(1) $D+Dm^{1/2}$ brojeva oblika $d+d'm^{1/2}$,

gdje je $d, d'\in D$.

Definicija djeljivosti je kao i uvijek: ako je $ab=c$ i pri tom $a, b, c\in(1)$, tada je c djeljivo sa a i b. Malo drukčiji je

2.2.2. *Pojam jednote ili jednotnog elementa u oblasti cijelih.* Svaki element iz oblasti cijelih koji u toj oblasti ima svoju recipročnu vrijednost zove se *jednota* ili *jednotni element* u toj oblasti cijelih. Svaki jednotni član može se označiti sa ε. Skup svih jednotnih članova neka bude (ε).

Imajmo na umu ovo: ako je I oblast cijelih ili integritetno područje, tada I kao takvo ima *svoj jedinični element* ili *jedinicu* — jedan jedini — (obično se označuje sa $1, j, u, e$, itd.). Druga je stvar to, a druga je stvar *jednota* ili *jednotan član* ε u I. Tako npr. u oblasti D cijelih brojeva, jedinični element je jedino broj 1 (jer iz $D\cdot x=xD\cdot=D\cdot$ nužno izlazi $x=1$).

No, uz 1 također je -1 jednota, jer i -1 ima u D svoju recipročnu vrijednost. Dakle u D vrijedi $\varepsilon=+1$, $\varepsilon=-1$.

Recimo u oblasti cijelih Gaussovih brojeva imamo bar ove 4 jednote: $\varepsilon=1,\ i,\ -1,\ -i$, jer svaki od tih brojeva zadovoljava jednakost $xx^{-1}=1$. Ujedno se vidi da drugih jednotâ tu i nema.

Jer ako je

$$\varepsilon = x + iy, \ \varepsilon^{-1} = u + iv,$$

tada iz

$$(x + iy)(u + iv) = 1$$

izlazi

$$xu - yv = 1$$

$$xv + yu = 0. \text{ Pri tom su } x, y, u, v \in D.$$

Odatle imamo

$$(xu - yv)^2 + (xv + yu)^2 = 1$$

$$(x^2 + y^2)(u^2 + r^{-2}) = 1.$$

Odatle probavanjem izlazi da je $\varepsilon \in \{1, -1, i, -i\}$.

Na sličan način se dokaže da oblast $D(2^{1/2})$ ima bar ove jednote: ± 1, $\pm (1 + 2^{1/2})$, $\pm (3 + 2 \cdot 2^{1/2})$, $\pm (1 - 2^{1/2})$, $\pm (3 - 2 \cdot 2^{1/2})$ (ima ih 10).

Tijelo $(R, +, .)$ realnih brojeva kao tijelo pogotovo je jedna „oblast cijelih"; u toj oblasti svaki broj $\neq 0$ je „jednotan" ali jedino je broj 1 jedinični element. Zbog tog preobilja jednotnih članova u R tu se na njih ni ne gleda s toga gledišta nego se traže baš oni članovi koji nisu jednotni — to je 0 i samo 0.

2.2.2.1. Teorem. *Svi jednotni elementi u oblasti cijelih čine množidbenu grupu, specijalno: produkt i kvocijent dvaju jednotnih članova opet je jednotan član.*

Sa pojmom jednotnog člana tijesno su povezani

2.2.3. Asocirani (pridruženi) članovi u oblasti cijelih.

2.2.3.1. Definicija. Član a je pridružen (asociran) članu b, ako je $a = \varepsilon b$ za neki jednotni član ε iz I.

Tako npr. u I-oblasti $(D, +, .)$ broju 3 pridružen je broj 3 te jedino još broj -3; u I-oblasti $D(i)$ broju 3 pridruženi su $3, 3i, -3, -3i$; u I-oblasti $(R, +, .)$ broju 3 pridruženi su svi realni brojevi $\neq 0$.

2.2.3.2. O pridruženim brojevima vidi se da vrijedi ovo: *Svojstvo pridruživanja je jedna relacija ekvivalencije.*

2.2.3.3. Skup svih elemenata oblasti I koji su pridruženi sa x može se označiti $A(x; I)$. On je $= x(\varepsilon) =$ skup svih $x\varepsilon$. Na taj način, I se cijepa na razrede $A(x, I)$ oblika $x(\varepsilon)$. Tako npr. D je unija razredâ:

$$\{0\}, \ \{-1, \ 1\}, \ \{-2, \ 2\}, \ldots$$

Ti su razredi dva po dva disjunktna.

U Gaussovu kolu $D(i)$ razredi su 4-člani (osim razreda $\{0\}$ koji se sastoji od 0) i ovakvog su oblika

$$\{c, ci, -c, -ci\} \text{ (4 vrha romba sa središtem 0)}$$

U svakoj oblasti cijelih treba promatrati funkciju $x \to x(\varepsilon)$.

2.3. Nerastavljivost ili nesvodljivost u I. Prosti elementi u kolu, odnosno u I.

2.3.1. Definicija. Član n iz integritetnog područja I je *nerastavljiv ili nesvodljiv* (ireducibilan) ako je $\neq 0$, različit od svakog ε te ako je djeljiv jedino sa ε i svakim svojim pridruženikom εn.

2.3.2. Član $x \neq 0$ integritetnog područja I je *rastavljiv ili svodljiv* (*reducibilan*), ako je on produkt od dva člana iz I, a da nijedan od tih faktora nije pridruženik elementa 1 ili elementa x.

Prema tome, čitavo I se cijepa u 4 dijela i to: $\{0\}$, skup pridruženika od 1, skup nerastavljivih (ireducibilnih) elemenata i skup rastavljivih elemenata.

Jedan ili oba od posljednjih dvaju skupova mogu biti prazni. Tako npr. u prstenu realnih ili kompleksnih brojeva nema nijednog nerastavljivog broja.

2.3.3. Prosti elementi. Element p iz I je prost ili prim u I ako

$$(\{b, c\} \subset I) \wedge p \mid bc \Rightarrow p \mid b \vee p \mid c \quad \text{(znak } \mid \text{ čitati „dijeli“).}$$

$\longrightarrow$ **2.3.4.** Teorem. *Svaki prost član p je nerastavljiv; obrat ne mora vrijedeti.* Neka je naime p prosto; neka je također $p = mn$; dakle

$$p \mid mn \quad \text{pa} \quad p \mid m \vee p \mid n; \quad \text{recimo neka} \quad p \mid m \quad \text{tj.} \quad m = p \cdot q \quad \text{dakle}$$

$$p = mn = (pq)\, n = p\,(qn), \quad \text{tj.} \quad p = p\,(qn) \Rightarrow 1 = qn; \qquad \text{dakle}$$

je n jednota, odnosno n je pridruženo jedinici.

Obrat ne vrijedi. Tako npr. u prstenu $(2\,D, +, .)$ član 30 je nerastavljiv ali nije prost, jer npr. 30 dijeli 6.10 premda ne dijeli ni 6 ni 10. U prstenu $D[\sqrt{-3}]$ koji je sastavljen od brojeva oblika $x + y\sqrt{-3}$ broj 2 je nerastavljiv jer jednadžba

$$2 = (x + y\sqrt{-3})\;(x - y\sqrt{-3}) = x^2 + 3\,y^2$$

nije moguća; naprotiv broj 2 tu nije prost jer je npr.

$$2 \mid 4 (\equiv (1 + \sqrt{-3})\,(1 - \sqrt{-3}) \quad \text{premda 2 ne dijeli ni } 1 + \sqrt{-3}$$
$$\text{ni } 1 - \sqrt{-3}.$$

2.3.4.1. U jednostavnijim prstenima kao npr. D, $D[x]$, $R[x]$, $D[i]$ svojstvo prostosti i nerastavljivosti se podudaraju.

Odnos između prostosti i nerastavljivosti vezan je uz jednoznačnost i višeznačnost faktorizacije u nerastavljive faktore kao što to pokazuje:

$\longrightarrow$ **2.3.5.** Teorem. *Ako je faktorizacija u nerastavljive elemente u jednoj oblasti cijelih jednoznačna, onda je u toj oblasti svaki nerastavljiv element i prost, dakle je tada nerastavljivo* $\equiv$ *prosto* (isp. npr. t. 2.6.4.6).

Dokaz. Neka je n nerastavljivo; dokažimo da je n prosto. Pa neka $n \mid bc$; tada rastavljanjem članova $a = \dfrac{bc}{n}$, b i c u nerastavljive elemente jednakost $na = bc$ imala bi kao posljedicu činjenicu da bi n kao nerastavljivo moralo biti pridruženo nekom faktoru od b ili c pa bi dakle n dijelilo b ili c.

2.4. Problem faktorizacije. — 2.4.1. Radi se o tome da se zadan element prikaže kao produkt drugih, specijalno, *nerastavljivih*, odnosno *prostih* članova, ukoliko je to moguće.

Tako npr. polinom x^3-1 kao član u $D[x]$ je produkt nerastavljivih jedinki $x-1$, x^2+x+1. Isto to vrijedi shvatajući x^3-1 kao član zajednice $R[x]$; no u još široj zajednici $C[x]$ svih polinoma sa kompleksnim koeficijentima, tročlan x^2+x+1 je složen (rastavljiv) jer je

$$x^2+x+1=\left(x-\frac{1+i\sqrt{3}}{2}\right)\left(x-\frac{1-i\sqrt{3}}{2}\right).$$

2.4.2. *Primjer broja* 5. On je nerastavljiv u kolu $(D; +, .)$; no broj 5 je rastavljiv u Gaussovu kolu $D(i)$, jer je $5=(1+2i)(1-2i)$, a ovi faktori nisu jednote niti su pridruženi sa 5. Može se pokazati da su oba ta faktora nerastavljiva i međusobno prosta u smislu da im je najveća zajednička mjera $=\varepsilon$.

Dokažimo da se broj 5 drukčije ni ne može rastaviti u nerastavljive faktore (ne gledajući na prisustvo pridruženih brojeva i jednotâ jer naravno $5=\varepsilon\cdot\varepsilon^{-1}\cdot 5$ za svaku jednotu $\varepsilon=\pm 1, \pm i$).

Naime iz

(1) $$(x+iy)(u+iv)=5$$

prelazeći na norme imamo

N(1) $$(x^2+y^2)(u^2+v^2)=25$$

i time smo iz kola $D(i)$ prešli u kolo D. Iz N(1) izlazi da je nužno

$$x^2+y^2\in\{1,\ 5,\ 25\}\ni u^2+v^2.$$

Članstvo 1 otpada jer bi to značilo da je $x+iy$ jednota a to nam ne treba. Prema tome imamo $x^2+y^2=5$. No, tu je jednadžbu lako riješiti; rješenja su joj $(\pm 1, \pm 2)$; to su rješenja i za (u, v). Isprobavanjem se vidi da imamo zaista $x+iy=\varepsilon(1+2i)$, $u+iv=\varepsilon^{-1}(1-2i)$, kao što smo i tvrdili.

Specijalno treba uočiti bitan prelaz iz (1) u N(1) jer smo uzimanjem norme na obe strane u jednadžbi (1) prešli time iz manje poznatog kola $D(i)$ na bolje poznato svakidašnje kolo D. Pojava je općenita.

2.4.3. Može se dokazati da je *faktorizacija u nerastavljive faktore jednoznačna i u Gaussovu kolu kao i u kolu D.* Uostalom, tako je Gauss i došao do toga da se uopće primijeti jednoznačnost rastavljanja prirodnih brojeva u nerastavljive faktore — stvar je previše svakidašnja da bi je čovjek svijesno ispitivao u kolu D. Ali, u kolu $D(i)$ stvar nije više tako očigledna (isp. opći teorem 2.7.4).

2.5. Prsten ili kolo $D[\sqrt{-5}]=D+D\sqrt{-5}$. — 2.5.1. Nađimo mu jednote, tj. nađimo mu parove (x, y) *cijelih racionalnih* brojeva za koje postoji sličan par (u, v) sa svojstvom

(2) $$(x+y\sqrt{-5})(u+v\sqrt{-5})=1.$$

Prelazeći na normu:

N(2) $$(x^2+5y^2)(u^2+5v^2)=1.$$

Sad smo u kolu D. Pa iz $N(2)$ očigledno izlazi $y=0=v$. Dakle je $x=\pm 1=v$; imamo jedino dva slučaja:

$$x=1, \quad y=0, \quad u=1, \quad v=0 \quad \text{(prvi slučaj)}$$
$$x=-1, \quad y=0, \quad u=-1, \quad v=0 \quad \text{(drugi slučaj).}$$

2.5.2. To znači da je $\varepsilon=\pm 1$. Tako vidimo da kolo $D[\sqrt{-5}]$ ima samo dvije jednote i to iste dvije ± 1 koje ima i naše obično kolo D.

Međutim, baš ta srodnost sa D na jednoj strani vuče za sobom veliku razliku između D i $D[\sqrt{-5}]$ na drugoj strani. Pogledajmo!

2.5.3. Rastavimo broj 9 u nerastavljive faktore! Kao pripadniku zajednice D, rastav je ovakav: $9=3\cdot 3$ (9 je čak kvadrat nerastavljivog broja 3). Da vidimo da li je to prim faktorizacija i u zajednici $D[(-5)^{1/2}]$.

Da li je 3 prosto i u $D[\sqrt{-5}]$? Ogledajmo rastav

$$(x+y\sqrt{-5})\,(u+v\sqrt{-5})=3. \tag{3}$$

Odatle prelazeći na norme:

$$(x^2+5y^2)\,(u^2+5v^2)=9. \tag{N(3)}$$

Tu smo sada na poznatom tlu, pa je jedan od faktora ili 1 ili 9; prvi slučaj otpada jer bi to značilo da je odgovarajući faktor u (3) neka jednota ε; dakle je $x^2+5y^2=9$.

2.5.4. Međutim odatle izlazi $x=\pm 3$, $y=0$ itd, pa se zaista vidi da je broj 3 sačuvao svoju nerastavljivost i u $D[\sqrt{-5}]$.

2.5.5. Međutim vidi se da je također

$$9=(2+\sqrt{-5})\,(2-\sqrt{-5}), \tag{4}$$

a dokazuje se upravo kao za broj 3 da su oba faktora u $(4)_2$ nerastavljivi u novoj zajednici $D[\sqrt{-5}]$. Nadalje, sva tri nerastavljiva broja

$$3, \quad 2+\sqrt{-5}, \quad 2-\sqrt{-5} \tag{5}$$

međusobno su nepridružena: nijedan ne izlazi iz kojeg drugog množenjem sa ε (vidjeli smo da je $\varepsilon=-1$, 1).

2.5.6. Nova pojava. Tako smo otkrili *novu pojavu: već tako bliska zajednica kao što je prsten $D[\sqrt{-5}]$ ne uživa fundamentalno svojstvo o jednoznačnosti faktorizacije*, jer eto njezin član 9 dopušta dvije nejednake prim faktorizacije:

$$9=3\cdot 3 \quad \text{te} \quad 9=(2+\sqrt{-5})\,(2-\sqrt{-5}). \tag{6}$$

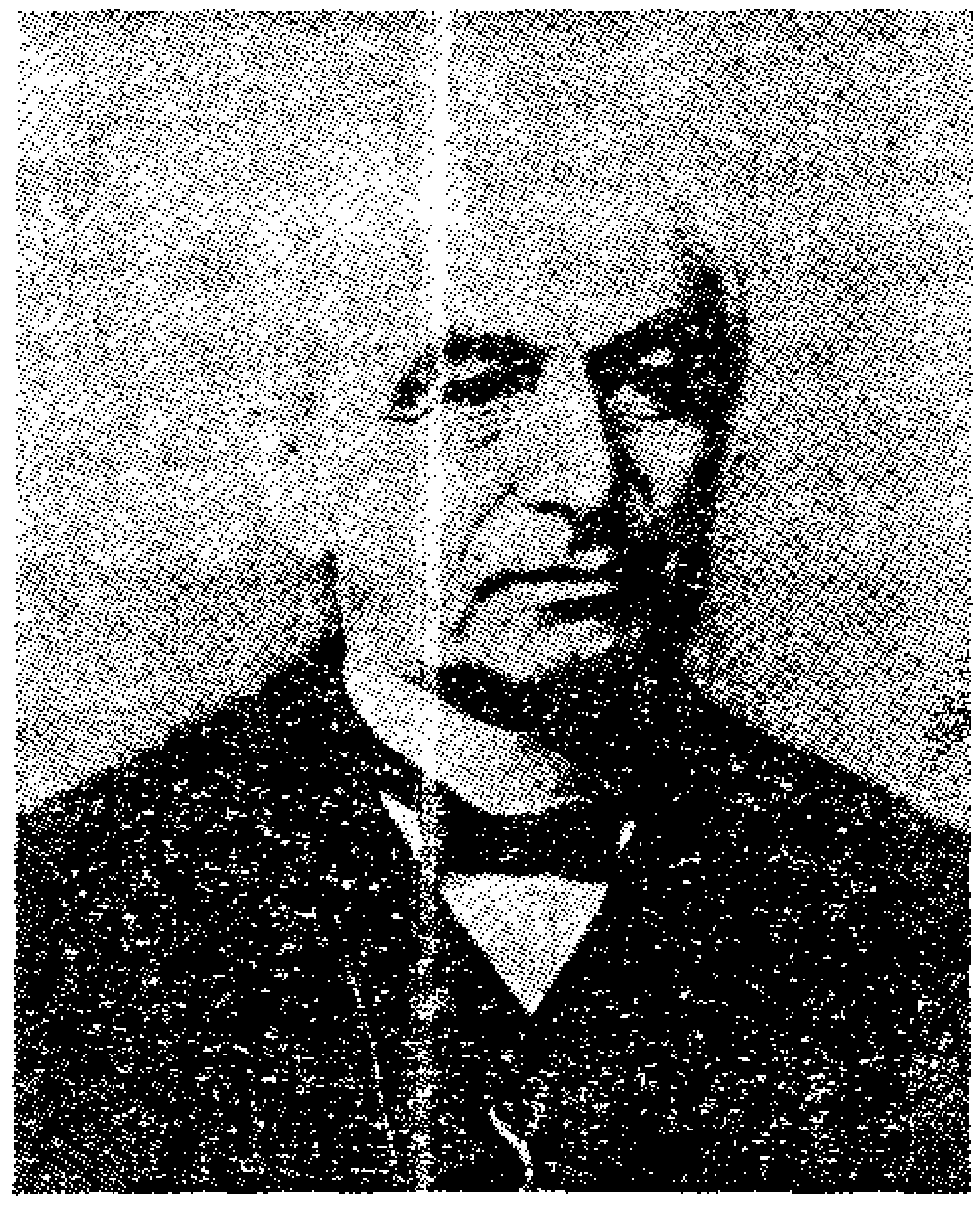
2.5.7. Odatle ujedno vidimo

$$3\cdot 3=(2+\sqrt{-5})\cdot(-2\sqrt{-5}) \tag{7}$$

da *produkt cijelih pa čak i produkt od dva nerastavljiva cijela može biti djeljiv trećim nerastavljivim cijelim koji nije pridružen nijednom od njih.*

Tu je pojavu otkrio polovinom 19. vijeka E. E. Kummer (1810—1893), njemački matematičar. To je bio povod da se uvedu tzv. *ideali*. Na tom su polju mnogo radili R. Dedekind (1831—1916) (v. sliku 1, § 1.3.) i Kronecker (1823—1891), njemački matematičari. Danas se zna da pri faktorizaciji češće nastupa nejednoznačnost nego jednoznačnost.

E. E. Kummer (1810—1893), začetnik teorije ideala.



L. Kronecker (1823—1891), poznat njem. matematičar.

2.5.8. Teško se čovjeku pomiriti s tako velikim iznenađenjem da tako reći na dlanu postoji zajednica kao što je prsten $D[\sqrt{-5}]$ pa da nema jednoznačne proste faktorizacije. Da razmatranje nije bilo pregrubo? Da nismo možda ispustili koji prost faktor itd. i da faktorizacija nije otišla dovoljno daleko! (isp. § 3).

2.6. Najveći (najmanji) zajednički djelitelj (kratnik). Relativno prosti članovi. — **2.6.1.** *Najveći zajednički djelitelj* dvaju ili više članova prstena definira se kao zajednički djelitelj tih elemenata koji je djeljiv *svakim* zajedničkim djeliteljem.

Naravno, najveći zajednički djelitelj d nije individualno određen, jer je i εd najveći djelitelj; pri tom ε znači bilo koji jednotni element.

Najveći zajednički djeljitelj od a, b označuje se kao i obično;

$$a\mathrm{M}b \quad \text{ili} \quad \mathrm{M}(a, b);$$

općenito, on nije jednoznačno određen.

Specijalno, ako je $a\mathrm{M}b = 1$, kaže se da su a, b međusobno prosti.

2.6.2. Za najveći zajednički djelitelj $d = a\mathrm{M}b$ u nekom kolu A vezan je skup dA svih produkata dA' pri $A' \in A$ — tu se nalaze svi zajednički djelitelji elemenata a, b.

Nastaje pitanje (isp. pogl. 6, § 10.6.) da li vrijedi ili ne vrijedi osnovna jednakost

$$aA + bA = (a\mathrm{M}b)A, \tag{1}$$

odnosno da li se aMb može linearno izraziti pomoću a, b s koeficijentima iz A.

Drugim riječima, da li vrijedi

(2) $$aMb = a\alpha + b\beta \quad \text{uz uslov} \quad \alpha \in A \text{ i } \beta \in A?$$

Relacija (2) vrijedi u kolu cijelih racionalnih brojeva, u kolu Gaussovih brojeva, itd.

2.6.3. Međutim, relacija (2) ne vrijedi npr. u kolu

(3) $$K = D[\sqrt{-5}].$$

Tako npr. promatrajmo proste brojeve: 3, $1+2\sqrt{-5}$ u kolu (3). Njihov najveći zajednički djelitelj je 1, jer smo vidjeli da su ti brojevi prosti i nerastavljivi. Dakle:

(4) $$3M(1+2\sqrt{-5}) = 1 \quad \text{u kolu } D[\sqrt{-5}].$$

Pokušajmo broj 1 izraziti u obliku (2) tj.

(5) $$3(x+y\sqrt{-5}) + (1+2\sqrt{-5})(u+v\sqrt{-5}) = 1,$$

gdje su x, y, u, $v \in D$.

$$3x + 3y\sqrt{-5} + u + 2u\sqrt{-5} + v\sqrt{-5} + 2\cdot(\sqrt{-5})^2 v = 1$$

Odatle na osnovu propisane veze $(\sqrt{-5})^2 = -5$ izlazi:

$$(3x+u-10v) + (3y+2u+v)\sqrt{-5} = 1.$$

Dalje prelazimo u kolo D:

$$\begin{array}{l} 3x+u-10v = 1 \\ 3y+2u+v = 0 \quad + \\ \hline 3(x+y+u-3v) = 1. \end{array}$$

A ta jednakost u kolu D naših običnih cijelih brojeva nije moguća. Dakle relacija (5) a time zbog (4) ni (2) u $D[\sqrt{-5}]$ ne stoji.

2.6.4. Euklidski prsteni. Oslanjajući se na Euklidov algoritam o dijeljenju brojeva, odnosno polinoma (isp. 6 § 10.3, pogl. 7 § 5.3) postavlja se

2.6.4.1. D e f i n i c i j a. Oblast I cijelih sa bar dva člana zove se Euklidov prsten, ako je svakom $i \in I \setminus \{0\}$ moguće pridružiti određen prirodni realni broj $vi \in \{0, 1, 2, \ldots\}$ i da je

(1) $$v(ab) \geq v(a),\ v(b),$$

te da vrijedi osnovni iskaz o dijeljenju:

$$\text{za } a,\ m \in I, \quad (m \neq 0),$$

postoje q, $r \in I$ sa svojstvom

(2) $$a = mq + r \quad \text{te}$$

(3) $$v(m) > v(r) \quad \text{ili} \quad r = 0.$$

2.6.4.2. Primjeri. Npr. u D se stavlja $vD^{\cdot}=|D^{\cdot}|$; u $K[x]$ se stavlja $va=$ stupanj od a za svako $a\in K[x]\setminus\{0\}$, zato je $K[x]$ Euklidov prsten za svako tijelo K.

⟶ **2.6.4.3. Teorem.** *U svakom Euklidovu prstenu može se za proizvoljne $a, b\in I$ odrediti $M(a, b)$ pomoću Euklidova algoritma. Specijalno je tada*

$$M(a, b)=a\cdot A+bA, \quad \textit{za nekoje elemente} \quad A, B \ \textit{u} \ I.$$

Dokaz je analogan dokazu za slučaj $I=D$, odnosno $I=R[x]$ (isp. pogl. 6, § 10.6, § 12.3).

⟶ **2.6.4.4. Teorem.** *Svaki strogo silazni diobeni lanac Euklidova prstena A_E je konačan, tj.*

Ako je $a_1, a_2, \ldots\in A_E$ te $a_{n+1}|a_n$, $a_n\neq a_{n+1}$, tada je skup $\{a_1, a_2, \ldots\}$ konačan.

Dokažimo najprije ovo.

2.6.4.4.1. Lema. *Ako su a, m članovi Euklidova prstena A_E, tada*

$$(1) \qquad (1)\,[m\,|\,a\wedge\neg\,(a\,|\,m)] \;\Rightarrow\; va>vm$$

(oznake su kao u definiciji **32, § 2.6.4.1**).

Uslov $(1)_1$ znači da je za neko $c\in A_E$

$$a=mc$$

i da c nije jednota prstena (v. 32, § 2.2.2). Neka, prema definiciji 2.6.4.1 bude

$$m=aq+r \quad \text{te ili} \quad r=0 \quad \text{ili} \quad va>vr.$$

Međutim, ne može biti $r=0$, jer bi to značilo da je $m=aq$, tj. $a|m$, u protivnosti sa $(1)_1$. No, $r\neq 0$ znači prema 2.6.4.1 da je

$$(2) \qquad v(a)>v(r).$$

Nadalje je $r=m-aq=m-(mc)q=m(1-cq)$. Kako je $1-cq\neq 0$ jer c nije jednota, uslov (1) u 2.6.4.1 traži $v(r)\geq vm$. A ovo zajedno sa (2) daje traženi zaključak $(1)_2$.

Time je lema dokazana; iz nje odmah izlazi i sam teorem 2.6.4.4 jer prema lemi $va_1>va_2>\cdots$ pa kao strogo silazan niz rednih brojeva mora taj niz biti konačan.

⟶ **2.6.4.5. Teorem. Svaki nerastavljiv član Euklidova prstena je prost, pa je nerastavljivo≡prosto** (isp. § 2.3.5).

Dokaz. Neka je p' nerastavljiv član u prstenu A_E; neka je $a, b\in A_E$ te $p'|(ab)$; to znači da je $ab=p'q$. Treba dokazati da je $p'|a\vee p'|b$.

Ako je $p'|a$, stvar je u redu. Ako nije $p'|a$, tada su p', a relativno prosti (zbog nerastavljivosti od p'). Dakle je $M(p', a)=1$ pa zato postoje elementi x, $y\in A_E$ za koje je $ax+p'y=1$. Odatle množeći sa b:

$$abx+bp'y=b.$$

Nadalje iz $ab=p'q$ izlazi množeći sa x:

$$abx=p'qx.$$

Odatle

$$p'qx + bp'y = b \qquad \text{tj.}$$

$$p'(qx + by) = b \qquad \text{dakle zaista } p' \mid b.$$

—→ **2.6.4.6. Teorem. U svakom Euklidovu prstenu primfaktorizacija je jednoznačna.**

Dokaz je isti kao u slučaju cijelih brojeva ili polinoma (6. § 14, 7 § 7.2.),

2.6.4.7. Korolar. Ako je K bilo koje tijelo, tada je u prstenu $K[x]$ primfaktorizacija provediva jednoznačno.

Teorem izlazi iz 2.6.4.7. i 2.6.4.2.

2.7. *PF*-prsteni. — 2.7.1. Definicija. Svaki prsten u kojem se svaki element $\neq 0$ može na jednoznačan način prikazati kao produkt prostih elemenata zove se *PF-prsten,* tj. primfaktorizacija je jednoznačno izvediva (pri tom se naravno ne gleda na redoslijed faktora kao ni na djelitelje jedinice).

Tako npr. $(D, +, .)$ je *PF*-prsten; međutim odmah ćemo dokazati jedan teorem iz kojeg će proizaći razni drugi *PF-prsteni.*

—→ **2.7.2. Teorem.** ***Neka je I oblast cijelih. Ako:***

(*i*) ***svaki nerastavljiv element iz I je prost;***

(*ii*) ***svaki čisto silazni diobeni lanac u I je konačan;***
onda I dopušta jednoznačnu faktorizaciju, tj. I je PF-prsten.

Dokaz. Iz uslova (*ii*) izlazi da je svaki član $a \in I \setminus \{0\}$ produkt od konačno mnogo nerastavljivih elemenata:

$$a = a_1 a_2 \ldots a_n; \tag{1}$$

zbog uslova (*i*) predstavlja (1) ujedno određenu primfaktorizaciju. Još treba dokazati jednoznačnost. Pa neka je također

$$a = p_1 p_2 \ldots p_r \tag{2}$$

primfaktorizacija od a. Iz (1) i (2) izlazi pišući

$$p_1 p_2 \ldots p_r = 1 \cdot p_1 p_2 \ldots p_r \quad \text{(ovo je po } (i) \text{ dopušteno):}$$

$$a_1 a_2 \ldots a_n = 1 \cdot p_1 p_2 \ldots p_r. \tag{3}$$

Pretpostavimo da je $n \neq r$, npr. $n < r$.

No, a_1 je prosto; zato a_1 dijeli neki faktor p_{v_1} produkta $(3)_2$; kako je i p_{v_1} prosto znači da su a_1, p_{v_1} pridruženi, tj. za neku jednotu e_1 je $a_1 = e_1 p_{v_1}$; skraćujući jednadžbu (3) sa p_1 izlazi

$$e_1 a_2 \ldots a_n = p_1' p_2' \ldots p'_{r-1}, \tag{3'}$$

pri čemu desna strana od (3′) izlazi iz $(3)_2$ brisanjem faktora p_{v_1}.

Na isti način zaključujemo da iz (3′) nastaje

$$(3'') \qquad e_1 e_2 a_3 \ldots a_n = p_1'' p_2'' \ldots p_{r-2}'',$$

pri čemu je e_2 jednota, a desna strana od (3″) nastaje iz produkta u $(3')_2$ ispuštanjem nekog od $r-1$ faktora. Postupak se nastavlja pa se nakon n koračaja dolazi do veze

$$(3^{(n)} \qquad e_1 e_2 \ldots e_n = 1 \cdot p_1^{(n)} p_2^{(n)} \ldots p_{r-n}^{(n)};$$

pri tom su $e_1, e_2, \ldots, e_n$ jednote. Napose prema $(3^{(n)})$ prost broj $p_1^{(n)}$ bio bi djelitelj jednote $e = e_1 e_2 \ldots e_n$, što je nemoguće. Dakle nije $n<r$. Isto tako nije $n>r$. Dakle je $n=r$.

Na osnovu teorema 2.6.4.3. — 2.6.4.5, 2.7.2. imamo

⟶ **2.7.3. Teorem.** ***Svaki Euklidov prsten A_E dopušta jednoznačnu primfaktorizaciju: A_E je PF-prsten; simbolički $A_E \in PF$.*** (v. t. 3.3.10).

Međutim. nije svaki član iz PF euklidski, jer npr. $D[x] \in PF$.

2.7.3.1. Naprotiv $D[x]$ nije A_E tj. nije euklidski. Kad bi naime bilo $D[x]$ neko A_E, moglo bi se za konstantu 2 i identičku transformaciju $jx = x$ koja je iz $D[x]$ i relativno prosta prema 2 (tj. $2\,\mathrm{M}\,j = 1$) naći određene članove $f(x), g(x) \in D[x]$ za koje je

$$x f(x) + 2 g(x) = 1;$$

odatle za $x=0$ izašlo bi $2g(0)=1$, što je nemoguće jer je $2g(0)$ paran cio broj.

Dakle nije $D[x]$ euklidsko; s druge strane dokazat ćemo da je $D[x] \in PF$; vrijedi naime

2.7.4. Teorem. Ako je cjelosna oblast I neki PF-prsten, tada je i $I[x]$ određen PF-prsten; i obrnuto. Simbolički,

$$I \in PF \Leftrightarrow I[x] \in PF \text{ (isp. 32 § 2.7.8).}$$

2.7.4.1. Drugi dio teorema je očigledan jer elementi prstena I kao konstante nalaze se i u $I[x]$ kao elementi. Zato nam još preostaje dokazati da $I \in PF \Rightarrow I[x] \in PF$. Dokaz izlazi iz teorema 2.7.2 jer $I[x]$ zadovoljava uslove (*i*), (*ii*), toga teorema 2.7.2. Uslov da $I[x]$ ima jedinicu je očigledan jer konstanta 1 je jedinični element od $I[x]$; uslove (*i*), *ii*), izreći ćemo kao teoreme 2.7.5. i 2.7.7.

2.7.5. Teorem. Ako $I \in PF$, onda svaki čisto silazni diobeni lanac članova prstena $I[x]$ jest konačan.

Dokaz. Neka je

$$a(x) \in I[x],\ a(x) = a_0 + a_1 x + \ldots + a_n x^n;$$

kako je $\{a_0, a_1, \ldots, a_n\} \subset I$, može se $d_a = M(a_0,, a_1, \ldots, a_n)$ odrediti; stavljajući

$$\frac{a_\nu}{d_a} = a^\star{}_\nu,\ a^\star = \sum_{\nu=0}^{n} a^\star{}_\nu x^\nu,$$

bit će $\qquad a(x) = d_a \cdot a^\star(x),\ M(a_0{}^\star, a_1{}^\star, \ldots, a^\star{}_n) = 1;$

pri tom je d_a određeno jednoznačno do jednotnog faktora; isto vrijedi za „primitivni" polinom $a^{\star}(x)$. Pri tom vrijedi

2.7.6. *Definicija primitivnih polinoma.* Polinom

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

je primitivan, ako je

$$M(a_0, a_1, a_2, \ldots, a_n) = 1.$$

Upravo dokazasmo da vrijedi

2.7.6.1. Lema. Iz

$$a(x) \in I[x], \quad a(x) \neq 0 \ \text{i} \ d_a = M(a_0, a_1, \ldots, a_n)$$

izlazi da je

$$a(x) = d_a \cdot a^{\star}(x), \quad \text{gdje je} \quad a^{\star}(x) \ \text{primitivno.}$$

Inače je važna

2.7.6.2. Gaussova lema. *Umnožak $f = gh$ dvojke primitivnih polinoma g, h je primitivan polinom* (isp. pogl. 7, § 7.4).

Stvarno, kad $f = gh$ ne bi bilo primitivno, tada bi neko prosto p dijelilo *svaki* koeficijent f_{γ} od f a ne bi dijelilo svaki koeficijent ni od g ni od h; neka je g_i (odnosno h_j) prvi koeficijent od g (odnosno od h) koji nije djeljiv sa p; tada se kao u 7, § 7.4 vidi da ni f_{i+j} nije dijeljivo sa p.

A sada nastavimo s dokazivanjem teorema 2.7.5; promatrajmo čisto silazan diobeni lanac polinoma $p(x) \in I[x]$:

$$(1) \qquad a(x) \underset{1}{|} b(x) \underset{1}{|} c(x) | \ldots \ (\text{definiramo } a \underset{1}{|} b \text{ kao } b \,|\, a).$$

$$a(x) \underset{1}{|} b(x) \Leftrightarrow d_a \underset{1}{|} d_b \wedge a^{\star}(x) \underset{1}{|} b^{\star}(x)$$

pri čemu ne može biti $\underset{1}{|}$ zamijenjeno sa $=$. Prema tome imamo

$$(2) \qquad d_a \underset{1}{|} d_b \underset{1}{|} d_c \ldots$$

$$(3) \qquad a^{\star}(x) \underset{1}{|} b^{\star}(x) \underset{1}{|} c^{\star}(x) \ldots;$$

pri tom svakom $|$ koji u (2) odnosno u (3) označuje znak $=$ odgovara u (3), odnosno u (2) znak $\underset{1}{|} \neq$.

U nizu (2) znak $\underset{1}{|}$ stoji konačno mnogo puta umjesto $=$, jer iz (3) izlazi za stepene

$$\text{st}\, a^{\star} \geq \text{st}\, b^{\star} \geq \text{st}\, c^{\star} \geq \ldots$$

s konačno mnogo znakova $>$ za $\geqq$.

U nizu (2) stoji $\underset{1}{|}$ konačno mnogo puta za $\neq$ jer je prema pretpostavci $I \in PF$. Dakle je niz (2) konačan; time je i niz (1) konačan.

—→ **2.7.7. Teorem.** ***Ako je $I \in PF$, onda je svaki nerastavljivi (ireducibilni) element $a(x)$ iz $I[x]$ prost.***

Dokaz. Ako je $a(x)$ konstanta p, tada je $p \in I$, pa je p kao nerastavljivo u $I \in PF$ ujedno u I prosto (teorem 2.3.5); dokažimo da je tada p prosto i u $I[x]$, tj. da pri

$$b(x),\ c(x) \in I[x]$$

vrijedi

(4) $$p \mid b(x)\, c(x) \Rightarrow p \mid b(x) \vee p \mid c(x).$$

No, $$b(x) = b_b \cdot b^\star(x),\ c(x) = d_c c^\star(x).$$

Prema Gaussovoj lemi 2.7.4.5. zaključujemo da je

$$d_{bc} = d_b d_c,\ (b(x)\, c(x))^\star = b^\star c^\star$$

pa rastav

$$bc = d_{bc}(bc)^\star$$

daje

$$bc = d_b \cdot d_c (bc)^\star.$$

Kako primitivan polinom $(bc)^\star$ ne može biti djeljiv sa p to relacija $p \mid bc = p \mid (d_b d_c)(bc)$ postaje $p \mid d_b d_c$; no sad smo u I pa zato

$$p \mid d_b d_c \Rightarrow p \mid d_b \vee p \mid d_c \quad \text{a time} \quad p \mid b \vee p \mid c.$$

Dakle je (4) ispravno.

Ako $a(x)$ nije konstanta, tada kao nerastavljiv, polinom $a(x)$ je primitivan ($a = a^\star$); kako je $b^\star c^\star$ primitivan polinom i $a \mid bc$, tj. $a \mid d_b d_c)(b^\star c^\star)$ znači da je

(5) $$a(x) \mid b^\star(x)\, c^\star(x).$$

Cijele racionalne funkcije $a(x)$, $b^\star(x)\, c^\star(x)$ su specijalni članovi prstena $K[x]$, gdje je K tijelo definirano kao $I \times (I \setminus \{0\})$ na isti način kao što se tijelo Q definira pomoću prstena D. No, $K[x] \in PF$; zato nerastavljivo $a(x)$ je prosto u $K[x]$, pa iz (5) izlazi

(6) $$a \mid b^\star \vee a \mid c^\star.$$

Recimo da je $a \mid b^\star$, tj. da je

(7) $$b^\star(x) = a(x) \cdot q(x), \quad \text{sa} \quad q(x) \in K[x].$$

Neka je

$$q(x) = \frac{r_0}{s_0} + \frac{r_1}{s_1} x + \frac{r_2}{s_2} x^2 \ldots + \frac{r_n}{s_n} x^n,$$

pri čemu su $r_i \in I$, $s_i \in I \setminus \{0\}$, $i = 1, 2, \ldots, n$. Ako je s najmanji zajednički kratnik od $s_0, s_1, \ldots, s_n$, bit će

$$q(x) = \frac{1}{s} t(x) \text{ uz } t(x) \in I[x],$$

odnosno

$$q(x) = \frac{1}{s} d_t t^\star(x);$$

skraćujući po potrebi razlomak $\frac{d_t}{s}$ izlazi

(8) $$q(x) = \frac{A}{B} t^\star(x),$$

gdje su A, B iz I te $A \mathrm{M} B = 1$.

Time (7) pomnoženo sa B a na osnovu (8) daje

(9) $$Bb^\star(x) = a(x) At^\star(x).$$

Na osnovu Gaussove leme je

$$(9)_2{}^\star = a(x)\, t^\star(x);$$

znači da je $$A = eB,$$
gdje je e neka jednota iz I te

$$b^\star = at^\star;$$

tj. $b^\star$ je djeljivo sa a i to u $I[x]$; tim prije je u $I[x]$ djeljivo i $b(x)$ sa a jer je $b(x) = d_b b^\star(x)$, pri čemu je $d_b \in I$.

Slično se iz $a \mid c^\star$ u $K[x]$ dokazuje $a \mid c$ u I. Time je teorem 2.7.7. dokazan. A to je bilo preostalo dokazati da zaključimo da vrijedi i sam teorem 2.7.4.

Kao poopćenje prvog dijela teorema 2.7.4. imamo

$\longrightarrow$ **2.7.8. Teorem.** ***Ako cjelosna oblast I dopušta jednoznačnu primfaktorizaciju, onda to vrijedi i za prsten $I[x_1, x_2, \ldots x_n]$, pri čemu je n bilo koji prirodni broj; simbolički:***

$$I \in PF \Rightarrow I[x_1, x_2, \ldots, x_n] \in PF.$$

Naravno, $I[x_1, \ldots, x_n]$ sastoji se od svih polinoma u odnosu na neodređenice $x_1, x_2, \ldots, x_n$ s koeficijentima iz I.

Dokaz se provodi *induktivno* s obzirom na broj n. Teorem je ispravan za $n = 1$ — to je upravo sadržaj teorema 2.7.4. Pretpostavimo da je teorem 2.7.8. ispravan za neko $n = k \geq 1$; dokažimo da je on ispravan i za $n = k + 1$. No, $I[x_1 \ldots x_{n+1}]$ je u odnosu na x_{k+1} određen prsten

$$I'[x_{k+1}] = I[x_1 \ldots x_k x_{k+1}] \text{ s koeficijentima iz } I[x_1 \ldots x_k];$$

no ovaj prsten po pretpostavci je PF-prsten; zato primjenom teorema 2.7.4. na taj PF-prsten izlazi upravo tvrdnja iz teorema 2.7.8. za $n = k + 1$.

2.9. Zadaci o oblasti cijelih.

1. Navedi bar jedan lanac u $(2D; |)$ koji ima: 1) 3; 2) 5; 3) n članova.
2. Isto pitanje za $(mD, |)$; pri tom je $m \in D \setminus \{0\}$.
3. Je li $(2D, +, .)$ oblast cijelih? 2) Dokaži da je svaki nerastavljiv član oblika $2(2k+1)$; 3) ako su p, q prosti prirodni brojevi >2, tada je $2pq$ nerastavljivo u $2D$ premda nije prosto u $2D$ (npr. $2pq$ dijeli $2p \cdot 2q$ premda ne dijeli ni $2p$ ni $2q$).

4. 1) Dokaži da je $(mD, +, .)$ oblast cijelih za svako $0 \neq m \in D$; 2) Navedi u $(3D, +, .)$ nekoliko nerastavljivih članova koji nisu prosti; 3) Da li za svako $m > 1$, $m \in D$ oblast $(mD, +, .)$ ima bar jedan nerastavljiv član koji nije prost?

5. Zašto se u $D[x]$ Euklidov algoritam ne može primijeniti na dvojku 1) $3, x$; 2) $7, 3x$?

6. Je li u $(mD, +, .)$ svaki diobeni 1) čisto silazni; 2) čisto uzlazni niz konačan?

7. Da li su pozitivni brojevi $2^{2^{-1}}, 2^{2^{-2}}, 2^{2^{-3}}, \ldots, 2^{2^{-n}}, \ldots$ algebarski cijeli brojevi? 2) Je li svaki od njih djeljiv svim narednima? 3) Je li u $(EA, +, .)$ svaki diobeni čisto uzlazni niz konačan?

8. Izvesti potpun dokaz da je $D[x_1, x_2]$ Euklidov prsten i da prsten $D[x_1, x_2]$ dopušta jednoznačnu faktorizaciju.

9. 1) U $D[i]$ prosti brojevi su upravo obični prosti brojevi koji su oblika $4n+3$; 2) nijedan prirodni broj p koji je prost u D i za koje je $p \equiv 1 \pmod 4$ nije prost u $D[i]$.

10. Iz zad. 9. 2) dokazati da je svako takvo p suma dvaju kvadrata (Fermat).

11. U $Q(\sqrt{-5})$ prosti su upravo oni prosti p iz D za koje je $\left(\frac{-3}{p}\right) = -1$.

3. POJAM IDEALA

3.0. Ideja. Riječ je o vrlo općem odnosu između cjeline C i pojedinog njena dijela C_0 koji je i sam zatvoren isto kao i što je *zatvoren s obzirom na djelovanje iz C*. Najobičniji je slučaj da se promatra ideal prstena i tijela, no može se promatrati i ideal grupe, grupoida itd. Ideali strukture S su ne samo odgovarajuće podstrukture od S nego još zadovoljavaju dodatni tipični *idealski zahtjev da su zatvorene prema djelovanju elemenata iz S.*

Radit ćemo s proizvoljnim prstenom $(A, +, .)$ (isp. definiciju u 26, § 7.9.5; također 6, § 6.2), pa ćemo se uvjeriti da je uloga ideala u prstenu slična ulozi invarijantne podgrupe u grupi.

3.1. Svojstvo nule u prstenu. Aditivni neutral 0 prstena A ima definiciono svojstvo da je $a+0=a=0+a$ za svako $a \in A$. Dokažimo

$\longrightarrow$ **3.1.1. Teorem o multiplikacionom svojstvu nule.** *Za svaki prsten $(A, +, .)$ i svako $a \in A$ vrijedi*

(1) $$a0 = 0 = 0a \qquad \text{tj.}$$

(2) $$A0 = \{0\} = 0A. \qquad \textit{Specijalno je } 0 \cdot 0 = 0.$$

Dokaz. V. 13, § 12.

3.1.2. *Ako je prsten A asocijativan i za svako* $a, b \in A$ *pri uslovu* $a \neq 0$ *sadrži bar jedno rješenje jednadžbe* $ax = b$, *tada je A bez nula-divizora, tj.* $A \setminus \{0\}$ *je grupoid prema množenju.*

Neka je

$$a, b \in A \setminus \{0\}, \quad \text{dakle} \quad a \neq 0 \neq b;$$

pretpostavimo da je ipak $ab = 0$. Tada je prema 3.1.1.

$$0 = 0 \cdot c = (ab)\, c \quad \text{za svako} \quad c \in A \quad \text{i specijalno za} \quad c = y,$$

gdje je $by = x$, $ax = a$. No, tada je

$$0 = (ab)\, y = a\,(by) = ax = a, \quad \text{tj.} \quad 0 = a, \quad \text{protivno sa} \quad 0 \neq a.$$

—→ **3.2. Množenje relativnih elemenata u prstenu.**

Pišemo li $0 + a = +a$, $0 - a = -a$, tada je u svakom prstenu

(1) $$+\boldsymbol{a} \cdot +\boldsymbol{b} = +(\boldsymbol{ab})$$

(2) $$+\boldsymbol{a} \cdot -\boldsymbol{b} = -(\boldsymbol{ab})$$

(3) $$-\boldsymbol{a} \cdot +\boldsymbol{b} = -(\boldsymbol{ab})$$

(4) $$-\boldsymbol{a} \cdot -\boldsymbol{b} = +(\boldsymbol{ab})$$

(5) $$\boldsymbol{a}^2 = (-\boldsymbol{a})^2.$$

D o k a z. Dokažimo (1).

$$+a \cdot +b = (0 + a)\ (0 + b) = 0 \cdot 0 + a \cdot 0 + 0 \cdot b + ab =$$
$$= 0 + 0 + 0 + ab = 0 + ab = +ab.$$

Obrazac (2) je ekvivalentan sa

(2′) $$+a \cdot -b + ab = 0.$$

Zato je dovoljno dokazati (2′). No,

$$+a \cdot -b + ab = +a \cdot -b + (+a)\ (+b) = +a\,(-b + b) = a \cdot 0 = 0.$$

Analogno je

$$-a \cdot +b = -(ab) \Leftrightarrow -a \cdot +b + ab = 0.$$

No, $$-a \cdot +b + ab = -a \cdot +b + (+a)\ (+b) = (-a + a)\ (+b) = 0 \cdot b = 0.$$

Još preostaje dokazati relaciju (4) koja je ekvivalentna sa

$$-a \cdot -b - ab = 0.$$

No, $$-a \cdot -b + (-a) \cdot (+b) = (-a)\ (-b + b) = -a \cdot 0 = 0.$$

Time je teorem 3.2. dokazan. Ujedno vidimo da su obrasci (1) — (4) posljedice aksiomâ grupe i aksioma o distributivnosti. Naglašavamo da (1) — (4) vrijedi za *svaki* (komutativni ili nekomutativni) prsten a ne samo za kojekakve prstene realnih ili kompleksnih brojeva.

3.3. Definicija ideala prstena $(A, +, .)$. Svaka podgrupa $(G, +)$ grupe $(A; +)$ za koju vrijedi $\quad a \in A,\ g \in G \Rightarrow ag \in G,$

tj.
$$\{ag;\ a \in A,\ g \in G\} \equiv AG \subset G$$

zove se *lijevi ideal prstena*; svaka aditivna podgrupa $(G, +)$ grupe $(A; +)$ za koju je
$$\{ga;\ g \in G,\ a \in A\} \equiv GA \subset G$$

zove se *desni ideal prstena*; pri tom je dakle $AG = \{ag;\ a \in A,\ g \in G\}$.

3.3.1. Obostrani ideal ili naprosto **ideal** u A zove se svaki podskup od A koji je istovremeno i desni i lijevi ideal.

Naravno ista definicija odnosi se i na *ideale tijela.*

3.3.2. Ne kažemo li obrnuto, pretpostavljat ćemo da je prsten komutativan pa se zato lijevi, desni i obostrani ideali podudaraju.

Npr. $2D$ je ideal prstena $(D, +, .)$.

3.3.3. *Nula-ideal prstena* je onaj ideal koji je sastavljen jedino od aditivno-neutralnog člana. *Jedinični ideal prstena* je onaj koji se podudara sa čitavim prstenom. Za svako $a \in A$ skup aA (odnosno Aa) je desni (lijevi) ideal.

3.3.4. Ideal proizveden zadanim podskupom S prstena A s jediničnim članom. To je skup (S) svih „linearnih kombinacija" $a_1 s_1 + a_2 s_2 + \ldots + a_n s_n$ pri čemu vrijedi
$$n \in N,\ \{a_1, \ldots, a_n\} \subset A,\ \{s_1, \ldots, s_n\} \subset S.$$

Neposredno se provjeri da je (S) ideal prstena A.

Umjesto $(\{s_1, s_2, \ldots, s_n\})$ piše se također $(s_1, s_2, \ldots, s_n)$ kao „oznaka" za ideal proizveden od $s_1, s_2, \ldots, s_n$.

Posebno, za svako $a \in A$ imamo odgovarajući »*glavni*« *ideal* $(a) = aA$.

3.3.5. Glavni ideali. Ideali oblika $xA \equiv \{xa;\ a \in A\}$ zovu se *glavni ideali*; pri tom je $x \in A$. Umjesto aA, odnosno Aa piše se naprosto (a). Tako npr. kad je riječ o prstenu D, onda (3) znači ideal $(3D, +, \cdot)$.

3.3.5.1. Da se izbjegne nesporazum može se uz redni broj formule staviti . (tačka); npr. (3) je ideal, a (3.) je oznaka formule.

3.3.6. Glavnoidealski prsteni. Ako je svaki ideal prstena A glavni, kaže se da je prsten *glavnoidealski.*

Tako npr. je u 6. § 12.2 dokazano da je $(D, +, \cdot)$ glavnoidealski prsten; na isti se način dokazuje

⟶ **3.3.7. Teorem.** ***Svaki euklidski prsten E* (isp. 2.6.4.) *je glavnoidealski, tj. svaki ideal je oblika aE, pri čemu a leži u E.***

Neka je naime I ideal euklidskog prstena E; ako je $I = \{0\}$, sve je dokazano; ako nije $I = \{0\}$, neka je i član iz I za koji je broj vi iz definicije 2.6.4.1.

minimalan; tada za svako $x \in I$ imamo $x = iq + r$, pri čemu je $q \in E$, $r \in I$ te ili $r = 0$ ili $vi > vr$; po definiciji elementa i slučaj $vi > vr$ ne dolazi u obzir; dakle je $r = 0$, tj. $x = iq$, tj. $x \in iA$, dakle zaista $I = iA$.

3.3.8. *Prsten* $D[x]$ *nije glavnoidealski.* Npr. ideal $(2; x)$ sastavljen od svih izraza $2a(x) + xb(x)$ uz uslov $a, b \in D[x]$ nije oblika $cD[x]$ ni za koje $c \in D[x]$.

3.3.9. Noetherovi prsteni. Prsten u kojem je **svaki** ideal proizveden od *konačnog podskupa* zove se *Noetherov prsten.*[1] Oni su prirodna generalizacija glavnoidealskih prstena (isp. § 3.3.6.).

U § 2.7.3. smo dokazali da je u svakom euklidskom prstenu E moguća jednoznačna primfaktorizacija; prema 3.3.7. E je glavnoidealski prsten. Da li možda teorem 2.7.3. vrijedi i za *svaki glavnoidealski prsten*? Odgovor glasi:

—→ **3.3.10. Teorem.** ***U svakom glavnoidealskom prstenu A s jedinicom vrijedi teorem o jednoznačnoj primfaktorizaciji. Drugim riječima, svaki glavnoidealski prsten A s jedinicom je P F-prsten*** **(isp. 2.7.1.).**

Teorem 3.3.10. ćemo dokazati na osnovu teorema 2.7.2, tj. dokazat ćemo da vrijedi 3.3.11. kao i 3.3.12.

3.3.11. Teorem. *U svakom glavnoidealskom prstenu s jedinicom svaki nerastavljivi član p' je prost.*

Neka $p' \mid (ab)$. Ako nije $p' \mid a$, dokažimo da $p' \mid b$. Naime, ako nije $p' \mid a$, onda su p', a relativno prosti tj. $p' M a = 1$ pa se dokaz provodi kao i u § 2.6.4.6. Jedino, treba obrazložiti da $p' M a$ stvarno postoji; a to se vidi iz činjenice, što je $p' M a$ upravo onaj član prstena A koji proizvodi ideal proizveden elementima p', a.

3.3.12. Teorem. *Ako je A glavnoidealski prsten s jedinicom, tada svaki strogo silazni diobeni lanac u A je konačan:*

$$(1) \qquad a_1 \underset{1}{|} a_2 \underset{1}{|} a_3 \underset{1}{|} a_4 \underset{1}{|} \cdots$$

je konačno; pri tom $x \underset{1}{|} y$ znači: x je djeljivo sa y ali y nije djeljivo sa x.

Neka je naime I skup svih članova prstena koji su djeljivi bar jednim članom iz (1). Tada je I ideal. Najprije, ako $x, y \in I$, tada neka a_ξ bude prvi član iz (1) koji dijeli x; isto tako neka a_η bude prvi član iz (1) koji dijeli y. Tada je $\xi \leq \eta$ ili $\xi > \eta$; ako $\xi \leq \eta$, tada $a_\eta \mid y$, $a_\eta \mid a_\xi$, što zajedno sa $a_\xi \mid x$ daje $a_\eta \mid x$; dakle a_η dijeli i x i y dakle i $x + y$, $x - y$, odakle izlazi da je I podgrupa prstena A. Slično za $\xi > \eta$. Očigledno je $AI \subset I$. Dakle je zaista I ideal. Po pretpostavci, I je glavni ideal, dakle $I = aA$ za neko $a \in A$. Neka je a_n *prvi* član u nizu (1) kojim je upravo to a djeljivo: $a_n \mid a$.

Tvrdimo da je a_n posljednji član niza (1). Kad bi naime postojalo a_{n+1}, bilo bi $a_{n+1} \mid a_n$; no zbog $a_{n+1} \in aA$ bilo bi $a \mid a_{n+1}$; dakle bi bilo $a_{n+1} \mid a_n \mid a \mid a_{n+1}$ što znači da bi a_n, a_{n+1} bili pridruženi, protivno pretpostavci da je $a_n \underset{1}{|} a_{n+1}$.

Time je dokazano 3.3.12 i 3.3.10.

[1] Prema njemačkoj matematičarki Emmy Noether (1882—1935), kćerki matematičara M. Noethera (1844—1921); isp. Math. Annalen 83 (1921) 24—66.

3.4. Računanje mod I, za zadan ideal I. — 3.4.1. Ideal kao podgrupa odnosno potprsten.

Svaki ideal prstena je određen potprsten. Ne mora svaki potprsten prstena $(A; +, \cdot)$ biti ideal. Specijalno je svaki ideal I prstena A određena podgrupa; zato se može promatrati pripadno cijepanje A/I i pripadna faktorska grupa odnosno pripadni faktorski prsten, sastavljen od svih skupova oblika

$$I + a \, (a \in A), \tag{1}$$

pri čemu se »računa« po prirodnim zakonima:

$$(I+a)+(I+b) = I+(a+b). \tag{2}$$

$$(I+a) \cdot (I+b) = I+(a \cdot b). \tag{3}$$

3.4.2. Faktorski ili kvocijentni prsten A/I. Drugim riječima, za svaki ideal I prstena A promatra se obitelj A/I svih skupova (1) pa se u njoj definira zbrajanje i množenje pomoću obrazaca (2) i (3).

Neposredno se provjerava da time A/I postaje prstenom.

3.4.3. Pridruživanje

$$a \in A \to \underline{a} = I + a \in A/I$$

zadovoljava

$$\underline{a+b} = \underline{a} + \underline{b}$$

$$\underline{ab} = \underline{a}\,\underline{b}$$

tako da se radi o *homomorfiji zadana prstena A na faktorski prsten A/I.* Pri tom svakom elementu $i \in I$ ideala I odgovara *»nula«* I faktorskog prstena.

3.4.4. Obrnuto, neka je $(A', +' \cdot')$ proizvoljan prsten koji je homomorfna slika prstena $(A, +, \cdot)$; tada svi elementi $a \in A$ koje homomorfija h prevodi u $0'$ prstena A' čine ideal $I = h^{-1}\{0'\}$ prstena A pa se lako vidi da su prsteni A/I, $(A', +', \cdot')$ izomorfni. Naime, preslikavanje f koje svakom $X \in A/I$ pridjeljuje element $fx \in A'$, gdje je $x \in X$, jest određena izomorfija između A/I, A'.

3.4.5. Izaberemo li iz svakog $X \in A/I$ neki član $x \in X$, dobije se određen skup P koji se zove *potpuno »predstavništvo prstena A modulo ideal I«*; naime kao i kod brojeva i funkcija, i ovdje se uvodi

3.4.6. Pojam kongruencije (klasifikacije) u odnosu na ideal I.

Ako je I ideal (prstena A), tada se kaže da je član a iz A kongruentan ili *podudaran* modulo I sa članom a_1 iz A i piše $a \equiv a_1 \pmod I$ onda i samo onda ako a, a_1 leže u jednom te istom razredu mod I, tj. ako je $I + a = I + a_1$, odnosno ako je $a - a_1 \in I$.

3.4.7. Neposredno se dokazuje da je za zadan ideal I kao modul relacija $\equiv$ određena relacija ekvivalencije.

3.4.8. Također se neposredno provjeravaju ova pravila o računanju s kongruencijama:

kongruencije $a \equiv a_1 \pmod{I}, \quad b \equiv b_1 \pmod{I}$

daju

$$a+b \equiv a_1+b_1 \pmod{I}$$
$$ab \equiv a_1 b_1 \pmod{I}$$
$$a^n \equiv a_1{}^n \pmod{I}$$

za svako $n \in N$.

3.5. Računanje s idealima.

Kako su ideali skupovi ili množine izvađene iz prstena ili kola A — u kojem se računa, to se *računanje (struktura) sa cjeline A prenosi i na računanje (strukturu) s idealima $I \subset A$.* Specijalno nas ovdje zanima zbrajanje i množenje ideala.

3.5.1. Zbrajanje ideala. — **3.5.1.1.** *Definicija sume.* Ako su I, J dva ideala, tad se pod sumom $I+J$ ideala I, J razumijeva skup svih suma $i+j$ njihovih članova $i \in I, j \in J$.

⟶ **3.5.1.2. Teorem.** ***Zbroj dvaju ideala I, J prstena A opet je ideal tog prstena A. Specijalno, zbroj dvaju glavnih ideala $(a)=aA$, $bA=(b)$ je određen ideal koji ne mora biti glavni ideal, tj. ne mora biti***

$$(1) \qquad aA+bA=cA$$

ni za koje $c \in A$.

Ako takvo c postoji, tj. vrijedi li (1), onda je $aMb=c$, što znači da je c upravo najveći zajednički djelitelj elemenata a, b.

Provjeravanje, odnosno dokaz toga teorema 3.5.1.2. je vrlo jednostavno: treba naime provjeriti da $I+J$ ispunjava sva četiri aksioma o grupi (17 § 6) kao i aksiom idealnosti $(I+J)A \subset I+J$. Posebno se vidi da je posljednji aksiom posljedica relacija

$$(I+J)A=IA+JA \text{ i } IA \subset I, \ JA \subset J.$$

3.5.2. Množenje ideala. — **3.5.2.1.** *Definicija produkta,* Pod produktom ili *umnoškom* $I \cdot J$ ideala I i ideala J razumijevamo skup svih elemenata

$$i_1 j_1 + i_2 j_2 + \cdots + i_n j_n$$

pri čemu n prolazi skupom N te

$$\{i_1, \ldots, i_n\} \subset I, \ \{j_1, \ldots, j_n\} \subset J.$$

Prema tome, produkt $I \cdot J$ definiramo ne kao inducirani proizvod

$$IJ=\{ij;\ i \in I, j \in J\}$$

nego kao ideal proizveden od tog induciranog proizvoda (isp. § 3.3.4).

Na sasvim sličan način se dokazuje

3.5.2.2. Teorem. **Produkt dvaju ideala prstena opet je ideal.**

3.5.3. Dijeljenje ideala. Dijeljenje ideala **ne definira se neposredno** kao obrat množenja nego se postavlja ova

3.5.3.1. Samostalna definicija kvocijenta ideala. *Kvocijent $I:J$ ideala I i ideala J je skup svih $a \in A$ za koji je $aJ \subset I$ tj.*

$$I:J = \{a;\ a \in A,\ aJ \subset I\}.$$

Lako se provjeri da je $I:J$ ideal i da vrijedi

3.5.3.2. Teorem. $I:J$ je najveći (tj. najobuhvatniji) ideal X za koji je

$$J \cdot X \subset I.$$

3.5.4. Presjek $I \cap J$ ideala I i ideala J također je ideal; zove se *najmanji zajednički kratnik od I, J* (isp. § 3.6.3.).

3.5.5. Teorem o računanju s idealima. ***Ako su B, C, D ideali prstena $(A, +, \cdot)$, tada je***

$$\mathbf{B \cdot C \subset B \cap C}, \tag{1}$$

$$\mathbf{(B+C) \cdot D = B \cdot D + C \cdot D}, \tag{2}$$

$$\mathbf{(B \cap C) : D = (B : D) \cap (C : D)}, \tag{3}$$

$$\mathbf{B : (C+D) = (B : C) \cap (B : D)}, \tag{4}$$

$$\mathbf{(B : C) : D = B : (C \cdot D)}. \tag{5}$$

Obrazac (3) [odnosno (4)] zove se *prvi* [*drugi*] *distributivni zakon dijeljenja ideala.*

Dokaz. Jednakost (2) vrijedi ne samo za ideale nego i za bilo kakve neprazne podskupove prstena. Relacija (1) izlazi neposredno iz definicije produkta $B \cdot C$ i iz svojstva idealnosti skupova B, C.

Dokažimo (3). Dokažimo najprije $(3)_1 \subset (3)_2$, tj. $x \in (3)_1 \Rightarrow x \in (3)_2$. No, $x \in (3)_1$ znači da je $xD \subset B \cap C$ tj. $xD \subset B$ i $xD \subset C$, dakle je $x \in B:D$ i $x \in C:D$, dakle $x \in (3)_2$. Idući natrag u tom lancu zaključivanja vidi se da je $(3)_2 \subset (3)_1$. Time je (3) dokazano.

Dokažimo (4).

$$x \in (4)_1 \Rightarrow x(C+D) \subset B \Rightarrow xC + xD \subset B$$
$$\Rightarrow (xC \subset B) \wedge (xD \subset B) \Rightarrow (x \in B:C)$$
$$\wedge\ (x \in B:D) \Rightarrow x \in (4)_2.$$

I dualno: $(4)_2 \subset (4)_1$.

Dokažimo (5).

$$x \in (5)_1 \Rightarrow xD \subset (B:C) \Rightarrow xD \cdot \in (B:C)$$
$$\Rightarrow xD \cdot C \subset B \Rightarrow xDC \subset B \Rightarrow x \in B:(CD). \qquad \text{I dualno.}$$

3.6. Djeljivost — **3.6.1.** Primjer. Ideal $6D$ je dio ideala $2D$ u jednu ruku, a u drugu ruku je $2|6$, tj. $6 \equiv 0 \pmod 2$. Analogno se postavlja

3.6.2. *Definicija djeljivosti među idealima.* Neka su I, J ideali: ako je $I \subset J$, kaže se da je: *I podideal* od *J* ili *da je I djeljivo sa J* pa se piše $J|I$ ili $I \equiv 0 \pmod J$; također se kaže da je *J nadideal* od *I* ili da *J* dijeli *I*. Kaže se da je *I kratnik od J*, odnosno da je *J mjera* (faktor) od *I*. Umjesto $a \in I$ piše se i $a \equiv 0 \pmod I$, jer je jasno da iz $a \in I$ izlazi $aA \subset I$ tj. $aA \equiv 0 \pmod I$.

Odmah se vidi da ta definicija prikladno prevodi osnovnu sliku o djeljivosti na razmatranja o relaciji inkluzije.

3.6.3. Najmanji (najveći) zajednički kratnik (faktor) zadanih ideala $I, J, \ldots$ jest onaj zajednički kratnik (faktor) kojim je djeljiv (kojeg dijeli) svaki zajednički kratnik (faktor) tih ideala.

⟶ **3.6.3.1. Teorem.** ***Presjek zadanih ideala jest najmanji zajednički kratnik tih ideala. Ideal proizveden unijom zadanih ideala jest najveći zajednički faktor tih ideala.***

3.7. Prost ideal ili primideal.

3.7.1. Definicija. Ako ideal P zadovoljava

$$P|ab \Rightarrow P|a \vee P|b$$

za svako $a, b \in A$, onda se kaže da je ideal P *prost ili prim u prstenu A*.

Drugim riječima, ako iz $a, b \in A$, $ab \in P$ izlazi $a \in P$ ili $b \in P$, onda je ideal P prost.

⟶ **3.7.2. Teorem.** ***Ideal je prost onda i samo onda, ako je faktorski prsten A/P bez nuladjelitelja, tj. ako iz $X, Y \in A/P$, $XY = P$ nužno izlazi $X = P$ ili $Y = P$.***

Dokaz. Neka je P prost ideal i neka za članove $P+a$, $P+b$ iz A/P vrijedi $(P+a)\cdot(P+b) = P$, tj. $P+ab = P$ tj. $ab \in P$; kako je P prosto, mora biti $a \in P$ ili $b \in P$, a time $P+a = P$ ili $P+b = P$.

Obrnuto, neka iz $a, b \in A$, $P+ab = P$ izlazi $a \in P$ ili $b \in P$; kako je $P+ab = P$ ekvivalentno sa $ab \in P$ znači to da iz $ab \in P$ izlazi $a \in P$ ili $b \in P$, pa je dakle P prosto.

3.7.3. Teorem. *Ideal I je prost onda i samo onda ako on dijeli produkt $J \cdot J'$, dvojke ideala jedino ako dijeli bar jedan od tih faktora.*

Dokaz. Ako je $JJ' \subset I$, $J \not\subset I$, $J' \not\subset I$, onda to znači da postoje $j \in J \setminus I$, $j' \in J' \setminus I$; kako je $jj' \in I$, znači da I ne bi bio prost. Ako I nije prosto, onda postoji $a, a' \in A \setminus I$ za koje je $aa' \in I$; to znači da za pripadne glavne ideale (a), (a'), (aa') imamo

$$(a) \not\subset I, \quad (a') \not\subset I, \quad (ab) \subset I, \quad \text{protivno pretpostavci o } I.$$

3.8. Maksimalni ideal. — **3.8.1.** Definicija. *Maksimalni ideal prstena A* je svaki ideal toga prstena A kojemu je jedino čitavo A pravi nadideal.

3.8.2. Teorem o postojanju maksimalnog nadideala. (W. Krull).[1] *Svaki pravi ideal I prstena s 1 sadržan je u bar jednom maksimalnom idealu I_m.*

Dokaz. Neka H znači obitelj svih ideala koji su $\supset I$ i $\not\in A$. Neka je L proizvoljan maksimalan podskup od parcijalno uređenog skupa H (uređajna relacija je inkluzija) sa svojstvom da bude

$$X, Y \in L \Rightarrow X \subset Y \vee X \supsetneqq Y;$$

postojanje »*maksimalna lanca*« L u $(H, \supset)$ je posljedica aksioma izbora. Stavimo

$$I_m = \cup X \qquad (X \in L).$$

Tada je I_m ideal. To se lako provjeri. No, I_m je i *maksimalan* ideal jer nije $1 \in I_m$.

3.8.3. Lema. *Za svaki maksimalni ideal M prstena A i svako $a \in A \setminus M$ imamo $M + aA = A$.*

Naime, lako se provjeri da je $M + aA$ ideal kojemu je M pravi dio; po definiciji 3.8.1. znači to da vrijedi 3.8.3.

3.8.4. Teorem. *Ako je ideal maksimalan, onda je on prost* (isp. 3.9.7).

Pretpostavimo naprotiv da postoji maksimalan ideal M prstena A i da M nije prosto. To znači da bi za neke $x, y \in A$ bilo $xy \in M$ premda nije $x \in M$ ni $y \in M$. No iz ovih relacija prema 3.8.3. imamo

$$A = M + xA, \ A = M + yA. \text{ Dakle je } A = AA = (M + xA)(M + yA) =$$
$$= (M + xAM + MyA) + xyA = M,$$

jer posebno iz $xy \in M$ izlazi $xyA \subset M$. Dakle bi bilo $A = M$, što se protivi definiciji od M kao pravog dijela od A.

3.8.4.1. Može se dokazati da obrat teorema 3.8.4 vrijedi npr. za prsten $D[x_1, \ldots, x_n]$ za svako $n \in N$.

3.8.4.2. *Primjer prosta ideala koji nije maksimalan*: Ideal (x) prstena $K[x, y]$ (K je proizvoljno tijelo) je prost ali nije maksimalan jer je sadržan u prostu idealu (x, y) (isp. teorem 3.9.7).

$\longrightarrow$ **3.8.5. Teorem. Ako je svaki ideal prstena A glavni, tada su prosti ideali upravo ideali pA, pri čemu je p prost član iz A.**

Dokažimo da je pA prost ideal: ako $xy \in pA$, tada je bar jedan od članova x, y u pA. No, $xy \in pA$ znači da je $xy = pa$ za neko $a \in A$. To znači da p dijeli produkt xy dakle i jedan od faktora x, y; npr. $p \mid x$ dakle $x = pa'$ sa $a' \in A$, tj. $x \in pA$.

Dokažimo obrat: neka je I prost ideal. Kako je po pretpostavci svaki ideal glavni, znači da je $I = aA$ za neko $a \in A$. Dokažimo da je a prosto tj. da za $b, c \in A$ vrijedi

(1) $$a \mid bc \Rightarrow a \mid b \vee a \mid c,$$

No, $(1)_1$ znači da je $bc = aa'$ za neko $a' \in A$; zato je $bc \in I$; odatle zbog pretpostavljene prostosti od I izlazi $b \in I \vee c \in I$.

[1] Wolfgang Krull (20. st.), njemački matematičar.

Ako je $b \in I = aA$, onda to znači da je $b = ay$ za neko $y \in A$; dakle je $a \mid b$. Analogno se dokazuje da $c \in I \Rightarrow a \mid c$. Time je (1) dokazano.

$\longrightarrow$ **3.8.6. Teorem.** ***Ako je u prstenu A s jedinicom svaki ideal glavni, tada je svaki ideal I koji je $\neq \{0\}$, A proizvod konačnog broja prostih ideala; drugim riječima, svaki glavno-idealski prsten je Dedekindov*** **(isp. 3.8.7.).**

Naime, iz $\{0\} \neq I = aA \neq A$ izlazi da nije $a \in \{0, 1\}$; prema teoremu 3.3.10 možemo a prikazati kao produkt prostih članova $p_1, p_2, \ldots, p_n$; no iz $a = p_1 \cdot p_2 \cdots p_n$ izlazi $aA = p_1 A \cdot p_2 A \cdots p_n A$.

3.8.6.1. Primjedba. Iskaz 3.8.6. ne mora ostati na snazi ako je prsten A bez jedinice; npr. $(2D, +, \cdot)$ je glavno-idealski ali nije Dedekindov.

3.8.7. Definicija Dedekindova prstena. Dedekindov prsten je svaka cjelosna oblast u kojoj je svaki ideal koji se razlikuje od $\{0\}$ i A produkt *konačna* broja *prostih* ideala.

3.9. Razlomljeni ideali. — **3.9.1.** Definicija. *Razlomljen ideal cjelosne oblasti* I s jedinicom je svaki skup oblika $\frac{I_0}{d}$; pri tom je I_0 bilo koji ideal, a d je proizvoljan član iz $I \setminus \{0\}$.

Posebno, *glavni razlomljeni ideali* u I jesu oni koji su oblika $\frac{(a)}{d}$.

Naravno, dijeljenje sa d ne mora biti izvedivo u I ali se izvodi jednoznačno u pripadnom kvocijentnom tijelu $I^{:}$; prema tome je $\frac{I_0}{d} \subset I^{:}$.

Kako je $\frac{I_0}{1} = I_0$, svaki ideal je ujedno i razlomljen pa se zove *cijelim idealom.*

Posebno, u tijelu $I^{:}$ član $\frac{a}{d}$ rađa $\frac{1}{d}(a)$ pa se zato glavni razlomljeni ideal $\frac{(a)}{d}$ može označivati i sa $\left(\frac{a}{d}\right)$.

3.9.2. *Množenje razlomljenih ideala* $\frac{1}{x}X, \frac{1}{y}Y$, definira se obrascem

$$\frac{1}{x}X \cdot \frac{1}{y}Y = \frac{1}{xy}XY.$$

Na taj način, skup razlomljenih ideala $\neq 0$ postaje *polugrupom* kojoj je samo ishodno *I jedinični član.* Važan je slučaj kad je ta polugrupa čak i grupa; to *će biti onda i samo onda ako je I Dedekindov prsten.*

3.9.3. *Obrativi razlomljeni ideali* jesu oni razlomljeni ideali B za koje postoji razlomljeni ideal X sa svojstvom $BX = I$; piše se $X = B^{-1}$.

3.9.3.1. Tako npr. za glavne razlomljene ideale $\neq 0$ je očigledno

$$\frac{1}{d}(a)\cdot\frac{1}{a}(d)=I;\ \text{kraće}\ \left(\frac{a}{d}\right)^{-1}=\left(\frac{d}{a}\right).$$

3.9.4. Teorem. *Svaki obrativi razlomljeni ideal B je Noetherov, tj. proizveden je od konačno mnogo članova kvocijentnog tijela I*.

Po definiciji je $BB^{-1}=I$; to posebno znači da za $1\in I$ imamo prikaz oblika

$$\sum_{\nu=1}^{n} b_\nu b_\nu'=1, \tag{1}$$

pri čemu je $n\in N$ te $b_\nu\in B$, $b'_\nu\in B^{-1}$ za $\nu=1, 2, \ldots, n$. Množeći jednakost (1) sa b za proizvoljno $b\in B$ izlazi

$$\sum_{\nu=1}^{n} b_\nu(b'_\nu b)=b$$

što znači da elementi $b_1, b_2, \ldots, b_n$ rađaju čitavo B, tj. $(b_1, b_2, \ldots, b_n)=B$.

3.9.5. *Produkt razlomljenih ideala $B_1, \ldots, B_n$ je obrativ onda i samo onda ako je svaki faktor B_ν obrativ.*

Najprije, ako je $B_\nu B_\nu^{-1}=I\,(\nu=1, 2, \ldots n)$, tada množeći te jednadžbe međusobno izlazi

$$\prod_\nu B_\nu B_\nu^{-1}=I^n$$

$$\prod_\nu B_\nu \prod_\nu B_\nu^{-1}=I \quad \text{tj.}$$

$$\Big(\prod_{\nu=1}^{n} B_\nu\Big)^{-1}=\prod_{\nu=1}^{n} B_\nu^{-1}.$$

S druge strane, ako postoji B^{-1} ideala $B=\prod B_\nu$, tada jednakost

$$B_k\Big(\prod_{\nu\neq k} B_\nu\Big)B^{-1}=I$$

pokazuje da B_k^{-1} postoji i da je $B_k^{-1}=\Big(\prod_{\nu\neq k} B_\nu\Big)B^{-1}$.

3.9.6. *Teorem o produktu prostih obrativih ideala. Ako su ideali $P_1, \ldots, P_n$ prosti i obrativi, tada jednakost*

$$B=\prod_{\nu=1}^{n} P_\nu$$

predstavlja jednoznačnu faktorizaciju ideala B u proste ideale.

Dokaz ćemo provesti induktivno u odnosu na n.

Slučaj $n=1$. Ne može biti

(1) $\qquad P_1=C_1C_2$, pri čemu su C_1, C_2 cijeli i $\neq I$.

Jer kako je P_1 prost ideal, to po definiciji iz (1) bi izlazilo $P_1 | C_1$ ili $P_1 | C_2$, tj. $P_1 \supset C_1$ ili $P_1 \supset C_2$. Dakle bi bilo

$$C_2 = I C_2 = P_1^{-1} P_1 C_2 \supset P_1^{-1} C_1 C_2 = P_1^{-1} = I,$$

što je nemoguće.

Opći slučaj: pretpostavimo da teorem vrijedi za $n = 1, 2, \ldots, m$; dokažimo ga i za $n = m+1$. Pa neka je

$$(2) \qquad (B =) \prod_{\nu=1}^{m+1} P_\nu = \prod_{k=1}^{e} C_k$$

pri čemu je C_k prost ideal pri $k = 1, 2, \ldots, e$. Kako C_1 dijeli B, mora C_1 dijeliti jedan od faktora $P_1, \ldots, P_{m+1}$, npr. $C_1 | P_1$. Iz $P_1 \subset C_1$ zbog obrativosti ideala C_1 slijedi:

$$P_1 = P_1 \cdot I = (P_1 C_1^{-1}) C_1 = C_0 C_1.$$

Tu je $C_0 = P_1 C_1^{-1}$. Prema dokazu za $n = 1$, ne može biti $C_0 \neq I$, jer je $C_1 \neq I$. No, iz $C_0 = I$ slijedi $P_1 = C_1$. Množeći jednadžbu (2) sa P_1^{-1} dobije se analogna jednadžba sa $n = m$ za koju po pretpostavci teorem vrijedi.

—→ **3.9.7. Teorem. U Dedekindovu prstenu svaki prosti ideal P je i maksimalan i obratljiv.**

Dokažimo najprije da je svaki obrativi prosti ideal P maksimalan.

Pretpostavimo, naprotiv, da P nije maksimalno nego da za neko $i \in I$ vrijedi

$$(1) \qquad P + i I \subsetneq I;$$

tada je tim prije $P + i^2 I \subsetneq I$ jer je $P + i^2 I \subset P + i I$. Na taj način imamo *prave* ideale $P + i I$, $P + i^2 I$ Dedekindova prstena I.

Promatrajmo njihove rastave

$$(2) \qquad P + i I = \prod_{i=1}^{m} C_i, \quad P + i^2 I = \prod_{j=1}^{n} D_j$$

u proste ideale C_i, D_j.

Promatrajmo rastavljanje I/P prstena I po idealu P; kako je $P \subsetneq C_i$, znači da će C_i biti unija određenih članova iz I/P; zbrajajući i množeći u I/P na uobičajeni način, vidi se da je I/P prsten a C_i/P, P_j/P njegovi određeni prosti ideali.

Iz jednakosti (2) izlazi neposredno i jednakost

$$I/P \cdot (P + i) = \prod_{i=1}^{n} C_i/P,$$

odakle dalje

$$(3) \qquad I/P \cdot (P + i)^2 = \prod_{i=1}^{m} (C_i/P)^2 = \prod_{j=1}^{n} (D_j/P).$$

No, ideal $I/P\cdot(P+i)^2$ je glavni $\neq\{0\}$, dakle je taj ideal obrativ (§ 3.9.3.1) pa su svi faktori u prikazu toga ideala obrativi (§ 3.9.5); zato po teoremu 3.9.6 oba se rastava u (3) podudaraju. Posebno to znači da je $n=2m$; a numeracija se može uvijek tako provesti da bude

$$C_i=D_{2i-2}=D_{2i}\ (i=1,2,\ldots,m)$$

No, $$P+i^2I=(P+iI)^2$$ te

$$P\subset(P+iI)^2\subsetneqq P^2+iI$$

pa za svako $p\in P$ postoji $y\in P^2$, $z\in I$ sa svojstvom da bude

$$p=y+iz.$$

Odatle izlazi $iz\in P$.

No, P je prost ideal; k tome $i\in P\setminus I$, dakle $z\in P$ pa je $P\subset P^2+iP$ dakle također $P=P^2+iP$. Odatle množenje sa P^{-1} daje

$$I=P+iI,$$

protivno sa (1); dakle je zaista P maksimalno.

Dokažimo još da je svako prosto $P\neq(0)$ obrativo. Za $p\in P\setminus\{0\}$ imamo glavni ideal $Ip\neq\{0\}$ i rastav $Ip=\prod_i P_i$ u proste ideale P_i; kako je Ip obrativo (§ 3.9.3.1), to su i prosti faktori P_i obrativi (§ 3.9.5) i maksimalni. No, $Ip\subset P$ dakle $P_i\subset P$ za neko i, tj. $P_i=P$ jer je P_i maksimalno. To znači da postoji P^{-1} kao P_i^{-1}.

⟶ **3.9.8. Teorem. U Dedekindovu prstenu svaki netrivijalni ideal dopušta jednoznačnu faktorizaciju u proste ideale.**

Teorem izlazi iz 3.9.6. i 3.9.7.

3.9.9. Teorem. Svaki razlomljeni ideal $B\neq\{0\}$ Dedekindova prstena je obratljiv pa svi ideali $\neq\{0\}$ čine množidbenu grupu.

Neka je $B=\dfrac{1}{d}B_0=(dI)^{-1}B_0$, gdje je B_0 ideal. Promatrajmo primfaktorizacije

$$B_0=\prod_i P_i,\quad dI=\prod_j Q_j;$$

kao produkt prostih ideala, ideali B_0, Id su obrativi i vrijedi specijalno $(dI)^{-1}=\prod Q_j^{-1}$ te

$$B=(dI)^{-1}B_0=\prod Q_j^{-1}\prod P_i;$$

odakle

$$B^{-1}=\prod_j Q_j\cdot\prod_i P_i^{-1}.$$

⟶ **3.10. Osnovni teorem. Cjelosna oblast je Dedekindov prsten onda i samo onda ako skup svih razlomljenih ideala $\neq\{0\}$ čini multiplikativnu grupu.**

Upravo dokazasmo da je uslov teorema *dovoljan*; dokažimo da je uslov i *nuždan*: ako cjelosna oblast I ima jedinicu 1 te ako skup svih razlomljenih ideala $\neq \{0\}$ čini grupu, onda je I Dedekindov prsten (§ 3.8.7) pa se svaki cijeli ideal B može predstaviti kao produkt od konačno mnogo prostih ideala.

Prema t. 3.8.4 dovoljno je dokazati da se B može prikazati kao produkt od konačno mnogo *maksimalnih* ideala.

Najprije, svaki *uzlazni* niz ideala

(1) $$B_1 \subset B_2 \subset \cdots$$

daje kao uniju ideal koji zbog svoje obratljivosti ima konačno mnogo izvodnica; to znači da niz (1) ima samo konačno mnogo različitih članova.

Pretpostavimo da postoji neki cio ideal B koji nije produkt maksimalnih ideala; možemo pretpostaviti da je B najobuhvatniji takav ideal. Neka je M maksimalan ideal $\supsetneqq B$ (naravno, B nije maksimalno); dakle je $1 \text{ non} \in M$, $MM^{-1} = I$ što sa $B \subset M$ daje $BM^{-1} \subset I$; BM^{-1} je (cio) ideal pa iz

(2) $$B = BI = B(MM^{-1}) = M(BM^{-1})$$

izlazi

(3) $$B \subset BM^{-1}.$$

Slučaj

(4) $$B \subsetneqq BM^{-1}$$

nije moguće, jer bi ideal BM^{-1} kao opsežniji od B bio rastavljiv u *maksimalne* ideale, a po (2) vrijedilo bi to i za B, protivno pretpostavci. Dakle zbog (3) moralo bi biti $B = BM^{-1}$ dakle

(5) $$BM = B$$

No, neka je

$$B = (b_1, b_2, \ldots, b_n).$$

Stavimo $B_\nu = (b_\nu, b_{\nu+1}, \ldots, b_n)$, $(\nu = 1, 2, \ldots, n)$ te $B_{n+1} = \{0\}$.

Dokažimo da postoji niz $m_\nu \in M$ $(\nu = 1, 2, \ldots, n+1)$ sa svojstvom

(6) $$1 \neq m_\nu, \ (1 - m_\nu) B \subset B_\nu.$$

Radimo postupno.

Jasno je da možemo staviti $m_1 = 0$ jer je $B_1 = B$; ako je postojanje članova m_ν dokazano za $\nu = 1, 2, \ldots, k < n+1$, dokažimo to i za $\nu = k+1$. Prema (6) i (5) znači da je

$$(1 - m_k) B = (1 - m_k) MB \subset MB_k,$$

dakle je posebno

$$(1 - m_k) b_k \in MB_k, \quad \text{tj.} \quad (1 - m_k) b_k = \sum_{j=k}^{n} m_{kj} b_j \quad \text{za neke } m_{kj} \in M.$$

Odatle izlazi $(1 - m_k - m_{kk}) b_k \in B_{k+1}$, tj. $(1 - m_k - m_{kk}) B_k \subset B_{k+1}$. Stavimo

$$1 - m_{k+1} = (1 - m_k)(1 - m_k - m_{kk});$$

bit će zbog

$$(1-m_k-m_{kk})\,B_k \subset B_{k+1}:$$

$$(1-m_{k+1})\,B=[(1-m_k-m_{kk})\,(1-m_k)\,B] \subseteq (1-m_k-m_{kk})\,B_k \subset B_{k+1},\ \text{tj.}$$

(7) $$(1-m_{k+1})\,B \subset B_{k+1},$$

pa je m_{k+1} traženi član iz B. No, (7) znači da bi bilo

(8) $$(1-m_{k+1})\,b=0$$

za svako $b \in B$, premda je $1 \neq m_{k+1}$; dakle bi se 0 moglo prikazati kao produkt dvojke članova $1-m_{k+1}$, b koji su oboje $\neq 0$, protivno pretpostavci da smo u cjelosnoj oblasti.

Time je osnovni teorem 3.10 potpuno dokazan.

3.11. Uspostava jednoznačne faktorizacije u prstenu $A=D[\sqrt{-5}]$.

3.11.1. Povratimo se na kolo $D[\sqrt{-5}]=A$ u kojem smo naišli na nejednoznačnost faktorizacije brojeva (v. 32, § 2.5). Imali smo jednakost

(1) $$9=3\cdot 3=p_1\cdot p_2,\quad \text{gdje je } p_1=2+\sqrt{-5},\ 2-\sqrt{-5}=p_2.$$

Dokazali smo da su 3, p_1, p_2 tri nejednaka prosta broja u kolu

$$D[\sqrt{-5}].$$

3.11.2. Faktorizacija ideala $3A$.

Kako ta stvar sada izgleda u svjetlu idealnih faktora i prostih ideala? Prvi odgovor je ovdje: broj 3 koji je sačuvao svoju prostu strukturu prelazom iz D u $D[\sqrt{-5}]$ i ostao prost broj ipak je takav da je u svjetlu finije skupovne strukture složen: pripadni ideal $3D[\sqrt{-5}]$ nije prost (kao što je $3D$ bio prost u kolu D) nego je složen; specijalno vrijedi:

(2) $$3A=(3A+p_1A)\cdot(3A+p_2A),\quad p_{1,2}=1\pm 2\sqrt{-5},$$

gdje je $A=D[\sqrt{-5}]$ ili kraće pisano:

(2') $$(3)=(3,\,p_1)\cdot(3,\,p_2).$$

Dokažimo relacije (2), (2'). No, produkt se množi tako da množimo rodne elemente u idealima na desnoj strani (2') ili kao množenje „binoma“ u (2) nadesno i znajući da je $A\cdot A=A$. Radimo npr. sa (2).

$$3A=3A\cdot 3A+p_1A\cdot 3A+3A\cdot p_2A+p_1Ap_2A=$$

$$=9A+(1+2\sqrt{-5})\,3A+3\,(1-2\sqrt{-5})\,A+(1-4\cdot -5)\,A,\qquad \text{tj.}$$

(3) $$3A=(9A+21A)+3\,[(1+2\sqrt{-5})\,A+3\,(1-2\sqrt{-5})\,A].$$

Tako vidimo da se u $(3)_2$ pojavljuje $9A+21A$. No to je $=(9M21)\,A=3A$; preostali dijelovi na desnoj strani $(3)_2$ relacije (3) su $\subset 3A$.

Time je relacija (2') dokazana: broj 3 je prošao probu i u kolu D i u kolu $A=D[\sqrt{-5}]$, ali probu idealâ nije prošao: on je složen, tj. pripadni „glavni ideal" — skup $3A$ — rastavlja se na još prostije sastojke.

3.11.3. S druge strane, dokažimo da su ideali

(4) $$P_1=(3,\ 1+2\sqrt{-5}),\ P_2=(3,\ 1-2\sqrt{-5}) \text{ prosti.}$$

Odmah se vidi da za svako $x\in A$ postoji cio racionalan broj c_x za koji je $x-c_x\in P_1$. Ako je naime $x=x_1+x_2\sqrt{-5}$, tada je $x=x_1-2x_2+x_2(2+\sqrt{-5})$ pa je dovoljno uzeti $c_x=x_1-x_2$.

3.11.4. A sada dokažimo da je P_1 prost ideal. Pa neka su x, y dva člana iz $D[\sqrt{-5}]$ za koje je $x\cdot y\in P_1$; prema upravo izrečenom, postoje cijeli racionalni brojevi c_x, c_y za koje $x-c_x, y-c_y$ a time i njihov produkt $(x-c_x)(y-c_y)$ leži u P_1. No, iz $x(y-c_y)\in P_1$, $y(x-c_x)\in P_1$ zaključujemo da su u P_1 također brojevi $xy, -c_xy, -c_yx$ dakle i broj

$$c_xc_y=(x-c_x)(y-c_y)-(xy+c_xy+c_yx).$$

To znači dakle da je $c_xc_y\in P_1$ a time je c_xc_y djeljivo sa 3; dakle je $3\mid c_x$ ili $3\mid c_y$, a time i $x\in P_1$ ili $y\in P_1$ ili oboje. To upravo kaže da je P_1 prost ideal.

Slično se dokazuje da je i $P_2=(3,\ 1-2\sqrt{-5})$ prost ideal.

Prema tome, rastav (2') predstavlja primfaktorizaciju ideala $3A$.

3.11.5. *Primfaktorizacija broja 9, odnosno ideala 9 A.*

To prema relaciji (2) znači da je $(3)=P_1P_2$ i dalje zbog

$$(9)=(3)(3)$$

daje

(8.) $$(9)=P_1P_1P_2P_2.$$

To je konačna primfaktorizacija broja 9, odnosno njegova ideala

$$(9)=9D[\sqrt{-5}].$$

3.11.6. *Primfaktorizacija broja* 21, *odnosno ideala* 21 A.

Još je markantnija stvar za broj 21. Jer

(9.) $$21=3\cdot 7=(1+2\sqrt{-5})(1-2\sqrt{-5})=(4+\sqrt{-5})(4-\sqrt{-5}),$$

a svi ti faktori su prosti brojevi u kolu $D[\sqrt{-5}]$ i međusobno nepridruženi. Međutim, u svjetlu ideala, faktorizacija izgleda drukčije; izgleda ovako:

(10.) $$(21)=P_1P_2Q_1Q_2,$$

gdje je

$$P_1=(3,\ 1+2\sqrt{-5})\quad P_2=(3,\ 1-2\sqrt{-5})$$

$$Q_1=(7,\ 1+2\sqrt{-5}),\ Q_2=(7,\ 1-2\sqrt{-5}).$$

P_1, P_2, Q_1, Q_2 su primideali, a prosti faktori u (9.) dalje se kao ideali faktoriziraju ovako:

(11.)
$$(3) = P_1 P_2, \ (7) = Q_1 Q_2,$$
$$(1+2\sqrt{-5}) = P_1 Q_1, \ (1-2\sqrt{-5}) = P_2 Q_2,$$
$$(4+\sqrt{-5}) = P_2 Q_1, \ (4-\sqrt{-5}) = P_1 Q_2.$$

3.11.7. Ako unesemo izraze (11.) u (10.), onda zbilja vidimo da smo opet pri *jednoznačnoj faktorizaciji*, ali ne više cijelih brojeva nego *pripadnih ideala.*

Stvar je prikazana na jednom primjeru. No, prema t. 2.7.8. jednoznačnost primfaktorizacije ideala vrijedi i to ne samo u kolu $D[\sqrt{-5}]$ ili bilo kojem kolu oblika $D[\sqrt{m}]$ ili $D\left[m^{\frac{1}{n}}\right]$ nego čak i u prstenu $E_e A$ svih cijelih algebarskih brojeva sadržanih u nekom konačnom raširenju tijela Q, pa ni općenitijim prstenima (isp. § 3.8.6). To je velika generalizacija onoga što znamo o faktorizaciji prirodnih brojeva, koju je genijalno obradio Euklid, nastavio i proširio na druge oblasti Gauss preko dvije hiljade godina kasnije s tim da ni 100 godina ne prođe pa da se može izreći teorem o jednoznačnosti primfaktorizacije ideala (v. § 3.9.8).

3.12. Prosti prsteni. — **3.12.1** D e f i n i c i j a. Ako prsten osim trivijalnih ideala (0) i (1) drugih ideala nema, prsten se zove *prostim* ili *prim* (isp. def. 17 § 17.1.2. proste grupe).

3.12.2. T e o r e m. *Svako tijelo je prost prsten. Svaki prsten s dijeljenjem je prost.* Pri tom vrijedi

3.12.3. D e f i n i c i j a. Prsten A sa svojstvom da za svako $a \in A \setminus \{0\}$ i svako $b \in A$ jednadžbe $ax = b$, $ya = b$ imaju bar po jedno rješenje iz A zove se *prsten s dijeljenjem* ili *diobeni prsten.*

Neka je naime A prsten s dijeljenjem; neka je I njegov ideal $\neq (0)$. Tada za proizvoljno $a \in I \setminus \{0\}$ i $b \in A$ jednadžba $ax = b$ ima rješenje x iz A; to znači da je $aA = A$, tj. $IA = A$ što zajedno sa $IA \subset I \subset A$ daje $I = A$.

⟶ **3.12.4.** **T e o r e m.** ***Skup A_{nn} svih matrica poretka (n, n) a s vrijednostima u nekom prstenu A s dijeljenjem čini prost prsten*** **(slučaj $n = 1$ daje t. 3.12.2.).**

D o k a z. Neka je $I \neq (0)$ ideal prstena A_{nn}; dokažimo da je $I = A_{nn}$. No, za svaku matricu $b \in A_{nn}$ imamo

$$b = \sum_{i,j=1}^{n} (b_{ij}(i,j), \quad \text{gdje je} \quad x(i,j)$$

matrica koja iz nula-matrice $0\ (n)$ nastaje zamjenjujući joj (i,j)-vrijednost 0 sa x. Zato je dovoljno pokazati da $b_{ij}(i,j) \in I$, pa da zaključimo da $b \in I$, tj. $I = A_{nn}$.

Neka je $b \neq 0\,(n)$ i npr. $b_{ij} \neq 0$; neka je $a \in A$ proizvoljno; tada za neke $x, y \in A$ vrijedi $y b_{ij} x = a$. Zato za proizvoljni par $r, s \in \{1, 2, \ldots, n\}$ vrijedi $a(r,s) = (y b_{ij} x)(r,s) =$ (kao što se lako provjeri) $= y(r,i)\, bx(j,s)$ pa je $a(r,s) \in I$ za svako $a \in A$; specijalno to vrijedi za $a = b_{ij}$ i $r = i, j = s$. Zato je zaista $b \in I$.

3.13. Ideali grupoida. — 3.13.1. Definicija. Svaki podgrupoid $(I, \cdot)$ grupoida $(G, \cdot)$ za koji je $GI \subset I$ zove se *lijevi ideal grupoida.* Analogno se definira *desni ideal grupoida* te *obostrani ideal grupoida.*

Ideali grupe se definiraju kao podgrupe I za koje vrijedi idealski uslov $GI \subset I$ (*lijevi ideali*), $IG \subset I$ (*desni ideali*), $GI \subset I \supset IG$ (*obostrani ideali*).

Svaki ideal grupe G podudara se sa G.

3.14. Zadaci o prstenima i idealima.

1. Ako je $(A, + \cdot)$ komutativan prsten s jedinicom 1, onda je i dualno $(A, \ominus, \oplus)$ komutativan prsten s jedinicom; pri tom se definira $a \ominus b \equiv = a + b - ab$, $a \oplus b = a + b - 1$. Kako glase neutralni elementi?

2. Skup A_{nn} svih matrica a formata (n,n) s vrijednostima u prstenu A čini prsten u kojemu svi članovi za koje 1) prvi stupac; 2) prva dva stupca; 3) bilo koji podskup stupaca imaju samo nule čini lijevi ideal; konkretizirati sa R_{22}.

2^d Dualno od zad. 2 a dobije se zamjenom stupac $\to$ redič, lijevi $\to$ desni.

3. Ako je I lijevi (desni) ideal prstena A_{nn}, tada postoji neki prirodni redni broj m i regularna matrica $a \in A_{nn}$ sa svojstvom da je $a^{-1} Ia$ ideal sastavljen od svih matrica iz A_{nn} kojima je posljednjih m stupaca (redaka) ispunjeno sa 0.

4. Skup A svih 1) realnih funkcija $f: R \to R$; 2) realnih polinoma $f(x)$ čini prsten $(A, + \cdot)$ kojemu je za svako $r \in R$ skup $A_r = \{f; f \in A, f(r) = 0\}$ određen ideal.

5. U prstenu svih realnih (kompleksnih) nizova nizovi koji konvergiraju prema 0 čine ideal.

6. Dokaži da je $EQ(\sqrt{-1}) = D[\sqrt{-1}]$ i da je prsten euklidski.

7 Promatraj prsten $Q(\sqrt{-3})$; 1) Je li prsten $A = EQ(\sqrt{-3})$ svih njegovih cijelih, jednak $D[\sqrt{-3}]$? 2) Dokaži da je A euklidski prsten

8. Dokaži da je $EQ(\sqrt{-5}) = D[\sqrt{-5}]$ i da u tom prstenu vrijedi $(3, 4 + \sqrt{-5}) \cdot (4 - \sqrt{-5}) = (1 - 2\sqrt{-5})$.

9. Neka je m cio racionalan broj koji nije djeljiv kvadratom prosta broja; 1) ako je $m \equiv 2 \pmod 4$ ili $m \equiv 3 \pmod 4$; tada je $EQ(m^{1/2}) = D[m^{1/2}] = = D + m^{1/2} D$; 2) ako je $m \equiv 1 \pmod 4$, tada je $EQ(m^{1/2}) = D + D\omega$, gdje je $\omega = \frac{1}{2}(1 + m^{1/2})$.

10. U glavnoidealskom prstenu svaki prost ideal koji nije nulaideal ni jedinični ideal je maksimalan.

11. Dva člana glavnoidealskog prstena međusobno su prosta onda i samo onda ako nemaju nikojeg zajedničkog primfaktora.

12. *Eisensteinov kriterij* (F. G. M. Eisenstein, 1823—1852)

1) Neka je p prost cio broj u prstenu D; neka polinom

$$a(x)=a_0+a_1x\cdots+a_nx^n\in D[x] \text{ zadovoljava:}$$

$$M(a_0,\ a_1,\ldots,\ a_n)=1,$$

$$\begin{matrix} n>0,\ a_n\not\equiv 0 \pmod p, \\ a_0\not\equiv 0 \pmod{p^2}; \end{matrix} \quad a_\nu\equiv 0 \pmod p \text{ pri } \nu\in\{0,\ 1,\ 2,\ldots,\ n-1\}$$

tada je $a(x)$ nesvodljivo (ireducibilno) u $D[x]$.

2) sličan iskaz dobiven zamjenom $D\to A$ za bilo koji prsten A.

13. *Lieov prsten.* 1) Definicija. Prsten $(A,\ +,\ \cdot)$ je *Lie-ov*[1] ako je $a^2=0$ te $(ab)c+(bc)c+(ca)b=0$ za svaku uređenu trojku članova iz A; 2) skup A svih vektora u Euklidskom prostoru R^3 je Lieov prsten u odnosu na zbrajanje i vektorsko množenje; 3) Ako je $(A,\ +,\ \cdot)$ asocijativno kolo, tada je $(A,\ +,\ \circ)$ Lieovo kolo; pri tom definiramo $a\circ b=ab-ba$.

14. *Alternirajući prsten.* 1) Opći prsten $(A,\ +,\ \cdot)$ (u smislu pogl. 26, § 7.9.6) je alternirajući ako je $a(ab)=(aa)b$, $(ab)b=a(bb)$ za svaki uređeni par $(a,\ b)$ članova prstena. Drugim riječima, stavimo li $[a,\ b,\ c]=(ab)c-a(bc)$, tada po definiciji prsten je alternirajući ako je $[a,\ a,\ b]=0=[a,\ b,\ b]$.

2) Prsten je alternirajući onda i samo onda ako je svaki potprsten generiran dvojkom članova asocijativan;

3) Ako je prsten alternirajući, tada je $[a,\ b,\ a]=0$.

15. *Asocijator* uređene trojke $a,\ b,\ c$ je

$$[a,\ b,\ c]=(ab)c-a(b,\ c).$$

U alternativnom prstenu A za svaku trojku $a_1,\ a_2,\ a_3\in A$ vrijedi

$[p_1,\ p_2,\ p_3]=\operatorname{sgn} p\, a_{p_1}\, a_{p_2}\, a_{p_3}$ za svaku permutaciju $p\in\{1,\ 2,\ 3\}!$; stavlja se $\operatorname{sgn} p=(-1)^{ip}$ (v. 3, § 8.5).

4. TIJELO ILI POLJE

Ideja tijela je svakako da se u zadanu skupu mogu vršiti sve četiri aritmetičke operacije (dijeljenje sa 0 se ne definira).

4.1. Definicija tijela. Svaki prsten s jedinicom u kojem je dijeljenje definirano jednoznačno zove se *tijelo* (*korporacija*) ili *polje* (dijeljenje sa 0 se isključuje).

Tijelo je *asocijativno* ili združivo (*komutativno*) ako je množenje asocijativno (komutativno). Tijelo ćemo označiti sa K ili potpunije sa $(K,\ +,\ \cdot)$ ili $K(+,\ \cdot)$; time se ističe skup K i algebarske operacije $+,\ \cdot$ u K.

[1] M. S. Lie (1842—1899), norveški matematičar.

4.1.1. Primjeri tijela: Q (tijelo svih racionalnih brojeva), R (tijelo realnih brojeva), A (tijelo algebarskih brojeva), $R(i)=K$ (tijelo kompleksnih brojeva), $D_p=(\{0, 1, 2, \ldots, p-1\}, +_p, \cdot_p)=$ tijelo cijelih ostataka modulo p (p je proizvoljan prost broj), $K(x)$ skup svih racionalnih funkcija (izraza) u x s koeficijentima iz K; $K(x_1, x_2, \ldots, x_n)$ (skup svih racionalnih funkcija veličina $x_1, x_2, \ldots, x_n$ s koeficijentima iz K); itd.

4.1.2. Primjedbe. Svako tijelo $(K, +, \cdot)$ je ujedno i aditivna komutativna grupa kao i cjelosna oblast; posebno, K obuhvata neutralna dva člana i to 0 i 1. Nadalje je tijelo bez nuladivizora: iz a, $b \in K$ i $ab=0$ izlazi $a=0$ ili $b=0$ ili $a=b=0$. Dakle $\{a, b\} \subset K \setminus \{0\} \Rightarrow ab \neq 0$.

4.1.3. U svakom asocijativnom tijelu čine elementi $\neq 0$ multiplikativnu grupu; ona se zove *množidbena grupa tijela.*

4.1.4. Podtijelo. Nadtijelo. Ako je $X \subset K$ te $(X, +, \cdot)$ tijelo, kaže se da je $(X, +, \cdot)$ *podtijelo od* $(K, +, \cdot)$; također se kaže da je $(K, +, \cdot)$ *nadtijelo, raširenje ili proširenje* od $(X, +, \cdot)$.

4.1.5. Specijalno, za svaki neprazni podskup E tijela K potpuno je određeno *minimalno podtijelo* koje obuhvata E a nalazi se u K; kaže se da je ono *proizvedeno skupom E.*

4.1.6. Izomorfizam tijelâ. Kaže se da je tijelo $(K, +, \cdot)$ *izomorfno* s tijelom $(K', +', \cdot')$ ako postoji tolikovanje t od K na K' sa svojstvom da

$$t(x+y)=tx+'\,ty$$

$$t(x \cdot y)=tx \cdot'\,ty;$$

pišemo $K \simeq K'$ i čitamo: K je izomorfno sa K' (prema tome je $tK=K'$).

Neposredno se dokazuje da je izomorfizam među tijelima određena *relacija ekvivalencije.*

Tako npr. pri svakom prostom broju p, tijelo D_p je izomorfno s tijelom $D/_{pD}$.

4.1.7. *Homomorfizam* se definira poput izomorfizma samo što preslikavanje ne mora biti obostrano jednoznačno.

4.2. Prosto tijelo — **4.2.1.** Definicija. Svako tijelo koje ne obuhvata manje podtijelo zove se *prosto tijelo* ili *primtijelo* ili *pratijelo.*

Tako npr. Q i D_p su prosta tijela.

—→ **4.2.2.** **Teorem.** ***Tijela***

(1) $\qquad Q, D_p \quad (p=2, 3, 5, \ldots;$ ***p prost prirodan broj***$)$

***jesu prosta tijela. Svako prosto tijelo je izomorfno s jednim jedinim od tih tijela. Svako tijelo obuhvata posve određeno prosto tijelo koje je izomorfno s jednim jedinim od tijelâ* (1).**

4.2.2.1. Korolar. *Svako beskonačno prosto tijelo je izomorfno s tijelom Q.*

4.2.2.2. Primjedba. Za razliku od prostih (jednostavnih) grupa, prstena, prosta tijela su posve određena i ima ih upravo prebrojivo mnogo koja nisu međusobno izomorfna.

Dokaz teorema 4.2.2. je jasan: tijelo K sadrži jedinicu 1 dakle i $1+1=2\cdot 2$, $1+1+1=3\cdot 1$ i uopće $(n+1)\cdot 1$ $(=\text{def})=n\cdot 1+1$.

Imamo dva slučaja koji se isključuju:

Prvi slučaj: U nizu

$$1,\quad 2\cdot 1,\quad 3\cdot 1,\ldots,\ n\cdot 1,\ldots\quad (n\in N) \tag{1}$$

nema jednakih članova. Tada K sadrži i

$$-1,\quad -2\cdot 1,\ldots,\ -n1,\ldots$$

jer je $(K, +)$ grupa. No, K kao tijelo sadrži i rješenje $x=\frac{m\cdot 1}{n\cdot 1}$ jednadžbe $(n\cdot 1)x=m\cdot 1$ za svako $n\in N$ i svako $m\in D$. Na taj način, svakom racionalnom broju $\frac{m}{n}$ odgovara posve određen član $\frac{m\cdot 1}{n\cdot 1}\in K$, pa se neposredno vidi da je to pridruživanje

$$\frac{m}{n}\to\frac{m\cdot 1}{n\cdot 1}$$

određen *izomorfizam*. Dakle, K obuhvata tijelo izomorfno sa Q.

Drugi slučaj: U nizu (1) ima jednakih članova; neka je npr.

$$m\neq n \text{ i } m\cdot 1=n\cdot 1 \quad \text{dakle } (n-m)\cdot 1=0.$$

Neka je p *prvi prirodni broj* za koji je $p\cdot 1=0$; tada je p *prost* broj; kad bi naime p bio složen broj $p=r\cdot s$, $1<r<p$, $1<s<p$, tada bi zbog $(rs)\cdot 1=$ $=(r\cdot 1)(s\cdot 1)$ bilo $(r\cdot 1)(s\cdot 1)=0$; dakle (jer je tijelo bez djelitelja nule) $r\cdot 1=0$ ili $s\cdot 1=0$, protivno definiciji broja p.

Dakle je p zaista prost broj. Pridruživanje

$$x\to x\cdot 1 \qquad (x=0,\ 1,\ 2,\ldots,\ p-1)$$

je izomorfija tijela D/pD i određena podtijela od K. Dakle K sadrži prosto tijelo izomorfno sa D/pD.

4.3. Karakteristika tijela. — **4.3.1.** Definicija. *Najmanji* prirodni broj p za koji je $p\cdot 1=0$ zove se *karakteristika* tijela K; ako je $n\cdot 1\neq 0$ za svako $n\in N$ kaže se da je tijelo *karakteristike* 0.

Prema tome, teorem 4.2.2. možemo izreći i ovako: *Svako tijelo sadrži prosto tijelo karakteristike* 0 *ili* p (p *prost broj*). *Specijalno*, Q *je karakteristike* 0, D/pD *je karakteristike* p.

4.4. Generiranje tijela.

Tijelo sadrži razne podgrupoide, podgrupe, potprstene i oblasti cijelih. I obrnuto, neke od tih struktura mogu se upotpuniti na tijela.

$\longrightarrow$ **4.4.1. Teorem.** **(0)** *Svaka cjelosna oblast I može se proširiti na tijelo $I^{:}$, a sastoji se od „razlomaka“ $\frac{a}{b}$ $(a \in I,\ b \in I \setminus \{0\})$ s kojima se radi po uobičajnim pravilima; specijalno stavljajući $\frac{a}{1} = a$, dobije se $I \subset I^{:}$*

(00) *Svako izomorfno preslikavanje f cjelosne oblasti I u neko tijelo K može se na jedan jedini način proširiti na izomorfiju F od $I^{:}$ u K i to relacijom*

(1) $$\frac{a}{b} \in I^{:} \setminus I \to F\frac{a}{b} = \frac{fa}{fb} \qquad \text{(isp. 17, 13.3.0).}$$

Dokaz teorema (0) se provodi upravo kao što se definira tijelo Q racionalnih brojeva pomoću prstena $(D, +, \cdot)$.

Dokažimo teorem (00).

Iz (1) izlazi $b \neq 0$ dakle i $fb \neq 0$; zato je

$$c = \frac{fa}{fb} \in K, \quad \text{tj.} \quad c = \frac{Fa}{Fb}.$$

Kako je F izomorfija, bit će $\frac{Fa}{Fb} = F\frac{a}{b}$. Dakle je zaista

$$F\frac{a}{b} = \frac{Fa}{Fb} = \frac{fa}{fb}, \qquad \text{tj. vrijedi (1).}$$

4.4.2. Teorem. Svaka konačna oblast I cijelih je tijelo (isp. 4.1).

Neka je naime $a \in I \setminus \{0\}$; treba dokazati da za svako $b \in I$ jednadžba $ax = b$ ima jedno jedino rješenje. No, preslikavanje $x \to ax$ je obostrano jednoznačno od I u I; kako je I *konačno*, mora biti ne samo $aI \subset I$ nego $aI = I$ pa je posebno za jedno jedino $x \in I$ ispunjeno $ax = b$; pišemo $x = a^{-1} b$.

4.4.3. Tipična konstrukcija tijela od p^n članova (p prost prirodan broj).

Neka je $P(x)$ normiran x-polinom stepena n s cijelim koeficijentima; reći ćemo da je on *nerastavljiv* mod. p, ako ne postoje dva polinoma g, h stepena $< n$ za koje bi bilo $P(x) \equiv g(x)\, h(x)$, (mod p).

U drugu ruku, prema osnovnom teoremu o dijeljenu polinoma (7, § 4.1) možemo svaki član iz $D[x]$ napisati u obliku

$$P(x) \cdot q(x) + r(x), \text{ gdje je } r(x) \equiv 0 \text{ ili je } r(x) \text{ stepena } < n.$$

Za a, $b \in D[x]$ pisat ćemo

(1) $$a \equiv b \quad (\text{mod } p,\ P(x))$$

ako su ostaci mod $P(x)$ od a, b kongruentni modulo p.

Ostatak mod $P(x)$ je svakako oblika

(2) $$r_0 + r_1 x + r_2 x^2 + \cdots + r_{n-1} x^{n-1}.$$

Međutim, svaki od koeficijenata r_v može biti proizvoljan u intervalu $Ip=\{0, 1, \ldots, p-1\}$ tako da u (2) imamo $\underbrace{pp\cdots p}_{n}$ izrazâ koji su nekongruentni mod p, P.

4.4.3.1 Teorem. **Svih p^n polinoma (2) čini tijelo mod p, $P(x)$.** — Zove se ***Galoisovo tijelo*** ili ***Galoisovo polje***.

Poslije ćemo u § 4.10.4. dokazati da je svako konačno tijelo K izomorfno s jednim takvim tijelom (E. R. Moore [1862—1932]; 1893) K komutativno; J. H. M. Wedderburn [1882—1948]; 1905).

4.4.4. Razredi ostataka i tijela.

⟶ **4.4.4.1. Teorem.** ***Neka je K zadano asocijativno tijelo, a $K[x]$ prsten x-polinomâ nad K; tada za svaki polinom $p\in K[x]$ imamo pripadni ideal $p\cdot K[x]$ i pripadni faktorski prsten***

(1) $$K[x]/p\,K[x] \text{ ili kraće } K[x]/p;$$

ako je $p=p_0+p_1x+p_2x^2+\cdots+p_nx^n$ nerastavljivo u $K[x]$, tada je $K[x]/p(x)$ asocijativno tijelo, a preslikavanje

(2) $$a\in K[x]\to \underline{a}\in K[x]/p$$

je homomorfizam; pri tom stavljamo

$$a\in K[x]\to \underline{a}=p\cdot K[x]+a \text{ tako da je dakle } a\in\underline{a}\in(1).$$

Vrijedi

(3) $$p\,\underline{x}=\underline{0} \text{ pri dogovoru } a=\underline{a}.$$

Drugim riječima, u faktorskom tijelu (1) ima polinom p (koji je bio nesvodljiv u $K[x]$) nulište i to upravo sam ideal $\underline{0}=x+p\cdot K[x]$.

Dokaz. Lako se provjeri da je skup (1) prsten i da mu je razred $\underline{1}$ jedinica. Dokažimo i uslov recipročnosti. Naime neka je $f(x)$ proizvoljan polinom nad K tako da ne bude $f\equiv 0 \pmod{p(x)}$. Kako je p nerastavljivo, bit će $M(f,p)=1$. To znači da jednadžba $f\cdot X+p\cdot Y=1$ ima rješenje sa $X, Y\in K[x]$. To upravo znači da je $fX\equiv 1 \pmod p$, tj. $X=f^{-1}$. Dakle je zaista i recipročnost osigurana. Neposredno se dokazuje da je (2) određen homomorfizam.

Nađimo $p(\underline{x})=p_0+p_1\underline{x}+p_2(\underline{x})^2+\cdots+p_n(\underline{x})^n$. Zbog homomorfizma (2), ovo je dalje $=p_0+p_1\underline{x}+p_2\underline{(x^2)}+\cdots+p_n\underline{(x^n)}=\underline{p\,x}$ dakle $=\underline{0}$. Drugim riječima vrijedi (3).

To znači da u faktorskom tijelu $K[x]/_{p(x)}$ polazna nesvodljiva jednadžba $px=0$ ima rješenje, npr. ideal $x=\underline{0}$.

4.4.4.2. Ako k tome svako $k\in K$ poistovetimo s pripadnim razredom $\underline{k}$, onda dobiveno faktorsko tijelo proširuje ishodno tijelo K, i u novom tijelu polinom $p(x)$ je rastavljiv, premda je u K nerastavljiv. Time se zapravo osnovni teorem algebre prikazuje u novom svjetlu (isp. 7 § 13.1, 29, § 6.5 — § 6.6).

4.5. Adjunkcija ili privezivanje.

4.5.1. *Pojam.* Neka je f nesvodljiv x-polinom s koeficijentima iz K. Ako sa a označimo, formalno, veličinu za koju je $f(a)=0$, tada imamo tijelo $K(a)$ koje iz K nastaje privođenjem ili adjunkcijom veličine a. Ako je $a \in K$, tada je $K(a)=K$. Zato se možemo ograničiti na slučaj a non$\in K$ *računajući formalno sa a kao da je neki član iz $K \setminus \{0\}$ držeći na umu relaciju $f(a)=0$; posebno se formalno stavlja $a^1=a$, $a^2=a \cdot a$,* itd.

$\longrightarrow$ **4.5.2. Teorem.** ***Ako je K tijelo i $f \in K[x]$ nesvodljiv polinom nad K pa ako je $fa=0$ (dakle a non $\in K$), tada je $K(a)$ tijelo, odnosno vektorski prostor nad K s bazom ili osnovom***

$$(1) \qquad a^0\,(=1),\ a,\ a^2, \ldots, a^{n-1},$$

pa se svaki element $v \in K(a)$ može na jednoznačan način prikazati u obliku $v=v_0 a^0+v_1 a+\cdots+v_{n-1} a^{n-1}$; pritom je $n=\mathrm{st}\, f$. Specijalno članovi (1) su linearno nezavisni u odnosu na tijelo K.

Ako je također $fb=0$, tada su tijela $K(a)$, $K(b)$ izomorfna; izomorfizam izmedu $K(a)$, $K(b)$ dobije se naprosto tako da se u svim algebarskim računima u $K(a)$ zamijeni a sa b.

4.5.3. Stepen tijela K' prema podtijelu K. Znak $[K':K]$.

Dimenzija vektorskog prostora $K(a)$ u odnosu na K zove se također *stepen* tijela $K(a)$ prema tijelu K i označuje se sa $[K(a):K]$. Općenito, ako je K' nadtijelo tijela K pa ako postoji n linearno nezavisnih članova $x_1 x_2 \cdots x_n$ iz K' sa svojstvom da je $K[x_1 x_2 \cdots x_n]=K'$, tada se broj n zove *stepen tijela K' prema tijelu K* i označuje sa $n=[K':K]$.

Dokaz teorema 4.5.2. Relacija $v \in K(a)$ znači da je $v=\dfrac{g(a)}{h(a)}$, gdje su $g, h \in K[a]$, tj. a-polinomi nad K; možemo pretpostaviti da su f, h međusobno prosti. Kad naime f, h ne bi bili međusobno prosti, bilo bi $f \mid h$ (jer je f ireducibilno nad K), a time $h(a)=0$ jer je $f(a)=0$. Prema tome, bilo bi

$$v=\frac{g(a)}{h(a)}, \quad \text{tj.} \quad v=\frac{g(a)}{0},$$

što isključujemo.

Dakle je $M(f, h)=1$. Zato jednadžba $fX+hY=1$ ima neko rješenje

$$X, Y \in K[x], \text{ a time i jednadžba } f \cdot Xg+hYg=g.$$

Dakle postoje polinomi $p(x)$, $Q(x)$ za koje je

$$f(x)\,p(x)+h(x)\,Q(x)=g(x).$$

Specijalno, za $x=a$ daje to

$$Q(a)=\frac{g(a)}{h(a)} \quad \text{dakle } Q(a)=v.$$

Prema tome, svaki član v je prikaziv kao a-polinom nad K. No, ako je taj prikaz stepena $\geq n$, može se on reducirati na stepen $<n$ pišući

$$Q(x)=f(x)\,q(x)+r(x), \text{ pri čemu je } r=0 \quad \text{ili} \quad \operatorname{st} r<\operatorname{st} f;$$

očigledno je tada $r(a)=v$.

Dokažimo da je polinom $r(x)$ stepena $<n$ jednoznačno određen zahtjevom $r(a)=v$, $r(x)\in K[x]$.

Pa neka je također $r_1(a)=v$, $r_1(a)\in K[a]$, $\operatorname{st} r_1<\operatorname{st} f$.

Tada bismo imali x-polinom $r_2(x)\equiv r(x)-r_1(x)\in K[x]$; taj je polinom r_2 stepena $<\operatorname{st} f$ i ima a kao nulište. Promatrajmo $M(r_2, f)$. Ta mjera ne može biti 1, jer bi inače jednadžba $r_2(x)\,X(x)+f(x)\,Y(x)=1$ imala rješenje X, Y u $K[x]$. Stavljajući $x=a$ postala bi ta jednadžba $0=1$— nemogućnost. Dakle je $M \neq 1$, a to znači da je r_2 identički 0, tj.

$$r(x)-r_1(x)\equiv 0, \quad \text{tj.} \quad r=r_1.$$

Dokažimo još da *su članovi* (1) *linearno nezavisni u odnosu na* K. Kad bi naime postojali koeficijenti $k_0, k_1, \ldots, k_{n-1}\in K$ ne svi $=0$ sa svojstvom

$$k_0+k_1 a+k_2 a^2+\cdots+k_{n-1} a^{n-1}=0,$$

onda to znači da bi a bilo nulište polinoma $k(x)$; kako je također $fa=0$ te kako je f nesvodljivo, bilo bi $f(x)\mid k(x)$, što je nemoguće jer je $\operatorname{st} k(x)<\operatorname{st} f(x)$.

Posljednja rečenica u teoremu je očigledna.

4.5.4. *Šta je* $K(c)$, ako *je* $c\in K(a)$? Naime vidjeli smo da se c može na jednoznačan način prikazati kao a-polinom nad K stepena $<\operatorname{st} f(=n)$:

$$c=c_0+c_1 a+c_2 a^2+c_{n-1} a^{n-1}. \tag{1}$$

Isto vrijedi za $a^\nu c$:

$$a^\nu c=c_{\nu 0}+c_{\nu 1} a+c_{\nu 2} a^2\cdots+c_{\nu\, n-1} a^{n-1} \quad (\nu=0, 1, 2, \ldots n-1).$$

Eliminirajući iz (1) veličine $1, a, a^2\cdots a^{n-1}$, dolazi se do uslova

$$\begin{vmatrix} c_{00}-c & c_{01}\cdots c_{0\,n-1} \\ c_{10} \quad c_{11}-c & c_{1\,n-1} \\ \cdots & \cdots \end{vmatrix}=0 \tag{2}$$

(isp. 11, § 10.7).

To je jednadžba n-og stupnja u c. Pa će biti $K(c)=K(a)$, onda i samo onda ako je jednadžba (2) nerastavljiva u prstenu $K[x]$.

Naime, samo će u tom slučaju biti

$$[K(c):K]=[K(a):K].$$

4.6. Općenito o proširenju tijela i adjunkciji.

4.6.1. $K[M]$, $K(M)$. Neka je K tijelo a K_1 neko prošireno tijelo, dakle $K_1\supset K$ Ako je M neki neprazan podskup od K_1, tada se sa $K(M)$ (odnosno

$K[M]$ označuje skup vrijednosti svih racionalnih (cijelih racionalnih) funkcija s konačno mnogo argumenata iz M i s koeficijentima iz K.

Kaže se da $K(M)$ nastaje adjungiranjem (priklapanjem) množine M množini K. Jasno je da je $K \subset K[M] \subset K(M) \subset K_1$.

Specijalno, ako je $M = \{x_1, x_2, \ldots, x_n\}$, tada se piše

$$K[\{x_1 \ldots x_n\}] = K[x_1, \ldots, x_n], \; K(\{x_1 \ldots x_n\}) = K(x_1, \ldots, x_n).$$

4.6.2. Ako je skup M jednočlan (odnosno konačan), tada se govori o *prostoj*, **jednostavnoj** (odnosno **konačnoj**) **adjunkciji** $K(M)$. Umjesto $(K(x_1))(x_2)$ pišemo $K(x_1)(x_2)$; isto tako definiramo

$$K(x_1)(x_2)(x_3) = (K(x_1)(x_2))(x_3); \quad \text{itd.}$$

$\longrightarrow$ **4.6.2.1. Teorem o postupnoj i simultanoj adjunkciji.**

Neka za tijela K_0, K_1, K_2 *vrijedi*

$$K_0 \subset K_1 \subset K_2$$

$$K_1 = K_0(M_1), \quad M_1 \subset K_1:$$

(1)

$$K_2 = K_1(M_2), \quad M_2 \subset K_2:$$

tada je

$$K_2 = K_0(M_1 \cup M_2), \quad tj.$$

umjesto postupne adjunkcije M_1 *pa* M_2 *može se na cilj stići jednokratnom adjunkcijom unije* $M_1 \cup M_2$.

Obrazac (1) se dokazuje tako da se dokaže da je ispravno u (1) znak $=$ zamijeniti sa $\subset$ i sa $\supset$. Tako npr. $(1)_2 \subset (1)_1$ znači da svaku racionalnu funkciju

$$F(x_1, x_2 \ldots x_n) = \frac{P(x_1 \cdots x_n)}{Q(x_1 \cdots x_n)} \quad \text{pri čemu je } \{x_1, \ldots, x_n\} \subset M_1 \cup M_2$$

možemo očigledno napisati i kao racionalnu funkciju

$$\frac{f(y_1 \cdots y_k)}{g(y_1 \cdots y_k)} \quad \text{pri čemu su } f, g \in K_1[y_1, \ldots, y_k] \text{ te } \{y_1, y_2, \ldots, y_k\} \subset M_2.$$

4.6.3. Ako svako $m \in M$ jest (nije) nulište nekog polinoma $f(x) \in K[x]$, tada se govori o *algebarskoj* (*transcendentnoj*) *adjunkciji*, odnosno o *algebarskom* (*trancendentnom*) *proširenju* $K(M)$ tijela K.

4.6.4. Stepen člana prema tijelu. Znak $[a:K]$.

Ako je $a \in K_1 \supset K$ te $fa = 0$ za neko $fx \in K[x]$, tada se kaže da je a *algebarsko nad* K; *najniži* stepen nesvodljivog takvog polinoma zove se *stepen od* a *u odnosu na* K i označuje se sa $[a:K]$.

Naravno, ako je $a \in K_1 \supset K$ algebarsko nad K, tada je $[a:K] \leq [K_1:K]$.

—→ **4.6.5. Osnovni teorem o stepenu tijela.**

Ako je K_1 konačno proširenje od K, a K_2 konačno proširenje od K_1, tada je i K_2 konačno proširenje od K i vrijedi

$$[K_2 : K] = [K_2 : K_1] \cdot [K_1 : K].$$

Dokaz. Relacija $n = [K_2 : K_1]$ znači da postoji n-člana baza $b_1, b_2, \ldots, b_n$ u K_2; pa za svako $k \in K_2$ imamo jednoznačan rastav

(1) $$k = \sum_j k_j b_j \quad \text{uz} \quad k_j \in K_1 \quad (j = 1, 2, \ldots, n).$$

Isto tako $m = [K_1 : K]$ znači da u K_1 postoji m-člana baza $a_1, a_2, \ldots, a_m$ u odnosu na K kao izvor koeficijenata; pa posebno za svako k_j iz (1) imamo jednoznačan rastav

(2) $$k_j = \sum_{i=1}^{m} k_{ij}\, a, \quad \text{uz} \quad k_{ij} \in K, \ (j = 1, 2, \ldots, n).$$

Stavljajući (2) u (1) izlazi

(3) $$k = \sum_{ij} k_{ij}\, a_i\, b_j, \qquad (i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n).$$

Dakle, linearna kombinacija od mn članova

(4) $$a_i\, b_j \in K$$

i s koeficijentima iz K daje svako $k \in K_2$. Dokažimo da su članovi (4) linearno nezavisni, tj. da iz

(5) $$\sum_{ij} x_{ij}\, a_i\, b_j = 0, \ x_{ij} \in K$$

izlazi

(6) $$x_{ij} = 0 \qquad (i = 1, 2, \ldots m;\ j = 1, 2, \ldots n).$$

No, (5) možemo srediti po b_j, pa zbog linearne nezavisnosti od $b_1, \ldots, b_n$ mora biti

(7) $$\sum_{i=1}^{m} x_{ij}\, a_i = 0 \qquad (j = 1, 2, \ldots, n).$$

A iz (7) zbog linearne nezavisnosti od $a_1, a_2, \ldots, a_m$ moraju za svako napisano j koeficijenti x_{ij} biti 0, pa time izlazi (6). To znači da je

$$[K_2 : K] = mn = [K_2 : K_1] \cdot [K_1 : K].$$

Induktivno po $m \in N$ dokazuje se

4.6.5.1. Teorem. Ako su brojevi

(1) $$[K_m : K_{m-1}],\ [K_{m-1} : K_{m-2}],\ \ldots\ [K_1 : K_0]$$

prirodni, tada je njihov produkt $= [K_m : K_0]$. Posebno, ako su brojevi (1) jednaki 2, tada je $[K_m : K_0] = 2^m$, pa se kaže da je K_m *kvadratno-korijensko raširenje od* K_0, odnosno da je svako $k_m \in K_m$ *kvadratno-korijenska veličina nad* K_0.

za bilo koje x', $x'' \in I$; tada za svako $x_0 \in I$ niz

$$x_0,\ x_1 = \varphi x_0,\ x_2 = \varphi x_1, \ldots,\ x_{n+1} = \varphi(x_n), \ldots \tag{2}$$

konvergira i iz $\lim\limits_{n\to\infty} \varphi x_n = \xi$ izlazi $\xi = \varphi \xi$.

Dokaz. Treba dokazati da se gotovo svi članovi niza (2) nalaze u proizvoljno kratkim intervalima, tj. da je $|x_n - x_s|$ proizvoljno mala veličina čim su n, s vrlo veliki brojevi. No

$$|x_n - x_s| = |\varphi x_{n-1} - \varphi x_{s-1}| \leq M \cdot |x_{n-1} - x_{s-1}|, \text{ tj.}$$

$$|x_n - x_s| \leq M |x_{n-1} - x_{s-1}|.$$

Iz istog je razloga to dalje

$$\leq M \cdot M |x_{n-2} - x_{s-2}|, \text{ itd.}$$

$$|x_n - x_s| \leq M^n |x_0 - x_{s-n}| \tag{3}$$

Kako je

$$|x_0 - x_{s-n}| \leq |x_0 - x_1| + |x_1 - x_2| + \cdots + |x_{s-n-1} - x_{s-n}| \leq |x_0 - x_1| + \\ + M|x_0 - x_1| + M^2 |x_0 - x_1| + \cdots + M^{s-n-1} |x_0 - x_1| \leq \\ \leq |x_0 - x_1| (1 + M + M^2 + \cdots) = \frac{1}{1-M} |x_0 - x_1|,$$

to (3) daje

$$|x_n - x_s| \leq \frac{M^n}{1-M} |x_0 - x_1|. \tag{4}$$

Kako je $\lim M^n = 0$ znači, prema (4), da zaista za svako $\varepsilon > 0$ postoji neki indeks n_0 tako da iz $n, s > n_0$ izlazi $|x_n - x_s| < \varepsilon$. Dakle je niz x_n Cauchyjev pa zato postoji $\xi = \lim\limits_{n\to\infty} x_n$.

Za element $\xi = \lim x_n$ imamo

$$|\varphi x_n - \varphi \xi| \leq M |x_n - \xi|, \text{ što zbog } |x_n - \xi| \to 0 \text{ znači da je}$$

$$\lim |\varphi x_n - \varphi \xi| = 0, \text{ tj. } |\xi - \varphi \xi| = 0, \text{ dakle je } \xi = \varphi \xi.$$

Dokažimo da je ξ *jedinstveno i da ne zavisi od* x_0. Ako umjesto x_0 uzmemo u I element $x_0' \neq x_0$, tada istim postupkom dolazimo do određena niza $x'_{n+1} = \varphi(x'_n)$, $(n = 0, 1, \ldots)$ i do elementa $\xi' = \lim x_n'$ za koji je $\xi' = \varphi \xi'$.

Pretpostavka

$$0 \neq |\xi' - \xi| = |\varphi \xi' - \varphi \xi|$$

u protivnosti je s relacijom

$$|\varphi \xi' - \varphi \xi| \leq M |\xi' - \xi| < |\xi' - \xi|.$$

Dakle je ξ jedina nepomična tačka funkcije φ.

⟶ 1.2.3. Teorem o kontrakciji ili stezanju i o nepomičnoj tački.

Ako je E bilo koji metrički potpuni prostor, a φ ***bilo koje neprekidno stezanje (kontrakcija) prostora E u sama sebe, tada postoji jedan jedini član***

Dokaz. *Slučaj* $p=0$: ako je $f(x)$ ireducibilan, tada f i f' ne mogu imati zajedničkog nulišta jer odatle bi izlazilo $f|f'$, što je nemoguće. Dakle je $M(f, f')=1$, što znači da su nulišta od f prosta.

Slučaj $p>0$. Jasno je da polinom $f(x^p)$ ima neprosto nulište; obrnuto ako je $f'(x)=0$, onda je $\nu f_\nu=0$ za $\nu=0, 1, 2, \ldots, n$; a to znači da je $f_\nu=0$ za svako ν koje je nedjeljivo sa p, tako da je

$$f(x)=f_0+f_p x^p+f_{2p}x^{2p}+\cdots=g(x^p),\ g \text{ polinom.}$$

⟶ **4.8. Teorem o jednostavnosti konačnih algebarskih raširenja (Abel).**

Neka je $K'=K(a_1, a_2, \ldots, a_n)$, gdje je n prirodan broj, a članovi a_2, $a_3, \ldots, a_n$ su separabilni u odnosu na K; tada postoji član $b\in K'$ sa svojstvom $K'=K(b)$, tj. $K(a_1, a_2, \ldots, a_n)=K(b)$. Posebno, svako separabilno konačno proširenje tijela je jednostavno (prosto).

Pri tom a_1 može biti i inseparabilno nad K.

Provedimo dokaz za $n=2$ i to za beskonačno K (za konačno K isp. § 4.10.3).

Neka je $f(x)$ ireducibilni polinom iz $K[x]$ za koji je $fa_1=0$; isto tako neka je $g(x)$ ireducibilni polinom iz $K[x]$ za koji je $ga_2=0$. Neka je

$$fx=(x-a_1)(x-c_2)\cdots(x-c_m),\ a_1=c_1$$
$$g(x)=(x-d_1)(x-d_2)\cdots(x-d_n),\ a_2=d_1.$$

Kako je a_2 separabilno, bit će $d_1\neq d_j$ za $j\neq 1$ pa možemo promatrati članove

$$\text{(1)}\qquad \frac{c_i-c_1}{d_j-d_1}\quad \text{za } i=1, 2, \ldots, m;\ j=2, 3, \ldots, n.$$

Kako je K beskonačno, postoji neko $c\in K'$ koje se razlikuje od svih članova (1). Stavimo

$$\text{(2)}\qquad b=a_1+ca_2$$

Tvrdimo da je

$$\text{(3)}\qquad K(b)=K(a_1, a_2)\ (\equiv K').$$

Jasno je da u (3) možemo znak $=$ zamijeniti sa $\subset$. Treba još dokazati da znak $=$ možemo zamijeniti i sa $\supset$; za to je dovoljno pokazati da $a_1, a_2\in K(b)$. No, ako

$$\text{(4)}\qquad a_2\in K(b),$$

tada će biti i $a_1\in K(b)$ jer je $a_1=b-ca_2$, a članovi b, c, a_2 su u $K(b)$. Dokažimo dakle (4).

Zbog (2) zadovoljava član a_2 jednadžbe

$$g(x)=0\qquad f(b-cx)=0.$$

Ostala nulišta od g jesu $d=d_2, d_3, \ldots, d_n$ i bit će

$$b-cd_j\neq c_i\ \text{ dakle }\ f(b-cd_j)\neq 0\ \text{ za } j=2, 3, \ldots, n.$$

To znači da je $x-a_2$ najveća zajednička mjera polinomâ $g(x)$, $f(b-cx)$; kako su koeficijenti tih polinoma u $K(b)$, bit će i koeficijenti od $x-a_2$ u $K(b)$, tj. specijalno $-a_2 \in K(b)$, time i $a_2 \in K(b)$. Dakle vrijedi (4) a time i (3).

Pretpostavimo da je teorem 4.8. dokazan za $n=2, 3, \ldots m$; dokažimo ga i za $n=m+1$. Imamo $K(a_1 a_2 \cdots a_n)=K(b')$.

$$K(a_1 a_2 \cdots a_m, a_{m+1})=K(b', a_{m+1})=(n=2)=K(b).$$

Time je teorem 4.8. potpuno dokazan za beskonačno K.

4.9. Kompozit zadanih tijela. — **4.9.1.** Definicija. *Najmanje* tijelo koje obuhvata tijela K_1, K_2 zove se kompozit tijelâ K_1, K_2.

Pojam kompozita ima smisla samo kad su K_1, K_2 podtijela nekog zadanog tijela. Tako npr. za zadana proširenja $K(x_1)$, $K(x_2)$ tijela K jasno je da je $K(x_1, x_2)$ kompozit tijelâ $K(x_1)$, $K(x_2)$.

4.9.2. Teorem. Ako su tijela K_1, K_2 raširenja nekog tijela K_0 pa ako postoje $x_1, x_2, \ldots, x_n$ sa svojstvom

(1) $$K_2=K_0(x_1, x_2, \ldots, x_n),$$

tada za kompozit K od K_1, K_2 vrijedi

(2) $$K=K_1(x_1, x_2, \ldots, x_n).$$

Posebno ako je (1) konačno algebarsko raširenje od K_0, tada se kompozit K od K_1, K_2 sastoji od svih skalarnih produkata

(3) $$a_1 b_1+a_2 b_2+\cdots+a_s b_s,$$

pri čemu vrijedi

$$\{a_1, a_2, \ldots, a_s\}\subset K_1, \ \{b_1, b_2, \ldots, b_s\}\subset K_2.$$

Dokaz. Iz (1) izlazi da

$$K\supset\{x_1, x_2, \ldots, x_n\} \text{ jer } K\supset K_2\supset\{x_1, \ldots, x_n\};$$

kako $K\supset K_1$, to će biti $(2)_1\supset(2)_2$. No, tijelo $(2)_2$ sadrži i K_1 i K_2 dakle sadrži i K. Odatle izlazi da (2) vrijedi.

Nadalje, ako su $x_1, x_2, \ldots, x_n$ algebarski u odnosu na K_0, onda su oni algebarski pogotovo u odnosu na K_1 jer je $K_1\supset K_0$ pa se svako $c\in K$ može izraziti kao cijela racionalna funkcija od $x_1 \cdots x_n$ s koeficijentima iz K_1, tj. c je suma od konačno mnogo izraza oblika $c_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, pri čemu je taj c-koeficijent iz K_1; nadalje je produkt $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ iz K_2 jer prema (1) imamo $\{x_1, \ldots, x_n\}\subset K_2$. Time je teorem 4.9.2. dokazan.

4.10. Konačna tijela ili Galoisova polja. — **4.10.1.** Svako *konačno* tijelo zove se i *Galoisovim poljem*; ako ono ima s članova, označuje se ono i sa $GF(s)$.

Vidjet ćemo da su konačna tijela komutativna (t. 4.10.3.) i da im je glavni broj oblika p^n (p prost broj) (t. 4.10.2). Konačna tijela dolaze u teoriji računskih strojeva pri građenju pamtila ili memorije tih strojeva (isp. R. L. Ashenhurst, The structure of multiple-coincidence selection systems, disertacija, Harvard Univ. 1956).

—→ **4.10.2. Teorem.** ***Karakteristika Galoisova polja je $\neq 0$, dakle određen prost broj. Kardinalni broj Galoisova tijela GF je p^n, pritom je p karakteristika a n broj elemenata baze tijela GF u odnosu na Ip.***

Naime, kad bi karakteristika bila 0, tada bi GF sadržavalo Q i bilo bi beskonačno.

Egzistencija baze je očigledna: uzme se proizvoljan član $b_1 \neq 0$; time imamo i članove $2b_1,\ 3b_1 \cdots (p-1)b_1$. U preostatku uzmemo član $b_2 \neq 0$, itd. Neka je $B = \{b_1, b_2, \ldots, b_n\}$ baza; baza je konačna jer je i samo tijelo F konačno. Tada je čitavo tijelo sastavljeno od članova oblika

$$d_1 b_1 + d_2 b_2 + \cdots d_n b_n, \quad \text{pri čemu je} \quad d_\nu \in Ip. \tag{1}$$

No broj tih izraza (1) je upravo p^n.

—→ **4.10.3. Teorem.** ***Svako konačno asocijativno tijelo K je komutativno; pripadna grupa $(K \setminus \{0\}; \cdot)$ je ciklična, pa je $K = D_\nu(\zeta)$; pri tom je p karakteristika tijela K a ζ neki primitivni korijen jedinice reda $s = kK - 1$ (kX znači kardinalni broj od X).***

Dokaz. Neka tijelo K ima b elemenata a središte $ZK\, q$ elemenata (ZK je skup svih članova iz K koji komutiraju sa svakim $k \in K$; isp. 17, § 9.5.). Dokazat ćemo da je $ZK = K$. Lako se dokaže da je ZK komutativno i asocijativno podtijelo od K. Neka je stupanj od K u odnosu na ZK jednak n i $a_1, a_2, \ldots, a_n$ jedna baza od K; tada se K sastoji od svih članova oblika

$$\sum_{\nu=1}^{n} x_\nu a_\nu, \quad (x_\nu \in ZK,\ \nu = 1, 2, \ldots, n).$$

Dakle je

$$b = q^n. \tag{1}$$

Za svako $a \in K$ promatrajmo pripadni normalizator $K_a = \{x;\ x \in K,\ ax = xa\}$. Također K_a je podtijelo kao što se lako vidi tako da imamo

$$ZK \subset K_a \subset K \quad (a \in K).$$

Za kardinalni broj kK_a podtijela K_a dokazuje se relacija poput (1):

$$kK_a = q^d, \tag{2}$$

pri čemu $d \mid n$; d zavisi općenito od a.

Promatrajmo sve razrede konjugiranosti grupe $(G, \cdot)$ gdje je $G = K \setminus \{0\}$, (isp. 17, § 15.4.); kao što znamo, oni su disjunktni podskupovi koji G iscrpljuju; svakom $x \in ZK$ odgovara jednočlan razred, a svakom eventualnom $a \in G \setminus ZK$ odgovara razred od

$$\frac{kG}{kG_a} = \frac{q^n - 1}{q^d - 1}$$

članova. Na taj način imamo

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}, \tag{3}$$

pri čemu se sumacija proteže na *eventualne* normalizatore $K_x \neq ZK$. Međutim, odmah ćemo zaključiti da takvih normalizatora nema jer u (3) mora stajati $n=1$. Pretpostavimo naprotiv da je $n>1$; promatrajmo tada polinom

$$\Phi_n(x) = \prod_{k \in \Phi(n)} \left(x - e^{\frac{2\pi i k}{n}}\right)$$

—produkt korijenskih faktora svih primitivnih korijena jedinice n-tog reda. Taj je polinom primitivan polinom s cijelim racionalnim koeficijentima i dijeli $x^n - 1$ kao i $\frac{x^n-1}{x^d-1}$ za svaki netrivijalni divizor d od n; to posebno znači da za prirodni broj $q>1$ cijeli broj $\Phi_n(q)$ dijeli q^n-1 kao i $\frac{q^n-1}{q^d-1}$ a time prema (3) također bi bilo $q-1$ djeljivo sa $\Phi_d(q)$. Međutim, to nije moguće jer je

$$q>1 \text{ te } |q-\xi| \geq |q - Re\,\xi| > |q-1|$$

za svako nulište ξ od $\Phi_n(x)$.

Dakle je tijelo K zaista komutativno.

Prema Fermatovu teoremu o grupama (17, § 18.12.4) za svako $a \in K \setminus \{0\}$ vrijedi $a^s = 1$, gdje je $s = kK - 1$. To znači da polinom $x^s - 1$ ima u $K\,s$ različitih nulišta; svako je to nulište prosto pa zato $(x^s-1)'_{x=a} = s \cdot a^{s-1}$ nije djeljivo sa p, tj. $M(p, s) = 1$. Može se dalje pokazati da je bar jedno od tih nulišta primitivno, recimo ζ; time je $\zeta^D = K \setminus \{0\}$, odnosno $D_p(\zeta) = K$ jer je 0 već u D_p.

Prema tome se K podudara sa skupom nulišta polinoma $x^{s+1} - x$.

$\longrightarrow$ **4.10.4. Teorem o izomorfizmu.** ***Ako dva asocijativna konačna tijela K, K' imaju jednako mnogo članova, onda su ona izomorfna.***

Dokaz. Neka je p karakteristika od K, a p' od K'; tada za kardinalne brojeve kK, kK' imamo $kK = p^m$, $kK' = p'^{m'}$ dakle $p^m = p'^{m'}$; kako su p, p' prosti brojevi nužno je $p = p'$, te $m = m'$.

No, prema teoremu 4.10.3, vrijedi $K = D_p(\zeta)$, $K' = D_p(\zeta')$; pišući svuda pri računanju ζ' umjesto ζ dobije se iz K upravo K' kao izomorfna slika od K.

4.10.5. Teorem o potenciranju na p i p^{-1}. U Galoisovu polju $GF(p^n)$ vrijedi

$$(1) \qquad (x+y)^p = x^p + y^p$$

$$(x-y)^p = x^p - y^p$$

pa je operacija $x \to x^p$ jednolisna (tj. $x \neq y \Rightarrow x^p \neq y^p$); drugim riječima, inverzna operacija $y \to y^{p^{-1}}$ je jednoznačna.

Dovoljno je dokazati (1). No, prema binomnom teoremu

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k};$$

međutim, pri $k=1, 2, \ldots, p-1$ broj $\binom{p}{k}$ je djeljiv sa p pa je zato odgovarajući član u binomskom razvoju jednak 0.

4.11. Savršena tijela. — **4.11.1.** *Definicija savršenosti.* Tijelo K je *savršeno* (*perfektno*) ako svaki ireducibilni polinom iz $K[x]$ ima samo prosta nulišta, tj. ako je svaki ireducibilni polinom separabilan. Ako tijelo nije savršeno, kaže se da je ono *nesavršeno*. Naravno, K je savršeno onda i samo onda ako je svaki polinom s kratnim nulištem rastavljiv.

4.11.2. Teorem. *Svako asocijativno tijelo karakteristike* 0 *je savršeno* (v. § 4.7.2).

Stvar je jasna, jer ako je $f(x) \in K[x]$ nerastavljiv, onda je nužno $M(f, f')=1$ jer bi inače moralo f dijeliti f'.

—→ **4.11.3. Teorem.** ***Svako tijelo karakteristike 0 je savršeno. Tijelo K karakteristike $p \neq 0$ savršeno je onda i samo onda ako je***

$$K=K^p \equiv (\text{def}) \{x^p;\ x \in K\}.$$

Dokaz. Svakako je $K^p \subset K$. Ako je $K^p \subset K$ i $a \in K \setminus K^p$, tada je polinom $f(x) \equiv x^p - a$ ireducibilan i neseparabilan (jer $f'(x) \equiv 0$ dakle $M(f, f') = f \neq 1$).

Obrnuto, ako je $K^p = K$, onda je K savršeno. Naime, neka je $f(x) \in K[x]$ nerastavljivo, i pretpostavimo da ipak f ima i neprosto nulište. Mora biti $M(f, f') \neq 1$ dakle $f | f'$ dakle $f' = 0$ dakle $f(x) \equiv f_0 + f_p x^p + f_{2p} x^{2p} + \cdots + f_{kp} x^{kp}$. No, zbog $K^p = K$ postoje članovi $a_0, a_1, a_2, \ldots, a_k$ kojima su p-te potencije po redu

$$a_0^p = f_0,\ a_1^p = f_p,\ a_2^p = f_{2p},\ \ldots,\ a_k^p = f_{kp}.$$

Prema tome $f(x)$ postaje

$$f(x) = a_0^p + a_1^p x^p + a_2^p x^{2p} + \cdots + a_k^p x^{kp} = a_0^p + (a_1 x)^p + \cdots + (a_k x)^p = (a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k)^p.$$

To znači da $f(x)$ ne bi bilo nerastavljivo, protivno pretpostavci.

Uslov $K^p = K$ je specijalno ispunjen pri svakom konačnom asocijativnom tijelu (isp. t. 4.10.5.); zato je K savršeno.

4.11.4. Teorem. *Ako svaki polinom $a(x) \in K[x]$ ima nulišta u K, tada je K savršeno.*

Naime, tada je svaki nerastavljivi polinom nužno linearan.

4.12. Zadaci o tijelima.

1. Navesti neku cjelosnu oblast I koja nije tijelo (prema § 4.2.2. I je nužno beskonačno).

2. Uvjeri se da je skup $\{0, 1, 2, 3\}$ tijelo ako se radi po ovim tablicama:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Dokaži da je ta grupa $(\{0, 1, 2, 3\}, +)$ izomorfna sa

$I_2 \oplus I_2 =$

$+$	00	11	01	10
00	00	11	01	10
11	11	00	10	01
01	01	10	00	11
10	10	10	11	00

, i da je preslikavanje

$00 \leftrightarrow 0$
$11 \leftrightarrow 1$
$01 \leftrightarrow 2$
$10 \leftrightarrow 3$ izomorfija.

3. Promatraj tročlano $GF(3)$; 1) dokaži da je $x^3 - x - 1$ nesvodljivo nad tim tijelom; 2) nađi sve kvadratne nesvodljive normirane polinome iz $GF(3)[x]$; 3) i dokaži da je $x^8 - 1$ djeljivo s produktom tih polinoma.

4. Promatraj $GF(3^2)$ i u njemu nulišta od $x^2 + 2x + 2$. Kako glasi tablica množenja?

5. Dokaži da je identično preslikavanje jedini automorfizam tijela $GF(p)$.

6. Operacija $a \star b = a^{\log_z b}$ (z je baza logaritma: pozitivan realan broj $\neq 1$). Neka je R_0 skup realnih brojeva >0; tada je $(R_0; \cdot; \star)$ tijelo s neutralnim članovima 1 prema $\cdot$ i z prema $\star$; tu je $a^{-1} = z^{1/\log a}$; specijalno je $a \star (bc) = (a \star b)(a \star c)$. Nadalje je $a \star z^n = a^n$, $a \star (a^{-1})^n = z^n$, $a^{-1} = a \star z^{-1}$, $az = (a^{-1}) \star (az)$ $(\neq z)$ (v. D. Miller, A new interpretation of the field postulates, Amer. Math. Monthly, 63 (1965), 574).

7. Ako karakteristika tijela K nije $=2$, tada je $K(x^{1/2}, y^{1/2}) = K(x, y, (x+y)^{1/2})$.

8. Odredi $Q[3^{1/2}, 5^{1/2}]$.

9. Odredi stepen broja $a = \frac{1}{2}(1 + 3^{1/2})$ u odnosu na Q, kao i pripadni minimalni polinom.

10. Nađi stepen $[Q' : Q]$ ako Q' znači: 1) $Q(3^{1/2}, i)$; 2) $Q(2^{1/2}, x)$ uz uslov $x^4 + 6x + 2 = 0$; 3) $Q(3^{1/2}, 5^{1/2}, 7^{1/2})$.

11. Je li $Q(\sqrt{-3}, \sqrt{5}) = Q(\sqrt{3}, \sqrt{-5})$?

12. Nađi najmanje tijelo brojeva u kojem je $\sqrt{2} + \sqrt{5}$; je li ono $= Q(\sqrt{2}, \sqrt{5})$?

13. Neka K, odnosno K' označuje: 1) $Q(\sqrt{2}, \sqrt{3})$, $Q(\sqrt{6})$; 2) $Q(2^{1/6})$, $Q(2^{1/2})$; 3) $Q((1+5^{1/2})^{1/2})$, $Q(5^{1/2})$; 4) $Q((1+2^{1/3})^{1/2})$, $Q(2^{1/3})$; 5) $GF(2^2)$, $GF(2)$; 6) $GF(2^3)$, $GF(2)$. Dokaži da je $K' \supset K$ i da $[K':K]$ iznosi po redu: 2, 3, 2, 2, 2, 3.

14. *Lürothov teorem*[1]. Svako tijelo B između K i $K(x)$ oblika je $B = K(y)$ za neko $y \in K(x)$.

Steinitz je 1910. mislio da bi slično bilo i za racionalne funkcije od *više* varijabli. Stvar ide za dvije varijable kao što je G. Castelnuovo dokazao još 1894, (*Sulla razionalità delle involutioni piane*, Math. Ann. 44 (1894) 125—155), ali ne ide već za 3 varijable (F. Enriques 1912, *Sopra una involuzione non razionale dello spazio*, Rendi Conti, Lincei 21 (1912), 81—83).

15. Odredi *najmanje* tijelo koje obuhvata 1) $Q(\sqrt{2})$, $Q(\sqrt{3})$; 2) $Q(\sqrt{2})$, $Q(\sqrt{3})$, $Q(\sqrt{7})$.

16. Dokaži: ako su tijela K_1, K_2 konačna raširenja tijela K_0, tada je i kompozit K od K_1, K_2 konačno raširenje od K_0.

17. Neka tijelo K bude karakteristike $\neq 2$; neka je $f: K \to K$ bilo kakvo jednoznačno preslikavanje sa svojstvom $f(x+y) = fx + fy$ te $f(z^{-1}) = (fz)^{-1}$ za $z \neq 0$; dokazati da je fK podtijelo izomorfno sa K i da je specijalno $f(x^n) = (fx)^n$ za $n = 2, 3, \ldots$

18. Ako je tijelo K raširenje tijela K_0, tada skup svih članova iz K koji su separabilni čine podtijelo od K.

5. OSNOVI GALOISOVE TEORIJE

Raširivanje tijela je u uskoj vezi s rješavanjem jednadžbi; kao što znamo (isp. 32, § 4.4.4), ako slučajno polinom $a(x) \in K_0[x]$ nema u K_0 nijedno nulište, može se K_0 raširiti na tijelo K u kojem $a(x)$ ima nulište. U vezi s jednadžbom $a(x) = 0$, odnosno s polinomom $a(x)$ te tijelima K_0, K uvodi se osnovni pojam: Galoisova grupa polinoma $a(x)$, odnosno Galoisova grupa tijela K u odnosu na podtijelo K_0. U toj grupi $G(K_0, K)$ na nov se i dalekosežan način ogledaju najvažnija svojstva polinoma $a(x)$ kao što je npr. njegova rješivost u radikalima, separabilnost itd. Osnovnim teoremom 5.3. uspostavljena je veza između (normalnih) tijelâ koja su smještena između K_0, K te (normalnih, podgrupâ grupe $G(K_0, K)$.

5.1. Neke vrsti raširenja tijela.

5.1.1. Korijensko tijelo polinoma $a(x) \in K_0[x]$ zove se svako nadtijelo od K koje obuhvata spektar σ_a od a (tj. sva nulišta od a); posebno je važno *minimalno* korijensko tijelo $K_0(\sigma_a)$. Ako ne kažemo izričito drukčije, bit će korijensko tijelo isto što i minimalno korijensko tijelo ili *spektralno tijelo.*

---

[1] P. Lüroth: Beweis eines Satzes über rationale Funktionen; Math. Ann. 9 (1876) 163—165.

Prema tome, svaki normirani polinom $a(x)$ može se prikazati u svojem korijenskom tijelu kao produkt linearnih normiranih binoma $x-c$ sa $c\in\sigma_a$.

5.1.2. *Prosto radikalno raširenje* tijela K_0 je svako minimalno korijensko tijelo dvočlana (binoma) x^n-c, gdje je $c\in K_0\setminus\{0\}$. Ono se iz K_0 dobije priklapanjem primitivnog nulišta ε_n binoma x^n-1 i proizvoljna nulišta ζ binoma x^n-c; dakle je $K_0(\varepsilon_n,\zeta)$ korijensko tijelo binoma x^n-c nad K_0.

5.1.3. Radikalno raširenje tijela K_0. To je svako nadtijelo K sa svojstvom da postoji konačan niz tijela $K_0\subset K_1\subset K_2\subset\cdots\subset K_m\equiv K$ tako da za svako $i\in\{1, 2, \ldots, m\}$ tijelo K_i bude prosto radikalsko raširenje tijela K_{i-1}.

Pojam je vrlo važan.

5.1.4. Normalno raširenje.

5.1.4.1. Definicija. Normalno raširenje zadana tijela K_0 je svako konačno raširenje K od K_0 s dodatnim važnim svojstvom da za svaki nesvodljivi polinom $a(x)\in K_0[x]$ relacija $\sigma_a\cap K\neq\varnothing$ povlači $\sigma_a\subset K$ dakle i $K_0(\sigma_a)\subset K$.

5.1.4.2. Definicija konjugiranosti nad K_0. Dva su člana z, $\bar z$ iz K koje proširuje K_0 međusobno spregnuta (konjugirana) nad K_0 onda i samo onda ako imaju isti minimalni vlastiti polimom, tj. ako postoji nesvodljiv polinom $p(x)\in K_0[x]$ tako da bude $\{z, \bar z\}\subset\sigma_p$.

5.1.4.3. Teorem. *Konačno algebarsko raširenje K tijela K_0 sa svojstvom da postoji neko proširenje L u kojem leži svako $\bar x$* za svako $x\in K_0$ *je normalno raširenje tijela K_0 onda i samo onda ako iz $x\in K\Rightarrow\bar x\in K$ za svako spregnuto $\bar x$ od x nad K.*

Teorem izlazi neposredno iz definicija 5.1.4 1. i 5.1.4.2.

5.1.4.4. Teorem. *Svako normalno raširenje K tijela K_0 ujedno je i korijensko tijelo nekog polinoma $a(x)\in K_0[x]$* (isp. § 5.1.1).

Dokaz. Iz definicije 5.1.4.1 izlazi da je $K=K_0(x_1, x_2, \ldots, x_n)$ za neki konačni skup $\{x_1, x_2, \ldots, x_n\}\subset K$. Neka je $m_\nu(x)$ minimalni mnogočlan od x_ν nad K_0; kako je $x_\nu\in\sigma_{m_\nu}$ a tijelo K normalno nad K_0 vrijedi $K_0(\sigma_{m_\nu})\subset K$ pa se u K polinom $m_\nu(x)$ raspada u linearne faktore. I produkt $m(x)=$ $=m_1(x)\cdots m_n(x)$ raspada se u K u linearne faktore pa je zato $K_0(\sigma_m)\subset K$; ta relacija sa $\{x_1, \ldots, x_n\}\subset\sigma_m$, $K\equiv K_0(x_1, \ldots, x_n)\subset K_0(\sigma_m)$ daje $K_0(\sigma_m)=K$, što se i tvrdi u teoremu 5.1.4.4.

Dokažimo i obrat prethodnog teorema:

5.1.4.5. Teorem. *Svako korijensko raširenje*

(1) $$K=K_0(\sigma_a)\quad uz\quad a(x)\in K_0[x]$$

ujedno je i normalno raširenje tijela K_0.

Dokaz. Neka je $m\in K[x]$ ireducibilno i $b\in\sigma_m\cap K_0$; dakle je $m(x)\equiv m_b(x)$ minimalni polinom od b nad K_0; treba dokazati da je

(2) $$\sigma_{m_b}\subset K.$$

No, zbog (1) može se b prikazati cijelo-racionalno pomoću članova iz $\sigma_a \equiv \{x_1, \ldots, x_n\}$, recimo

(3) $$b = c(x_1, x_2, \ldots, x_n).$$

Za svaku permutaciju $p \in \{1, 2, \ldots, n\}! = S_n$ imamo polinome

(4) $$c_p(x_1, \ldots, x_n\} \equiv c(x_{p_1}, x_{p_2}, \ldots, x_{p_n}).$$

Neka je

(5) $$C(x, x_1, \ldots, x_n) = \prod_p (x - c(x_{p_1} x_{p_2} \ldots x_{p_n})), \quad (p \in S_n).$$

Polinom (5) je stepena $n!$ prema x; njegovi koeficijenti su simetrične funkcije veličina $x_1, x_2, \ldots, x_n$; zato se oni mogu cjeloracionalno izraziti pomoću koeficijenata $a_1, a_2, \ldots, a_n$ zadanog polinoma $a(x)$ pa je zato polinom (5) član od $K_0[x]$.

No, zadano $b \in K$ je nulište od (5) (uvrstiti p = identična permutacija); zato minimalni polinom $m_b(x)$ dijeli C, tj. $\sigma_{m_b} \subset \sigma_C \subset K$, dakle zaista svi konjugati od b nad K_0 leže u K, za čim smo i išli.

5.1.4.6. Teorem. *Ako je K normalno raširenje od K_0, pa ako je tijelo K_1 između K_0 i K, tada je K normalno raširenje i od međutijela K_1.*

Dokaz. Neka je $a(x) \in K_0[x]$ sa svojstvom da bude $K_0(\sigma_a) = K$. Iz $K_0 \subset K_1$ izlazi da je $a(x) \in K_1[x]$ kao i $K_0(\sigma_a) \subset K_1(\sigma_a) \subset K$. Odatle i iz $K_0(\sigma_a) = K$ izlazi $K_1(\sigma_a) = K$, dakle je K normalno nad K_1.

5.1.4.7. Teorem o uslovnoj prelaznosti svojstva normalnosti

Normalno proširenje K_1 tijela K koje je normalno proširenje od K_0 jest normalno proširenje od K_0 onda i samo onda, ako postoji mnogočlan $a(x) \in K_0[x]$ sa svojstvom da njegovo korijensko tijelo nad K bude upravo K_1 tj. da bude $K(\sigma_a) = K_1$.

Nužnost. Neka je K_1 normalno proširenje od K_0; tada za neki polinom $b \in K_0[x]$ imamo $K_1 = K_0(\sigma_b)$, gdje je σ_b spektar (skup nulišta) od b. No, prema pretpostavci je $K_0 \subset K$; zato

(1) $$K_0(\sigma_b) \equiv K_1 \subset K(\sigma_b);$$

kako je $K \subset K_1$ i $\sigma_b \subset K_1$, bit će

(2) $$K(\sigma_b) \subset K_1.$$

Iz (1) i (2) izlazi $K_1 = K(\sigma_b)$ pri nekom $b \in K_0[x]$.

Dovoljnost. Neka je K normalno nad K_0 a K_1 normalno nad K te

(3) $$K_1 = K(\sigma_b) \quad \text{za neko } b \in K_0[x];$$

kako je K normalno nad K_0, to je $K = K_0(\sigma_a)$ za neko $a(x) \in K_0[x]$. Zato jednadžba (3) daje

$$K_1 = (K_0(\sigma_a))(\sigma_b) = K_0(\sigma_b \cup \sigma_a) = K_0(\sigma_{ab}),$$

tj. K_1 je korijensko tijelo polinoma ab nad K_0; tim samim je K_1 normalno raširenje od K_0.

5.2. *Galoisova grupa $G(K_0, K)$ tijela K nad podtijelom K_0. Galoisova grupa jednadžbe (polinoma).*

5.2.1. Definicija Galoisove grupe (č. Galoaove grupe). Skup svih automorfizama a nadtijela K tijela K_0 za koje je

(1) $$a(x) = x \quad \text{za svako} \quad x \in K_0$$

zove se Galoisova grupa tijela K u odnosu na podtijelo K_0; označuje se sa $G(K_0, K)$.

Drugim riječima $G(K_0, K)$ je *grupa* svih permutacijâ a tijela K za koje vrijedi (1) te

$$a(x+y) = a(x) + a(y), \quad a(xy) = a(x)\, a(y)$$

za svako $x, y \in K$.

Ubuduće, pretpostavljat ćemo pa je K *konačno* raširenje od K_0.

Jasno je da je skup $G(K_0, K)$ zaista grupa u odnosu na slaganje automorfizama.

5.2.2. Grupa zadana polinoma (zadane jednadžbe).

Ako polinom $a(x)$ ima koeficijente iz tijela K_0, tada se grupa $G(K_0, K_0(\sigma))$ zove grupa polinoma $a(x)$ (jednadžbe $a(x) = 0$); pri tom je $K_0(\sigma_a)$ minimalno nadtijelo od K_0 u kojem leže sva nulišta polinoma $a(x)$.

5.2.3. Teorem. *Ako je $g(k_1, k_2, \ldots, k_s) = 0$ bilo kakva jednadžba, pri čemu je $\{k_1, k_2, \ldots, k_s\} \subset K$ i $g(x_1, \ldots, x_s) \in K_0[x_1, \ldots, x_s]$, tada za svako $a \in G(K_0, K)$ izlazi*

(1) $$g(ak_1, ak_2, \ldots, ak_s) = 0;$$

i obratno, ako neki automorfizam a tijela K ostavlja netaknutu svaku cjeloracionalnu vezu nad K_0, tada je a član Galoisove grupe.

Dokaz. Neka zadana jednadžba (1) eksplicitno glasi

(2) $$\sum g_{e_1 e_2 \ldots e_s} k_1^{e_1} k_2^{e_2} \ldots k_s^{e_s} = 0,$$

pri tom su $e_1, \ldots, e_s$ neodrečni cijeli brojevi i

$$g_{e_1 e_2 \ldots e_s} \in K_0 \quad \text{dakle i} \quad a g_{e_1 \ldots e_s} \in K_0.$$

Djelujući na (2) sa a izlazi zbog distributivnosti od a prema $+$:

$$\sum a(g_{e_1 \ldots e_s} k_1^{e_1} \ldots k_s^{e_s}) = a\,0$$

i dalje zbog $a\,0 = 0$ i zbog distributivnosti od a prema množenju:

$$\sum a g_{e_1 \ldots e_s}\, a(k_1^{e_1}) \ldots a(k_s^{e_s}) = 0$$

(dalje zbog $a(x) = x$, $x \in K_0$):

$$\sum g_{e_1 \ldots e_s} (ak_1)^{e_1} \ldots (ak_s)^{e_s} = 0$$

tj. vrijedi (1).

Time je prva polovina teorema dokazana.

Druga polovina teorema izlazi iz toga da je za svaki automorfizam o kojemu je riječ $ax=x$, $(x \in K_0)$.

5.2.3.1. Korolar. *Svaki član Galoisove grupe $G(K_0, K)$ prevodi svako $c \in K$ u određen konjugiran član $\bar{c} \in K$.*

Naime, ako je $m_c(x) \in K_0[x]$ minimalni polinom od c, tada je $m_c(c)=0$ a odavle za svako $a \in G(K_0, K)$ imamo

$$a(m_c(c)) = a\,0, \quad \text{tj.} \quad m_c(ac)=0, \quad \text{tj.} \quad ac \in \sigma(m_c).$$

⟶ **5.2.4. Teorem o broju članova Galoisove grupe.** *Neka je tijelo K separabilno normalno raširenje tijela K_0; tada je*

$$k\,G(K_0, K) = [K:K_0] \qquad \text{(isp. § 4.5.3);}$$

riječima: *Galoisova grupa ima upravo onoliko članova kolik je stepen $n=[K:K_0]$ proširenog normalnog tijela K u odnosu na ishodno tijelo K_0.*

Dokaz. Neka je (isp. t. 4.8)

$$K = K_0(x_1) \tag{1}$$

i neka je $p(x) \in K_0[x]$ minimalni polinom od x_1 nad K_0 stepena n.

Svakom članu $c \in K$ pripada jednoznačno određen niz članova

$$c_0,\ c_1,\ \ldots,\ c_{n-1},$$

iz K_0 tako da bude

$$c = c_0 + c_1 x_1 + c_2 x_1^2 + \cdots + c_{n-1} x_1^{n-1} \equiv c(x_1). \tag{2}$$

Posebno za $c=x_1$ dobivamo

$$x_1 = 0 + 1\,x_1 + 0 \cdot x_1^2 + \cdots + 0 \cdot x_1^{n-1} = 1 \cdot x_1. \tag{2'}$$

Neka su $x_1, x_2, \ldots, x_n$ nulišta polinoma $p(x)$. Za svako $\nu \in \{1, 2, \ldots, n\}$ preslikavanje $c \in K \to h_\nu c \equiv c_0 + c_1 x_\nu + c_2 x_\nu^2 + \cdots + c_{n-1} x_\nu^{n-1}$ je određen član grupe $G(K_0, K)$; time se dobije svih n članova grupe $G(K_0, K)$ pa je $G(K_0, K) = \{h_1, h_2, \ldots, h_n\}$.

Zaista, neka je $a \in G(K_0, K)$; tada iz (2) izlazi

$$a(c) = c_0 + c_1(ax_1) + c_2(ax_1)^2 + \cdots + c_{n-1}(ax_1)^{n-1} \in K, \tag{3}$$

jer je ax_1 konjugirano sa x_1 (§ 5.2.3.1).

Isto tako iz $b \in G(K_0, K)$ izlazi

$$b(c) = c_0 + c_1(bx_1) + \cdots + c_{n-1}(bx_1)^{n-1} \in K.$$

Iz $a \neq b$ proizlazi $a(x_1) \neq b(x_1)$. Kad bi naime bilo $a(x_1)=b(x_1)$, bilo bi $b^{-1}a(x_1)=x_1$, što znači da bi automorfizam $b^{-1}a \in G(K_0, K)$ ostavljao na miru tačku $x_1 \in K$; no time bi prema (2) bilo također

$$(b^{-1}a)\,c = c_0 + c_1 b^{-1}ax_1 + \cdots + c_{n-1}(b^{-1}ax_1)^{n-1} =$$

$$= c_0 + c_1 x_1 + \cdots + c_{n-1} x_1^{n-1} = c, \quad \text{tj.} \quad (b^{-1}a)\,c = c$$

za svako $c \in K$; to znači, da je $b^{-1}a = 1$, dakle $a = b$. Dakle je zaista

(4) $kG \leq n$. Dokažimo da je $kG \geq n$ (4′)

i specijalno da je svaki član $x_\nu \in \sigma_p$ oblika ax_1 za neko $a \in G$.

Naime, ako umjesto x_1 u $(2)_2$ pišemo x_ν, tada se dobije izraz

(5) $$c_0 + c_1 x_\nu + c_2 x_\nu^2 + \cdots + c_{n-1} x_\nu^{n-1} \overset{\text{def}}{=} h_\nu c.$$

Uvrstimo li tu posebno $c = x_1$, tada prema (2′) izlazi

(5′) $$x_\nu = h_\nu x_1.$$

Dokažimo ovo:

Preslikavanje $K \ni c \to h_\nu c$ je automorfizam, tj. $h_\nu \in G$.

Najprije ćemo dokazati da za svaki polinom $g(x) \in K_0[x]$ vrijedi

(6) $$h_\nu g(x_1) = g(x_\nu).$$

To je jasno, ako je $\operatorname{st} g < n$; ako je $\operatorname{st} g \geq n = \operatorname{st} p(x)$, odredimo kvocijent $q(x)$ i ostatak $r(x)$ tako da bude

$$g(x) = p(x)\; q(x) + r(x) \quad \text{te} \quad r(x) \equiv 0 \quad \text{ili} \quad \operatorname{st} r < \operatorname{st} p.$$

Odatle

$$g(x_1) = p(x_1)\; q(x_1) + r(x_1), \quad \text{tj.} \quad g(x_1) = r(x_1)$$

jer je $p(x_1) = 0$.

Zato je

$$h_\nu g(x_1) = h_\nu r(x_1) = r(h_\nu x_1) = g(h_\nu x_1)$$

jer je $p(x_\nu) = 0$.

Time je formula (6) dokazana.

Dokažimo da h_ν prevodi sumu u sumu, a produkt u produkt. Ako je naime uz (2) također $d = d(x_1)$ za proizvoljno $d \in K$, tada je

$$c + d = c(x_1) + d(x_1)$$
$$cd = c(x_1)\; d(x_1)$$

pa odatle prema (6) imamo

$$h_\nu (c + d) = (c(x) + d(x))_{x = x_\nu} = c(x_\nu) + d(x_\nu) = h_\nu c + h_\nu d,$$
$$h_\nu (cd) = c(x_\nu)\, d(x_\nu) = h_\nu c \cdot h_\nu d.$$

Dakle je h_ν homomorfizam tijela K u sama sebe.

Još treba pokazati da je ne samo $h_\nu K \subset K$ nego također $h_\nu K = K$ i da iz $c \in K \setminus \{0\}$ proizlazi $h_\nu c \neq 0$. No, kako je $c \neq 0$, postoji $c^{-1} \in K$ pa iz $cc^{-1} = 1$ izlazi $h_\nu ch_\nu c^{-1} = h_\nu 1$, što zajedno sa $h_\nu c^{-1} = (h_\nu c)^{-1}$, $h_\nu 1 = 1$ daje $h_\nu c\, (h_\nu c)^{-1} = 1$, dakle zaista $h_\nu c \neq 0$. Najzad, $h_\nu K = K_0(x_\nu) = K_0(x_1) = K$. Dakle je $h_\nu \in G(K_0, K)$ za $\nu = 1, 2, \ldots, n$.

Kako iz $\nu \neq \nu'$ imamo $x_\nu \neq x_{\nu'}$ znači to da je $h_\nu x_1 \neq h_{\nu'} x_1$ tj. $h_\nu \neq h_{\nu'}$. Prema tome, u grupi $G(K_0, K)$ imamo bar n članova h_ν $(\nu = 1, 2, \ldots, n)$, čime je dokazano i (4′). Iz (4) i (4′) izlazi sam teorem, jer minimalni polinom $p(x)$ separabilnog elementa x_1 ima samo prosta nulišta. Time je osnovni teorem 5.2.4. dokazan.

Kako prema (5′) imamo $h_\nu x_1 = x_\nu$ $(\nu = 1, 2, \ldots, n)$ i kako je $h_\nu \in G$, to znači da specijalno za $\nu = u, t$ imamo $h_u x_1 = x_u$, $h_t x_1 = x_t$ odakle eliminacijom x_1:

$$x_1 = h_u^{-1} x_u, \quad h_t h_u^{-1} x_u = x_t, \quad \text{odnosno} \quad a x_u = x_t \quad \text{za} \quad a = h_t h_u^{-1}.$$

5.2.5. Teorem. *Dva člana x, y tijela K međusobno su konjugirana nad K_0 onda i samo onda ako za neko $a \in G(K_0, K)$ vrijedi $ax = y$, odnosno $x = a^{-1} y$.*

Ako za neko $a \in G(K_0, K)$ vrijedi $ax = y$, tada su elementi x, $y \in K$ naravno spregnuti nad K_0. Obrnuto, neka su elementi x, $y \in K$ spregnuti nad K_0, tj. neka postoji izomorfizam polja $K(x)$ na polje $K_0(y)$ koji x prevodi u y, a elemente polja K_0 ostavlja na miru. Tada se taj izomorfizam može proširiti bar na jedan način do izomorfizma polja K_0 na K, dakle do nekog elementa a grupe $G(K_0, K)$. No, tada je, naravno, $y = ax$.

5.2.6. Primjer. Promatramo li tijelo R realnih brojeva te $R(i)$, $i^2 = -1$, tada je grupa $G(R, R(i))$ sastavljena od dva člana i to iz identičkog preslikavanja i iz konjugiranja: $z \in R(i) \to \bar{z} \in R(i)$ (zrcaljenje na realnoj osi).

⟶ 5.3. Osnovni teorem Galoisove teorije — veza između podtijelâ od K i podgrupâ od G.

5.3.1. Teorem. **(0)** ***Neka je tijelo K normalno raširenje tijela K_0; neka je M proizvoljno (normalno) međutijelo: $K_0 \subset M \subset K$; tada je $G(M, K)$ = skup svih automorfizama $a: K \to K$ za koje je $am = m$ za svako $m \in M$ određena (normalna) podgrupa Galoisove grupe $G(K_0, K)$ i ima $[K:M]$ članova.***

(00) ***Neka je F bilo koja (normalna ili invarijantna) podgrupa grupe $G = G(K_0, K)$; tada je skup***

$$M = \{x;\ x \in K,\ fx = x \text{ za svako } f \in F\}$$

određeno (normalno) nadtijelo od K_0; to podtijelo od K možemo označiti sa $K(F, G)$.

(000) ***Vrijedi***

$$(\star) \qquad G(K(F, G), K) = F$$

za svaku podrupu F od $G = G(K_0, K)$, kao i

$$(\star\star) \qquad K(G(M, K), G) = M$$

za svako međutijelo $K_0 \subset M \subset K$.

Posebno je $K(G(K_0, K), K) = K_0$.

5.3.2. Dokaz teorema (0). Jasno je da je $G(M, K)$ podgrupa od $G(K_0, K)$ jer je $M \supset K_0$. Ako je k tome M normalno raširenje od K_0, tada iz $m \in M$ proizlazi $gm \in M$ za svaki automorfizam $g \in G(K_0, K)$ jer su m, gm međusobno konjugirani. Prema tome, potfunkcija:

$$g \mid M$$

preslikava tijelo M izomorfno na sama sebe, pa je

$$g \mid M \in G(K_0, M).$$

Tako se dobije svaki član grupe $G(K_0, M)$.

Nadalje iz g, $g_1 \in G(K_0, K)$ izlazi očigledno

$$gg_1 \mid M = g \mid M \cdot g_1 \mid M.$$

To znači da je

$$g \to g \mid M \ (g \in G(K_0, K))$$

određen homomorfizam h grupe $G(K_0, K)$ na grupu $G(K_0, M)$. Jezgro $J = h^{-1}\{1\}$ toga homomorfizma sastoji se od svih $g \in G$ za koje je $gm = m$ za svako $m \in M$; prema tome $J = G(M, K)$. Kako je jezgro J svakog endomomorfizma grupe normalna podgrupa, znači da je zaista $G(M, K_0)$ normalna podgrupa od $G(K_0, K)$.

Ujedno primjenom teorema 17, § 12.5.5 o vezi između homomorfizma i izomorfizma dobili smo ovaj

5.3.2.1 Teorem. *Za svako normalno tijelo M smješteno između K_0 i normalna proširenja K vrijedi $G(K_0, M) \cong G(K_0, K)/G(M, K)$, tj. Galoisova grupa međutijela M izomorfna je s faktorskom grupom Galoisove grupe tijela K nad K_0 i grupe istog tijela K nad međutijelom M.*

Kako prema t. 5.2.4. grupa $G(M, K)$ ima upravo $[K:M]$ članova, time je teorem (0) dokazan.

5.3.3. Dokaz teorema (00). Ako je F podgrupa od G, onda je $K(F, G) \equiv M$ podtijelo od K a obuhvaća K_0; to se lako provjeri.

Pretpostavimo još da je F normalna podgrupa od G, tj.

$$gfg^{-1} = f_1 \quad \text{za svako} \quad f \in F$$

i svako $g \in G$; pri tom $f_1 \in F$ zavisi od f i g.

Tada jednadžba $f_1 m = m \ (m \in M)$ postaje

$$gfg^{-1} m = m, \quad \text{tj.} \quad f(g^{-1} m) = g^{-1} m, \quad \text{dakle} \quad g^{-1} m \in M.$$

Prema tome, iz $m \in M$ izlazi $g^{-1} m \in M$, tj. elementi koji su sa m konjugirani također leži u M. To znači da je zaista $K(F, G)$ normalno raširenje tijela K_0.

5.3.4. Dokaz teorema (000).

Dokažimo relaciju (★). Promatrajmo element $x_1 \in K$ za koji je $K_0(x_1) = K$ dakle i $M(x_1) = K$. Neka je $g(x) = \prod_{i \in F} (x - i\, x_1)$; pri svakom automorfizmu $f \in F$ preslikava se σ_g na sama sebe; zato svaki simetrični polinom veličina iz σ_g prelazi pomoću f u sama sebe; to posebno vrijedi za koeficijente polinoma g; zato koeficijenti od g leže u $K(F, G)$. Zato minimalni polinom od x_1 nad $K(F, G)$ dijeli $g(x)$, što znači da mu je stepen $\leq kF$. No, taj stepen je $= [K:M]$; dakle je $[K:M] \leq kF$; tu je $M = K(F, G)$.

No,

(1) $$[K:M] = k\,G(M,\ K)$$

(isp. § 5.2.4), dakle je

(2) $$k\,G(M,\ K) \leq k\,F.$$

Kako se $G(M,\ K)$ sastoji od svih automorfizama tijela K koji ostavljaju netaknut svaki element od M, znači to da $G(M,\ K) \supset F$ pa zato relacije (1) i (2) daju

(3) $$k\,(G(M,\ K)) = k\,F = [K:M];$$

dakle zaista vrijedi (*).

Dokažimo i (**): Neka je $K_0 \subset M \subset K$; stavimo $F = G(M,\ K)$; dokažimo da vrijedi (**).

Jasno je da je $M \subset K(F,\ G)$. Prema osnovnom teoremu 32, § 4.6.5 imamo

(5) $$[K:K(F,\ G)] \cdot [K(F,\ G):M] = [K:M].$$

No, prva zagrada u $(5)_1$ je $= k\,F$; prema (3) je $(5)_2 = k\,F$; zato jednadžba (5) postaje

$$k\,F \cdot [K(F,\ G):M] = k\,F, \qquad \text{tj.}$$

$$[K(F,\ G):M] = 1, \qquad \text{dakle}$$

$$K(F,\ G) = M,$$

što upravo znači da vrijedi (**).

Time je osnovni teorem 4.3.1 potpuno dokazan.

5.4. Normalna raširenja sa razrješivom Galoisovom grupom.

U 17, § 19 upoznali smo pojam (raz)rješive grupe. Nastaje pitanje kad je Galoisova grupa $G = G(K_0,\ K)$ rješiva (K_0 je neko tijelo, a K raširenje od K_0). Pitanje je u vezi s algebarskim rješenjem jednadžbi i s (prostim) radikalskim raširenjem tijela (isp. § 5.1.2, § 5.1.3).

5.4.1. Definicija algebarske jednadžbe $a(x) = 0$ rješive radikalima. Kaže se da se nulište x_1 polinoma $p(x) \in K_0[x]$ može nad K_0 izraziti algebarski ili pomoću radikala, ako se x_1 može iz koeficijenata p_ν dobiti pomoću konačna broja prvih 4-ju operacija i potenciranjâ s eksponentima oblika m^{-1} pri $m \in N$, tj. ako postoji radikalsko raširenje K tijela K_0 sa svojstvom $x_1 \in K$.

Ako je svako nulište od $p(x)$ predočivo radikalima kaže se da je $p(x)$ (odnosno $p(x) = 0$) *rješivo radikalima.*

⟶ **5.4.2. Osnovni teorem.** ***Ireducibilna algebarska jednadžba $a(x) = 0$ s koeficijentima iz tijela K_0 rješiva je radikalima onda i samo onda ako je Galoisova grupa te jednadžbe $a(x) = 0$ rješiva (isp.*** **32, § 5.2.2).**

Nužni dio teorema. Prema pretpostavci korijensko tijelo $K=K_0(\sigma_p)$ je radikalsko raširenje od K_0; prema 5.4.8 postoji neko *normalno radikalsko raširenje* K_1 od K_0 za koje je $K \subset K_1$; ova relacija prema niže navedenom osnovnom teoremu 5.4.3 ima za posljedicu rješivost grupe $G(K_0, K_0(\sigma_p))$.

Dovoljni dio teorema 5.4.2. Prema pretpostavci, grupa $G_p = G(K_0, K_0(\sigma_p))$ je razrješiva; to prema dovoljnom dijelu istog osnovnog teorema 5.4.3 znači da je tijelo $K_0(\sigma_p)$ sadržano u nekom normalnom radikalnom raširenju K_1 tijela K_0; a to upravo znači da je $p(x)=0$ rješivo pomoću radikala.

—→ **5.4.3. Osnovni teorem.** ***Neka je tijelo K normalno raširenje tijela K_0. Galoisova grupa $G=G(K_0, K)$ je rješiva onda i samo onda ako je K sadržano u nekom normalnom radikalskom raširenju K_1 tijela K_0.***

Pri tom vrijedi

5.4.4. Definicija. Raširenje tijela K_0 koji je u odnosu na K_0 i normalno (§ 5.1.4) i radikalsko proširenje (§ 5.1.3) zove se normalno radikalsko raširenje od K_0.

Dokaz teorema 5.4.3 je dosta dug.

5.4.5. Nužni dio teorema 5.4.3. Ako je $G=G(K_0, K)$ razrješivo i K normalno, tada je K podtijelo nekog normalnog radikalskog raširenja K_1 od K_0.

5.4.5.1. Prvi slučaj: *tijelo K je ciklično raširenje od* K_0 (tj. Galoisova grupa $G=G(K_0, K)$ je ciklična). Neka je dimenzija od K prema K_0 jednaka n, tj. $[K:K_0]=n$; neka je $\varepsilon=\varepsilon_n$ primitivni korijen jedinice n-og reda tijela K_0; stavimo $K_1=K(\varepsilon)$; tada je K_1 normalno nad K i nad K_0 (isp. t. 5.1.4.7). Ujedno je jasno da je K_1 najmanje tijelo koje obuhvata i K i $K_0(\varepsilon)$. Zato je grupa $F=G(K_0(\varepsilon), K_1)$ izomorfna s nekom podgrupom grupe $G(K_0, K)$; naime, svako a iz $G(K_0(\varepsilon), K_1)$ ograničeno na K daje neki element iz $G(K_0, K)$. Tako se $G(K_0(\varepsilon), K_1)$ homomorfno preslikava na $G(K_0, K)$. Ovaj homomorfizam je injektivan, jer se svaki element iz $G(K_0, K)$ može najviše na jedan način proširiti do izomorfizma polja K_1 koji ostavlja na miru element ε. Kako je po pretpostavci ova grupa ciklična i ima $n=[K:K_0]$ članova, znači da kardinalni broj $d=[K_1:K_0(\varepsilon)]$ grupe F mora biti djelitelj broja n i da je F ciklična grupa; njen izvodni član ε_d kao potencija od $\varepsilon=\varepsilon_n$ leži u $K_0(\varepsilon)$ pa je K_1 ciklično raširenje tijela $K_0(\varepsilon)$ koje sadrži ε_d; u § 5.4.7 dokazat ćemo da je zato K_1 prosto radikalsko raširenje od $K_0(\varepsilon)$; kako je opet $K_0(\varepsilon)$ prosto radikalsko raširenje od K_0, znači da je K_1 radikalsko normalno raširenje od K_0.

5.4.5.2. Opći slučaj: neka je K normalno raširenje od K_0 s razrješivom grupom $G=G(K_0, K)$; neka je

$$(1) \qquad G_0\,(\equiv G) \supsetneq G_1 \supsetneq \cdots \supsetneq G_r = (e)$$

„razrješivi niz podgrupa" od G[1] (isp. 17, § 11.3); dokažimo da je K podtijelo nekog normalnog radikalskog raširenja K_1 od K_0. Dokaz ćemo izvesti induktivno

---

[1] tj. kompozicioni niz (1.) podgrupâ od G s komutativnim faktorskim grupama $G_{\rho-1}/G_\rho$ pri $\rho = 1, 2, \ldots, r$ (isp. 17, 17.1.3).

po broju r. Slučaj $r=1$ dokazan je u 5.4.5.1. Pretpostavimo da je tvrdnja dokazana za svako normalno tijelo kojemu pripadna Galoisova grupa ima rješavajući niz (1) sa $\leq r$ članova. Neka je sada K normalno nad K_0 i neka pripadna grupa $G=G(K_0\, K)$ ima razrješivi niz od $1+r$ članova. Promatrajmo podgrupu G_1 iz (1.) te tijelo $L=K(G_1,\, G)=\{x;\ x\in K,\ ax=x \text{ za } a\in G_1\}$. Tijelo L je normalno nad K_0, a njegova grupa $G(K_0,\, L)$ je izomorfna sa G_0/G_1 pa je dakle ciklična. Naime, G_0/G_1 je prosta grupa (isp. 17, § 11.13), a kako je ona prema pretpostavci komutativna, izlazi iz 17, § 20.2 da je kardinalni broj grupe G_0/G_1 prost broj; zato je ona ciklična. Prema § 5.4.5.1 L je sadržano u nekom normalnom radikalskom raširenju M tijela K_0. Neka je N kompozit od M i K (v. § 4.9.1); tada je $G(M,\, N)$ izomorfno s nekom podgrupom od $G(L,\, K)=G_1$; no G_1 pa dakle i svaka podgrupa od G_1 dakle i $G(M,\, N)$ ima razrješivi niz od $\leq r$ članova; prema pretpostavci indukcije znači to da je N dakle i K sadržano u nekom normalnom radikalskom raširenju R tijela M; kako je M radikalsko raširenje od K_0, znači da je R radikalsko raširenje od K_0. No, kako je svako radikalsko raširenje dio nekog normalnog radikalskog raširenja S (t. 5.4.8) znači da je zaista K dio normalnog radikalskog raširenja S od K_0.

5.4.6. D o k a z d o v o l j n o g d i j e l a t e o r e m a 5.4.3: Ako je normalno raširenje K od K_0 dio normalnog radikalskog raširenja K_1 od K_0, tada je grupa $G=G(K_0,\, K)$ rješiva.

5.4.6.1. Ako je K_1 normalno radikalsko raširenje od K_0, tada je grupa $G(K_0,\, K_1)$ razrješiva.

Neka je naime

$$K_0 \equiv L_0 \subsetneqq L_1 \subsetneqq \cdots \subsetneqq L_r \equiv K_1 \tag{1}$$

niz tijelâ tako da pri $\rho=1,\, 2, \ldots,\, r$, tijelo $L_\rho \neq L_0$ bude prosto radikalsko raširenje od $L_{\rho-1}$ (v. § 5.1.3). Nizu (1) tijelâ odgovara prema osnovnom teoremu 5.3.1 niz grupâ

$$G_0 \equiv G(K_0,\, K_1) \supsetneqq \cdots \supsetneqq G_\rho = G(L_\rho,\, K_1) \supsetneqq \cdots \supsetneqq G_r = (e) \tag{2}$$

$$(\rho = 1,\, 2, \ldots,\, r-1).$$

Kako je L_ρ normalno raširenje od $L_{\rho-1}$, grupa G_ρ je normalna podgrupa od $G_{\rho-1}$ (t. 5.3.1. (0)). No, prema 5.3.2.1 faktorska grupa $G_{\rho-1}/G_\rho$ je izomorfna sa grupom $G(L_{\rho-1},\, L_\rho)$ koja je razrješiva, jer je L_ρ prosto radikalsko raširenje od $L_{\rho-1}$ (isp. § 5.1.2). No, postojanje niza (2) s rješivim faktorima $G_\rho/G_{\rho-1}$ ima za posljedicu rješivost same grupe $G_0=G(K_0,\, K_1)$ (v. 17, § 19.3).

5.4.6.2. Opći slučaj iskaza 5.4.6; promatrajmo grupu $G(K_0,\, K)$; ona je izomorfna s nekom faktorskom grupom G' od $G(K_0,\, K_1)$; no kako je $G(K_0,\, K_1)$ rješiva grupa, rješiva je i grupa G' dakle i $G(K_0,\, K)$.

Time je i drugi dio teorema 5.4.3 dokazan.

Nedokazani dio t. 5.4.3 izlazi iz

5.4.7. T e o r e m o cikličkom raširenju (isp. 5.4.5.1). *Ako tijelo K_0 sadrži primitivni korijen jedinice $\varepsilon=\varepsilon_n$ reda n pa ako je K cikličko raširenje stepena n od K_0, tada je prosto radikalsko raširenje dobiveno pomoću ireducibilna binoma oblika $x^n - c \in K_0[x]$, tj. K se dobije iz K_0 priklapanjem elementa $c^{1/n}$.*

Dokaz. Kako je $[K:K_0]=n$, postoji ireducibilan polinom $p(x)\in K_0[x]$ i nulište x_1 od $p(x)$ tako da je $K=K_0(x_1)$. U vezi sa ε i x_1 dokažimo iskaze 5.4.7.2—5.4.7.4 odakle će izaći i sam teorem 5.4.7. Najprije evo jedne korisne definicije.

5.4.7.1. Definicija Lagrangeove rezolvente. Za proizvoljno $x_1\in K$ i proizvoljan cio broj d uz primitivni korijen jedinice reda n, ε, pripadna Lagrangeova rezolventa je:

$$(\varepsilon^d, x_1)\equiv\sum_{\nu=0}^{n-1}\varepsilon^{\nu d}g^{\nu}x_1, \tag{1}$$

pri čemu je g generator cikličke grupe $G(K_0, K)=G$; prema tome je

$$G=\{1, g, g^2, \ldots, g^{n-1}\}.$$

5.4.7.2. Lema. Za bar jednu vrijednost

$$d\in\{0, 1, \ldots, n-1\} \quad \text{vrijedi} \quad (\varepsilon, x_1^d)\neq 0.$$

Dokaz. U obrnutom slučaju bilo bi

$$(\varepsilon, x_1^d)=0 \qquad (d=0, 1, 2, \ldots, n-1); \tag{2}$$

to je skup od n linearnih homogenih jednadžbi za veličine $\varepsilon^0=1, \varepsilon, \ldots, \varepsilon^{n-1}$; zato bi moralo biti (v. 11, § 10.7)

$$\begin{vmatrix} 1 & 1 & \cdots 1 \\ x_1 & gx_1 & \cdots g^{n-1}x_1 \\ x_1^2 & gx_1^2 & \cdots g^{n-1}x_1^2 \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ x_1^{n-1} & gx_1^{n-1} & \cdots g^{n-1}x_1^{n-1} \end{vmatrix}=0, \ \text{tj.} \ \begin{vmatrix} 1 & 1 & \cdots 1 \\ x_1 & gx_1 & \cdots g^{n-1}x_1 \\ x_1^2 & (gx_1)^2 & \cdots (g^{n-1}x_1)^2 \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ x_1^{n-1} & (gx_1)^{n-1} & \cdots (g^{n-1}x_1)^{n-1} \end{vmatrix}=0. \tag{3}$$

jer automorfizam g zadovoljava $g^{\nu}x_1^m=(g^{\nu}x_1)^m$.

No, $(3)_1$ je Vandermondova determinanta veličinâ $x_1, gx_1, g^2x_1, \ldots, g^{n-1}x_1$ među kojima nema jednakih; zato je ta determinanta $\neq 0$ (isp. 11, § 11.5), što se protivi relaciji (3). Time je 5.4.7.2 dokazano.

5.4.7.3. Lema. Ako je $k\in K$ i $(\varepsilon, k)\neq 0$, tada je $K=K_0(k)$.

Jasno je da je $K\supset K_0(k)$; zato je $F\equiv G(K_0(k), K)$ određena podgrupa F od $G\equiv G(K_0, K)$; kako je G ciklična grupa od n članova, ciklična je i podgrupa F i ima $m=\frac{n}{d}$ članova, gdje je d indeks podgrupe F. Ujedno je g^d generator podgrupe F (jer je g generiralo G); zato je $g^dk=k$ (jer $k\in K_0(k)$). Imamo dalje:

$$(\varepsilon, k)\equiv\sum_{\nu=0}^{n-1}\varepsilon^{\nu}g^{\nu}k=\sum_{r=0}^{m-1}\sum_{s=0}^{d-1}\varepsilon^{rd+s}g^{rd+s}k=$$

$$=\sum_{s=0}^{d-1}\varepsilon^s g^s k\sum_{r=0}^{m-1}\varepsilon^{rd}.$$

Međutim, posljednja suma je za $d \neq n$ jednaka $\frac{1-\varepsilon^n}{1-\varepsilon^d}=0$ (jer je $\varepsilon^n=1$); zbog $(\varepsilon, k) \neq 0$ ne može dakle biti $d \neq n$ nego $d=n$, tj. $m=\frac{n}{d}=1$ što znači da je $F=\{1\}$, tj. $K_0(k)=K$, što se i trebalo dokazati.

5.4.7.4. Lema. Ako je $k \in K$, $(\varepsilon, k) \neq 0$, tada element $b=(\varepsilon, k)$ zadovoljava $K=K_0(b)$, $b^n \in K_0$, binom x^n-b^n je nesvodljiv nad K_0 a pripadno korijensko tijelo je upravo K.

Neka opet g označuje izvodnicu grupe $G(K_0, K)$; zbog $\varepsilon \in K_0$, bit će $g\varepsilon^r=\varepsilon^r$ za svaki cio broj r; zato je za svaki cio broj t:

$$g(\varepsilon^t, k)=g\sum_{\nu=0}^{n-1}\varepsilon^{\nu t}g^\nu k=\sum_{\nu=0}^{n-1}\varepsilon^{\nu t}g^{\nu+1}k=(\text{zbog } g^n=e,\ \varepsilon^n=1)$$

$$=\varepsilon^{-t}(\varepsilon^t; k), \text{ tj. } g(\varepsilon^t, k)=\varepsilon^{-t}(\varepsilon^t, k). \tag{1}$$

Posebno je za $t=1$ $g(\varepsilon, k)=\varepsilon^{-1}(\varepsilon, k)$ odakle potencirajući na t:

$$g(\varepsilon, k)^t=[g(\varepsilon, k]^t=\varepsilon^{-t}(\varepsilon, k)^t. \tag{2}$$

Dijeleći (1) sa (2) i stavljajući

$$\frac{(\varepsilon^t, k)}{(\varepsilon, k)^t}=c_t \tag{3}$$

izlazi $gc_t=c_t$ a odatle dalje $g^\nu c_t=c_t$ $(\nu=0, 1, \ldots, n)$ tj. c_t je invarijantno prema svakom članu grupe $G(K_0; K)$; to znači da je $c_t \in K_0$ pa zato

$$(\varepsilon^t, k) \in K_0(b) \tag{3'}$$

za svaki cijeli broj t; pri tom je $b=(\varepsilon, k)$.

Dokažimo sada da je $K=K_0(b)$. Promatrajmo izraz

$$I=\sum_{t=0}^{n-1}(\varepsilon^t, k)=\sum_{t=0}^{n-1}\sum_{\nu=0}^{n-1}\varepsilon^{\nu t}g^\nu k=\sum_{\nu=0}^{n-1}g^\nu k\sum_{t=0}^{n-1}\varepsilon^{\nu t}.$$

Posljednja suma pri $\nu \neq 0$ daje $\frac{\zeta^{\nu n}-1}{\zeta^\nu-1}=0$; zato izraz I postaje $I=nk$, tj.

$$\sum_{t=0}^{n-1}(\varepsilon^t, k)=nk. \tag{4}$$

No, prema $(3)_1$ svi sumandi u $(4)_1$ leže u $K_0(b)$; zato također $nk \in K_0(b)$, dakle i $k \in K_0(b)$, dakle $K_0(k) \subset K_0(b)$, tj. $K \subset K_0(b)$. Ta relacija zajedno sa $b \in K$ i $K_0(b) \subset K$ daje traženu jednakost $K=K_0(b)$.

Iz jednadžbe (2) za $t=n$ izlazi $gb^n=b^n$, a odatle ponovnim djelovanjem sa g zaključujemo da svaki član grupe G ostavlja na miru b^n; zato je $b^n \in K$. Prema tome je $x^n-b^n \in K_0[x]$; kako je b nulište od $p(x) \equiv x^n-b^n$ i kako je $K=K_0(b)$, $[K:K_0]=n=\operatorname{st} p$, znači da je $p(x)$ ireducibilan član prstena $K_0[x]$. Time je 5.4.7.4 dakle i 5.4.7 dokazano.

5.4.8. Teorem. *Ako je K radikalsko raširenje tijela K_0, tada postoji neko normalno radikalsko raširenje nK_0 od K_0 za koje je $K \subset nK_0$.*

Dokaz. Promatrajmo niz

(1) $$K_0 \subset K_1 \subset \cdots K_{m-1} \subset K_m \equiv K$$

sa svojstvom da pri $0<\mu \leq m$ tijelo K_μ bude prosto radikalsko raširenje od $K_{\mu-1}$ (isp. 5.1.3). Teorem ćemo dokazati indukcijom po m. Ako je $m=1$, dovoljno je staviti $nK=K$. Pretpostavimo da je teorem 5.4.6 ispravan za svako K kojemu niz (1) ima r članova, tj. $m=r-1$; dokažimo da je iskaz 5.4.6 ispravan i za slučaj kada u (1) stoji $m=r$. Naime, po pretpostavci

(1) $$K = K_{r-1}(\varepsilon_n, x_1)$$

gdje je ε_n neki n-ti primitivni korijen jedinice, a x_1 je nulište od $x^n - c$ pri $c \in K_{r-1}$; n je neki prirodan broj; po indukcionoj pretpostavci postoji normalno radikalsko raširenje K_0' od K_0 sa svojstvom $K_{r-1} \subset K_0'$. Posmatrajmo minimalni polinom $p(x)$ od c u odnosu na K_0; neka je $p(x)=(x-c_1)(x-c_2)\cdots(x-c_s)$, $c=c_1$. Neka je $x_\sigma{}^n = c_\sigma$ pri $\sigma=1, 2, \ldots, s$. Tvrdimo da tijelo

(2) $$K_0'(\varepsilon_n, x_1, \ldots, x_s)$$

predstavlja traženo tijelo nK_0 iz teorema 5.4.6. Kako je (2) radikalsko raširenje od K_0' s nizom prostih radikalskih raširenja

$$K_0' \subset K_0'(\varepsilon_n, x_1) \subset K_0'(\varepsilon_n, x_1, x_2) \subset \cdots \subset K_0'(\varepsilon_n, x_1, x_2, \ldots, x_s)$$

a kako je K_0' radikalsko raširenje od K_0, znači da je tijelo (2) radikalsko raširenje od K_0; naravno, zbog (1) vrijedi $(2) \supset K$.

U drugu ruku, promatrajmo $q(x) \equiv p(x^n) \in K_0[x]$; spektar σ_q polinoma $q(x)$ obuhvata $\{x_1, x_2, \ldots, x_s\}$; ostala nulišta od $q(x)$ oblika su $\varepsilon_n{}^\nu x_\sigma$ i dakle leže u tijelu (2); drugim riječima spektar σ_q leži u (2) pa zato tijelo (2) obuhvata korijensko tijelo Q polinoma $q(x)$ nad tijelom K_0'; tj. $(2) \supset Q$. No, iz $K_0' \subset Q$, $\{\varepsilon_n, x_1, \ldots, x_s\} \subset Q$ izlazi $K_0'(\varepsilon_n, x_1, \ldots, x_s) \subset Q$, tj. $(2) \subset Q$. Ova relacija s prethodnom daje jednakost $(2)=Q$. Prema tome, tijelo (2) je korijensko tijelo nad K_0' polinoma $q(x) \in K_0[x]$; kako je K_0' normalno raširenje od K_0, to po teoremu 5.1.4.7 zaključujemo da je zaista i tijelo (2) normalno raširenje tijela K_0. Time je teorem 5.4.8 dokazan.

5.5. Galoisova grupa polinoma kao permutaciona grupa.

Neka je $p(x) \in K_0[x]$ polinom kojemu su sva nulišta prosta (polinom $p(x)$ ne mora biti ireducibilan nad K_0); neka su

(1) $$x_1, x_2, \ldots, x_n$$

sva različita nulišta od $p(x)$; tada svaki član g Galoisove grupe G_p polinoma $p(x)$ prevodi niz (1) u određenu permutaciju $x_{g_1}, x_{g_2}, \ldots, x_{g_n}$ toga niza. Slaganju automorfizama u G_p odgovara slaganje odgovarajućih permutacija (1), tj. odgovara slaganje u simetričnoj grupi S_n svih permutacija množine (1). Prema tome, G_p je izomorfno nekoj podgrupi od S_n pa zato kardinalni broj kG od G je djelilac kardinalnog broja $n!$ grupe S_n.

5.5.1. Definicija tranzitivnosti. Grupa H permutacija množine M je *tranzitivna*, ako svakoj uređenoj dvojki x, y članova iz M odgovara neko $h \in H$ sa svojstvom $hx = y$.

5.5.2. Teorem. *Galoisova grupa G_p polinoma $p(x)$ s* ***nejednakim** nulištima*[1] *izomorfna je s nekom podgrupom G_p' simetrične grupe S_n; pri tom je n stepen polinoma $p(x)$. Podgrupa G_p' je tranzitivna onda i samo onda, ako je polinom $p(x)$ nesvodljiv.*

Ako je $p(x) \in K_0[x]$ ireducibilno, tada je tranzitivnost grupe G_p' dokazana u § 5.2.5. Dokažimo da vrijedi obrat. Neka je x_1 nulište od $p(x)$ a $m(x)$ minimalni polinom od x_1; dakle je $m(x_1) = 0$. Neka je x_k proizvoljno nulište od $p(x)$; tada, po pretpostavci, postoji neki automorfizam $a \in G_p$ za koji je $ax_k = x_1$; ujedno je

$$0 = a\,0 = am(x_1) = m(a x_1) = m\,x_k, \quad \text{tj.} \quad m(x_k) = 0;$$

dakle x_1, x_k zadovoljavaju isti minimalni polinom $m(x)$; kako je x_k bilo koje nulište od $p(x)$, i ima samo jedan par nerealnih nulišta (Sturm, 29 § 5.4); kako su nulišta od $p(x)$ prosta, znači zaista da je $p(x) : m(x)$ konstanta, odnosno $p(x)$ je ireducibilno.

⟶ 5.5.3. Galoisova grupa može biti izomorfna sa S_n.

Teorem. ***Ako je realni polinom $a(x) \in R[x]$ ireducibilan i prosta stepena p te ima upravo 2 prosta nerealna nulišta, tada je Galoisova grupa polinoma $a(x)$ izomorfna sa simetričnom grupom S_p brojeva 1, 2, ..., p pa jednadžba $a(x) = 0$ nije rješiva radikalima za $p \geq 5$.***

Dokaz. Neka je $x_1, x_2, \ldots, x_p$ spektar polinoma $a(x)$, i neka su x_1, x_2 nerealni; tada su x_1, x_2 međusobno konjugirani: $\overline{x_1} = x_2$. Konjugiranje $x \to \overline{x}$ u tijelu $K = R(x_1, x_2, \ldots, x_p)$ je određen član Galoisove grupe $G = G(R, K)$; tome automorfizmu odgovara transpozicija $(x_1\ x_2)$ u spektru σ_a, jer svaki preostali član ξ iz σ_a prelazi u sama sebe $(\overline{\xi} = \xi)$. Na taj način, G_a' je grupa permutacija množine σ_a od p članova; grupa G_a' sadrži transpoziciju $(x_1\ x_2)$, i tranzitivna je (t. 5.5.2); zato je $G = \sigma_a!$, tj. G_a' obuhvata svih $p!$ permutacija množine σ_a (isp. t. 5.5.4). Kako je grupa S_n nerješiva za $n > 4$, znači to prema osnovnom teoremu 5.4.2 da je jednadžba $a(x) = 0$ nerješiva radikalima čim je $p \geq 5$. Tako npr. ako je q prost cio broj, tada je polinom $a\,x \equiv x^5 + q\,x + q$ ireducibilan nad Q (Eisensteinov kriterij, t. 3.14.12) i pripadna Galoisova grupa je S_5, dakle je nerješiva. Ako je $b(x) \in Q[x]$ proizvoljno, tada je $a(x)\,b(x) \in Q[x]$; jednadžba $a(x)\,b(x) = 0$ nije rješiva radikalima jer $a(x) = 0$ nije rješivo radikalima.

5.5.4. Teorem o simetričnoj grupi S_p. ***Ako je p prost broj, a G tranzitivna podgrupa od S_p sa svojstvom da za bar dva različna broja x, y iz 1, 2. ..., p postoji transpozicija $(x\ y) \in G$, tada je $G = S_p$.***

---

[1] Prema tome, riječ je o separabilnu *polinomu* $p(x)$.

Dokažimo najprije ovo:

5.5.4.1. Lema. *Neka je n prirodan broj, G tranzitivna podgrupa od S_n sa svojstvom da postoji bar jedna transpozicija $(c\ x)\in G$; neka je C skup sastavljen od c i od svih x za koje je $(c\ x)\in G$, dakle*

$$C=\{c,\ x;\ x\in\{1,\ 2,\ \dots,\ n\},\ (c\ x)\in G\};$$

tada kardinalni broj $k=k\,C$ od C je divizor od n.

Stvarno, neka je

(1) $\quad n=kq+r,\quad q\in N,\quad 0\le r\le k-1;\quad$ dakle je $kq\le n<k\,(q+1)$.

Tvrdimo da je $r=0$; broj q je prirodan.

Pretpostavimo da je $r>0$. Tada postoji $x_1\in[1\,..\,n]\setminus C$, a zbog tranzitivnosti grupe G postoji permutacija $t_1\in G$ za koju je $t_1\,c=x_1$; lako se vidi da su skupovi C, $t_1\,C$ disjunktivni. Kako svaki od ta dva skupa ima po k članova, postojalo bi $x_2\in[1\,..\,n]\setminus(C\cup t_1\,C)$; neka je t_2 permutacija od G za koju je $t_2\,x_2=x_2$; lako se vidi da su skupovi C, $t_1\,C$, $t_2\,C$, disjunktivni; induktivno bismo tako došli do nejednakih brojeva $x_1,\ x_2,\ \dots,\ x_{q-1}$ iz $[1,\,..,\,n]$ i permutacijâ $t_1,\ \dots,\ t_{q-1}$ za koje je $t_{i-1}\,c=x_i$ te za koje su skupovi C, $t_1\,C$, $t_2\,C,\ \dots,\ t_{q-1}\,C$ dva po dva bez zajedničkog člana. Zato bi postojalo

$$x_q\in[1\,,\,..\,,n]\setminus(C\cup t_1\,C\cup\cdots\cup t_{q-1}\,C)$$

kao i permutacija $t_q\in G$ za koju je $t_q\,c=x_q$; tako bismo dobili disjunktne skupove

(2) $$C,\ t_1\,C,\ t_2\,C,\ \dots,\ t_q\,C$$

od kojih svaki ima po k članova; dakle bi bilo $n\ge k\,(q+1)$, protivno s relacijom (1). Tim protivurječjem dokazana je lema.

Još nam preostaje dokazati da su skupovi (2) disjunktni (mimoležni).

Stavimo $t_0=(1)$ (identitet) i pretpostavimo da je

$$t_i\,C\cap t_j\,C\ne\varnothing \qquad (\text{pri nekom } 0\le i<j\le q).$$

Tada postoji

(3) $$z'\in C\cap t_i^{-1}\cdot t_j\,C.$$

To je nemoguće. Naime, ako za $z\in C$ stavimo $z'=t_i^{-1}\cdot t_j\,z$, tada, zbog (4) $z=c\vee(c\,z)\in G$, vrijedi (5) $z'=c'\vee(c'\,z')\in G$. Osim toga (6) $c'\notin C$, jer $t_i^{-1}\cdot t_j\,c\in C$ povlači $t_j\,c\in t_i\,C$, protivno pretpostavki da $t_j\,c\notin t_i\,C$ $(i=0,\ 1,\ \dots,\ j-1)$.

Ako, dakle, vrijedi (3), tada je zbog (6) sigurno $z'\ne c'$, pa prema (4) i (5) mora biti:

$$(c\ c')=(c'\ z')\ (c\ z')\ (c'\ z')\in G\quad(\text{ako je } z'\ne c)$$

odnosno

$$(c\ c')=(z'\ c')=(c'\ z')\in G\quad(\text{ako je } z'=c),$$

dakle u oba slučaja

$$(c\ c')\in G,\ \text{tj. } c'\in C,$$

što se protivi uslovu (6).

Dokažimo sada i sam teorem; sada je n neki prost broj p, pa je dakle također $k=p$, tj. $q=1$, tj. $\{1, 2, \ldots, n\}=C$. No, za bilo koja dva različna člana x, y iz C imamo transpozicije $(c\ x)$, $(c\ y)$ iz G; kako je $(c\ x)\ (c\ y)\ (c\ x)=$ $=(x\ y)$, znači da je također $(x\ y)\in G$. Drugim riječima, G sadrži *svaku transpoziciju* množine $\{1, \ldots, n\}$; zato G sadrži i *svaku permutaciju* toga skupa jer se svaka permutacija od $\{1, \ldots, n\}$ može prikazati kao proizvod od konačno mnogo transpozicija (v. 3, § 8.6.3). Time je teorem 5.5.4 dokazan.

⟶ **5.5.5. Teorem. Nerješivost simetrične grupe S_n pri $n>4$. Za svaki prirodni broj $n>4$ grupa S_n je nerješiva** (isp. 17, § 19).

To izlazi iz činjenice da je pri $n>4$ alternirajuća grupa A_n svih parnih permutacija prosta (teorem 5.5.6) tako da S_n ima jedan jedini kompozicioni niz i to S_n, A_n, $\{e\}$.

Pripadne faktorske grupe su

$$S_n/A_n,\quad A_n/\{e\}$$

pa je posebno grupa $A_n/\{e\}$ izomorfna sa A_n pa (kao ni A_n) grupa $A_n/\{e\}$ nije komutativna; prema 17, § 19.3 znači to da grupa S_n nije rješiva.

Zato nam još preostaje da dokažemo

⟶ **5.5.6. Teorem** ***(prostost grupe A_n pri $n>4$). Ako je prirodni broj $n>4$, grupa A_n svih parnih permutacija množine $\{1, \ldots, n\}$ je prosta (E. Galois)*** (isp. 17, § 11.1.1).

I grupe A_2, A_3 su proste; grupa A_4 nije prosta.

Dokaz. Neka je I invarijantna podgrupa od A_n te $I\neq\{e\}$; dokažimo da je $I=A_n$ pri $n>4$.

Prvi slučaj: postoji 3-člani ciklus $(abc)\in I$.

Dokažimo da tada *svaki* 3-člani ciklus (xyz) pripada grupi I. Naime, permutacije $f=\begin{pmatrix} a\,b\,c\,d\,e\ldots \\ x\,y\,z\,t\,u\ldots \end{pmatrix}$, $g=\begin{pmatrix} a\,b\,c\,d\,e\ldots \\ x\,y\,z\,u\,t\ldots \end{pmatrix}=f(ut)$ jesu dva člana iz S_n koji su različnog pariteta; dakle je jedna od permutacija f, g u A_n, npr. $f\in A_n$. Kako je

$$f(abc)f^{-1}=(xyz),\quad \text{zaista je}\quad (xyz)\in I.$$

No, svaki član $p\in A_n$ kao parna permutacija može se prikazati kao proizvod parna broja dvočlanih ciklusa; a kako je $(kl)\,(ij)=(ikl)\,(ijl)$ ako je $\{i, j\}\cap\{k, l\}\neq\emptyset$ $(ik)\,(ij)=(ijk)$ zaključujemo da je p proizvod i samih 3-članih ciklusa pa kao i ti ciklusi leži u I.

Dakle je zaista $A_n\subset I$.

No, uvijek postoji 3-člani ciklus $(abc)\in I$. Neka je naime $p\in I$; prikažemo li permutaciju p kao proizvod ciklusa, tada imamo ove i samo ove tri mogućnosti (0), (00), (000):

(0) Bar jedan ciklus $f=(abcd\cdots)$ od 4 ili više članova pojavljuje se kao faktor od p; ciklus $g=(bcd)$ leži u A_n; zato konjugat $gfg^{-1}=h$ leži u I; no lako se provjeri da je $f^{-1}h=(abd)$ željeni 3-člani ciklus iz I.

(00) Faktori-ciklusi od p jesu što dvočlani što točlani, i pojavljuje se bar jedan dvočlan ciklus (ab); kako je p parna permutacija, razabiramo da p ima paran broj 2-članih ciklusa; dakle je p oblika

$$p=\cdots(cd)(ab).$$

Konjugiramo li p sa $h=(abc)$, dobije se član $q=hph^{-1}=\cdots(ad)(bc)$. Vidi se da je $s=p^{-1}q\equiv(ac)(bd)\in I$.

Neka je $x\in\{1,\ldots,n\}\setminus\{a,b,c,d\}$; tada je $(acx)\in A_n$ pa je

$$t\equiv(acx)\,s\,(acx)^{-1}=(cx)(bd)\in I.$$

Kako je $(axc)=ts\in I$, znači da zaista I sadrži 3-člani ciklus (axc).

(000) Svi ciklusi od p su 3-člani i ima ih bar 2:

$$p=\cdots(a'b'c')(abc).$$

Tada je

$$q\equiv(ca'b')\,p\,(ca'b')^{-1}=\cdots(b'cc')(aba')\in I.$$

Iz p^{-1}, $q\in I$ izlazi $p^{-1}q\in I$ što sa $p^{-1}q=(bc'a'cb')$ daje $(bc'a'cb')\in I$, tj. nalazimo se u slučaju (0).

Prostota grupa A_2, A_3 i neprostota od A_4 mogu se dokazati kao vježbe.

Time je 5.5.6 potpuno dokazano.

5.6. Galoisova teorija i kvadratne jednadžbe.

Riješimo jednadžbu

(1) $$x^2+bx+c=0.$$

Neka su joj x_1, x_2 traženi korijeni.

Galoisova grupa je izomorfna sa S_2 i sastoji se od identične transformacije kao i od permutacije $g:x_1\leftrightarrow x_2$. Kako je primitivni korijen jedinice reda 2 jednak -1, to Lagrangeove rezolvente prema 5.4.7.1 pri $d=0$, 1 glase

$$\left((-1)^0,\ x_1\right)=x_1+x_2=-b$$

$$\left((-1)^1,\ x_1\right)=x_1-x_2.$$

Stavimo $L=(-1,\ x_1)=x_1-x_2$. Tada se vidi da je

(2) $$x_{1,2}=\frac{-b\pm L}{2}$$

te $$L^2=x_1^2+x_2^2-2x_1x_2=b^2-4c,$$

tj.

(3) $$L=(b^2-4c)^{1/2}.$$

Stavimo li (3) u (2), dobije se poznata formula za korijene jednadžbe (1). Adjunkcijom veličine (3) tijelu u kojemu leže koeficijenti b, c jednadžbe (1) dobije se korijensko tijelo K polinoma (1).

5.7. Galoisova teorija i kubna jednadžba

(1) $$x^3+px+q=0.$$

Polazimo od nekog tijela K_0 brojeva u kojem su i koeficijenti p, q. Neka je x_1, x_2, x_3 spektar trinoma (1), tako da je

$$K=K_0(x_1,\ x_2,\ x_3) \text{ korijensko tijelo polinoma (1).}$$

Prema teoremu 5.5.3 Galoisova grupa trinoma, odnosno jednadžbe (1) je S_3 u kojoj je

$$S_3 \underset{\neq}{\supset} A_3 \underset{\neq}{\supset} \{e\}$$

jedini kompozicioni niz. Tome nizu prema 5.3.1. odgovaraju tijela

$$K_0 \underset{\neq}{\subset} M \underset{\neq}{\subset} K, \quad \text{takva da je} \quad G(M,\ K)=A_3.$$

No, grupa A_3 je ciklična; generator joj je ciklus $g=(x_1 x_2 x_3)$; kako je $\varepsilon=\frac{1}{2}\left(-1+\sqrt{-3}\right)$ primitivni korijen jedinice reda 3, Lagrangeove rezolvente prema 5.4.7.1. glase:

(2) $$(\varepsilon^0,\ x_1)=x_1+gx_1+g^2x_1=x_1+x_2+x_3=0$$

$$(\varepsilon,\ x_1)=x_1+\varepsilon gx_1+\varepsilon^2 g^2 x_1=x_1+\varepsilon x_2+\varepsilon^2 x_3=x_1+\varepsilon x_2+\bar{\varepsilon} x_3$$

$$(\varepsilon^2,\ x_1)=x_1+\varepsilon^2 gx_1+\varepsilon^4 g^2 x_1=x_1+\varepsilon^2 x_2+\varepsilon x_3=x_1+\bar{\varepsilon} x_2+\varepsilon x_3.$$

Kako je M skup svih fiksnih elemenata pri automorfizmima koji odgovaraju grupi A_3, razabiremo da x_1 non$\in M$ jer $gx_1=x_2 \neq x_1$; mi naime razmatramo opći slučaj trinoma (1). Dakle je $x_1 \in K \setminus M$ pa je zato

$$K=M(x_1);$$

naime, između M i K nema nikakva tijela.

No, znajući da je

$$x_1+x_2+x_3=0$$

$$x_1 x_2+x_1 x_3+x_2 x_3=p$$

$$x_1 x_2 x_3=-q,$$

i stavljajući

(3) $$(x_1-x_2)(x_1-x_3)(x_2-x_3)=V,$$

vidi se da je

$$V = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 - x_1 x_2^2 - x_2 x_3^2 - x_3 x_1^2,$$

(4) $$V^2 = -4p^3 - 27q^2$$

(5) $$(\varepsilon, x_1)^3 = -\frac{27}{2} q + \frac{3}{2} \sqrt{-3}\, V$$

(6) $$(\varepsilon^2, x_1)^3 = -\frac{27}{2} q - \frac{3}{2} \sqrt{-3}\, V.$$

Zbrojimo li jednadžbe (2), dobije se

$$(\varepsilon^0, x_1) + (\varepsilon, x_1) + (\varepsilon^2, x_1) = 3x_1,$$

što s obzirom na relacije (4), (5), (6) daje upravo Cardanovu formulu

(7) $$x_1 = \left(-\frac{q}{2} + \sqrt{\frac{-D}{108}}\right)^{1/3} + \left(-\frac{q}{2} - \sqrt{\frac{-D}{108}}\right)^{1/3}, \quad \text{gdje je}$$

$$D = V^2 = -4p^3 - 27q^2 \text{ (isp. 5, § 6.3).}$$

5.8. Na sličan bi se način moglo doći do rješenja jednadžbe 4. stepena.

5.9. Primjedba. Opisani način rješavanja jednadžbe stepena 2, 3, 4 dugujemo Lagrangeu (isp. str. 148); taj je način imao znatan uticaj na Galoisovu stvaralačku misao.

5.10. Zadaci o Galoisovoj teoriji.

1. Neka su tijela K_0, K_1, K_2 takva da je $K_0 \subset K_1 \subset K_2$; ako je K_2 normalno nad K_0, tada je K_2 normalno i nad K_1.

2. *Galoisova rezolventa* zadana polinoma $a(x) \in K_0[x]$ je svaki nad $K_0[x]$ ireducibilni polinom kojemu je korijensko tijelo ujedno korijensko tijelo jednačine $f(x) = 0$.
   Dokazati: ako je $a(x)$ svoja vlastita Galoisova rezolventa, tada je $a(x)$ normalno; i obratno.

3. Ako su $$f(x) = (x - x_1)(x - x_2) \cdots (x - x_m)$$ $$g(x) = (x - y_1)(x - y_2) \cdots (x - y_n)$$
   dva člana iz $K[x]$, tada je
   $$\prod_{i=1}^{m} \prod_{j=1}^{n} (x_i - y_j) \in K.$$

4. Neka je $x^3 + px + q$ ireducibilan trinom nad $K_0 = Q(p, q)$; dokaži da je Galoisova grupa toga trinoma ili A_3 ili S_3, već prema tome da li je diskriminanta D oblika k^2 ili $\mp k^2$, pri čemu je $k \in K_0$.

5. Izraz $x^3 - 2$ nije normalan nad Q ali jest normalan nad $Q(\sqrt{-3})$. Kako glasi korijensko tijelo od $x^3 - 2$ u odnosu na Q?

6. Dokaži da je Galoisova grupa polinoma $x^4+x^3+x^2+x+1$ nad tijelom Q racionalnih brojeva izomorfna s grupom permutacija koju rađaju

$$(1),\quad (1\,2\,4\,3),\quad (1\,4)(2\,3),\quad (1\,3\,4\,2).$$

7. Nad tijelom Q odredi Galoisovu grupu polinoma:
   1) $1+x+x^2+x^3+x^4+x^5$; 2) $x^5-10x+2$.

8. Služeći se Eisensteinovim kriterijem (§ 3.14.12) navesti za svaki prost broj p polinom kojemu je Galoisova grupa u odnosu na Q upravo S_p.

9. Dokazati da je svaka konačna grupa G izomorfna s Galoisovom grupom nekog polinoma (koji naravno zavisi od G).

10. Neka je K_0 podtijelo tijela R realnih brojeva; neka je p prost broj; ako je $a \in K_0$, tada je dvočlan x^p-a ili nesvodljiv nad K_0 ili on ima nulište u K_0.

11. Neka je polinom $a(x) \equiv x^3+px+q$ nerastavljiv nad tijelom $K_0=Q(p,q)$; ako je x_1 nulište polinoma $a(x)$, D diskriminanta od $a(x)$, tada je $K_0(D^{1/2}, x_1)$ korijensko tijelo od $a(x)$; izraziti ostala nulišta od $a(x)$ pomoću x_1, $D^{1/2}$.

12. *Ciklične jednadžbe*. Ako je grupa jednadžbe $a(x)=0$ prema tijelu K_0 ciklična, kaže se da je jednadžba *ciklična prema* K_0. Dokaži:
    1) ako je K_0 neko tijelo brojeva te $a(x)$ polinom nad K_0 stepena 3 i s diskriminantom $D=k^2$ gdje je $k \in K_0$, tada je $a(x)$ ciklično;
    2) za svaki prost broj p polinom $1+x+x^2+\cdots+x^{p-1}$ je cikličan nad K_0.

6. LINEARNI PROSTORI. A-MODULI. LINEARNE ALGEBRE

6.0. *Linearne ili vektorske prostore* izučavali smo dosad u više navrata, pa smo upoznali kako su oni važna vrsta algebarskih struktura.

Oni su poseban slučaj tzv. A-modula. Pri tom vrijedi

6.0.1. A-moduli. Definicija. Neka je $(A, +, \cdot)$ zadan prsten; pod *lijevim* [*desnim*] *A-modulom* razumijevamo svaku *komutativnu grupu* $(M, +)$ (nazvana *modul*) koja dopušta operaciju

$a \in A,\ m \in M \rightarrow am \in M$ [odnosno $ma \in M$] sa svojstvima

$$\begin{array}{r|l} a(m+m')=am+am' & (m+m')\,a=ma'+m'\,a \\ (a+a')\,m=am+a'\,m & m\,(a+a')=ma+ma' \\ a\,(a'\,m)=(aa')\,m & (ma)\,a'=m\,(aa'). \end{array}$$

6.0.2. Odmah se vidi da u slučaju tijela K odgovarajući obostrani K-modul M znači vektorski prostor nad K ukoliko je $1\cdot m=m$ za svako $m \in M$.

6.0.3. Posebne vektorske prostore nazvali smo *linearnim algebrama*; definicije u vezi s linearnim algebrama navedene su u pogl. 26, § 7.9.

Važni primjeri linearnih algebri konačne dimenzije su: algrebra $(R, +, \cdot)$ realnih brojeva (dimenzija ili stupanj je $d=1$), realna algebra $R(i)$ kompleksnih brojeva $(d=2)$ te realna algebra Qu kvaterniona $(d=4)$; Qu se sastoji od svih izraza oblika $a_0 \cdot 1 + a_1 e_1 + a_2 e_2 + a_3 e_3$, pri čemu veličine $1, e_1, e_2, e_3$ zadovoljavaju tablicu množenja iz 23, § 8.7; koeficijenti a_0, a_1, a_2, a_3 prolaze nezavisno tijelom realnih brojeva R.

Sve su te tri algebre asocijativne, jedinične i s dijeljenjem. Zanimljivo je da drugih konačno-dimenzionalnih i asocijativnih jediničnih algebara s dijeljenjem nad R ni nema (Frobenius, 1879). To ćemo i dokazati (v. t. 6.2). Ta pravilnost vrijedi ne samo za realno tijelo R nego za svako tzv. *realno-zatvoreno tijelo.*

6.1. Definicija realno-zatvorena tijela. Tijelo K_r je realno-zatvoreno ako ima ova tri svojstva:

(0) *Tijelo je formalno-realno,* tj. član -1 iz K_r nije kvadrat niti je suma od dva ili više kvadrata članova iz K_r;

(00) Svaki polinom neparna stepena i s koeficijentima iz K_r ima bar jedno nulište u K_r;

(000) $K_r = K_r{}^2 \cup (-K_r{}^2)$, tj. svaki član tijela K_r je oblika x^2 ili $-x^2$ pri čemu je $x \in K_r$.

Tako npr. skup svih realnih algebarskih brojeva je realno-zatvoren i $\neq R$. Svako realno-zatvoreno tijelo K_r ima dosta svojstava od tijela R realnih brojeva, premda ne mora biti $K_r = R$.

Specijalno se za svako realno-zatvoreno tijelo K_r može promatrati tijelo $K_r(i)$, gdje je $i^2 = -1$ pa je sigurno $K_r \subsetneq K_r(i)$. *Tijelo* $K_r(i)$ je *algebarski-zatvoreno,* tj. svaki polinom $a(x) \in K_r[x]$ ima u $K_r(i)$ bar jedno nulište. Nad K_r se može promatrati i kvaternionska algebra

$$Qu(K_r) = \{a_0 \cdot 1 + a_1 e_1 + a_2 e_2 + a_3 e_3; \quad a_0, a_1, a_2, a_3 \in K_r;$$

pri tom vrijedi tablica 23, § 8.7}.

$\longrightarrow$ **6.2. Teorem (Frobenius, 1879).** ***Neka je K_r bilo koje realno-zatvoreno tijelo; tada svaka asocijativna diviziona jedinična algebra L konačne dimenzije nad K_r izomorfna je s K_r ili s $K_r(i)$, $(i^2 = -1)$ ili s kvaternionskom algebrom $Qu(K_r)$ nad K_r.***

Dokaz teorema 6.2 izlazi iz svojstava 6.2.1—6.2.8 algebre L.

Neka je e jedinica algebre L; neka je n dimenzija od L.

6.2.1. Algebra L obuhvata podalgebru $eK_r = \{ex; x \in K_r\}$ koja je izomorfna s tijelom K_r; preslikavanje $x \in K_r \to e \cdot x \in eK_r \subset L$ je izomorfija.

6.2.2. Zbog kraćeg izražavanja pretpostavit ćemo da je $eK_r = K_r$, tj. da tijelo K_r i algebra L imaju isti jedinični element $e = 1$.

Ako je $K_r = L$, teorem 6.2 je dokazan. Zato možemo pretpostaviti da je $K_r \subset L$ i da postoji neko

(1) $$l \in L \setminus K_r \qquad \text{(isp. 6.2.2).}$$

6.2.3. *Algebra L je kvadratna nad K_r*, tj. svaki član $l \in L$ zadovoljava jednadžbu oblika

(2) $$l^2 = xl + y,$$

odnosno

(3) $$\left(l - \frac{x}{2}\right)^2 = \frac{x^2}{4} + y, \quad \text{za neko} \quad x, y \in K_r.$$

Naime, ako je n dimenzija od L (dakle $n < \infty$), tada su elementi

$$l^0 = 1, \ l, \ l^2, \ldots, \ l^n$$

linearno zavisni nad K_r: postoji netrivijalan niz $a_0, a_1, \ldots, a_n$ članova iz K_r tako da polinom — skalarni umnožak

$$f(x) = \sum_{\nu=0}^{n} a_\nu x^\nu$$

ima stepen > 0 i da se poništava pri $x = l$, tj. $f(l) = 0$.

No, radi svojstava 6.1 (00) može se $f(x)$ prikazati kao umnožak od konačno mnogo polinoma stepena ≤ 2, i s koeficijentima u K_r: bar jedan od tih faktora $g(x)$ dopušta l kao svoje ništište jer je K_r bez djelitelja nule; ako je st $g = 2$, cilj je postignut; ako nije st $g = 2$ tada je $l \in K_r$ (isp. 6.2.2) pa (2) vrijedi npr. za $l = x$, $y = 0$.

Dakle zaista vrijedi (2); kako je $2 \neq 0$ (inače bi bilo $1^2 = -1$, u protivnosti sa 6.1 (0)) (v. 6.3.6) možemo promatrati $\frac{x}{2} \in K_r$ pa iz (2) neposredno izlazi (3).

6.2.4. Pri uslovu (1) ne može $(3)_2$ biti oblika k^2, pri $k \in K_r$.

Dakle prema 6.1 (000) postoji neko $k \in K_r$ sa svojstvom

$$\frac{x^2}{4} + y = -k^2.$$

Odatle i iz (2) izlazi

$$\left(l - \frac{x}{2}\right)^2 = -k^2,$$

i dalje:

$$\left(\frac{l - \frac{x}{2}}{k}\right)^2 = -1,$$

odnosno

(4) $$i^2 = -1 \quad \text{uz oznaku} \quad i = \frac{l - \frac{x}{2}}{k}.$$

Naravno, i non$\in K_r$ zbog (4) i zbog 6.1 (0); adjunkcijom člana i u K_r dobije se $K_r(i)$ pa je $K_r \subset K_r(i) \subset L$; $K_r(i)$ je podalgebra od L.

Ako je $K_r(i) = L$, teorem 6.2 je dokazan; zato nam preostaje još slučaj da postoji neko

$$m \in L \setminus K_r(i). \tag{4'}$$

6.2.5. *Antikomutator* $l_1 l_2 + l_2 l_1$ *svake dvojke* $l_1, l_2 \in L$ *izražava se linearno pomoću* $l_1, l_2, 1$ *s koeficijentima iz* K_r, tj. $l_1 l_2 + l_2 l_1 = h_1 l_1 + h_2 l_2 + h_3$ *pri* $h_1, h_2, h_3 \in K_r$; *posebno za prethodno promatrane članove* $i, m \in L$ *je*

$$im + mi = ai + bm + c \quad \text{za neke} \quad a, b, c \in K_r. \tag{5}$$

To izlazi iz formule

$$l_1 l_2 + l_2 l_1 = (l_1 + l_2)^2 - l_1^2 - l_2^2$$

zamjenjujući kvadrate izrazima (2).

6.2.6. Lema. *Iz* $i, m \in L$, $i^2 = -1$ *te*

$$m^2 = r\, m + s, \quad \text{pri} \quad r, s \in K_r \qquad \text{(isp. (2)) izlazi} \tag{6}$$

$$im + mi = ri + c \quad [\text{isto } r \text{ se javlja u (6) i (7)}]. \tag{7}$$

Stvarno, neka su $u, v \in K$ proizvoljni $\neq 0$; tada prema 6.2.3. vrijedi

$$(ui + vm)^2 = x'(ui + vm) + y' \quad \text{za neke} \quad x', y' \in K_r. \tag{8}$$

No, izraz (8), možemo direktno izračunati držeći na umu da je $i^2 = -1$:

$$(ui + vm)^2 = -u^2 + uv(im + mi) + v^2 m^2.$$

Ta jednadžba s obzirom na (8), (5) i (6) daje

$$x'(ui + vm) + y' = -u^2 + uv(ai + bm + c) + v^2(rm + s). \tag{9}$$

Kako su $1, i, m$ linearno nezavisni članovi od L jednadžba (9) pokazuje da su koeficijenti tih veličina na lijevoj i desnoj strani od (9) jednaki; posebno izjednačujući koeficijente od i, odnosno od m izlazi

$$x'u = uva; \qquad x'v = uvb + v^2 r.$$

Odatle uz uslov $u \neq 0 \neq v$ izlazi

$$x' = va, \qquad x' = ub + vr$$

odakle dalje izlazi

$$ub = v(a - r). \tag{10}$$

Posebni slučaj

$$u = 1 = v, \quad \text{odnosno} \quad u = 1,\ v = -1 \qquad \text{daje}$$

$$b = a - r, \quad \text{odnosno}$$

$$b = -a + r.$$

Zbrajanjem, odnosno oduzimanjem izlazi odatle $2b = 0$, odnosno $0 = 2a - 2r$, odatle (karakteristika tijela je $\neq 2$) $b = 0$, $a = r$; time prema (5) zaista stoji (7).

6.2.7. Potprostor $K_r\{1, i, m\}$ generiran skupom $\{1, i, m\}$ sadrži neki član j za koji je

(11) $$j^2=-1, \quad ij+ji=0.$$

Stvarno, opći član toga potprostora je

(12) $$n=k_1+k_2 i+k_3 m, \quad \text{pri čemu je} \quad k_1, k_2, k_3 \in K_r.$$

Dakle je

$$n^2=k_1^2-k_2^2+k_3^2 \underbrace{(rm+s)}_{m^2}+2k_1k_2i+2k_1k_3m+k_2k_3\underbrace{(im+mi)}_{ri+c},$$

(13) $$n^2=(k_1^2-k_2^2+k_3^2 s+k_2k_3c)+(k_3r+2k_1)(k_3m+k_2i).$$

Uz uslov

(14) $$k_3 r+2k_1=0$$

bit će

(15) $$n^2=k_1^2-k_2^2+k_3^2 s+k_3k_3 c \in K_r.$$

Tim dvjema relacijama može se udovoljiti za svako dano $k_3 \neq 0$; time je još parametar k_2 neodređen, pa možemo staviti još jedan zahtjev npr. da i, n antikomutiraju, tj. da bude

(16) $$in+ni=0.$$

S obzirom na (12) te $i^2=-1$ poprima (16) oblik

$$(-2k_2+k_3c)+(2k_1+k_3r)i=0,$$

odnosno zbog (14):

(17) $$-2k_2+k_3c=0.$$

Iz (14) i (17) određujemo za proizvoljno $k_3 \neq 0$ veličine $k_1, k_2 \in K_r$, a time prema (12) i $n \in L$ za koje će automatski vrijediti (15), (16).

No, zbog uslova $k_3 \neq 0$ razbiremo da je

(18) $$n \operatorname{non}\in K_r \quad (\text{premda je } n^2 \in K_r)$$

jer bismo iz $n \in K_r$ i jednakosti (12) zaključili da su 1, i, m linearno zavisni (a znamo da su oni linearno nezavisni).

Poslužimo se sada svojstvom 6.2 (000) tijela K_r; kako prema (15) vrijedi $n^2 \in K_r$ svojstvo 6.2 (000) iskazuje da je $n^2=t^2$ ili $n^2=-t^2$ za neko $t \in K_r$. Slučaj $n^2=t^2$ nije moguć jer bi odatle izlazilo $n=t$ ili $n=-t$, protivno sa (18). Dakle je $n^2=-t^2$ za neko $t \in K$.

Stavimo li dakle $j=t^{-1}n$, bit će zaista $j^2=-1$, $ij+ji=0$ što smo i tvrdili u 6.2.7.

6.2.8. *Stavimo* $k=ij$; *tada članovi*

(19) $1,\ i,\ j,\ k$ *čine bazu t algebre* L;

veličine $1,\ i,\ j,\ k$ *zadovoljavaju kvaternionsku tablicu množenja iz poglavlja* 23, § 8.7.[1]) *pa je* L *kvaternionska algebra nad* K_r.

Lako se provjeri da se veličine (19) množe prema pomenutoj tablici; tako npr. množeći (16) sa t^{-1} izlazi $ij+ji=0$, tj. $ij=-ji$. Zato je npr.

$$k^2=(ij)(ij)=(-ji)(ij)=-j(ii)j=-j\cdot -1\cdot j=j^2=-1.$$

Dokažimo da su veličine (19) linearno nezavisne.

Kako su $1,\ i,\ j$ međusobno linearno nezavisni, dovoljno je pokazati da se k ne može izraziti pomoću $1,\ i,\ j$. Pretpostavimo, naprotiv, da je

$$k=a+ib+jc \text{ za neke članove } a,\ b,\ c\in K_r.$$

Pomnožimo li tu jednadžbu sprijeda sa i izlazi (isp. 23, § 8.7)

$$-j=ia-b+kc, \text{ te dalje eliminacijom od } k:$$

$$-j=ia-b+(a+ib+jc)c$$

$$-j=-b+ac+i(a+bc)+jc^2. \tag{20}$$

Zbog linearne nezavisnosti članova $1,\ i,\ j$ izlazi iz (20) jednakost $-1=c^2$ što je zbog $c\in K_r$ u protivnosti sa svojstvom 6.1. (0) realno-zatvorena tijela K_r.

Još preostaje dokaz da je $K_r\{1,i,j,k\}=L$, tj. *da svakom članu* $x\in L$ *pripada neka uređena četvorka* $x_1,\ x_2,\ x_3,\ x_4\in K_r$ *sa svojstvom*

$$x=x_1+x_2i+x_3j+x_4k. \tag{21}$$

U tu svrhu za $x\in L$ primijenimo lemu 6.2.6. promatrajući umjesto dvojke (i,m) ove dvojke: (i,x), (j,x), (k,x), dakle

$$\begin{aligned} ix+xi&=r_1i+c_1\\ jx+xj&=r_2j+c_2\\ kx+xk&=r_3k+c_3\end{aligned} \tag{22}$$

pri tom je $\{r_1,r_2,r_3,c_1,c_2,c_3\}\subset K_r$. Zato je

$$k(ix+xi)j-j(jx+xj)+k(kx+xk)=k(r_1i+c_1)j-$$
$$-j(r_2j+c_2)-k(r_3k+c_3),$$

$$jxj+kxk+x-jxj+x-kxk=-r_1i-c_1+r_2-jc_2+r_3-kc_3$$

$$2x=(-r_1+r_2+r_3)1-c_1i-c_2j-c_3k.$$

To znači da vektori $1,i,j,k$ zaista razapinju $2x$, a time i samo x. Time je dokaz teorema 6.2. završen.

---

[1]) Dovoljno je pisati $e_1=i$, $e_2=j$, $e_3=k$.

6.3. Zadaci o linearnim algebrama.

0. Ako je M aditivna grupa, a A prsten endomorfizama od A, tada je M određen A-modul pri čemu je $am = a(m)$.

1. Neka je V skup svih radijus-vektora $\overrightarrow{OX}$, pri čemu X prolazi: 1) zadanom pravuljom, 2) zadanom ravninom, 3) prostorom. Je li V linearna algebra ako se vrši spoljno ili vektorsko množenje u V? Ako V jest linearna algebra, može li imati jedinicu? Da li je V asocijativna algebra?

2. Neka je n prirodni broj; čine li sve realne matrice x formata (n, n) linearnu algebru s dijeljenjem? A sve regularne x?

3. Dokazati da pridruživanje

$$r_0 + i\, r_1 \leftrightarrow \begin{bmatrix} r_0 & -r_1 \\ r_1 & r_0 \end{bmatrix} = r$$

predstavlja izomorfiju između tijela $(R(i), +, \cdot)$ kompleksnih brojeva i tijela R_2 realnih matrica r formata (2, 2) gornjeg oblika; specijalno je $r^* \leftrightarrow r_0 - i\, r_1$. Drugim riječima, sve matrice $r = \begin{bmatrix} r_0 - r_1 \\ r_1 \quad r_0 \end{bmatrix}$ nad tijelom R daju tijelo R_2 izomorfno sa $R(i)$ (isp. 10, § 4.7.8).

4. 1) Sve matrice $a = \begin{bmatrix} \bar{a}_0 - \bar{a}_1 \\ a_1 \quad a_0 \end{bmatrix}$ nad tijelom R_2 (zad. 3) čine tijelo R_4 izomorfno s tijelom kvaterniona nad R (s obzirom na zad. 3. znači to da je algebra kvaterniona R_4 nad R građena kao „algebra kompleksnih brojeva" nad tijelom $R(i)$).

   2) Stavimo $e_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $e_1 = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $e_3 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$; pridružimo matrici a izraz $a' = a_{00} \cdot e_0 + a_{10}\, e_1 + a_{01}\, e_2 + a_{11}\, e_3$ (pri tom za svaki kompleksni broj z pišemo $z = z_0 + i\, z_1$); to je pridruživanje obostrano jednoznačno, vrijedi $(a^*)' = a_{00}\, e_0 - a_{10}\, e_1 - a_{01}\, e_2 - a_{11}\, e_3$ pa je $R\{e_0, e_1, e_2, e_3\}$ upravo algebra kvaterniona, kojoj članovi e_0, e_1, e_2, e_3 čine bazu; provjeriti da ti članovi imaju tablicu množenja poput one u 23, § 8.7.

   3) Stavi li se $a\, a^\star \equiv N(a) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, tada je $N(a) = \sum_{m,n=0}^{1} a_{mn}{}^2 \geq 0$ realno te dakle $N(a) = 0 \Leftrightarrow a = 0$; $N(a\, b) = N(a)\, N(b)$;

   4) Ako su $a, b \in R_4$ pri čemu a nije nula-matrica, tada

$$a\, x = b \;\Rightarrow\; x = (a^\star a)^{-1}\, a^\star\, b.$$

5. *Cayleyevi brojevi ili oktave.*

   1) *Definicija oktava.* Oktave ili Cayleyevi brojevi jesu uređeni parovi (a, b) kvaterniona pri čemu se definira $(a, b) + (c, d) = (a + c, b + d)$,

$(a, b) \cdot r = (a\,r, b\,r)$ za svako $r \in R$; $(a, b) \cdot (c, d) = (a\,c - d^\star b, b\,c^\star + d\,a)$; skup oktava označit ćemo sa R_8.

2) R_8 je linearna algebra nad R koja nije asocijativna ali jest alternirajuća; posebno za matrice $0(2) \in R_4$; $1(2) \in R_4$, e_1, e_2, e_3 i stavljajući $a = (0(2), 1(2))$, $e_\nu' = (e_\nu, 0)$ $(\nu = 1, 2, 3)$ vrijedi

$$(a\,e_1')\,e_2' = (0(2), -e_3) \neq (0(2), e_3') = a\,(e_1'\,e_2') \quad \text{(isp. zad. 3.2).}$$

3) Definiramo li konjugiranje kao $(a, b)^\star = (a^\star, -b)$, tada je ono distributivno prema $+, \cdot$, tj. $(x+y)^\star = x^\star + y^\star$, $(x\,y)^\star = y^\star x^\star$; pri čemu se za $x \in R$ element $(r \cdot 1(2), 0(2)) \in R_8$ poistovećuje sa r.

4) Norma od $x \in R_8$ definira se kao $N(x) = x\,x^\star$; vrijedi

$$x\,x^\star = x^\star x \in R, \; N x = 0 \Leftrightarrow x = 0, \; N(x\,y) = N(x)\,N(y);$$

$$x = (x_1, x_2) \Rightarrow N(x) = N(x_1) + N(x_2);$$

5) Neka $a \in R_8$, $a \neq 0$, $b \in R_8$; tada $a\,x = b \Rightarrow x = \frac{1}{N(a)} a^\star b$;

$$y\,a = b \Rightarrow y = \frac{1}{N(a)} b\,a^\star.$$

6) Ako pođemo od tijela R_4 kvaterniona pa nad njim pokušamo graditi oktave kao „kompleksne brojeve", tj. kao matrice oblika $\begin{bmatrix} a & -b^\star \\ b & a^\star \end{bmatrix}$ (pri $a, b \in R_4$), tada se vidi da se dobije komutativna aditivna grupa ali da se ne dobije multiplikativni grupoid.

6. Karakteristika svakog formalno-realnog tijela K_r je 0 (isp. 6.1. (0)).

Literatura

Kuroš, [3].

7. BOOLEOVE ALGEBRE

Sredinom prošlog stoljeća naišao je G. Boole na zanimljive oblasti računanja a u vezi s logikom (isp. pogl. 1). Oblast se znatno razvila, pogotovo posljednjih tridesetak godina; razmatranja su vezana i s logičkom stranom teorije računskih strojeva.

Posebno, za svaku množinu M imamo pripadni partitivni skup PM koji je pogodna oblast za računanje pomoću spajanja ($\cup$), sječenja ($\cap$) i dopunjavanja ili komplementiranja.

7.1. Mreža ili mrežast skup. U pogl. 2, § 11. definirali smo mrežu kao svaki uređen skup $(M, \leq)$ sa svojstvom da iz $x \in M$ i $y \in M$ izlazi $\inf\{x, y\} \in M$ i $\sup\{x, y\} \in M$; to znači specijalno da postoji određen član $\inf\{x, y\}$ iz M kao i $\sup\{x, y\}$ iz M.

Tako npr. imamo mreže $(N, \leq)$, $(N, |)$, $(PM, \subset)$ za svaki skup M.

Odmah ćemo vidjeti kako se mreže kao uređeni skupovi mogu definirati također kao posebne komutativne polugrupe.

—→ **7.1.1. Teorem.** *Neka je $(M, \leq)$, mreža; pišemo li*

(1) $$\inf\{x, y\} = x \cdot y, \qquad \sup\{x, y\} = x \vee y,$$ (1^d)

tada su

(2) $$(M, \vee) \text{ i } (M, \cdot)$$

komutativne polugrupe sa ovim svojstvima „apsorpcije“:

(3) *ili* (A) $\quad x \vee (x\, y) = x, \quad$ (3^d) *ili* (A^d) $\quad x(x \vee y) = x.$

I obrnuto, ako su (2) *komutativne polugrupe sa svojstvom* (3), (3^d) *pa ako definiramo*

(4) $$x \vee y = x \Leftrightarrow x \geq y,$$

tada je $\geq$ *uređajna relacija pa je* $(M, \leq)$ *mreža sa svojstvom* (1) *i* (1^d).

Vrijedi ekvivalencija

(5) $$x \vee y = x \Leftrightarrow x y = y.$$

Zato je zgodno mrežasti skup označivati ne samo sa $(M, <)$ nego i sa $(M, \vee, \cdot)$ pa čak i sa $(M, \vee, \cdot, <)$.

Dokaz prvog dijela je neposredan jer se odgovarajuća svojstva lako provjere; tako npr. svojstvo (3) znači da je $\sup\{x, \inf\{x, y\}\} = x$, tj. da je $x \leq x$; $\inf\{x, y\} \leq x$ i da iz $t \leq \{x, y\}$ izlazi $t \leqslant \inf\{x, y\}$. Međutim, sve to izlazi neposredno iz definicija člana $\inf\{x, y\}$.

Dokaz drugog dijela teorema, kojim se M kao polugrupa pretvara u mrežu je dulji i sastoji se od niza zaključaka 7.1.1.0—7.1.1.4.

7.1.1.0. Dokažimo (5), i to najprije $(5)_1 \Rightarrow (5)_2$. Zaista, u mreži M $x \vee y = x$ povlači:

$$x y = (\text{po } (5)_1) = (x \vee y)\, y = (\text{po } (3^d)) = y.$$

Dualno se dokazuje $(5)_2 \Rightarrow (5)_1$.

Dokažimo najprije ovo zanimljivo

7.1.1.1. Svojstvo idempotencije: $x x = x$, $x \vee x$ *za svako* $x \in M$.

Naime $x x = (\text{po (3) za } y = x) = x\,(x \vee (x\, x)) = (\text{po } (3^d)) = x$. Dualno:

$$x \vee x = (\text{po } 3^d \text{ za } y = x) = x \vee (x \cdot (x \vee x)) = (\text{po } (3)) = x.$$

7.1.1.2. Refleksivnost. $x \geqq x$.

Naime $x \geq x \Leftrightarrow x \vee x = x \Leftrightarrow$ (prema § 7.1.1.1) $x = x$.

7.1.1.3. Antisimetrija. $x \geq y \wedge y \geq x \Rightarrow x = y$.

Dokaz. Prema pretpostavci je $x \geq y$, tj. $x \vee y = x$ kao i $y \geq x$, tj. $y \vee x = y$.

Dakle: $x = x \vee y = (\text{komutativnost!}) = y \vee x = y$, tj. $x = y$.

7.1.1.4. Tranzitivnost. $x \leq y \leq z \Rightarrow x \leq z$.

Dokaz. $x \vee z = $ (zbog $y \vee z = z$) $= x \vee (y \vee z) = $ (asoc.) $= (x \vee y) \vee z = $ (zbog $x \vee y = y$) $= y \vee z = z$, dakle $x \vee z = z$, tj. $z \geq x$.

Svojstva 7.1.1.2—4 iskazuju da je relacija $\geq$ uređajna u M.

Dokažimo (1) i (1^d).

Najprije $x \cdot y$ je minoranta od $\{x, y\}$; naime $x \cdot y \leq x$, jer $x \vee (xy) = x$ po (3); isto tako $y \vee (xy) = y \vee (yx) = $ (po (3)) $= y$, tj. $xy \leq y$.

Dokažimo da je xy najveća minoranta od x, y, tj. da

$$z \leq x \wedge z \leq y \Rightarrow z \leq x \cdot y.$$

Imamo redom:

$$z \leq x \Leftrightarrow z \vee x = x \Leftrightarrow zx = z$$

$$z \leq y \Leftrightarrow z \vee y = y \Leftrightarrow zy = z.$$

Odatle

$$(zx)(zy) = zz$$

$$(xz)(zy) = z$$

$$x(zz)y = z$$

$$xzy = z$$

$$(xy)z = z \Leftrightarrow (xy) \vee z = xy \Rightarrow z \leq xy.$$

Dualno se dokazuje relacija (1^d).

Time je teorem 7.1.1 dokazan.

7.1.2. *Najmanji član O i najveći član I mreže* $(M, <)$. To su članovi za koje je $O \leq M \leq I$. Mreža može imati O ali ne I ili I ali ne O ili oboje ili nijedno.

7.1.2.1. Za svaki član a mreže sa O vrijedi $aO = O$; za svaki član a mreže M s I vrijedi $aI = a$.

7.1.3. σ-mreža. Potpuna mreža. Definicija. Uređen skup $(M, \leq)$ zove se σ-mreža ako za svaki *prebrojiv*[1] dio X iz M postoje određeni članovi $\inf X \in M$ i $\sup X \in M$. Uređen skup $(M, \leq)$ je potpuna mreža ako iz $X \subset M$ izlazi $\inf X \in M$, $\sup X \in M$; posebno, to znači da tada postoji $\inf M \overset{\text{def}}{=} O = $ najmanji član u M, tj. $O \in M$, kao i $\sup M \overset{\text{def}}{=} I = $ najveći član u M, tj. $M \ni 1$, $M \leq I$.

Npr. $\inf (N, |) = 1$; $\sup (N, |)$ ne postoji.

7.1.3.1. *Lako se dokazuje da je svaka konačna mreža potpuna.*

7.1.4. Distributivne mreže. — 7.1.4.1. Definicija. Mreža $(M, \vee, \cdot)$ je *distributivna* (*razdjelna*), ako vrijedi

(D) $$(x \vee y)z = xz \vee yz, \quad (xy) \vee z = (x \vee z)(y \vee z).$$ (D^d)

[1] To znači da je X konačno ili ima $\aleph_0$ članova (v. Kurepa Đ. [1], § 6.1).

7.1.4.2. Teorem. *U svakoj mreži uslov* (D) *i uslov* (D^d) *su ekvivalentni, pa je mreža distributivna ako ispunjava* (D) *ili* (D^d).

(D) $\Rightarrow$ (D^d). Izračunajmo $(D^d)_2$:

$(x \vee z)(y \vee z) =$ (prema (D)) $= (x \vee z) y \vee (x \vee z) \cdot z =$ (prema (D) i 3^d) $=$

$= [x y \vee z y] \vee z =$ (asoc.) $= x y \vee (z y \vee z) =$ (kom.) $= x y \vee (z \vee z y) =$

$=$ (prema A) $= x y \vee z = (D^d)_1$.

(D^d) $\Rightarrow$ (D). Dokaz izlazi iz posljednjeg dokaza permutacijom znakova $\cdot$, $\vee$, pri čemu $x \cdot y$ pišemo kao $x y$ (bez tačke).

7.1.5. Mreža s komplementiranjem. — 7.1.5.1. Definicija. U mreži $(M, \leq)$ sa krajevima O, I komplement od $a \in M$ je svako rješenje $x \in M$ jednadžbi $a x = O$, $a \vee x = I$; pisat ćemo $x = a^-$ ili $x = a'$; a^-, odnosno a' ćemo zvati *komplementom od a.*

Mreža s (*jednoznačnim*) *komplementiranjem* jest ona u kojoj svaki član ima (*jednoznačno određen*) komplement, koji leži u mreži.

Npr. u mreži $(P\,S, \subset)$ za svako $X \in S$ je $\bar{X}$ jednako $S \setminus X$.

7.2. Booleova algebra. Elementarna svojstva.

7.2.1. Definicija. Svaka distributivna mreža s krajevima O i I i koja dopušta komplementiranje zove se *Booleova algebra*; možemo je označiti sa $(M, \leq, O, I, \vee, \cdot, ^-)$ da se vidi relacija poretka kao i operacije $\vee, \cdot, ^-$, te elementi O, I.

7.2.2. Primjeri. (*i*). Za svaki skup S imamo Booleovu algebru $(P\,S; \subset)$.

(*ii*) Svako polje skupova (isp. 7.4.1) je Booleova algebra u odnosu na skupovne elementarne operacije $\cup$, $\cap$, $\complement$.

(*iii*). Važan primjer Booleove algebre je $(\{0, 1\}, \vee, \wedge, \neg) \equiv I2$, pri čemu $\vee$, $\wedge$, $\neg$ označuje disjunkciju, konjunkciju i negaciju (isp. pogl. 1).

7.2.3. Teorem. *Spajanje i sječenje su izotone operacije*:

$$a \leq b \Rightarrow a \vee c \leq b \vee c.$$

$$a \leq b \Rightarrow a c \leq b c.$$

Općenitije

$$a \leq b \wedge a' \leq b' \Rightarrow a \vee a' \leq b \vee b' \tag{2}$$

za bilo koje $a, a', b, b' \in M$.

Slično za sječenje.

Naime $a \vee b = b$, $a' \vee b' = b'$ daje $(a \vee b) \vee (a' \vee b') = b \vee b'$, tj.

$(a \vee a') \vee (b \vee b') = b \vee b'$ dakle (2).

7.2.2.1. Posljedica. $a, a' \leq b \Rightarrow a a' \leq b$.

—→ **7.2.4.** Teorem. *Komplementiranje je jednoznačno određeno*:

$$\left.\begin{array}{l} a \vee x = 1 \\ a \cdot x = 0 \end{array}\right\} \Rightarrow x = a^- \text{ tj. } x \leq a^- \wedge x \geq a^-,$$

pri čemu je a^- bilo koji fiksiran komplement od a.

Dokaz. $x = 0 \vee x = (a a^-) \vee x = (a \vee x)(a^- \vee x) = 1.\ (a^- \vee x) = a^- \vee x,$

tj. $x \geq a^-$.

Dualno

$$x = 1\, x = (a \vee a^-)\, x = (a x) \vee (a^- x) = 0 \vee (a^- x) = a^- x, \quad \text{tj.} \quad x \leq a^-.$$

7.2.5. Korolar. $a^{--} = a$.

Naime, po definiciji je

$$\begin{array}{l} a(a^-) = 0 \\ a \vee a^- = 1 \end{array}, \text{ tj. } \begin{array}{l} a^- \vee a = 1 \\ a^- a = 0 \end{array}, \text{ tj. } a = a^{--}.$$

—→ **7.2.6. Da Morganov obrazac.**

$$(a\, b)^- = a^- \vee b^-; \quad \textit{i dualno} \quad (a \vee b)^- = a^- b^-.$$

Dovoljno je pokazati da veličina $x = a^- b^-$ zadovoljava

(1) $(a \vee b)\, x = 0$ tj. $(a x) \vee (b x) = 0$

(2) $(a \vee b) \vee x = 1$ $(a \vee x) \vee (b \vee x) = 1.$

Stvarno je

$$a x = a(a^- b^-) = (\text{asoc.}) = (a a^-)\, b^- = 0\; b^- = 0,$$

$$b x = x b = (a^- b^-)\, b = a^- (b^- b) = a^- 0 = 0.$$

Odatle izlazi (1).

$$(a \vee b) \vee (a^- b^-) = ((a \vee b) \vee a^-)\; ((a \vee b) \vee b^-) = 1. \quad 1 = 1.$$

Dakle vrijedi i (2).

Time je drugi dio obrasca dokazan. Prvi dio se dokazuje dualno.

7.2.7. Teorem. $a < b \Rightarrow a^- > b^-$.

Dokaz. $a < b \Rightarrow a \vee b = b \wedge a \neq b \Rightarrow (a \vee b)^- = b^- \Rightarrow a^- b^- = b^- \Rightarrow a^- > b^-$, $a^- \neq b^-$.

7.3. Ideali i filtri Booleove algebre $(B, \leq, \vee, \cdot, ^-)$.

7.3.1. Definicija. *Ideal Booleove algebre* je svaki *početni* komad od $(B, \leq)$ koji je grupoid s obzirom na prvu operaciju $\vee$. Dualno je *filtar* ili *dualni ideal*: to je *svaki završni* komad J uređena skupa $(B, \leq)$ uz uslov da $(J, \cdot)$ bude grupoid. Ako je ideal (filtar) $\neq 0$ i $\neq B$ zove se on *pravi ideal* (*pravi filtar*).

Specijalno su važni *maksimalni ideali* (*filtri*): to su oni pravi ideali (filtri) kojima je *B jedini pravi nadideal* (*nadfiltar*).

7.3.2. Lema. *Ako je I (maksimalan) ideal, tada je $I^- = \{i^-;\ i \in I\}$ (maksimalan) filtar.*

Zato je dovoljno promatrati ideale jer prelaz na filtre je jasan.

⟶ **7.3.3.** **Teorem.** ***Pravi ideal I je maksimalan onda i samo onda ako iz $x \in B$ izlazi***

$$x \in I \quad \textit{ili} \quad x^- \in I. \quad \textit{I dualno za filtre.}$$

Nužnost: Ako je I_m maksimalan ideal, onda iz $x \in B$ izlazi

$$x \in I_m \quad \text{ili} \quad x^- \in I_m$$

(oboje ne može jer bi inače bilo $x \vee x^- = 1 \in I_m$ pa I_m ne bi bio prav). Ako $x\,\mathrm{non}\in I_m$, tada I_m i x generiraju određen ideal I_x pa je jasno da je $I_m \subset I_x$; kako je I_m maksimalno znači da je $I_x = B$. Dakle je $1 \in I_x$ pa zato za neko $i \in I_m$ vrijedi $1 \leq i \vee x$ dakle $1 = i \vee x$ jer je I_x generiran elementima oblika $i \vee x$. Prema tome

$$x^- \leq i \text{ jer } x^- = x^- \cdot (i \vee x) = x^- \cdot i \vee x^- \cdot x = x^- \cdot i, \quad \text{dakle je} \quad x^- \in I_m.$$

Dovoljnost: ako $a \in B \Rightarrow a \in I$ ili $a^- \in I$, tada je ideal I maksimalan. Pa neka je $I_1 \neq I$ jedan nadideal ideala I i $x \in I_1 \setminus I$; dakle je $x^- \in I$ pa tim prije $x^- \in I_1$.

Iz x, $x^- \in I_1$ izlazi $1 \in I_1$ dakle I_1 nije pravi ideal.

Dakle je $I_m = I$; to znači da je I zaista maksimalan ideal.

7.3.4. Dijadski homomorfizam. Homomorfizam algebre $(B, \leq, \vee, \cdot)$ na dvočlanu Booleovu algebru $I2$ iz § 7.2.2. zove se *dijadski homomorfizam*.

Odmah se vidi da je ispravna ova

7.3.4.1. Veza između maksimalnih ideala i dijadskih homomorfizama.

Neka je I_m maksimalan ideal; stavimo

$$h(x) = 0 \text{ za } x \in I_m$$

$$h(x) = 1 \text{ za } x\ \mathrm{non}\in I_m,$$

tada je h očigledno dijadski homomorfizam.

S druge strane, ako je h homomorfizam od B na $\{0, 1\}$, tada je jezgro toga homomorfizma određen maksimalan ideal.

⟶ **7.3.5.** **Teorem.** (***veza ideal ↔ maksimalan nadideal***).

***Svaki pravi ideal Booleove algebre B sadržan je u nekom maksimalnom idealu* (isp. § 3.8.2).**

Dokaz. Polazimo od proizvoljnog dobrog uređenja (v. Đ. Kurepa [1], § 12)

$$b_0,\ b_1, \ldots,\ b_\xi, \ldots,\ (\xi < \beta)$$

algebre B; definirajmo ideale $I_0,\ I_1, \ldots,\ I_\xi, \ldots$ ovako:

$I_0 = I$; za svako $0 < \nu < \beta$ definirajmo kao I_ν onaj ideal koji generiraju element b_ν i elementi iz $\bigcup\limits_{\alpha<\nu} I_\alpha$, ukoliko je taj ideal pravi ideal; ukoliko bi taj ideal I_ν bio $= B$, stavlja se $I_\nu = \bigcup\limits_{\gamma<\nu} I_\gamma$. Prema tome ili je $b_\nu \in I_\nu$ ili je $b_\nu \operatorname{non} \in I_\nu$. Neka je I_m unija svih ideala I_ξ. Tada je I_m maksimalan ideal. Prema § 7.3.3. dovoljno je dokazati da iz $b \in B$ izlazi ili $b \in I_m$ ili $b^- \in I_m$.

Neka je $b = b_\nu$ u gornjem dobrom uređenju.

Prvi slučaj: $b_\nu \in I_\nu$; dakle je $b \in I_\nu$.

Drugi slučaj: Nije $b_\nu \in I_\nu$; tada je $I_\nu = \bigcup\limits_{\gamma<\nu} I_\gamma$, pa I_ν i b_ν generiraju čitavo B. Prema narednoj lemi 7.3.5.1. zaključujemo da je $b^- \in I_\nu$ dakle i $b^- \in I_m$.

Dakle je zaista I_m maksimalan ideal.

7.3.5.1. Lema. *Ako pravi ideal I zajedno s $b \in B$ generira čitavu algebru B, onda je $b^- \in I$.*

Dokaz. Ideal I_b koji generiraju I i b sastavljen je od elemenata oblika $x \leq i \vee b$; dakle je $I_b = I \vee b$. Zato je posebno $1 = i \vee b$ za neko $i \in I$. No, ta relacija iskazuje da je $i \geq b^-$; na taj način imamo

$$b^- = b^- \cdot 1 = b^-(i \vee b) = b^- i \vee 0 = b^- i, \text{ tj. } b^- = b^- i \text{ dakle } b^- \leq i \text{ dakle } b^- \in I,$$

jer je I početni odlomak od $(B, \leq)$.

7.4. O nekim tijelima skupova. — 7.4.1. Definicija. *Tijelo* ili *polje skupova* definiramo kao svaku nepraznu obitelj T skupova $\subset M$ sa svojstvom da iz $X, Y \in T$ izlazi

$$X \cup Y \in T, \quad X \cap Y \in T \quad M \setminus X \in T.$$

Lako se provjeri.

7.4.2. *Svako tijelo skupova je određena Booleova algebra u odnosu na skupovne operacije $\cup$, $\cap$, C i relaciju $\subset$.*

Zanimljivo je da vrijedi i obrat (isp. § 7.5.2).

7.4.3. Reducirano tijelo skupova izvađenih iz M. To je svako tijelo K skupova $\subset M$ koje ima svojstvo da svakom dvočlanom skupu $\{x, y\} \subset M$ odgovara neko $A \in K$ sa svojstvom da presjek $\{x, y\} \cap A$ bude jednočlan.

7.4.4. Teorem. *Svako tijelo K skupova $\subset M$ izomorfno je nekom reduciranom tijelu skupova.*

Pri $\{x, y\} \subset M$ definirajmo relaciju $x \sim_K y$ u tom smislu da K ne razlikuje x i y, tj. da nijedan član od K ne sadrži jedan jedini član iz $\{x, y\}$; tada je $\sim_K$ određena relacija ekvivalencije; time se zadani skup M kao i svaki njegov podskup M_0 razbija u skupove oblika $M_0 \cap C$, gdje je C proizvoljni razred neodjeljivih tačaka. Posebno svakom članu $X \in K$ odgovara tako određena obitelj X' razredâ $C(x)$, $(x \in X)$; preslikavanje $X \in K \rightarrow X'$ prevodi K izomorfno u određeno tijelo K' skupova; no K' svakako razlikuje članove od M'.

7.4.5. Perfektno tijelo skupova. *Tijelo* ili *polje* K skupova $\subset E$ zove se *perfektnim* ili *savršenim* ako je svaki maksimalni filtar određen jednim jedinim elementom iz E kao skup svih članova iz K koji sadrže taj element iz E; E tu znači proizvoljan skup.

Tako npr. svako *konačno* tijelo K skupova je perfektno. Naime, neka je I maksimalan filtar tijela K, a P presjek svih članova iz I; tada je naravno $P \in I$, jer je I konačno; nadalje je $P \neq \emptyset$ jer bi inače bilo $I = K$. Svaki član skupa P određuje filtar I. Prema tome, I može biti određeno i sa više članova. Naravno, ako je tijelo K još i reducirano, onda je svaki maksimalni filtar I tijela K određen jednom jedinom tačkom skupa E.

7.4.6. Teorem. *Tijelo K svih otvoreno-zatvorenih skupova bikompaktna topološkog prostora je perfektno.*

U obrnutom slučaju bilo bi $P = \bigcup I = \emptyset$ odakle prelazeći na komplemente $CP = \bigcap C| = C\emptyset =$ prostor E. No, kako je prostor E bikompaktan, a članovi od CI otvoreno-zatvoreni, postojalo bi konačno mnogo članova iz CI koji bi prekrivali E; presjek komplemenata tih skupova bio bi P pa kao presjek od konačno mnogo članova filtra I bilo bi $P \in I$; dakle bi bilo $\emptyset \in I$ a time $I = K$, protivno pretpostavci da je I maksimalan filtar u K (v. § 7.3.1.). Dakle je $P \neq \emptyset$, a naravno, svakim $x \in P$ određen je i sam filtar I.

Naravno, presjek P nije općenito jednočlan. No, ako je tijelo K reducirano, tada je $\bigcap I$ jednočlan skup za svaki maksimalni filtar I tijela K.

7.4.7. Teorem. *Ako je K reducirano perfektno tijelo skupova iz M, tada se skup M može tako bikompaktno topologizirati da obitelj svih njegovih otvoreno-zatvorenih skupova bude upravo ishodno skupovno tijelo K.*

Dokaz. 1. Topologiju u M ćemo definirati time što ćemo tijelo K proglasiti bazom otvorenih okolina i prema tome podskup $X \subset M$ smatrati otvorenim onda i samo onda ako je X unija neke podobitelji od K.

2. *Svako $X \in K$ je i zatvoreno* jer $N \setminus X \in K$ pa je X komplement otvorena skupa $M \setminus X$.

3. *Prostor je topološki i zadovoljava Hausdorffovu aksiomu odvajanja,* jer je K reducirano nad M.

4. *Prostor M je bikompaktan,* tj. svaki otvoren pokrivač Π od M obuhvata konačan pokrivač Π_0, dakle je $\bigcup \Pi_0 = M$.

Naravno, možemo pretpostaviti $\Pi \subset K$, jer je dovoljno svako X zamijeniti kakvom obitelji skupova iz K kojima je X unija.

No, kad pokrivač Π ne bi bio svodljiv ni na koji konačan potpokrivač Π_0, tada bi pokrivač Π generirao određen *pravi* ideal, recimo I.

Neka je I_m maksimalni pravi ideal $\supsetneq I$ (isp. § 7.3.5). Tome maksimalnom idealu I_m odgovara maksimalni filtar I_m^- tijela K. Kako je K po pretpostavci perfektno, postojao bi neki element $a \in M$ koji bi generirao filtar I_m^- kao skup svih $X \in K$ za koje je $a \in X$; to znači da bi za ideal I_m vrijedilo

$$I_m = \{X;\ X \in K,\ a \operatorname{non} \in X\};$$

kako $I \supset \Pi$ znači to da bi bilo $a \operatorname{non} \in X$ za svako $X \in \Pi$, protivno pretpostavci da je Π pokrivač od M.

5. *Svaki FG-skup $X \subset M$ član je u K.*

Naime, X je unija određene obitelji $O \subset K$; no X je zatvoren skup bikompaktna prostora M, zato pokrivač O obuhvata konačan potpokrivač O_0, tj. $\cup O_0 = X$; no unija od *konačno mnogo* elemenata iz K opet je u K; dakle je zaista $X \in K$.

6. *Bikompaktni prostor M jednoznačno je određen gornjim zahtjevima.*

Neka su naime M_1, M_2 dvije bikompaktne topologije množine M za koje vrijedi iskaz teorema. Specijalno se K podudara s obitelji svih GF-skupova u M_1 kao i sa obitelju svih GF-skupova iz M_2; dakle je svako $X \in K$ otvoreno i u M_1 i u M_2 pa je identično preslikavanje $j: M_1 \to M_2$ neprekidno i u M_1; isto je takvo inverzno preslikavanje neprekidno, pa se dakle radi o homeomorfizmu j: $M_1 \to M_2$ između prostorâ M_1, M_2.

7.5. Teoremi o reprezentaciji.

7.5.1. Teorem. *Neka je Φ neki skup maksimalnih filtara Booleove algebre B; za $b \in B$ neka $\Phi(b)$ označuje sve članove $\Phi^{\cdot}$ iz Φ za koje je $b \in \Phi^{\cdot}$; prema tome $\Phi(b)$ je određena obitelj maksimalnih filtara od B. Obitelj $\Phi(B)$ svih $\Phi(B^{\cdot})$ je jedno reducirano tijelo skupova nad Φ; preslikavanje*

(1) $\quad B^{\cdot} \to \Phi(B^{\cdot})$ *je homomorfizam od B na $\Phi(B)$.*

U slučaju da ***svakom*** *$B^{\cdot} \neq 0$ odgovara neko $\Phi^{\cdot} \ni B^{\cdot}$, tada je preslikavanje (1) izomorfizam.*

Dokaz. Dokažimo da pri b_1, $b_2 \in B$ vrijedi

(2) $$\Phi(b_1 b_2) = \Phi(b_1) \cap \Phi(b_2).$$

Naime, $\Phi(b_1 b_2)$ je skup svih filtara $F \in \Phi$ sa svojstvom $b_1 \cdot b_2 \in F$; no relacija $b_1 \cdot b_2 \in F$ je ekvivalentna sa $b_i \in F$, što znači da

$$F \in \Phi(b_i) \, (i = 1, 2), \quad \text{tj.} \quad F \in \Phi(b_1) \cap \Phi(b_2).$$

Time je homomorfizam (2) dokazan.

No, filtar F je maksimalan; to znači da zbog $F \in \Phi(b_1) \Leftrightarrow b_1 \in F$ imamo $b_1^- \operatorname{non} \in F$, tj. $b_1^- \in CF$, tj. $\Phi(b_1)^- = \Phi(b_1)^- =$ komplement od $\Phi(b_1)$ u $P\Phi$.

Podtijelo $\Phi(B)$ je reducirano u Φ.

Naime, za različne maksimalne filtre F_1, $F_2 \in \Phi$ postoji tačka $b \in B$ koja je u jednom a nije u drugom od filtara F_1, F_2; neka je npr.

$$b \in F_2 \setminus F_1, \quad \text{onda to znači} \quad b \in F_2 \quad \text{dakle} \quad \Phi(b) \ni F_2$$
$$b \operatorname{non} \in F_1 \quad \text{dakle} \quad \Phi(b) \operatorname{non} \ni F_1.$$

Najzad, ako iz $b \neq 0$ izlazi $\Phi b \neq \emptyset$, dokažimo da je (1) izomorfizam. Naime, ako su a, b različni članovi iz B, onda je $\Phi(a) \neq \Phi(b)$; u obrnutom slučaju bilo bi $\Phi(a) = \Phi(b)$, tj. $\Phi(a) \setminus \Phi(b) = \emptyset$, tj. $\Phi(a) \cap \Phi(b^-) = \emptyset$ dakle $\Phi(a \cdot b^-) = \emptyset$, pa dakle članu $ab^- \in B \setminus \{0\}$ ne bi odgovaralo $\Phi(ab^-) \neq \emptyset$, protivno pretpostavci,

—→ **7.5.2. Stoneov teorem (1934—1938).** ***Svaka Booleova algebra B je izomorfna s tijelom skupova i to specijalno s reduciranim tijelom svih otvoreno-zatvorenih skupova nekog bikompaktnog topološkog prostora.***

7.5.3. Kažemo li da je prostor *potpuno nesvezan* (totally disconnected) ako njegova obitelj otvoreno-zatvorenih skupova daje reducirano tijelo skupova, tada se gornji teorem može izreći i ovako:

—→ **7.5.4. Teorem (M. H. Stone).** ***Svaka Booleova algebra izomorfna je s tijelom svih otvoreno-zatvorenih skupova nekog bikompaktnog posve nesvezanog prostora.***

Dokaz. Neka Φ u prethodnom teoremu 7.5.1 označuje obitelj M svih maksimalnih filtara Booleove algebre B. Neka je $b \in B \setminus \{0\}$; tada b generira određen pravi glavni filtar koji možemo proširiti do maksimalnog filtra $F(b)$. Dakle je $b \in F(b) \in \Phi(b) \in \Phi$ za svako $b \in B \setminus \{0\}$.

Prema teoremu 7.5.1 preslikavanje $b \to \Phi(b)$ je izomorfizam između B i nekog reduciranog tijela K iz $P\Phi$, pridružujući pritom $0 \in B$ sa $\varnothing \in P\Phi$.

Dokažimo da je K perfektno. Neka je naime F proizvoljan maksimalan filtar u K; zbog izomorfizma $B \longleftrightarrow K$ skup $S = \{b;\ b \in B$ za koje je $\Phi(b) \in F\}$ jest određen maksimalni filtar algebre B. Promatrajmo sámo S; tada je

$$F \ni \Phi(b) \in F \Leftrightarrow b \in S \qquad \text{dakle}$$

$$\Phi(b) \in F \Leftrightarrow S \in \Phi(b).$$

To znači da je F određeno upravo elementom $S \in \Phi$, pa je dakle K savršeno tijelo skupova. Time je teorem dokazan.

7.5.5. **Booleova algebra i topologija.** Iz 7.5.4 zaključujemo da je izučavanje Booleove algebre usko vezano s topologijom — i to s onim dijelom topologije koji izučava *Stoneove prostore* (tj. bikompaktne nesvezane prostore).

Zanimljivo je pri tom pogledati što pojedinom pojmu Booleove algebre B odgovara u pripadnom Stoneovu prostoru $S(B)$; neka je upravo $i: B \to PS(B)$ izomorfizam o kojem je riječ; tada je iB upravo obitelj $GF(SB)$ svih GF-skupova prostora $S(B)$.

Ako je I ideal algebre B, tada $iI := \bigcup_{x \in I} ix$ kao unija G-skupova je otvoren skup prostora; na taj način se dobije svaki otvoren skup G; naime, skup $i^{-1}G$ svih $b \in B$ za koje $ib \subset G$ je određen ideal, i očigledno je $i(i^{-1}G) = G$.

Prelazeći na dualna razmatranja zaključujemo da filtri algebre i F-skupovi prostora međusobno odgovaraju jedni drugima.

Posebno, nula-ideal algebre $\longleftrightarrow$ prazni skup prostora; jedinični filtar odgovara čitavu prostoru, pravi filtri (ideali) algebre odgovaraju pravim zatvorenim (otvorenim) skupovima prostora; maksimalni filtri algebre odgovaraju jednočlanim skupovima prostora, a maksimalni ideali komplementima jednočlanih skupova.

7.5.6. Konačne Booleove algebre.

Uzmimo slučaj da je Booleova algebra B konačna; tada je i prostor $S(B)$ konačan; ako $S(B)$ ima n članova, tada njegovi otvoreno-zatvoreni skupovi čine partitivni skup $PS(B)$ od 2^n članova; to znači da je $kB = 2^n = 2^{kSB}$.

Prema tome imamo

7.5.6.1. Teorem. *Konačne Booleove algebre su nužno izomorfne s partitivnim skupovima.*

Specijalno, Booleovoj algebri $\{0, 1\}$ odgovara Stoneov jednočlani prostor. Jednočlanoj Booleovoj algebri odgovara prazni prostor.

Nadalje:

7.5.6.2. Teorem. *Izomorfizam* ***konačnih*** *Booleovih algebri i istobrojnost Booleovih algebri međusobno su ekvivalentna svojstva.*

Iz gornjeg teorema 7.5.6.2 o konačnim Booleovim algebrama izlazi i

7.5.6.3. Teorem. *Svaka Booleova algebra duljine $n < \infty$ izomorfna je s partitivnim skupom PIn (pri tom, duljinu algebre B definiramo kao za jedinicu umanjeni supremum kardinalnih brojeva svih lanaca iz $(B, <)$).*

7.5.6.4. Teorem. *Stoneov prostor $S(B)$ Booleove algebre B je metričan onda i samo onda ako je Booleova algebra prebrojiva.*

To je neposredna posljedica Urysohnova teorema da je bikompaktni T_2-prostor metričan onda i samo onda ako ima prebrojivu bazu otvorenih skupova. Naime, gornje preslikavanje $b \to \Phi(b)$ daje bazu otvorenih skupova prostora $S(B)$.

7.6. U kakvoj je zavisnosti kSB od kB za bilo koju Booleovu algebru? U § 7.5.6.1 smo vidjeli da za svako konačno B imamo $kB = 2^{kSB}$.

7.6.1. Teorem. *Ako je B atomarno i beskonačno, tada je $kS(B) = 2^{kB}$, tj. Booleova algebra tada ima 2^{kB} maksimalnih filtara.*[1]

Dokaz. Možemo uzeti da je $B = PM$, gdje je M beskonačan skup; kako su maksimalni filtri od B određene obitelji skupova, a kako svih tih obitelji ima 2^{kB}, znači da maksimalnih filtara ima $\leq 2^{kB}$, tj. $\leq 2^{2^{kM}}$ (1).

U drugu ruku PM sadrži tijelo skupova izomorfno s tijelom $F_{0, 2^{kM}}$ svih GF-skupova Kartezijeva produkta od 2^{kM} dvočlanih T_2-prostora. Promatrajmo specijalno slučaj da je M svuda gust skup u prostoru $D_{2^{kM}} = \prod_{t \in PM} \{0, 1\}_t$ (egzistenciju takvog M pokazali su *Hewitt* 1946. i *Marczewski* 1947.).

Tada preslikavanje

$$A \to iA := A \cap M \quad (A \in F_{0, 2^{kM}})$$

je izomorfizam od $F_{0, 2^{kM}}$ prema PM.

---

[1] Isp. *B. Pospišil*, Remark on bicompact spaces, Ann of Math. 38 (1937) 845—846. A. Tarski, Ideale in vollständigen Mengenkörpern, Fund. Math., 32 (1939) 45—63, 33 (1945) 51—65.

To ujedno znači da postoji neprekidno preslikavanje prostora SPM na

$$D_{2^{kM}} \text{ — dakle je } k\,SPM \geq k\,D_{2^{kM}} = 2^{2^{kM}} \tag{2}$$

Iz (1) i (2) izlazi odgovarajuća jednakost u teoremu.

Prema tome, u slučaju beskonačnog PM sadrži PM maksimalnih filtara maksimalan moguć broj tj. $2^{2^{kM}}$, tako da maksimalnih filtara ima vrlo mnogo.

Može se dokazati

7.6.2. Teorem (*Lindenbaum—Tarski*). *Booleova algebra B je izomorfna sa PM onda i samo onda ako za svako $x \in B/\{0\}$ postoji bar jedan prvi element u $B\,(0;\,x]$, tj. neki neposredni nasljednik od 0 je prethodnik od x.*

7.7. Booleovi prsteni. — **7.7.0.** U Booleovoj algebri $(B, \vee, \cdot)$ je svojstvo idempotentnosti za obje operacije (spajanje $\vee$ i sječenje) svojstvo koje se mnogo razlikuje od operacija s brojevima ali je ono istinito pri skupovnim operacijama spajanja i sječenja. Mogu se promatrati prsteni s analognim svojstvom s obzirom na drugu operaciju. Tako nastaje

7.7.1. *Definicija Booleoviih prstena.* Prsten $(A, +, \cdot)$ je Booleov ako je idempotentan u odnosu na množenje:

$$aa = a, \quad (a \in A).$$

7.7.2. Lema. *U Booleovu prstenu je $a = -a$.*

Drugim riječima karakteristika Booleova prstena je $= 2$.

Naime

$$a + x = (a + x)(a + x) = aa + xa + ax + xx =$$

$$= a + (xa + ax) + x = (a + x) + (xa + ax);$$

odatle dodajući $-(a + x)$ izlazi

$$0 = xa + ax. \quad \text{Specijalno za} \quad x = a \quad \text{imamo}$$

$$0 = aa + aa, \quad \text{tj.} \quad 0 = a + a, \quad \text{dakle} \quad a = -a.$$

7.7.3. Lema. *Svaki Booleov prsten je komutativan.*

Naime $xy - yx = xy + y \cdot (-x) =$ (prema 7.7.2.) $xy + yx = 0$

tj. $xy - yx = 0$

dakle $xy = yx$.

$\longrightarrow$ **7.7.4.** ***Teorem o vezi Booleovih algebara i Booleovih prstena. Postoji obostrano jednoznačna veza između Booleovih algebri i Booleovih prstena s jedinicom.***

(i) Polazeći od Booleove algebara $(B, <, \vee, \cdot, -)$ ***i stavljajući***

(1) $$a + b = (ab^{-}) \vee (a^{-} b),$$

dobije se Booleov prsten $(B, +, \cdot)$ ***s jedinicom*** $I = 1$ ***i*** $O = 0$;

(ii) Ako je $(A, +, \cdot)$ ***bilo koji Booleov prsten s jedinicom*** **1**, ***tada stavljajući***

(2) $$a \vee b = a + b - ab$$

dobijemo Booleovu algebru

$$(A, \vee, \cdot, -) \text{ kojoj je } I = 1 \text{ te } a^- = 1 - a.$$

Pri tom (prim) idealima odgovaraju (prim) ideali.

7.7.5. Prvi dio: *prelaz od Booleove algebre* $(B, <, \vee, \cdot, ^-)$ *na Booleov prsten* $(B, +, \cdot)$.

Definirajmo $a+b$ pomoću (1); imamo posebno

$$a + a = (aa^-) \vee (a^- a) = O \vee O = O;$$

$$O + a = (0 \cdot a^-) \vee (0^- a) = O \vee a = a;$$

dakle je O neutral prema $+$. Dalje je

$$a + b = (ab^-) \vee (a^- b) = (\text{po distribuciji}) =$$

$$= \underbrace{(a \vee a^-)}_{I} (b^- \vee a^-) (a \vee b) \underbrace{(b^- \vee b)}_{I} = (a \vee b) \cdot (a^- \vee b^-).$$

Dakle je

(3) $$a + b = (a \vee b)(a^- \vee b^-), \quad \text{odakle} \quad a + b = b + a.$$

Dalje iz (3) po De Morganovu obrascu 7.2.6 izlazi:

(4) $$(a+b)^- = (a^- \cdot b^-) \vee (ab);$$ zato je

$$(a+b) + c = [(a+b) \vee c]\,[(a+b)^- \vee c^-] =$$

$$= [(\{a \vee b\}\, \{a^- \vee b^-\}) \vee c]\,[(\{a^- b^-\} \vee \{ab\}) \vee c^-] =$$

$$= [ba^- \vee ab^- \vee c]\,[a^- b^- \vee ab \vee c^-] = ca^- b^- \vee cab \vee ba^- c^- \vee ab^- c^-,$$

jer ostali sumandi su O zbog $xx^- = O$. Dakle je

(5) $$(a+b) + c = ca^- b^- \vee cab \vee ba^- c^- \vee ab^- c^-.$$

Transpozicijom $a \longleftrightarrow c$ prelazi (5) u

(6) $$(c+b) + a = ac^- b^- \vee acb \vee bc^- a^- \vee cb^- a^-.$$

Kako je $(5)_2 = (6)_2$, bit će i $(5)_1 = (6)_1$ tj.

$$(a+b) + c = (c+b) + a = a + (b+c).$$

Odatle izlazi asocijativni zakon.

Još preostaje provjeriti distributivni zakon.

$$ac + bc = (\text{prema } (1))\,[(ac)\,(b^- \vee c^-)] \vee [(a^- \vee c^-)\,(bc)] = acb^- \vee a^- bc =$$

$$= (\text{distributivnost od } \cdot \text{ prema } \vee)\,[(ab^-) \vee (a^- b)]\,c = (a+b)\,c.$$

Dakle je distribucija na snazi.

Prema tome se dobije komutativan Booleov prsten s jedinicom.

7.7.6. D r u g i k o r a k:

Prelaz od Booleova prstena $(A, +, \cdot)$ *na* $(A, \leq, \vee, \cdot, ^-)$.

Neka je sada obrnuto zadan Booleov jedinični prsten $(A, +, \cdot)$. Definirajmo $\vee$ pomoću (2) i stavimo $a^- = 1 - a$; dokažimo da je $(A, +, \cdot)$ Booleova algebra. Uvedimo relaciju $\leq$, odnosno $\geq$ tako da vrijedi

(7) $$a \geq b \Leftrightarrow ab = b \Leftrightarrow b \leq a.$$

7.7.6.1. Relacija $\geq$ je uređajna relacija:

$a \geq b$ zbog $aa = a$ (svojstvo idempotencije)

$a \geq b \wedge a \leq b \Rightarrow a = b;$

naime

$$b = ab = ba = a \quad \text{dakle} \quad a = b.$$

Dokažimo $\quad a \geqq b \geqq c \Rightarrow a \geqq c.$

$$ab = b$$

$$\underline{bc = c} \qquad ac = ?$$

$$ac = a(bc) = (ab)c = bc.$$

Dakle $ac = c$, tj. $a \geqq c$.

7.7.6.2. Nadalje je $0 \leq a \leq 1$ jer je $a0 = 0$, $a1 = a$.
Prema tome se dobije uređen skup $(A, \leq)$ sa krajnjim članovima 0,1.

7.7.6.3. Nadalje $a \geq ab$ jer $a(ab) = (aa)b = ab$; isto tako $b \geq ba$.

7.7.6.4. L e m a. *Ako je* $a, b \in A$, *tada* $\inf\{a, b\}$ *postoji, i jednako je* $a \cdot b$.
Naime, svakako je $a \geq ab$, $b \geq ab$ dakle je ab minoranta od a, b.
Dokažimo da je to *najveća* minoranta. Neka je

$$x \leq a, \quad \text{tj.} \quad ax = x$$

$$x \leq b, \quad \text{tj.} \quad bx = x;$$

tada je

$$(ab)x = ax = x \quad \text{tj.} \quad (ab)x = x \quad \text{tj.} \quad ab \geq x.$$

Dakle je zbilja $a \cdot b = \inf\{a, b\}$.

7.7.6.5. *Promatrajmo* $a^- = 1 - a$; *tad je preslikavanje* $a \to a^-$ *obostrano jednoznačno i opadajuće.*

Naime ako je $\quad a \leq b$, tj. $ab = a$, $\quad$ tada imamo

$$a^- b^- = (1 - a)(1 - b) = 1 - a - b + ab = 1 - a - b + a = 1 - b,$$

$$\text{tj.} \quad a^- b^- = b^-, \quad \text{tj.} \quad a^- \geq b^-.$$

Dakle je $\quad 1 - (1 - a)(1 - b) = a + b - ab = a \vee b.$

7.7.6.6. Tada je $a \leq a \vee b$ jer $a(a \vee b) = a^2 + ab - ab = a$ Isto tako e $b \leq a \vee b$.

Nadalje je $a \vee b = \sup\{a, b\}$ kao što se lako vidi.

Najzad, $a \cdot a^{-} = a \cdot a^2 = 0$,

$$a \vee a^{-} = a + a^{-} + a \cdot a^{-} = a + 1 - a + 0 = 1.$$

Prema tome je dobivena mreža s komplementiranjem i s $0 = O$ te $1 = I$.

7.7.6.7. Još preostaje da se dokaže distributivnost od $\cdot$ prema $\vee$, i od $\vee$ prema.; imamo

$$a(b \vee c) = a(b + c - bc) = ab + ac - abc =$$

$$(\text{zbog } aa = a,\ abc = a\,abc = ab\,ac) = ab + ac - ab\,ac = (ab) \vee (ac).$$

Isto tako

$$(ab) \vee c = ab + c - abc = ab + ac - abc + c^2 - bc - abc -$$

$$- ac + abc = (a + c - ac)(b + c - bc) = (a \vee c)(b \vee c).$$

Time je sve dokazano.

7.7.6.8. Primjeri:

(*i*) Booleova algebra $(\{0, 1\}, \vee, \wedge, \urcorner)$ i prsten $(I2;\ +_2,\ \cdot_2)$ odgovaraju međusobno.

(*ii*) Booleova algebra $(PM, \cup, \cap, C)$ i prsten $(\{0, 1\}^M;\ +_2,\ \cdot_2)$ odgovaraju međusobno.

7.8. Primjedba. Booleova algebra je poseban slučaj mreže; a mlada *teorija mreža* se vrlo razvila i predstavlja posebno poglavlje algebre; postoje analogije između teorije grupa i teorije mreža (v. Birkhoff [1]).

7.9. Zadaci o mrežama i Booleovim algebrama.

1. Promatraj Booleovu algebru $(P\{1, 2, 3\}, \subset)$ i pripadni Booleov prsten; kako glasi tablica zbrajanja toga prstena? (isp. definiciju 7.7.4).

2. Dokaži da skup svih rješenja jednadžbe $x^2 = x$ u komutativnom prstenu A karakteristike 2 čine Booleov potprsten od A.

3. Neka je $(B, \leq)$ Booleova algebra;
1) ako je $\{a, b\} \subset B$, $a \leq b$, tada je i interval $B[a, b]$ Booleova algebra;
2) svaka homomorfna slika Booleove algebre opet je Booleova algebra;
3) svaka podmreža Booleove algebre ne mora biti Booleova podalgebra.

4. 1) U svakoj mreži vrijedi

$$ab \vee bc \vee ca \leq (a \vee b)(b \vee c)(c \vee a); \tag{1}$$

ako tu umjesto $\leq$ može stajati znak $=$, onda se sa med (a, b, c) označuje izraz $(1)_1$, odnosno $(1)_2$;
1) ako je mreža distributivna, tada

$$\text{med}\,(a, b, c) = b \Leftrightarrow ac \leq b \leq a \vee c;$$

3) u Booleovoj algebri vrijedi $\text{med}\,(a^{-} b^{-} c^{-}) = (\text{med}\,(a, b, c))^{-}$, kao i $ab^{-} \vee a^{-} b = ab\,(a \vee b)^{-} \vee (ab)^{-}(a \vee b)$.

5. *Oduzimanje u Booleovoj algebri* $(A, \vee, \cdot, ^-)$. Neka $a-b$ znači rješenje jednadžbi $bx=O$, $b\vee x=a\vee b$; $a-b$ je *relativni komplement od b u mreži* $[O, a\vee b]$. Tada je: 1) $a-b=ab^-$; 2) $a-a=O$; 3) $a-(b-c)=(a-b)\vee(ac)$; 4) $a-(b\vee c)=(a-b)(a-c)$; 5) $a-bc=(a-b)\vee(a-c)$.

6. *Račun sudova i Booleova algebra* (isp. pogl. 1). Neka je S skup svih sudova; za svako $s\in S$ neka $\underline{s}$ bude pripadni razred, tj. skup svih članova iz S koji su ekvivalentni sa s. Neka je B skup svih razreda $\underline{s}$ pri $s\in S$; pri $a, b\in B$ definirajmo $a\vee b=\underline{a_1\vee b_1}$, $a\wedge b=\underline{a_1\wedge b_1}$, $a^-=\underline{\neg a_1}$ pri $a_1\in a$, $b_1\in b$. Tada je $(B, \vee, \wedge, ^-)$ Booleova algebra kojoj je skup svih $\underline{i}$, pri $i\in B$, $vi=1$ jedan prost ideal. Dr. r. sudovi čine Booleovu algebru u kojoj istiniti sudovi čine određen prost ideal (B o o l e, 1847).

7. *Potpune* (*kompletne*) *mreže*. To su uređeni skupovi $(S, \leq)$ sa svojstvom da iz $X\subset S$, izlazi $\inf X\in S$, $\sup X\in S$; specijalno je tada $\sup\varnothing\in S$ pa $\sup\varnothing$ označuje minimalni član u $(S, \leq)$. Govori se o *σ-mrežama,* ako posljednje relacije vrijede pri uslovu da X ima $\leq\aleph_0$ članova. Dokaži da je $(PS, \subset)$ kompletna mreža.

8. *O distributivnosti.* 1) Promatrajmo distributivnu mrežu $(L, \vee, \wedge)$; tada za proizvoljne prirodne brojeve m, n i nizove $a_{1\mu}\in L$, $a_{2\nu}\in L$ vrijedi

$$(a_{11}\vee a_{12}\vee\cdots\vee a_{1m})\wedge(a_{21}\vee\cdots\vee a_{2n})=\bigvee_{\mu,\nu} a_{1\mu}\wedge a_{2\nu};$$

pri tom $\mu\in\{1, 2, \ldots, m\}$, $\nu\in\{1, 2, \ldots, n\}$.

2) Općenito, neka je I proizvoljan pun skup; neka svakom $i\in I$ bude pridružen pun skup J_i; svakom $j_i\in J_i$ neka je pridružen neki član $a_{ij_i}\in L$; ako su skupovi I, J_i konačni, tada vrijedi

$$\bigwedge_{i\in I}\bigvee_{j_i\in J_i} a_{ij_i}=\bigvee_{f\in S}\bigwedge_{i\in I} a_{if(i)}, \tag{1}$$

pri tom f prolazi skupom S svih jednoznačnih funkcija sa svojstvom

$$\operatorname{Dom} f=I,\ f(i)\in J_i\ (i\in I).$$

Vrijedi i dualna formula $(1)^d$ koja iz (1) izlazi permutirajući $\vee\leftrightarrow\wedge$.

Posebno, (1) vrijedi za Booleove algebre pri konačnim skupovima I, J_i; ako su skupovi I, J_i beskonačni, tada (1), $(1)^d$ ne moraju nužno vrijediti.

3) Vrijedi li (1) i $(1)^d$ za svake indeksne skupove I, J_i, kaže se da je struktura *potpuno distributivna.*

4) Potpuna ili kompletna Booleova algebra je potpuno distributivna onda i samo onda ako je ona izomorfna s Booleovom algebrom oblika $(PS, \cup, \cap, C)$ pri nekom skupu S (A. T a r s k i, 1930).

5) Ako je Booleova algebra kompletna, tada je ona beskonačno distributivna u smislu da za svaki element a i podskup X algebre vrijedi $a\wedge\bigvee_{x\in X} x=\bigvee_{x\in X} a\wedge x$; i dualno (J. von N e u m a n n, 1936).

9. *Slobodne izvodnice.* Neka je L mreža a X njen podskup; kaže se da je X skup *slobodnih generatora* od L ako se svaki homomorfizam od X u neku mrežu M može proširiti na homomorfizam čitave mreže $L \to M$. Mreža (Booleova algebra) je *slobodna* i ima n slobodnih generatora (izvodnicâ) ako obuhvata skup od n slobodnih generatora koji je rađaju ili generiraju.
Neka $FL\,(n)$ znači slobodnu mrežu od n generatora; dokazati:
1) $FL\,(2)$ ima 4 člana; 2) $FL\,(3)$ je beskonačno; 3) $FL\,(4)$ sadrži beskonačan lanac; 4) Svaka 4-člana Booleova algebra B je slobodna; generator joj je član $x \in B \setminus \{0, 1\}$, pa je $B = \{0, 1, x, x^{-}\}$; 5) Skup $F_{0,n}$ svih otvoreno-zatvorenih skupova Descartesova produkta od n dvočlanih Hausdorffovih prostora $\{0, 1\}$ je skupovna Booleova algebra sa n slobodnih generatora G_ν koji su antiprojekcije od 1; pritom ν prolazi skupom indeksa od n članova; G_ν je skup svih tačaka produkta kojima je ν-ta koordinata $= 1$.

Literatura

Birkhoff [1]; Kuroš [3]; Rudeanu [1]; Sikorski [1]; Szász [1].

8. SVEOPĆE (UNIVERZALNE) ALGEBRE ILI Δ-ALGEBRE. UREĐENE ALGEBRE

To je zapravo drugi naziv za *algebarske strukture*, pri čemu je bitno da se radi o nekom osnovnom skupu A i o određenom (konačnom ili beskonačnom) *nizu operacija* u A.

8.1. Pojam n-arne operacije. Neka je n redni broj (n može biti 0, konačan ili beskonačan); tada A^n znači skup svih uređenih n-torki elemenata iz A; posebno $A^0 = \varnothing$ (prazan skup); pod *n-arnom operacijom u A* razumijevamo svako jednoznačno preslikavanje f sa svojstvom

(1) $$\operatorname{Dom} f \subset A^n, \quad \operatorname{Antidom} f \subset A;$$

posebno, pri $n = 0$ imamo *nularnu operaciju* f koja praznom skupu $\varnothing$ pridružuje neki član $f\varnothing \in A$.

Primijetimo da u (1) ne mora biti $\operatorname{Dom} f = A^n$; ne mora biti ni $\operatorname{Antidom} f = A$.

8.1.1. Izbor ili odlikovanje određena člana u skupu shvatamo kao određenu 0-arnu operaciju, tako npr. neutralni element grupe je rezultat 0-arne operacije u toj grupi.

8.2. Definicije. — 8.2.1. Sveopća algebra. Svaka uređena dvojka (M, s) proizvoljna skupa M i proizvoljna niza s operacijâ u M zove se *sveopća* (*univerzalna*) *algebra* ili naprosto *algebra*. Redni broj niza s označivat ćemo sa γs i zvati *visinom algebre* (M, s). Za pojedini član s_i niza s pisat ćemo također $s_i \in s$.

8.2.2. Tip algebre. Ako je niz $s = s_0, s_1, \ldots, s_\xi, \ldots$ $(\xi < \gamma)$ zadani niz operacijâ, neka bude $\Delta = \rho_0, \rho s_1, \ldots, \rho s_\xi, \ldots$ $(\xi < \gamma)$ niz ρs rednih brojeva ρs_ξ, pri čemu ρs_ξ označuje da je s_ξ određena ρs_ξ-operacija u A.

Niz $\Delta = \rho s$ zove se *tip algebre* (A, s).

8.2.3. Jednakotipne algebre. Algebra (A, s) je jednakotipna s algebrom (A', s'), ako je niz ρs permutacija niza $\rho s'$ (v. poglavlje 3 § 9.3).

8.3. Primjeri univerzalnih algebara.

8.3.1. *Grupoid kao algebra.* Svaki grupoid $(G, \cdot)$ je algebra (G, s); tu je $s = \cdot$, tj. s je jednočlan niz sastavljen od binarne operacije s oblasti G^2; tip te algebre je $\Delta = (2) =$ jednočlani niz sa članom $= 2$.

8.3.2. *Grupa kao algebra.* Svaka grupa $(G, \cdot)$ je algebra (G, s), pri čemu je s tročlan niz (f_2, f_1, f_0); f_2 je operacija reda 2; f_1 je operacija reda 1, a označuje se obično sa $x \to x^{-1}$; f_0 je operacija reda 0, a ima za svrhu da ukaže na neutralni član grupe (v. 8.1.1). Dakle je $\Delta = \rho s = (2, 1, 0)$.

8.3.3. *Prsten kao algebra.* Možemo pretpostaviti da je riječ o prstenu $(A, +, \cdot)$ sa bar 2 člana; tada je taj prsten algebra (A, s), pri čemu je

$$s = (f_2, f_1, f_0; g_2; l_x, d_x)_{x \in M};$$

pri tom f_2, f_1, f_0 znače isto što i u 8.3.2; g_2 je proizvoljna operacija reda 2 u A; za dano $a \in A$ znači l_a pridruživanje od A u sama sebe oblika

$$A \ni x \to a x \in A;$$

isto tako znači d_a pridruživanje $x \to x a$.

8.3.4. *Uređen skup kao algebra.* Neka je $(M, \leq)$ uređen pun skup; možemo ga shvatiti kao algebru $(M; s)$; ako je M jednočlan, možemo shvatiti $s = (f_1)$; ako M ima bar 2 člana, možemo shvatiti $s = (f_0, g_0, f_2, g_1)$; neka je m_0 tačka od M koja je 0-operacijom f_0 izabrana u M; isto tako neka je m_1 tačka od M koja je izabrana u M posredstvom operacije g_0; tada postavljamo ove uslove:

(1) $$m_0 \neq m_1;$$

(2) *Refleksivnost.* $$f_2(x, y) = m_0 \Leftrightarrow x = y \in M,$$

tj. $f_2^{-1}(m_0)$ je sastavljeno od svih (m, m), $(m \in M)$;

(3) *Antisimetrija.* Ako je $g_2(x, y) = m_1$, onda $g_2(y, x)$ nije definirano.

(4) *Tranzitivnost.* Ako je $g_2(x, y) = g_2(y, z) = m_1$, tada je $g_2(x, z) = m_1$.

Pišemo li

(5) $$x < y \Leftrightarrow g_2(x, y) = m_1$$

(6) $$x \| y \Leftrightarrow x \neq y \wedge g_2(x, y) \neq m_1 \wedge g_2(y, x) \neq m_1,$$

tada se vidi da je relacija $<$ uređajna u skupu M.

Time je dokazano da su uređeni skupovi određene algebarske strukture, odnosno da je teorija uređenih skupova određena algebarska oblast. Zato je prirodno promatrati pojedine algebarske strukture koje su uređene (potpuno ili djelomično); na taj način imamo *uređene grupoide, uređene prstene, uređena tijela, uređene algebre* itd. *U svakom slučaju je riječ o skupu koji je i uređen i određena algebarska struktura; no osim toga uvijek se mora naznačiti kako se operacije dotične algebarske strukture vladaju prema uređenosti.*

8.4. Uređen grupoid. Definicija. *Uređen grupoid* je svaka uređena trojka $(G, +, \leq)$ sa ova tri svojstva:

(*i*) (*Uslov grupoida*): $(G, +)$ je grupoid;

(*ii*) (*Uslov uređenja*): $(G, \leq)$ je uređen skup (pogl. 3, § 13);

(*iii*) (*Uslov monotonosti*):

Za svako $g \in G$ preslikavanja

$$x \in G \rightarrow g+x$$

$$x \in G \rightarrow x+g$$

jesu *monotona* tj. zadovoljavaju uslovu

$$x \leq x' \Rightarrow g+x \leq g+x' \wedge x+g \leq x'+g.$$

Na sličan se način definira uređena polugrupa, uređena kvazigrupa (pogl. 17, § 8.8), *uređena pseudogrupa* (pogl. 17, § 8.9), *uređena grupa* (isp. pogl. 17, § 8.4)): umjesto uslova grupoida dolazi odgovarajući uslov polugrupe, kvazigrupe, pseudogrupe, grupe.

8.4.1. Primjedba. Ako je neki skup G grupoid $(G, +)$ i uređen kao $(G, \leq)$, tada to još ne znači da je $(G, +, \leq)$ *uređen grupoid*; tu se samo radi o *uređenju grupoida* $(G, +)$; no to uređenje ne mora biti vezano sa zadanom operacijom $+$ uslovom monotonosti.

8.4.2. Primjedba. Skup $(G, \leq)$ može biti *posve* (*lančasto*) *uređen* ili samo djelomično uređen. Ako su x, x' neusporedivi članovi grupoida $(G, +, \leqslant)$, tada, ipak, za neko $g \in G$ članovi $g+x$, $g+x'$ mogu biti usporedivi.

8.5. Pozitivni (negativni) članovi. Ako je uređen grupoid snabdjeven neutralnim članom 0 pa ako pri $g \in G$ vrijedi $0 < g$ (odnosno $g < 0$), onda se kaže da je g *pozitivno* (odnosno *negativno*); tada sa $G(0, \cdot)$ (odnosno $G(\cdot, 0)$) označujemo skup svih pozitivnih (negativnih) članova uređena grupoida.

Posebno u svakoj uređenoj grupi imamo skup pozitivnih članova, skup negativnih članova te skup sastavljen od 0 i od svih članova grupe koji su s 0 neusporedivi; ta su tri skupa dva po dva disjunktna.

8.5.1. Primjer. Skup rednih prirodnih brojeva 0, 1, 2, ... je uređena polugrupa bez ikojeg negativnog elementa. Skup cijelih (racionalnih, realnih) brojeva je određena posve uređena aditivna (zbrojidbena) grupa.

8.5.2. Primjer. Skup R svih realnih brojeva >0 je *multiplikativna* uređena grupa u kojoj „pozitivni" (negativni) članovi jesu rješenja relacije $x > 1$ (odnosno $x < 1$); riječ je o uređenju po veličini.

8.5.3. Primjer. Skup $R(i)$ svih kompleksnih brojeva je uređena aditivna grupa stavljajući $a+bi \leq c+di$ onda i samo onda ako je $a \leq c \wedge b \leq d$.

8.6. Nekoliko teorema.

8.6.1. Lema. *Ako je* $(G, +, \leqslant)$ *uređena grupa, tada* $0<g\in G \Rightarrow 0>-g$; *isto tako* $0>h\in G \Rightarrow 0<-h$. *Nadalje, pri* $\{x, x'\}\subset G$ i $g\in G$:

$$(0) \qquad \begin{cases} x<x' \Rightarrow g+x<g+x' \\ x<x' \Rightarrow x+g<x'+g \end{cases}.$$

Naime iz

$$(1) \qquad 0<g$$

izlazi prema uslovu 8.4 (*iii*) o monotoniji da je

$$(2) \qquad -g+0\leq -g+g;$$

no, tu umjesto znaka $\leq$ ne može stajati znak $=$, jer iz $-g+0=-g+g$ izlazi dodavajući lijevo g:

$$g+(-g+0)=g+(-g+g), \text{ i dalje } (g+(-g))+0=$$
$$=(g+(-g))+g, \text{ tj. } 0+0=0+g, \text{ tj. } 0=g, \text{ protivno s (1).}$$

Dakle (2) glasi

$$-g+0<-g+g, \text{ tj. } -g<0, \text{ tj. } 0>-g.$$

Slično se dokazuju veze (0).

⟶ **8.6.2.** Teorem. *Ako uređen grupoid* $(G, +, \leqslant)$ *ima neutralni član* 0, *tada iz* $0<g\in G$ ili $0>g\in G$ *izlazi da je niz*

$$(1) \qquad g, 2g, 3g, \ldots, ng, \ldots$$

uzlazan pri $g>0$, *a silazan pri* $g<0$;

dakle je skup $Ng=\{g, 2g, 3g, \ldots\}$ *lanac.*

U slučaju da je taj grupoid grupa, niz (1) *je čisto uzlazan pri* $g>0$, *a čisto silazan pri* $g<0$, *pa je skup* Ng *beskonačan lanac.*

Dokaz. Neka je npr. $0<g$; odatle prema uslovu 8.4 (*iii*) o monotoniji izlazi $0+g\leq g+g$, tj. $g\leq 2g$; odatle na isti način $g+g\leq 2g+g$, tj. $2g\leq 3g$, itd.

U slučaju da je $(G, +)$ grupa, tada prema (0) u 8.6.1 iz $0<g$ nužno izlazi $g<2g$, a odatle dalje iz istog razloga $g+g<2g+g$, tj. $2g<3g$, itd. induktivno $ng<(n+1)g$ za svako $n\in N$.

8.6.3. Posljedica. Uređena grupa $(G, +, \leqslant)$ je posve (linearno) uređena onda i samo onda ako je svako $g\in G$ usporedljivo sa 0.

8.6.4. Teorem. Svaka posve ili linearno uređena grupa G je bez torzije (pogl. 17, § 7.10).

Naime, teorem iskazuje da iz $0\neq g\in G$ izlazi da je skup

$$Dg=\{dg;\ d\in D\}$$

beskonačan. No, zbog linearne uređenosti od $(G, \leqslant)$ izlazi da je ili $g<0$ ili $g>0$. Zato prema 8.6.2. izlazi da je skup Ng a tim prije skup Dg beskonačan.

8.6.5. Teorem. *Ako je uređena grupa* $(G, +, \leqslant)$ *periodična, tada je* $(G, \leqslant)$ *antilanac, tj. za svaka dva različna člana* a, b *iz* G *vrijedi* $a \| b$ *u smislu da nije ni* $a<b$ *ni* $b<a$.

Kad bi naime postojala dva različna usporedljiva člana a, b u G, tada bi član $g=a-b$ bio >0 ili <0, već prema tome da li je $a>b$ ili $a<b$; pa bi skup Ng bio beskonačan, protivno pretpostavci da je grupa periodična (isp. pogl. 17, § 7.10).

⟶ **8.6.6.** T e o r e m. *Ako je* $(G, +, \leqslant)$ *uređena grupa, tada je skup*

$$P=G[0, \cdot]=\{x;\ x\in G,\ x\geq 0\}$$

podpolugrupa P od $(G, +)$ s ova 3 svojstva:

(i) $\quad 0\in P$;

(ii) $\quad p\in P\wedge -p\in P \Rightarrow p=0$, tj. $P\cap -P=\{0\}$;

(iii) $\quad g\in G,\ p\in P \Rightarrow -g+p+g\in P$.

I obratno: obuhvata li grupa G neku polugrupu P sa svojstvima (i), (ii), (iii) tada definirajući

$$(1) \qquad a\leq b \Leftrightarrow b-a\in P,$$

dobijamo uređenu grupu $(G, +, \leqslant)$ *za koju je* $G[0, \cdot)=P$.

Dokaz teorema 8.6.6 provodi se neposredno primjenom leme 8.6.1, odnosno uslova monotonije. Dokažimo npr. da polugrupa P uređene grupe $(G, +, \leq)$ zadovoljava (iii). No iz $x\geq 0$ izlazi $x+g\geq 0+g$, tj. $x+g\geq g$; odatle dalje zbog monotonije izlazi $-g+(x+g)\geq -g+g$, tj. $-g+x+g\geq 0$.

Slično se dokazuje i drugi dio teorema: relacija $\leq$ definirana pomoću (1) u grupi $(G, +)$ je uređajna, zadovoljava uslovu monotonije prema $+$ te uslov da je P upravo skup svih $x\in G$ za koje je $0\leq x$.

8.6.7. T e o r e m. *Ako grupa* $(G, +)$ *obuhvata neku polugrupu* P *sa svojstvima* 8.6.6 (i)—(iii) *te za koju je* $G=P\cup(-P)$ tada je $(G, \leqslant)$ *lanac; pri tom definiramo* $a\leq b \Leftrightarrow b-a\in P$.

Teorem je neposredna posljedica drugog dijela teorema 8.6.6, teorema 8.6.1. i posljedice 8.6.3.

8.7. Maksimalna ili završna uređenost grupe. Svaka grupa $(G, +)$ se naravno može shvatiti uređenom pri *minimalnom* uređenju pri kojem je G *antilanac* (dakle bez različnih usporedljivih članova). To je slučaj kad je polugrupa P iz teorema 8.6.6 sastavljena od 0.

No, neka je $U(G)$ skup svih polugrupa $(P, +)\subset(G, +)$ koje zadovoljavaju uslovima 8.6.6 (i), (ii), (iii). Tako dobijemo uređen skup $(U(G), \subset)$, pa za svako $P\in(UG, \subset)$ imamo odgovarajuću uređenu grupu $(G, +, <_P)$; ako su P, Q dva člana iz UG tada pri $P\subset Q$ vrijedi

$$g<_P g' \Rightarrow g<_Q g',$$

pa uređenje $<_Q$ proširuje uređenje $<_P$ grupe $(G, +)$. Pri tom vrijedi.

8.7.1. D e f i n i c i j a. Uredimo li neki skup S relacijom $\leq_1$, i relacijom $\leq_2$, tada se kaže da *uređenje* $(S, \leq_2)$ *raširuje* (*produžuje*) *uređenje* $(S, \leq_1)$, *ako*

$$s, s'\in S\wedge s\leq_1 s' \Rightarrow s\leq_2 s';$$

to je *raširenje stvarno* ako uređenje $(S \leq_2)$ sadrži najmanje jedan par usporedljivih tačaka koje su u uređenju $(S, \leq_1)$ neusporedljive.

No, ako je L *lanac* iz $(UG, \subset)$, tada očigledno i unija $\cup L$ svih članova iz L član je u UG; posebno, ako je L *maksimalan lanac* od $(U(G), \subset)$, tada je $\cup L$ *završni član u* $(UG, \subset)$, *pa se odgovarajuće uređenje grupe više ne može proširiti: uređenje je završno ili maksimalno.* No, postojanje maksimalnih lanaca u svakom uređenom skupu je posljedica aksioma izbora (v. Đ Kurepa [1] str. 172). Dakle vrijedi

8.7.2. Teorem. *Svaka grupa dopušta bar jedno završno (maksimalno) uređenje; općenito ono nije lančasto.*

Naravno, jedna te ista grupa može imati više završnih uređenja. Nastaje ovaj

8.7.3. Problem. *Što je nužno i dovoljno pa da bar neko (svako) završno, maksimalno uređenje zadane (uređene) algebarske strukture bude lanac?*

U općem slučaju, prethodni problem još nije riješen; no riješen je za grupe i prstene (v. t. 8.7.5 i t. 8.9.4)). Posebno, kao zaključak radova više matematičkih radnika (F. Levi, Šimbireva, L. Fuchs) dokazat ćemo teorem 8.7.5 Japanca Ohnishi-ja.

8.7.4. *Polugrupa* P_g. Neka je $(G, +)$ grupa i $g \in G$; neka P_g označuje presjek svih polugrupa P sa svojstvima 8.6.6 (i) — (iii) i $g \in P$ ukoliko postoji bar jedno $P \ni g$; ako takvo P ne postoji neka P_g bude prazan skup.

⟶ **8.7.5.** Teorem. (Masao Ohnishi, Osaka Math. J. 2 (1950) 161—164). Neka je $(G, +)$ grupa. Svako maksimalno uređenje $(G, +, \leq)$ grupe $(G, +)$ je lančano onda i samo onda ako su ispunjena ova dva uslova:

(0) Za svako $g \in G$ polugrupa $P \ni g$ postoji;

(00) $$g \in G \wedge \{x, y\} \subset P_g \setminus \{0\} \Rightarrow P_x \cap P_y \neq \{0\}.$$

8.7.5.1. *Uslovi teorema su potrebni: ako je svako neraširivo uređenje grupe lančasto, tada su uslovi* (0), (00) *na snazi.*

Pa neka je $(G, +, \leq)$ lančano uređena grupa, a P skup svih $x \in G$ za koje je $x \geq 0$. Tada je $G = P \cup (-P)$; a kako i P i $-P$ zadovoljavaju uslov 8.6.6 (i)—(iii)), uslov 8.7.5 (0) je ispunjen. Dokažimo da je ispunjeno i 8.7.5 (00). Pretpostavimo da (00) ne vrijedi nego da za neke $g, x, y \in G$ imamo $(00)_1$ kao i

(1') $$P_x \cap P_y = \{0\}.$$

Neka je tada $P_x - P_y = P$; i to P zadovoljava uslove 8.6.6 (i)—(iii); (v. 8.7.5.2); posebno je $x = x - 0 \in P$ kao i $-y = 0 - y \in P$; odatle $y \in -P$.

Zato zbog (00) imamo

(1) $$0 \neq x \in P_g \cap -P \vee 0 \neq y \in P_g \cap -P.$$

No, uređenje izazvano polugrupom P može se prema pretpostavci raširiti na lančasto uređenje nekom polugrupom $P' \supset P$. Zato je $G = -P' \cup P'$, pa je specijalno za ono g iz $(00)_1$

$$g \in -P' \vee g \in P'$$

$$P_g \subset -P' \vee P_g \subset P'$$

$$(2) \qquad P_g \cap P' \subset -P' \cap P' = \{0\} \vee P_g \cap -P' \subset P' \cap -P' = \{0\};$$

kako je $P \subset P'$, $-P \subset -P'$, relacije (1) i (2) bi dale

$$x \in \{0\} \vee y \in \{0\},$$

što je u protuslovlju sa (00). Time je svojstvo 8.7.5 (00) dokazano.

8.7.5.2. Lema. *Neka je* $(G, +)$ *grupa a* UG *skup svih podpolugrupa* $(P, +)$ *te grupe za koje vrijede uslovi* 8.6.6 *(i)—(iii). Tada*

$$(1) \qquad P, Q \in U(G) \wedge P \cap (-Q) = \{0\} \Rightarrow P + Q \in U(G).$$

Dokažimo najprije da je $P+Q$ grupoid (a time i podpolugrupa): iz $p+q \in P+Q$, $p'+q' \in P+Q$ izlazi $(p+q)+(p'+q') \in P+Q$ jer je

$$(2) \qquad (p+q)+(p'+q') = (p+[q+p'-q]) + (q+q') \text{ i } q+p'-q \in P.$$

Jasno je da je $0 \in P+Q$ i $(P+Q) \cap (-(P+Q)) = \{0\}$.
Pokažimo svojstvo 8.6.6 *(ii)*:

$$(3) \qquad x, \ -x \in P+Q \Rightarrow x = 0.$$

Najprije

$$(4) \qquad p+q=0 \Rightarrow p=0=q.$$

Naime,

$$p+q=0 \Rightarrow p=-q \Rightarrow p \in P \wedge p \in -Q \Rightarrow \text{(prema pretpostavci leme)}$$

$$p=0 \Rightarrow q=0.$$

Nadalje, neka (5) $p+q$, $-(p+q) \in P+Q$ dakle $-(p+q) = p'+q'$ dakle

$$0 = (p+q)+(p'+q') = (p+[q+p'-q]) + (q+q') \Rightarrow \text{(prema (4))}$$

$$p+[q+p'-q] = 0 = q+q'.$$

Dakle $q, q' = -q \in Q$, tj. prema uslovu 8.6.6 *(ii)* je $q=0$, dakle $q'=0$, dakle $p+[0+p'-0]=0$, tj. $p+p'=0$ i dalje radi 8.6.6 *(ii)* $p=p'=0$.

Dakle zaista (5) $\Rightarrow p+q=0$, što znači da je (3) ispravno.
Dokažimo i 8.6.6 *(iii)* za $P+Q$:

$$-g+p+q+g = (-g+p+g)+(-g+q+g) = p'+q' \in P+Q.$$

8.7.5.3. *Uslovi teorema* 8.7.5 *su dovoljni: ako su ispunjeni uslovi* (0), (00), *tada je svako završno uređenje grupe* $(G, +, \leq)$ *lančasto.*

Pa neka polugrupa $(P, +)$ daje završno uređenje $(G, +, \leq)$ tako da bude $P = G[0, \cdot)$. Kad to uređenje ne bi bilo lančasto, postojao bi prema 8.6.7 neki član $g \in G \setminus (P \cup -P)$. Promatrajmo sada P_g iz uslova (0) i skup $P_g \cap P$.

Prvi slučaj: $P_g \cap P = \{0\}$. Dakle je $-P_g \cap -P = \{0\}$, tj. $P_{-g} \cap -P = \{0\}$ (jer je $-P_g = P_{-g}$). Po lemi 8.7.5.2 zaključujemo da bi bilo $P_{-g} + P \in U(G)$, pa bi taj član od $U(G)$ obuhvatao P kao i $-g$ koje nije u P; međutim, to se protivi pretpostavci da je P završni član u uređenom skupu $(U(G), \subset)$.

Drugi slučaj: $P_g \cap P \neq \{0\}$; tada je nužno $-P_g \cap P = \{0\}$ (v. 8.7.5.4), tj. $P_{-g} \cap P = \{0\}$; prema lemi 8.7.2 zaključujemo da bi bilo

$$P \subsetneq P + P_g \in U(G),$$

protivno pretpostavci da je P završni član u $(U(G), \subset)$).

8.7.5.4. Lema.

Neka je $(G, +)$ *grupa; tada za svako* $g \in G$, $P \in U(G)$ *imamo*

$$P \cap P_g \neq \{0\} \Rightarrow P \cap P_{-g} = \{0\} \tag{1}$$

(oznake su kao u 8.7.4, 8.7.5.2).

Pretpostavimo da (1) ne stoji; to znači da bi postojali članovi

$$x \in P \cap P_g \setminus \{0\}, \qquad y \in P \cap P_g \setminus \{0\}; \qquad \text{odatle}$$

$$\{-x, y\} \subset P_{-g} \setminus \{0\},$$

pa po uslovu (00)

$$P_{-x} \cap P_y \neq 0. \tag{2}$$

No kako je $-x \in -P$, dakle $P_{-x} \subset -P$ te $P_y \subset P$ bilo bi

$$P_{-x} \cap P_y \subset -P \cap P, \text{ što s (2) daje } \{0\} \neq -P \cap P;$$

a to je u protivurječju s uslovom 8.6.5 (*ii*).

8.7.7. Teorem. (*E. P. Šimbireva; Mat. Sbornik, Moskva* 20 (1947) 145—178).

Svako neraširivo uređenje svake komutativne grupe bez torzije je lančasto.

Naime, svaka takva grupa zadovoljava oba uslova (0), (00) iz § 8.7.5, jer je $P_0 = \{0\}$, $P_g = \{0g = 0, g, 2g, 3g, \ldots\}$ za svako $g \in G \setminus \{0\}$; posebno, tada $\{x, y\} \subset P_g \setminus \{0\}$ daje $x = mg$, $y = ng$ za neke prirodne brojeve m, n; prema tome $0 \neq gmn \in P_x \cap P_y$, tj. uslov 8.7.5 (00) je na snazi.

8.7.7.1. Teorem. (*F. Levi, Rendiconti Palermo* 35 (1913), 225—236).

Svaka komutativna grupa bez torzije dopušta lančasto uređenje.

8.8. Arhimedove uređene grupe.

8.8.1. Definicija. Lančasto uređena grupa $(G, +, \leq)$ je Arhimedova ako zadovoljava ovaj

8.8.2. *Arhimedov postulat. Za svaku dvojku pozitivnih članova a, b grupe postoji neki prirodni broj n (zavisan od a, b) sa svojstvom*

$$na > b.$$

Uloga Arhimedova postulata je vrlo velika u teoriji mjerenja i u primjenama. Sad ćemo dokazati jedan teorem koji nam kazuje kako je Arhimedov postulat veliko ograničenje.

Sl. 32.8.8.2. Arhimed

⟶ **8.8.3. Teorem.** (*O. Hölder [1859-1937]; 1901*).[1] ***Svaka lančasto uređena Arhimedova grupa (G, +) je komutativna i izomorfna s nekom podgrupom grupe (R, +) realnih brojeva koji su uređeni po veličini.***

Promatrajmo skup $G(0, \cdot)$ svih pozitivnih članova grupe.

8.8.3.1. Prvi slučaj; *skup* $G(0, \cdot)$ *ima prvi član*, npr. a; tada za svako $a \le g \in G$ postoji prirodan broj $n = n(a, g)$ za koji je

$$na \le g < (n+1)\,a, \qquad \text{tj.}$$

$$0 \le g - na < a;$$

odatle, po definiciji članova a, n izlazi

$$0 = g - na, \quad \text{tj.} \quad g = na;$$

prema tome, promatrana grupa bila bi izomorfna sa grupom $(D, +, \leqslant)$ cijelih brojeva, jer je preslikavanje

$$n \in D \to na \in G$$

izomorfizam ili sličnost.

---

[1] O. Hölder, *Leipziger Ber.* 53 (1901), 1—64, posebno str. 13—14.

8.8.3.2. Drugi slučaj: *Skup* $G(0, \cdot)$ *nema prvog člana*, tj. svakom $0<g\in G$ pridruženo je bar jedno $x\in G$ za koje je $0<x<g$, dakle $0<-x+g$. Naravno, x zavisi od g. Dokažimo da se može tražiti da bude također

(1) $$2x\leq g.$$

Ako već nađeno x zadovoljava (1), stvar je gotova; a ako je slučajno $2x>g$, dakle $0>-x+g-x$ dakle $0+g>(-x+g)+(-x+g)$, onda $y=-x+g$ zadovoljava i (1) i $0<y<g$.

8.8.3.2.0. *Dokažimo da je grupa komutativna*; naravno da je dovoljno dokazati da je

(2) $$a+b=b+a \quad \text{za} \quad a, b\in P=G[0, \cdot);$$

komutator od a, b je

$$k=[a, b]=a+b-a-b$$

pa je zato dovoljno dokazati da je $k=0$ (isp. 17, § 18.1). Inače bi bilo $k\neq 0$, dakle $k>0$ ili $k<0$; obradimo slučaj $k>0$, jer bi inače bilo dovoljno umjesto k promatrati $-k$. No iz $0<k$ upravo zaključismo da postoji $x\in G$ za koje je

(3) $$0<x<k, \quad 2x\leq k;$$

iz istog razloga možemo pretpostaviti da je $x<a$, $x<b$ jer je G lančasto.

Kako grupa zadovoljava Arhimedovu postulatu, postojat će prirodni brojevi m, n za koje je

$$mx\leq a<(m+1)x, \qquad nx\leq b<(n+1)x$$

dakle

$$a+b<(m+n+2)x$$

$$-a-b\leq -(m+n)x;$$

odatle zbrajanjem:

$$(a+b)-a-b<2x, \quad \text{tj.} \quad k<2x,$$

u protivnosti sa (3).

8.8.3.2.1. Dokažimo sada da se izborom proizvoljna člana $e\in G(0, \cdot)$ može svako $g\in G$ prikazati u obliku $g=x_g e$, pri čemu je x_g određen realan broj (nazvan *apscisa člana* g). Najprije ćemo pretpostaviti da je $g>0$. Neka je pri $0<g$

(4) $$Q_g=\left\{\frac{m}{n}\,;\ m, n\in N,\ me\leq ng\right\}.$$

Dokažimo da iz $q\in Q_g$ i $q'\leq q$ izlazi $q'\in Q_g$. Neka je naime

$$q=\frac{m}{n},\ q'=\frac{m'}{n'} \text{ dakle } m'n\leq mn', \text{ dakle } (m'n)e\leq(mn')e$$

dakle

$$m'ne\leq n'me\leq n'ng, \quad \text{jer je } me\leq ng.$$

Dakle je $m'ne\leq n'ng$, a time i $m'e\leq n'g$ tj. $q'=\dfrac{m'}{n'}\in Q_g$.

S druge strane, ako vrijedi Arhimedov postulat, to će za neko $m \in N$ biti $me > g$ dakle $\frac{m}{1}$ non$\in Q_g$, tj. $m \in Q(0, \infty) \setminus Q_g$.

Zato je specijalno $\sup Q_g$ određen realan broj koji je potpuno određen elementom g (pri fiksnom e); tako se dobije preslikavanje

(5) $$g \in G \to I(g) := \sup Q_g \in Q.$$

Dokažimo da iz $g \leq g'$ izlazi $I(g) \leq Ig'$. Naime ako je $me \leq ng$, tada je pogotovo $me \leq ng'$, tj. $\frac{m}{n} \in Q_{g'}$, tj. $Q_g \subset Q_{g'}$, tj. $Ig \leq Ig'$. Odmah ćemo vidjeti da iz $g < g'$, izlazi $Ig < Ig'$, tako da je *preslikavanje* (5) *čisto uzlazno*. To je očigledna posljedica relacije

(6) $$I(g+g') = Ig + Ig', \quad Ig > 0 \text{ pri } g > 0.$$

Dokažimo (6). Neka je $q = \frac{m}{n} \in Q_g$, $q' = \frac{m'}{n'} \in Q_{g'}$; dakle je

$$n' \cdot |me \leq ng, \; m'e \leq n'g'| \cdot n$$

$$mn'e \leq nn'g, \; m'ne \leq nn'g';$$

zbrajajući: $mn'e + m'ne \leq nn'g + nn'g' =$ (zbog dokazane komutativnosti) $= nn'(g+g')$, tj. $\frac{mn'+m'n}{nn'} \in Q_{g+g'}$, dakle $\frac{m}{n} + \frac{m'}{n'} \in Q_{g+g'}$.

I odatle $Q_g + Q_{g'} \subset Q_{g+g'}$.

Prelazeći na supreme dobijemo

(7) $$I_g + I_{g'} \leq I_{(g+g')}.$$

Na dualan način (zamjena $\leq \leftrightarrow \geq$) dokazuje se relacija

$$Q(I_g, \infty) + Q(I_{g'}, \infty) \subset Q(I_{(g+g')}, \infty)$$

što s relacijom

$$Q(I_g, \infty) + Q(I_{g'}, \infty) = Q(I_g + I_{g'}, \infty)$$

daje

$$Q(I_g + I_{g'}, \infty) \subset Q(I_{(g+g')}, \infty);$$

odatle izlazi

(8) $$I_g + I_{g'} \geq I_{(g+g')}.$$

Iz (8) i (7) izlazi i tražena linearnost (6).

Stavimo $x_0 = 0$ te $x_g = x_{-g}$ pri $g < 0$; tada se vidi da preslikavanje $g \in G \to x_g$ preslikava izomorfno uređenu grupu $(G, +, \leq)$ na neku podgrupu grupe $(R, +, \leq)$.

Time je Hölderov teorem dokazan.

8.9. Uređen prsten (uređeno kolo). Uređeno tijelo.

8.9.1. Definicija. *Uređen prsten* ili *uređeno kolo* je svaki prsten (kolo) $(A, +, \cdot)$ u kojem je definirano neko uređenje $\le$ sa svojstvom da $(A, +, \le)$ bude uređena grupa u kojoj je skup svih članova koji su ≥ 0 zatvoren u odnosu na drugu operaciju („množenje") tj.

(1) $$0 \le a \in A \wedge 0 \le b \in A \Rightarrow ab \ge 0.$$

Slično se definira uređeno tijelo $(K, +, \cdot, \leqslant)$.

Tada se govori: o uređenom prstenu $(A, +, \cdot, \le)$, o skupu $A(0, \cdot)$. pozitivnih članova, o skupu $A(\cdot, 0)$ negativnih članova, o uređenoj grupi $(A, +, \le)$, o uređenom grupoidu $(A[0, \cdot), \le)$ itd.

8.9.1.1. Primjedba. Skup pozitivnih članova ne mora biti grupoid u odnosu na množenje; ali ako je prsten bez djelitelja nule, tada je grupoid i $(A(0, \cdot), \cdot)$ a ne samo $(A[0, \cdot), \cdot)$.

Elemente od A označivat ćemo u ovom dijelu sa $a, a', \ldots b, c, \ldots$

8.9.1.2. Teorem. (isp. § 8.6.6.). *Ako je* $(A, +, \cdot \leqslant)$ *uređen prsten, tada je* $P = A[0, \cdot)$ *podpolugrupa od* $(A, +)$ *s ova 3 svojstva:*

(*i*) $P \cap -P = \{0\}$,

(*ii*) $-A + P + A \subset P$,

(*iii*) $PP \subset P$.

I obrnuto, obuhvata li grupa $(A, +)$ *neku polugrupu* $(P, +)$ *sa svojstvima* (*i*), (*ii*), (*iii*), *tada definirajući* $\le$ *pomoću*

$$a \leqq b \Leftrightarrow b - a \in P$$

dobijemo uređen prsten $(A, +, \cdot, \leqslant)$ *za koji je* $P = A(0, \cdot)$.

Dokaz teorema je neposredan.

8.9.2. Teorem o množenju u uređenom kolu.

(1) $$a \ge 0 \wedge b \le 0 \Rightarrow ab \le 0 \qquad (\textit{te naravno } ba \le 0);$$

(2) $$a \le 0 \wedge b \le 0 \Rightarrow ab \ge 0.$$

Specijalno

(3) $$c > 0 \wedge a \le b \Rightarrow ca \le cb$$

(4) $$c < 0 \wedge a \le b \Rightarrow ca \ge cb.$$

Uvijek je $a^2 = (-a)^2 \ge 0$.

Ako je prsten bez djelitelja nule, tj. ako $a \ne 0 \wedge b \ne 0 \Rightarrow ab \ne 0$ tada u (1)—(4) treba provesti supstituciju $\le \to <$, $\ge \to >$.

Teorem je posljedica teorema 32, § 3.2 te zaključka

$$a \ge 0 \Leftrightarrow -a \le 0, \quad -(-a) = a.$$

8.9.2.1. Primjedba. U uređenu prstenu $(A, +, \cdot, \leq)$ zakon monotonije vrijedi za prvu operaciju $+$, ali ne vrijedi za drugu operaciju $\cdot$, pa čak ne mora vrijediti ni u skupu $A(0, \cdot)$. Zato u uređenom prstenu naglasak je više na vezi između $\leq$ i $+$ nego na vezi između $\cdot$ i $\leq$. Tako npr. uređeno tijelo je arhimedsko onda ako je ono arhimedsko u odnosu na $+$ (a ne nužno u odnosu na $\cdot$).

8.9.3. Teorem. *Svaki lančasto uređeni prsten s jedinicom* 1 *sadrži podprsten D* 1 *koji je i uređajno sličan i izomorfan s uređenim prstenom* $(D, +, \cdot, \leq)$ *svih cijelih racionalnih brojeva; zato je svaki takav prsten karakteristike* 0. *Ako je* $(D, +, \cdot, \leq_1)$ *bilo koji lančasto uređen prsten, tada su uređeni skupovi* $(D, \leqslant)$, $(D, \leq_1)$ *slični, a identično preslikavanje je jedini sličnosni izomorfizam između* $(D, +, \cdot, \leq)$ *i* $(D, +, \cdot, \leq_1)$.

Dokaz je jednostavan!

Kao rezultat niza radova (E. Artin — O. Schreier, *Abh. Math. Sem.* Hamburg, 5 (1926) 83—115; E. Serre, C. r. Paris 229 (1949) 576—7; T. Szele, Proc. Amer. Math. Soc. 3 (1952) 410—413; R. E. Johnson, ibidem 414—416; V. D. Poderjugin, Uspjehi mat nauk, Moskva 9: 4 (1954) (211—216) imamo ovaj

—→ **8.9.4. Teorem.** ***Prsten A je lančasto uređen prsten bez djelitelja nule onda i samo onda ako je različna od nule svaka suma od konačno mnogo sumanada od kojih je svaki sumand produkt tzv. „parnog sloga" s proizvoljnim rasporedom zagrada*** (to je važno za slučaj da prsten nije asocijativan). Pritom radi kratkoće neka je na snazi ova

8.9.4.1. Definicija. *Parni slog zadanih članova* je bilo koji konačni niz kojemu su članovi $\neq 0$ i to tako da se svaki član sloga pojavljuje *paran* broj puta kao član toga sloga.

8.9.4.2. *Uslov teorema* 8.9.4 *je nuždan.* Neka je S proizvoljan paran slog; dakle je i broj članova niza S paran broj, $2n$; nizu S pridružit ćemo niz S' i to tako da svaki eventualni član S_n koji je <0 nadomjestimo sa $-S_n$. Kako je slog paran, jasno je da je $\prod S_n = \prod S_n'$ i da je taj produkt >0 jer je prsten bez nuladjelitelja. Isto tako će biti i suma takvih članova $\neq 0$.

Uslovi teorema 8.9.4. *su dovoljni.* To će izaći iz činjenicâ 8.9.4.3 - 8.9.4.9.

8.9.4.3. Lema. *Prsten je bez djelitelja nule*:

$$a \in A \setminus \{0\},\ b \in A \setminus \{0\} \Rightarrow ab \neq 0.$$

Inače bi bilo $ab = 0$ dakle također $(ab)(ab) = 0$, protivno uslovu o parnom slogu.

Dokažimo da *se prsten može snabdjeti lančanim uređenjem.*

U tu svrhu ćemo dokazati da postoji maksimalna polugrupa P koja će poslužiti kao skup članova ≥ 0.

8.9.4.4. *Definicija A'-skupa. Skup* A_P.

Nazovimo *A'-skupom* svaki podskup $X \subset A \setminus \{0\}$ sa svojstvima:

α) $$x \in X \Rightarrow -x \operatorname{non}\in X;$$

β) neka $x_1, x_2, \ldots, x_k \in X$, $a_1, a_2, \ldots, a_n \in A \setminus \{0\}$, $\{n, k\} \subset \{0, 1, 2, \ldots\}$ i $k+n>0$; neka je σ proizvoljna suma proizvoljna sloga svih tih elemenata; tada postoji bar jedna supstitucija t

$$a_\nu \to ta_\nu \in \{+a_\nu, -a_\nu\} \quad (\nu = 1, 2, \ldots, n) \tag{1}$$

sa svojstvom da pri toj supstituciji σ postane $t\sigma \neq 0$, (ako je npr. $\sigma \neq 0$ tada je dovoljno staviti $a_\nu \to a_\nu$).

Skup A_P definiramo kao onaj koji je sastavljen od svih A'-podskupova prstena A.

8.9.4.5. Lema. *Iz* $Z \in A_P$ *i* $0 \neq -a, a$, $\{-a, a\} \cap Z = \emptyset$ *izlazi da je bar jedan od skupova* $Z \cup \{a\}$, $Z \cup \{-a\}$ *član od* A_P.

Pretpostavimo da nije $Z \cup \{a\} \in A_P$ niti $Z \cup \{-a\} \in A_P$; onda to znači da postoje neki članovi σ_1, σ_2 iz A koji su građeni poput sume σ u uslovu β) pri izboru

$$x_1 = z_1^{(i)} \ldots, \; x_{k_i} = z_{k_i}^{(i)}, \; x_{k_{i+1}} = (-a)^i, \; (i = 1, 2), \tag{2}$$

za x-ove is uslova β), te $a_\nu = a_{\nu_i}^{(i)} \in A \setminus \{0\}$ $(i = 1, 2)$, i da za svaku odgovarajuću supstituciju t_i bude $t_i \sigma_i (z_1^{(i)} \cdot \cdot z_{k_i}^{(i)}, (-1)^i a, a_1^{(i)}, \ldots, a_{\nu_i}^{(i)} = 0$ pri $i \in \{1, 2\}$. No, tada bi $\sigma_1 (z_1^{(1)}, \ldots, z_{k_1}^{(1)}, a, a_1^{(1)}, \ldots, a_{\nu_1}^{(1)}) \cdot \sigma_1 (z_1^{(1)}, \ldots, z_{k_1}^{(1)}, -a, a_1^{(1)}, \ldots, a_{\nu_1}^{(1)}) \cdot \sigma_2 (z_1^{(2)}, \ldots, z_{k_2}^{(2)}, a, a_1^{(2)}, a, a_1^{(2)}, \ldots, a_{\nu_2}^{(2)})$. $\sigma_2 (z_2^{(2)}, \ldots, z_{k_2}^{(2)}, -a, a_1^{(2)}, \ldots, a_{\nu_2}^{(2)})$ bilo odgovarajuće $\sigma = \sigma (z_1^{(1)}, \ldots, z_{k_1}^{(1)}, z_1^{(2)}, \ldots, z_{k_2}^{(2)}; a, a_1^{(1)}, \ldots, a_{\nu_1}^{(1)}, a_1^{(2)}, \ldots, a_{\nu_2}^{(2)})$ pri izboru članova (2) za $x_1 \cdots x_k$, odnosno pri izboru članova $a, a^{(i)} \cdots a_{n_i}^{(i)}$, $(i = 1, 2)$ za niz $a_1, \ldots a_n$ iz β), pa bi pri svakoj pripadnoj supstituciji t bilo $t\sigma = 0$, protivno pretpostavci da $Z \in A_P$ i da Z ispunjava β).

8.9.4.6. Lema. *Prazni skup je član od* A_P; *za svako* $a \in A \setminus \{0\}$ *vrijedi*

$$\{a\} \in A_P \vee \{-a\} \in A_P.$$

Drugi dio leme izlazi iz prvog dijela leme i leme 8.9.4.5. pri $Z = \emptyset$.

Zato je dovoljno dokazati

$$\emptyset \in A_P; \tag{3}$$

da to dokažemo, dovoljno je pokazati da uslov β) stoji. No, taj se uslov u tom slučaju svodi na izbor $k = 0$, $n \geq 1$ i članove

$$a_\nu \in A \setminus \{0\}, \; (\nu = 1, 2, \ldots, n), \tag{4}$$

i promatranje proizvoljne sume σ kojoj je svaki sumand neki produkt nekog sloga od tih a_ν. Kad ne bi bilo (3), tada bi za neko $\sigma = \sigma'$ pri svakoj transformaciji (1) bilo $t\sigma' = 0$. Odmah će nas ta pretpostavka dovesti do protivurječja time što ćemo izgraditi neko $\sigma = \bar{\sigma}$ za koje je $t\bar{\sigma} = 0$, i da pri tom svaki sumand od $\bar{\sigma}$ bude produkt „parnog sloga" članova (4). Konstrukcija od $\bar{\sigma}$ je postepena. Počnimo sa a_1; ako se a_1 pojavljuje (ne pojavljuje) u svakom (nikom) sumandu σ' neparan broj puta, onda ćemo promatrati $f_1 = \sigma' a_1$ kao sumu produkata sloga u kojem se a_1 pojavljuje paran broj puta (odnosno stavit ćemo $f_1 = \sigma'$), pa ćemo promatrati f_1 u odnosu na a_2.

Ako a_1 dolazi u bar jednom sumandu od σ' paran broj puta, a u nekom drugom sumandu neparan broj puta, neka je $\sigma' = \sigma_0' + \sigma_1'$, pri čemu je σ_0' (odnosno σ_1') suma svih sumanada od σ' u kojima se a_1 pojavljuje paran (neparan) broj puta.

Zamijenimo li a_1 sa $-a_1$ izlazi izraz $\sigma_0' - \sigma_1'$ koji isto kao i $\sigma' = \sigma_0' + \sigma_1'$ ostaje 0 pri svakoj supstituciji oblika (1); isto će svojstvo imati i suma $(\sigma_0' + \sigma_1') + (\sigma_0' - \sigma_1') = (\text{komutativnost!}) = 2\sigma_0'$. No, odgovarajući slog za $2\sigma_0'$ sadrži a_1 u svakom sumandu paran broj puta. Radeći sada sa $2\sigma_0'$ i članom a_2 dobije se analogna redukcija u odnosu na a_2; itd. Nakon n koračaja dolazi se na neku sumu $\bar{\sigma}$ traženog oblika; time smo u kontradikciji sa pretpostavljenim svojstvom prstena A.

8.9.4.7. Lema. *Ako je L proizvoljan lanac uređena skupa $(A_P, \subset)$, tada je* $\bigcup\limits_{X \in L} X \in A_P$. *Posebno to vrijedi ako je L maksimalan lanac.*

Dokaz je očigledan.

8.9.4.8. Lema. *Ako je L* **maksimalan** *lanac u $(A_P, \subset)$, tada je skup* $L_0 = \bigcup\limits_{X \in L} X$ *i aditivan i multiplikativan podgrupoid kola $(A, +, \cdot)$.*

Stvarno, *ako je $a, b \in L_0$, tada je $a + b \in L_0$.* Naime, $a + b \neq 0$ jer primjenom svojstava β) za slučaj $x_1 = a$, $x_2 = b$, $k = 2$, $n = 0$ suma $\sigma = a + b$ ne dopušta nikakve supstitucije (1) pa kad bi bilo $\sigma = a + b = 0$, bilo bi također $t\sigma = 0$, što se protivi sa svojstvom β). Dakle je zaista $\sigma = a + b \neq 0$.

No, ne može biti $-\sigma \in L_0$ jer bi inače bilo $a + b + \sigma = 0$, i taj izraz je 0 pri svakoj transformaciji oblika (1); a to se protivi svojstvu β) A'-skupa L_0. Dakle je $L_0 \in A_P$, $-(a+b) \operatorname{non} \in L_0$; znači da je $L_0 \cup \{a+b\} \in A_P$, tj. $a + b \in L_0$, jer bi inače $L = L_0 \cup \{a+b\}$ bio lanac u $(A_P, \subset)$ veći od maksimalnog lanca L_0.

Analogno, $$a, b \in L_0 \Rightarrow ab \in L_0.$$

Naime, $ab \neq 0$ jer je prsten bez djelitelja nule (v. 8.9.4.3). Kao i maloprije sa $a + b$ dokazuje se sada da je $-ab \operatorname{non} \in L_0$, i dalje $ab \in L_0$.

8.9.4.9. Lema. *Ako je L maksimalan lanac u $(A_P, \subset)$, tada se pomoću skupa* $P = \{0\} \cup L_0$, $\bigcup\limits_{X \in L} X = L_0$ *prsten $(A, +, \cdot)$ uređuje lančasto stavljajući*

$$a \leq b \Leftrightarrow b - a \in P.$$

Lema izlazi iz prethodne leme i teorema 8.9.1.2, jer na osnovu 8.9.4.5 zaključujemo da je $A = P \cup (-P)$.

Time je i dovoljni dio teorema 8.9.4 dokazan.

8.9.5. Teorem. *Prsten koji je komutativan i asocijativan je lančasto uređena oblast cijelih onda i samo onda ako je ta oblast formalno-realna u ovom smislu:*

τ) *Kvadrat svakog topa kao i suma od konačno mnogo kvadrata topova opet je top* [1]; *simbolički:*

---

[1] *Top prstena* znači ne biti jednak nuli (odnosno ne biti neutralni član prema zbrajanju).

$$x_\nu \neq 0 \Rightarrow \sum_{\nu=1}^{n} x_\nu^2 \neq 0, \quad (\nu=1, 2, \ldots, n;\ n \in \{1, 2, 3, \ldots\}).$$

Teorem je specijalan slučaj teorema 8.9.4; naime, zbog pretpostavljene komutativnosti i asocijativnosti produkt članova svakog „parnog sloga" je oblika x^2 (v. § 8.9.4.1).

Poseban slučaj od 8.9.5 je

8.9.5.1. Teorem. *Tijelo kompleksnih brojeva nije lančasto uređajno tijelo jer je u njemu* $1^2 + i^2 = 0$, *premda* $0 \notin \{1, i\}$.

⟶ **8.9.6. Teorem.** ***Svako formalno-realno komutativno tijelo*** **(isp. 32, § 6.1. (0))** $(K, +, \cdot)$ ***za koje je***

(1) $$-K^2 \cup K^2 = K$$

postaje lančano uređeno tijelo definirajući

(2) $$a \leq b \Leftrightarrow b - a \in K^2.$$

Naime, neposredno se provjeri da skup $P = K^2$ zadovoljava uslovima teorema 8.9.1.2. Provjerimo još da je $(K^2, +)$ grupoid. Pa neka je $a, b \in K^2$, tj. $a = x^2$, $b = y^2$ pri nekom $\{x, y\} \subset K$; možemo pretpostaviti da je

(3) $$x \neq 0 \neq y;$$

tada zbog uslova (1) imamo

$$x^2 + y^2 \in -K^2 \cup K^2, \text{ dakle } x^2 + y^2 \in -K^2 \text{ ili } x^2 + y^2 \in K^2;$$

prvi slučaj nije moguć jer bi to značilo da je

(4) $$x^2 + y^2 = -t^2, \quad t \in K^2;$$

kako je prema topovskom uslovu (τ): $x^2 + y^2 \neq 0$ dakle $-t^2 \neq 0$ mora biti $t \neq 0$ (jer se radi o prstenu, tijelu, dakle o strukturi u kojoj $t^2 \neq 0 \Rightarrow t \neq 0$). Množeći (4) sa t^{-1} izlazi $(xt^{-1})^2 + (yt^{-1})^2 = -1$, u protivnosti sa 6.1. (0). Zato je $x^2 + y^2 \in K^2$. Dakle je zaista $(K^2, +)$ grupoid.

Prema tome, relacijom $\leq$ postaje tijelo K-uređenim — međutim, to je uređenje čak lančasto jer zbog pretpostavke (1), ukoliko nije $a \leq b$, tj. ukoliko nije $b - a \in K^2$ bit će $b - a \in -K^2$, tj. $a - b \in K^2$ pa će znači biti $b \leq a$.

⟶ **8.9.7. Teorem.** ***Ako je*** $(I, +, \cdot, \leqslant)$ ***lančasto uređena oblast cijelih, tada se to uređenje na jednoznačan način prenosi na pripadno tijelo***

(1) $$(I^:, +, \cdot, \leq)$$

razlomaka i to propisom

(2) $$\frac{a}{b} < 0 \Leftrightarrow ab < 0;$$

time se dobije lančasto-uređeno tijelo $(I^:, +, \cdot, \leqslant)$.

D o k a z. Pretpostavimo da je tijelo $I^{:}$ lančasto uređeno pomoću neke relacije $<'$ koja proširuje $<$; pa neka je $0<\frac{a}{b}\in I^{:}$; dakle je $b\neq 0$, $0<b^2$, $0<'b^2$ pa je zato $0<'\frac{a}{b}\cdot b^2$, tj. $0<'ab$ dakle $0<ab$ (jer po pretpostavci relacija $<'$ podudara se sa $<$ u I).

S druge strane, ako je $ab<0$ u I, bit će $ab<'0$ što sa $0<'(b^{-1})^2$ daje $0<'ab\cdot\left(\frac{1}{b}\right)^2$, tj. $0<'ab^{-1}$. Dakle $0<ab \Rightarrow 0<'ab^{-1}$.

Time je dokazana jednoznačnost eventualnog lančastog uređenja od $I^{:}$, koje proširuje lančasto uređenje od I. Još preostaje da se provjeri da se propisom (2) tijelo (1) zaista uređuje lančasto, i posebno da

$$(0<'x)\wedge(0<'y) \Rightarrow (0<'x+y)\wedge(0<'xy) \text{ pri } \{x, y\}\subset I^{:}.$$

A to se dokazuje isto kao u slučaju $D^{:}$, tj. u slučaju racionalnih brojeva.

8.9.8. T e o r e m. *Ako lančasto uređen asocijativan prsten A zadovoljava Arhimedovu postulatu* (v. § 8.8.2), *tada je prsten komutativan; sadrži li prsten i jedinicu j, tada je identično preslikavanje $A\to A$ jedini sličnosni automorfizam prstena.*

Dokažimo komutativnost $ab=ba$ tj. $c\equiv ab-ba=0$; dovoljno je da to dokažemo pri $a>0$, $b>0$. Time je $na>0$ za svako $n\in N$ pa po Arhimedovu postulatu svakom $n\in N$ odgovara određen prirodni najmanji broj n' sa svojstvom

$$(\star)\qquad (n'-1)\,b\leq na<n'\,b.$$

Odatle

$$nc=n\,(ab-ba)=(\text{zbog } n\cdot ba=b\cdot na)=$$
$$=(na)\,b-b\,(na)<(n'\,b)\,b-b\,((n'-1)\,b)=b^2,$$

tj. za svako $n\in N$ imamo $nc<b^2$. Zato ne može biti $c>0$ niti $c<0$ jer bi bio povređen Arhimedov postulat za dvojku brojeva c, b^2 odnosno $-c$, b^2. Dakle je $c=0$ što je i trebalo dokazati.

S druge strane, neka je s sličnost i automorfizam od prstena A na sama sebe; po pretpostavci A ima jedinicu j pa za $b=j$ gornja relacija $(\star)$ postaje

$$(n'-1)\,j\leq na<n'\,j.$$

Odatle djelovanjem sa s zbog $sj=j$:

$$(n'-1)\,j\leq nsa<n'\,j, \quad \text{dakle} \quad -j<n\cdot(a-sa)<j$$

i to za svako $n\in N$. Opet kao maloprije sa c zaključujemo da nije ni

$$a-sa<0 \text{ ni } a-sa>0, \text{ nego je } a-sa=0, \text{ tj. } sa=a$$

za svako $a\in A$.

—→ **8.9.9. Teorem o Arhimedovu prstenu** (Ja. V. Hion, 1954)[1]

Svaki arhimedovski lančasto-uređen prsten

(1) $$(A, +', \cdot', \leq')$$

je komutativan i asocijativan; postoji podgrupa** $(G, +, \leq)$ **tijela

(2) $$(R, +, \cdot, \leq)$$

realnih brojeva sa svojstvom da je zadani prsten (1) izomorfno-sličan ili sa trivijalnim prstenom grupe

$$(G, +, \leq) \; (tj.\; GG=\{0\}) \quad ili\ sa\ realnim\ prstenom \quad (G, +, \cdot, \leq).$$

U posljednjem slučaju izomorfija od** A **prema** R **je oblika

$$a \in A \to kI(a), \quad pri\ nekom\ k \in R \setminus \{0\};$$

$I(a)$ ***je preslikavanje definirano u** § 8.8.3.2.1; **tako će biti npr. za svaki prsten** (1) **koji je bez nuladjelitelja.***

Dokaz. Prema Hölderovu teoremu iz § 8.8.3. grupa $(A, +, \leq)$ prstena je uređajno-slična i izomorfna s nekom uređenom podgrupom $(G, +, \leq)$ realnih brojeva. Posebno, uzmemo li za član e u dokazu 8.8.3.2.1 da bude $e>0$, tada preslikavanje

(3) $$a \in A \to I(a)$$

koje smo definirali u 8.8.3.2.1 je i sličnost i izomorfizam između uređene grupe $(A, +', \leq')$ prstena (1) i uređene podgrupe

(4) $$(IA, +, \leq)$$

tijela realnih brojeva.

Neka preslikavanjem (3) operacija $\cdot'$, u (1) prelazi u operaciju $\times$, tj. stavimo

(5) $$I(a \cdot' b) = I(a) \times I(b).$$

Time imamo prsten

(6) $$(IA, +, \times, \leq),$$

pri čemu je IA skup svih Ia pri $a \in A$; znakovi $+, \leq$ imaju značenje kao u (2).

Dalje za svako $c \in IA$ imamo endomorfizam

(7) $$y \in IA \to c \times y$$

realne grupe (4) u samu sebe; taj je endomorfizam uzlazan pri $c>0$, a silazan pri $c<0$. Zato je (§ 8.9.10) taj endomorfizam obična proporcionalnost, tj. postoji realan broj r_c sa svojstvom

(7_1) $$c \times y = r_c y, \quad r_c \geq 0 \Leftrightarrow c \geq 0, \quad (c, y \in IA).$$

[1] Ja. V. Hion, Uspjehi mat. nauk 9: 4 (62) (1954) 237—242; također G. Tallini, Atti Acad. Lincei Roma (8) 18 (1955) 367—373.

Time zakon distributivnosti $(c+d)\times y = c\times y + d\times y$ prstena (7) postaje

$$r_{c+d}\,y = r_c\,y + r_d\,y, \qquad \text{tj.}$$

(8) $$r_{c+d} = r_c + r_d.$$

Dakle je pridruživanje

(9) $$c \to r_c \qquad (c \in IA)$$

endomorfizam uređene realne grupe (4) u uređenu grupu $(R, +, \leq)$; on je uzlazan pri $c>0$ a silazan pri $c<0$. Prema § 8.9.10 preslikavanje (9) je proporcionalnost pa postoji broj $k \in R$, $k \geq 0$ za koji je

(10) $$r_c = kc$$

(dakle kc je obični realni produkt).

Time (7) postaje

(11) $$c\times y = kcy, \quad (c, y \in Ia).$$

Ako je $k=0$, prsten (6) je trivijalan.

Neka je zato $k \neq 0$, dakle $k>0$ ili $k>0$.

Neka je $k>0$. Tada je preslikavanje

$$\varphi : y \to ky \quad (y \in IA)$$

uređajno slični izomorfizam grupe $(IA, +, \leq)$ na grupu $(G, +, \leq)$, a iz (11) slijedi

$$\varphi(cxy) = k \cdot kc \cdot y = \varphi(c) \cdot \varphi(y).$$

To znači da je preslikavanje

$$a \to k \cdot I(a) \quad (a \in A)$$

uređajno slični izomorfizam prstena (1) na prsten

$$(G, +, \cdot, -).$$

8.9.10. Teorem. *Neka je $(G, +, \leq)$ bilo koja podgrupa grupe $(R, +, \leq)$ realnih brojeva; ako je h proizvoljan monoton homomorfizam $(G, +, \leq)$ u $(R, +, \leq)$, tada postoji neki broj K sa svojstvom*

(0) *$hg = kg$ za svako $g \in G$; pri tom je $k \geq 0$ (odnosno $k \leq 0$) ako je h uzlazno (silazno) preslikavanje.*

Dokaz Obradimo slučaj da je h uzlazno, tj. $x \leq y \Rightarrow hx \leq hy$. Ako postoji bar neko $a \in G \setminus \{0\}$ za koje je $ha=0$, tada $hg=0$ za svako $g \in G$. Naime, možemo pretpostaviti da je $a>0$, $g>0$. Ako je $0<g<a$, onda je $h\,0 \leq hg \leq ha$. Ako je $g>a$, tada za neko $n \in N$ imamo $na>g$ što sa $h(na) = nha = 0$, $hg \geq h\,0 = 0$, opet daje $hg=0$.

Ako $g \in G \setminus \{0\} \Rightarrow hg \neq 0$, tada je očigledno h izomorfizam.

Dokažimo da je preslikavanje $g \to hg$ proporcionalnost, tj.

(1) $$\frac{hg}{hg'} = \frac{g}{g'} \text{ za svako } g, g' \in G \text{ pri } g' \neq 0.$$

Ograničimo se na slučaj $g > 0$, $g' > 0$, dakle $hg > 0$, $hg' > 0$. Kad ne bi bilo (1), bilo bi ili $\frac{hg}{hg'} < \frac{g}{g'}$ ili $\frac{hg}{hg'} > \frac{g}{g'}$, Neka je tada $\frac{m}{n}$ racionalan broj i $\frac{hg}{hg'} < \frac{m}{n} < \frac{g}{g'}$, $m > 0$, $n > 0$; dakle bi bilo

(2) $$nhg < mhg',$$

(3) $$mg' < ng;$$

međutim, djelujemo li na (3) sa h, dobijemo $mhg' < nhg$, što je u protivurječju sa (2).

Dakle (1) stoji; a to znači da postoji neki broj $k \neq 0$ za koji vrijedi (0).

Naravno, $k > 0$ ako je h čisto uzlazno.

Analogno se obrađuju i ostali slučajevi.

$\longrightarrow$ **8.9.11. Teorem o tijelu realnih brojeva.** ***Svako lančasto uređeno tijelo K koje je zdesna potpuno (kompletno) u smislu da za svaki neprazan zdesna ograđen skup $X \subset K$ izlazi $\sup X \in K$ jest izomorfnoslično s tijelom $(R, +, \cdot, \leq)$ realnih brojeva uređenih po veličini i dualno, zamjenjujući: zdesna $\to$ slijeva, sup $\to$ inf. Posebno, tijelo K je i asocijativno i komutativno (isp. § 8.11.10.).***

Dokažimo da u tijelu K vrijedi Arhimedov postulat. U protivnom slučaju, postojala bi dva člana $a, b \in K$ za koje je $0 < a < b$ i $na \leq b$ za svako $n \in N$; dakle bi skup Na bio zdesna omeđen članom b. Prema uslovu desne potpunosti postojalo bi $\sup Na \equiv a' \in K$. No, kako je $Na + a \subsetneqq Na$ bilo bi odatle $\sup (Na + a) \leq Na$, tj. $a' + a \leq a'$, u protivnosti sa zakonom monotonije prema kojem je $a' + a > a'$.

Dakle je K lančasto uređeno tijelo K koje zadovoljava Arhimedov postulat; zato prema Hionovu teoremu 8.9.9 K je izomorfno-slično s nekim podtijelom R' realnih brojeva. No, poput K i tijelo R' je zdesna potpuno; a odatle izlazi da je nužno $R' = R$. Q. E. D.

8.9.11.1. Primjedba. Teoremom 8.9.11 dana je vanredno lijepa intuitivna karakterizacija tijela R realnih brojeva sjedinjujući u sebi intuitivne momente da je R svagdašnji okvir za računanje s uređenim i usporedljivim veličinama za koje je na snazi princip monotonije i ograđenosti: ako je monoton niz ograđen sa desne (lijeve) strane, tada je njemu pridružen određen supremum (infimum) iz promatranog tijela.

Teoremom 8.9.11 može se definirati i euklidska pravulja (i to upravo kao tijelo K) pa Euklidska ravnina (kao Descartesov kvadrat od K) itd, za prostore sa 3 i više dimenzija.

8.9.11.2. Primjedba. Teorem 8.9.11 može se dokazati i kraće, ne idući nužno preko Hionova teorema i to tako da se dokaže da je K komutativno tijelo (isp. 8.8.3.2.0), a onda da se izborom jediničnog elementa $e \in K$ provedu razmatranja iz § 8.8.3.2.1; tamošnje preslikavanje

$$g \in K \to I(g) \in R$$

je tražena izomorfna sličnost, $K \leftrightarrow R$, i to jedna jedina! (v. 8.9.8).

8.10. Apsolutna vrijednost. Norma. — **8.10.0.** Za svaki realni broj x definira se apsolutna vrijednost $|x|$ kao x pri $x \geq 0$ odnosno kao $-x$ pri $x<0$; neposredno se vidi da je $|x| = \sup\{x, -x\}$. Za svaki kompleksni broj ili kvaternion x također se definira $|x|$ i to kao $+(Nx)^{1/2}$, pri čemu je $Nx = xx^\star$, gdje je $x^\star$ konjugat od x. Znamo da je apsolutna vrijednost od velike važnosti i to posebno iz razloga što $|x-y|$ znači razdaljinu između x, y; pri tom x, y mogu biti brojevi ili kvaternioni. Označimo li sa $\nu(x)$ bilo $|x|$ bilo $(Nx)^{1/2}$, jasno je da su ispunjeni uslovi (0), $(\cdot)$, $(-)$ iz § 8.10.1.

Pri tom se radi o preslikavanju ν od prstena A prema množidbenom grupoidu realnih brojeva ≥ 0. Međutim, umjesto toga grupoida možemo promatrati bilo koji lančasto uređen grupoid s nulom. Tako dolazimo do pojma norme.

8.10.1. *Definicija norme u prstenu. Prsten s normom.* Zadan je prsten

(1) $$(A, +, \cdot)$$

i lančasto uređen grupoid (pisan množidbeno)

(2) $$(G, \cdot, 0; \leq)$$

s nulom, tj. s elementom $0 \in G$ za koji je $0g = g0 = 0$ i $0 \leq g$ za svako $g \in G$. Ujedno pretpostavljamo da je G i aditivan grupoid $(G, +)$ sa 0 kao neutralnim članom:

(4) $$0+g=g+0=g \text{ za svako } y \in G,$$

tako da imamo strukturu

(5) $$(G, +, \cdot, 0; -)$$

uređenog dvojnog grupoida sa 0. Takva se struktura javlja posebno pri svakom uređenom prstenu kao skup svih članova toga prstena koji su ≥ 0.

Norma ili vrednovanje (valuacija) prstena (1) s vrijednostima u grupoidu (2) je svako jednoznačno preslikavanje $\nu: A \to G$ za koje su ispunjena ova tri uslova:

(0) $$\nu(x) \geq 0, \ \nu x = 0 \Leftrightarrow x = 0;$$

$(\cdot)$ ili $(\cdot)_=$ $$\nu(xy) = \nu(x)\,\nu(y);$$

$(-)$ $$\nu(x-y) \leq \nu(x) + \nu(y).$$ Pri tom je $\{x, y\} \subset A$.

Tada se govori *o prstenu* (1) *s normom ili vrednovanjem u grupoidu* (2), ili kraće o G-normiranom prstenu.

Naravno, grupoid (2) vrijednosti ν može biti u vezi i sa samim zadanim prstenom (1); specijalno ako je $(A', +, \cdot \leq)$ bilo koji lančasto uređen prsten, tada skup

$$A'[0, \cdot) = \{x;\ x \in A';\ 0 \leq x\}$$

može poslužiti kao „vrijednosni grupoid" (2).

U posebnom slučaju kad je i vrijednost valuacije u ishodnom prstenu govori se o *samovrednovanju ili o autonormi prstena.*

Najpoznatiji je slučaj kad je norma realna: $G \subset (R, +, \cdot, <)$; tada se norma od x često označuje sa $\|x\|$.

8.10.1.1. *Pseudonorma.* Ako se uslov $(\cdot)_=$ zamijeni uslovom

$$(1)_{\leqslant} \qquad v(xy) \leqq v(x)\, v(y),$$

onda se govori o *pseudonormi prstena* (1).

8.10.1.2. *Nearhimedska norma.* Zamijeni li se u definiciji norme uslov $(-)_{\leqslant}$ uslovom

$$(-)_{\sup} \qquad v(x-y) \leq \sup\{v(x),\ v(y)\},$$

tada se govori o *nearhimedskoj normi.*

Postojanje G-norme u zadanu prstenu (1) odražava se na grupoidu (2); i obrnuto, posebno u slučaju kada norma poprima svaku vrijednost od G.

8.10.1.3. Primjedba. O nearhimedovskoj normi može se govoriti već i onda kada umjesto dvojnog grupoida (5) dolazi grupoid $(G, \cdot, 0, -)$ i preslikavanje $v: A \to G$ s uslovima (0), $(\cdot)$ te $(-)_{\sup}$.

8.10.2. Teorem. Pri svakoj normi ili valuaciji $v: A \to G$ vrijedi

(1) $\qquad v(-a) = v(a)$

(2) $\qquad v(a+b) \leq v(a) + v(b) \qquad$ pri uslovu $(-)_{\leqslant}$

(3) $\qquad v(a+b) \leq \sup(v(a),\ v(b)) \qquad$ pri uslovu $(-)_{\sup}$

Dokaz. Iz $-a = 0 - a$ izlazi $v(-a) = v(0-a)$ (prema uslovu $(-)_{\leqslant}$) $\leq v(0) + v(a) = v(a)$, tj. $v(-a) \leq v(a)$; pišući tu $-a$ umjesto a izlazi $v(--a) \leq v(-a)$. Iz te dvije relacije izlazi (1). Pišući u uslovu $(-)_{\leqslant}$ odnosno $(-)_{\sup}$ znak $-b$ umjesto b, dobiju se na osnovu (1) relacije (2) i (3).

8.10.3. Teorem o međuvezi prstena i skupa vrijednosti svake njegove norme.

Neka su $(G, \cdot, \leqslant)$ lančasto uređen grupoid s nulom, $a\,(A, +, \cdot)$ *neki prsten sa G-normom; neka je* $vA = G$.

(*i*) *Ako A ima jedinični član* 1, *tada je* $v(1)$ *jedinični član u G;*

(*ii*) *ako prsten A ima (nema) nuladjelitelje, tada to vrijedi i za G.*

(*iii*) *ako prsten A jest (nije) komutativan (asocijativan), tada grupoid G jest (nije) komutativan (asocijativan).*

(*IV*) *Ako je prsten A asocijativno tijelo, tada je* $(G \setminus \{0\}, \cdot)$ *podgrupa grupoida* $(G, \cdot)$.

D o k a z. (i) Iz $a \cdot 1 = a = 1 \cdot a$ izlazi na osnovu uslova $(\cdot)_=$:

$$v(a\,1) = v\,a = v(1\,a), \quad \text{tj.}$$

(1) $$v(a)\,v(1) = v\,a = v(1)\,v(a).$$

Zbog $vA = G$ znači (1) da je $v(1)$ jedinični član u G.

(ii). Neka prsten A ima [nema] nuladjelitelje; to znači da za neko [svako] $\{a, a'\} \subset A \setminus \{0\}$ vrijedi $a\,a' = 0$ [odnosno $a\,a' \neq 0$]; odatle zbog uslova (0) i $(\cdot)_=$ izlazi

$$v(a)\,v(a') = 0 \ \text{[odnosno } v(a)\,v(a') \neq 0],$$

i

$$v(a) \neq 0, \ v(a') \neq 0 \ \text{[odnosno } v(a) = 0 = v(a')],$$

što znači da G ima [nema] nuladjelitelja.

(iii) izlazi iz:

$$a\,b\,\mathrm{r}\,b\,a \Leftrightarrow v(a)\,v(b)\,\mathrm{r}\,v(b)\,v(a) \quad \text{pri } \mathrm{r} \in \{=, \neq\}$$

$$(a\,b)\,c\,\mathrm{r}\,a\,(b\,c) \Leftrightarrow (v(a)\,v(b))\,v(c)\,\mathrm{r}\,v(a)\,(v(b)\,v(c)), \text{ pri } \mathrm{r} \in \{=, \neq\}.$$

(IV) izlazi iz (i), (ii), (iii).

8.10.4. T e o r e m. Svaki lančasto uređen prsten $(A, +, \cdot)$, ima najmanje jednu svojstvenu normu; posebno $|a| = \sup\{-a, a\}$ je određena svojstvena norma.

Imajući na umu pravila o relativnom množenju u prstenu (pogl. 32 § 3.2) i posebno u uređenu prstenu (§ 8.9.2) dokaz teorema 8.10.4 teče upravo kao npr. u slučaju kola cijelih racionalnih brojeva.

8.10.5. Slučaj realne norme. Promatrajmo sada slučaj da je norma realan broj ≥ 0. Pokažimo vezu između arhimedskog uređenja i arhimedske norme.

$\longrightarrow$ **8.10.5.1.** T e o r e m. *Neka je K tijelo snabdjeveno realnom normom $x \to v(x)$. Ta je norma nearhimedska, tj.*

(1) $$v(x - y) \leq \sup\{v\,x, v\,y\}$$

onda i samo onda ako je

(2) $$v(nj) \leq 1$$

za svaki prirodni broj n; pri tom je j jedinica tijela K.

Dokažimo (1) $\Rightarrow$ (2). Kako je $v(-y) = v(y)$ (isp. 8.10.2. (1)), bit će za svaki prirodni broj n

$$v((n+1)j) = v(nj + j) = v(nj - (-j)) \leq \sup\{v\,nj, v(-j)\}, \quad \text{tj.}$$

$$v((n+1)j) \leq \sup\{v(nj), 1\}, \quad (n = 1, 2, \ldots) \text{ jer je } v(-j) = v\,j = 1.$$

Polazeći na desnoj strani od n na $n-1$ pa na $n-2$, itd. razbiremo da zaista vrijedi relacija (2).

Dokažimo (2) $\Rightarrow$ (1). Kad taj zaključak ne bi bio ispravan, postojala bi dvojka $\{x, y\} \subset K$ za koju je

(3) $$v(x-y) > \sup\{v x, v y\}, \text{ odnosno } v(x+y) > \sup\{v x, v y\} \equiv M.$$

Naravno, da bi bilo $x+y \neq 0$ jer iz $x+y=0$ zbog uslova (0) o normi izlazilo bi

$$v(x+y) = v(0) = 0,$$

što se protivi sa (3), jer je $M \geq 0$.

No, prema teoremu 8.10.3 (*iii*) tijelo K je komutativno i asocijativno jer je protuoblast norme komutativna i asocijativna. Zato u tijelu K vrijedi formula za razvoj binoma pa za svaki prirodni broj n imamo:

$$(v(x+y))^n = v(x+y)^n = v \sum_{\nu=0}^{n} \binom{n}{\nu} x^\nu y^{n-\nu} \leq$$

$$\leq \sum_{\nu=0}^{n} \binom{n}{\nu} (v x)^\nu (v y)^{n-\nu} \leq \sum_{\nu=0}^{n} (v x)^\nu (v y)^{n-\nu}$$

$$\leq \sum_{\nu=0}^{n} M^\nu \cdot M^{n-\nu} = (1+n) M^n,$$

gdje je $M = \sup\{v x, v y\}$.

Dakle je

$$(v(x+y) M^{-1})^n \leq 1+n \quad \text{za svako} \quad n \in N,$$

odnosno stavljajući

(4) $$v(x+y) \cdot M^{-1} = 1+z:$$

(5) $$(1+z)^n \leq 1+n \quad \text{na svako} \quad n \in N.$$

No, iz (4) i (3) izlazi $z > 0$ pa je

$$(1+z)^n = 1 + nz + \binom{n}{2} z^2 + \cdots > 1 + n \cdot \frac{n-1}{2} z^2 > 1+n$$

za svaki prirodni broj n za koji je $1 < \frac{n-1}{2} z^2$, tj. za koji je $n > 2z^{-2} + 1$.

Dakle će za takvo n biti $(1+z)^n > 1+n$, u protivurječju sa (5).

Time je teorem 8.12.5.1 dokazan.

8.10.5.2. p-adske norme u tijelu Q. Neka je p prost racionalan broj; za svaki racionalan broj $q = \frac{q_1}{q_2} \neq 0$ stavimo $p(q) = p^{-\alpha}$ pri čemu je broj α definiran jednakošću $q = \frac{m}{n} p^\alpha$ uz uslove $m \in D$, $n \in N$, $M(m, p) = 1 = M(n, p)$; to upravo znači da p ne dijeli ni m ni n; stavimo $p(0) = 0$. Lako se provjeri da je preslikavanje $q \in Q \to p(q) \in Q^+ \cup \{0\}$ određena nearhimedska valuacija. Provjerimo npr. aksiom $(-)_{\sup}$.

Neka je $q, r \in Q \setminus \{0\}$ te $q = x p^a$, $r = y p^b$, pri čemu su x, y racionalni brojevi kojima ni brojnik ni nazivnik nije djeljiv sa p. Neka je npr. $a \leq b$; tada je $q - r = (y p^{b-a} - x) p^a = z p^c$ pri čemu je $c \geq a$ i $p(q-r) = p^{-c} \leq p^{-a}$; tj. $p(q-r) \leq \sup\{p(q), p(r)\}$.

8.10.6. Realna norma u K i pripadni razdaljinski prostor. Upravo kao i u slučaju tijela realnih ili kompleksnih brojeva tako je *svako tijelo* (*čak i svaki skup*) *K s realnom normom određen metrički ili razdaljinski prostor u kojemu* $v(x-y)$ *označuje razdaljinu članova* x, y. Tako dobijemo dosta uzak no važan razred metričkih prostora.

Kao i svaki metrički prostor tako se i tijelo K s realnom normom može *upotpuniti* (*kompletirati*) na *potpun* (*kompletan*) metrički prostor $\tilde{K}$ ukoliko K nije potpun prostor (isp. Đ. Kurepa [1], § 30.3.2); posebno, skup svih Cauchy-evih nula-nizova $k_1, k_2, \ldots$ članova iz K čine određen ideal (n) u prstenu K_c svih Cauchy-evih nizova nad K pa je zapravo $\tilde{K} = K_c/(n)$, tj. $\tilde{K}$ je skup razreda $(n) + x$; pri tom se računanje u $K_c/(n)$ definira na uobičajen način.

8.10.7. Henselovi p-adski brojevi (p prost broj). Promatramo li prsten Q racionalnih brojeva i p-adsku normu $p(q)$ iz t. 8.10.5.2 tada kompletiranje odgovarajućeg metričkog prostora Q dovodi do tijela $\tilde{Q}(p)$ *Henselovih p-adskih brojeva*; oni se upotrebljavaju u teoriji algebarskih brojeva.[1]

8.10.8. Normirani vektorski prostori. Neka je V vektorski prostor nad zadanim normiranim tijelom K, s normom v i s vrijednostima norme u nekom tijelu K'. Svako preslikavanje $x \in V \to n(x) \in K'$ za koje vrijedi uslov (0), $(\cdot)_{\leq}$ i jednakost

$$n(K \cdot V \cdot) = v(K \cdot)\, n(V .) \tag{1}$$

zove se *norma prostora V.*

Tako npr. vektorski realni prostor R_3 je normiran stavljajući $n(x_1, x_2, x_3) = + (x_1^2 + x_2^2 + x_3^2)^{1/2}$.

Najobičniji slučaj je da je norma realan broj ≥ 0; označuje se obično sa $\|x\|$.

Svaki vektorski prostor s realnom normom shvatamo i kao *razdaljinski prostor*: dovoljno je $v(x-y)$ proglasiti *razdaljinom* između x, y.

8.10.9. Banachovi prostori. Svaki vektorski normirani metrički kompletni prostor koji dopušta definiciju razdaljine $\rho(x, y)$ pomoću realne norme $\|x-y\|$ zove se *Banachov prostor nad R.*

8.10.10. Normirana linearna algebra ili algebra s normom. To je svaki normirani vektorski prostor u kojem norma zadovoljava dodatnu relaciju.

$$\|ab\| \leq \|a\| \cdot \|b\|.$$

8.10.11. Banachova algebra nad K je svaka linearna algebra nad K koja je ujedno i Banachov prostor nad K.

---

[1] Vidjeti K. Hensel *Theorie der algebraischen Zahlen* I, Leipzig-Berlin 1908. XII + 350 str.

Prema tome u Banachovoj algebri s normom $x \to \|x\|$ vrijedi i *nejednakost* (1) $\|ab\| \leq \|a\| \cdot \|b\|$ *kao i jednakost* $\|K \cdot B^{\cdot}\| = |K^{\cdot}| \cdot \|B^{\cdot}\|$; pri tom je $K^{\cdot} \to |K^{\cdot}|$ norma tijela K.

Npr. prostor $R_3 = \{(x_1, x_2, x_3);\ x_1, x_2, x_3 \in R\}$ sa množenjem $(x_1, x_2, x_3)(y_1, y_2, y_3) = (x_1 y_1, x_2 y_2, x_3 y_3)$ i normom $\|(x_1 x_2 x_3)\| = \sup\{x_1, x_2, x_3\}$ je trodimenzionalna Banachova algebra nad R.

Izučavanje Banachovih algebara i normiranih prstena uopće danas je vrlo važno matematičko područje.

Navedimo bez dokaza ovaj

8.10.12. Teorem. Svaka linearna asocijativna kompleksna algebra s dijeljenjem koja dopušta realnu pseudonormu izomorfna je s tijelom $R(i)$ kompleksnih brojeva (Mazur 1938, Geljfand 1941).[1]

$\longrightarrow$ **8.10.13. Teorem o linearnim realnim algebrama (Albert, 1947)**[2] ***Svaka realna linearna algebra $\mathcal{A}$ s konačnim brojem dimenzija dopušta realnu pseudo-normu; dopušta li $\mathcal{A}$ i realnu normu (a ne samo pseudo-normu) i ima li $\mathcal{A}$ jedinicu, tada je algebra $\mathcal{A}$ nužno izomorfna s tijelom realnih brojeva ili s tijelom kompleksnih brojeva ili s tijelom Hamiltonovih kvaterniona ili s algebrom Cayleyevih oktava*** **(32 § 6.3.4).**

Neka čitalac pogleda dokaz u samom Albertovu članku ili u knjizi Kuroš [2] str. 337—343; dokaz je prilično dug i svodi se na 32 § 6.2. Zadovoljimo se ovdje da dokažemo ono o normi da tako vidimo kako je pseudo-norma općenitija od norme.

Naime, prema 26 § 7.8 npr. skup R_{nn} svih realnih matrica formata (n, n) jest linearna algebra; ona ima n^2 dimenzija; prema tome postoji be konačno mnogo [samo četiri] linearnih realnih algebri s jedinicom koje su snabdjevene realnom pseudo-normom [normom] (isp. također 31 § 1.7.5).

Neka je $e_1 e_2 \cdots e_n$ baza linearne realne algebre, s tablicom množenja

(1) $$e_i e_j = \sum_{k=1}^{n} b_{ij}{}^{k} e_k.$$

Jasno je da za svako $r \in R \setminus \{0\}$ vektori $f_\nu = r e_\nu$ također čine bazu algebre i da za odgovarajuću tablicu množenja

(2) $$f_i f_j = \sum_{\nu=1}^{n} c^{\nu}{}_{ij} f_\nu \quad \text{vrijedi} \quad c_{ij}{}^{k} = r\, b_{ij}{}^{k}$$

No, parametar $r \neq 0$ možemo tako odabrati da bude

(3) $$|c_{ij}{}^{k}| \leq n^{-1}.$$

Stavimo za svako

(4) $$a = \sum_{e=1}^{n} a_e f_e$$

(5) $$\nu(a) = \sum_{e=1}^{n} |a_e|.$$

[1] v. elementaran dokaz S. Kametani, J. Math. Soc. Japan 4 (1952) 96—99.

[2] A. A. Albert, Annals of Math. 48 (1947) 495—501.

Tada je $a \in \mathcal{A} \to v(a) \in R$ realna pseudo-norma.

Dovoljno je dokazati da je $v(aa') \leq v(a)\, v(a')$, za svako a iz (4) i svako

$$a' = \sum_{e=1}^{n} a_e' f_e \in \mathcal{A}.$$

No,

$$aa' = \left(\sum_{i=1}^{n} a_i f_i\right)\left(\sum_{j=1}^{n} a_j' f_j\right) = \sum_{i,j=1}^{n} a_i a_j' f_i f_j =$$

$$= \sum_{i,j=1}^{n} a_i a_j' \sum_{e=1}^{n} c_{ij}^e f_e = \sum_{e=1}^{n} \left(\sum_{i,j=1}^{n} c_{ij}^e a_i a'_j\right) f_e.$$

Dakle po definiciji (5) je

$$v(aa') = \sum_{e=1}^{n} \left| \sum_{i,j=1}^{n} c_{ij}^e a_i a_j' \right| \leq \sum_{i,j=1}^{n} |c_{ij}^e| \;\; |a_i| \;\; |a_j'|$$

$$(\text{zbog } (3)) \leq \sum_{i,j=1}^{n} |a_i| \cdot |a_j'| = v(a)\, v(a').$$

Dakle zaista $v(aa') \leq v(a)\, v(a')$.

8.11. Zadaci o općim algebrama.

1. Neka je A krug, kružnica, lopta, kugla, elipsoid, hiperboloid, 1) da li je određivanje $f_0 : A \to A$ središta A određena 0-arna operacija u A? Je li dakle (A, f_0) algebra? 2) A određivanje žarišta od A?

2) Kako se definira: 1) $(D, +)$, 2) $(D, +, \cdot)$, 3) $(D, +, \cdot, \leq)$ kao algebra $(D; s)$? Odrediti tip $\Delta = \rho s$ te algebre (v. § 8.1).

3. Navesti jednu algebru $(\{0, 1\}, s\})$ tipa $(0, 1, 1)$.

4. Navesti kako relacija ekvivalencije u skupu M može se shvatiti kao algebarska struktura, odnosno kao algebra. Konkretizirati npr. za $N \times N$ kao skup cijelih racionalnih brojeva (x, y) za koji je $(x, y) = (x' \; y') \Leftrightarrow x + y' = x' + y$.

5. Opisati kako se uređuje tijelo $(R, +, \cdot)$ realnih brojeva po veličini; dokazati da je to lančasto uređenje jedino.

6. Da li uređenje tijela kompleksnih brojeva propisom $x + i\, y \leq x' + i\, y' \Leftrightarrow x \leq x' \wedge y \leq y'$ daje 1) uređen skup, 2) uređeno tijelo? Navesti koji maksimalan lanac, odnosno maksimalan antilanac u tom uređenju.

7. Kako glasi definicija uređena množidbena grupoida $(G, \cdot, \leq)$; provesti razmatranja iz § 8.4. — 8.8.3. shvatajući grupu multiplikativno (a ne aditivno).

8. Ako je $(G, +, \leq)$ uređena grupa, onda je i $(G, +, \geq)$ uređena grupa. Vrijedi li odgovarajući iskaz za 1) prstene, 2) cjelosne oblasti, 3) tijela?

9. *Neprekidne lančaste grupe.* 1) To je svaka lančasta grupa G u kojoj nema susjednih članova i u kojoj postoji sup $X \in G$ za svaki zdesna omeđeni skup X. 2) U svakoj nepraznoj neprekidnoj komutativnoj lančastoj grupi ima, za svako $a \in N$, jednadžba $ax = g \in G$ jedno jedino rješenje $\in G$; označuje se sa $\frac{g}{a}$ ili $a^{-1} g$; 3) Može li se tu N zamijeniti sa $Q \diagdown \{0\}$, $R \diagdown \{0\}$?

10. Svaka neprekidna lančasto uređena grupa zadovoljava Arhimedovu postulatu pa je izomorfno-slična s grupom $(R, +, \leq)$ realnih brojeva (isp. § 8.9.11).

11. Neka je (1) $(G, +, \leq)$ proizvoljna uređena polugrupa s jedinicom; dokazati da skup G_c svih uzlaznih preslikavanja $f : G \rightarrow G$ čini uređenu polugrupu (2) $(G_c, +, \leq)$ s jedinicom; ta polugrupa (2.) obuhvaća jednu polugrupu izomorfnu sa danom (1.); pri tom se za $f, f' \in G_c$ definira $f \leq f' \Leftrightarrow fg \leq f' g$, $(f + f') g = fg + f' g$ $(g \in G)$. Ako je grupa (1.) neprazna, lančasto uređena i neprekidna u Dedekindovu smislu, onda su grupe (1.), (2.) izomorfno-slične.

12. Neka je $(G, +, \leq)$ uređen modul (17 § 6.3); dokazati da za svaki prirodni broj n preslikavanje (1) $g \rightarrow ng$, odnosno (2) $g \Rightarrow -n \cdot g$ daje izomorfnu sličnost modula $(G, +, \leq)$ odnosno modula $(G, +, \geq)$ na sama sebe.

13. Ako je $(A, +, \cdot, \leq)$ uređen prsten, tada za svako $n \in N$ imamo (1) $a < b \Leftrightarrow a^n < b^n$, (2) $b < a \Leftrightarrow a^{-n} < b^{-n}$ ukoliko a^{-1}, b^{-1} postoje.

14. U lančasto uređenu prstenu A postoji najviše jedno rješenje jednadžbe $x^{2n-1} = a$; pri tom je $a \in A$, $n \in N$ proizvoljno zadano.

15. Ako se prsten može lančasto urediti tako da je svaki pozitivni član kvadrat ili suma kvadrata, tada je to uređenje jedino.

16. Neka je $(A, +, \cdot)$ proizvoljan prsten bez nuladjelitelja; neka je $(A', +', \cdot' <')$ proizvoljan lančast prsten s jedinicom $1'$; definiramo li $v : A \rightarrow A'$ pomoću $v\,0 = 0'$, $v(A \diagdown \{0\}) = \{1'\}$, tada se dobije određena norma (zove se *trivijalna norma prstena* A s vrijednostima u A'.

17. Svako konačno asocijativno tijelo dopušta jedino trivijalnu normu. Vrijedi li to i za pseudo-normu?

18. Neka je a proizvoljan prirodan broj > 1; za svaki racionalni broj $q = \frac{q_1}{q_2}$ neka $a(0) = 0$ i $a(q)$ bude $a^{-\alpha}$, pri čemu je α rješenje jednadžbe $q = \frac{m}{n} a^{\alpha}$ uz uslove $M(m, a) = 1 = M(n, a)$. Što je nužno i dovoljno da preslikavanje $q \in Q \rightarrow a(q)$ bude norma? Isp. § 8.10.5.2).

19. Neka je $(A, +, \cdot, \leq)$ lančasto uređen komutativan prsten sa 1; označimo li sa P skup svih članova iz $A[x]$ kojima je najstariji koeficijent > 0 pa ako u $A[x]$ definiramo $f < g \Leftrightarrow g - f \in P$, tada je prsten

$(A[x], +, \cdot, \leq)$ lančast ali u njemu ne vrijedi Arhimedov postulat. Promatrati specijalne slučajeve $A \in \{Q, R, Q(\sqrt{2})\}$.

20. Neka je S metrički (ili topološki) prostor; označimo sa R^S skup svih jednoznačnih funkcija $f: S \to R$ (R je skup realnih brojeva); definirajući u R^S znakove $+, \cdot, <$ na uobičajen način: $(f+g)\,x = fx + gx$, $(fg)\,x = fx \cdot gx$, $f \leq g \Leftrightarrow fx \leq gx$ za svako $x \in R$, dokazati: 1) $(R^S, +, \cdot, \leq)$ je uređen prsten i to mrežast prsten pri čemu je $(\sup\{f, g\})(x) = \sup\{fx, gx\}$ i dualno za $\inf\{f, g\}$; 2) Isto vrijedi i za potprsten $G = R_c{}^S$ sastavljen od svih *neprekidnih* funkcija $f \in R^S$; 3) Isto vrijedi i za skup $C^\star$ svih *omeđenih neprekidnih* funkcija $f \in R^S$; 4) Dokazati da je svaki *maksimalni* ideal u $R_c{}^S$ prost (to vrijedi ne samo za prsten $R_c{}^S$ nego za svaki prsten A); 5) Preslikavanje $f \in R_{c\star}{}^S \to \|f\| = \sup|fx|$ je realna norma u $R_{c\star}{}^S$, kojom taj skup prelazi u Banachovu algebru; dokazati da je $\|f\| = \inf\{r;\ r \in R;\ |f| \leq r\}$. 6) Za svako $s \in S$ neka $R_c{}^S(s) = \{f;\ f \in R_c{}^S;\ f(s) = 0\}$; tada se dobije podalgebra ali bez jedinice. 7) Promatrati specijalno slučaj $S = \{1, 2, \ldots, n\}$; tada je $R_{c\star}{}^S = R^S = R_n$.

Literatura za poglavlje 32:

Za § 1: Bachmann [1] V; Behnke [1]; Birkhoff — Mac Lane [1]; Gel'fond [1]; Lejeune — Dirichlet [1]; Obreškov [2]; Plemelj [1]; Steinitz [1].

Literatura za paragrafe ², 3, 4, 6:

Behnke [1]; Birkhoff — Mac Lane [1]; Bourbaki [1]; Jacobson [1]; Krull [1]; Lugowski — Weinert [1] II; Mac Duffee [2]; Najmark [1]; Plemelj [1]; Waerden [1]; Weber [1]; Zariski — Samuel [1].

32 § 6: *Galoisova teorija*

Literatura

Birkhoff — Mac Lane [1]; Bourbaki [1]; Dubreil — Jacotin [1]; Hasse [3]; Lang [1]; Lugowski — Weinert [1] III; Postnikov [1]; Sierpiński [2]; Stojaković [1]; van der Waerden [1] I.

32 § 7: *Boole-ove algebre*:

Birkhoff [1]; Kuroš [3]; Rudeanu [1]; Sikorski [1]; Szász [1].

Literatura za § 8:

Albert [1], [2]; Cohn [1]; Deuring [1]; Kuroš [3].

P O G L A V L J E 33.

PREDSTAVLJANJE (REPREZENTACIJA) ALGEBARSKIH STRUKTURA

0. UVODNA RAZMATRANJA O REPREZENTACIJI

Kad se izučavaju pojedine algebarske strukture, upada u oči vrlo velika *raznovrsnost operacija* koje se pojavljuju pri raznim strukturama. Zato je od znatne važnosti sagledati strukture s bolje poznatim operacijama a pomoću kojih se izomorfno ili bar homomorfno može predstaviti svaka struktura određene vrsti. Tako npr. već znamo da se svaka grupa može predstaviti izomorfno pomoću grupe permutacija (Cayley, 17 § 8.5). Također smo spoznali da se svaka Booleova algebra može izomorfno predstaviti pomoću tijela skupova (Stoneov teorem 32, § 7.5.4). To su dva važna teorema o predstavljanju, a važnost im izlazi upravo iz činjenice što se pomoću tih predstavljanja operacije konkretiziraju.

Vrlo važna vrst reprezentacija je predstavljanje grupa pomoću grupa kojima su članovi matrice a operacija u grupi je množenje matrica; tada se govori o *matričnoj reprezentaciji grupe*. Kako su grupe, i u primjenama osobito funkcije definirane na grupama, vrlo važne a ujedno i jednostavne algebarske strukture, pitanje reprezentacije grupâ uopće i pitanje matrične reprezentacije posebno je važno i osobito mnogo ispitivano. Osobito je ispitivano da li se zadana grupa može predstaviti pomoću ortogonalnih matrica, unitarnih matrica, itd. jer takve reprezentacije imaju važno svojstvo da *reducibilnost* daje *potpuni reducibilnost* bar u slučaju kad je riječ o konačnim grupama (v. § 2.6).

Navest ćemo nekoliko činjenica iz te matematičke oblasti koja nalazi znatne primjene u teoretskoj fizici i drugim naukama

1. POJAM REPREZENTACIJE GRUPE $(G, \cdot)$ EKVIVALENTNOST REPREZENTACIJA

1.1. Definicija predstavljanja. Pod *predstavljanjem* (*reprezentacijom*) zadane grupe $(G, \cdot)$ razumijemo svaku *homomorfiju te grupe* tj. svaki postupak h kojim, iz $g \in G$ izlazi da je hg određen član neke grupe $(G', \cdot')$ sa svojstvom da je pri $g \in G$, $g_1 \in G$ ispunjeno

(1) $$h(g \cdot g_1) = hg \cdot' hg_1 .$$

Ako je homomorfizam h ujedno izomorfizam, tada se govori o *vjernom ili izomorfnom predstavljanju* zadane grupe.

1.2. Najobičniji slučaj reprezentacije grupe jest da je $(G', \cdot')$ grupa matrica nad zadanim tijelom K (npr. nad R, $R(i)$) ili grupa linearnih operatora, odnosno endomorfizama vektorskog prostora V_n nad K pri $\dim V_n = n$; tu dakle svakom članu $g \in G$ odgovara određen linearan regularan operator $h(g) \in GL_n(K)$ pri čemu vrijedi (1); sa $GL_n(K)$ ili LK_n označujemo grupu svih endomorfizama vektorskog prostora V nad K pri uslovu $\dim V = n$ (isp. pogl. 26 § 7.4). Specijalno, ako je $h(g) \in R_{nn}$ (odnosno $h(g) \in R(i)_{nn}$) govori se o *realnoj* (*kompleksnoj*) *matričnoj reprezentaciji*; s takvim ćemo reprezentacijama uglavnom i radii. Zato ćemo uglavnom pretpostavljati da radimo s matricama konačna formata, odnosno s linearnim operatorima u prostoru od n dimenzija.

1.3. Ekvivalentnost reprezentacija. Ako je

$$g \to a(g) \tag{1}$$

matrična reprezentacija grupe G, tada je za svaku regularnu matricu t za koju $ta(g)t^{-1}$ postoji, pridruživanje $g \to ta(g)t^{-1}$ također reprezentacija grupe G; kaže se da je ta reprezentacija *ekvivalentna* sa reprezentacijom (1). Ako je k tome t unitarno (ortogonalno), onda se govori o unitarno-ekvivalentnim (ortogonalno-ekvivalentnim) reprezentacijama $g \to a(g)$, $g \to ta(g)t^{-1}$.

Prema tome ekvivalencija reprezentacija definira se pomoću sličnosti matrica, odnosno pomoću sprezanja matrica.

1.4. Slučaj konačne ciklične grupe C_n pri $n \in N$. Grupa C_n se sastoji npr. od n rotacija pravilna n-terekuta oko glavne osi toga mnogokuta (glavna os je $\perp$ na ravninu mnogokuta).

Neka je g generator grupe C_n dakle $C_n = \{g^0, g, g^2, \ldots, g^{n-1}\}$; ako je,

$$\varepsilon = \varepsilon_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = e^{i\frac{2\pi}{n}}, \text{ odnosno } \varepsilon = \begin{bmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix},$$

tada je npr.

$$g^\nu \to \varepsilon^\nu \ (\nu = 0, 1, 2, \ldots, n-1), \text{ odnosno } g^\nu \to \begin{bmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}^\nu$$

određena izomorfna transformacija Γ_1' grupe C_n na množidbenu grupu kompleksnih brojeva ε^ν, pri čemu je

$$g^\nu \to \varepsilon^\nu \ (\nu = 0, 1, \ldots, n-1).$$

izomorfija od $(G, \cdot)$ na n-člani skup kompleksnih brojeva $e^{i\frac{2\pi}{n}}$ $(\nu=0, 1, \ldots, n-1)$.

Uostalom za $\nu \in \{0, 1, \ldots, n-1\}$ imamo reprezentaciju

$\Gamma_\nu : g^k \to \varepsilon^{\nu k} \in C_n$; posebno je

$\Gamma_{\nu g^0} = 1, \quad g_k g^\nu = \varepsilon^k$. Na taj način nastaje ova

Tablica predstavljanja grupe C_n:

	e	g	g^2	$\ldots g^{n-1}$
Γ_0	1	1	1	$\ldots 1$
Γ_1	1	ε	ε^2	$\ldots \varepsilon^{n-1}$
Γ_2	1	ε^2	$\varepsilon^{2\cdot 2}$	$\ldots \varepsilon^{2(n-1)}$;
. . .	. . .	. . .	. . .	. . .
Γ_{n-1}	1	ε^{n-1}	$\varepsilon^{2(n-1)}$	$\ldots \varepsilon^{(n-1)(n-1)}$

tu je $\Gamma_\nu = \Gamma_1^{\nu}$ $(\nu=0, 1, 2, \ldots, n-1)$

1.5. Predstavljanje konačnih komutativnih grupa G. Prema osnovnom teoremu 17, § 20.9.2. ima takva grupa G *bazu* pa smo zato G i mogli izomorfno ostvariti na način opisan u poglavlju 17 § 20.9.5 pomoću nizova korijena jedinice određena reda.

1.6. Opći teorem o predstavljanju grupa pomoću matrica. *Svaka grupa $(G, \cdot)$ može se izomorfno predstaviti pomoću matrica; posebno se za oblast svih dobivenih matrica može uzeti Descartesov kvadrat $G \times G$ i za svako $g \in G$ definirati preslikavanje-matricu d_g ovako:*

(1) $$g \in G \to d_g \quad \textit{stavljajući pri} \quad x, y \in G:$$

(2) $$d_g(x, y) = \delta_{x, gy} = \begin{cases} 1 \\ 0 \end{cases} \text{pri} \begin{cases} x = gy \\ x \neq gy. \end{cases}$$

Pridruživanje (1) je izomorfizam između zadane grupe $(G, \cdot)$ i dobivene množidbene grupe d_G svih matrica d_g $(g \in G)$.

D o k a z. Neka su $g, h \in G$; produktu $gh \in G$ članova g, h iz G odgovara prema (2) d_{gh} za koju je

(3) $$d_{gh}(x, y) = \begin{cases} 1 \\ 0 \end{cases} \text{pri} \begin{cases} x = ghy \\ x \neq ghy. \end{cases}$$

S druge strane, nađimo produkt $d_g d_h$ matricâ d_g, d_h. Imamo $(d_g d_h)(x, y) =$ $=$ po definiciji produkta $= \sum_{z \in G} d_g(x, z)\, d_h(z, y)$.

Tu su $=0$ svi sumandi osim jednog; a onaj sumand koji je $\neq 0$ je $=1$ a dobije se pri uslovima $d_g(x, z) = 1 = d_h(z, y)$, tj. pri $x = gz$, $z = hy$, dakle $x = ghy$. Drugim riječima

(4) $$(d_g d_h)(x, y) = \begin{cases} 1 \\ 0 \end{cases} \text{pri} \begin{cases} x = ghy \\ x \neq ghy. \end{cases}$$

No, (4) po definiciji (3), znači da je $d_{gh} = d_g d_h$. Dakle je pridruživanje $g \to d_g$ homomorfija. A kako iz $g \neq h$ izlazi $d_g \neq d_h$, znači to da je pridruživanje $g \to d_g$ izomorfija. Time je teorem 1.6 dokazan.

1.6.1. Primjedba. Teoremom 1.6 osigurana je *matrična* reprezentacija grupa; to predstavljanje je vrlo neekonomično jer su dobivene matrice prevelika formata i zavisne od $(G, \cdot)$. Tako npr. za cikličnu grupu C_{10} daje teorem 1.6 reprezentaciju pomoću matrica d_g koje su doduše građene jednostavno ali im je format 10×10 prevelik; svakako je matrična (čak i skalarna) reprezentacija grupe C_{10} pomoću brojeva $\varepsilon_{10}{}^{\nu}$ iz § 1.4 znatno ekonomičnija.

Zato je jasno da je pri reprezentiranju grupa skupom matrica korisno povesti računa i o tome da format dobivenih matrica bude što manji.

Primjenimo nešto od onoga što znamo o hermitskim matricama pa odmah dokažimo.

—→ 1.7. Osnovni teorem o predstavljanju konačnih grupa pomoću unitarnih matrica (I. Schur-Auerbach).

(*i*) ***Svaka konačna grupa je izomorfna s nekom grupom unitarnih matrica, tj. matricâ a za koje je $a^* a = 1$.***

(*ii*) ***Svaka matrična reprezentacija $g \in G \to h(g)$ konačne grupe G pomoću kompleksnih (realnih) matricâ $h(g)$ konačna formata ekvivalentna je s određenom unitarnom (ortogonalnom) matričnom reprezentacijom grupe.***

Dokaz. Neka je $g \in G \to h(g)$ određena izomorfna reprezentacija grupe G pomoću kvadratnih matrica $h(g)$ određena formata (n, n). Promatrajmo jediničnu pozitivno definitnu hermitesku formu $x^\star x = (x, x) = \sum_{\nu=1}^{n} x_\nu \bar{x}_\nu$; transformirajmo je pomoću matrice $h(g)$ stavljajući $x = h(g)\, y$; time se dobije nova forma

$$y^\star h^\star(g)\, h(g)\, y = (h(g)\, y,\ h(g)\, y);$$

i ona je pozitivno definitna; isto tako je i forma

$$f(y) \equiv \sum_{g \in G} y^\star h^\star(g)\, h(g)\, y \tag{1}$$

pozitivno definitna hermitska forma s matricom $H = \sum_{g \in G} h^\star(g)\, h(g)$.

Ako je $h(g_0)$ ona matrica koja odgovara nekom fiksiranom elementu g_0 iz G, tada forma (1) djelovanjem matrice $h_0 = h(g_0)$ prelazi u samu sebe jer se transformacija svodi na eventualni drukčiji raspored sumanada u (1), tj.

$$h(g_0)^\star H h(g_0) = H, \quad (g_0 \in G). \tag{2}$$

Stavimo li naime $y = h(g_0)\, z$ prelazi (1) u formu

$$z^\star h(g_0)^\star H h(g_0)\, z = z^\star \Big[\sum_{g \in G} h(g_0)^\star h^\star(g)\, h(g)\, h(g_0)\Big] z = \tag{3}$$

$$= z^\star \sum_{g \in G} h^\star(g g_0)\, h(g g_0)\, z = f(z)$$

jer zajedno sa g, član $g g_0$ prolazi grupom G.

Sa druge strane, postoji *unitarna* matrica u za koju je uHu^{-1} dijagonalna matrica, recimo λ:

(4) $$uHu^{-1} = \lambda = \operatorname{diag}[\lambda_1, \lambda_2, \ldots, \lambda_n], \text{ dakle}$$

(5) $$H = u^{-1}\lambda u.$$

Kako je H *hermitsko*, to je λ realno (27 § 10.2(3)); kako je k tome H *pozitivno definitno*, bit će $\lambda_\nu > 0$ ($\nu = 1, 2, \ldots, n$); zato možemo promatrati *pozitivni antikvadrat* $+\lambda^{1/2}$ od λ:

(6) $$+\lambda^{1/2} = \operatorname{diag}[+\lambda_1{}^{1/2}, +\lambda_2{}^{1/2}, \ldots, +\lambda_n{}^{1/2}].$$

Tada je hermitska matrica

(7) $$a = u^{-1}(+\lambda^{1/2})\,u$$

antikvadrat od H, tj. zadovoljava $a^2 = H$ kao što se neposredno vidi.

Promatrajmo funkciju

(8) $$g_0 \in G \to ah(g_0)\,a^{-1}$$

i dokažimo da je to tražena *unitarna reprezentacija* koja je ekvivalentna sa zadanom reprezentacijom $g \to h(g)$. Kako je (8) očigledno određena reprezentacija ekvivalentna sa zadanom $g \to h(g)$, sve se svodi na to da sagledamo da je matrica

$$q = ah(g_0)\,a^{-1}$$

unitarna, tj. da je $qq^\star = 1_n$, odnosno $q^\star q = 1_n$. No, zbog (7) i $u^\star = u^{-1}$ imamo

$$q^\star = u^{-1}(+\lambda^{-1/2})\,uh(g_0)^\star u^{-1}(+\lambda^{1/2})\,u \quad \text{pa je}$$

$$q^\star q = [u^{-1}(+\lambda^{-1/2})\,uh(g_0)^\star u^{-1}\underbrace{(+\lambda^{1/2})\,u][u^{-1}(+\lambda^{1/2})}_{\lambda}\,uh(g_0)\,u^{-1}(+\lambda)^{-1/2}\,u =$$

$$= (\text{zbog } (5)) = u^{-1}(+\lambda^{-1/2})\,\underbrace{uh(g_0)^\star\, Hh(g_0)\,u^{-1}}_{H \text{ zbog } (2)}(+\lambda^{-1/2})\,u =$$

$$= (\text{zbog } (2) \text{ i } (4)) = u^{-1}\underbrace{(+\lambda^{-1/2})\,\lambda\,(+\lambda^{-1/2})}_{1_n}\,u = u^{-1}\,1_n\,u = u^{-1}u = 1_n.$$

Time je osnovni teorem 1.7 dokazan.

2. SVODLJIVA (REDUCIBILNA) I NESVODLJIVA ILI IREDUCIBILNA PREDSTAVLJANJA

2.1. Definicija svodljiva operatora. Linearni operator $L: V \to V$ je *svodljiv* (*reducibilan*) ako postoji neki *pravi* potprostor V' od V koji je invarijantan prema tom preslikavanju, tj. $LV' \subset V'$, $\{0\} \subsetneq V' \subsetneq V$.

2.2. Definicija svodljiva skupa operatora. Skup S linearnih operatora koji djeluju u vektorskom prostoru V je *svodljiv* (*reducibilan*), ako u V postoji neki *pravi* potprostor V' koji je invarijantan prema *svakom* članu $f \in S$, tj.

$$\{O\} \subsetneq V' \subsetneq V, \quad fV' \subset V' \text{ za svako } f \in S.$$

2.2.1. Ako koordinatne vektore baze izaberemo tako da prvih k koordinatnih vektora razapinje taj invarijantni potprostor V', tada će [koordinate reda $k+1, \ldots, n$ tih vektora biti $= 0$ pa će] matrični zapis operatora L biti oblika

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}; \tag{1}$$

pri tom su A, C kvadratne matrice; matrica B kao ni jugozapadna 0-matrica u (1) ne moraju biti kvad.atne.

Na osnovu toga se postavlja

2.3. Definicija svodljivih matrica. Skup S matrica je *svodljiv* ili *reducibilan*, ako postoji matrica c tako da za svako $x \in S$ matrica cxc^{-1} bude oblika (1).

2.3.1. Definicija potpuno svodljivih matrica. Skup S matrica je *potpuno svodljiv* ako za neku matricu c sve matrice cxc^{-1} $(x \in S)$ imaju kvazidiagonalan oblik $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$; pri tom su A, B kvadratne matrice (općenito nejednaka formata).

2.4. Definicija nesvodljivosti. Negacija svodljivosti (reducibilnosti) zove se *nesvodljivost* (*ireducibilnost*).

2.4.1. Jasno je šta će značiti da skup matrica (linearnih operatora) nije potpuno svodljiv.

Međutim, znamo da je svaka reprezentacija konačne grupe ekvivalentna s nekom reprezentacijom te grupe pomoću *unitarnih* matrica ili što je isto unitarnih operatora koji djeluju u unitarnom prostoru (v. § 1.7.). Ako je V' netrivijalan invarijantan potprostor, tada će vektori iz invarijantnog potprostora V' ostati u potprostoru V', a vektori iz prostora $V'^{\perp}$ ostaće u$V'^{\perp}$; to znači da će, u odnosu na bazu prostora V sastavljenu od baze potprostora V' i baze potprostora $V'^{\perp}$, zapis operatora biti kvazidijagonalan, tj. oblika $\begin{bmatrix} X & 0 \\ 0 & Y \end{bmatrix}$ (isp. pogl. 27 § 6.3).

Tako smo dokazali

⟶ **2.5.** Teorem. **Svaka svodljiva konačna grupa unitarnih matrica konačna formata je potpuno svodljiva.**

Kombinirajući taj rezultat s teoremom 1.7 izlazi

⟶ **2.6. Osnovni teorem** ***(Maschke H., Math. Annalen* 52 (1899) 363):**

Svaka svodljiva konačna grupa linearnih operatora je ekvivalentna s potpuno svodljivom grupom operatora. Specijalno, svaka svodljiva unitarna reprezentacija konačne grupe je ekvivalentna s potpuno svodljivom unitarnom reprezentacijom.

2.7. Prikazivanje reducibilne unitarne reprezentacije pomoću ireducibilnih. Ako je

(1) $$g \in G \to h(g)$$

unitarna svodljiva reprezentacija grupe G, u unitarnom prostoru V, $\dim V < \infty$ pa ako je V' pravi invarijantan potprostor od V u odnosu na sve operatore $h(g)$ $(g \in G)$, tada je $g \in G \to h(g) \mid V'$ reprezentacija od G u prostor V' (manje dimenzije). Naime, za svako $v' \in V'$ imamo $h(g)\, v' \in V'$.

Neka je $V_1' = \{y;\ y \in V,\ y \perp V'\}$ ortogonalni komplement od V' u prostoru V; tada znamo (pogl. 27 § 6.6) da je i V_1' pravi invarijantni potprostor od V u odnosu prema $h(g)$, jer je $h(g)$ unitarno.

Tako imamo dvije unitarne reprezentacije grupe G, i to

$$g \in G \to h(g) \mid V', \qquad g \in G \to h(g) \mid V_1'.$$

Naime $h(g)\, V' \subset V'$, $\quad h(g)\, V_1' \subset V_1'$.

Ako se koji od potprostora V', V_1' može još dalje prikazati kao direktna suma pravih potprostora koji su invarijantni prema $h(g)$ $(g \in G)$, možemo u njima promatrati i odgovarajuće reprezentacije grupe G. Proces rastavljanja možemo nastavljati sve dok je to moguće, tj. *dok ne dođemo do nesvodljivih unitarnih reprezentacija grupe G u prave invarijantne potprostore $V_1, V_2, \ldots, V_r$ prostora V* pri čemu je

(2) $$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r.$$

Zbog pretpostavke $\dim V < \infty$, proces rastavljanja (2) mora se završiti nakon konačno mnogo koračaja. Neka je $\rho \in \{1, 2, \ldots, r\}$ i $e^{(\rho)} = (e^\rho{}_1, e^\rho{}_2, \ldots, e^\rho{}_{s_\rho})$ ortonormirana baza u V_ρ; naravno, vektori

$$e^1{}_1,\ e^1{}_2, \ldots,\ e^1{}_{s_1},\ e^2{}_1, \ldots,\ e^2{}_{s_2}, \ldots,\ e^r{}_1, \ldots,\ e^r{}_{s_r}$$

čine *ortonormiranu bazu* prostora V u kojoj se reprezentacija h grupe G zapisuje

kvazi-dijagonalnom matricom $\begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \cdots & \\ & & & A_r \end{bmatrix}$

pri čemu je A_ρ kvadratna matrica formata (s_ρ, s_ρ). Na taj način imamo

2.7.1. Teorem. ***Svaka unitarna svodljiva reprezentacija h konačne grupe G može se prikazati kvazi-dijagonalno pomoću određenih unitarnih nesvodljivih reprezentacijâ grupe G; tj. unitarna reprezentacija h je ili nesvodljiva ili je direktna suma ireducibilnih unitarnih reprezentacija grupe G.***

—→ **2.8.** Osnovni teorem o skalarnim matricama $\lambda \mathrm{I}$, odnosno o ireducibilnim reprezentacijama (I. Schur, 1905)[1].

[1] I Schur, Neue Begründung der Gruppencharaktere, Sitzunsberichte d. Berl. Ak. 1905, 406.

Neka je G konačan množidben nesvodljiv grupoid unitarnih matrica.

(*i*) *Kratnik λI jedinične matrice (λ je skalar) je jedina matrica za koju je*

(1) $$gx = xg \quad \text{za svako } g \in G.$$

(*ii*) *Ako su* $$g \in G \to m(g)$$ $$g \in G \to s(g)$$

dva ireducibilna predstavljanja grupe G koja nisu ekvivalentna, tada za matricu x iz uslovâ $m(g)\,x = xs(g)$ pri $g \in G$ izlazi $x =$ konstanta $\mathbf{0}$.

Jasno je da za svaki skalar λ matrica $x = \lambda I$ zadovoljava (1). Obratni dio teorema (*i*) i teorem (*ii*) izvest ćemo iz ove *Schurove leme* koja je i sama po sebi zanimljiva.

$\longrightarrow$ **2.8.1. Lema o alternativi.** (Schur). *Neka je M (odnosno S) nesvodljiv skup linearnih operatora vektorskog prostora U (odnosno V) od konačno mnogo dimenzija n (odnosno r) u sama sebe. Neka za linearni operator $a_{(n,\,r)}$: $V \to U$ vrijedi*

(1) $$Ma = aS$$

u smislu da je skup $Ma = \{ma;\ m \in M\}$ jednak skupu $aS = \{as;\ s \in S\}$. Tada je ili $a = 0$ ili $\dim U \equiv n = r \equiv \dim V$, $\det a \neq 0$; u posljednjem slučaju sistemi M, S su ekvivalentni.

Dokaz leme. Uslov (1) kazuje da su vektori-stupci $a_{.\rho}$ od a formata $(n, 1)$ i dakle članovi u $U = \operatorname{Dom} m$ pri $m \in M$; zato oni razapinju određen potprostor U' od U. No, U' je invarijantan prema $m \in M$ jer je $ma_{.\rho} \in U'$. Stvarno je $ma_{.\rho} =$ (prema (1) za neko $s \in S$) $= (as_{.\rho}) = [a_{1.}\, s_{.\rho}\, a_{2.}\, s_{.\rho} \ldots,\ a_{n.}\, s_{.\rho}]^T =$

$$= \sum_{\alpha=1}^{r} \left[a_{1\alpha}\, s_{\alpha\rho},\ a_{2\alpha}\, s_{\alpha\rho},\ \ldots,\ a_{n\alpha}\, s_{\alpha\rho} \right]^T = \sum_{\alpha=1}^{r} \left[a_{1\alpha}\, a_{2\alpha} \cdots a_{n\alpha} \right]^T s_{\alpha\rho} =$$

$$= \sum_{\alpha=1}^{r} a_{.\alpha}\, s_{\alpha\rho} \in U'.$$

Zbog pretpostavljene nesvodljivosti skupa M vrijedi ili $U' = \{0\}$ dakle $a_{.\nu} = \vec{0}$, tj. $a = 0$ ili je $U' = U$; time je $\dim V \geqq \dim U$, tj. $r \geq n$.

No, iz (1), odnosno iz

(2) $$m\,a = a\,s,$$

prelazeći na transponate izlazi

$$a^T m^T = s^T a^T$$

pa prethodni slučaj sada daje ili $a^T = 0$ ili $r \leq n$.

Oba slučaja dakle daju ili $a = 0$ ili $r = n = \dim U$ pa su vektori-stupci $a_{.\rho}$ $(\rho = 1, 2, \ldots, n)$ linearno nezavisni; dakle $\det a \neq 0$; zato postoji a^{-1} pa iz (2), odnosno iz (1) vidimo da su M, S međusobno ekvivalentni. Time je Schurova alternativa 2.8.1 dokazana.

2.8.2. Dokaz teorema 2.8. (*i*).

Pa neka matrica a komutira sa svakim $g \in G$:

(1) $$ga = ag.$$

Neka je λ_0 koja svojstvena vrijednost kompleksne matrice a; dakle je

(2) $$\det(a - \lambda_0 I) = 0;$$

λ_0 postoji jer je a konačna formata.

No, ako vrijedi (1), tada vrijedi također

$$g(a - \lambda_0 I) = (a - \lambda_0 I)\, g, (g \in G);$$

odatle prema lemi 2.8.1 izlazi ili $a - \lambda_0 I = 0$ ili $\det(a - \lambda_0 I) \neq 0$; kako druga mogućnost zbog (2) otpada, znači da ostaje jedino moguće

$$a - \lambda I = 0, \quad \text{tj.} \quad a = \lambda I,$$

a to Schurov teorem 1.8. (*i*) i tvrdi.

2.8.3. Teorem 2.8. (*ii*) izlazi neposredno iz 2.8 (*i*) jer u Schurovoj alternativi mogućnost $\det a \neq 0$ otpada zbog pretpostavljene neekvivalentnosti reprezentacijâ $M = \{m(g);\ g \in G\}$, $S = \{s(g);\ g \in G\}$. Time je važni Schurov teorem 2.8. potpuno dokazan.

⟶ **2.9. Teorem (kriterij o ireducibilnosti).** ***Matrična reprezentacija $g \to h(g)$ konačne grupe G je nesvodljiva onda i samo onda ako osim skalarne matrice nema nijedne druge matrice koja bi komutirala sa svakom matricom $h(g)$ $(g \in G)$ te reprezentacije*** (isp. § 3.9.1).

Nužni dio teorema je dokazan u t. 2.8 (*i*). Dovoljni dio teorema izlazi iz činjenice da pri svakoj svodljivoj reprezentaciji $h|G$ postoji i *neskalarna* matrica x za koju je $x\,h(g) = h(g)\,x$, $(g \in G)$.

Stvarno, kako je $h\,|\,G$ svodljivo, reprezentacija h je ekvivalentna s nekim kvazidijagonalnim oblikom

$$\begin{bmatrix} A(g) & & \\ & B(g) & \\ & & C(g) \end{bmatrix} \text{ (isp. t. 2.6); pri tom su}$$

$A(g)$, $B(g)$, $C(g)$ ... kvadratne matrice. Prema tome, $h(g)$ je oblika

$$h(g) = t \begin{bmatrix} A(g) & \\ & B(g) \end{bmatrix} t^{-1} \text{ za neku regularnu matricu } t.$$

Promatrajmo tada matricu

$$d = t \begin{bmatrix} \alpha\, 1_{s_1} & \\ & \beta\, 1_{s_2} \end{bmatrix} t^{-1},$$

pri čemu je 1_{s_2} jedinična matrica formata (s_2, s_2) = format od $B(g)$; α, β su skalari. Neposredno se provjeri da je $h(g)\,d = d\,h(g)$ za svako $g \in G$. To znači specijalno da u slučaju $\alpha \neq \beta$ matrica d nije skalarna a ipak komutira sa $h(g)$ za svako $g \in G$.

—→ **2.10. Teorem o ortogonalnosti.**

(i) ***Svako nesvodljivo unitarno predstavljanje h duljine s konačne grupe G***

$$g \to h(g), \quad Dom\, h(g) = (s, s)$$

daje s^2 ***ortogonalnih funkcija*** $g \in G \to h_{ij}(g)$, $(i, j = 1, 2, \ldots, s)$. ***Vrijedi***

$$(h_{i\mu}, h_{j\nu}) \overset{\text{def}}{=} \sum_{g \in G} h_{i\mu}(g)\, \overline{h_{j\nu}(g)} = \frac{n}{s}\, \delta_{ij}\, \delta_{\mu\nu},$$

dakle specijalno $(h_{i\mu}, h_{j\nu}) = 0$ ***pri*** $(i, \mu) \neq (j, \nu)$ ***(isp. pogl. 16 § 7.3). Pri tom je*** $n = k\,G$ = ***broj članova grupe G.***

(ii) ***Komponente*** h_{ij} ***svakog nesvodljivog unitarnog predstavljanja grupe G ortogonalne su na komponentama svakog drugog nesvodljivog predstavljanja h′ grupe G koje nije sa h ekvivalentno, tj.***

$$(h_{ij}, h'_{i'j'}) = 0.$$

2.10.1. Dokaz teorema 2.10 (*i*) Svakom $g \in G$ pripada linearni operator (npr. matrica) $h(g)$; za proizvoljnu (s, s)-matricu b imamo na taj način matricu $h(g)\,b\,h(g^{-1})$ kao i „aritmetičku sredinu“:

$$a = \frac{1}{k\,G} \sum_{g \in G} h(g)\, b\, h(g^{-1}) \text{ tih matrica.}$$

Dokažimo da *matrica a komutira sa* $h(x)$ *za svako* $x \in G$, tj.

$$h(x)\,a = a\,h(x) \quad (x \in G). \tag{1}$$

Naime, imamo

$$h(x)\,a = h(x) \frac{1}{kG} \sum_g h(g)\, bh(g^{-1}) = \frac{1}{kG} \sum_g h(x)\,(g)\, bh(g^{-1}) =$$

$$\frac{1}{kG} \sum_g h(xg)\, bh(g^{-1}) = (\text{stavljajući } g' = xg, \text{ tj. } x^{-1}g' = g, g'^{-1}x = g^{-1}) =$$

$$= \frac{1}{kG} \sum_g h(g')\, bh\underbrace{(g'^{-1}x)}_{h(g'^{-1})h(x)} = \left[\frac{1}{kG} \sum_g h(g')\, bh(g'^{-1})\right] h(x) = ah(x).$$

Dakle (1) stoji.

Kako je $h|G$ nesvodljiva reprezentacija konačne grupe G, teorem 2.7. (i) kaže da je matrica a oblika $a=\lambda I$, pri čemu naravno $\lambda=\lambda(b)$ zavisi od matrice b; to znači da za dano b imamo skalarne jednakosti:

(2) $$a_{ij}=\frac{1}{kG}\sum_g\sum_{\mu\nu} h_{i\mu}(g)\, b_{\mu\nu}\, h_{\nu j}(g^{-1})=\lambda(b)\,\delta_{ij}.$$

No, po pretpostavci, matrica $h(g^{-1})$ je unitarna, tj. zadovoljava relaciju $z^{\star}=z^{-1}$, odnosno $z=\overline{z^{-1}}^{T}$. Dakle je

$$h(g^{-1})=(\overline{h(g^{-1}))^{-1}}^{T}=[\text{zbog } h(g^{-1})=(h(g)^{-1}]=\overline{h(g)}^{T}, \text{ odnosno}$$

(3) $$h_{\nu j}(g^{-1})=[\overline{h(g)}^{T}]_{\nu j}=\overline{h_{j\nu}(g)}.$$

Zato (2) pomnoženo sa kG daje

$$(kG)\,a_{ij}=\sum_{\mu,\nu} b_{\mu\nu}\sum_g h_{i\mu}(g)\,\overline{h_{j\nu}(g)}=(kG)\,\lambda(b)\,\delta_{ij}, \quad \text{tj.}$$

(4) $$kG\,a_{ij}=\sum_{\mu,\nu} b_{\mu\nu}\,(h_{i\mu},\ h_{j\nu})=kG\,\lambda(b)\,\delta_{ij}.$$

Pustimo li u (2) da bude $i=j=\sigma=1,2,\ldots,s$, pa odgovarajućih s jednakosti zbrojimo, dobijemo

(5) $$\operatorname{Tr} a=\frac{1}{kG}\sum_g\sum_{\sigma,\mu,\nu=1}^{s} h_{\nu\sigma}(g^{-1})\,h_{\sigma\mu}(g)\,b_{\mu\nu}=\lambda(b)\,s.$$

No, $1=h(I)=h(h^{-1}g)=h(g^{-1})=h(g)$, tj.

$\delta_{\nu\mu}=h_{\nu\mu}(I)=\sum_\sigma h_{\nu\sigma}(g^{-1})\,h_{\sigma\mu}(g)$; zato (5) prelazi u oblik

$$\operatorname{Tr} a=\frac{1}{kG}\sum_g\sum_{\mu,\nu}\delta_{\nu\mu}\,b_{\mu\nu}=\lambda(b)\,s, \quad \text{tj.}$$

$$\operatorname{Tr} a=\sum_{\mu,\nu}\delta_{\nu\mu}\,b_{\mu\nu}=\lambda(b)\,s, \quad \text{dakle}$$

$$\operatorname{Tr} a=\sum_{\mu} b_{\mu\mu}=\lambda(b)\,s, \quad \text{tj.}$$

(6) $$\operatorname{Tr} a=\operatorname{Tr} b=\lambda(b)\,s.$$

Iz (4) i (6) izlazi:

(7) $$\sum_{\mu,\nu} b_{\mu\nu}\,(h_{i\mu},\ h_{j\nu})=\frac{kG}{s}\,\delta_{ij}\operatorname{Tr} b$$

za svaku matricu b formata (s, s).

Uzmimo posebno $b=e(\mu,\nu)$ (pogl. 27 § 18.6.1) tj. $b_{\mu\nu}=1$, a inače $b_{jk}=0$ pri $(j,k)\neq(\mu,\nu)$. Kako je $\operatorname{Tr} e(\mu\,\nu)=\delta_{\mu\nu}$, znači da izraz $(7)_2$ pri $b=e(\mu,\nu)$ postaje upravo $(0)_2$. Isto tako za matricu $b=e(\mu,\nu)$ izraz $(7)_1$ se reducira na $(0)_1$. Drugim riječima jednakost (7) koja vrijedi za svaku matricu b vrijedi i posebno za $b=e(\mu, \nu)$ i tada (7) postaje upravo tražena jednakost (0) o ortogonalitetu u teoremu 2.9. (*i*).

2.10.2. Dokaz teorema 2.10. (*ii*). Dokaz ćemo izvesti iz teorema 2.8. (*ii*). Za proizvoljno $g \in G$ promatrajmo matrice (operatore) $h(g)$, $h'(h^{-1})$ te za proizvoljno saglasno b produkt

$$h(g)\, bh'(g^{-1}).$$

Postavimo

$$a=\frac{1}{n} \sum_{g \in G} h(g)\, bh'(g^{-1}).$$

Kao i malo prije, lako se vidi da je $h(g)\, a = ah'(g)$; kako su $g \to h(g)$, $g \to h'(g)$ dva neekvivalentna nesvodljiva predstavljanja grupe G, zaključujemo prema teoremu 2.8. (*ii*) da je matrica a nula, i to *pri svakom izboru od b.*

Dakle je

$$\sum_{g \in G} h(g)\, bh'(g^{-1}) = 0,$$

odnosno uzimajući (i, i')-komponentu

$$\sum_{g \in G} [h(g)\, bh'(g^{-1})]_{ii'} = 0.$$

Na osnovu definicije produkta matricâ u zagradi [ ] znači to da je

$$\sum_{g \in G} \sum_{j,j'=1}^{s} h_{ij}(g)\, b_{jj'}\, h'_{j'i'}(g^{-1}) = 0; \text{ tj.}$$

$$(1) \qquad \sum_{j,j'} b_{jj'} \sum_{g} h_{ij}(g)\, h'_{j'i'}(g^{-1}) = 0.$$

No, zbog unitarnosti matrice $h'(g^{-1})$ imamo

$$h'_{j'i'}(g^{-1}) = \overline{h'_{i'j'}(g)},$$

pa prethodna formula (1) postaje

$$(2) \qquad \sum_{i,j'=1}^{s} b_{jj'}\,(h_{ij'},\, h'_{i'j'}) = 0.$$

Posebnim izborom $b=e(j, j')$ (pogl. 27 § 18.6.1) za matricu b uvjeravamo se da se (2) svodi na traženu relaciju (00) o ortogonalnosti.

—→ 2.11. Osnovni teorem o prostoru $P=R(i)^G$ svih jednoznačnih kompleksnih funkcija s oblasti G. (W. Burnside) (1852—1927; 1905).[1]

Vektorski prostor $P=R(i)^G$ ima kG dimenzija. Ako je

$$(1) \qquad I=\{h_1, h_2, \ldots, h_r\}$$

skup svih unitarnih nesvodljivih reprezentacijâ

$$x \in G \to h_\rho(x) \quad (\rho=1,2, \ldots, r)$$

[1] W. Burnside, London Math. Soc. Proc. (2) 3 (1905), 430.

grupe G među kojima nema ekvivalentnih, pa ako je matrica

$$h_\rho(x) = [h_{j\sigma\rho}(x)]_{j,\sigma=1\cdots s_\sigma}$$

duljine s_ρ, tada su funkcije

(2) $$x \in G \to h_{j\sigma\rho}(x) \quad (j, \sigma = 1, 2, \ldots, s_\rho;\ \rho \in \{1, 2, \ldots, r\})$$

linearno nezavisne nad tijelom $R(i)$ kompleksnih brojeva i čine vektorsku bazu prostora P: svaka funkcija $f: G \to R(i)$ je linearna kombinacija s koeficijentima iz $R(i)$ funkcijâ (2) kojih ima

(3) $$S \equiv s_1^2 + s_2^2 + \cdots + s_r^2.$$

Vrijedi

(4) $$s_1^2 + s_2^2 + \cdots + s_r^2 = kG, \text{ tj. } S = kG.$$

U § 3. ćemo dokazati da je r broj razredâ grupe G.

2.11.1. D o k a z. Najprije je jasno da su funkcije (2) određeni članovi prostora P.

Linearna nezavisnost nad $R(i)$ funkcijâ (2) izlazi iz teorema 2.10 o ortogonalnosti.

2.11.2. Iz istog je razloga $S \le \dim P$.

2.11.3. Imamo $\dim P = kG$.

Naime $n\,(\equiv kG)$ funkcijâ

(5) $$g \in G \to \varphi_g$$

za koje je

$$\varphi_g(x) = \delta_{g,x}, \quad (g, x \in G)$$

čine vektorsku bazu prostora P jer s jedne strane te funkcije su linearno nezavisne nad $R(i)$, a sa druge strane svako $f \in P$ je linearna kombinacija funkcijâ (5) jer je

$$x \in G \to fx = \sum_{g \in G} \varphi_g(x) f(g).$$

Iz 2.11.2. i 2.11.3. izlazi

(6) $$S \le kG \; (= \dim P).$$

Dokazat ćemo da u (6) znak $\le$ znači upravo $=$, i da S funkcijâ (2) čini vektorsku bazu prostora P. U tu svrhu definirajmo i izučimo:

2.11.4. Operator desne translacije: $f \in P \to R_g f$. Neka je $g \in G$ fiksirano; promatrajmo ono preslikavanje

(7) $$\begin{cases} f \in P \to R_g f \text{ za koje je} \\ R_g f(x) = f(xg) \text{ za svako } x \in G. \end{cases}$$

Na taj način dobivamo kG preslikavanjâ (7) prostora P u sama sebe. Dokažimo:

2.11.5. Lema. *Pridruživanje* (7) *je određena unitarna reprezentacija grupe* G *u prostor* P, *tj.*

(8) $$R_{g_1 g} = R_{g_1} R_g \qquad (g_1, g \in G)$$

u smislu da $R_{g_1 g} f = R_{g_1} R_g f$, $(f \in P)$, *tj.*

(9) $$R_{g_1 g} f(x) = R_{g_1} R_g f(x) \text{ pri } x \in G.$$

Reprezentacija (7) zove se **regularna reprezentacija grupe** G; objekti te reprezentacije su članovi od $R(i)^G$.

Dokaz. Za fiksirano $g \in G$ promatrajmo funkciju

$$x \in G \to f(xg) = f_g(x);$$

tada je

$$R_{g_1 g} f(x) \overset{\text{def}}{=} f(x g_1 g) \overset{\text{def}}{=} f_g(x g_1) \overset{\text{def}}{=} R_{g_1} f_g(x) = R_{g_1} f(xg) = R_{g_1} R_g f(x).$$

Dakle zaista vrijedi (9), a time i (8). Još preostaje da dokažemo da je operator (7) unitaran; u tu svrhu je dovoljno dokazati da taj operator R_g čuva skalarni produkt u P:

(10) $$f, \varphi \in P \Rightarrow (f, \varphi) = (R_g f, R_g \varphi) \text{ za svako } g \in G.$$

No, $$(R_g f, R_g \varphi) \overset{\text{def}}{=} \sum_{x \in G} (R_g f)(x) \overline{(R_g \varphi)(x)} = \sum_{g \in G} f(xg) \overline{\varphi(xg)}.$$

No, pridruživanje $x \in G \to xg$ je *permutacija od* G pa se zato posljednja suma razlikuje od $\sum_{x \in G} f(x) \overline{f(x)}$ jedino u redoslijedu pribrojnikâ; vrijednost tih suma je dakle ista; a to znači da vrijedi (10).

2.11.6. Duljina ili dimenzija regularne unitarne reprezentacije $g \in G \to R_g$ je $n(=kG)$.

2.11.7. Primijenimo na unitarnu regularnu reprezentaciju $g \to R_g$ teorem 2.7.1; prema tome teoremu, reprezentacija R_g se zapisuje kvazidijagonalno pomoću nesvodljivih prikaza; to znači da se prostor $P = R(i)^R$ prikazuje kao ortogonalna suma unitarnih potprostora, npr.

(12) $$P = P_1 \oplus P_2 \oplus P_3 \cdots \oplus P_p.$$

Za svako $\pi \in \{1, 2, \ldots p\}$ potprostor P_π preslikava se u sama sebe pomoću nesvodljivog predstavljanja

(13) $$R_g \mid P_\pi \text{ (restrikcija od } R_g \text{ na } P_\pi).$$

Kako je (13) nesvodljivo, bit će, za svako $x \in G$, $(R_g \mid P_\pi)(x)$, kvadratna matrica duljine d_π, gdje je $d_\pi = \dim P_\pi$. Neka je

$$e^\pi = e_1{}^\pi, \; e_2{}^\pi, \ldots, e^\pi{}_{d\pi}$$

ortonormirana baza u P_π; to posebno znači da pri $x \in G$ imamo

$$e_j{}^\pi(x) \in R(i) \quad (j = 1, 2, \ldots, d_\pi).$$

Djelovanjem operatora R_g na funkciju $e_j^\pi \in P$ zbog $R_g e_j^\pi \in P_\pi$ imamo

$$e_j^\pi(xg) \text{ (radi 7))} = R_g e_j^\pi(x) = \sum_{k=1}^{d_\pi} (R_g | P_\pi)_{kj} e_k^\pi(x), \quad (x \in G).$$

Odatle posebno pri $x = 1$:

$$e_j^\pi(g) = \sum_{k=1}^{d_\pi} (R_g | P_\pi)_{kj} e_j^\pi(1), \quad (j = 1, 2, \ldots, d_\pi).$$

Prema tome, baza e^π potprostora P_π a time i sam potprostor P_π može se izraziti pomoću funkcija — komponenata operatora $R_g | P_\pi$.

To vrijedi za $\pi = 1, 2, \ldots, p$. Kako su funkcije — komponente

(14) $$(R_g | P_\pi)_{kj} \quad (k, j = 1, 2, \ldots, d_\pi; \quad \pi = 1, 2, \ldots, p)$$

prostora P, specijalno to znači da vrijedi

$$s_1^2 + s_2^2 + \cdots + s_p^2 \geq \dim P \;(= kG).$$

Povratimo se na (1). Kako je $R_g | P_\pi$ ireducibilna reprezentacija od G, zaključujemo prema definiciji mnogosti I u (1) da je reprezentacija $R_g | P_\pi$ ekvivalentna s jednim (jedinim) članom h_{k_π} iz (1); to znači da je svaki član iz P_π linearan spoj komponenata reprezentacije h_{k_π}; tih komponenata ima $d^2{}_{k_\pi}$. To vrijedi za $\pi = 1, 2, \ldots, p$. Odatle zbog (12) zaključujemo da je svaki član iz P linearna kombinacija nad $R(i)$ funkcijâ-komponenata

(15) $$g \in G \to h_{\sigma j \rho}(g) \in R(i), \quad (j, \sigma = 1, 2, \ldots, s_\rho; \; \rho = 1, 2, \ldots, r);$$

s_ρ je duljina matrice $h_\rho(g)$. Broj funkcijâ (15) je tačno

$$s_1^2 + s_2^2 + \cdots + s_r^2.$$

Kako su h_ρ, $(\rho = 1, 2, \ldots, r)$ ireducibilne i neekvivalentne unitarne reprezentacije od G, znači to prema teoremu o ortogonalnosti da u (15) imamo najobuhvatniji skup linearno nezavisnih funkcija $G \to R(i)$; njihov je dakle broj $\dim P$, odnosno $s_1^2 + s_2^2 + \cdots + s_r^2$. Odatle zaključujemo da vrijedi (4).

Q. E. D.

3. KARAKTER ILI TRAG ZADANE REPREZENTACIJE.

Trag $\operatorname{Tr} a$ matrice a definira se kao $\operatorname{Tr} a = \sum a_{ii}$ (isp. 27 § 8.1). Zanimljivo je da u vezi s matričnom reprezentacijom $h: G \to K_{ss}$ grupe G (dakle je članu $g \in G$ pridružena matrica $h(g)$ formata (s, s)) ima važnu ulogu ovakva

3.1. Definicija karaktera zadane reprezentacije. *Karakter matrične reprezentacije*

$$g \in G \to x(g) \in K_{ss}$$

jest funkcija

$$g \in G \to \chi(g) \equiv \operatorname{Tr} h(g) \; (\equiv \sum_{\sigma=1}^{s} h_{\sigma\sigma}(g)).$$

3.1.1. Tako npr. reprezentaciji $g \to d_g$ iz § 1.6 pripada karakter $g \to \operatorname{Tr} d_g = \delta_{1g} \cdot kG$; naime dijagonala od d_g je konstanta 0 pri $1 \neq g$, odnosno konstanta 1 pri $1 = g$.

Kako slične matrice imaju jednak trag, znači to da ekvivalentne reprezentacije grupe imaju jednake karaktere. Vrijedi i obrat, pa tako imamo

$\longrightarrow$ **3.2. Teorem.** ***Nesvodljive matrične reprezentacije konačne grupe G ekvivalentne su onda i samo onda ako imaju jednak karakter.*** (isp. t. 3.6).

Treba dakle dokazati ovo: ako su

$$g \in G \to h(g) \in K_{ss}, \quad g \in G \to h'(g) \in K_{ss}$$

dvije *nesvodljive* reprezentacije grupe G u grupu K_{ss} sa svojstvom

$$(1) \qquad \operatorname{Tr} h(g) = \operatorname{Tr} h'(g), \quad (g \in G)$$

onda su te reprezentacije h, h' ekvivalentne, Stvarno, kada h, h' ne bi bile ekvivalentne reprezentacije, tada bi prema teoremu ortogonalnosti 2.8. (*ii*) bilo posebno

$$\sum_g h_{\sigma\sigma}(g)\, \overline{h'_{\sigma'\sigma'}(g)} = 0, \quad (\sigma, \sigma' = 1, 2, \ldots, s).$$

Zbrojimo li tih s jednakosti za $\sigma = 1, 2, \ldots, s$ pa opet zbrojimo dobivenih s jednakosti za $\sigma' = 1, 2, \ldots, s$ izlazi jednakost

$$(2) \qquad \sum_g \operatorname{Tr} h(g)\, \overline{\operatorname{Tr} h'(g)} = 0, \text{ tj. bilo bi}$$

$$(\operatorname{Tr} h, \operatorname{Tr} h') = 0.$$

Međutim po obrascu (0) iz § 2.8. (*i*) poseban slučaj $i = \mu$, $j = \nu$ daje

$$\sum h_{ii}(g)\, \overline{h_{jj}(g)} = \frac{kG}{s} \delta_{ij} \qquad (i, j = 1, 2, \ldots, s).$$

Sumiramo li te jednakosti po $i, j = 1, 2, \ldots, s$ izlazi

$$(3) \qquad (\operatorname{Tr} h, \operatorname{Tr} h) = kG, \text{ što bi s pretpostavkom (1) dalo}$$

$$(4) \qquad (\operatorname{Tr} h, \operatorname{Tr} h') = kG \neq 0, \text{ u protivnosti sa (2).}$$

Relacije (2) i (3) možemo izraziti i kao

3.2.1. Teorem. *Ako je I bilo koji skup ireducibilnih unitarnih reprezentacija konačne grupe G, tada su funkcije $g \in G \to Tr\, h(g)$, $(h \in I)$ linearno nezavisne nad $R(i)$; vrijedi*

$$(Tr\, h,\ Tr\, h') = kG \cdot \delta_{hh'}.$$

3.3. Teorem. *Neka je $Cl\,G$ skup svih razreda konjugiranosti grupe G (svako $A \in Cl\,G$ je najobuhvatniji skup konjugiranih članova iz G; isp.* 17. § 15.4); *neka je $H = HG$ najobuhvatniji skup nesvodljivih matričnih reprezentacija grupe G u kojem nema ekvivalentnih reprezentacija; tada imamo ove relacije:*

$$(i) \qquad h \in H \Rightarrow \sum_X Trh(X)\, \overline{Trh(X)}\, kX = kG, \quad (X \in Cl\,G);$$

$$(ii) \qquad h, h' \in H \Rightarrow \sum Trh(X)\, \overline{Trh'(X)}\, kX = kG\, \delta_{hh'};$$

pri tom stavljamo $Trh\,X = Trhx$ *pri* $x \in X$, $\delta_{hh'} = \begin{cases} 0 \\ 1 \end{cases}$ *pri* $\begin{cases} h \neq h' \\ h = h'. \end{cases}$

(*iii*) $$k\,HG \leq k\,Cl\,G, \quad tj. \quad k\,HG \leq r.$$

U § 3.4 ćemo dokazati da je $k\,HG = r$.

D o k a z. Formula (*i*) izlazi neposredno iz formule 3.2 (3); formula (*ii*) izlazi iz (2) i iz (*i*).

U vezi sa (*iii*) pridružimo svakom $h \in H$ ovaj niz odnosno funkciju n_h:

$$\left(\frac{k\,X}{k\,G}\right)^{1/2} Trh\,X, \quad (X \in Cl\,G);$$

taj niz shvaćen kao stupac-vektor je član prostora K_{r1}; no ti vektori

$h \in H \to n_k$ su prema (*ii*) ortonormirani dakle ih ima $\leq$ dim $K_{r1} = r$; a to se upravo i iskazuje relacijom (*iii*).

——→ **3.4. T e o r e m.** ***Neka je*** $Cl\,G$ ***skup svih klasâ (razredâ) konjugiranosti grupe G; neka je*** $H = HG$ ***skup svih nesvodljivih neekvivalentnih unitarnih reprezentacija od G, a*** $\chi\,HG$ ***skup pripadnih karakterâ***

(1) $$g \in G \to \chi(g) = \mathrm{Tr}\,h(g) \quad (h \in HG);$$

ako je G konačno, tada funkcije* (1) *čine bazu vektorskog prostora

(2) $$R(i)^{Cl\,G}; \text{ vrijedi}$$

(3) $$\dim R(i)^{Cl\,G} = k\,HG\ (\equiv r).$$

To znači da sa r označujemo broj razreda konjugiranosti grupe G.

Drugim riječima, prostor kompleksnih funkcija koje su definirane u skupu $Cl\,G$ ***svih razreda ima dimenziju upravo r.***

Dokaz teorema 3.4 izvest ćemo iz Burnside-ova teorema 2.11. Naime, umjesto člana $F|Cl\,G$ iz prostora (2) možemo promatrati odgovarajuću funkciju $f|G$ od G u $R(i)$ stavljajući $x \in G \to fx = f\,Clx$, pri čemu je $x \in Clx \in Cl\,G$. Drugim riječima $f|G$ je konstanta $f\,A$ na svakom razredu $A \in Cl\,G$.

No, prema teoremu 2.11 funkcije $x \in G \to h_{ij}(x)$, $(h \in HG)$ čine bazu u prostoru $R(i)^G = P$ pa je dakle

$$fx = \sum_{i,j,h} C_{ij}{}^{(h)} h_{ij}(x), \quad (h \in HG,\ i, j = 1, 2, \ldots, s(h);$$

$h(x)$ je formata $(s(h), s(h))$; $C_{ij}{}^{(h)}$ su konstante).

Pišući tu umjesto x izraz $g^{-1}xg$ za proizvoljno $g \in G$ izlazi (zbog $fx = f(f^{-1}xg)$):

$$f(x) = \sum_{i,j,h} C_{i,j}{}^{(h)} h_{ij}(g^{-1}xg) = \sum_{i,j,h} C_{i,j}{}^{(h)} [h(g^{-1})\,h(x)\,h(g)]_{ij} =$$

$$= \sum_{i,j,h} C_{i,j}{}^{(h)} \sum_{\alpha\beta} h(g^{-1})_{i\alpha} (h(x))_{\alpha\beta} (h(g)_{\beta j}$$

Sumirajući te relacije po $g \in G$ izlazi

$$k\,G \cdot fx = \sum_{i,j,h} C_{i,j}{}^{(h)} \sum_{\alpha\beta} (h\,(x))_{\alpha\beta} \sum_{g} h\,(g^{-1})_{i\alpha}\,(h\,(g))_{\beta j} =$$

$$= (\text{zbog } h\,(g^{-1})_{i\alpha} = \overline{h\,(g)_{\alpha i}}) = \sum_{i,j,h} C_{ij}{}^{(h)} \sum_{\alpha,\beta} (h_{\alpha\beta}\,(x) \sum_{g} h\,(g)_{\beta j}\, \overline{h\,(g)_{\alpha i}}.$$

Dakle

$$k\,G \cdot fx = \sum_{i,j,h} C_{ij}{}^{(h)} \sum_{\alpha\beta} h\,(x)_{\alpha\beta} \cdot (h_{\beta j},\, h_{\alpha i}).$$

Po teoremu 2.10 (i) je $(h_{\beta j},\, h_{\alpha i}) = \dfrac{k\,G}{s\,(h)}\, \delta_{\alpha\beta}\, \delta_{ij}$; zato prethodna relacija postaje dijeleći je sa $k\,G$:

$$fx = \sum_{i,j,h} C_{ij}{}^{(h)} \sum_{\alpha\beta} h_{\alpha\beta}\,(x)\, \frac{1}{s\,(h)}\, \delta_{\alpha\beta}\, \delta_{ij};$$

dakle se može pretpostaviti $\alpha = \beta$, $i = j$:

$$fx = \sum_{i,h} C_{ii}{}^{(h)} \sum_{\alpha} h_{\alpha\alpha}\,(x)\, \frac{1}{s\,(h)} = \sum_{i,h} \frac{1}{s\,(h)}\, C_{ii}{}^{(h)}\, \mathrm{Tr}\, h\,(x),$$

tj.

$$fx = \sum_{i,h} \frac{1}{s\,(h)}\, C_{ii}{}^{(h)}\, \mathrm{Tr}\, h, \quad (i = 1, 2, \ldots, s\,(h),\ h \in HG).$$

Time je dokazano da se fx izražava pomoću funkcijâ $\mathrm{Tr}\, h\,(x)$, $(h \in HG)$. Linearna nezavisnost funkcija $g \to \mathrm{Tr}\, h\,(g)$, $(h \in HG)$ iskazana je u § 3.2.1.

$\longrightarrow$ **3.4.1. Korolar.** ***Broj unitarnih neekvivalentnih reprezentacija konačne grupe G jednak je broju r (= k Cl G) razredâ konjugiranosti grupe G.***

3.4.2. Teorem o reprezentaciji komutativnih grupa. *Svaka nesvodljiva unitarna reprezentazija konačne komutativne grupe G je numerička, tj. dunjine* 1; *takvih neekvivalentnih reprezentacija ima upravo $r = k\,G$.*

Naime, ako je G komutativna grupa, tada je svaki razred konjugiranosti jednočlan pa je $k\,Cl\,G = k\,G$, tj. $r = n$. Zato Burnside-ova jednakost (4) u § 2.11. postaje

$$s_1{}^2 + s_2{}^2 + \cdots + s_n{}^2 = n$$

što zajedno sa $s_\nu \in \{1, 2, \ldots\}$ daje $s_\nu = 1$ za $\nu = 1, 2, \ldots, n$. Drugim riječima, teorem 3.4.2. je dokazan.

$\longrightarrow$ **3.5. Teorem.** ***Neka je HG skup svih nesvodljivih unitarnih neekvivalentnih reprezentacija konačne grupe G; ako je u bilo koja unitarna reprezentacija od G u prostoru U, tada svakom $h \in HG$ pripada jedan jedini broj $u_h \in \{0, 1, 2, \ldots\}$ — — učestalost ili kratnost ireducibilne reprezentacije h u reprezentaciji u — sa svojstvom***

$$u = diag\,[\cdot\ \cdot \underbrace{hh \cdot h \cdot}_{u_h} \cdot\ ]_{h \in HG}$$

ili simbolički

(1) $$u = \sum_{h \in HG} u_h h;$$

vrijedi

(2) $$u_h = \frac{1}{kG} (\chi(u), \chi(h));$$

pri tom $u_h h$ označuje kvazidijagonalnu matricu diag $[\underbrace{h, h, \ldots, h}_{u_h}]$.

Dokaz. U § 2.7.1 samo dokazali *postojanje* neodrečnih cijelih brojeva u_h za koje vrijedi (1); dokažimo sada da su ti brojevi određeni *jednoznačno.* Prelazeći u (1) na pripadne karaktere imamo

(3) $$\chi(u) = \sum_h u_h \chi(h).$$

Neka je $h' \in HG$ fiksirano; tada imamo pripadni karakter $\chi(h')$; množeći (3) hermitski-skalarno sa $\chi(h')$ dobivamo

(4) $$(\chi(u), \chi(h')) = \sum_h u_h (\chi(h), \chi(h')).$$

Odatle prema 3.2.1 izlazi

(5) $$(\chi(u), \chi(h')) = \sum_{h \in HG} u_h (\delta_{h, h'}) kG.$$

Kako sumandi pri $h \neq h'$ otpadaju preostaje samo slučaj $h = h'$ pa (5) daje

$(\chi(u), \chi(h)) = u_h kG$ za svako $h \in HG$. A to se i tvrdi jednakošću (2).

⟶ **3.5.1.** ***Teorem o regularnoj reprezentaciji konačne grupe G. Takozvana regularna reprezentacija***

(1) $$\begin{cases} g \in G \to d_g, \text{ pri čemu je za } x, y \in G: \\ d_g(x, y) = \delta_{x, gy} = \begin{matrix} 1 \\ 0 \end{matrix} \text{ pri } \begin{matrix} x = gy \\ x \neq gy \end{matrix} \end{cases}$$

jest unitarna reprezentacija grupe; njen karakter χ^{reg} zadovoljava

(2) $$\chi^{reg}(g) = \delta_{1g} = \begin{matrix} 1 \\ 0 \end{matrix} \text{ pri } \begin{matrix} 1 = g \in G \\ 1 \neq g \in G. \end{matrix}$$

Vrijedi

(3) $$d_g = \sum_{h \in HG} s_h h,$$

tj. svaka ireducibilna unitarna reprezentacija h grupe G pojavljuje se u regularnoj reprezentaciji upravo s_h puta, gdje s_h označuje duljinu reprezentacije h.

D o k a z. U § 1.6. dokazano je da je pridruživanje (1) zaista reprezentacija od G; formula (2) dokazana je u § 3.1.1. Dokažimo da je d_g unitarno, tj. da je

$$(d_g\, d_g^\star)\,(x, y) = \delta_{x,y}. \tag{4}$$

No,

$$\sum_{z \in G} d_g\,(x, z)\,(d_g)^\star\,(z, y) = \sum_{z \in G} \delta_{x,gz}\,\overline{\delta_{y,gz}}. \tag{5}$$

Ako je $x=y$, onda je $x=gz_0$ za neko $z_0 \in G$ pa je $\delta_{xgz_0}\overline{\delta_{xgz_0}} = 1 = \delta_{xx}$. Ako je $x \neq y$, onda relacije $x=gz=y$ ne mogu biti ispunjene pa je zato bar jedan od brojeva δ_{xgz}, δ_{ygz} jednak 0, tj. $=\delta_{xy}$. To znači da je zaista $(5)_2 = \delta_{xy}$; dakle (4) stoji.

Dokažimo (3). Primijenimo gornji teorem 3.5. na unitarnu reprezentaciju d; obrasci (1) i (2) iz § 3.5. onda daje

$$d = \sum_{h \in GH} d_h\, h,$$

$$d_h \equiv \frac{1}{k\,G}\,(\chi^{reg}, \chi\,(h)).\ \text{No ovo je dalje } = \frac{1}{k\,G} \sum_{g \in G} \chi^{reg}\,(g)\,\chi\,(g) =$$

$$= \frac{1}{k\,G}\,\chi^{reg}\,(1)\,\chi\,(1) + \sum_{1 \neq g} \chi^{reg}\,(g)\,\chi\,(g) = \frac{1}{k\,G} \cdot k\,G \cdot s_h + \sum_{1 \neq g} 0 \cdot\ \chi\,(g) = s_h.$$

Dakle je zaista $d_h = s_h$.

Kombinirajući teoreme 3.2, 3.5 izlazi da je u teoremu 3.2 dopušteno brisati pridjev „Nesvodljiv"; time dobivamo

—→ **3.6. T e o r e m.** ***Matrične unitarne reprezentacije h, h' konačne grupe G ekvivalentne su onda i samo onda ako imaju jednak karakter.***

3.7. Primitivni karakteri grupe G. Tablica.

3.7.1. D e f i n i c i j a. *Karakter svake nesvodljive unitarne reprezentacije grupe zovemo* **primitivni karakter** *te grupe*

Prema osnovnom teoremu 3.4, odnosno prema 3.4.1. broj primitivnih karaktera konačne grupe G je $r \equiv$(broj razreda konjugiranosti od G).

3.7.2. Korisno je da se od primitivnih karaktera napravi ovakva tablica.

Tablica primitivnih karaktera grupe G.

Pri tom je $d_1{}^2 + d_2{}^2 + \cdots + d_r{}^2 = n\,(\equiv k\,G)$.

	Cl_1	Cl_2	$\cdot\cdot$	Cl_j	$\cdot\cdot$	Cl_r
	1	r_2	$\cdot\cdot$	r_j	$\cdot\cdot$	r_r
$h^{(1)}$	$d_1 = 1$	1	$\cdots$		$\cdot\cdot$	1
$h^{(2)}$	d_2	$\chi_2^{(2)}$	$\cdots$		$\cdot\cdot$	$\chi_r^{(2)}$
$\downarrow\ \cdot$	$\cdot$	$\cdot$	$\cdots$		$\cdots$	
$h^{(i)}$	d_i	$\cdot$	$\cdot\cdot$	$\chi_j^{(i)}$	$\cdots$	
$\cdot$	d_r	$\chi_r^{(r)}$	$\cdots$		$\cdot\cdot$	$\chi_r^{(r)}$
$h^{(r)}$	$\cdot$	$\cdot$	$\cdots$		$\cdots$	

Prvi vanjski (gornji) *redak* tablice sadrži nanizano svih r razreda grupe G; posebno je razred Cl_1 sastavljen od neutralnog člana grupe G; neposredno ispod Cl_j stoji r_j ($=k\,Cl_j=$ broj članova u Cl_j); time se dobije drugi vanjski redak; prvi vanjski *stupac* sačinjavaju svih r ireducibilnih reprezentacija $h^{(1)}$, $h^{(2)}, \ldots, h^{(r)}$; vrijednosti karaktera $\chi^{(i)}$ sastavljene su u i-ti redak, tako da $\chi_j^{(i)}$ označuje vrijednost karaktera χ^i u klasi Cl_j. Specijalno se u *prvi stupac* tablice stavlja $\chi_1^{(i)}=d_i=$ dimenzija reprezentacije; naime $h^{(i)}(1)$ je identični operator pa mu je trag jednak duljini d_i jedinične matrice kojom je operator $h^{(i)}(1)$ predstavljen (tu je 1 jedinični član grupe).

3.7.3. Primjer. *Tablica primitivnih karaktera kvaternionske grupe* glasi

	Cl_1	Cl_2	Cl_3	Cl_4	Cl_5
	1	1	2	2	2
$h^{(1)}$	1	1	1	1	1
$h^{(2)}$	1	1	1	-1	-1
$h^{(3)}$	1	1	-1	1	-1
$h^{(4)}$	1	1	-1	-1	1
$h^{(5)}$	2	-2	0	0	0

Naime razredi grupe $Qu=\{1, -1, i\ -i, j, -j, k, -k\}$ jesu:

$$\{1\},\ \{-1\},\ \{-i, i\},\ \{-j, j\},\ \{-k, k\}.$$

Dakle je $r=5$, $n=k\,Qu=8$.

Za dimenzije d_1, d_2, d_3, d_4, d_5 reprezentacije rješavamo jednadžbu

$$d_1^2+d_2^2+d_3^2+d_4^2+d_5^2=8$$

u prirodnim brojevima i pri uslovu $d_1 \leq d_2 \leq d_3 \leq d_4 \leq d_5$.

Tada nužno izlazi

$$d_1=d_2=d_3=d_4=1,\ d_5=2.$$

Time se dobije prvi stupac tablice χ.

Zbog unitarnosti reprezentacije prva 4 retka matrice χ su ispunjena sa ± 1; lako se provjeri da napisane vrijednosti karakterâ $\chi^{(1)}$, $\chi^{(2)}$, $\chi^{(3)}$, $\chi^{(4)}$ odgovaraju.

Reprezentacija h dimenzije 2 dana je ovim matricama:

$$h(1)=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\ h(-1)=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix},\ h(i)=\begin{bmatrix}0 & i\\ i & 0\end{bmatrix},\ h(-i)=\begin{bmatrix}0 & -i\\ -i & 0\end{bmatrix},$$

$$h(j)=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\ h(-j)=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},\ h(k)=\begin{bmatrix}-i & 0\\ 0 & i\end{bmatrix},\ h(-k)=\begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix}.$$

Pri tom argument i u $h(i)$ nije isto što i unutar [ ]. Ta reprezentacija je izomorfizam.

—→ **3.7.4.** ***Teorem o tablici karakterâ. Neka je*** $\chi = [\chi_j^{\,i}]_{i,j=1,2,\ldots,r}$ ***tablica primitivnih karaktera konačne grupe*** G***; tada vrijedi***

(1) $$\sum_{\rho=1}^{r} r_\rho \chi_\rho^{\,i} \overline{\chi_\rho^{\,j}} = kG \cdot \delta_{ij} \qquad \textit{(ortogonalnost redaka)}$$

(2) $$\sum_{\rho=1}^{r} \chi_i^{\,\rho} \overline{\chi_j^{\,\rho}} = \frac{kG}{r_i} \delta_{ij} \qquad \textit{(ortogonalnost stupaca).}$$

Dokaz formule (1). Za primitivne karaktere $\chi^{(i)}$, $\chi^{(j)}$ imali smo

$$(\chi^i, \chi^j) = kG\,\delta_{ij}$$

(v. § 3.2.1), tj.

(3) $$\sum_{g \in G} \chi^{(i)}(g)\, \overline{\chi}^{(j)}(g) = kG\,\delta_{ij}.$$

No, kako je $h^{(j)}(g)$ unitarno, to je

(4) $$\overline{\chi}^{(j)}(g) = \chi^{(j)}(g^{-1}), \text{ pa (3) postaje}$$

(5) $$\sum_{g \in G} \chi^i(g)\, \chi^j(g^{-1}) = kG\,\delta_{ij}.$$

Kada pri sumaciji (5) član $g \in G$ prođe razredom Cl_ρ od r_ρ članova, tada i g^{-1} leži u nekom razredu pa je produkt $\chi^{(i)}(g)\,\chi^{(j)}(g^{-1})$ konstanta u svakom razredu; zato se sumacija po G u (5) može nadomjestiti na sumaciju po skupu razredâ pa (5) zbog (4) daje upravo traženu formulu (1).

Dokaz formule (2). Podijelimo li (1) sa kG izlazi

(5) $$\sum_{\rho=1}^{r} \chi_\rho^{\,i} \frac{\overline{\chi_\rho^{\,j}}\, r_\rho}{kG} = \delta_{ij} \qquad (i, j = 1, 2, \ldots, r).$$

Izraz $(5)_1$ je produkt i-tog retka matrice χ i j-tog stupca matrice b za koju je $b_{\rho j} = \frac{r_\rho}{kG} \overline{\chi_\rho^{\,j}}$ pa kako $i, j \in \{1, \ldots, r)$ znači to da je $\chi b = 1\,(r)$, odnosno $b = \chi^{-1}$. Zato jednakost $\chi^{-1}\chi = 1\,(r)$ postaje $b\chi = 1\,(r)$, odnosno $\sum_{\rho=1}^{r} b_{i\rho} \chi_i^{\,\rho} = \delta_{ij}$. tj.

(6) $$\sum_{\rho=1}^{r} \frac{r_i}{kG} \overline{\chi_i^{\,\rho}} \chi_j^{\,\rho} = \delta_{ij} \qquad (i, j = 1, 2, \ldots, r)$$

Množeći jednakost (6) sa $\frac{kG}{r_i}$ dobije se upravo traženo (2).

Time je teorem 3.7.4. dokazan. Pri dokazu nam je služio

—→ **3.7.5. Teorem.** ***Ako je*** $g \to h(g)$ ***unitarna reprezentacija konačne grupe*** G***, tada je i*** $g \to h(g^{-1})^\star$ ***unitarna reprezentacija i vrijedi*** $\mathrm{Tr}\, h(g^{-1}) = \mathrm{Tr}\, h(g)$ (v. § 4.0.1).

Imamo

$$h(g^{-1})^\star = \left((h(g))^{-1}\right)^\star = h(g)$$

kao i

$$\operatorname{Tr} h(g^{-1}) = \operatorname{Tr}\left(h(g)\right)^{-1} = \operatorname{Tr}\left(h(g)\right)^\star = \overline{\operatorname{Tr} h(g)}.$$

O algebarskoj naravi karaktera reprezentacije.

—→ 3.8. **Teorem.** ***Za svaku unitarnu reprezentaciju $g \to u(g)$ konačne grupe G odgovarajući karakter $\chi g \to \operatorname{Tr} u(g)$ je cio algebarski broj i to korijen jedinice ili suma od konačno mnogo korijena jedinice.***

Dokaz. Za dano $x \in G$ neka je $\pi = \pi(x)$ period od x (v. 17 § 7.9); tada matrice

$$1,\ u(x),\ u(x^2),\ \ldots,\ u(x^{\pi-1})$$

obrazuju određenu cikličku grupu C. Neka je f nesvodljiva unitarna reprezentacija od C; kako je f nesvodljiva, to je f matrica duljine 1 (isp. § 3.4.2), jer broj razreda u C je upravo kC - naime, razredi su jednočlani i oblika $\{g\}$ $\{g \in C\}$. Burnsideva relacija (v. § 2.11 (4)) tada glasi $\sum_{i=1}^{kC} d_i^2 = kC,\ d_i \in N$; odatle nužno izlazi $d_i = 1$.

Dakle je zaista $f(x)$ neki broj b, tj. $f(x) = b$.

Zbog $x^\pi = 1$ i $f(x^\pi) = f(1) = 1$, odnosno $(fx)^\pi = 1$ vrijedi

$$b^\pi = 1 \tag{1}$$

Dakle je broj b korijen jedinice reda π.

No, polazna reprezentacija u od C je direktna suma nesvodljivih reprezentacijâ $f(x)$, dakle se zapisuje dijagonalno a vrijednosti b po dijagonali zadovoljavaju (1): dakle je $\chi(x)$ zaista suma korijenâ jedinice π-tog reda. Kako je broj b cio algebarski broj, a suma od konačno mnogo cijelih algebarskih brojeva opet je cio algebarski broj (32 § 1.7.6), teorem 3.8.1. je dokazan.

3.9. O ireducibilnim (nesvodljivim) reprezentacijama

Znamo da su nesvodljive reprezentacije osnovni materijal iz kojih se grade sve reprezentacije (v. t. 2.7). Zato je važno spoznati da li je dana unitarna reprezentacija svodljiva ili nije te naći one ireducibilne reprezentacije iz kojih se dana reprezentacija izgrađuje.

—→ **3.9.1. Teorem (kriterij o ireducibilnosti).** ***Reprezentacija $u(g)$, $(g \in G)$: je nesvodljiva onda i samo onda ako joj je skalarni kvadrat karaktera jednak broju kG članova grupe G, tj.***

$$(\chi u,\ \chi u) = kG, \tag{1}$$ ***odnosno***

$$u_1^2 + u_2^2 + \cdots + u_r^2 = 1 \tag{2}$$ ***pri čemu je***

$$u = u_1 h_1 + u_2 h_2 + \cdots + u_r h_r \tag{3}$$

jednoznačni rastav od u na ireducibilne reprezentacije $h_1, h_2, \ldots, h_r$ (isp. § 3.5). Ako je u svodljivo, tada u (1), (2) umjesto znaka = stoji znak $>$, i obrnuto (isp. §. 2.9).

D o k a z. Ako je u nesvodljivo, tada je $u = h_{\rho_0}$ za neko jednoznačno određeno $\rho_0 \in \{1, 2, \ldots, r\}$, tj. $u_{\rho_0} = 1$, $u_\rho = 0$ za preostale ρ; to znači da se (2) svodi na $u_{\rho_0}{}^2 = 1$. I obrnuto, vrijedi li (2), tada je jedan jedini sumand u_{ρ_0} u (2) jednak 1 a svaki preostali je $= 0$, što znači da se (3) svodi na $u = h_{\rho_0}$ tj. u je nesvodljivo.

Sa druge strane, prelazeći na karaktere relacija (3) daje

$$\chi = u_1 \chi_1 + u_2 \chi_2 + \cdots + u_r \chi_r \qquad \text{pa je}$$

$$(\chi, \chi) = \left(\sum_{\rho=1}^{r} u_\rho \chi_\rho, \sum_{\sigma=1}^{r} u_\sigma \chi_\sigma \right) = \sum_{\rho, \sigma=1}^{r} u_\rho u_\sigma (\chi_\rho, \chi_\sigma)$$

$$= (\text{prema § 3.2.1}) = \sum_{\rho, \sigma=1}^{r} u_\rho u_\sigma k G \delta_{\rho\sigma} = \sum_{\rho=1}^{r} u_\rho^2 k G, \text{ tj.}$$

$$(\chi, \chi) = \left(\sum_{\rho=1}^{r} u_\rho^2 \right) k G. \tag{4}$$

Iz (4) se neposredno zaključuje da u teoremu 3.9.1 vrijedi i ono što je rečeno o svodljivim reprezentacijama.

⟶ **3.9.2.** ***Teorem o duljini nesvodljivih reprezentacija. Duljina d_i svake ireducibilne reprezentacije h_i konačne grupe G je divizor od kG, tj. $d_i \mid kG$, ($i = 1, 2, \ldots, r$).***

D o k a z. Prema teoremu 3.7.4 (1) imamo

$$\sum_{\rho=1}^{r} r_\rho{}^i \chi_\rho{}^i \overline{\chi_\rho{}^i} = kG.$$

Odatle dijeleći sa d_i:

$$\sum_{\rho=1}^{r} \frac{r_\rho \chi_\rho{}^i}{d_i} \overline{\chi_\rho{}^i} = \frac{kG}{d_i}. \tag{1}$$

No, prema teoremu 3.8. broj $\chi_\rho{}^i$ je cio algebarski broj; takav je i broj $\overline{\chi_\rho{}^i}$ te $\frac{r_\rho}{d_i} \chi_\rho{}^i$ (isp. 3.9.5.3) kao i sumand u (1); dakle je i suma $(1)_1$ član od EA ($\equiv$skup cijelih algebarskih brojeva); dakle je također $\frac{kG}{d_i} \in EA$, a time i $\frac{kG}{d_i} \in D$ (v. 32, § 1.2.2.1).

3.9.3. Brojevi $C_{ij\rho}$ ($i, j, \rho = 1, 2, \ldots, r$). Neka je $g \in G \to h(g)$ nesvodljiva reprezentacija duljine d grupe G; neka su

$$Cl_1, Cl_2, \ldots, Cl_r$$

svi razredi konjugiranosti grupe G; u vezi s razredom Cl_i promatrajmo matricu

$$(1) \qquad A_i \equiv \sum_{g_i} h(g_i) \quad (g_i \in Cl_i).$$

Na taj način imamo i matricu

$$A_i A_j = \sum_{g_i \in Cl_i}^{r} h(g_i) \sum_{g_j \in Cl_j} h(g_j) = \sum_{g_i, g_j} h(g_i) h(g_j).$$

Neka $c_{ij\rho}$ kazuje na koliko se načina produkt $h(g_i) h(g_j)$ ostvaruje kao $h(g_\rho)$ pri $g_\rho \in Cl_\rho$; naime, prema 17 § 15.5 produkt $Cl_i Cl_j$ je unija određenih razreda Cl_ρ; tada imamo jednakosti:

$$(2) \qquad Cl_i Cl_j = \sum_{\rho=1}^{r} c_{ij\rho} Cl_\rho, \quad (i, j = 1, 2, \ldots, r), \quad c_{ij\rho} \in \{0, 1, 2, \ldots\}.$$

3.9.4. Brojevi η_ρ $(\rho = 1, 2, \ldots, r)$. Matrica A_i komutira sa matricom $h(g)$ za svako $g \in G$ jer

$$h(g) A_i = h(g) \sum_{g_i} h(g_i) = \sum_{g_i} h(g) h(g_i) = \sum_{g_i} h(gg_i) = (\text{jer je}$$

$$g\, Cl_i = Cl_i\, g) = \sum h(g_i g) = \sum h(g_i) h(g) = \left(\sum h(g)\right) h(g) = A_i h(g).$$

Prema 33 § 2.8. zaključujemo da vrijedi

3.9.4.1. Lema. *Postoji određen skalar* η_i *za koji je*

$$(1) \qquad A_i = \eta_i \cdot 1_d;$$

vrijedi

$$(2) \qquad \eta_i = \frac{r_i \chi_i}{d};$$

pri tom r_i *kazuje koliko* Cl_i *ima članova.*

Druga jednakost leme izlazi iz prve jednakosti promatrajući pripadne karaktere.

3.9.4.2. Lema.

$$\frac{r_i \chi_i}{d} \cdot \frac{r_j \chi_j}{d} = \sum_{\rho=1}^{r} c_{ij\rho} \frac{r_\rho \chi_\rho}{d}; \quad c_{ij\rho} \in \{0, 1, 2, \ldots\}; \quad (i, j, \rho = 1, 2, \ldots, r).$$

To izlazi iz (2) u 3.9.4. na osnovu (1) iz 3.9.5.1.

3.9.4.3. Lema. *Brojevi*

$$\frac{r_i \chi_i}{d} \quad (i = 1, 2, \ldots, r)$$

su cijeli algebarski brojevi.

Ta će činjenica odmah izaći kao posljedica ove leme:

3.9.4.4. Lema. *Zadan je proizvoljan r-član niz brojeva*

(1) $$y_1, y_1, \ldots, y_r$$

od kojih je bar neki $\neq 0$; *neka su* $a_{j\rho}$ $(j, \rho = 1, 2, \ldots, r)$ (*cijeli*) *racionalni brojevi*; *tada svaki broj* x *za koji je*

(2) $$xy_j = \sum_{j=1}^{r} a_{j\rho}\, y_\rho \quad (j = 1, 2, \ldots, r)$$

est (*cio*) *algebarski broj* (isp. 32, § 1.2.1).

Naime, svedemo li jednadžbe (2) na nulti oblik, dobije se r linearnih *homogenih* jednadžbi za r brojeva (1); kako je bar jedan od brojeva (1) različit od 0, mora determinanta sistema (2) biti $=0$, tj. $\det(a - x) = 0$; razvijemo li tu determinantu kao x-polinom, izlazi

$$(-1)^r x^r + f_{r-1} x^{r-1} + \cdots + f_1 x + f_0 = 0.$$

No, koeficijenti f_ρ se tvore iz a_{ij} pomoću prve 3 računske operacije; zato su f_r (cijeli) racionalni brojevi, pa je dakle x (cio) algebarski broj.

Istinitost leme 3.9.5 3. izlazi iz 3.9.5.4. uzimajući za

$$x = \frac{r_i \chi_i}{d}, \quad y_j = \frac{r_j \chi_j}{d}, \quad a_{j\rho} = c_{j\rho}$$

i promatrajući za svako $i \in \{1, 2, \ldots, r\}$ odgovarajući sistem iz 3.9.5.2.

U vezi s teoremom 3.9.2. može se dokazati ovakvo pooštrenje od 3.9.2.

3.9.5. Teorem (Ito). *Duljina d svake ireducibilne reprezentacije konačne grupe G je djelilac indeksa svake maksimalne normalne komutativne podgrupe od G.*

Tako npr. kvaternionska grupa *Qu* ima 8 članova pa zato teoremom 3.9.2. dobivamo da je $d \in \{1, 2, 4, 8\}$. Sa druge strane, *Qu* ima 5 normalnih komutativnih podgrupa, od čega su 3 maksimalne i imaju po 4 člana; to znači da je indeks svake od njih jednak 2. Prema 3.9.6 mora dakle biti $d \mid 2$, tj. $d \in \{1, 2\}$. U tablici 3.7.3 vidimo stvarno da je $d_1 = d_2 = d_3 = d_4 = 1$, $d_5 = 2$. Ujedno na osnovu teorema 3.9.1. uvjeravamo se da je svih pet karaktera u tablici 3.7.3. primitivno.

3.9.6. Teorem o ireducibilnim jednodimenzionalnim predstavljanjima. *Svaka konačna grupa G ima upravo* $s = kG/kG'$ *ireducibilnih jednodimenzionalnih predstavljanja a proizlaze iz s ireducibilnih predstavljanja faktorske komutativne grupe* G/G'; *pri tom je* G' *derivat grupe* G (v. 17 § 18.3).

Dokaz. Prema 17 § 18.6. grupa G' je invarijantna podgrupa od G, a faktorska grupa G/G' je komutativna; zato ona dopušta upravo $s = kG/G' = \frac{kG'}{kG}$ nesvodljivih predstavljanja koja su nužno jednodimenzionalna (§ 3.4.2) i svaka od njih daje predstavljanje od G.

Sa druge strane, ako je h bilo koje jednodimenzionalno predstavljanje konačne grupe G, onda je hG kao konačna multiplikativna podgrupa od $R(i)$ nužno ciklična i izomorfna sa G/y, gdje je $y=\{g;\ g\in G,\ hg=1\}$ (isp. 17 § 12.5.5); prema 17 § 18.6 (*ii*) vrijedi $y\supset G'$, pa zato h možemo dobiti kao jednu od gornjih s reprezentacija.

Kako je i $g\in G\to \det h(g)$ jednodimenzionalno predstavljanje grupe G, iz posljednjeg zaključka izlazi

3.9.6.1. Teorem. *U skupu unitarnih predstavljanja, u, konačne grupe G čine oni u za koje je* $\det u=1$ *normalni divizor kojemu je faktorska grupa ciklična.*

4. VEZE MEĐU REPREZENTACIJAMA ZADANE GRUPE

4.0. Uvodna razmatranja. Riječ je o tome da se zadanoj (unitarnoj) reprezentaciji

(1) $$g\in G\to h(g) \quad \text{grupe } G,$$

pri čemu je $\boldsymbol{h}(g)$ operator u nekom vektorskom prostoru U s konačno mnogo dimenzija, pridruži opet neka unitarna reprezentacija sa svojim prostorom operiranja, odnosno da se *uređenu paru* (h_1, h_2) *reprezentacija pridruži njihov proizvod* $h_1\times h_2$ kao određena reprezentacija. Općenito iz poznatih reprezentacija konstruiraju se nove reprezentacije iste grupe u nadi da se nađu sve ireducibilne reprezentacije. Pri tom važnu ulogu ima teorem 3.4. prema kojem je svaka unitarna reprezentacija $\boldsymbol{u}$ određena, *do na ekvivalentnost*, svojim karakterom, tj. funkcijom $g\in G\to\chi(g)=Tr\,\boldsymbol{u}(g)$.

4.0.1. Primjer kontragredijentnih reprezentacija. Pridružimo li reprezentaciji $g\in G\to h(g)$ grupe G preslikavanje $h^{\sim}(g)=h(g^{-1})^T$, vidi se da se dobije reprezentacija grupe G, a zove se *kontragredijent* reprezentacije h (isp. § 3.7.5).

4.1. Produkt reprezentacijâ. Zadan je uređen par $(h^{(1)}, h^{(2)})$ unitarnih reprezentacija

$$g\in G\to h^{(1)}(g) \text{ nad prostorom } U^{(1)} \text{ i s karakterom } \chi_1(g)=Tr\,h^{(1)}(g),$$

$$g\in G\to h^{(2)}(g) \text{ nad prostorom } U^{(2)} \text{ i s karakterom } \chi_2(g)=Tr\,h^{(2)}(g).$$

Odaberimo u $U^{(1)}$ bazu $e^{(1)}=(e_1{}^1, e_2{}^1, \ldots, e_{s_1}{}^1)$, a u $U^{(2)}$ vektorsku bazu $e^{(2)}=(e_1{}^2, e_2{}^2, \ldots, e_{s_2}{}^2)$. Pri $\varepsilon\in\{1,2\}$ operator $\boldsymbol{h}^{(\varepsilon)}(g)$ zapisuje se u bazi $e^{(\varepsilon)}$ matricom $h^{(\varepsilon)}(g)$, pri čemu je

$$\boldsymbol{h}^{(\varepsilon)}(g)\,e_i{}^{(\varepsilon)}=\sum_{\alpha=1}^{s_\varepsilon} h^{(\varepsilon)}{}_{\alpha i}(g)\,e^{(\varepsilon)}{}_{\alpha i}.$$

4.1.1. No, uređenoj dvojki $(U^{(1)}, U^{(2)})$ prostorâ pridružujemo (isp. 34, § 2.1.1) tzv. *tenzorski produkt* $U^1\otimes U^2$ prostorâ U^1, U^2 i to kao prostor kojemu simbolički produkti

$$(e_i{}^1, e_j{}^2)\overset{\text{def}}{=\!=}e_i{}^1\otimes e_j{}^2\overset{\text{def}}{=\!=}e_i{}^1 e_j{}^2\ (i=1,2,\ldots,s_1;\ j=1,2,\ldots,s_2)$$

čine bazu; dakle je $\dim(U^1 \otimes U^2) = \dim U^{(1)} \dim U^{(2)}$. U tom prostoru, za zadano $g \in G$, određen je ovakav linearan operator h:

(1) $$h(g)\, e_i^1 e_j^2 \overset{\text{def}}{=} h^{(1)}(g)\, e_i^{(1)} h^{(2)}(g)\, e_j^{(2)} \overset{\text{def}}{=} \sum_{\alpha,\beta} h_{\alpha i}^{(1)}(g)\, h_{\beta j}^{(2)}(g)\, e_\alpha^1 e_\beta^2.$$

4.1.2. Pridruživanje $g \to h(g)$ zadovoljava uslovu

(2) $$h(g_1 g) = h(g_1)\, h(g) \quad \text{(teorem 4.1.3)},$$

pa je ono zato određena reprezentacija grupe G nad prostorom $U_1 \otimes U_2$; reprezentacija h zove se *proizvod* ili *produkt reprezentacije* $h^{(1)}$ *i reprezentacije* $h^{(2)}$ grupe G pa pišemo $h = h^{(1)} h^{(2)}$ odnosno

(3) $$g \in G \to h(g) = h^{(1)} h^{(2)}(g).$$

4.1.3. Teorem. *Iz $g_1, g \in G$ izlazi $h(g_1 g) = h(g_1)\, h(g)$.*

Riječ je o tome da se provjere relacije

(3) $$h(g_1 g)\, e_i^1 e_j^2 = h(g_1)\, h(g)\, e_i^1 e_j^2 \quad (i = 1, 2, \ldots, s_1; j = 1, 2, \ldots, s_2).$$

No,

$$(4)_1 = h(g_1 g)\, e_i^1 e_j^2 = (\text{prema } (3)) =$$

$$[h^{(1)}(g_1 g)\, h^{(2)}(g_1 g)]\, e_i^1 e_j^2 = (\text{prema } (2)) =$$

$$[h^{(1)}(g_1)\, h^1(g)\, h^{(2)}(g_1)\, h^{(2)}(g)] = (\text{prema komutaciji i združivanju}) =$$

$$= [h^{(1)}(g_1)\, h^{(2)}(g_1)]\, [h^{(1)}(g)\, h^{(2)}(g)]\, e_i^1 e_j^2 =$$

$$= h(g_1)\, h(g)\, e_i^1 e_j^2 = (4)_2.$$

4.1.4 Teorem. *Ako je reprezentacija h proizvod reprezentacije h^1 od G i reprezentacije h^2 od G, tada je karakter χh od h jednak produktu karaktera χ_1 od h^1 i karaktera χ_2 od h^2, tj. $\chi = \chi_1 \chi_2$ u smislu da vrijedi $g \in G \to \chi(g) = \chi_1(g)\, \chi_2(g)$.*

Naime, dijagonalni članovi matrice $h(g)$ jesu (isp. 26 § 6.6):

$$(h(g)\, e_i^1 e_j^2)_{ij} = (\text{prema (1) stavljajući } \alpha = i,\ \beta = j) = h^1{}_{ii}(g)\, h^2{}_{jj}.$$

Sumiramo li to po $i = 1, 2, \ldots, s_1$ te po $j = 1, 2, \ldots, s_2$ dobije se $\operatorname{Tr} h(g)$, tj. $\chi(g)$ pa je dakle

$$\chi(g) = \sum_{i,j} h^1{}_{ii}(g)\, h^2{}_{jj}(g) = \sum_i h^1{}_{ii} \sum_j h^2{}_{jj}(g) = \chi_1(g)\, \chi_2(g).$$

4.2. Kroneckerov ili tenzorski produkt matrica i produkt reprezentacijâ.

4.2.1. *Direktni ili tenzorski ili Kroneckerov produkt $a \times b$ matrice a* i matrice b definira se kao matrica $a \times b$ za koju je

(1) $$a_{ij}\, b_{i'j'} = (a \times b)_{ii', jj'} [\equiv (a \times b)_{(ii'), (jj')}] \quad \text{(isp. 11 § 14.20).}$$ [1]

[1] Umjesto (i, i') pišemo naprosto ii', ukoliko ne bi bilo zabune.

To znači da se *svaka vrijednost od a* množi *svakom vrijednosti od b* pa je zato skup D_1 $(a \times b)$ redaka od $a \times b$ jednak $D_1 a \times D_1 b$, tj.

(2) $$D_1 (a \times b) = D_1 a \times D_1 b, \text{ te}$$

(3) $$D_2 (a \times b) = D_2 a \times D_2 b;$$ pri tom se u $(2)_2$ i $(3)_2$ radi o *Descartesovu množenju skupova,* dakle za dani skup A i dani skup B imamo

$$A \times B \overset{\text{def}}{=} \{(x, y);\ x \in A,\ y \in B\}.$$

4.2.2. *Unutrašnji direktni produkt* niza $f = f_1 f_2, \ldots$ matricâ i jednakobrojnog niza $\varphi = \varphi_1, \varphi_2, \ldots$ matrica definira se kao niz

$$f \otimes \varphi = f_1 \times \varphi_1, f_2 \times \varphi_2, \ldots$$

4.2.3. *Vanjski direktni produkt niza (skupa) a matricâ i niza (skupa) b* matricâ jest

$$a \times b = \{a_i \times b_j;\ a_i \in a,\ b_j \in b\}.$$

Sad možemo dokazati

—→ **4.2.4. Teorem o vezi množenja reprezentacija s direktnim množenjem matrica.**

Matrica reprezentacije $g \to h(g)$ koja je produkt reprezentacije h^1 i reprezentacije h^2 iste grupe G jest unutrašnji produkt matrica prve reprezentacije i matricâ druge reprezentacije:

$$g \in G \to h^1(g) \times h^2(g).$$

Naime, relacija (1) u 4.1.1. iskazuje da je $(\alpha\beta)$, $(ij))$ — komponenta matrice $h(g)$ jednaka

$$(h(g))_{((\alpha,\beta),(ij))} = (h^{(1)}(g))_{\alpha i} (h^2(g)_{\beta j} = h^1{}_{\alpha i}(g)\, h^2{}_{\beta j}(g), \text{ tj.}$$

$$h_{\alpha\beta,\, ij}(g) = h^1{}_{\alpha i}(g)\, h^2{}_{\beta j} \quad (\alpha, i = 1, 2, \ldots, s_1;\ \beta, j = 1, 2, \ldots, s_2), \text{ tj.}$$

$$h_{\alpha\beta,\, ij}(g) = (h^1(g) \times h^2(g))_{\alpha\beta,\, ij}.$$

A to upravo znači da je $h(g) = h^1(g) \times h^2(g)$.

Dokažimo sada i ovaj teorem koji dolazi pri razmatranju o reprezentacijama:

—→ **4.2.5. Teorem.** ***Skup svih ortogonalnih, odnosno jediničnih, odnosno unitarnih matrica konačna formata čine po određen grupoid u odnosu na direktno množenje matricâ.***

Ograničimo se da dokažemo onaj dio teorema koji se odnosi na unitarne matrice: ako je a unitarna (m, m) — matrica, a b unitarna (n, n) — matrica, tada je $a \times b\ (= c)$ unitarna (mn, mn) — matrica.

Dovoljno je dokazati da je

(1) $$(c_{\cdot jj'},\ c_{\cdot kk'}) = \delta_{(jj'),\,(kk')}.$$

No,

$$(1)_1 \overset{\text{def}}{=} \sum_{(i,i')} c_{(i,i'),\,(j,j')} \overline{c}_{(i,i')\,(k,k')} \overset{\text{def}}{=} \sum_{(ii')} a_{ij}\, b_{i'j'}\, \overline{a}_{ik}\, \overline{b}_{i'k'} =$$

$$= \Big(\sum_i a_{ij} \overline{a}_{ik}\Big)\Big(\sum_i b_{i'j'} \overline{b}_{i'k'}\Big) = \delta_{jk}\, \delta_{j'k'} = \delta_{jj',kk'} = (1)_2.$$

4.3. Direktno množenje grupa i vanjsko direktno množenje skupa matrica.

$\longrightarrow$ **Teorem.** (*i*). *Ako su G_1, G_2 konačne grupe, pa ako je Γ^1 ireducibilna reprezentacija od G_1, a Γ^2 ireducibilna reprezentacija od G_2, tada je vanjski produkt* (1) $\Gamma^1 \times \Gamma^2$ *ireducibilna reprezentacija od direktnog produkta* (2) $G_1 \times G_2$ *grupe G_1 i grupe G_2. Svaka nesvodljiva reprezentacija od* (2) *je oblika* (1).

(*ii*). *Matrica primitivnih karaktera direktnog produkta $G_1 \times G_2$ je direktni produkt tablice primitivnih karaktera od G_1 i tablice primitivnih karaktera od G_2* (isp. § 3.7.2).

Teorem (*ii*) neposredno izlazi iz teorema (*i*). Ilustrirajmo teorem na primjeru.

4.3.1. *Dijedarska grupa D_2 kao $C_2 \times C_2$.* Dijedarska grupa D_2 (isp. 17 § 7.7) sastoji se od rotacije a oko p za π rad koja zadanu pravulju q prevodi u samu sebe, zatim od rotacije b oko p za π rad koja pravulju $p \perp q$ prevodi u samu sebe, zatim od rotacije $ab(=ba)$ i mirovanja e (naravno, pravulje p i q se sijeku). Vidi se da je $D_2 = \{e, a\} \times \{e, b\}$, tj. $D_2 = C_2 \times C_2$, jer su grupe $\{e, a\}$, $\{e, b\}$ izomorfne s cikličnom dvočlanom grupom C_2. Tablica karakterâ od C_2 glasi

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \text{ dakle } \begin{array}{c|cc} C_2 & 1 & 1 \\ \hline \Gamma_0 & 1 & 1 \\ \Gamma_1 & 1 & -1 \end{array}; \text{ prema teoremu } (ii)$$

zaključujemo na osnovu $D_2 = C_2 \times C_2$ da tablica primitivnih karaktera od D_2 glasi

$$\begin{array}{c|cccc} D_2 & 1 & 1 & 1 & 1 \\ \hline \Gamma_0 & 1 & 1 & 1 & 1 \\ \Gamma_1 & 1 & -1 & 1 & -1 \\ \Gamma_2 & 1 & 1 & -1 & -1 \\ \Gamma_3 & 1 & -1 & -1 & 1 \end{array}$$

A to se neposredno provjerava!

5. PRIMJERI O REPREZENTACIJI GRUPA

5.0. Dosad smo imali već nekoliko slučajeva reprezentacija grupâ, i to specijalno: ciklična grupa C_n (§ 1.4), konačne komutativne grupe (§ 1.5), kvaternionska grupa Qu (§ 4.3.1). Sada ćemo navesti još nekoliko slučajeva.

Prema teoremu 3.4, odnosno 3.4.1 važno je odrediti skup ClG klasa konjugiranosti grupe G i posebno broj $r\,(\equiv kClG)$ tih klasa ili razreda te prirodnobrojevna rješenja jednadžbe $d_1^2 + d_2^2 + \ldots + d_r^2 = n$, gdje je $n = kG$.

5.1. Predstavljanje grupe G_T pravilna tetraedra.

5.1.1. Neka je 1 2 3 4 pravilan tetraedar T; tada grupu G_T tetraedra T sačinjavaju: e (identičko preslikavanje), 3 rotacije za π rad, 4 rotacije za $2\pi/3$ rad i 4 rotacije za $4\pi/3$ rad. Dakle je $n = kG_T = 12$. Ispisujemo li odgovarajuće permutacije vrhova 1, 2, 3, 4 grupa G_T se raspada na ova 4 razreda konjugiranosti:

1) $Cl_1=\{e\}$; 2) $Cl_2=$ skup članova reda $2=\{(12)(34), (13)(24), (14)(23)\}$,
3) $Cl_3=\{(123), (214), (341), (432)\}$;
4) $Cl_4=\{(124), (213), (342), (431)\}$; pri tom se služimo predočivanjem permutacije pomoću ciklusâ (isp. 3 § 8.8.6).

Dakle je $r=4$. Vidi se da je $G_T\cong A_4$.

No, derivat G'_T grupe G_T ima 4 člana, pa je indeks derivata $s=\frac{12}{4}=3$; prema 3.9.7 dopušta zato G_T 3 jednodimenzionalna nesvodljiva predstavljanja, tj. $d_1=d_2=d_3=1$. Zato Burnside-ova jednadžba $\sum_{i=1}^{4} d_i^2=12$ daje $d_4=3$.

Na osnovu toga može se napisati:

5.1.2. *Tablica primitivnih karaktera grupe G_T tetraedra:*

	Cl_1	Cl_2	Cl_3	Cl_4
	1	$3\rho_2$	$4\rho_3$	$4\rho_3^2$
Γ_1	1	1	1	1
Γ_2	1	1	ε	ε^{-1}
Γ_3	1	1	ε^{-1}	ε
Γ_4	3	-1	0	0

Pri tom je ρ_k rotacija za $2\pi/k$ rad, $\varepsilon=e^{2\pi i/3}=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}=-\frac{1}{2}+\frac{i}{2}\sqrt{3}$.

5.1.3. Reprezentaciju Γ_4 duljine 3 daju same rotacije prostora predočene kao linearne transformacije; zato te transformacije čine nesvodljivu reprezentaciju.

5.2. Grupa G_K kocke odnosno grupa G_O oktaedra.

5.2.1. O grupi G_K bilo je govora u poglavlju 17, §§ 7.11, 12.8.15, 15.4.4. Posebno je $n=24$, $G_K\cong S_4$ (17 § 12.8.5), $r=5$; razredi su:

$$Cl_1=\{e\},\ Cl_2=R_2,\ Cl_3=R_3,\ Cl_4=R_4,\ Cl_5=R_4^2,$$

pri čemu se R_k^i sastoji od svih članova grupe kojima je red jednak $\frac{k}{i}$. Grupa G_K ima dva generatora a, b za koje vrijede relacije:

$$a^4=b^3=e,\ ab^2a=b,\ aba=ba^2b$$

(npr. a može označivati rotaciju za $\pi/2$ rad oko glavne osi kocke, b može značiti rotaciju za $2\pi/3$ rad oko dijagonale kocke). Nadalje je

$$G'_K\cong G_T,\ \text{tj.}\ s=\frac{k\,G_K}{k\,G'_K}=2.$$

Zato prema § 3.9.7 grupa G_K ima dvije jednodimenzionalne nesvodljive unitarne reprezentacije Γ_1, Γ_2, tj. $d_1=d_2=1$. Zato se Burnside-ova jednadžba svodi na

$$1^2+1^2+d_3^2+d_4^2+d_5^2=24,$$

odnosno

$$d_3^2+d_4^2+d_5^2=22.$$

Brojevi d_3, d_4, d_5 su ≤ 4, no nijedan od njih ne može biti $=4$ jer bi npr. $d_3=4$ imalo za posljedicu $d_4^2+d_5^2=6$, a ova jednadžba nad N nema rješenja. Dakle je $\{d_3, d_4, d_5\} \subset \{1, 2, 3\}$, a lako se vidi da je $d_3=2$, $d_4=d_5=3$.

5.2.2. *Tablica primitivnih karaktera grupe* G_K [*odnosno grupe* S_5 (isp. 5.5.6.1]:

	Cl_1	Cl_2	Cl_3	Cl_4	Cl_5
	e	$8\rho_3$	$3\rho_4^2$	$6\rho_2$	$6\rho_4$
Γ_1	1	1	1	1	1
Γ_2	1	1	1	-1	-1
Γ_3	2	-1	2	0	0
Γ_4	3	0	-1	1	-1
Γ_5	2	0	-1	-1	1

5.2.3. Reprezentacija Γ_5 je obična linearna transformacija (rotacija) iz analitičke geometrije.

5.2.4. Vrijedi $\Gamma_4=\Gamma_5\Gamma_i$ $(i=2, 3)$.

5.2.5. *Grupa* G_0 *oktaedra je izomorfna, odnosno jednaka sa grupom kocke* jer su kocka i oktaedar polarni međusobno; posebno, središta strana kocke (oktaedra) vrhovi su određenog oktaedra (kocke).

5.2.6. *Grupa* G_K *je izomorfna sa grupom* $G_{T'}$ *rotacija i simetrija pravilna tetraedra.*

5.2.7. Prema tome, tablica u 5.2.2. prikazuje primitivne karaktere i grupe G_K i grupe G_O i grupe $G_{T'}$.

5.3. Grupa G_I ikozaedra. Grupa G_D dodekaedra.

5.3.1. Grupa G_I ikozaedra (isp. 17 § 7.12). Ta se grupa sastoji od ovih rotacija:

1) Po 4 rotacije (za $\alpha={}^{2\pi}/_5$ rad, 2α, 3α, 4α) oko svake osi kroz vrh ikozaedra; to daje $6.4=24$ rotacije;
2) Po jedna rotacija za π rad oko osi koja spaja središta dvaju bridova; to daje $15.1=15$ članova grupe G_I;
3) Po 2 rotacije (za $2\pi/3$ rad, $4\pi/3$ rad) oko svake osi koja spaja težišta dviju paralelnih stranica ikozaedra; to daje $10.2=20$ članova grupe;
4) Mirovanje e.

Svega G_I ima $24+15+20+1=60$ članova, dakle $n=60$.

5.3.2. Razredi grupe G_I jesu: $Cl_1=\{e\}$, $Cl_2=15$ rotacija za π oko svake od 15 osi simetrije ikozaedra; os simetrije spaja središta dvaju paralelnih bridova ikozaedra; $Cl_3=20$ rotacija poretka 3 (rotacije za $2\pi/3$ ili $4\pi/3$) spomenute pod 3); $Cl_4=12$ rotacija za kut $\pm 4\pi/5$; Cl_5 sastoji se od 12 rotacija za kut $\pm 4\pi/5$ rad.

5.3.3. *Grupa* G_I *nema prave invarijantne podgrupe* X jer bi X moralo biti unija od nekih razreda Cl_1—Cl_5 a s druge strane broj d članova od X morao bi dijeliti 60; a jednostavno provjeravanje pokazuje da takvo X ne postoji.

5.3.3.1. Zato G_1 nema, osim trivijalne, nijedne reprezentacije duljine 1.

5.3.4. Ikozaedar i 5 upisanih oktaedara. Ikozaedar ima $v_0 = 12$ vrhova, $v_1 = 30$ bridova i $v_2 = 20$ stranica te 15 osi simetrije; svaka os simetrije ikozaedra spaja središta dvaju paralelnih bridova. Svaka os simetrije je okomita na po dvije osi simetrije. Na taj način osi simetrije raspoređuju se u pet skupina po tri osi koje su međusobno okomite. Svaka takva trojka osi simetrije ikozaedra određuje oktaedar kojemu su vrhovi upravo krajevi osi, odnosno središta bridova ikozaedra u kojima osi simetrije pogađaju bridove. Na taj način *dobivamo 5 oktaedara upisanih zadanom ikozaedru*. Pri svakoj rotaciji $\rho \in G_I$ skup tih oktaedara O_1, O_2, O_3, O_4, O_5 međusobno se permutiraju, a svi članovi grupe G_I koji određeni oktaedar O_i prevode u sama sebe, dakle opet u O_i, čine podgrupu od 12 članova koja je izomorfna sa grupom G_T tetraedra, odnosno sa A_4.

5.3.5. *Grupa G_I je izomorfna sa A_5*, tj. sa grupom parnih permutacija skupa S od 5 elemenata (u sadašnjem slučaju možemo kao S birati upravo rečenih 5 oktaedara).

Zato se grupa G_I može ostvariti i pomoću svih parnih permutacija od 5 nezavisnih varijablâ x_1, x_2, x_3, x_4, x_5. Karakter te reprezentacije Γ duljine 5 je lako odrediti: $\operatorname{Tr}\Gamma(e) = 5$, $\operatorname{Tr}\Gamma(12)(34) = 1$, jer permutaciji (12) (34) (5)

odgovara matrica $\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ kojoj je trag $= 1$.

Isto tako se vidi da je $(123) \in Cl_3$ i da permutaciji (123) (4) (5) odgovara

matrica $\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ kojoj je trag $= 2$; dakle je $\chi x = 2$ za svako $x \in Cl_3$.

Isto se vidi da iz $x \in Cl_4 \cup Cl_5$ izlazi $\chi x = 0$. Prema tome je karakter od Γ određen. Da li je reprezentacija Γ ireducibilna?

U tu svrhu je nužno i dovoljno da bude

$$(1) \qquad \sum_{\rho=1}^{r} r_\rho \chi Cl_\rho \overline{\chi Cl_\rho} = k G \qquad \text{(isp. § 3.9.1).}$$

Kod nas je lijeva strana

$$(1)_1 = 1 \cdot 5 \cdot 5 + 15 \cdot 1 \cdot 1 + 20 \cdot 2 \cdot 2 + 12 \cdot 0 + 12 \cdot 0 > 60$$

Dakle prema § 3.9.1 reprezentacija Γ nije ireducibilna. Međutim, uklonimo li Γ_1 pa promatramo razliku karakterâ od Γ i Γ_1 izlaze vrijednosti:

$$4 \text{ u } Cl_1, \ 0 \text{ u } Cl_2, \ 1 \text{ u } Cl_3, \ -1 \text{ u } Cl_4, \ -1 \text{ u } Cl_5;$$

pripadni skalarni kvadrat je

$$(1)_1 \equiv 16 + 0 + 20 + (-1)^2 \cdot 12 + (-1)^2 \cdot 12 \text{ tj. } 60;$$

dobije se karakter ireducibilne reprezentacije (označimo je sa Γ_4):

$$\Gamma_4 : 4 \quad 0 \quad 1 \quad -1 \quad -1.$$

5.3.6. Potpuna tablica primitivnih karaktera grupe G_I glasi:

	Cl_1	Cl_2	Cl_3	Cl_4	Cl_5
	e	$15\,\rho_3$	$20\,\rho_5$	$12\,\rho_5$	$12\,\rho_5{}^2$
Γ_1	1	1	1	1	1
Γ_2	3	-1	0	$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1-\sqrt{5})$
Γ_3	3	-1	0	$\frac{1}{2}(1-\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$
Γ_4	4	0	1	-1	-1
Γ_5	5	1	-1	0	0

5.3.7. Grupa G_D dodekaedra. Kako je dodekaedar polaran sa ikozaedrom, grupa G_D je izomorfna sa G_I, odnosno sa A_5. Skupu od 5 upisanih oktaedara odgovara sada skup od 5 kocaka upisanih u dodekaedar i kojima su vrhovi u vrhovima dodekaedra.

Kao i u slučaju grupe G_I grupa G_D dopušta realnu i vjernu reprezentaciju.

5.4. Reprezentacija dijedarske grupe D_n.

5.4.1. Slučaj grupe D_2 razmatran je u § 4.3.1.

5.4.2. Pri $n>1$ dijedarska grupa D_n je grupa što pripada pravilnoj n-stranoj uspravnoj prizmi, odnosno pravilnom poligonu od n stranica (isp. 17 § 7.7). Grupa D_n sastoji se od n rotacijâ za $n' \cdot \frac{2\pi}{n}$ rad ($n'=0, 1, 2, \ldots, n-1$) oko *glavne* osi prizme i od n rotacijâ za π rad oko svake od n sporednih osi prizme.

Dakle je $k\, D_n = 2\,n$.

5.4.3. Razredi konjugiranosti grupe D_n.

Označimo sa b rotaciju za $2\pi/n$ rad oko *glavne* osi; tada rotacije $b, b^2, \ldots, b^n\,(=1)$ čine cikličku podgrupu C_n od D_n. Neka su $u_1, u_2, \ldots, u_n$ *sporedne* osi pravilne prizme, neka je a_ν rotacija prostora za π rad oko osi u_ν; dakle je $a_\nu{}^2=1$. Nadalje je

$$b a_\nu b = a_\nu, \quad a_\nu^{-1} b a_\nu = b^{-1}, \quad a_\nu^{-1} b^2 a_\nu = b^{-2}, \quad \cdots$$

kao što se neposredno vidi.

To znači da su rotacije b, b^{-1} spregnute, isto kao b^2, b^{-2} pa b^3, b^{-3}, itd. Elementi b^k, $b^{\pm l}$ ($|k|=|l|$) nisu konjugirani jer nemaju isti red. Kako je C_n normalna podgrupa grupe $D_{n'}$ nije b^k konjugirano ni sa jednim $x \in D_n \setminus C_{n'}$ pa imamo ove razrede konjugiranosti grupe D_n:

(1) $\{e\}, \{b, b^{-1}\}, \{b^2, b^{-2}\}, \ldots, \{b^m, b^{-m}\}$ pri $n=2m+1$

(2) $\{e\}, \{b, b^{-1}\}, \{b^2, b^{-2}\}, \ldots, \{b^m\}$ pri $n=2m$.

Prema tome u (1), odnosno (2) imamo $E\,\frac{n}{2}+1$ razreda konjugiranosti od D_n.

Još dolaze razredi rotacijâ a_ν. Kako rotacija b prevodi os u_1 u os u_3, a u_3 u $u_5, \ldots,$ te u_2 u u_4, te u_4 u $u_6, \ldots$ to se rotacije $a_1, a_3, \ldots$ konjugirane isto kao i $a_2, a_4, a_6, \ldots$. Ako je n parno, tada a_1 nije konjugirano sa a_2 pa uz (2) dobivamo još dva razreda po $\frac{n}{2}=m$ članova; dakle svih razreda ima $1+\frac{n}{2}+2$, tj. $r=\frac{n}{2}+3$.

Ako je n neparno, tada b prevodi u_n u u_1 pa su sve rotacije a_ν međusobno spregnute preko b i čine n-član razred; to prema (1) znači da je

$$r=1+m+1=1+\frac{n-1}{2}+1+\frac{n+3}{2}.$$

Tako smo dokazali

5.4.3.1. Teorem. *Broj razreda konjugiranosti grupe* D_n *je* $r=\frac{1}{2}(n+1)$ *pri neparnom n, odnosno* $r=\frac{1}{2}n+3$ *pri parnom n.*

Također se neposredno provjeri da vrijedi

5.4.4. Teorem. *Derivat* D_n' *grupe* D_n *ima n članova pri neparnom n, odnosno ima* $\frac{n}{2}$ *članova pri parnom n.*

Naime, derivat D'_n se sastoji od rotacijâ $b^{2\pi}(\nu=0, 1, 2, \ldots, n-1)$ kojih ima $\frac{n}{2}$ različnih ili n različnih, već prema tome da li je n parno ili neparno.

5.4.5. Teorem. *Jednodimenzionalnih nesvodljivih unitarnih reprezentacija grupe* D_n *ima* $\begin{cases} 2 \text{ pri neparnom } n \\ 4 \text{ pri parnom } n. \end{cases}$

To izlazi iz 3.9.7 i 5.4.4.

U drugu ruku, ciklična podgrupa $C_n=\{b^\nu;\ \nu=1, 2, \ldots, n\}$ je očigledno maksimalna invarijantna podgrupa od D_n indeksa $s=2$; zato prema 3.9.3 duljina svake ireducibilne unitarne reprezentacije od D_n je 1 ili 2.

Na osnovu toga rezultata i činjenicâ 5.4.3.1, 5.4.5 imamo

5.4.6. Teorem. *Ako je n parno [neparno], tada* D_n *ima dvije [4] jednodimenzionalne nesvodljive reprezentacije; preostale nesvodljive reprezentacije su duljine 2 i ima ih* $\frac{n}{2}-1$ $\left[\text{odnosno } \frac{n-1}{2}\right]$.

5.4.7. Tablica primitivnih karaktera grupe D_n pri $n=2m+1$, $\varphi=2\pi/n$:

	$\{1\}$	$\{b, b^{-1}\}$	$\{b^2, b^{-2}\}$	$\cdots$	$\{b^m, b^{-m}\}$	$\{a_1, \ldots, a_n\}$
	1	2	2	$\cdots$	2	n
Γ_1	1	1	1	$\cdots$	1	1
Γ_2	1	1	1	$\cdots$	1	-1
Γ_3	2	$2\cos\varphi$	$2\cos 2\varphi$	$\cdots$	$2\cos m\varphi$	0
Γ_4	2	$2\cos 2\varphi$	$2\cos 4\varphi$	$\cdots$	$2\cos 2m\varphi$	0
.	.	.	.	$\cdots$	.	.
Γ_{m+2}	2	$2\cos n\varphi$	$2\cos 2n\varphi$	$\cdots$	$2\cos m^2\varphi$	0

5.4.8. Tablica primitivnih karaktera grupe D_n pri $n=2m$, $\varphi=2\pi/n$:

	$\{1\}$	$\{b, b^{-1}\}$	$\{b^2, b^{-2}\}$	$\cdots$	$\{b^{m-1}, b^{-(m-1)}\}$	$\{b^m\}$	Cl_{m+2}	Cl_{m+3}
	1	2	2	$\cdots$	2	1	m	m
Γ_1	1	1	1	$\cdots$	1	1	1	1
Γ_2	1	1	1	$\cdots$	1	1	-1	-1
Γ_3	1	-1	1	$\cdots$	$(-1)^{m-1}$	$(-1)^m$	1	-1
Γ_4	1	-1	1	$\cdots$	$(-1)^{m-1}$	$(-1)^m$	-1	1
Γ_5	2	$2\cos\varphi$	$2\cos 2\varphi$	$\cdots$	$2\cos(m-1)\varphi$	$2\cos m\varphi$	0	0
Γ_6	2	$2\cos 2\varphi$	$2\cos 4\varphi$	$\cdots$	$2\cos 2(m-1)\varphi$	$2\cos m\varphi$	0	0
.	.	.	.	$\cdots$	.	.	.	.
Γ_{m+3}	2	$2\cos(m-1)\varphi$	$2\cos 2(m-1)\varphi$	$\cdots$	$2\cos(m-1)^2\varphi$	$2\cos(m-1)m\varphi$	0	0

Pri tom je $Cl_{m+2}=\{ab^{2\nu};\ \nu=0, 1, 2, \ldots\}$, $Cl_{m+2}=\{ab^{2\nu+1};\ \nu=0, 1, 2, \ldots\}$.

5.4.9. Ireducibilne reprezentacije $\Gamma_1, \Gamma_2, \ldots$ grupe D_n. Γ_1 je konstanta 1. Reprezentacija Γ_2 određena je sa $\Gamma_2(a)=-1$, $\Gamma_2(b)=1$.

Neka je $\varepsilon_n=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$; tad možemo staviti

$$\Gamma_{2+\mu}a=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, \quad \Gamma_{2+\mu}b=\begin{bmatrix}\varepsilon_n{}^{\mu} & 0\\ 0 & \varepsilon_n{}^{-\mu}\end{bmatrix}, \quad (\mu=1, 2, \ldots, m).$$

U slučaju $n=2m+1$ reprezentacije $\Gamma_{2+\mu}$ su nesvodljive.

U slučaju $n=2m$ stavljamo $\Gamma_3 a=1$, $\Gamma_3 b=-1$

$$\Gamma_4 a=-1, \quad \Gamma_4 b=-1$$

$$\Gamma_{4+\mu}(a)=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, \quad \Gamma_{4+\mu}b=\begin{bmatrix}\varepsilon_n{}^{\mu} & 0\\ 0 & \varepsilon_n{}^{-\mu}\end{bmatrix} \quad (\mu=1, 2, \ldots, n-1).$$

Matrice $\Gamma_\alpha x$ za $x\in D_n\setminus\{a, b\}$ određuje se pomoću $\Gamma_\alpha a$, $\Gamma_\alpha b$, jer a, b generiraju D_n pa time $\Gamma_\alpha a$, $\Gamma_\alpha b$ generiraju $\Gamma_\alpha x$ za svako $x\in D_n$.

5.5. Predstavljanje simetrične grupe S_n.

5.5.1. Grupa S_n definirana je (kao i A_n) u 17 § 7.4. Neposredno se dokazuje da je *derivat od* S_n *upravo podgrupa* A_n svih parnih permutacija. Kako je $k\,A_n=\frac{1}{2}k\,S_n$ (v. 3 § 8.7.2), *ima* S_n *upravo dvije reprezentacije duljine* 1 (v. § 3.9.7) i to: reprezentaciju

$$\Gamma_1\,|\,S_n=\text{konstanta } 1$$

i reprezentaciju Γ_2 koja je $=1$ na A_n, a jednaka -1 na $S_n\setminus A_n$; dakle je $p\in S_n\to\Gamma_2 p=\operatorname{sgn} p=(-1)^{ip}$ (*ip* je broj inverzija permutacije *p*; v.3 § 8.5).

5.5.2. Particija prirodnog broja *n*. *Particija* ili *razbijanje* od *n* je svaki skup prirodnih brojeva s ponavljanjem kojima je suma $=n$; ili ekvivalentno: particija od *n* je svaki silazni niz prirodnih brojeva kojima je suma $=n$.

Particija $n=\sum_{\nu=1}^{n}\nu\alpha_\nu$, pri čemu je $\alpha_\nu\in\{0,\ 1,\ 2,\dots,\ n\}$ označuje se sa $[1^{\alpha_1}2^{\alpha_2}\dots n^{\alpha_n}]$.

5.5.2.1. *Broj različnih particija od n označuje se sa* $r(n)$. Npr. $r(4)=5$ jer je $4=4$, $4=3+1$, $4=2+2$, $4=2+1+1$, $4=1+1+1+1$. Kad $n\to\infty$, tada je $r(n)\sim\frac{1}{4n\sqrt{3}}e^{\pi\sqrt{2n/3}}$ (Hardy — Ramanujan).

Imamo ovu tablicu

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$r(n)$	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176	231	297	395	490	627

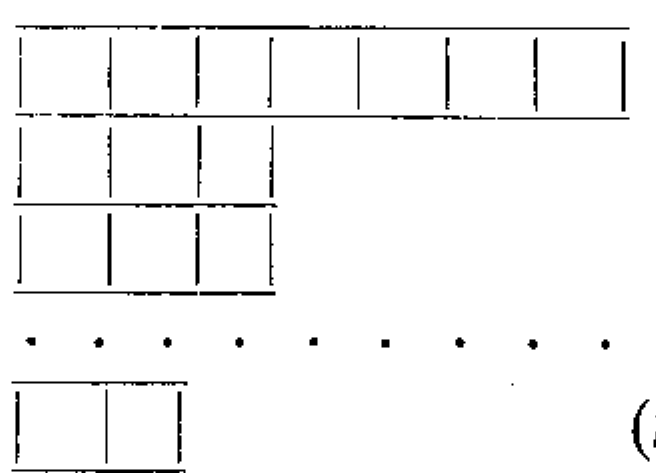
30	50	70	100
5 604	204 266	4 087 968	190 569 292

.

5.5.2.2. Particije i Youngove tablice. Svakoj particiji ili raspodjeli

$$n=x_1+x_2+\dots+x_m \text{ pri } x_1\ge x_2\ge\dots\ge x_m\ge 1$$

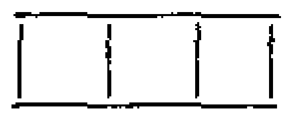
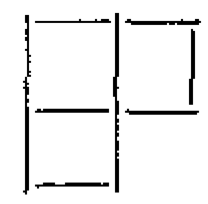
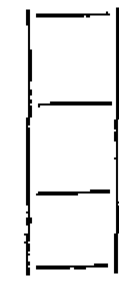
broja *n odgovarajuća Youngova tablica* ili *shema* izgleda ovako:



(prvi niz od x_1 pretinaca, na broju x_1)
(drugi niz „ „ „ x_2)

(*m*-ti niz pretinaca; ima ih x_m).

Prema tome, tu imamo *n* pretinaca (poljâ) raspoređenih u blokove; te pretince numeriramo sa 1, 2, ..., *n* (npr. po stupcima odozgo prema dolje i od lijeve strane prema desno, ili po recima onako kako pišemo, ili bilo kako drukčije).

Npr. broju 3 odgovaraju ove particije s odgovarajućom Youngovom shemom: $3=3$ . $3=2+1$ , $3=1+1+1$ .

Jasno je da i obrnuto iz svakog rasporeda od n pločica ili pretinaca nanizanih tako da svaki naredni redak ima manje članova ili najviše jednako mnogo članova, daju određenu particiju kojoj je ta shema pridružena.

5.5.2.3. Teorem (0). *Svakoj raspodjeli $n=x_1+x_2+\ldots+x_m$ pri čemu je $x_1\geq x_2\ldots\geq x_m$ te $\{x_1, x_2, \ldots x_m\}\subset N$ odgovara razred međusobno spregnutih permutacija iz S_n; taj se razred označuje sa $[x_1\, x_2\ldots x_m]$ a sastoji se iz svih $p\in S_n$ kojima faktorizacija u cikluse glasi*

(1) $\qquad p= z_1 z_2\ldots z_m$; *pri tom z_μ za svako $\mu\in\{1, 2, \ldots, m\}$ znači ciklus od x_μ članova* (isp. 3 § 8.8.6); *vrijedi* $\{1, 2, \ldots, n\}=$ $=z_1\cup z_2\cup\ldots\cup z_m$.

(00). *Razred konjugiranosti koji odgovara particiji*

$$n=\sum_{\nu=1}^{n}\nu\alpha_\nu \text{ ima} \tag{2}$$

$$\frac{n!}{\alpha_1!\,\alpha_2!\ldots\alpha_n!\,2^{\alpha_2}\cdot 3^{\alpha_3}\ldots n^{\alpha_n}} \text{ članova.} \tag{3}$$

Dokaz. Ako proizvoljno $q\in S_n$ rastavimo u disjunktne cikluse $c_1, c_2\ldots c_\gamma$ tako da unija (zbir) tih ciklusa bude $\{1, 2, \ldots, n\}$, tada *duljine tih ciklusa daju određenu particiju broja n.* Ako analogno pri $q'\in S_n$ imamo rastav

$$q'=c_1'\,c_2'\ldots c'_{\gamma'}, \tag{4}$$

možemo zahtijevati da bude

$$kc_1\geq kc_2\geq\ldots\geq kc_\gamma\geq 1 \tag{5}$$

$$kc'_1\geq kc'_2\geq\ldots\geq kc'_{\gamma'}\geq 1. \tag{5'}$$

Ako je

$$\gamma=\gamma',\ kc_i=kc'_i \text{ za } i=1, 2, \ldots, \gamma, \tag{6}$$

tada su permutacije q, q' spregnute i vrijedi

(7) $\qquad q'=sqs^{-1}$, pri čemu s označuje onu permutaciju $s\in S_n$ za koju je $sc_i=c'_i$ u smislu da iz $c_i=(c_{i_1}c_{i_2}\ldots c_{i_{l_i}})$ izlazi da je $c'_i=(sc_{i_1}sc_{i_2}\ldots sc_{i_{l_i}})$ pri $i=1, 2, \ldots, \gamma$. I obrnuto, ako vrijedi (7), (5), (5'), tada vrijedi (6); to se neposredno provjeri. To se posebno provjerava pregledno radeći s Youngovim shemama pri čemu ciklusu c_i za kc_i članova od q pridružujemo i-ti redak od kc_i pločica Youngove sheme.

Dokažimo obrazac (00). Slučaj da je $\alpha_\nu=0$ za $\nu=1,2,\ldots,n-1$ te $\alpha_n=1$ (particija $n=n$) je dokazan u 3 § 8.8.4 jer se tada broj (3) svodi na broj bitno različitih cikličnih permutacija skupa od n predmeta.

(i) Obradimo slučaj da je $n=e_1+e_2+\ldots+e_m$, $e_1>e_2>\ldots>e_m\geq 1$. Tada prvi Youngov redak možemo ispuniti sa e_1 brojeva iz $\{1,2,\ldots,n\}$ na $\binom{n}{e_1}$ načina, od kojih svako popunjenje daje po $(e_1-1)!$ bitno različnih cikličkih permutacija (isp. 3 § 8.8.4); od preostalih $n-e_1$ brojeva možemo popuniti drugi Youngov redak na $\binom{n-e_1}{e_2}$ načina; taj redak daje $\binom{n-e_1}{e_2}(e_2-1)!$ bitno različnih ciklusa duljine e_2, itd. Prema tome, svih permutacija kojima faktori ciklusi imaju po redu $e_1>e_2>\ldots>e_m$ članova ima

$$\binom{n}{e_1}(e_2-1)!\binom{n-e_1}{e_2}(e_2-1)!\cdots\binom{n-e_1-e_2\ldots-e_{m-2}}{e_{m-1}}e_{m-1}-1)!$$
$$\binom{n-e_1-\ldots-e_{m-1}}{e_m}e_m-1)!$$

A taj produkt je, kao što se vidi, jednak $\dfrac{n!}{e_1e_2\ldots e_m}$; a to znači da se dobije izraz (3) jer su eksponenti $\alpha_\mu\in\{0,1\}$ i to $\alpha_\mu=1$ onda i samo onda ako je $\mu\in\{e_1,e_2,\ldots,e_m\}$.

(ii) Obradimo slučaj da je

$$n=e_1+e_1+\ldots+e_1=ae_1. \tag{8}$$

Tada se Youngova shema sastoji od a redova pločica, po e_1 pločica u svakom retku. Promatrajući sva bitno različna ciklična uređenja u svakom retku i imajući u vidu da su jednakobrojni redići ravnopravni — čime se broj bitno različnih permutacija umanjuje $a!$ puta, zaključujemo da broj različnih permutacija koje proizvedu particiju (8) ima

$$\frac{1}{a!}\binom{n}{e_1}(e_1-1)!\binom{n-e_1}{e_1}(e_1-1)!\ldots\binom{n-(a-2)e_1}{e_1}(e_1-1)!\ (e_1-1)!$$

Lako se izračuna da je taj produkt $=\dfrac{n!}{a!\,e_1{}^a}$.

Na osnovu slučajeva (i), (ii) dokazuje se lako i opći obrazac (3), naime, jednakobrojni redići Youngove sheme mogu se međusobno permutirati, a ciklusi iz nejednakobrojnih redića mogu se međusobno kombinirati svaki za svakim.

5.5.3. Formiranje nesvodljivih prikazivanja grupe S_n.

Pođimo od neke raspodjele broja n i pripadne Youngove sheme Y; tada je naravno S_n izomorfno sa grupom svih permutacija klijetaka od Y. Neka je $P(Y)$, odnosno $Q(Y)$ skup svih permutacija iz S_n koje svaki redak [stupac] od Y prevode u sama sebe.

Definirajmo, u zavisnosti od Y, preslikavanje

$$x\in S_n\to\varphi x=\begin{cases}0 & \text{ako je } x\notin Q(Y)P(Y)\\ \operatorname{sgn} q & \text{ako je } x=qp \text{ pri nekom } q\in Q(Y) \text{ i nekom } p\in P(Y).\end{cases} \tag{1}$$

Prema tome, φ je preslikavanje od S_n u $\{-1, 0, 1\}$; time su određene funkcije

$$t \in S_n \to \varphi_t, \text{ gdje je} \tag{2}$$

$$\varphi_t(x) \equiv \varphi(xt) \quad (x \in S_n)$$

kao i prostor V, nad tijelom kompleksnih brojeva, svih funkcijâ (2).

Sagradimo predstavljanje grupe S_n ovako:

$$g \in S_n \to \Gamma(g) \text{ pri čemu je} \tag{3}$$

$$\Gamma(g)\,\varphi_t(x) = \varphi_t(xg) = \varphi(xgt) = \varphi_{gt}(x), \text{ tj.}$$

$$\Gamma(g)\,\varphi_t = \varphi_{gt} \qquad (g, t \in S_n). \tag{4}$$

Obrazac (4) pokazuje da $\Gamma(g)$ pridružuje članu $\varphi_t \in V$ određen član $\varphi_{gt} \in V$; nadalje je

$$\Gamma(g_1 g)\,\varphi_t(x) = \varphi_t(xg_1 g) = \varphi(xg_1 gt) =$$

$$= \varphi_{gt}(xg_1) = \Gamma(g_1)\,\varphi_{gt}(x) = \Gamma(g_1)\,\Gamma(g)\,\varphi_t(x)), \text{ tj.}$$

$$\Gamma(g_1 g)\,\varphi_t(x) = \Gamma(g_1)\,\Gamma(g)\,\varphi_t(x) \quad (t, x \in S_n), \text{ specijalno}$$

$$\Gamma(g_1 g)\,\varphi_t = \Gamma(g_1)\,\Gamma(g)\,\varphi_t \quad (t \in S_n), \text{ što znači da je}$$

$$\Gamma(g_1 g) = \Gamma(g_1)\,\Gamma(g). \tag{5}$$

Dakle je (3) određena *reprezentacija* grupe S_n nad prostorom V.

Može se dokazati da je ta reprezentacija nesvodljiva i da je neekvivalentna sa svakom reprezentacijom grupe S_n koja se dobije na opisan način polazeći od neke *različne raspodjele* broja n.

Ako pođemo od raspodjele

$$n = e_1 + e_2 + \ldots + e_m, \; e_1 \geq e_2 \geq \ldots \geq e_m \geq 1 \tag{6}$$

broja n, tada se može dokazati da je duljina d opisane reprezentacije jednaka

$$d = \frac{n!\,\Delta(l_1, l_2, \ldots, l_m)}{l_1!\, l_2! \ldots l_m!}, \text{ pri čemu je} \tag{6'}$$

$$l_\mu = e_\mu + m - \mu \;\; (\mu = 1, 2, \ldots, m) \quad \text{te}$$

$$\Delta(l_1, l_2, \ldots, l_m) = 1 \text{ ili } \prod_{i<j=1}^{m} (l_i - l_j) \text{ već prema tome da li je}$$

$m = 1$ ili $m > 1$.

5.5.4. *Primjer grupe* S_3 *i raspodjele* $3 = 2 + 1$ *odnosno sheme* $\begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \\ \cline{1-1}\end{array}$ (v. G. Ja. Ljubarskij, str. 78). Tu je $P = \{e, (13) = 321\}$, $Q = \{e, (12)\}$, $e = 123$.

Dakle je $QP=\{e,\ (13),\ (12),\ 312\}$. Funkcija (1), tj. φ_{123} kao i ostale funkcije (2) daju ovu tablicu:

x	e	132	213	231	312	321
$\varphi_x=\varphi_{123}\,x$	1	0	-1	0	-1	1
$\varphi_{132}(x)$	0	1	0	-1	1	-1
$\varphi_{213}(x)$	-1	-1	1	1	0	0
$\varphi_{231}(x)$	0	1	0	-1	1	-1
$\varphi_{312}(x)$	-1	-1	1	1	0	0
$\varphi_{321}(x)$	1	0	-1	0	-1	1

Od tih 6 funkcijâ $\varphi,\ \varphi_{132},\ \varphi_{213},\ \varphi_{231},\ \varphi_{312},\ \varphi_{321}$ funkcije $\varphi,\ \varphi_{213}$ su linearno nezavisne, a ostale se izrazuju pomoću njih jer je

(7) $$\varphi_{132}\equiv-\varphi-\varphi_{213}=\varphi_{231},\quad \varphi_{312}=\varphi_{213},\quad \varphi_{321}=\varphi.$$

Zato je za dano $g\in S_3$ operator $\Gamma(g):V\to V$ određen svojim vrijednostima $\Gamma(g)\varphi_{123},\ \Gamma(g)\varphi_{213}$. No, prema (4) je

$$\Gamma(g)\,\varphi_{123}=\varphi_{g\,123}=\varphi_g$$

$\Gamma(g)\,\varphi_{213}=\varphi_{g\,213}$. Npr. $g=312$ daje

$$\Gamma(312)\,\varphi_{123}=\varphi_{312}=(\text{prema }(7))=\varphi_{213}=0\cdot\varphi_{122}+1\cdot\varphi_{213}$$

$$\Gamma(312)\,\varphi_{213}=\varphi_{312\cdot 213}=\varphi_{132}=(\text{prema }(7))=-\varphi-\varphi_{213}.$$

Zato se operator $\Gamma(312)$ pri bazi $\varphi_{123},\ \varphi_{213}$ zapisuje matricom

$$\Gamma(312)=\begin{bmatrix}0 & -1\\ 1 & -1\end{bmatrix}.$$

Na sličan se način dobije:

$$\Gamma(123)=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad \Gamma(132)=\begin{bmatrix}-1 & 0\\ -1 & 1\end{bmatrix}.\quad \Gamma(213)=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},$$

$$\Gamma(231)=\begin{bmatrix}-1 & 1\\ -1 & 0\end{bmatrix},\quad \Gamma(321)=\begin{bmatrix}1 & -1\\ 0 & -1\end{bmatrix}.$$

Tako dobivenih 6 matricâ $g\in S_3\to\Gamma(g)$ predočuju *vjerno* grupu S_3; karakter χ toga predočenja je

$$2,\quad 0,\quad 0,\quad -1,\quad -1,\quad 0.$$

Skalarni kvadrat toga karaktera je $2\cdot 2+(-1)(-1)+(-1)(-1)=6=kS_3$, pa je zaista predočenje nesvodivo (isp. § 3.9.1).

5.5.5. Može se dokazati da pri $n>4$ svaka nesvodljiva reprezentacija grupe S_n duljine >1 nužno je vjerna reprezentacija.

5.5.6. Tablica primitivnih karaktera simetričnih grupa S_4, S_5, S_6.

5.5.6.1. *Grupa* S_4 (isp. § 5.2.2)

Youngova shema	1^4	$1^2, 2$	$1, 3$	2^2	4	Razredi ili klase
	1	6	8	3	6	Broj članova razreda
4	1	1	1	1	1	
1^4	1	-1	1	1	-1	
$1, 3$	3	1	0	-1	-1	
2^2	2	-1	1	2	0	
$1^2, 2$	3	1	-1	1	-1	

5.5.6.2. *Grupa* S_5

Razredi ili klase s brojem članova u razredu:

Shema	1^5	$1^3, 2$	$1^2, 3$	$1, 2^2$	$1, 4$	$2, 3$	5
	1	10	20	15	30	20	24
5	1	1	1	1	1	1	1
1^5	1	-1	1	1	-1	-1	1
$4, 1$	4	2	1	0	0	-1	-1
$3^2, 5$	5	1	-1	1	-1	1	0
$3, 1^2$	6	0	0	-2	0	0	1
$1, 2^2$	5	-1	-1	1	1	1	-1
$2^3, 1$	4	-2	1	0	0	1	-1

5.5.6.3. *Karakteri grupe* S_6

Razredi s brojem članova

Shema	1^6	$1^4,2$	$1^3,3$	$1^2,2^2$	$1^2,4$	$1,2,3$	$1,5$	2^3	$2,4$	3^2	6
	1	15	40	45	90	120	144	15	90	40	120
6	1	1	1	1	1	1	1	1	1	1	1
1^6	1	−1	1	1	−1	−1	1	−1	1	1	−1
5 1	5	3	2	1	1	0	0	−1	−1	−1	−1
$2, 1^4$	5	−3	2	1	−1	0	0	1	−1	−1	1
4, 2	9	3	0	1	−1	0	−1	3	1	0	0
$2^2, 1^2$	9	−3	0	1	1	0	−1	−3	1	0	0
$4, 1^2$	10	2	1	−2	0	−1	0	−2	0	1	1
$3, 1^3$	10	−2	1	−2	0	1	0	2	0	1	−1
3^2	5	1	−1	1	−1	1	0	−3	−1	2	0
2^3	5	−1	−1	1	1	1	0	3	−1	2	0
3,2,1	16	0	−2	0	0	0	1	0	0	−2	0

5.5.6.4. *Karakteri grupe* S_7

Razredi s brojem članova

Shema	1^7	$1^5,2$	$1^4,3$	$1^3,2^2$	$1^3,4$	$1^2,2,3$	$1^2,5$	$1,2^3$	$1,2,4$	$1,3^2$	$1,6$	$2^2,3$	$2,5$	$3,4$	7
	1	21	70	105	210	420	504	105	630	280	840	210	504	420	720
7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1^7	1	−1	1	1	−1	−1	1	−1	1	1	−1	1	−1	−1	1
6, 1	6	4	3	2	2	1	1	0	0	0	0	−1	−1	−1	1
$2, 1^5$	6	−4	3	2	−2	−1	1	0	0	0	0	−1	1	1	1
5, 2	14	6	2	2	0	0	−1	2	0	−1	−1	2	1	0	0
$2^2, 1^3$	14	−6	2	2	0	0	−1	−2	0	−1	1	2	−1	0	0
$5, 1^2$	15	5	3	−1	1	−1	0	−3	−3	0	0	−1	0	1	1
$3, 1^4$	15	−5	3	−1	−1	1	0	3	−1	0	0	−1	0	−1	1
4, 3	14	4	−1	2	−2	1	−1	0	0	2	0	−1	−1	1	0
$2^3, 1$	14	−4	−1	2	2	−1	−1	0	0	2	0	−1	1	−1	0
4,2,1	35	5	−1	−1	−1	−1	0	1	1	−1	1	−1	0	−1	0
1^2	35	−5	−1	−1	1	1	0	−1	1	−1	−1	−1	0	1	0
$4, 1^3$	20	0	2	−4	0	0	0	0	0	2	0	2	0	0	−1
$3^2, 1$	21	1	−3	1	−1	1	1	−3	−1	0	0	1	1	−1	0
$3, 2^2$	21	−1	−3	1	1	−1	1	3	−1	0	0	1	−1	1	0

5.6. Predstavljanje beskonačnih grupa.

Posebno je pitanje kako se predstavljuju *beskonačne* grupe; naravno, problematika je poput one pri *konačnim* grupama, samo što će sredstva i *metode* biti drukčiji i općenito zamršeniji. Od beskonačnih grupa valja spomenuti posebno: grupu translacija prostora R_n od n dimenzija, ortogonalnu grupu O_n (isp. 20 § 4), unitarnu grupu U_n svih unitarnih (n, n) — matrica, itd.

Zadovoljimo se da prikažemo grupu Z rotacija prostora R_3 oko zadane osi.

5.6.1. Predstavljanje grupe Z rotacija oko zadane osi.

Frupa Z je komutativna; zato su ireducibilna predstavljanja od Z numerička (isp. § 3.4.2). Pišemo li Z aditivno pa ako je riječ o predstavljanju $g \in Z \to \Gamma(g) \in R(i)$, odnosno o pripadnom karakteru $g \in Z \to \chi(g)$, tada se radi o *funkcionalnoj* vezi

(1) $$\chi(\alpha+\beta) = \chi(\alpha)\chi(\beta)$$

pri čemu član g iz Z određujemo veličinom α kuta za koji se rotacija g izvodi. Tako dolazimo na zadatak da se riješi funkcionalna jednadžba (1). Kako se varijabla α pri $g = g(\alpha)$ mijenja neprekidno, najjednostavnije je pretpostaviti da je tražena funkcija $\chi(x)$ *neprekidna* pa i *derivabilna* (*izvodljiva*). Uz uslov izvodljivosti od χ, deriviranje po β pri $\beta = 0$ prevodi (1) u

(2) $$\chi'(\alpha) = \chi(\alpha)\chi'(0).$$ Odavde

(3) $$\chi(\alpha) = e^{\chi'(0)\alpha}.$$

Uslov $\chi(0) = \chi(2\pi)$ daje

(4) $$1 = e^{\chi'(0)2\pi}.$$

Iz (4), bar za jednoznačne funkcije $\alpha \to \chi(\alpha)$ izlazi

(5) $$i\chi'(0) = m \in D, \text{ tj. } \chi'(0) = -im, \ (m = 0, \ \pm 1, \ \pm 2, \ldots).$$

Tako dobijemo beskonačno mnogo neekvivalentnih reprezentacija

$$\chi(\alpha) = e^{-im\alpha} \quad (m \in D)$$

pomoću kojih se izgrađuje svaka jednoznačna neprekidna reprezentacija od Z nad $R(i)$.

6. Zadaci o predstavljanju grupa.

1. Kako glasi unitarna reprezentacija ciklične grupe C_n pri $n = 1,2,3, \ldots, 10$? Napisati pripadnu tablicu primitivnih karaktera. 2) Koliko ima nesvodljivih reprezentacija grupe C_n među kojima nema ekvivalentnih?
2. Ako svakoj *ortogonalnoj* matrici ω formata (3, 3) pridijelimo 1) $|\det \omega|$, 2) $\det \omega$, dobije li se pri tom (ireducibilna) reprezentacija ortogonalne grupe O_3 rotacijâ prostora oko zadane tačke O?
3. Pitanje, poput prethodnoga pitanja, za unitarne matrice i pripadnu grupu U_2 svih unitarnih matrica duljine 2.
4. Napisati eksplicitno sve ireducibilne reprezentacije diedarske grupe D_n pri $n = 2, 3, 4, 5, 6, 7, 8, 9, 10$; napisati pripadnu tablicu karakterâ (isp. 33 § 5.4.7—9).

5. Koliko grupa 1) tetraedra, 2) oktaedra, 3) dodekaedra ima unitarnih neekvivalentnih reprezentacija? (isp. 33 § 3 9.4).

6. Nađi direktni produkt tablice primitivnih karaktera grupe tetraedra i tablice grupe: 1) S_2, 2) S_3, 3) S_n, 4) tetraedra, 5) oktaedra, 6) ikozaedra, 7) kvaternionske grupe.

7. Pomoću kriterija o nesvodljivosti (33 § 2.9) provjeriti nesvodljivost opisanih reprezentacija grupâ G_T, G_O, C_4, D_n, itd.

8. Neka su $g \to h(g)$, $g \to h'(g)$ dva ekvivalentna unitarna predstavljanja grupe G nad prostorom V, odnosno V'. Neka je zadana baza e u V. Dokazati da u V' postoji baza e' sa svojstvom da matrični zapis operatora $h(g)$ pri izboru baze e bude isti kao i matrični zapis operatora $h'(g)$ pri bazi e'. Promjenom koordinatne baze e u V prelazi reprezentacija od G nad V u ekvivalentnu reprezentaciju od G nad V'.

9. Svaka ireducibilna matrična reprezentacija duljine d konačne grupe G obuhvata upravo d^2 linearnih matrica (Burnside).

10. **Karakteri zadana broja mod n.** 1) Zadan je prirodni broj n; time je određeno $\varphi(n)$ brojeva i odgovarajuća grupa $(\Phi(n), \cdot)$ brojeva iz $\{0, 1, \ldots, n-1\}$ koji su prosti prema n; stavimo li $x \in D \to \chi(x) = \chi(x_0)$. gdje je $x \in nD + x_0$, $x_0 \in \Phi(n)$ i stavimo li $\chi(x) = 0$ za svaki cio broj koji nije prost prema n dobije se određen (primitivan?) karakter broja x pri mod n. 2) Napisati sve primitivne karaktere brojeva 1, 2, 3, ..., ..., 9, 10 mod 10; 3) — 5) isto kao pod 2) ali s obzirom na modul 9, 11, 12. Prolazi li x potpun sistem ostataka mod n, tada je

$$\sum_x \chi(x) = \begin{matrix} \varphi(n) & \text{pri } \chi \neq \chi_0 \\ 0 & \text{pri } \chi \neq \chi'_0 \end{matrix}.$$ Dokaži da za dani broj n ima konačno mnogo različnih karaktera mod n, i da svaki karakter ima i neke korijene jedinice kao svoje vrijednosti.

11. *Kroneckerov simbol* $\left(\frac{d}{n}\right)$, $d \in D$, $n \in N$. Neka je $d \in 4D \cup (4D+1)$ i neka je d bez kvadratna faktora >1; stavimo:

$$\left(\frac{d}{p}\right) = 0 \text{ pri } p \mid d;$$

$$\left(\frac{d}{2}\right) = \begin{matrix} 1 \\ -1 \end{matrix} \text{ pri } \begin{cases} d \in 8D+1 \\ d \in 8D+5; \end{cases}$$

$\left(\frac{d}{m}\right)$ neka bude Legendreov simbol pri $p > 0$ i za slučaj da p ne dijeli n (isp. 22 § 7.4);

$$\left(\frac{d}{m}\right) = \prod_{\nu=1}^{n} \left(\frac{d}{p_\nu}\right) \text{ pri } m = \prod_{\nu=1}^{n} p_\nu;$$ posebno je $\left(\frac{d}{1}\right) = 1$. 1) Do-

kazati da Kroneckerov simbol proširuje Legendreov simbol. Pri svakom naznačenom d također je funkcija $x \in N \to \left(\frac{\pm d}{x}\right)$ karakter pri mod d; 3) za neko $x \in N$ je $\left(\frac{d}{x}\right) = -1$.

12. Odrediti sve raspodjele broja 3 i naći pripadne ireducibilne reprezentacije grupe S_3 (raspodjela $3 = 2 + 1$ obrađena je u 33 § 5.5.4).

13. Promatraj Youngovu shemu koja odgovara raspodjeli $5 = 3 + 2$ broja 5; 1) na koliko se načina u polja te sheme mogu upisati brojevi 1, 2, 3, 4, 5 tako da u svakom retku sheme brojevi rastu od lijeve strane nadesno, a u svakom stupcu brojevi rastu odozgo naniže? 2) Poređaj leksikografski sve tako dobivene „*standardne permutacije*“ nižući elemente permutacije onako kako se nalaze redom u shemi; npr. $\begin{matrix} 1 & 3 & 5 \\ 2 & 4 & \end{matrix}$ daje permutaciju 1 3 5 2 4; 3) slična pitanja za svaku raspodjelu broja 5; 4) Usporedi dobivene brojeve s *prvim* stupcem tablice karakterâ grupe S_5 u 33 § 5 5.6.2 i uvjeri se da je prvi stupac sačinjen upravo od broja standardnih permutacija unutar odgovarajuće Youngove sheme.

14. Pitanje poput pitanja 13 a u vezi sa $n = 4$ (isp. 33 § 5.5.6.1).

15. Pitanje poput pitanja 13 a u vezi sa $n = 6$ (isp. 33 § 5.5.6.3).

16. Pitanje poput pitanja 13 a u vezi sa $n = 7$ (isp. 33 § 5.5.6.4).

17. Za svaki broj $n \in \{2, 3, 4, \ldots\}$ i svaku raspodjelu ρ broja n duljina pripadnog ireducibilnog predstavljanja grupe S_n jednaka je broju permutacija od $1, 2, \ldots, n$ koje rastu u svakom retku i svakom stupcu Youngove sheme koja je pridružena raspodjeli ρ (A. Young; dokaz pogledati u knjizi Boerner [1] str. 108—111).

18. *Prsten grupe*. Svakoj grupi G pridjeljujemo određen prsten A_G na taj način da elemente od G shvatimo kao slobodne izvodnice u A_G i da dopuštamo formalno množenje $ag (= ga)$ pri $a \in A$, $g \in G$. Prsten A_G je u uskoj vezi s reprezentacijom grupe G. Inače, grupa G i prsten A_G imaju isti jedinični član.

    Ako je G konačno, stavimo $s \equiv \sum_{x \in G} x$; tada je $s \in A_G$ i vrijedi $gs = s$ za svako $g \in G$. Odredi $Gs = \{gs; g \in G\}$. Teorija o reprezentaciji grupe G može se razviti promatranjem prstena (algebre) A_G (isp. Boerner [1] str. 49—; Hall [1], Waerden [2], str. 179—).

Literatura

Boerner [1]; Bourbaki [1]; Burnside [1]; Gantmaher [1]; Kurepa Sv. [1]; Kuroš [3]: L'ubarski [1]; Serre [1]; Speiser [1]; Vilenkin [1]; Waerden [1]; Weyl [2]; Wintner [1].

POGLAVLJE 34.

ALGEBRA TENZORA

0. UVODNA RAZMATRANJA

Vektori, matrice, kvadratne forme usko su vezani s pojmom linearnih (vektorskih) prostora (13 § 3.1, 26 § 1.1.) i s linearnim transformacijama tih prostora (26 § 2.1). Sada ćemo upoznati jednu *posebnu vrstu vektora* koji se zovu *tenzori* i koji predstavljaju dalju razgradnju i primjenu ideja vezanih za vektorske prostore, i koji omogućuju da od zadanih vektorskih prostora gradimo nove vektorske prostore i s njima izvodimo pojedine algebarske operacije.

Za tenzorsku vrstu vektora posebno je važan „tenzorski produkt vektora" (v. § 1.9); pri tome se valja sjetiti da općenito ni skalarni ni vektorski produkt dvaju vektora nije definiran (isp. 25. poglavlje).

Kako se radi o dvije vrste vektora — *kovarijantni i kontravarijantni vektori* — vrlo je korisno to razlikovanje unijeti i u način označavanja vektora. Uopće, problematika u vezi s linearnim funkcijama od više vektorskih promjenljivicâ usko je vezana: s upotrebom mnogih indeksa, sumacijâ i promjenâ koordinatnih baza i s predstavljanjem tih funkcija pri promjenama koordinatne baze i njihovih veza sa općim linearnim grupama.

Posebno je od bitne važnosti kako se pojedina veličina-koordinata vlada pri promjenama koordinatnih baza.

Kako bi se sve to moglo lakše pratiti i dobiti bolji uvid u zakone pri linearnim transformacijama, bit će korisno uvesti nove konvencije o simbolici i označavanju.

1. NEKOLIKO OSNOVNIH DOGOVORA I ČINJENICA

1.1. Pojava gornjih i donjih indeksa. Ako izričito ne kažemo drukčije *eksponent će imati ulogu indeksa*; prema tome x^2 neće značiti $x\,x$ nego $x^{(2)}$; isto tako x^n će značiti $x^{(n)}$ a ne $\underbrace{x\,x\,x \ldots x}_{n}$ (n je prirodan broj). Na taj način npr. a_k^2 stoji umjesto $(a_k)^{(2)}$ ili $(a^{(2)})_k$. Govorit ćemo o *donjim indeksima* i o *gornjim indeksima.*

Ta alternativa je u vezi s alternativom „kovarijantan—kontravarijantan", odnosno „redak — stupac".

1.1.1. Posebno, kad se govori o matrici a i njenim vrijednostima a_{ij}, pisat ćemo a_j^i umjesto a_{ij}, tj. $a_j^i = a_{ij}$ (*gornji indeks označufe retke a donji indeks označuje stupce*).

1.2. Tenzorski ili Einsteinov način oznake sumiranja. Ako se u nekom monomu pojavi *isti indeks i kao gornji indeks i kao donji indeks*, onda to znači (osim ako se ne kaže suprotno) da se po tom indeksu treba sumirati (zbrajati); pri tom se zna uvijek kolika je oblast (domen) svakog indeksa.

Tako npr. $a_j^i b_i^k$ znači $\sum a_j^i b_i^k$. Ako i protječe skupom $\{1, 2, 3, 4\}$, onda je dakle

$$a_j^i b_i^k \overset{\text{def}}{=\!=} \sum_{i=1}^{4} a_j^i b_i^k = a_j^1 b_1^k + a_j^2 b_2^k + a_j^3 b_3^k + a_j^4 b_4^k .$$

1.3. Oznaka članova raznih baza vektora. Radi li se o nekom vektorskom prostoru V, njegovoj bazi $e = (e_1\ e_2 \ldots e_n)$ i vektorima e_i, tada ćemo neku drugu bazu toga prostora općenito označivati upotrebom apostrofa dakle e' a članove te baze nećemo (kao dosad) označavati sa $e'_1, e'_2, \ldots, e'_n$ nego kao $(e_{1'}, e_{2'}, \ldots e_{n'},)$; prema tome $e_{i'}$ je i-ti član nove baze e' (a ne i'-ti član stare baze e). Isto tako članovi baze e'' bili bi $e_{1''}, e_{2''}, \ldots$

1.4. Kontravarijantne koordinate vektora. Ako je V prostor a $(e_1 e_2 \ldots e_n)$ njegova baza, tada smo za svako $v \in V$ imali rastav

$$v = \sum_{\nu=1}^{n} v_\nu e_\nu;$$

da se možemo služiti tenzorskom konvencijom o zbrajanju pisat ćemo v^ν umjesto v_ν i tako dobiti

$$v = v^\nu e_\nu \left(= \sum_{\nu=1}^{n} v_\nu e_\nu \right);$$

v_ν se zove *ν-ta koordinata vektora v,* i to *kontravarijantna ν-ta koordinata vektora v.*

Kovarijantne koordinate vektora $v \in V$ jesu skalarni produkti

$$(v,\ e_\nu)\ (\nu = 1, 2, \ldots n);$$

prema tome $(v,\ e_\nu)$ je definirano samo ako je definirano skalarno množenje vektora (isp. 25. poglavlje).

1.5. Pridruživanje V → V*. Vrlo je važno pridruživanje $V \to V^*$ kojim svakom vektorskom prostoru V pridružujemo *dual* V^* toga prostora (isp. 26 § 2.4).

Po definiciji, V^* se sastoji od svih aditivnih homogenih preslikavanja

$$x \in V \to L\,x \in K$$

prostora V u tijelo K nad kojim je prostor V i definiran (najvažniji su slučajevi $K = R$, $K = R(i)$).

⟶ **1.5.1. Teorem.** ***Ako je*** **dim** $V = n \in N$, ***tada je*** **dim** $V^{\star} = $ **dim** V; ***štaviše neka je*** $e = (e_1, e_2, \ldots e_n)$ ***baza u*** V ***i*** $\nu \in \{1, 2, \ldots, n\}$; ***neka je*** e^i ***ona linearna forma*** e^i: $V \to K$ ***za koju je***

$$e^i(e_k) = \delta^i_k \equiv \begin{cases} 1 \\ 0 \end{cases} pri \ \begin{cases} i = k \\ i \neq k \end{cases};$$

tada je $(e^1, e^2, \ldots, e^n)$ ***vektorska baza prostora*** $V^{\star}$ i zove se *dual baze e* i označuje se sa $e_{\star}$, tj. $e_{\star} = (e^1, e^2, \ldots, e^n)$.

Naime, iz $v = v^k e_k$ imamo

$$e^\nu v = e^\nu v^k e_k = v^k e^\nu e_k = v^k \delta^\nu_k = v^\nu.$$

Za svako $F \in V^{\star}$ imamo

$$F v = F v^\nu e_\nu = v^\nu F e_\nu = F e_\nu v^\nu = F e_\nu e^\nu v.$$

Drugim riječima

$$F v = F e_\nu e^\nu v, \text{ odnosno } F = F e_\nu e^\nu;$$

broj $F e_\nu$ zove se ν*-ta kovarijantna koordinata vektora F u bazi e* i označuje se sa F_ν; dakle

$$F_\nu = F e_\nu, \quad F = F_\nu e^\nu.$$

Posebno, pomoću (e_ν) određeno je i F_ν i e^ν.

Dakle zaista „vektori“ e^ν razapinju $V^{\star}$; dokažimo još da su oni linearno nezavisni, tj. da

$$\lambda_\nu e^\nu = 0 \Rightarrow \lambda_\nu = 0.$$

No, $\lambda_\nu e^\nu = 0$ znači $v \in V \Rightarrow \lambda_\nu e^\nu v = 0$;

posebno pri $v = e_i$ znači to da je

$$\lambda_\nu e^\nu e_i = 0, \text{ tj. } \lambda_\nu \delta^\nu_i = 0 \text{ tj. } \lambda_i = 0.$$

1.5.2. Definicija. Svaki vektor iz V zove se kontravarijantnim vektorom; svaki vektor iz $V^{\star}$ zove se *kovarijantnim vektorom.*

⟶ **1.6. Teorem.** ***Ako vektorski prostor V ima konačnu dimenziju, onda je V refleksivan prostor u smislu da vrijedi*** $(V^{\star})^{\star} = V$ ***(Dual duala je ishodni prostor V); ako je e baza u V, a*** $e_{\star}$ ***baza u*** $V^{\star}$ ***koja je sa e dualna, onda je*** $(e_{\star})_{\star} = e$.

Dokaz.

Naime, dokažimo da između V, $V^{\star\star}$ postoji određen izomorfizam koji je *definiran bez posredstva koordinatne baze.* Posebno za svako $u \in V$ i svako $v^{\star} \in V^{\star}$ izraz $v^{\star}(u)$ je potpuno obređen član iz tijela K nad kojim je V definirano! Pišući po definiciji

(1) $$u(v^{\star}) \stackrel{\text{def}}{=} v^{\star}(u),$$

dokažimo da je

(2) $$v^{\star} \in V^{\star} \to u(v^{\star}) \in K$$

linearna homogena forma s vrijednostima u K; dakle je

$$u \in (V^\star)^\star \, (\equiv V^{\star\star}) \quad \text{tj.} \quad V \subset V^{\star\star}.$$

Dokažimo da je preslikavanje (2) aditivno, tj. pri

$$v^\star, w^\star \in V^\star \qquad \text{imamo}$$

$$u(v^\star + w^\star) = u(v^\star) + u(w^\star).$$

No ta je jednakost ekvivalentna sa

$$(v^\star + w^\star)(u) = v^\star(u) + w^\star(u).$$

A ta je relacija ispravna jer se tako upravo i definira suma $v^\star + w^\star$ članova $v^\star$, $w^\star$ iz $V^\star$. Isto tako je ispravno

$$u(\lambda v^\star) = \lambda u(v^\star)$$

jer je ta jednakost ekvivalentna s jednakosti

$$(\lambda v^\star) u = v^\star(\lambda u);$$

a ta jednakost je upravo definicija produkta $\lambda v^\star$ pri $\lambda \in K$, $v^\star \in V^\star$.

Ako je $u \neq t \in V$, *tada se preslikavanje* (2) *i preslikavanje* $v^\star \to t(v^\star)$ *razlikuju.* U obrnutom slučaju bilo bi

$$u(v^\star) = t(v^\star), \text{ tj. } v^\star(u) = v^\star(t), \text{ tj. } v^\star(u-t) = 0.$$

Međutim, odatle nužno izlazi $u - t = 0$, tj. $u = t$, jer za svako $0 \neq x \in V$ postoji bar jedno $v^\star \in V^\star$ za koje je $v^\star(x) \neq 0$ (npr. stavljajući $v^\star = 1$ po nekoj bazi prostora V u kojoj je uključen i sam vektor x).

Dakle je *preslikavanje* $u \in V \to (u | V^\star \to K)$ *zaista prirodno izomorfno smještavanje prostora* V *u* $V^{\star\star}$; u tom je smislu $V \subset V^{\star\star}$; kako je

$$n = \dim V = \dim V^\star, \ \dim V^\star = \dim V^{\star\star}, \text{ to je } \dim V = \dim V^{\star\star},$$

pa zbog $\dim V < \aleph_0$ i $V \subset V^{\star\star}$ izlazi da je zaista $V = V^{\star\star}$.

Dokaz je tekao a da nije bilo govora o bazi e u V; ako je prostor V snabdjeven određenom bazom (e_i), tada je prostor $V^\star$ snabdjeven dualnom bazom (e^j) za koju je po definiciji $e^j(e_i) = \delta_i^j$. Obrazac (1) pri $u = e_i$, $v^\star = e^j$

postaje $$e_i(e^j) = e^j(e_i) = \delta_i^j, \quad \text{tj.} \quad e_i(e^j) = \delta_i^j.$$

Drugim riječima, ono što vrši e^j na e_i vrši i e_i na e^j: rezultat δ_i^j je isti; a to znači da postupak koji vodi od e na $e_\star$ primjenjen na $e_\star$ daje opet polaznu bazu e. Time je teorem 1.6. potpuno dokazan.

1.7. Kontravarijantnost i kovarijantnost.

1.7.1. Definicija. Neka je V zadan vektorski prostor nad nekim tijelom K; članovi iz V zovu se kontravarijantni vektori; uz zadanu bazu $(e_1, e_2, \ldots, e_n)$ i zadano $v \in V$ veličine v^ν za koje je $v = v^\nu e_\nu$ zovu se *kontravarijantne koordinate* kontravarijantnog vektora v u odnosu na bazu e. Članovi iz $V^\star$ zovu se kovarijantni vektori; za dano $v^\star \in V^\star$ veličine $v^\star{}_\nu$ za koje je $v^\star = v^\star{}_\nu e^\nu$, pri čemu je $e^\nu e_k = \delta_k^\nu$ zovu se *kovarijantne koordinate kovarijantnog vektora* $v^\star$.

Prema tome, svaki kovarijantni (kontravarijantni) vektor ima pri svakoj bazi svoje kovarijantne (kontravarijantne) koordinate; a ako je vektorski prostor euklidski, tj. prostor R^n s pitagorovskom definicijom razdaljine među tačkama, tada se na osnovu teorema 1.6.1. lako vidi da svaki njegov vektor ima i jednu i drugu vrstu koordinata; ako je baza ortonormirana, obje se vrste koordinata poklapaju.

1.7.2. Kako je $V = V^{\star\star}$ znači to da su vektori iz V također kovarijantni (kao članovi iz $(V^\star)^\star$); iz istog su razloga članovi iz $V^\star$ kontravarijantni uzimajući $V^\star$ kao ishodni prostor.

1.8. Još o promjeni baza (isp. 23 § 3).

Izborom baze e u vektorskom prostoru V određuje se svaki vektor $v \in V$ odgovarajućim koordinatama prema toj bazi. Promjenom baze prostora promijene se i koordinate istog vektora. A promjena baza opisuje se grupom regularnih matrica. Kako dobiti pregledan uvid u veze među bazama i koordinatama u V te u odgovarajućim dualnim bazama $V^\star$?

Služeći se gornjim i donjim indeksima te tenzorskim dogovorom o sumiranju odgovor na prethodno pitanje daje

⟶ **1.8.1. Teorem.** *Zadan je vektorski prostor* $V = V_m$ *od* m *dimenzija* $(<\infty)$ *i u njemu vektorska baza* $e = (e_1 e_2 \ldots e_m)$*; time je automatski određen dualni prostor* $V^\star$ *kao i dualna baza* $e_\star = (e^1, e^2, \ldots e^m)$*. Pomoću regularne* (m, m)*-matrice* $a = [a_{ij}] = [a_j^i]$ *uvedimo u* V *novu bazu*

$$e' = (e_{1'}, e_{2'}, \ldots e_{m'}) \qquad \textit{ovako;}$$

(1) $$e' = e\,a, \text{ tj. } [e_{1'}\, e_{2'} \ldots e_{n'}] = [e_1\, e_2 \ldots e_n] \begin{bmatrix} a_1^1\, a_2^1 \ldots a_n^1 \\ \cdots\cdots \\ a_1^n\, a_2^n \ldots a_n^n \end{bmatrix} \qquad \textit{tj.}$$

(B) $$e_{j'} = a_{j'}^i e_i .$$

Bazi e' *u* V *odgovara dualna baza* $e'_\star$ *u prostoru* $V^\star$.

(0) *Tada za svaki kontravarijantni vektor* $v \in V$ *imamo stare i nove kontravarijantne koordinate* v^i, $v^{j'}$:

(2) $v = v^i e_i = v^{j'} e_{j'}$ *, i odgovarajuće veze oblika*

(3) $v^i = a_{j'}^i v^{j'}$ *, odnosno* $v^{j'} = (a^{-1})_i^{j'} v^i$.

(00) *Istom matricom* $a_{j'}^i$ *uspostavlja se određena veza među dualnim bazama* $e_\star = (e^1, e^2, \ldots e^m)$, $e'_\star = (e^{1'}, e^{2'}, \ldots, e^{m'})$ *i to relacijama*

(B~) $$e^i = a_{j'}^i \cdot e^{j'}$$

(veza B~ je kontragredijentna prema vezi (B) jer se u (B) nova baza izražava starom bazom, a u (B~) izražava se stara baza novom bazom (izražajna matrica je ista u oba slučaja!).

(000) *Za svaki kovarijantni vektor* $v^\star \in V^\star$ *imamo rastave u staroj dualnoj bazi*

$$e_\star = (e^1, e^2, \ldots e^m) \textit{ i u novoj dualnoj bazi } e'^\star = (e^{1'}, e^{2'}, \ldots, e^{m'})$$

i pripadne kovarijantne komponente $v_i{}^\star$ *(stare)* $v_{j'}{}^\star$ *(nove):*

(5) $$v^\star = v_i{}^\star e^i = v_{j'}{}^\star e^{j'},$$

kao i pripadne kovarijantne transformacije:

(6) $$v_{j'}{}^\star = a^i_{j'} v_i{}^\star, \text{ odnosno } v_i{}^\star = (a^{-1})^{j'}_i v_{j'}{}^\star.$$

U svim gornjim vezama među istorodnim veličinama pri staroj bazi i pri novoj bazi javlja se ista matrica s rodnim elementom $a^i_{j'}$; a iz $a^i_{j'}$ se uspostavlja veza tako da se formalno $a^i_{j'}$ pomnoži s nekim simbolom oblika c_i ili $c^{j'}$ kako bi se time automatski imalo sumaciju po indeksu i odnosno j'; a onda se dobiven rezultat izjednači sa $c_{j'}$ odnosno c^i (indeks po kojem se ne sumira prenosi se s jedne strane jednakosti na drugu stranu jednakosti).

1.8.1.⋆ Teorem

(0)⋆ *Isto tako ako je* $e_i = b^i_{j'} e^{j'}$ (a staru bazu izražavamo novom!) *tada je* $e_{j'} = b^i_{j'} e_i$ *(mnemotehnički ta veza nastaje ovim redom:*

$$b^i_{j'}$$
$$b^i_{j'} e_i$$
$$e_{j'} = b^i_{j'} e_i).$$

(00)⋆ *Nadalje za svako* $v \in V$ *imamo kontravarijantne koordinate (koordinate nose gornje indekse)*

$$v^{j'} = b^{j'}_i v^i.$$

(000)⋆ *Za svako* $v^\star \in V^\star$ *imamo kovarijantne koordinate (donji indeksi na koordinatama):*

$$v^\star_i = b^{j'}_i v^\star_{j'}.$$

Bez gornjih konvencija o indeksima, apostrofima indeksa i sumaciji iskaz osnovnog teorema 1.8.1 bio bi nepregledan.

Teorem 1.8.1 izlazi iz 23 § 3 i relacijâ $e^i e_j = \delta^i_{j'}$ odnosno iz relacija

$$e^i v = v^i, \quad e^{i'} v = v^{i'} \quad \text{te} \quad e_i v^\star = v^\star_i.$$

Uistinu, unese li se $e_{j'}$ prema (B) u (2) izlazi (3). Dokažimo veze (B~). Svakako je

(7) $$e^{j'} = c^{j'}_i e^i$$

za neku regularnu matricu c.

Iz (7) izlazi

$$e^{j'}(e_k) = c^{j'}_i e^i(e_k) = c^{j'}_i \delta^i_k = c^{j'}_k, \qquad \text{tj.}$$

(8) $$e^{j'}(e_k) = c^{j'}_k.$$

S druge strane iz

$$\delta^{j'}_{i'} = e^{j'}(e_{i'}) = e^{j'}(a^k_{i'} e_k) = a^k_{i'} e^{j'}(e_k) \qquad \text{izlazi da je}$$

(9) $$e^{j'}(e_k) = (a^{-1})^{j'}_k.$$

Iz (8) i (9) izlazi da je $a^{-1}=c$, tj. $e^{j'}=(a^{-1})_i^{j'}e^i$ odakle $a_{j'}^i e^{j'}=e^i$, što se i tvrdi relacijama (B~).

Relacije (5), (6) izlaze iz dokazanih relacija (2), (3) zamjenama

$$v \to v^\star, \quad e_i \to e^i, \quad a \to a^{-1}, \quad v^j \to v_j^\star.$$

I preostali dio teorema 1.8.1 se dalje lako dokazuje.

Evo još daljih primjera o transformacijama.

1.8.2. Umjesto *kontravarijantnog* vektora $v=v^i e_i$ možemo promatrati proizvoljnu *linearnu homogenu funkciju* veličinâ v^i:

$$v \in V \to L(v) = L(v^i e_i) = L(e_i)\, v^i \in K,$$

i gledati kako se transformiraju njeni koeficijenti $L(e_i) \in K$ pri transformaciji $e_{j'}=a_{j'}^i e_i$; tada prema (3) imamo

$$L(e_i)\, v^i = L(e_i)\, a_{j'}^i v^{j'},$$

tj. novi koeficijenti forme su $a_{j'}^i L(e_i)$, i izražavaju se iz starih koeficijenata $L(e_i)$ *istom* transformacijom a kojom se *nova* baza izražava pomoću *stare* koordinatne baze. Tako vidimo da je zaista opravdano linearne forme $f: V \to K$ zvati kovarijantnim vektorima i definirati dual $V^\star$ kao skup upravo takvih linearnih forama $V \to K$.

1.8.3. Umjesto *kovarijantnog vektora* $v^\star = v_j^\star e^j$ možemo promatrati proizvoljnu linearnu formu (funkciju) kovarijantna vektora $v^\star$:

$$v^\star \in V^\star \to L(v^\star) \in K,$$

i gledati kako se pri promjeni baze u V transformiraju koeficijenti te funkcije. Imamo

$$L(v^\star) = L(v_j^\star e^j) = v_j^\star L(e^j);$$

koeficijenti su $L(e^j) \in K$; ako je $e_{j'} = a_{j'}^i e^{j'}$, tada je

$$L(e^j)\, v_j^\star = L(e^j)(a^{-1})_j^{i'} v_{i'}^\star.$$

Tu se pojavljuje inverzna matrica a^{-1}; to je u skladu s nazivom da su članovi od $V^{\star\star}$ kontravarijantni vektori iz V.

1.8.4. *Dvojako linearne forme vektora.* Riječ je o formi (funkciji) $L(x, y)$ (ili naprosto $L(x, y)$ pri čemu $x \in X$, $y \in Y$, $\{X, Y\} \subset \{V, V^\star\}$.

Imamo ove slučajeve:

1) oba argumenta su kontravarijantna $x, y \in V$,

2) $x \in V$, $y \in V^\star$

3) $x \in V^\star$, $y \in V$

4) $x, y \in V^\star$.

Već prema tome o kojem se slučaju radi očekujemo da će se pri promjeni (B) baze koeficijenti forme L vladati na odgovarajući način.

Obradimo npr. slučaj $L\ (v,\ v^\star)$. Imamo

$$L\,(v,\ v^\star) = L\,(v^i\,e_i,\ v_k^\star\,e^k) =$$

(zbog linearnosti od L prema prvom argumentu)
$= v^i L\,(e_i,\ v_k^\star\ v^k) =$ (zbog linearnosti od L prema 2. argumentu) $= v_i\,L\,(e_i, e^k)\,v_k^\star$. Dakle je L funkcija komponenata v^i, $v_k^\star$ s koeficijentima $L\ (e_i, e^k) \in K$; stavimo $L\ (e_i,\ e^k) = L_i{}^k$ odnosno L_i^k.

Dakle je riječ o funkciji

$$\text{(1)} \qquad v^i\,L_i^k\,v_k^\star\ \left(=\sum_{i,\,k=1}^{m} v^i\,L_i^k\,v_k^\star\right).$$

Na osnovu promjene (B) koordinatne baze izraz (1) postaje na osnovu 1.8.1.:

$$a_{k'}^i\,v^{k'}\,L_i^k\,(a^{-1})_k^{j'}\,v_{j'}^\star;$$

tj. novi koeficijenti su

$$L_{k'}^{j'} = a_{k'}^i\,L_i^k\,(a^{-1})_k^{j'};$$

vidimo da se uz donji indeks zadana koeficijenta javlja matrica a a uz gornji indeks matrica a^{-1}.

Odgovarajući bi se zaključak dobio promatrajući i ostale vrste dvaput linearnih (bilinearnih) formi:

$$L\,(v_{(1)}\,v_{(2)}),\ L\,(v^\star,\ v),\ L\,(v_{(1)}^\star,\ v_{(2)}^\star).$$

1.8.5. Multilinearne forme vektora.

Posve analogno se definiraju i obrađuju *triput* (*trojako*) *linearne forme* $L\,(x,\,y,\,z)$ i uopće r-puta linearne forme $L\,(\vec{x}\,(1),\ \vec{x}\,(2),\,\ldots,\ \vec{x}\,(r))$ ili kraće $L\,(x\,(1),\ x\,(2),\ldots,x\,(r))$ pri čemu je $x\,(\rho) \in V$ ili $x\,(\rho) \in V^\star$.

Tako npr. za slučaj linearne forme $L\,(x,\,y,\,z^\star)$ bilo bi

$$L\,(x, y,\ z^\star) = x^i\,y^j\,z_k^\star\,L\,(e_i\,e_j\,e^k) = x^i\ y^j\ z_k^\star\,L_{ij}^k.$$

Poslije promjene (B) koordinatne baze izlazi

$$L = a_{\alpha'}^i\,a_{\beta'}^j\,(a^{-1})_k^{\gamma'}\,L_{ij}^k\,x^{\alpha'}\,y^{\beta'}\,z_{\gamma'}^\star.$$

Drugim riječima, novi su koeficijenti

$$a_{\alpha'}^i\,a_{\beta'}^j\,L_{ij}^k\,(a^{-1})_k^{\gamma'};$$

oni se iz starih koeficijenata dobiju tako da u vezi s *donjim indeksima* djeluje *transformaciona matrica a*, a u vezi sa *gornjim indeksima* djeluje *inverzna matrica* a^{-1} (zapravo kontragredijentna matrica $a^\sim$; isp. 25 § 7.4.4).

Kraće se kaže da je *forma dvaput kovarijantna i jedanput kontravarijantna* (pri tome ne zaboravimo da su argumenti-vektori forme bila dva kontravarijantna i jedan kovarijantni vektor).

1.9. Formalni ili tenzorski produkt dvaju vektora.

1.9.1. Neka je $(e_1\, e_2 \ldots e_m)$ baza u V_m a $(f_1, f_2, \ldots, f_n)$, baza u V_n te

$(f^1, f^2, \ldots, f^n)$ dualna baza u $V_n^\star$.

Zadan je kontravarijantan vektor $v = v^i\, e_i \in V_m$ i kovarijantan vektor

$$w^\star = w_j\, e^j \in V_n^\star \text{ (ne mora biti } m = n).$$

Nađimo formalno produkt

$$(1) \qquad v \otimes w \stackrel{\text{def}}{=} (v^i\, w_j)\, e_i \otimes f^j,$$

pri čemu $e_i \otimes f^j$ pri $i \in \{1, \ldots, m\}$, $j \in \{1, 2, \ldots, n\}$ *smatramo linearno nezavisnim vektorima.* Promjenom

$$(\mathrm{B})\; e_{i'} = a^i_{i'} e_i,\; f_{j'} = b^j_{j'} f_j$$

bazâ izraz (1) postaje

$$v^i\, w_j\, (a^{-1})^{i'}_i\, e_{i'} \otimes b^j_{j'}\, f^{j'} = (a^{-1})^{i'}_i\, b^j_{j'}\, v^i\, w_j\, (e_{i'} \otimes f^{j'}).$$

U novim komponentama javlja se $a^{-1} = b$ u vezi sa v^i te a u vezi sa w_i.

Analogno bi pri $v(1) \in V_m$, $v(2) \in V_m$, u vezi sa produktom $v(1) \otimes v(2)$ u produktu dolazilo a^{-1} dvaput, a u vezi s produktom $v(1) \otimes v(2) \otimes w(3)^\star$ došlo bi u produktu a^{-1} dvaput te b jedanput.

Na osnovu gornjih primjera i rasuđivanja postavlja se ova definicija tenzorskog produkta vektorskih prostora.

2. OKO DEFINICIJE TENZORA

2.1. Tenzorski produkt dvaju prostora (isp. 33 § 4.1.1)

2.1.1. Definicija. Nad nekim tijelom K zadan je vektorski prostor V_m i u njemu baza $(e_1, e_2, \ldots, e_m)$, te vektorski prostor V_n i baza $(f_1, f_2, \ldots, f_n)$. *Tenzorski produkt prostora V_m i prostora V_n* jest onaj vektorski prostor $V_m \otimes V_n$ nad K kojemu su uređeni parovi (e_μ, f_ν) članovi baze; piše se $e_\mu \otimes f_\nu$ umjesto (e_μ, f_ν) *i pri tom računamo na uobičajen način,* specijalno za svako $\lambda \in K$ zahtijevamo da bude

$$\lambda\,(e_\mu \otimes f_\nu) = (\lambda\, e_\mu) \otimes f_\nu = e_\mu \otimes (\lambda f_\nu),$$

$$x \otimes y + x \otimes y' = x \otimes (y + y') \text{ (svojstvo aditivnosti).}$$

Prema tome iz $t \in V_m \otimes V_n$ izlazi da je

$$t = t^{\mu\nu}\,(e_\mu \otimes f_\nu) \quad \text{pri čemu je } t^{\mu\nu} \in K.$$

Naravno, $\quad \dim\,(V_m \otimes V_n) = \dim V_m \cdot \dim V_n = m \cdot n.$

Svaki član vektorskog prostora $V_m \otimes V_n$ zove se *tenzor nad V_m i nad V_n*. (isp. § 4.8).

2.1.2. *Definicija dijade.* Specijalno, za svako $x \in V_m$ i svako $y \in V_n$ tenzorski produkt $x \otimes y$ je određen član t iz $V_m \otimes V_n$ i zove se *dijada*; pišemo

$$t = x \otimes y. \text{ Ako je } x = x^\mu e_\mu,\; y = y^\nu f_\nu,$$

$$\text{tada je } \quad t = x^\mu y^\nu e_\mu \otimes f_\nu, \quad \text{tj.} \quad t^{\mu\nu} = x^\mu y^\nu.$$

To znači *da je tenzor t suma od $\leq mn$ dijada oblikâ*

$$(y^\nu e_\mu) \otimes (x^\mu f_\nu).$$

2.1.3. *Skalare,* tj. članove tijela K zvat ćemo *tenzori razreda* 0.

2.2. Tenzorski produkt (opći slučaj).

2.2.1. Definicija. Neka je zadan prirodan broj r te r-član niz

(1) $$V(1),\ V(2), \ldots, V(r)$$

vektorskih prostora nad tijelom K s bazama

(2) $$e(1) = (e(1)_{i_1})_{i_1}, \ldots, e(r) = (e(r)_{i_r})_{i_r}.$$

Shvatimo li uređene r-torke

$$(x, y, \ldots, z) \stackrel{\text{def}}{=} x \otimes y \otimes \ldots \otimes z \text{ pri } x \in e(1),\ y \in e(2), \ldots, z \in e(r)$$

kao *linearno nezavisne vektore s kojima se računa po svagdašnjim pravilima* o nekomutativnim monomima, posebno

(3) $$\lambda(x \otimes y \otimes \ldots \otimes z) = (\lambda x) \otimes y \otimes \ldots \otimes z = x \otimes (\lambda y) \otimes \ldots \otimes z =$$
$$= \ldots = x \otimes y \otimes \ldots \otimes (\lambda z), \text{ pri } \lambda \in K \quad \text{(svojstvo homotetičnosti)},$$
$$x \otimes y \otimes \ldots \otimes z + x' \otimes y \otimes \ldots \otimes z = (x + x') \otimes y \otimes \ldots \otimes z,$$
$$x \otimes y \ldots \otimes z + x \otimes y \ldots \otimes z' = x \otimes y \ldots \otimes (z + z') \text{ (svojstvo aditivnosti)},$$

tada skup

(4) $$e(1) \otimes e(2) \otimes \ldots \otimes e(r)$$

svih takvih uređenih r-torki *razapinje određen vektorski prostor* koji se zove *tenzorski produkt prostorâ* $V(1)$, $V(2) \ldots V(r)$, a označuje se sa

(5) $$W = V(1) \otimes V(2) \otimes \ldots \otimes V(r).$$

2.2.2. *Tenzor.* Svaki član t iz vektorskog prostora (5) zove se *tenzor nad* prostorima $V(1), \ldots, V(r)$. Kaže se da je svaki taj tenzor *razreda r;* ako u nizu $V(1), V(2), \ldots, V(r)$ ima p kontravarijantnih i q kovarijantnih članova, tada se kaže da je t *kontravarijantan p puta i kovarijantan q puta,* ili kraće da je t *tenzor razreda $(p+q)$.*

Dimenzija prostora W iz (5) je umnožak dimenzija njegovih faktora

$$V(1), \ldots, V(r).$$

2.2.3. *Tenzorske potencije zadana prostora $V_m = V$.* Definicija. Tenzorski produkt oblika $\underbrace{V \otimes V \otimes \ldots \otimes V}_{k}$ zove se *k-ta tenzorska potencija prostora V,* i označuje se sa $V^{(k)}$.
Posebno se stavlja $V^{(1)} = V$.

2.2.4. *Definicija r-ade.*

Specijalno za svaki r-niz vektorâ

$$v(\rho) \in V(\rho) \quad (\rho = 1, 2, \ldots r)$$

imamo pripadni tenzor

$$\overset{r}{\underset{\rho=1}{\otimes}} v(\rho) = v(1) \otimes v(2) \otimes \ldots \otimes v(r);$$

svaki takav tenzor koji je tenzorski produkt od r vektorâ zove se *r-ada.*

Posebne r-ade su one kojima su faktori uzeti iz bazâ prostorâ $V(\rho)$; takve r-ade su oblika

$$(\star) \qquad e(1)_{i_1} \otimes e(2)_{i_2} \otimes \ldots \otimes e(r)_{i_r}.$$

Sve takve r-ade čine bazu (osnovu) samog vektorskog prostora W.

Naravno, pomnoži li se r-ada $(\star)$ nekim skalarom λ dobit će se opet r-ada, npr. r-ada $(\lambda\, e(1)_{i_1}) \otimes e(2)_{i_2} \otimes \ldots \otimes e(r)_{i_r}$; specijalno, rastav proizvoljna tenzora $t \in W$ u komponente po bazi vektorâ oblika $(\star)$ daje:

2.2.5. Teorem. *Svaki tenzor razreda r nad prostorima: $V(1)$ s bazom $(e(1)_{i_1})$, $V(2)$ s bazom $(e(2)_{i_2}), \ldots$, $V(r)$ sa bazom $(e(r)_{i_r})$ je suma od određena broja r-ada:*

$$t = t^{i_1 i_2 \cdots i_r} (e(1)_{i_1} \otimes \ldots \otimes e(r)_{i_r});$$

broj sumanada je $\leq \dim V(1) \cdot \dim V(2) \ldots \dim V(r)$.

2.3. Afinori ili afini tenzori.

U specijalnom slučaju ako je svaki od prostora $V(1), V(2), \ldots, V(r)$ član iz $\{V_m, V_m^\star\}$, odgovarajući tenzori, tj. članovi iz (5) zovu se *afini tenzori ili afinori nad prostorom V_m*; on je p puta kontravarijantan ako niz (1) sadrži p puta V_m kao član; tenzor t je q puta kovarijantan ako se $V_m^\star$ u nizu (1) nalazi q puta kao član.

Tako npr. članovi iz $V_m^{(2)}$ (odnosno iz $V_m^{\star(2)}$) jesu afinori razreda 2 koji su 2 put kontravarijantni (kovarijantni); posebno $v(1) \otimes v(2) \in V^{(2)}$ jesu kontravarijantne dijade; tenzori oblika $v(1) \otimes v(2) \otimes v(3)^\star \in V_m^{(2)} \otimes V_m^\star$ jesu trijade nad V_m a 2-put su kontravarijantne i 1-put kovarijantne.

2.3.1. Koordinate afinora. Neka je tenzor t nad vektorskim prostorom V_m afinor razreda r i to kontravarijantnosti p i kovarijantnosti $q = r - p$; dakle je

$$(1) \qquad t \in V_m^{(c_1)} \otimes V_m^{\star(c_2)} \otimes V_m^{(c_3)} \otimes V_m^{\star(c_4)} \ldots \text{ pri } c_1 + c_3 + \cdots = p,\ c_2 + c_4 \ldots = q,\ c_i > 0.$$

Neka je $(e_1, e_2, \ldots, e_m)$ baza u V_m, a $(e^1, e^2, \ldots, e^m)$ dualna baza u $V_m^\star$; tada bazu u $V_m^{c_1}$ čine vektori $(e_{i_{11}} e_{i_{12}} \ldots e_{i_1 c_1})$ pri čemu se indeksi $i_{11}, i_{12}, \ldots, i_{1c_1}$ kreću nezavisno u skupu $\{1, 2, \ldots, m\}$; dakle je $\dim V_m^{(c_1)} = m^{c_1}$; isto tako bazu u $V_m^{\star(c_2)}$ čine vektori $(e^{i_{21}}, e^{i_{22}}, \ldots, e^{i_2 c_2})$ pri čemu se indeksi i_{21}, i_{22}, i_{2c_2} kreću nezavisno u $\{1, 2, \ldots, m\}$. Analogno za prostore $V_m^{(c_3)}, V_m^{\star(c_4)}$ itd. Odatle izlazi da bazu samog prostora

$$(2) \qquad V_m^{(c_1)} \otimes V_m^{\star c_2} \otimes \cdots$$

čine vektori oblika

$$(3)\qquad e_{i_{11}} \otimes e_{i_{12}} \otimes \cdots \otimes e_{i_1 c_1} \otimes e^{i_{21}} \otimes e^{i_{22}} \otimes \cdots \otimes e^{i_{2c_2}} \otimes e_{i_{31}} \cdots$$

$$\stackrel{\text{def}}{=\!=} e^{i_{21}\, i_{22} \ldots i_{2c_2}\, i_{41} \ldots i_{4c_4} \ldots}_{i_{11}\, i_{12} \ldots i_{1c_1}\, i_{31} \ldots i_{3c_3} \ldots}$$

pri čemu svako i_{jk} za dato (j, k) prolazi skupom $\{1, 2, \ldots, m\}$; zato je

$$(4)\qquad t = t^{i_{11}\, i_{12} \ldots i_{1c_1}\, i_{31} \ldots i_{3c_3} \ldots}_{i_{21}\, i_{22} \ldots i_{2c_2}\, i_{41} \ldots i_{4c_4} \ldots}\; e^{i_{21} \ldots i_{2c_2}\, i_{41} \ldots i_{4c_4} \ldots}_{i_{11}\, i_{12} \ldots i_{1c_1}\, i_{31} \ldots i_{3c_3} \ldots}$$

Kako je tenzor (3) određena r-ada, to obrazac (4) kazuje da je na snazi

2.3.2. Teorem. Svaki afinor razreda r nad prostorom V_m je suma od r-ada na broju $\leq m^r$ (isp. § 2.2.5).

Obrazac (4) vrijedi pri svakoj koordinatnoj bazi. Posebno, promjenom (B) $e_{i'} = a^i_{i'} e_i$ koordinantne baze u V_m dobiju se određene baze u faktorima od prostora (2) kao i u samom prostoru (2); za tu bazu imamo za t izraz (4') koji iz (4) izlazi tako da svakom indeksu i dodamo apostrof. Isto tako neka (3') znači relaciju koja iz (3) izlazi pišući svuda i' umjesto i.

No, prema § 1.6.1 imamo

$$e_{i'_{11}} = a^{i_{11}}_{i'_{11}} e_{i_{11}}, \ldots, \quad e^{i_{21}} = a^{i_{21}}_{i'_{21}} e^{i'_{21}}, \ldots$$

Tu se svako i_A i svako i'_B mijenjaju nezavisno u skupu $\{1, 2, \ldots, m\}$. Stavimo li te izraze u (4') to s obzirom na (4) izlazi

$$t^{\ldots\alpha\ldots}_{\ldots\beta\ldots}\, e^{\ldots\beta\ldots}_{\ldots\alpha\ldots} = t = t^{\ldots\alpha'\ldots}_{\ldots\beta'\ldots}\, e^{\ldots\beta'\ldots}_{\ldots\alpha'\ldots} = \ldots t^{\ldots\alpha'\ldots}_{\ldots\beta'\ldots}\, a^{\alpha}_{\alpha'} \ldots (a^{-1})^{\beta'}_{\beta} \ldots e^{\ldots\beta\ldots}_{\ldots\alpha\ldots}$$

Dakle izlazi

→ **2.3.3. Teorem**

$$t^{\ldots\alpha\ldots}_{\ldots\beta\ldots} = (a^{-1})^{\beta'}_{\beta} \ldots a^{\alpha}_{\alpha'} \ldots t^{\ldots\alpha'\ldots}_{\ldots\beta'\ldots}, \qquad \textit{odnosno}$$

$$t^{\ldots\alpha'\ldots}_{\ldots\beta'\ldots} = a^{\beta}_{\beta'} \ldots (a^{-1})^{\alpha'}_{\alpha} \ldots t^{\ldots\alpha\ldots}_{\ldots\beta\ldots}$$

Riječima: promjenom baze obrascem **(B)** *svakoj koordinati* $t^{\ldots\alpha\ldots}_{\ldots\beta\ldots}$ *tenzora* t *u staroj bazi odgovara koordinata* $t^{\ldots\alpha'\ldots}_{\ldots\beta'\ldots}$ *istog tenzora* t *u novoj bazi (svakom kontravarijantnom indeksu kao i svakom kovarijantnom indeksu pripiše se apostrof!); vrijedi*

$$t^{\ldots\alpha'\ldots}_{\ldots\beta'\ldots} = \ldots a^{\beta}_{\beta'} \ldots (a^{-1})^{\alpha'}_{\alpha} \ldots t^{\ldots\alpha\ldots}_{\ldots\beta\ldots};$$

tj. svakom kontravarijantnom indeksu α *odgovara pred* t *faktor* $(a^{-1})^{\alpha'}_{\alpha}$ *(kako bi se po tome indeksu moglo sumirati od* **1** *do* m*); svakom kovarijantnom indeksu* β *u koordinati odgovara ispred koordinate faktor* $a^{\beta'}_{\beta}$ *(kako bi se i po* β *moglo sumirati od* **1** *do* m*).*

Čak bi se umjesto a^{-1} moglo pisati naprosto a uz dogovor da za matricu $a = [a^i_{j'}]$ vrijedi $a^{-1} = [a^{j'}_i]$.

2.3.4. Držat ćemo se dogovora da za matricu $a=[a^i_{j'}]$ imamo

$$a=[a^i_{j'}] \Leftrightarrow a^{-1}=[a^{j'}_i] \quad \text{(apostrof je na gornjem indeksu).}$$

Premještanje apostrofa sa kovarijantnog donjeg (kontravarijantnog gornjeg) indeksa u oznaci matrice na kontravarijantni gornji (kovarijantni donji) indeks znači prelaz od matrice na inverznu matricu; apostrof uz kontravarijantni indeks označuje inverznu matricu.

Drugim riječima, $[a^i_{j'}]$ je matrica kojoj inverzna glasi $[a^{j'}_i]$.

Zato pri promjeni $e_{j'}=a^i_{j'}e_i$ baze koordinate v^i vektora v postaju

$$v^i=a^i_{j'}v^{j'}, \quad \text{odnosno} \quad v^{i'}=a^{i'}_j v^j.$$

Isto tako

$$v^{i_1}w^{i_2}=a^{i_1}_{i'_1}a^{i_2}_{i'_2}v^{i'_1}w^{i'_2}, \quad v^{i_1}w_{i_2}=a^{i_1}_{i'_1}v^{i'_1}a^{i'_2}_{i_2}w_{i'_3} \quad \text{itd.}$$

Tako vidimo da je uvedena simbolika vrlo prikladna za pregledno prikazivanje afinih tenzora.

Vrijedi i obrat teorema 2.3.3; radi lakšeg pisanja, iskažimo ga za specijalan slučaj $r=3$, $p=2$, $q=1$.

2.3.5. Teorem. *Imamo li pri svakoj uređenoj dvojki* (e,e') *bazâ* (e_i), $(e_{i'})$ *prostora* V *veličine* $t^{\alpha\beta}_{\gamma}$, *odnosno* $t^{\alpha'\beta'}_{\gamma'}$ *za koje vrijedi*

$$t^{\alpha'\beta'}_{\gamma'}=a^{\alpha'}_{\alpha}a^{\beta'}_{\beta}a^{\gamma}_{\gamma'}t^{\alpha\beta}_{\gamma}, \tag{1}$$

tada je

$$t=t^{\alpha\beta}_{\gamma}e^{\gamma}_{\alpha\beta}=t^{\alpha'\beta'}_{\gamma'}e^{\gamma'}_{\alpha'\beta'} \tag{2}$$

tenzor nad V *i to razreda* $(2+1)$ (*kontravarijantnosti*: 2, *kovarijantnosti*: 1).

Dokaz: Formalno, promatrajmo veličinu

$$t=t^{\alpha\beta}_{\gamma}e^{\gamma}_{\alpha\beta}; \tag{3}$$

tada je formalno t član od $V\otimes V\otimes V^*$ ukoliko se naknadno vidi da se prikaz od t uz bazu e' vlada prema pravilima o prikazima vektora pri raznim bazama. No, prelaskom na bazu e' prostora V, prelazi (3) u $t^{\alpha'\beta'}_{\gamma'}e^{\gamma'}_{\alpha'\beta'}$ dakle prema uslovu (1) prelazi (3) u (1) pa se t zaista pri prelazu $e\to e'$ vlada kao vektor i kao član od $V\otimes V\otimes V^*$.

Time je teorem 2.3.5 dokazan.

Teoreme 2.3.3, 2.3.5 možemo izreći kao

$\longrightarrow$ **2.4.** ***Kriterij o tenzorima. Zadan je prirodni broj*** r ***te redni brojevi*** p, q ***za koje je*** $p+q=r$; ***zadani su: vektorski prostor*** $V=V_m$ ***nad tijelom*** K, ***baza*** (e_i) ***u*** V ***te preslikavanje***

$$(i_1, i_2, \ldots, i_p; j_1 j_2 \ldots j_q)\to t^{i_1\ldots i_p}_{j_1\ldots j_q}$$

kojim se svakom r-nizu brojeva iz $\{1,2,\ldots,m\}$, $m=\dim V$, ***pridjeljuje određeni član iz*** K; ***da vrijednosti*** $t^{i_1\ldots i_p}_{j_1\ldots j_q}$ ***budu koordinate tenzora nad*** V ***razreda*** $(p+q)$

nužno je i dovoljno da za svaku drugu bazu ($e_{i'}$) prostora V odgovarajuće vrijednosti $t^{i'_1\ldots i'_p}_{j'_1\ldots j'_q}$ zadovoljavaju

$$(*)\qquad t^{i'_1\ldots i'_p}_{j'_1\ldots j'_q} = a^{i'_1}_{i_1}\ldots a^{i'_p}_{i_p}\, a^{j_1}_{j'_1}\ldots a^{j_p}_{j'_p}\, t^{i_1\ldots i_p}_{j_1\ldots j_q}.$$

2.5. Euklidski ili Descartesovi tenzori. To su tenzori (afinori) nad prostorima nad tijelom R realnih brojeva, pri tom su prostori-faktori kao i tenzorski produkt tih prostora snabdjeveni ortonormiranom bazom vektora. Prema tome, vladanje koordinata *euklidskih tenzora* ispituje se samo prema *ortogonalnim matricama* (pri ispitivanju afinora, u igri je potpuna linearna grupa transformacija a sastavljena je od svih regularnih kvadratnih matrica dane duljine).

2.5.1. *Kontravarijantnost i kovarijantnost prema deriviranju*

U slučaju euklidskih tenzora možemo kontravarijantnost i kovarijantnost izraziti pomoću deriviranja. Radi li se o prostoru R^m od m dimenzija, tada u bazi (e_i) tačke iz R^m neka nose oznaku $(x^i)=(x^1x^2\ldots x^m)$, a u bazi ($e_{i'}$) oznaku $(x^{i'})$; tada postoje veze

$$(1)\qquad x^i = x^i(x^{1'},\ldots,x^{m'})$$

kao i obrnute veze

$$(2)\qquad x^{i'} = x^{i'}(x^1,\ldots,x^m);$$

te su veze linearne pa ih možemo pisati

$$(3)\qquad x^i = a^i_{j'}x^{j'}\qquad \text{što zbog}$$

$$(4)\qquad a^i_{j'} = \frac{\partial x^i}{\partial x^{j'}}\qquad \text{postaje}$$

$$(5)\qquad x^i = \frac{\partial x^i}{\partial x^{j'}}x^{j'} \equiv \left(\sum_{j'=1}^{m}\frac{\partial x^i}{\partial x^{j'}}x^{j'}\right)$$

(*derivira se po novim varijablama*).

Pri tom se služimo konvencijom da indeks pod znakom ∂ nazivnika označuje *donji* indeks (pa makar on formalno bio pisan kao eksponent).

2.5.2. Isto tako je $x^{i'}=(a^{-1})^{i'}_i x^i$ odakle $(a^{-1})^{i'}_i = \dfrac{\partial x^{i'}}{\partial x^i}$ odnosno

$$x^{i'} = \frac{\partial x^{i'}}{\partial x^i}x^i \qquad (\textit{derivira se po starim varijablama}).$$

Drugim riječima, svaki koeficijent kovarijantne matrice je derivat stare varijable po novoj varijabli; svaki koeficijent nekovarijantne matrice je derivat nove varijable po staroj varijabli. Na taj način, deriviranje po novim varijablama ima kovarijantni karakter a deriviranje po starim varijablama ima kontravarijantni karakter.

2.5.3. Na osnovu obrasca

$$a^i_{j'} = \frac{\partial x^i}{\partial x^{j'}}, \quad (a^{-1})^{j'}_i = \frac{\partial x^{i'}}{\partial x^i}$$

transformacione formule (*) iz § 2.4 postaju

$$(**) \qquad t^{i'_1 i'_2 \dots i'_p}_{j'_1 j'_2 \dots j'_q} = \frac{\partial x^{i'_1}}{\partial x^{i_1}} \dots \frac{\partial x^{i'_p}}{\partial x^{i_p}} \frac{\partial x^{j_1}}{\partial x^{j'_1}} \dots \frac{\partial x^{j_p}}{\partial x^{j'_p}} t^{i_1 i_2 \dots i_p}_{j_1 j_2 \dots j_q}.$$

2.5.4. Međutim transformacione formule (**) mogu se promatrati ne samo za linearne veze (1) i (2) nego za bilo kakve veze (1), (2) uz uslov da postoje napisani parcijalni izvodi $\frac{\partial x^i}{\partial x^{i'}}$, $\frac{\partial x^{i'}}{\partial x^i}$ te da pripadne funkcijske determinante $\det\left[\frac{\partial x^i}{\partial x^{i'}}\right]$, $\det\left[\frac{\partial x^{i'}}{\partial x^i}\right]$ ne budu nigdje 0.

Uz te pretpostavke veličine (iz teorema 2.4):

$$t^{i_1 \dots i_p}_{j_1 \dots j_q} \quad \text{odnosno} \quad t^{i'_1 \dots i'_p}_{j'_1 \dots j'_q}$$

pri koordinatnom sistemu bez crtica i sa crticama ne moraju biti brojevi nego su općenito funkcije mjesta ili položaja

$$(x^1 \dots x^m), \quad \text{odnosno} \quad (x^{1'} \dots x^{m'}).$$

2.5.5. Tako npr. ako je riječ o prostoru R^3 i o funkciji

$$f\,(x^1\; x^2\; x^3), \quad \text{odnosno} \quad f\,(x^{1'},\, x^{2'},\, x^{3'}) \text{ u } R^3,$$

tada imamo funkcije mjesta

$$t_i \overset{\text{def}}{=} \frac{\partial f}{\partial x_i}, \quad t_{i'} \overset{\text{def}}{=} \frac{\partial f}{\partial x^{i'}}.$$

Zbog $\frac{\partial f}{\partial x^{i'}} = \frac{\partial f}{\partial x^i} \frac{\partial x^i}{\partial x^{i'}} = t^i \frac{\partial x^i}{\partial x^{i'}}$ izlazi da je $t^{i'} = \frac{\partial x^i}{\partial x^{i'}} t^i$.

Prema tome u danoj tački prostora R^3 (odnosno R^m) funkcije t_i su tenzori razreda $(0+1)$ tako da možemo govoriti o *tenzorskom polju* u smislu da svakoj tački neke oblasti iz R^3 odgovara određen tenzor.

Na osnovu gornjih razmatranja postavlja se ova

2.6. Definicija tenzorskog polja u prostoru R^m. Neka su

$$t^{i_1 \dots i_p}_{j_1 \dots j_q}, \quad \text{odnosno} \quad t^{i'_1 \dots i'_p}_{j'_1 \dots j'_q}$$

funkcije tačke $T=(x^i)$, odnosno (x') u nekoj oblasti O prostora R^m; te su funkcije koordinate tenzora razreda $(p+q)$ u svakoj tački promatrane oblasti onda i samo onda ukoliko za svaki koordinatni sistem S, odnosno S' vrijedi

(**) iz § 2.5.3; ukoliko (**) vrijedi, onda je svakoj tački T promatrane oblasti O pridružen određen tenzor; govori se o *tenzorskom polju nad oblasti O.*

Prethodna definicija je vrlo efikasna u izučavanju euklidskih tenzorskih polja. Specijalni slučaj tenzorskih polja su vektorska polja.

3. RAČUNANJE S TENZORIMA

3.0. Treba imati na umu da su tenzori posebni vektori (naime: elementi tenzorskog produkta vektorskih prostora); zato se izjednačavanje tenzora, zbrajanje tenzora i množenje tenzora skalarom definira upravo kao i kad je riječ o vektorima.

No, konkretno, najčešće izučavamo tenzore preko koordinata tenzora; zato je potrebno odnose i računanja s tenzorima provoditi i pomoću koordinata tenzora a u zavisnosti s odabranom vektorskom bazom prostora odakle su tenzori uzeti kao članovi.

Na taj način, svaki tenzor ima oblik određene linearne sume kojoj su koeficijenti koordinate tenzora (isp. § 2.2.1. (4)).

3.1. Pri odabranoj bazi $(e(\rho)_i)$ u prostoru $V(\rho)$ određena je i baza e samog prostora W iz § 2.2.2. (5) kao i koordinate svakog tenzora $t \in W$ i to prema sadržini teorema 2.2.4.

Izabere li se u $V(\rho)$ neka druga baza $(e(\rho)_{i'_\rho})$ vezama

(1) $$e(\rho)_{i'_\rho} = a(\rho)^{j_\rho}_{i'_\rho}\, e(\rho)_{j_\rho}$$

tada tom istom tenzoru t odgovaraju, u novoj bazi, koordinate prema identitetu

(2) $$t^{i_1 i_2 \dots i_r}(e(1)_{i_1} \otimes \dots \otimes e(r)_{i_r}) = (t=)\, t^{i'_1 \dots i'_r}\, e(1)_{i'_1} \otimes \dots \otimes e(r)_{i'_r}.$$

Veze između starih i novih koordinata jesu ove:

(3) $$t^{i_1 \dots i_r} = a(1)^{i_1}_{i'_1}\, a(2)^{i_2}_{i'_2} \dots a(r)^{i_r}_{i'_r}\, t^{i'_1} \dots t^{i'_r}.$$

Te se veze dobiju uvrštavajući izraze (1) u (2) i izjednačavajući koeficijente od $$e(1)_{i_1} \otimes \dots \otimes e(r)_{i_r}.$$

3.2. Jednakost tenzora. Pri danoj bazi, tenzori su jednaki onda i samo onda ako su odgovarajuće koordinate jednog i drugog tenzora međusobno jednake.

Odmah se vidi ovo: ako je svaka koordinata tenzora t jednaka odgovarajućoj koordinati tenzora u pri *nekoj* bazi, vrijedit će ista stvar pri *svakoj* koordinatnoj bazi.

3.2.1. Specijalno, dva afinora jednaka su onda i samo onda ako su oba istog razreda r, oba istog reda kontravarijantnosti, oba istog reda kovarijantnosti i oba imaju iste odgovarajuće koordinate.

3.3. Zbrajanje tenzora.

Suma $t+u$ tenzora t i tenzora u definira se onda i samo onda ako su t, u u jednom te istom vektorskom prostoru; tada se svaka koordinata od $t+u$ definira tako da se zbroji odgovarajuća koordinata od t i odgovarajuća koordinata od u.

Zato npr. tenzor t_{ij} i tenzor u^{ij} ne mogu se zbrajati; naprotiv, tenzor $t=t_k^{ij}$ i tenzor $u=u_k^{ij}$ mogu se zbrajati i to koordinatno:

$$t_k^{ij}+u_k^{ij}=(t+u)_k^{ij}.$$

3.4. *Produkt skalara* λ *i tenzora* t uvijek se definira kao onaj tenzor kojemu je svaka koordinata produkt od λ i odgovarajuće koordinate od t.

3.5. Produkt ili umnožak dvojke tenzora. Posebno se ističe definicija produkta uređene dvojke tenzora (isp. također § 4.8).

3.5.1. Ako je zadan tenzor $t\,(1)$ s koordinatama $t\,(1)_{J_1}^{I_1}$ i tenzor $t\,(2)$ s koordinatama $t\,(2)_{J_2}^{I_2}$, tada se (*tenzorski*) *produkt* od $t\,(1)$ i $t\,(2)$ definira pomoću koordinata

$$t_{J_1 J_2}^{I_1 I_2} \overset{\text{def}}{=} t\,(1)_{J_1}^{I_1}\; t\,(2)_{J_2}^{I_2}; \quad \text{piše se } t=t\,(1)\otimes t\,(2).$$

Pri tom $I_1\, I_2$ znači niz koji počinje sa nizom I_1 a preostatak je upravo niz I_2. Pri tom se suponira da su nizovi I_1, I_2, J_1, J_2 bez ikojeg zajedničkog člana; ako taj uslov nije ispunjen, promijenit ćemo oznaku tako da ga zadovoljimo; npr. produkt od t^i, t_{ij} jest $=t^i\otimes t_{kj}=t^i{}_{kj}$ (a nije t^i_{ij}).

3.5.2. Analogno se definira tenzorski produkt

$$t\,(1)\otimes t\,(2)\otimes\ldots\otimes t\,(n)$$

od bilo kojeg n-članog niza $t\,(1)$, $t\,(2), \ldots, t\,(n)$ tenzora (n je prirodan broj); taj tenzorski produkt postoji bez obzira na razred, red kontravarijantnosti, red kovarijantnosti faktora; jedino, svi faktori moraju biti u vezi s vektorskim prostorima nad jednim te istim tijelom K.

3.5.3. Neposredno se provjerava da je tenzorsko množenje tenzora distributivno prema zbrajanju tenzora, i to distributivno s lijeve strane i s desne strane.

3.5.4. Neposredno se provjeri da za svaki skalar λ, svaki tenzor t i svaki tenzor u vrijedi

$$\lambda\,(t\otimes u)=(\lambda t)\otimes u=t\otimes(\lambda u).$$

3.6. Sažimanje (kontrakcija) ili podmlađivanje tenzora.

3.6.1. Ako tenzor ima bar jedan gornji i bar jedan donji indeks pa se uoči određen gornji indeks i određen donji indeks, tada se *podmlađivanje* ili *sažimanje* (*kontrakcija*) *tenzora po uočenoj dvojki indeksa* sastoji u tom da se ta dva uočena indeksa *izjednače* i onda izvede odgovarajuća sumacija po tom simbolu-indeksu; rezultat se naznačuje i brisanjem uočene dvojke indeksâ (rodno ime tenzora može se pri tom promijeniti, npr. umjesto t pišemo u).

Npr. radi li se o tenzoru t_k^{ij}, tada se sažimanje na paru (j, k) vrši ovako

$$t_k^{ij} \to t_j^{ij} = \sum_j t_j^{ij} = u^i;$$

dobije se nov tenzor razreda za 2 manji nego što je bio razred tenzora na početku.

⟶ **3.6.2. Teorem.** ***Rezultat sažimanja tenzora razreda $(p+q)$ pri $p, q > 0$ je tenzor razreda $((p-1)+(q-1))$.***

Dokažimo npr. da iz tenzora t_{ln}^{ijk} sažimanjem po $k = n$ nastaje tenzor

(1) $$u_l^{ij} = t_{lk}^{ijk}.$$

Po osnovnom svojstvu o transformaciji tenzora t (teorem 2.4) dovoljno je pokazati obrazac

(2) $$u_{l'}^{i'j'} = a_i^{i'} a_j^{j'} a_{l'}^{l} u_l^{ij}.$$

No, za dani tenzor t po istom teoremu imamo

$$t_{l'n'}^{i'j'k'} = a_i^{i'} a_j^{j'} a_\alpha^{k'} a_{l'}^{l} a_{n'}^{\beta} t_{l\beta}^{ij\alpha} = a_i^{i'} a_j^{j'} a_{l'}^{l} \left(a_\alpha^{k'} a_{n'}^{\beta}\right) t_{l\beta}^{ij\alpha}.$$

Ako provedemo sažimanje po $\alpha = \beta$ izlazi zbog

$$a_\alpha^{k'} a_{n'}^{\alpha} = \delta_{n'}^{k'}:$$

$$t_{l'k'}^{i'j'k'} = a_i^{i'} a_j^{j'} a_{l'}^{l} \delta_{n'}^{k'} u_l^{ij};$$

posebno, pri $k' = n'$ izlazi dalje

(3) $$t_{l'k'}^{i'j'k'} = a_i^{i'} a_j^{j'} a_{l'}^{l} u_l^{ij}; \text{ zbog } t_{l'k'}^{i'j'k'} = u_{l'}^{i'j'} \text{ (isp. identitet (1))}$$

znači (3) da zaista vrijedi (2).

3.6.3. *Uzastopno sažimanje.* Izvede li se na rezultatu sažimanja tenzora opet sažimanje i to ponovi dok se ne iscrpu svi kovarijantni ili svi kontravarijantni indeksi dobit će se najzad skalar ili vektor.

Tako npr. iz tenzora $t_{j_1 j_2 j_3 j_4}^{i_1 i_2 i_3}$ imamo npr. ova sažimanja:

$$t_{j_1 j_2 j_3 j_4}^{i_1 i_2 i_3} \xrightarrow{(i_1 = j_2)} t_{j_1 j_2 j_3 j_4}^{j_2 i_2 i_3} = u_{j_1 j_3 j_4}^{i_2 i_3} \xrightarrow{(i_2 = j_1)} t_{j_1 j_3 j_4}^{j_1 i_3} = v_{j_3 j_4}^{i_3} \to t_{i_3 j_4}^{i_3} = v_{j_4}.$$

Rezultat je kovarijantan vektor.

3.6.4. Sažimanje tenzora t_j^i odgovara tragu matrice $[t_j^i]$.

3.6.5. *Sažimanje kombinirano s tenzorskim množenjem.* Često se provodi sažimanje tenzorskog produkta. Tako npr. pri množenju matrice

$$[a_j^i] \text{ matricom } [b_k^j] \text{ izlazi } a_j^i b_k^j = a_{jk}^{ij} = c_k^i.$$

Skalarni produkt dvaju vektora je sažimanje tenzorskog produkta tih vektora.

3.6.6. *Dizanje donjeg indeksa.*

Pomnožimo li kovarijantni vektor v_i tenzorom g^{jk} izlazi tenzor t s koordinatama $t_i^{jk} = v_i g^{jk}$ pa sažimanje po $i=j$ daje

$$v_i g^{ik} \to t_i^{ik} = u^k = v,$$

dobije se kontravarijantni vektor; formalno:

$$v_i \to u^k \text{ (ili čak } v_i \to v^i);$$

dakle je donji indeks postao gornjim indeksom.

Isto se tako množenjem i sažimanjem može iz kontravarijantna vektora dobiti kovarijantan vektor; radi se po obrascu:

$$v^i g_{jk} \to v^i g_{ik} = t_{ik}^i = v_k.$$

Ta operacija formalno izgleda kao da smo indeks i spustili, tj.

$$v^i \to v_k \text{ (ili čak } v^i \to v_i).$$

Spustimo li u t_{klm}^{ij} indeks i izlazi t_{klmi}^{j}; spustimo li i indeks j, izlazi t_{klmij}. Ta se operacija može provesti prethodnim množenjem tenzorom $g_{i_1 i_2 i_3 i_4}$ i onda provesti sažimanje:

$$t_{klm}^{ij} g_{i_1 i_2 i_3 i_4} \to t_{klmi_1 i_2 i_3 j}^{ij} = u_{klmi_1 i_2 i_3}^{i} \overset{(i=i_3)}{\longrightarrow} v_{klm i_1 i_2}.$$

3.6.7. Na taj način vidimo kako je dovoljno izučiti tenzore zadana tipa npr. tenzore s gornjim indeksima jer se donji indeksi mogu podignuti i tako dobiti odgovarajuće čisto kontravarijantne tenzore.

4. PRIMJERI TENZORA. JOŠ DVA KRITERIJA O TENZORIMA

Prethodna razmatranja pokazuju kako se na čest način nailazi na tenzore. Zato je od važnosti navesti i još koji primjer tenzora (posebno nad euklidskim prostorima R^m) kao i uočiti još koji kriterij na osnovu kojega se prepoznavaju tenzori od netenzora. Imajmo na umu sliku da je tenzor razreda r nad prostorom R^m nešto što zavisi od svih r nizova brojeva $\{1, 2. \ldots, m\}$ i od skupa svih koordinatnih baza prostora R^m (odnosno skupa svih regularnih matrica širine m).

4.1. Svaki tročlani stupac t^j $(j=1, 2, 3)$ pisan kao $\begin{bmatrix} t^1 \\ t^2 \\ t^3 \end{bmatrix}$ jest tenzor razreda 1 i to kontravarijantnosti 1 uz uslov da promjenom $e_{j'} = a_{j'}^{i} e_i$ baze imamo novi stupac $\begin{bmatrix} t^{1'} \\ t^{2'} \\ t^{3'} \end{bmatrix}$ za koji je $t^j = a_{j'}^{j} t^{j'}$, odnosno $t^{j'} = a_j^{j'} t^j$, tj.

$$\begin{bmatrix} t^1 \\ t^2 \\ t^3 \end{bmatrix} = a \begin{bmatrix} t^{1'} \\ t^{2'} \\ t^{3'} \end{bmatrix} \text{ odnosno } \begin{bmatrix} t^{1'} \\ t^{2'} \\ t^{3'} \end{bmatrix} = a^{-1} \begin{bmatrix} t^1 \\ t^2 \\ t^3 \end{bmatrix}.$$

Prema tome uz takav dogovor matrice-stupci jesu kontravarijantni tenzori (vektori) razreda 1. To izlazi posebno iz teorema 2.4.

4.2. Uz danu koordinatnu bazu prostora R^3, svaki tročlani redić $t_i (i = 1, 2, 3)$ pisan kao $[t_1, t_2, t_3]$ jest tenzor razreda 1 i to kovarijantnosti 1 uz dogovor da promjenom (B) baze taj isti tenzor glasi $[t_{1'}, t_{2'}, t_{3'}]$ pri čemu je $t_j = a_j^{j'} t_{j'}$, odnosno $t_{j'} = a_{j'}^{j} t_j$ tj. $[t_1 t_2 t_3] = [t_{1'} t_{2'} t_{3'}] a^{-1}$, odnosno $[t_{1'} t_{2'}, t_{3'}] = [t_1 t_2 t_3] a$.

4.3. *Matrica* $[t_{ij}] = t$ *pri danoj vektorskoj bazi.* Ona dolazi u sklopu $t_{ij} v^i w^j$, tj. kao matrica dvaput linearne forme komponenata kontravarijantnih vektora v, w.

Nakon promjene (B) koordinatne baze imamo

$$t_{ij} = a_i^{i'} a_j^{j'} t_{i'j'}, \quad \text{odnosno} \quad t_{i'j'} = a_{i'}^{i} a_{j'}^{j} t_{ij}.$$

Dakle je t_{ij} tenzor razreda 2 i to razreda 2 kovarijantnosti (v. § 2.4). Drugim riječima, 2 put kovarijantni tenzor razreda 2 ostvaren je kao 2-put linearna forma komponenata kontravarijantnog vektora.

4.4. Analogni se iskazi dobiju za afinore t^{ij}, t_j^i razreda $(2 + 0)$, odnosno razreda $(1 + 1)$.

4.5. Na taj način, specijalno, uz zadanu vektorsku bazu R^3, svaka kvadratna realna matrica t duljine 3 može poslužiti kao podloga za definiciju tenzora razreda 2 nad prostorom R^3; treba samo odrediti dogovorno da se pri promjeni B koordinatne baze koordinate od t vladaju u skladu s oznakom t_{ij} ili t_j^i ili t^{ij}; sama matrica t bez dodatnog zahtjeva o tom transformiranju nije još tenzor; t kao matrica postoji bez obzira na bazu vektorskog prostora R^3, naprotiv, t kao vektor bitno je vezano za skup svih vektorskih baza prostora R^3, odnosno za potpunu linearnu grupu toga prostora.

S tim u vezi dokažimo:

⟶ **4.6.1. Teorem.** ***Ako je*** $t = t_{ij} e^{ij}$ ***tenzor, onda za svaku dvojku*** (v, w) ***kontravarijantnih vektora vrijedi***

$$t_{ij} v^i w^j = t_{i'j'} v^{i'} w^{j'} \tag{1}$$

pri svakoj promjeni koordinatne baze.

I obrnuto: imamo li u svakoj bazi sistem od n^2 ***skalara*** t_{ij}***, takvih da za svaki par vektora i za svake dvije baze e, e' vrijedi*** (1), ***onda su*** t_{ij} ***koordinate tenzora (kvocijentni kriterij; H. Weyl).***

Dokaz. Najprije,

$$t_{ij} v^i w^j = a_i^{k'} a_j^{l'} t_{k'l'} a_{m'}^{i} v^{m'} a_{n'}^{j} w^{n'} = (a_i^{k'} a_{m'}^{i})(a_j^{l'} a_{n'}^{j})\ t_{k'l'} v^{m'} w^{n'} = t_{i'j'} v^{i'} w^{j'}$$

jer su obe zagrade $= \delta_{m'}^{k'}$, odnosno $\delta_{n'}^{l'}$; dakle, ako su t_{ij} koordinate tenzora, onda (1) stoji.

Dokažimo i obrat. Polazimo od (1) pa je

$$t_{i'j'} v^{i'} w^{j'} = (t_{ij} v^i w^j =)\ t_{ij} a_{i'}^{i} v^{i'} a_{j'}^{j} w^{j'}.$$

Odatle radi proizvoljnosti vektorâ v, w dobivamo

$$t_{i'j'} = a_{i'}^{i} a_{j'}^{j} t_{ij}.$$

A to upravo znači da se komponente tenzora transformiraju na željeni način karakterističan za tenzor.

4.6.2. Analogan iskaz vrijedi i za funkcije t^{ij} i t_j^i a u vezi s uređenom dvojkom $(v^\star, w^\star)$ odnosno $(v^\star, w)$; pri tom, zvjezdicom označujemo da je riječ o kovarijantnom vektoru (odnosno o kovarijantnim koordinatama vektora).

Kao što smo dokazali teorem 4.6.1. tako se dokazuje i

$\longrightarrow$ **4.6.3.** Teorem (*kriterij pomoću invarijantnosti*). *Da funkcija* $(i_1, i_2, \ldots, i_r) \to t^{i_1 i_2 \ldots i_r}$ *bude r-puta kontravarijantan tenzor nad prostorom* R^m *nužno je i dovoljno da za svaki r-niz* $v(1)_{i_1}, v(2)_{i_2}, \ldots, v(r)_{i_r}$ *kovarijantnih vektora i za svaku dvojku* (e, e') *koordinatnih baza prostora* R^m *vrijedi*

$$t^{i_1 \ldots i_r} v_{i_1} v_{i_2} \ldots v_{i_r} = t^{i'_1 \ldots i'_r} v(1)_{i'_1} \ldots v(r)_{i'_r} .$$

Općenitije isto se tako dokazuje

4.6.4. Teorem. *Neka je r prirodni broj; neka su p, q redni brojevi za koje je* $p+q=r$; *ako svakoj uređenoj dvojki* $((i_1 \ldots i_p); (j_1 \ldots j_q))$ *pridružimo*

$$\textit{skalar} \quad t^{i_1 \ldots i_p}_{j_1 \ldots j_q}, \quad \textit{tada će} \quad t = t^{i_1 \ldots i_p}_{j_1 \ldots j_q} e^{j_1 \ldots j_q}_{i_1 \ldots i_p}$$

biti tenzor razreda $(p+q)$ *onda i samo onda ako pri svakoj promjeni* (B) *koordinatne baze, svaku p-torku kovarijantnih vektorâ* $v(1), \ldots, v(p)$ *i svaku q-torku kontravarijantnih vektora* $w(1), \ldots, w(q)$ *vrijedi*

$$t^{i_1 \ldots i_p}_{j_1 \ldots j_q} v(1)_{i_1} \ldots v(p)_{i_p} w(1)^{j_1} \ldots w(q)^{j_q} =$$

$$= t^{i'_1 \ldots i'_p}_{j'_1 \ldots j'_q} v(1)_{i'_1} \ldots v_{i'_p} w(1)^{j'_1} \ldots w(q)^{j'_q} .$$

4.6.5. Teorem. *Niz od* m^{p+q} *veličinâ* $t^{i_1 \ldots i_p}_{j_1 \ldots j_q}$ *(oznaka je kao u t.* 4.6.4) *predstavlja koordinate tenzora razreda* $(p+q)$ *onda i samo onda ako je ispunjen jedan od ova dva uslova:*

(0) *Za svaki p-član niz*

$$w(1) = (w(1)_{i_1}), \; w(2) = (w(2)_{i_2}), \; w(p) = (w(p)_{i_p})$$

kovarijantnih vektora nad R^m, *veličine*

$$(1) \qquad t^{i_1 \ldots i_p}_{j_1 \ldots j_q} w(1)_{i_1} \ldots w(p)_{i_p}$$

su koordinate kovarijantna vektora razreda q nad prostorom R^m.

(00) *Za svaki q-član niz*

$$v(1) = (v(1)^{j_1}), \ldots, v(q) = (v(q)^{j_q})$$

kontravarijantnih vektora razreda r nad prostorom R^m *veličine*

$$t^{i_1 \dots i_p}_{j_1 \dots j_q} v(1)^{j_1} \dots v(q)^{j_q}$$

su koordinate kontravarijantnog vektora razreda p nad R^m.

Dokažimo npr. slučaj (0). Nužnost uslova izlazi iz teorema 3.6.2. o sažimanju primjenjujući taj teorem uzastopno p puta na indeks i_1 pa na indeks i_2 itd. do i_p.

Dokažimo i dovoljnost uslova (0). Naime, ako su (1) koordinate kovarijantnih vektora $v(1) = (v(1)^{j_1}), \dots, v(q) = (v(q)^{j_q}$ suma

$$t^{i_1 \dots i_p}_{j_1 \dots j_q} w(1)_{i_1} \dots w(p)_{i_p} v(1)^{j_1} \dots v(q)^{j_q}$$

je nezavisna od koordinatne baze (isp. t. 4.6.4); po istom teoremu to upravo znači da veličine $t^{i_1 \dots i_p}_{j_1 \dots j_q}$ predstavljaju upravo m^{p+q} koordinata tenzora t razreda $(p+q)$ nad prostorom R^m.

U vezi sa sažimanjem i množenjem tenzora dokažimo ovaj

4.7. K r i t e r i j o t e n z o r i m a. *Neka je* $\rho \in \{1, 2, \dots, r\}$ *i neka je* $(e(\rho)_{i_\rho})$ *baza u zadanu prostoru* $V(\rho)$ *nad* K; *neka je* $(i_1, i_2, \dots, i_r) \to t^{i_1 \dots i_r}$ *funkcija koja svakom nizu* $(i_1, \dots, i_r)$ *pridjeljuje skalar* $t^{i_1 \dots i_r}$ *pri tom* $i_\rho \in \{1, 2, \dots, \dim V(\rho)\}$; *tada će* $t = t^{i_1 \dots i_r} e_{i_1 \dots i_r}$ *biti tenzor onda i samo onda ako za svaki tenzor u razreda* $(0+2)$ *funkcija* $(i_1 i_2 \dots i_r) \to t^{i_1 i_2 \dots i_r} u_{i_1 i_2}$ *predstavlja koordinate određena tenzora razreda r-2.*

Uslov teorema je nuždan; to izlazi iz teorema 3.6.2. Dokažimo da je uslov teorema i dovoljan. Odaberimo specijalno tenzor u tako da bude $u_{i_1 i_2} = x_{i_1} y_{i_2}$ (dakle je $u = x \otimes y$); tada imamo tenzorske koordinate

$$u^{i_3 \dots i_r} = t^{i_1 i_2 \dots i_r} x_{i_1} y_{i_2} \text{ razreda } ((r-2)+0). \tag{1}$$

To znači (isp. § 2.4) da pri proizvoljnoj promjeni baze vrijedi

$$u^{i'_3 \dots u'_r} = a^{i'_3}_{i_3} \dots a^{i'_r}_{i_r} u^{i_3 \dots u_r} = a^{i'_3}_{i_3} \dots a^{i'_r}_{i_r} t^{i_1 i_2 \dots i_r} x_{i_1} y_{i_2}.$$

Odatle prema (1)

$$t^{i'_1 i'_2 \dots i'_r} x_{i'_1} y_{i'_2} = a^{i'_3}_{i_3} \dots a^{i'_r}_{i_r} t^{i_1 i_2 \dots i_r} x_{i_1} y_{i_2}.$$

Zbog

$$x_{i'_1} = a^{i_1}_{i'_1} x_{i_1}, \; y_{i'_2} = a^{i_2}_{i'_2} y_{i_2}$$

izlazi iz prethodne jednakosti identitet

$$t^{i'_1 i'_2 i'_3 \dots i'_r} a^{i_1}_{i'_1} a^{i_2}_{i'_2} x_{i_1} y_{i_2} = a^{i'_3}_{i_3} \dots a^{i'_r}_{i_r} t^{i_1 i_2 \dots i_r} x_{i_1} y_{i_2}.$$

Odatle zbog proizvoljnosti skalara $x_{i_1} y_{i_2}$ izlazi odgovarajuća jednakost bez faktora x_{i_1}, y_{i_2}; dobivena jednakost je ekvivalentna s jednakosti

$$t^{i'_1 i'_2 \dots i'_r} = a_{i_1}^{i'_1} a_{i_2}^{i'_2} a_{i_3}^{i'_3} \dots a_{i_r}^{i'_r} t^{i_1 i_2 \dots i_r};$$

a to prema t. 2.4. upravo znači da je tenzor t razreda $(r+2+0)$ nad prostorom V.

Slično se dokaz izvodi za slučaj razreda $(0+s)$ pri $s \leq r$.

Time je kriterij 4.7. dokazan.

4.8. O ulozi koordinatne baze pri tenzorskom množenju.

4.8.1. U § 2 definirali smo tenzorski produkt $V_m \otimes V_n$ prostora V_m i prostora V_n na osnovi koordinatne baze (e_μ) u V_m i baze (f_ν) u V_n. Posebno, za svako $x \in V_m$ i svako $y \in V_n$ imamo rastav

$$x = x^\mu e_\mu, \quad y = y^\nu f_\nu$$

i pripadnu dijadu (isp. § 2.1.2)

(1) $$t \overset{\text{def}}{=} (x^\mu e_\mu) \otimes (y^\nu f_\nu) = x^\mu y^\nu (e_\mu \otimes f_\nu).$$

Tu je $\mu = 1, 2, \dots, m$; $\nu = 1, 2, \dots, n$.

Za neku drugu bazu $(e_{\mu'})$ prostora V_m i bazu $(f_{\nu'})$ prostora V_n imamo analogno

$$x = x^{\mu'} e_{\mu'}, \quad y = y^{\nu'} f_{\nu'} \qquad \text{te pripadnu dijadu}$$

(2) $$t' = (x^{\mu'} e_{\mu'}) \otimes (y^{\nu'} f_{\nu'}) = x^{\mu'} y^{\nu'} (e_{\mu'} \otimes f_{\nu'}).$$

4.8.2. Neka su baze (e_μ), $(e_{\mu'})$ vezane sa

(3) $$e_{\mu'} = a_{\mu'}^{\mu} e_\mu$$

(matrica je a), a baze (f_ν), $(f_{\nu'})$ neka su vezane pomoću

(4) $$f_{\nu'} = c_{\nu'}^{\nu} f_\nu \qquad \text{(matrica je } c).$$

Tada su

(5) $$(e_\mu \otimes f_\nu), \ (e_{\mu'} \otimes f_{\nu'}) \quad \text{baze prostora } V_m \otimes V_n \text{ pa je}$$

(6) $$(e_{\mu'} \otimes f_{\nu'}) = a_{\mu'}^{\mu} c_{\nu'}^{\nu} \ (e_\mu \otimes f_\nu).$$

Vezu među tim bazama prostora $V_m \otimes V_n$ obavlja matrica $d = a \otimes c$ (kroneckerski produkt matrice a i matrice c; isp. 33 § 4.2.1).

4.8.3. Prema osnovnom teoremu 23 § 3.3 o bazama i koordinatama znači to da za koordinate $t^{\mu\nu}$, $t^{\mu'\nu'}$ dijade t u bazama (5) vrijedi

(7) $$t^{\mu\nu} = a_{\mu'}^{\mu} c_{\nu'}^{\nu} t^{\mu'\nu'}.$$

Nađimo izraz t'. Imamo

$$t' = (\text{prema (2) i (6)}) = t^{\mu'\nu'} a^{\mu}_{\mu'} c^{\nu}_{\nu'} (e_{\mu} \otimes f_{\nu}) = (\text{prema (7)})$$

$$= t^{\mu\nu} (e_{\mu} \otimes f_{\nu}) = (\text{prema (1)}) = t. \qquad \text{Tj.}$$

(8) $$t' = t.$$

Prema tome imamo

4.8.4. Teorem. *Dijada određena vektorom $x \in V_m$ i vektorom $y \in V_n$ ne zavisi od odabrane koordinatne baze u prostoru V_m niti od odabrane koordinatne baze u prostoru V_n.*

Kako je, prema 2.1.2, svaki član iz $V_m \otimes V_n$ suma od $\leq mn$ dijada, zaključujemo da je i sam tenzorski produkt $V_m \otimes V_n$ kao i njegovi članovi— tenzori — nezavisan od upotrebljenih baza u faktorima V_m, V_n.

4.8.5. Slično se dokazuje da i *tenzorski produkt od bilo kojeg konačnog niza vektorskih prostora nad istim tijelom ne zavisi od upotrebljenih baza* (isp. § 2.2).

5. OSNOVNI METRIČKI TENZOR U EUKLIDSKOM PROSTORU R^m

5.0. Već smo se dobro upoznali s razlikovanjem kontravarijantnih vektora iz V i kovarijantnih vektora-članova iz V^*. Međutim, sada ćemo dokazati da to razlikovanje u euklidskim prostorima R^m ne postoji jer je R^m samo sebi dualno. Ipak je važno govoriti o *kontravarijantnim i kovarijantnim koordinatama* vektora iz R^m.

5.1. Teorem. *Svaki euklidski prostor E je sam sebi dualan, tj. $E = E^*$* (isp. 25 § 2; 25 § 3.2).

Dokaz. Nula-vektor $\vec{0}$ iz E i konstantu 0 iz E^* (isp. 34 § 1.5) dovedimo u međusobnu vezu.

Neka je $0 \neq a \in E$ proizvoljno; tada skalarno množenje

(1) $$x \in E \to (x, a)$$

je određena linearna forma u E, tj. određen član od E^*; na taj način svako $a \in R$ kao nosilac funkcije (1) je član od E^*.

Dokažimo da se tako dobije svako $L \in E^*$, tj. da vrijedi

5.1.2. Lema. *Svakom linearno-homogenom pridruživanju*

$$x \in E \to L(x) \in R$$

odgovara jedno jedino $l \in E$ za koje je

$$L(x) = (x, l);$$

pri tom je E euklidski prostor konačne dimenzije.

D o k a z l e m e. Neka je E_0 skup svih $x \in E$ za koje je $L(x)=0$; naravno, E_0 je potprostor od E. Ako je $E^0=E$, dovoljno je staviti $l=\vec{0}$. Ako je $E_0 \neq E$, neka je a proizvoljan član iz E koji je $\perp E_0$, tj. za koji je

$$(2) \qquad (x_0, a)=0 \quad (x_0 \in E_0).$$

Naravno, a postoji. Stavljajući

$$(3) \qquad l=\frac{L(a)}{(a, a)}a,$$

dokažimo da je

$$(4) \qquad l(x)=(x, l) \quad (x \in E).$$

Naime, prema (2) vrijedi (4) za svako $x \in E_0$; nadalje (4) vrijedi i za $x=a$, jer

$$(a, l)=\left(a, \frac{L(a)}{(a, a)}a\right)=(\text{prema } 25 \ \S\ 2.1.\ S_1)=\left(\frac{L(a)}{(a, a)}a,\ a\right)$$

$$=(\text{prema } 25 \ \S\ 2.1.\ S_2)=\frac{L(a)}{(a, a)}(a, a)=L(a), \text{ jer } a \neq 0 \Rightarrow (a, a) \neq 0.$$

No, za svako $x \in E$ vektor $x_0 \overset{\text{def}}{=} x-ya$ pri $y=\dfrac{Lx}{La}$ je član od E_0 pa je prema dokazanom: $L(x_0)=(x_0, l)$. Tada je

$$L(x)=L(x_0+y\,a)=L(x_0)+L(y\,a)=(\text{jer je } y \text{ skalar})=(x_0, l)+y\,L\,a=$$
$$=(x_0, l)+y\,(a, l)=(x_0, l)+(y\,a, l)=(x_0+y\,a, l)=(x, l).$$

Dakle (4) stoji pa je lema dokazana; time je i teorem dokazan.

5.1.3. Na osnovu dokazanog teorema svaki vektor $x \in R^m$ je i kontravarijantan i kovarijantan pa zato pri zadanoj bazi (e_i) iz R^m imamo odgovarajuću dualnu bazu (e^j) u R^m te kontravarijantne koordinate x^i i kovarijantne koordinate x_j za koje je

$$x^i e_i = x = x_j e^j, \quad e^j e_i = \delta^j_i.$$

5.2. Neka je u euklidskom prostoru R^m data koordinatna baza

$$(e_i)=(e_1, e_2, \ldots, e_m);$$

time je određena i dualna baza

$$(e^j)=(e^1, e^2, \ldots, e^m)$$ jer iz zahtjeva

$$(0) \qquad e^i e_j = \delta^i_j$$

izlazi da su matrice (e^j), (e_i) recipročne, tj.

$$(1) \qquad \begin{bmatrix} e^1 \\ e^2 \\ \vdots \\ e^m \end{bmatrix} = [e_1\ e_2 \ldots e_m]^{-1}$$

(pri tom e^i ispisujemo kao redak, a e_j kao stupac). Zato relacija (1) ispisano glasi

$$(2)\qquad [e^i]=\begin{bmatrix} e^{11} & e^{12}\dots e^{1m} \\ \dots\dots\dots\dots & \\ e^{m1} & e^{m2} \quad e^{mm}\end{bmatrix}=\begin{bmatrix} e_{11} & e_{1m} \\ \dots\dots & \\ \dots\dots & \\ e_{m1} & e_{mm}\end{bmatrix}^{-1}=\left(\frac{fe_i}{\det[e_j]}\right)^T.$$

5.3. Veza među kontravarijantnim i kovarijantnim komponentama vektora.

Neka je x proizvoljan vektor iz R^m; tada imamo kontravarijantne komponente x^i prema $x=x^i e_i$ te kovarijantne komponente x_j prema $x=x_j e^j$.

No, iz te jednakosti izlazi

$$e_i\, x=e_i\,(x_j\, e^j)=x_j\,(e_i\, e^j)=x_j\,\delta_i^j=x_i. \qquad \text{Dakle je}$$

$$(3)\qquad x_i=e_i\, x. \qquad \text{Analogno}$$

$$(4)\qquad x^i=e^i\, x.$$

Izrazimo jedne koordinate pomoću drugih!

$$x_i=e_i\, x=e_i\,(x^j\, e_j)=x^j\,(e_i\, e_j), \quad \text{tj.}$$

$$(5)\qquad x_i=g_{ij}\, x^j \qquad \text{stavljajući}$$

$$(6)\qquad g_{ij}=e_i\, e_j.$$

Analogno je

$$(7)\qquad x^j=g^{jk}\, x_k \qquad \text{stavljajući}$$

$$(8)\qquad g^{jk}=e^j\, e^k.$$

Stavimo li

$$(9)\qquad g_j^i=e^i\, e_j=e_j\, e^i, \qquad \text{tada prema (0) imamo}$$

$$(10)\qquad g_j^i=\delta_j^i=\begin{cases}1 \\ 0\end{cases}\text{pri}\begin{cases}i=j \\ i\neq j\end{cases}.$$

Stavimo li izraz za x^j iz (7) u (5) izlazi

$$(11)\qquad x_i=g_{ij}\, g^{jk}\, x_k.$$

Relacija (11) vrijedi identički za svaki niz brojeva $x_1, x_2, \dots, x_m$; to znači da pri $i=k$ imamo $1=g_{(k)j}\, g^{j(k)}=\sum_j g_{(k)j}\, g^{j(k)}$ (zagrađeno (k) znači da se po k ne sumira).

Pri $i\neq k$ imamo $0=g_{ij}\, g^{jk}$, tj.

$$(12)\qquad g_{ij}\, g^{jk}=\delta_k^i.$$

Tako smo dokazali

→ **5.4. Teorem.** *Matrica $g=[g_{ij}]$ i matrica $[g^{jk}]$ međusobno su inverzne, pa je $g^{jk}=\dfrac{fg_{kj}}{\det g}$, gdje je fg_{kj} kofaktor od g_{kj}.*

5.5. Osnovni metrički afinor.

5.5.1. Dobili smo komponente $[g_{ij}] = e_i e_j$, odnosno $g^{ij} = e^i e^j$, odnosno $g_j^i = e^i e_j$. Radi li se pri tom o komponentama tenzora razreda 2? Jest!

Neka su naime x, y proizvoljni vektori iz E^m; kako su x, y i kontravarijantni i kovarijantni, to imamo obje vrste koordinata:

$$x = x^i e_i = x_j e^j$$

$$y = y^i e_i = y_j e^j.$$

Zato skalarni produkt $x\,y$ možemo izraziti:

1) pomoću kontravarijantnih koordinata: 2) pomoću kovarijantnih koordinata; 3) pomoću x^i, y_j te 4) pomoću x_i, y^j. U svim slučajevima dobivena vrijednost je ista i ne zavisi od izbora koordinatne baze.

No radimo li npr. sa kontravarijantnim komponentama, tada je

$$xy = (x^i e_i)\ (y^j e_j) = (e_i e_j)\, x^i y^j, \text{ tj.}$$

$$xy = g_{ij}\, x^i y^j.$$

Dakle zaista g_{ij} su koeficijenti bilinearne forme $g_{ij}\, x^i\, y^j$ koja pri svakoj koordinatnoj promjeni ima jednu te istu vrijednost; prema rezultatu iz 2.3.6 znači to da su g_{ij} komponente tenzora.

Isto tako

$$xy = g^{ij}\, x_i\, y_j \quad \text{te}$$

$$xy = g_j^i\, x_i\, y^j = (\text{prema (10)}) = x_i\, y^i \text{ jer je } g_j^i = \delta_j^i.$$

5.5.2. *Definicija osnovnog metričkog tenzora.* Dobiveni tenzor s komponentama g_{ij} zove se *osnovni metrički tenzor.* On je razreda 2; taj je tenzor simetričan, tj. $g_{ij} = g_{ji}$. Slično vrijedi za tenzor s koordinatama g^{ij}, odnosno g_j^i; dakle je

$$g^{ij} = g^{ij}, \quad g_j^i = g_i^j.$$

Tako smo dokazali

→ **5.5.3.** ***Teorem o osnovnom metričkom tenzoru. U svakom euklidskom prostoru R^m dimenzije m i s dualnim bazama (e_i), (e^j), veličine $g_{ij} = e_i\, e_j$, odnosno $g^{ij} = e^i\, e^j$ odnosno $g_j^i = e^i\, e_j$ jesu komponente jednog te istog tenzora koji se pojavljuje pri skalarnom množenju svake dvojke vektora iz E^m; pri tom su matrice g_{ij}, g^{ij} međusobno inverzne, a matrica g_j^i je jedinična.***

6. SIMETRIČNI TENZORI. KOSOSIMETRIČNI TENZORI

Sami nazivi govore o čemu je riječ. Te dvije vrste tenzora imaju veliku teoretsku i praktičku vrijednost. Posebno, vanjski („vektorski“) produkt vektora ulazi u kososimetrične tenzore.

6.1. Definicija simetričnosti (kose simetričnosti). Neka je t tenzor (nad prostorom $V=V_m$; prostor V je definiran nad nekim tijelom K karakteristike $\neq 2$); neka je (e_i) baza prostora V a $t^{i_1\ldots i_p}_{j_1\ldots j_q}$ koordinate tenzora t u odnosu na bazu (e_i); *tenzor t je simetričan (kososimetričan) ako pri svakoj transpoziciji jednorodnih indeksa svaka koordinata od t prelazi u samu sebe (u suprotnu vrijednost).*

6.1.1. *Konvencija.* Svaki skalar smatramo i simetričnim i kososimetričnim tenzorom razreda 0. Isto tako svaki tenzor razreda 1 smatramo i simetričnim i kososimetričnim.

6.1.2. Posebno se samo po sebi razumijeva da je svaki kontravarijantan tenzor razreda p simetričan (kososimetričan) onda i samo onda ako svaka permutacija gornjih indeksa u koordinatama od t prevodi svaku koordinatu x u samu sebe (u $-x$).

6.1.3. Dualno vrijedi za kovarijantne tenzore $t_{j_1 j_2 \ldots j_q}$.

Lako se dokazuje ovo

6.2. *Ako su pri nekoj koordinatnoj bazi (e_i) prostora V koordinate tenzora t simetrične (kososimetrične) funkcije svojih donjih, odnosno gornjih indeksa, onda su koordinate od t u odnosu na svaku koordinatnu bazu od V simetrične (kososimetrične) funkcije svojih donjih (gornjih) indeksa.*

6.3. Definicija *simetričnosti prema P.* Neka je P bilo koji podskup od $\{1, 2, \ldots, p\}$, pri čemu je p razred kontravarijantnosti tenzora t; tada se kaže da je t simetrično (kososimetrično) u odnosu na indekse iz P, ako svaka transpozicija u P prevodi t u t (odnosno u $-t$).

6.3.1. Lema. *Ako je t kososimetrično u odnosu na indekse iz P, onda svaka koordinata x od t u kojoj se javljaju dva jednaka indeksa iz P zadovoljava $2x=0$ (dakle $x=0$ ukoliko karakteristika tijela K nije $=2$).*

Naime ako je $x=t^{\cdots i\cdot u\cdots i\cdots}$ koordinata od t, tada transpozicija odgovarajućih indeksa $i\ldots i$ daje formalno opet x a s druge strane daje $-t^{\cdots i\cdots\cdot i\cdots}$ $=-x$ zbog kose simetrije. Dakle je $x=-x$, tj $2x=0$.

6.3.2. Korolar. *Kososimetrični tenzor razreda $(p+0)$ ili razreda $(0+p)$ nad prostorom V_m od m dimenzija je nužno nula-tenzor za svako $p>m$.*

6.4. Polivektor. Forme.

Svaki kososimetrični tenzor razreda $(p+0)$ nad V zove se *polivektor*; posebno pri $p=0$ i $p=1$ govorimo i o skalarima kao 0-vektorima i kontravarijantnim vektorima kao 1-vektori. Dualno, svaki kososimetrični tenzor razreda $(0+q)$ nad V zove se *q-forma* ili *polivektor*; pri tom dopuštamo da bude $q=0$ (skalari) kao i $q=1$ (kovarijantni vektori nad V).

Posebno govorimo o bivektorima ($p=2$), trivektorima ($p=3$) te o 2-formama ($q=2$), 3-formama ($q=3$), itd.

Prema tome, polivektori su posebni kososimetrični tenzori i to upravo oni koji su čistokontravarijantni ili čistokovarijantni. Ako je t neki p-vektor (q-forma) nad V, onda to znači da je

$t\in V^{\wedge(r)}$ (odnosno $t\in V^{*\wedge(q)}$) u smislu naredne oznake.

Prema tome, pri svakoj transpoziciji donjih indeksa prelazi t u t (odnosno $-t$); isto tako pri svakoj transpoziciji gornjih indeksa prelazi t u t (odnosno u $-t$)

6.4.1. *Prostor* $V^{\wedge(p)}$. Skup svih p-vektora (q-formi) nad V označuje se sa

$$V^{\wedge(p)} \text{ (odnosno } V^{\star\wedge(q)});$$

znak $\wedge$ će značiti vanjsko množenje (isp. § 7) članova iz V (odnosno iz $V^\star$).

6.5. Koordinate kososimetričnih tenzora.

6.5.1. Primjer. Promatrajmo npr. posve simetrični tenzor $t = t^{ijk} e_{ijk}$ razreda $(3+0)$ nad prostorom V_4 od 4 dimenzije.

Taj tenzor ima 4^3 koordinate t^{ijk} jer se indeksi i, j, k, kreću nezavisno u $\{1, 2, 3, 4\}$. Međutim, ako skup $\{i, j, k\}$ ima manje od 3 člana, tada je $t^{ijk} = 0$; zato možemo pretpostaviti da je skup $\{i, j, k\}$ tročlan. Možemo pretpostaviti da je $i<j<k$; tada za svaku permutaciju $c = c_i, c_j, c_k$ od i, j, k imamo odgovarajuću komponentu $t^{c_i c_j c_k} e_{c_i c_j c_k} = \operatorname{sgn} c\, t^{ijk} e_{c_i c_j c_k}$, gdje je $\operatorname{sgn} c = (-1)^{Ic}$; Ic je broj inverzija permutacije c. Na taj način uz 3-člani podniz i, j, k od $1, 2, 3, 4$, vezana je suma

$$t^{ijk} (\operatorname{sgn} c\, e_{c(ijk)}) = t^{ijk} \operatorname{sgn} c\, e_{c_i c_j c_k}$$

od $3!$ komponenata tenzora t; kako takvih suma ima $\binom{4}{3}$, znači da kososimetrični tenzor t razreda $(3, 0)$ nad V_4 ima najviše $\binom{4}{3}\, 3!$ koordinata koje su $\neq 0$.

6.5.2. Striktne koordinate kososimetričnih tenzora.

Definicija. Neka je (e_i) baza prostora V_m; neka je t tenzor nad V_m razreda $(p+q)$ i neka su $t^{i_1 \ldots i_p}_{j_1 \ldots j_q}$ koordinate od t u bazi (e_i); svaka koordinata od t za koju je i niz gornjih indeksa čisto uzlazan ($i_1 < i_2 < \cdots < i_p$ ukoliko je $p > 1$) i niz donjih indeksa čisto uzlazan (tj. $j_1 < j_2 < \cdots < j_q$, pri $q > 1$) zove se *striktna* ili *bitna koordinata tenzora t*.

6.5.3. Lema. *Tenzor t razreda $(p+q)$ nad V_m pri $m = \dim V$ ima upravo*

$$\binom{m}{p}\binom{m}{q} \quad \textit{striktnih koordinata.}$$

Naime, $\binom{m}{p}$ je broj čisto uzlaznih p-članih nizova iz $\{1, 2, \ldots, m\}$ a $\binom{m}{q}$ je broj čisto uzlaznih q-članih nizova iz $\{1, 2, \ldots, m\}$ a svaki takav p-člani (q-člani) niz može doći u gornje (donje) indekse određene striktne koordinate od t.

6.5.4. Teorem. *Svaki kososimetrični tenzor t razreda $(p+q)$ nad prostorom V_m od m dimenzija ima najviše $\binom{m}{p}\, p!\, \binom{m}{q}\, q!$ koordinata koje su $\neq 0$.*

Stvarno, neka je

$$t^i_j = t^{i_1 \ldots i_p}_{j_1 \ldots j_q} \tag{1}$$

striktna koordinata od t; neka je f proizvoljna permutacija niza $i=i_1\ldots i_p$; tada imamo koordinatu $t_j^{fi}=\operatorname{sgn} f\, t_j^i$; isto tako pri proizvoljnoj permutaciji g skupa $j=\{j_1,\ldots,j_q\}$ imamo koordinatu (2) $\operatorname{sgn} g\ \operatorname{sgn} f\, t_j^i = t_{g(j_1)\ldots g(j_q)}^{f(i_1)\ldots f(i_p)}$.

Uz striktnu koordinatu t_j^i dobivamo tako $p!\ q!$ koordinata oblika (2). Kako striktnih koordinata prema 6.5.3. ima $\binom{m}{p}\binom{m}{q}$ znači da koordinata bez jednakih istorodnih indeksa ima zaista upravo

$$\binom{m}{p} p!\ \binom{m}{q} q; \text{ jer pri } \begin{bmatrix} i \\ j \end{bmatrix} \neq \begin{bmatrix} i' \\ j' \end{bmatrix} \text{ izlazi } \begin{bmatrix} fi \\ gj \end{bmatrix} \neq \begin{bmatrix} f'i' \\ g'j' \end{bmatrix}$$

za svaki strogo uzlazni podniz $\begin{cases} i' \\ j' \end{cases}$ od $1, 2, \ldots, m$ kao i svaku permutaciju $\begin{cases} f' \\ g' \end{cases}$ od $\begin{cases} i' \\ j' \end{cases}$.

6.5.5. Korolar (posljedica). *Svaki kososimetrični tenzor t razreda $(p+0)$ nad prostorom V_m od m dimenzija ima najviše $\binom{m}{p} p!$ koordinata koje su $\neq 0$ (predmnijevamo da broj 2 nije karakteristika tijela K nad kojim je V_m definirano)* (isp. korolar 6.3.2).

Specijalno svaki kososimetrični tenzor t razreda $(2+0)$ dopušta rastav

$$t=\sum_{i<j} t^{ij}(e_{ij}-e_{ji}), \qquad \text{odnosno}$$

(1)
$$t=t^{ij}e_i\wedge e_j=(t^{ij}e_i)\wedge e_j,$$

stavljajući
$$e_i\wedge e_j=e_i\otimes e_j-e_j\otimes e_i.$$

Tu se pojavljuje izraz $e_i\otimes e_j-e_j\otimes e_i$ koji mjeri odstupanje tenzorskog množenja od komutativnosti, a zove se *vanjski produkt vektora e_i i vektora e_j*.

6.6. Kososimetrični tenzori razreda $(m+0)$ nad V_m. *Neka je t kososimetričan tenzor i razreda $(m+0)$ nad V_m dimenzije m. Tada t ima jednu jedinu striktnu komponentu i to $t^{1,2\ldots m}$; pri promjeni koordinatne baze $e_{i'}=a_{i'}^i e_i$ množi se ta koordinata sa* $\det a^{-1}$. *Svaka druga komponenta je oblika $t^{i_1\ldots i_m}$, gdje je i permutacija od $1, 2, \ldots, m$, pa je*

(1)
$$t^{i_1 i_2\ldots i_m}=(-1)^{I(i_1\ldots i_m)}t^{12\ldots m},$$

$$t=\sum_i (-1)^{I(i_1\ldots i_m)}t^{12\ldots m}e_{i_1}\otimes e_{i_2}\otimes\cdots\otimes e_{i_m},\quad i\in\{1, 2, \ldots, m\}!).$$

Dokaz. Prema osnovnom obrascu 2.4 imamo

$$t^{1'2'\ldots m'}=a_{i_1}^{1'}a_{i_2}^{2'}\ldots a_{im}^{m'}t^{i_1\ldots i_m}=(\text{prema (1)})=$$

$$=a_{i_1}^{1'}\ldots a_{im}^{m'}(-1)^{I(i_1\ldots i_m)}t^{1\ldots m}=\left((-1)^{I(i_1\ldots i_m)}a_{i_1}^{1'}\ldots a_{im}^{m'}\right)t^{1\ldots m}$$

$$=(\det a_{ij'}^{j'})\,t^{1\ldots m}=\det(a^{-1})\,t^{1\ldots m}.$$

6.6.1. Posljedica. U euklidskom prostoru R^3 miješani produkt $(x \times y)\ z$ kontravarijantnih vektora $x, y, z \in R^3$ je kososimetričan tenzor razreda $(3+0)$ pa se promjenom koordinatne baze njegova striktna koordinata množi sa $\det a^{-1}$; zato se ta koordinata zove *pseudo-skalar* a ne skalar; naime, ako je $\det a \neq 1$ tada broj $t^{1\,2\,3}$ ne ostaje nepromijenjen pri promjeni koordinatne baze.

6.7. Kosa simetrizacija.

6.7.1. Promatrajmo nad prostorom V_m zadan tenzor, npr. čisto kontravarijantni tenzor $t = t^{i_1 i_2 \cdots i_p} e_{i_1 \ldots i_p}$ razreda $(p+0)$.

Za zadan p-član niz $i = i_1 \ldots i_p$ brojeva iz $\{1, 2, \ldots, m\}$ možemo promatrati bilo koju permutaciju $f\ i = f\ i_1, f\ i_2 \ldots f\ i_p$ toga niza i signaturu $\operatorname{sgn} f = (-1)^{If}$ te permutacije. Kad bi t bio kososimetričan tenzor, bilo bi

$$t^{fi}\ e_{fi} = (\operatorname{sgn} f\ t^i)\ e_{fi} = t^i \operatorname{sgn} f\ e_{fi}.$$

Zato je prirodno promatrati izraz

$$e_{(i)} = \sum_{fi} \operatorname{sgn} f\ e_{fi},$$

pri čemu se sumira po svim permutacijama $f\ i$ danog niza i. Na taj način imamo tenzore $e_{(i)}$, $t^i\ e_{(i)}$ pa vidimo da je t linearna kombinacija tenzorâ $e_{(i)}$; ovi tenzori tvore bazu u prostoru $V_m^{\wedge(p)}$ svih kososimetričnih tenzora nad V_m razreda $(p+0)$. Dakle vrijedi

6.7.2. Teorem. *Ako je $n \leq m$, tada je* $\dim V_m^{\wedge(n)} = \binom{m}{n}$.

6.7.3. *Prelaz $t \to A\,t$.* Uz svaku koordinatu t^i tenzora t i svaku permutaciju f niza $i = i_1 \ldots i_p$ možemo promatrati tenzor

$$\frac{1}{p!} \sum_f \operatorname{sgn} f \cdot t^{fi}\ e_{fi}. \tag{1}$$

Učinimo li analognu „kosu simetrizaciju" svake koordinate tenzora t i rezultate zbrojimo, dobit ćemo jednoznačno određen izraz. Označimo ga sa $A\,t$.

6.7.4. Lema. *Za svaki tenzor t također je $A\,t$ tenzor; tenzor $A\,t$ je kososimetričan; $A\,(A\,t) = A\,t$. Ako je t kososimetričan tenzor, tada je $A\,t = t$ (to je i razlog da smo u definiciji* (1) *dijelili sa $p\,!$).*

Za dokaz je dovoljno vidjeti da je izraz (1) kososimetričan tenzor istog razreda kojeg je i tenzor kojemu je t^i jedina koordinata koja je eventualno $\neq 0$.

No, jasno je da je izraz (1) tenzor istog razreda kojeg i tenzor s jednom jedinom koordinatom t^i.

Dokažimo da je (1) antisimetrično.

Naime, provedemo li proizvoljnu transpoziciju $x \longleftrightarrow y$ dvaju članova iz skupa $S = \{1, 2, \ldots, p\}$, preći će skup $S!$ svih permutacija od S opet u sama sebe, samo pri tom permutacija $f \in S!$ i permutacija $f(x, y)$ imaju protivne signature tj.

$$\operatorname{sgn} f = -\operatorname{sgn}(f(x\ y));$$

sam izraz (1) transpozicijom (x, y) postaje

$$\frac{1}{p!} \sum_{f \in S} \operatorname{sgn} f \cdot t^{(x,y)fi} e_{(x,y)fi} = \frac{1}{p!} \sum_{(x,y)f} -\operatorname{sgn}(x, y) f e^{(x,y)fi} e_{(x,y)fi}$$
$$= -(1).$$

6.7.5. P r i m j e r. Neka je

$$t = t^{1\,2\,3} e_{1\,2\,3} + t^{2\,3\,4} e_{2\,3\,4};$$

tada je (množeći odmah sa 3!)

$$3!\ A\, t = t^{1\,2\,3} e_{1\,2\,3} - t^{1\,3\,2} e_{1\,3\,2} - t^{2\,1\,3} e_{2\,1\,3} + t^{2\,3\,1} e_{2\,3\,1} +$$
$$+ t^{3\,1\,2} e_{3\,1\,2} - t^{3\,2\,1} e_{3\,2\,1} + t^{2\,3\,4} e_{2\,3\,4} - t^{2\,4\,3} e_{2\,4\,3} -$$
$$- t^{3\,2\,4} e_{3\,2\,4} + t^{3\,4\,2} e_{3\,4\,2} + t^{4\,2\,3} e_{4\,2\,3} - t^{4\,3\,2} e_{4\,3\,2}.$$

Očigledno je $A\, t$ antisimetrično.

6.8. Kosa simetrizacija (ili alterniranje) u odnosu na zadan skup indeksa.

6.8.0. Radi jednostavnosti uzmimo neki kontravarijantan tenzor t^i razreda $(p+0)$.

6.8.1. Neka je $S \subset \{1, 2, 3, \ldots, p\}$; provesti kosu simetrizaciju nad tenzorom t u odnosu na skup S indeksâ znači promatrati tenzor $u = A_S t$ koji se iz tenzora t dobije tako da se svaki sumand koordinata $t^i e_i$ od t zamijeni izrazom

$$\frac{1}{s!} \sum_{f \in S!} \operatorname{sign} f\, t^{fi} e_{fi};$$

pri tom je s broj članova od S; sa $f\, i$ označujemo niz $i_{f1}, \ldots i_{fp}$ koji iz niza $i = i_1, i_2 \ldots, i_p$ nastaje djelovanjem permutacije kao funkcije; pri $k \notin S$ uzimamo $f_k = k$.

Pišemo $u = A_S t$.

Tenzor $A_S t$ je kososimetričan u odnosu na skup indeksa iz S.

6.8.2. L e m a. *Ako postoji suma tenzora t, u, tada za proizvoljne skalare λ, μ i proizvoljan dopustiv skup indeksa I vrijedi*

$$A_I(\lambda\, t + \mu\, u) = \lambda\, A_I\, t + \mu\, A_I\, u.$$ Dokaz je očigledan.

6.8.3. L e m a. *Ako je $B \subset C \subset \{1, 2, \ldots, p\}$, tada za kose simetrizacije A_B, A_C proizvoljna tenzora t razreda $(p+0)$ vrijedi*

$$A_C(A_B\, t) = A_C\, t.$$

Dokaz. Bez uštrba na općenitost možemo se ograničiti na slučaj da je npr. $B=\{1, 2, \ldots, b\}$, $C=\{1, 2, \ldots, c\}$ i pri tom $b \leqslant c$. Promatrajmo koordinatu $t^{i_1 \ldots i_b \ldots i_p}$; tada imamo

$$A_B t^i = \frac{1}{b!} \sum_{\beta \in (1, \ldots, b)!} \operatorname{sgn} \beta \, t^{i_{\beta(1)} \ldots i_{\beta(b)} i_{b+1} \ldots i_p}$$

$$A_C (A_B t^i) = \frac{1}{b!} \sum_{\beta} \operatorname{sgn} \beta \, A_C (t^{i_{\beta(1)} \ldots i_{\beta(b)} i_{b+1} \ldots i_p}) =$$

$$= \frac{1}{b!} \sum_{\beta} \operatorname{sgn} \beta \frac{1}{c!} \sum_{\pi \in (1, \ldots c)!} \operatorname{sgn} (\pi \beta^{-1}) \, t^{i_{\pi_1} i_{\pi_2} \ldots i_{\pi_b} \ldots i_{\pi_p}}.$$

β^{-1} je permutacija koja je u $\{1, 2, \ldots, b\}$ obrnuta sa β, a u $\{b+1, \ldots, p\}$ je identitet. Zbog $\operatorname{sgn} \pi\beta^{-1} = \operatorname{sgn} \pi \operatorname{sgn} \beta^{-1}$, $\operatorname{sgn} \beta^{-1} = \operatorname{sgn} \beta$

gornji je izraz dalje

$$= \frac{1}{b!} \sum_{\beta} \left(\frac{1}{p!} \sum_{\pi} \operatorname{sgn} \pi \, t^{i_{\pi_1} \ldots i_{\pi_p}} \right) = \frac{1}{b!} \sum_{\beta} A_C t^{i_1 \ldots i_p} = A_C t^{i_1 \ldots i_p}.$$

7. VANJSKI PRODUKT UREĐENE DVOJKE VEKTORA. BIVEKTOR

7.1. Definicija. *Vanjski produkt* uređene dvojke (x, y) vektora x, y jest

$$x \wedge y \stackrel{\text{def}}{=} x \otimes y - y \otimes x.$$

Prema tome, vanjski umnožak od x i y svodi se na tenzorsko množenje od x i y i od y i x; zato je i $x \wedge y$ određen tenzor, i to kososimetričan tenzor.

Odmah vidimo da je $x \wedge x = 0$ za svaki vektor x.

Neposredno se provjere ove činjenice 7·2—7·4:

7.2. Vanjski produkt uređene dvojke vektora je kososimetričan, distributivan i prema prvom i prema drugom faktoru a *izlučan* je prema svakom skalaru, tj. za svaki skalar λ vrijedi

$$\lambda (x \wedge y) = (\lambda x) \wedge y = (x \wedge \lambda y).$$

7.3. Teorem. Ako je (e_i) proizvoljna baza prostora V_m, vanjski produkti

$$e_i \wedge e_j \quad (i < j \leqslant m)$$

čine bazu prostora $V_m^{\wedge(2)}$ svih kososimetričnih tenzora razreda $(2+0)$ nad prostorom V_m; posebno je $\dim V_m^{\wedge(2)} = \binom{m}{2}$.

Neposredno se provjeri da je $V_m^{\wedge(2)}$ zaista vektorski potprostor prostora $V_m^{(2)}$ svih dvojako kontravarijantnih tenzora razreda $(2+0)$ nad V.

Nadalje, za svako $t \in V_m^{\wedge(2)}$ imamo $t = t^{ij} e_{ij} = \sum_{i<j} t^{ij} e_{ij} + t^{ii} e_{ii} + \sum_{i>j} t^{ij} e_{ij}$

$$= (\text{zbog } t^{ii} = 0,\ t^{ij} = -t_{ji}) = \sum_{i<j} t^{ij} e_{ij} - \sum_{j>i} t^{ij} e_{ji} = \sum_{i<j} t^{ij} (e_{ij} - e_{ji}) =$$

$$= \sum_{i<j} t^{ij} e_i \wedge e_j.$$

Dakle članovi $e_i \wedge e_j$ razapinju prostor $V' = V_m^{\wedge(2)}$. No, $e_i \wedge e_j$ su linearno nezavisni, jer bi svaka linearna netrivijalna veza članova $e_i \wedge e_j$ značila također netrivijalnu vezu članova e_i, u protivnosti s pretpostavkom da su e_i linearno nezavisni.

7.4. *Pseudo-vektorski karakter* veličine

$$x \wedge y, \text{ pri } x = \begin{bmatrix} x^1 \\ x^2 \\ x^3 \end{bmatrix}, \quad y = \begin{bmatrix} y^1 \\ y^2 \\ y^3 \end{bmatrix}.$$

Na taj način vidimo da imamo vektorske prostore V_m, $V_m^{(2)}$, $V^{\wedge(2)}$ i njihove odgovarajuće članove. Neka su (e_i), $(e_{i'})$ dvije baze u V_m a vezane pomoću

(1) $$e_{j'} = a_{j'}^i e_i, \text{ odnosno } e_i = a_i^{j'} e_{j'}.$$

Neka su $e_i \otimes e_j$, $e_{i'} \otimes e_{j'}$ odgovarajuće baze od $V_m^{(2)}$; neka su

$$e_i \wedge e_j \,(i<j), \quad e_{i'} \wedge e_{j'} \,(i'<j')$$

odgovarajuće baze u $V_m^{\wedge(2)}$.

Promatrajmo proizvoljni tenzor $t \in V_m^{\wedge(2)}$; dakle je

(2) $$t = t^{ij} e_i \wedge e_j \quad (i<j).$$

Kako je također $t \in V_m^{(2)}$, vrijedit će (isp. § 2.5)

$$t^{i'j'} = a_i^{i'} a_j^{j'} t^{ij} = \frac{\partial x^{i'}}{\partial x^i} \frac{\partial x^{j'}}{\partial x^j} t^{ij}.$$

Kako je t kososimetrično, to je $t^{ii} = 0 = t^{i'i'}$ te $t^{ij} = -t^{ji}$; zato gornji izraz za $t^{i'j'}$ daje

$$t^{i'j'} = a_i^{i'} a_j^{j'} t^{ij} + (a_j^{i'} a_i^{j'} \cdot -t^{ij}) \quad (i<j), \quad \text{tj.}$$

(3) $$t^{i'j'} = (a_i^{i'} a_j^{j'} - a_j^{i'} a_i^{j'})\, t^{ij} \quad (i<j).$$

Tu formulu možemo pisati i ovako

(4) $$t^{i'j'} = \frac{D(x^{i'} x^{j'})}{D(x^i x^j)} t^{ij} \quad (i<j), \qquad \text{stavljajući}$$

$$\frac{D(x^{i'} x^{j'})}{D(x^i x^j)} = a_i^{i'} a_j^{j'} - a_j^{i'} a_i^{j'} \quad \text{jer je } a_i^{i'} = \frac{\partial x^{i'}}{\partial x^i} \qquad \text{(isp. §. 2.5.1).}$$

Na taj način vidimo da se striktne koordinate t^{ij} (dakle je $i<j$) ne transformiraju na isti način kao obične koordinate t^{ij} (bez ograničenja na uslov $i<j$) jer bez uslova $i<j$ odnosno $i'<j'$ znamo da vrijedi

$$t^{i'j'} = a_i^{i'} a_j^{j'} t^{ij} = \frac{\partial x^{i'}}{\partial x^i} \frac{\partial x^{j'}}{\partial x^j} t^{ij} \text{ (isp. § 2.5).}$$

Specijalno za vanjski produkt $x(1) \wedge x(2)$ vektora $x(1) = (x^i)$ i vektora $x(2) = y = (y^i)$ transformacione formule za striktne koordinate nisu oblika (2) nego su oblika (3).

7.5. *Poseban slučaj euklidskog prostora* $R^3 = V$. Promotrimo poseban slučaj $m = 3$, tj. $V_m = V_3$. Ako su $x = (x^i)$, $y = (y^i)$ kontravarijantni vektori nad R^3, tada je

$$x \wedge y = x \otimes y - y \otimes x = (x^1 y^2 - x^2 y^1) e_{12} + (x^2 y^3 - x^3 y^2) e_{23} + \\ + (x^3 y^1 - x^1 y^3) e_{31}.$$

Tada su striktne koordinate od $t \in V^{\wedge(2)}$ ove:

$$t^{12},\ t^{13},\ t^{23}.$$

Stavimo

$$v^1 = t^{23},\ v^2 = t^{31},\ v^3 = t^{12}$$

(oznake v^2, v^3 izlaze iz v^1 cikličkom transformacijom). Analogno

$$v^{1'} = t^{2'3'},\ v^{2'} = t^{3'1'},\ v^{3'} = t^{1'2'}.$$

Promatrajmo u R^3 bazu (e_i); stavimo

(1) $$e_1 \wedge e_2 = E_3,\ e_2 \wedge e_3 = E_1,\ e_3 \wedge e_1 = E_2.$$

Na taj način, svaki kososimetrični tenzor $t \in R^3$ glasi

(2) $$t = t^{12} E_3 + t^{23} E_1 + t^{31} E_2.$$

Nameće se usklađenija oznaka;

(3) $$t^1 = t^{23},\ t^2 = t^{31},\ t^3 = t^{12},$$

nameće se misao kao da bi $t = \begin{bmatrix} t^1 \\ t^2 \\ t^3 \end{bmatrix}$ bio kontravarijantan vektor, dakle

(4) $$t = t^i E_i;$$ da li je ta misao ispravna?

Pri nekoj drugoj koordinatnoj bazi $(e_{i'})$ bilo bi analogno

(4') $$t = t^{i'} E_{i'}$$

uz oznake koje iz oznaka u (1)—(3) izlaze stavljajući apostrof na svaki gornji i na svaki donji indeks.

Time pri promjeni koordinatne baze 7.4 (1) formule 7.4 (3) postaju

(5) $$t^{1'} = (a_2^{2'} a_3^{3'} - a_3^{2'} a_2^{3'}) t^1 + \ldots \text{ciklički}.$$

Koeficijenti na desnoj strani jesu komponente vektorskog produkta

$$a^{2'} \times a^{3'} \text{ redaka } a^{2'}, a^{3'}.$$

Pri tom $a^{i'}$ naznačuje i-ti redak matrice a^{-1}; isto tako a^i označuje i-ti redak od a. Dakle je

(5) $$t^{1'} = (a^{2'} \times a^{3'})^1 t^1 + (a^{3'} \times a^{1'})^2 t^2 + (a^{1'} \times a^{2'})^3 t^3;$$

tu svuda eksponenti znače gornje indekse. Izrazi za $t^{2'}$, $t^{3'}$ dobiju se cikličkom zamjenom.

S druge strane, za svaku regularnu (3, 3)-matricu a lako se vidi da vrijedi

$$(6)\qquad a^{-1}=\frac{1}{\det a}\begin{bmatrix} a_2\times a_3\\ a_3\times a_2\\ a_1\times a_3\end{bmatrix}=\frac{1}{\det a}\begin{bmatrix} a_2^2a_3^3-a_2^3a_3^2 & a_2^3a_3^1-a_2^1a_3^3 & a_2^1a_3^2-a_2^2a_3^1\\ \cdots & \cdots & \cdots\\ & \text{ciklička zamjena donjih indeksa} & \end{bmatrix}$$

Ako tu umjesto a^{-1} odnosno a pišemo a^{-1}, znači to da vrijedi

$$(7)\qquad a=\frac{1}{\det a^{-1}}\begin{bmatrix} a_2^{-1}\times a_3^{-1}\\ \\ \cdots\cdots\end{bmatrix}=\frac{1}{\det a^{-1}}\begin{bmatrix} a_2^{2'}a_3^{3'}-a_2^{3'}a_3^{2'},\ \dots\\ \\ \text{ciklički}\end{bmatrix}$$

Specijalno je dakle $a_1^1=\det a^{-1}(a_2^{2'}a_3^{3'}-a_2^{3'}a_3^{2'})$, $a_2^1=$

$$=\det a^{-1}(a_2^{3'}a_3^{1'}-a_2^{3'}a_3^{1'}),\quad a_3^1=\det a^{-1}(a_2^{1'}a_3^{2'}-a_2^{2'}a_3^{1'}).$$

Ako te izraze uvrstimo u obrazac (5), izlazi

$$(8)\qquad t^{1'}=\det a^{-1'}a_1^1t^1+\det a^{-1}\cdot a_2^1t^2+\det a^{-1}a_3^1t^3=\det a^{-1}\cdot a_i^1t^i.$$

Slično za $t^{2'}$, $t^{3'}$ pa tako imamo

$$(9)\qquad t^{i'}=\det a^{-1}\cdot a_i^{i'}t^i.$$

7.5.1. Na taj način vidimo da stvarno — osim kad je $\det a^{-1}=1$, veličine t^i nisu koordinate kontravarijantnog vektora. Naime, tada se u transformacionim formulama pojavljuje još i faktor $\det a^{-1}$ odnosno

$$(10)\qquad \det\left(\frac{\partial\,(x^i)}{\partial\,(x^{j'})}\right)^{-1},$$

gde je (10) funkcijska determinanta starih varijabla prema novim varijablama.

U vezi s gornjim primjerom postavlja se

7.6. *Definicija relativnih tenzora* (*pseudo-tenzor*). Zadani su redni brojevi p, q i broj M; pseudo-tenzor razreda $(p+q)$ i težine M nad prostorom V_m sa zadanom bazom (e_i) je svaki sistem funkcija

$$\begin{bmatrix} i\\ j\end{bmatrix}_e=\begin{bmatrix} i_1, i_2\cdots i_p\\ j_1\ j_2\cdots j_q\end{bmatrix}\to t_j^i$$

koji ima svojstvo da za svaku drugu koordinatnu bazu $(e_{i'})$ prostora V_m odgovarajuće koordinate $t_{j'}^{i'}$ glase

$$t_{j'_1\dots j'_q}^{i'_1\dots i'_p}=\left(\det\frac{\partial x^\mu}{\partial x^{\mu'}}\right)^M t_{j_1\dots j_q}^{i_1\dots i_p}\cdot\frac{\partial x^{i'_1}}{\partial x^{i_1}}\cdots\frac{\partial x^{i'_p}}{\partial x^{i_p}}\,\frac{\partial x^{j_1}}{\partial x^{j'_1}}\cdots\frac{\partial x^{j_q}}{\partial x^{j'_q}};$$

pri tom svi indeksi-varijable $i_1, i_1', \dots j_q, j_q'$ prolaze nezavisno skupom $\{1, 2, \dots, m\}$; sa $\left[\dfrac{\partial x^\mu}{\partial x^{\mu'}}\right]$ označuje se Jacobijeva ili funkcijska matrica funkcijâ $x^\mu=x^\mu(x^{1'},\dots,x^{m'})$ $(\mu=1, 2, \dots, m)$ kojom su vezane stare koordinate x^μ i nove koordinate $x^{\mu'}$ tačke-vektora $x\in V_m$.

U slučaju $p=0$, $q=0$ govori se o *pseudo-skalarima težine M*.

Na osnovu činjenica iz § 2.5 zaključujemo da pseudo-tenzori težine $M=0$ daju upravo tenzore; naime ako je težina $M=0$, tada prema teoremu 2.3 i 2.5.3 pseudo-tenzor t postaje tenzorom.

Na osnovu definicije 7.6 imamo

7.7. Teorem. *Vanjski produkt kontravarijantnih vektora u Euklidskom prostoru R^3 je pseudo-vektor težine* -1 (isp. 7.5.1); *miješani produkt* $(x\times y)z$ *kontravarijantnih vektora u prostoru R^3 je pseudo-skalar težine* -1 (isp. § 6.6.1).

8. VANJSKI PRODUKT UREĐENE *n*-TORKE VEKTORA. VANJSKA ALGEBRA

8.1. Zadan je vektorski prostor $V=V_m$ od m dimenzija nad tijelom K karakteristike $\neq 2$; u V je zadana neka baza (e_i); za svaki redni broj p imamo tenzorsku potenciju $V_m^{(p)}$ (isp. § 2.2.3) kao i potprostor $V_m^{\wedge(p)}$ sastavljen od svih kososimetričnih članova iz $V_m^{(p)}$; posebno, ako je $p>m$ (odnosno $p=m$), tada je $V_m^{\wedge(p)}$ sastavljeno od nula-tenzora (isp. 8.6) (odnosno od pseudo-skalara težine -1) (isp. 6.6).

Po dogovoru je $$V_m^{\wedge(0)}=K,\quad V_m^{\wedge(1)}=V_m.$$

8.2. Unija $V_m^{\wedge}$ prostorâ $V_m^{\wedge(p)}$ $(p=0,1,\ldots)$ kao algebra.

U toj uniji ili zbiru definirali smo vanjski produkt $x\wedge y$ za svako

$$x, y\in V_m^{\wedge(0)}\cup V_m^{\wedge(1)}.$$

Sada ćemo definirati $x\wedge y$ za svako $x\in V^{\wedge}$ i svako $y\in V^{\wedge}$.

Neka je B proizvoljan b-vektor (dakle $B\in V_m^{\wedge(b)}$; neka je C proizvoljan c-vektor, tj. $C\in V_m^{\wedge(c)}$; dakle je $B=0$ pri $b>m$; pri $b\leq m$ imamo za svaki b-podniz $X=X_1<X_2<\cdots<X_b$ od $1, 2, \ldots, m$ odgovarajuću striktnu koordinatu B^X kao i odgovarajuću komponentu

$$B^X E_X\,,\ \text{gdje je } E_X=\sum_\beta \operatorname{sgn}\beta\cdot e_{\beta_1}\otimes e_{\beta_2}\otimes\cdots\otimes e_{\beta_b}\overset{\text{def}}{=} e_{x_1}\wedge e_{x_2}\wedge\cdots\wedge e_{x_b}\,.$$

Na taj je način

$$B=\sum_X B^X E_X\quad (X\subseteq\{1,2,\ldots,m\}, k\,X=b).$$

Isto tako je

$$C=\sum_Y C^Y E_Y\ \text{pri}\ Y\subset\{1,2,\ldots,m\}, k\,Y=c.$$

Definirat ćemo $B\wedge C$ ovako:

$$B\wedge C=\sum_{X,Y} B^X C^Y E_X\wedge E_Y,$$

stavljajući

$$E_X \wedge E_Y = \begin{cases} 0 \text{ pri } X \cap Y \neq \emptyset \\ \operatorname{sgn}(X_1 X_2 \ldots X_b Y_1 Y_2 \ldots Y_c) E_{X \cup Y}, \text{ pri } X \cap Y = \emptyset; \end{cases}$$

$$E_{X \cup Y} = \operatorname{sgn} z_1 z_2 \ldots z_{b+c} e_{z_1} \otimes z_{z_2} \otimes \cdots \otimes e_{z_{b+c}};$$

pri tom niz $z_1, z_2, \ldots, z_{b+c}$ prolazi svim permutacijama niza

$$X_1 X_2 \ldots X_b Y_1 Y_2 \ldots Y_c.$$

8.3. Odmah se vidi da je $B \wedge C$ određen $(b+c)$-vektor i da vanjski produkt zavisi linearno od prvog faktora B i drugog faktora C.

8.4. Teorem. *Vanjsko množenje je asocijativno;* $(V_m^\wedge, \wedge)$ *je asocijativan grupoid:* iz $B, C, D \in V_m^\wedge$ *izlazi* $(B \wedge C) \wedge D = B \wedge (C \wedge D) \overset{\text{def}}{=} B \wedge C \wedge D$.

Dokaz. Neka je

$$B \in V_m^{\wedge(\beta)}, \quad C \in V_m^{\wedge(\gamma)}, \quad D \in V_m^{\wedge(\delta)}; \qquad \text{tada je}$$

$$B = A^X E_X, \quad C = C^Y E_Y, \quad D = D^Z E_Z;$$

pri tom su X, Y, Z proizvoljni podskupovi od $\{1, 2, \ldots, m\}$ sa β odnosno γ odnosno δ članova. Dalje je

$$B \wedge C \overset{\text{def}}{=} \sum_{X, Y} B^X C^Y (-1)^{I(X, Y)} E_{X \cup Y}$$

$$(1) \qquad (B \wedge C) \wedge D \overset{\text{def}}{=} \sum_{X, Y, Z} B^X C^Y (-1)^{I(X, Y)} D^Z (-1)^{I(X \cup Y, Z)} E_{X \cup Y \cup Z}.$$

Možemo pretpostaviti da su skupovi X, Y, Z dva po dva disjunktna; kako je svaki od skupova X, Y, Z sređen po veličini, bit će

$$(2) \qquad I(X \cup Y, Z) = I(X, Z) + I(Y, Z)$$

$$(3) \qquad I(X, Y \cup Z) = I(X, Y) + I(X, Z).$$

Zato u (1) možemo dalje nastaviti

$$(4) \qquad (B \wedge C) \wedge D = \sum_{X, Y, Z} (-1)^{I(X, Y) + I(X, Z) + I(Y, Z)} B^X C^Y D^Z E_{X \cup Y \cup Z}.$$

Na isti se način dobije da je $B \wedge (C \wedge D)$ upravo $(4)_2$, a time se dobije tražena asocijativnost.

8.4.1. Primjedba. Vektorsko množenje $(x, y) \to x \times y$ u Euklidskom prostoru R^3 nije asocijativno, kao što se lako pokazuje i to posebno zato što je $(x \wedge y) \wedge z$ komplanarno sa zagrađenim vektorima x, y.

8.5. Na osnovu asocijativnosti definira se induktivno vanjski produkt bilo kojeg konačnog niza članova iz $V_m^\wedge$.

8.6. Teorem. Vanjsko množenje je kososimetrično: svaka transpozicija faktora u $B \wedge C \wedge \ldots \wedge L$ prevodi rezultat u suprotan; specijalno, ako niz članova iz $V_m^\wedge$ ima bar dva jednaka člana, tada je odgovarajući vanjski produkt nula.

Posebno iz

$$x(\sigma) \in V^{(1)}, \quad (\sigma = 1, 2, \ldots, s) \qquad \text{izlazi}$$

$$x(1) \wedge x(2) \wedge \ldots \wedge x(s) = \sum_{f \in (1,2,\ldots,s)!} \operatorname{sgn} f \cdot x(f_1) \wedge x(f_2) \wedge \ldots \wedge x(f_s).$$

8.7. Linearna zavisnost vektora i vanjski produkt tih vektora.

⟶ **8.7.1. Teorem.** *Neka je n prirodan broj* ≥ 2; *n-član niz kontravarijantnih vektora*

(1) $$x(1), \ldots, x(n)$$

prostora V_m *od m dimenzija je linearno zavisan onda i samo onda ako je vanjski produkt tih vektora* $= \mathbf{0}$.

Uslov je nuždan: ako su vektori linearno zavisni, vanjski produkt im je nula. Naime, zbog zavisnosti vektora može se neki od njih npr. prvi, $x(1)$, izraziti linearno pomoću ostalih:

$$x(1) = c_2\, x(2) + \cdots + c_n\, x(n), \text{ pri } c_\nu \in K.$$

To zbog linearnosti produkta znači da je

$$x(1) \wedge x(2) \wedge \ldots \wedge x(n) = [c_2\, x(2) + \cdots + c_n\, x(n)] \wedge$$

$$x(2) \wedge \ldots \wedge x(n) = \sum_{\nu=2}^{n} c_\nu [x(\nu) \wedge x(2) \wedge \ldots \wedge x(n)] =$$

$$= 0 + \cdots + 0 = 0$$

(naime prvi i ν-ti faktor u [ ] međusobno su jednaki).

Uslov je dovoljan: ako je

(2) $$x(1) \wedge x(2) \wedge \ldots \wedge x(n) = 0,$$

tada su vektori (1) linearno zavisni. Kada bi naime vektori (1) bili linearno nezavisni, tada bi se u prostoru V_m mogla izgraditi baza (e_ν) sa $e_\nu = x(\nu)$ $(\nu = 1, 2, \ldots, n)$; time prema 6.7.2—3 vanjski produkti po n članova iz niza (e_μ) tvore bazu B prostora $V_m^{\wedge(n)}$; baza B ima upravo $\binom{m}{n}$ članova, pa zato nijedan od njenih članova ne smije biti $= 0$, protivno pretpostavci (2).

8.7.2. Posljedica. Vektori x, y, z euklidskog prostora R^3 linearno su zavisni onda i samo onda ako je $x \wedge y \wedge z = 0$.

9. ZADACI O TENZORIMA

1. Zadan je prostor V_m (npr. $m = 3$) i član $v \in V_m$. Ako pri *svakoj* bazi (e_i) prostora V_m promatramo koordinate v^i za koje je $v = v^i\, e_i$ pa ako promatramo tablicu: 1) $t^{ij} = v^i v^j$, 2) $t^{ijk} = v^i v^j v^k$, tada je t dvojako, odnosno trojako kontravarijantan tenzor nad V_m.

2. 1) Dokaži da je jedinična matrica δ^i_j mješoviti tenzor razreda $(1+1)$ nad prostorom V_m pri zadanoj bazi. 2) Svi tenzori razreda 2 kojima su sve komponente, pri svakoj bazi, međusobno jednake, nužno je oblika $k \cdot \delta^i_j$, gde je k konstanta.

3. Uočiti da je tenzor t razreda $(p+q)$ nad V određeno preslikavanje t Dekartovskog produkta $\{1, 2, \ldots, m\}^{p+q} \times B$, gde je B skup svih koordinatnih baza prostora V_m, pri čemu za baze $e=(e_i)$, $e'=(e_{i'}) \in B$ veze $e_{i'}=a^i_{i'} e_i$ imaju za posljedice veze iz § 2.4. među odgovarajućim koordinatama od t u bazi e i bazi e'.

4. Zadan je prostor $V=V_m$ (npr. $V_m=R_3$) i uređen par (1, 2) brojeva; promatraj tenzorske produkte $V \otimes V^{\star(2)}$, $V^{\star(2)} \otimes V$, $V^\star \otimes V \otimes V^\star$. Da li su ti vektorski prostori: a) različni, b) izomorfni?

5. Neka su p, q članovi iz N; tada za zadan prostor V nad tijelom K ima $\frac{(p+q)!}{p!\,q!}$ različitih tenzorskih produkata prostora V koji su p puta kontravarijantni i q puta kovarijantni; svi su ti prostori međusobno izomorfni.

6. Neka u pravokutnom koordinatnom sistemu prostora R^3 vektor $y=(y^i)_i$ zavisi od parametra α; da li su 1) $\left(\frac{dx^i}{d\alpha}\right)$, 2) $\frac{d^2x^i}{d\alpha^2}$ koordinate vektora? Ako jesu, radi li se o kontravarijantnom ili kovarijantnom vektoru?

7. 1) U koordinatnom prostoru R^3 zadana je funkcija $f=f(x^1\,x^2\,x^3)$ s neprekidnim derivatima $\frac{\partial f}{\partial x^i}$; dokaži da je grad $f=\left[\frac{\partial f}{\partial x^i}\right]$ kovarijantan vektor. Konkretizirati npr. $f=(x^1)^2+(x^2)^2+(x^3)^3$. 2) Ako je x, $y \in R^3$, dokaži da su veličine $(y_i - x_i)_i$ $(i=1, 2, 3)$ koordinate kontravarijantnog vektora nad R^3. 3) Dokaži da su koeficijenti diferencijalne forme $ds^2=(dx^1)^2+(dx^2)^2+(dx^3)^2$ komponente kovarijantnog tenzora; dokaži da u polarnim sfernim koordinatama r, γ, θ komponente glase: $g_{11}=1$, $g_{22}=r^2$, $g_{33}=r^2\sin^2\varphi$, a inače $g_{ij}=\delta_{ij}$.

8. U prostoru R^3 s ortogonalnom bazom uzeti stupce matrice

$$c=\begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 3 \\ 0 & 3 & 4 \end{bmatrix}$$

kao novu koordinatnu bazu; kako glasi dualna baza?

9. *Napetost kao primjer kovarijantna tenzora razreda* $(0+2)$.
Pođimo od nekog elastičnog tijela u R^3 pa neka u koordinatama $y^1 y^2 y^3$ element luka unutar tog tijela glasi (1) $ds_0^2=a_{ij}\,dy^i\,dy^j$; tu su a_{ij} zadane funkcije varijablâ y^1, y^2, y^3. Neka elastična deformacija tijela T bude dana relacijama $x^i=f^i(y^1 y^2 y^3)$ $(i=1, 2, 3)$; neka u tako deformiranom tijelu diferencijal luka bude

$$ds^2=g_{\alpha\beta}\,x^\alpha\,x^\beta,$$

tada je $$dy^{\alpha} = \frac{\partial y^{\alpha}}{\partial x^{i}} dx^{i},$$ pa izraz (1) postaje

$$ds_0^2 = h_{\alpha\beta}\, dx^{\alpha}\, dx^{\beta}$$ pri čemu je

$$h_{\alpha\beta} = a_{ij} \frac{\partial y^{i}}{\partial x^{\alpha}} \frac{\partial y^{j}}{\partial x^{\beta}}.$$

Dalje je $$ds^2 - ds_0^2 = 2\, \varepsilon_{\alpha\beta}\, dx^{\alpha}\, dx^{\beta},$$ gdje je

$$\varepsilon_{\alpha\beta} = \frac{1}{2} (g_{\alpha\beta} - h_{\alpha\beta}).$$

Tako smo dobili veličine $\varepsilon_{\alpha\beta} = \varepsilon_{\alpha\beta}(x^1, x^2, x^3)$ koje zavise od odabranih koordinata u deformiranom tijelu. Za svaki drugi koordinatni sistem $x^{j'}$ bilo bi analogno

$$ds^2 - ds_0 = 2\, \varepsilon_{\alpha'\beta'},\, dx^{\alpha'}\, dx^{\beta'},$$ pri čemu je

$$\varepsilon_{\alpha'\beta'} = \frac{\partial x^{i}}{\partial \alpha'} \frac{\partial x^{j}}{\partial \beta'} \varepsilon_{ij}.$$

Drugim riječima, funkcije $\varepsilon_{\alpha\beta}$ $(\alpha, \beta = 1, 2, 3)$ definiraju koordinate tenzora razreda $(0+2)$. Taj se tenzor zove *tenzor napetosti* i vrlo je važan u teoriji elastičnosti.

10. Napisati obrasce za transformaciju svih vrsta tenzora razreda: 1) 3; 2) 4; 3) 5.

11. Ako su t^{ij}, u^{ij} tenzori nad V, dokazati da je $t \otimes u$ tenzor razreda $(4+0)$.

12. Tenzorski produkt od t^{ij}, u_{ij} je tenzor razreda $(2+2)$.

13. Ako je t^{ij} tenzor, prikaži ga kao sumu simetričnog tenzora i kososimetričnog tenzora. Je li taj prikaz jedinstven?

14. Ako je t_j^i tenzor razreda $(1+1)$, dokazati da i kofaktori $f\; t_j^i$ obrazuju tenzor razreda $(1+1)$.

15. 1) Je li jednakost $t = u$ među tenzorima t, u nezavisna od baze promatranog prostora? 2) Je li u označavanju koordinatâ tenzora t važno ime (oznaka) pojedinih indeksa? Npr. mogu li se koordinate tenzora t razreda $(1+1)$ označiti sa t_j^i, t_i^j, t_β^α, t_y^x?

16. Ako su v_i koordinate kovarijantnog vektora v, tada su razlike

$$\frac{\partial v_i}{\partial x^j} - \frac{\partial v_j}{\partial x^i}$$

koordinate kososimetrična kovarijantna tenzora razreda $(0+2)$.

17. Postoji li suma tenzora: 1) t^i, u^j; 2) t^i, u_j; 3) t_i, u^j; 4) t_i, u_j? Odredite razred kontravarijantnosti i razred kovarijantnosti od $t+u$, ukoliko $t+u$ postoji.

18. Isto pitanje za tenzorski produkt $t \otimes u$.

19. Odredi $t \otimes u$ tenzorâ: 1) t^{ij}, u^{ij}, 2) t^{ij}, u_{ij}; 3) t_j^i, u_j^i; 4) t_{ij}, u^{ij}.

20. Podmladi tenzor t_l^{ijk} po indeksu
1) $i=l$; 2) $j=l$; 3) $k=l$. Dobiju li se jednaki tenzori?

21. Na koliko se načina može provesti jednokratno podmlađivanje ili sažimanje tenzora razreda 1) $(2+3)$; 2) $(3+2)$; 3) $(4+3)$; 4) $(p+q)$?

22. Na koliko se načina može provesti dvojako sažimanje tenzora iz zad. 21?

23. Tenzoru t^i nad prostorom R^3 s bazom (e_i) odredi kososimetrični tenzor $A\,t$ (isp. § 6.7.3).

24. Isto pitanje za tenzor t^{ij}. Koliko $A\,t$ može imati koordinata $\neq 0$?

25. Nađi tenzorski produkt tenzorâ: 1) t^{ijk}, u_{jk}^{i} 2) t^{ijkl}, u_{ijkl}; 3) t_{kl}^{ij}, u_{lk}^{ij} i provedi sažimanje produkta po a) prvoj gornjoj i prvoj donjoj varijabli, 2) posljednjoj donjoj i posljednjoj gornjoj varijabli.

26. Nađi vanjski produkt $x\wedge y$ vektora 1) $x=[2,\ 3,\ 4]^T$, $y=[1, -3,\ 6]^T$.

27. Radimo u Euklidskom prostoru R^3. 1) Za vektorsko množenje vrijedi $(x\times y)\times z+(y\times z)\times x+(z\times x)\times y=0$. Može li se tu znak $\times$ zamijeniti sa $\wedge$? 2) Vrijedi $(a\times b)\times(c\times d)=b\ (acd)-a\ (bcd)$, stavljajući $(x\,y\,z)=\det\,[x, y, z]$. Smije li se tu znak $\times$ zamijeniti sa $\wedge$?

28. Dokazati da je $x\wedge y\wedge\ldots\wedge z=A\,(x\otimes y\otimes\ldots\otimes z)$, tj.

$$\bigwedge_{i=1}^{r} x(i)=A\bigotimes_{i=1}^{r} x(i).$$

29. Navesti nekoliko članova iz $V^\wedge$ i razmatrati vanjske algebre $V^\wedge$ ako V znači prostor: 1) R^2, 2) R^3, 3) R^4.

30. Neka je $f(u,\ v)$ bilinearna regularna forma nad V, tj. pri $u,\ v\in V$ je $f\ (u,\ v)\in K$; ako je dim $V\in N$, tada za svako $v^\star\in V^\star$ postoji jedno jedino $v\in V$ za koje je $v^\star\ (u)=f\ (u, v)$ za svako $u\in V$; drugim riječima preslikavanja $u\in V\to f\ (\mathrm{u},\ v)$ pri $v\in V$ daju sve članove iz $V^\star$. Konkretiziraj f.

Literatura

Anđelić [2]; Bilimović [1]; Bourbaki [1]; Kočin [1]; Križanić [1]; Kurepa Sv. [1]; Lang [1]: Lichnerowicz [1].

POGLAVLJE 35.

HISTORIJAT ALGEBRE

1. POČECI ALGEBRE

Algebra kao nauka o brojevima i o operacijama s brojevima vanredno je stara nauka. Teško je stvoriti sliku kako i gdje se algebra počela razvijati. U svakom slučaju, kao plod dugog iskustva i u borbi s prirodnim silama i s okolinom a u nastojanju da očuva sebe i svoju vrstu i da život svoj učini mogućim i što podesnijim čovjek je došao do saznanja o broju, o operacijama i zakonima o brojevima, o vrstama brojeva i njihovoj primjeni i o najraznovrsnijim nadgradnjama brojeva (vektori, matrice, tenzori itd).

Vrlo je dalek put od primitivnih predodžbi o broju, zapisivanju broja, računanju pa do današnjeg stanja u matematici u kojem algebra zauzima jedno od najznačajnijih mjesta.

2. POČECI POJMA BROJA, BROJENJA

I najprimitivniji čovjek i najzaostalija ljudska plemena imaju smisao, instinkt i predodžbu o broju, premda u vrlo nejednakoj mjeri i opsegu. Zanimljivo je da i nekoje ptice (npr. vrana) pa i nekoji kukci (npr. genus Eumenus) imaju neki instinkt za broj (naravno za vrlo male brojeve 1, 2, 3, 4); poznato je da se pokušavalo dresirati pse i konje da broje. Zanimljivo je da i čovjek na današnjem visokom stupnju svojeg razvoja nema jasne predstave o veličini broja iznad 6, osim ako se služi važnom operacijom — brojenjem i uspoređivanjem. Bez uspoređivanja raznovrsnih predmeta i skupova ne može se ni zamisliti upotreba i svjesni postanak broja.

Također treba razlikovati poimanje *pojedinih brojeva* od poimanja skupa svih brojeva određene vrste. Tako npr. premda se s pojedinim prirodnim brojevima radilo i u prethistorijsko doba, shvatanje skupa svih prirodnih brojeva još nije provedeno dosljedno čak ni u grčkoj matematici premda u radovima Platona (—430. do—340), Euklida (—365? do —275?), Diofanta (?3. st.) ima o tome raznih istraživanja (tako npr. u Platonu se nalazi misao da parnih i neparnih prirodnih brojeva ima jednako mnogo); naime, bez principa potpune indukcije ili kojeg ekvivalentnog svojstva ne može se ispravno shvatiti skup svih prirodnih brojeva.

Posebne poteškoće su postojale u otkrivanju i shvatanju negativnih brojeva, iracionalnih brojeva i kompleksnih brojeva.

3. STAROEGIPATSKA ALGEBRA

3.1. *Kalendar iz — 4241. godine kao mjerilo matematičkog standarda.* Valjda prvi poznat događaj u zbivanjima ljudi predstavlja godina 4241. prije naše ere kada se u starom Egiptu uveo kalendar: godina se sastojala od 12 mjeseci po 30 dana i 5 dana za svetkovine; a kako je kalendar bio vrlo tačan, prirodno je pretpostaviti da je on osnovan na osnovu velikog životnog iskustva i razvijenih matematičkih preračunavanja.

3.2. Već u vrijeme drevnog carstva u Egiptu (oko 3600—2700. godine prije naše ere) matematika je u Egiptu bila sigurno na relativno visokom stupnju; naime, u to doba građene su velelepne faraonske grobnice — piramide —, građeni veliki kanali, nasipi, rezervoari za vodu, vršena premjeravanja zemljišta, popis zemlje, stoke, ljudi, zlata, a i znanje u astronomiji je već bilo toliko da su bili u stanju da predskazuju kada će Nil plaviti.

3.3. Iz toga doba potječe i prvo poznato matematičko ime: Imhotep, arhitekt i matematičar.

A jasno je da takva djelatnost nosi u sebi mnogo matematičkih situacija i radnji.

3.4. *Ahmesova računica.* Iz vremena srednjeg carstva (2000—1710. prije n.e.) imamo dragocjene podatke i najstarije matematičke knjige, a to su *Londonski papirus ili Papirus Rhind* (oko — 18 st.) ili *Ahmesova računica*[1] te *Moskovski papirus* (oko — 20 st.). Moskovski papirus ima 25 zadataka a londonski 85 zadataka.

3.5. *Računske operacije.* Zanimljivo je da su Egipćani izvodili množenje pomoću udvajanja a dijeljenje pomoću raspolavljanja. Od razlomaka su najprije radili služeći se sa $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}$, a kasnije i sa $\frac{1}{3}, \frac{2}{3}$, a najzad sa $\frac{1}{n}$.

Ostale razlomke prikazivali su aditivno pomoću prethodnih; npr. $\frac{4}{5} = \frac{1}{30} + \frac{1}{10} + \frac{2}{3}$; za razlomke $\frac{2}{3}$ (n neparno) Londonski papirus daje razlaganja za $n=3, 4, 5, \ldots, 101$; tako npr. $\frac{2}{3} = \frac{1}{2} + \frac{1}{6}$, $\frac{2}{101} = \frac{1}{101} + \frac{1}{202} + \frac{1}{303} + \frac{1}{606}$.

3.6. *Linearne jednadžbe.* Egipćani su rješavali linearne jednadžbe *metodom pogrešne podstavke.* Tako npr. jednadžbu $x + \frac{1}{7}x = 19$ iz 24. zadaće Londonskog papirusa rješava tako da stavi približno $x_1 = 7$ a onda to x_1 ubacuje u lijevu stranu jednadžbe i nalazi određenu vrijednost $r_1 = x_1 + \frac{1}{7}x_1$; zatim određuje $x_1 \frac{r}{r_1} = x$ kao pravo rješenje. Općenito, ako je $\left(\frac{a_1}{b_1} + \frac{a_2}{b_2} + \cdots + \frac{a_n}{b_n}\right) x = c$, stavi se $x_1 = b_1 b_2 \ldots b_n$ pa se izračuna $\left(\frac{a_1}{b_1} + \cdots + \frac{a_n}{b_n}\right) x_1 = c_1$, a onda se nađe traženo rješenje x_1 u vidu $x = x_1 \cdot \frac{c}{c_1}$.

[1]) Ahmes je ime egipatskog skriba ili pisara; vrlo je bio cijenjen poziv skriba. Rhind je ime Engleza koji je u 19. st. otkrio Ahmesovu računicu.

3.7. *Jedan od prvih sistema jednadžbi.* U Ahmesovoj računici nalazi se i jedan zadatak koji u današnjoj simbolici daje ovaj sistem jednadžbi: $x^2+y^2=100$, $y=\frac{3}{4}x$. To je prvi poznat sistem jednadžbi; navedeno je i ispravno rješenje $x=8$, $y=6$ a dobiveno je »*metodom pogrešnog položaja*«.

4. MEZOPOTAMIJSKA ALGEBRA. GLINENE PLOČICE

4.1. U Mezopotamiji — u prostoru između Eufrata i Tigrisa — u vremenu od četiri tisućljeća do naše ere bile su razvijene pojedine države; specijalno je najprije bila država Sumerana, na jugu i država Akadijaca na sjeveru; te su države pokorili, sjedinili i proširili Babilonci i najzad Asirci. U tom međurječju razvila se matematika do dosta visokog stupnja; pisali su na glinenim pločicama pa su se zato mnogi njihovi rezultati sačuvali. Do danas je od oko 500.000 sačuvanih i sakupljenih pločica dešifrirano samo nekoliko stotina.

4.2. *Počeci pozicionog* ili *mjestovnog sistema.* Na tom prostoru razvio se polupozicioni sistem sa bazom 60 u višim društvenim krugovima i bazom 10 u nižim društvenim krugovima.

4.3. *Algebarske jednadžbe.* Babilonci su znali rastavljati pojedine polinome na produkte polinoma stupnja ≤ 2 i time rješavati jednadžbe. Dokumenti o matematici Babilonaca odnose se na vremensko razdoblje od oko 2000 godina (—2186.) do početka naše ere).

4.3.1. Babilonske glinene pločice sadrže rješenja raznih *kubnih jednadžbi* oblika $x^3+b\,x^2+c=0$; oni su takve jednadžbe svodili na standardni oblik $y^3+y^2=d$ (množeći polaznu jednadžbu sa b^{-3} i stavljajući $y=x/p$); ako je $d>0$, tada se y dobije pomoću tablica od n^3+n^2 ukoliko je d u tablicama.

Upute, zapravo recepti za rješavanje zadataka, nisu ničim obrazloženi niti se izričito zahtijeva da se rezultat provjeri. Vrlo je vjerovatno da je takva situacija nastala zato što su rezultati i metode bili čuvani kao tajna povlaštenih krugova koji su do gornjih rezultata dolazili.

4.3.2. Pomoću svojih numeričkih tablica Babilonci su riješili oko 55 posebnih sistema jednadžbi tipa

$$x\,y=600$$

$$(a\,x+b\,y)^2+c\,x+d\,y=e.$$

Babilonci su kvadratne iracionalitete aproksimirali na osnovu ispravne formule $(a^2+b^2)^{1/2}=a^2+\frac{b^2}{2a}$ (javlja se kasnije nakon skoro 2000 godina kod Herona iz Aleksandrije) kao i pomoću neispravne formule $(a^2+b^2)^{1/2}=a^2+2\,a\,b^2$.

4.3.3. Godine 1939. otkopani su u Suzama novi tekstovi na klinastom pismu koji su 1950. odgonetnuti; time se došlo do novih saznanja o dosta visokom matematičkom znanju Babilonaca, a posebno jedna pločica sadrži zadatak koji danas algebarski rješavamo *jednačinom 8. stepena* (dotada se znalo samo za probleme vezane uz jednačine stepena ≤ 6).

4.4. *Tragovi negativnih brojeva.* Vanredno je zanimljivo da u babilonskoj matematici imamo tragove negativnih brojeva i to u bar 3 navrata u vezi s rješavanjem simultanih jednadžbi. Vrijedno je istaknuti da babilonski astronomi u —4 stoljeću ispravno barataju s pravilima o množenju relativnih brojeva; međutim, to znanje je palo u zaborav!

4.5. *Osvrt na matematiku Babilonaca.* Kako je država Babilonaca, odnosno Asiraca, imala vrlo velik ugled i trajale su dosta dugo, sigurno je da je uticaj tih država bio velik ne samo u političkom nego i u kulturnom i tehničkom pogledu; posebno se može pretpostaviti da su neki rezultati matematike tih država prešli u Indiju, Kinu i Egipat, a time preko Grka i Arapa također u Evropu.

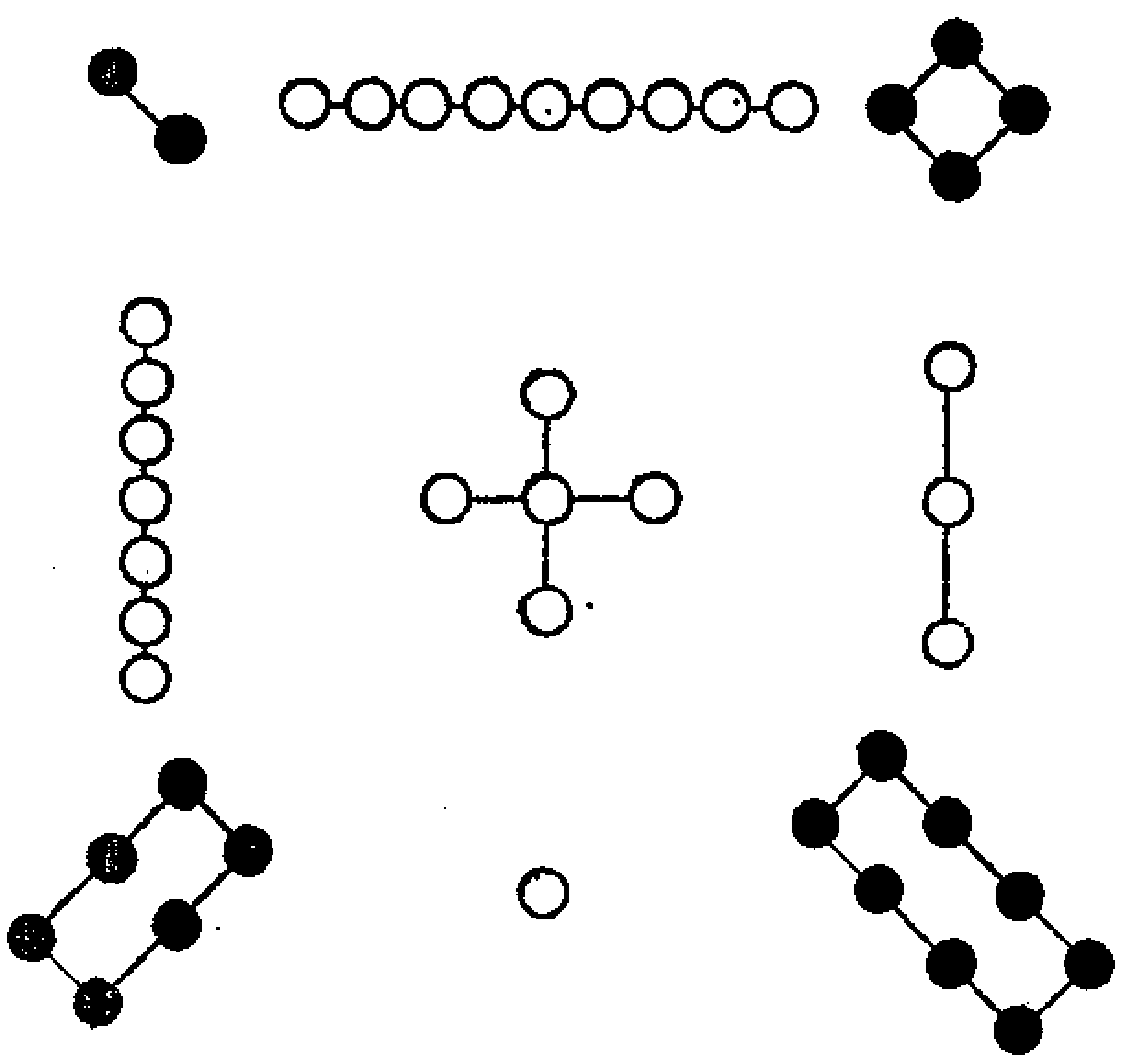
U saglasnosti sa despotskim i apsolutističkim političkim uređenjem u tim starim carstvima kao i u Egiptu, i matematika je u njima nosila karakter despotsko-normativan i receptualan, odnosno empiričan; matematičko znanje je kao tajna prenošeno s oca na sina, odnosno od žreca na žreca.

Istom je u demokratskoj Grčkoj došlo do procvata matematike temeljene na obrazlaganjima i dokazima.

5. ALGEBRA U KINI

5.1. Već u 13. st. prije naše ere nalaze se u Kini brojevi zapisani u decimalnom sistemu; zapisivanje je ostvarivano pomoću štapića, a pisalo se na kori drveta; zato i nema mnogo ostataka, pogotovo što u —213. godini po zapovjedi utemeljitelja dinastije Tzin moralo se spaliti sve knjige i sve što je bilo napisano.

5.2. Poznata je *knjiga o permutacijama* (*I-king*) vjerojatno iz 12. st. prije n. e. U njoj je specijalno *Pa-kua* (8 kua) — zapravo svi tročlani nizovi od dva predmeta: — (*yang, Muško*) i — — (*ying, žensko*); ako se prvi simbol uzme za 1 a drugi za 0, dobiju se tako dijadski prikazi brojeva 0, 1, 2, . . . 7. U tom djelu dolazi i magični kvadrat (Sl. 35.5.2.1) ostvaren kao ornament pomoću »muških« (neparnih) bijelih brojeva — kuglica i pomoću ženskih (parnih) crnih kuglica (Sl. 35.5.2.2).



Sl. 35.5.2.1.

4	9	2
3	5	7
8	1	6

Sl. 35.5.2.2.

5.3. Vjerojatno iz vremena dinastije HAN (vladala je od 206. prije naše ere do 184. god. n. ere) sačuvalo se djelo nepoznata autora: *Vještina računanja u 9 poglavlja*; posebno, 7. poglavlje govori o višku i manjku — metoda rješavanja linearne jednadžbe s jednom nepoznanicom uz pretpostavku da znamo jedno rješenje naviše i jedno rješenje naniže; 8. poglavlje obrađuje račun na šahovskoj ploči: linearna jednadžba se svojim koeficijentima predstavlja u jednom stupcu tablice pa se s tim podacima radi direktno; metoda nas podsjeća na današnju matričnu.

5.4. No pojedina imena su sačuvana istom iz 3. st. (?); tako npr. Liu Hui izračunava $\pi=3,14159$, a Sun Ce (Sun Tzi) traži najmanji broj koji podijeljen sa 3 daje ostatak 2, a ostatak 3 pri diobi sa 5, odnosno ostatak 2 pri diobi sa 7.

5.5. U djelu »*Dragocjeno ogledalo četiri elementa*« koje je kineski matematičar Ču Ši Kej objavio 1303. nalazi se »*Pascalov trokut*« pod nazivom »*dijagram stare metode kako da se nađu potencije*«. Ta 4 elementa u pitanju jesu proizvoljne nepoznanice koje dolaze pri rješavanju neodređenih jednadžbi. Vješto rješava numeričke jednadžbe višeg reda.

6. GRČKA ALGEBRA

6.1. *Prvi algebarski teorem.* Grci su znatno unapredili algebru, uglavnom na geometrijskoj osnovi. Poznata je *Timaridova epantema* (cvijet): pitagorovac Timarid od Parosa (oko —380.) promatra sistem jednadžbi koji u današnjem načinu pisanja glasi:

$$\begin{aligned} &x_1+x_2+\cdots+x_n=s\\ &x_1+x_2=a_1\\ &x_1+x_3=a_2\\ &\cdot\ \cdot\ \cdot\ \cdot\ \cdot\\ &x_1+x_n=a_{n-1} \end{aligned}$$

i nalazi

$$x_1=\frac{1}{n-2}(a_1+a_2\cdots+a_{n-1}-s).$$

Time je prvi put izrečen jedan algebarski teorem.

6.2. *Hipokrat od Hiosa* (rođen oko 470. prije n. e.; razlikovati ga od liječnika istog imena) uveo je naziv *dynamis* za kvadrat broja, odakle današnji latinizirani oblik *potencija* za stepen ili moć; razradio je metodu dokaza pomoću metode reductio ad absurdum (svođenje na protivuslovlje); problem udvostručenja kocke sveo je na određivanje veličina x, y za koji je $a:x=x:x=y:2a$ (odakle $x^3=2a^3$); riješio je problem koji bi danas bio prikazan jednadžbom $x^2+\left(\frac{3}{2}\right)^{1/2}ax=a^2$. Poznate su Hipokratove lunule ili Hipokratovi mjesečići.

6.3. *Euklid* (—3. st.). Euklid je živio u —3. stoljeću koje je zlatno stoljeće za grčku matematiku jer su u tom stoljeću živjeli Euklid, Eratosten, Arhimed i Apolonije.

Glavno Euklidovo matematičko djelo zove se ΣΤΟΙΧΕΙΑ (*Elementi*) — neke vrste enciklopedija ondašnje grčke matematike u 13 knjiga. Stoljećima su te knjige služile kao udžbenici; prevođene su na mnogobrojne jezike. Na naš jezik ih je preveo i dao im komentar *A. Bilimović* u izdanju Matematičkog instituta Srpske akademije nauka (Beograd 1949—1957).

Specijalno se aritmetika i algebra obrađuju naročito u knjigama: V—X. Tako npr. zakon distribucije množenja prema zbrajanju dolazi u II (1), tj. u knjizi I § 1), V (1, 2, 5), VII (5, 6); kvadratna jednadžba $x^2+ax=a^2$ (*zlatni rez*) rješava se, naravno na geometrijski način, u II (11) a kvadratne jednadžbe $ax^2-bx+c=0$, $ax^2+bx-c=0$ u VI (28, 29). Već u VII (1) tumači se *Euklidov algoritam dijeljenja* a u § 2 već se pomoću toga određuje najveća zajednička mjera brojeva. U VII (24—26) dokazuju se osnovni stavci o prostim i međusobno prostim brojevima; u §§ 31—32 dolazi rastavljanje brojeva na proste faktore pri čemu se kao u § 1 uzima automatski da je skup prirodnih brojeva bez beskonačnih regresija; dalje se određuje najmanji zajednički kratnik zadanih brojeva. U IX (20) se dokazuje da *prostih brojeva ima beskonačno mnogo*; u IX (36) se dokazuje teorem o *savršenim brojevima.* U VII (16) obrađuje se komutativni zakon za množenje. U Euklida nema nigdje numeričkog primjera.

6.4. *Arhimed* (—287. do —212), slavni matematičar iz Sirakuze, jedan od najvećih matematičara uopće, radio je dosta i s algebarskim problemima, premda uglavnom na geometrijski ili mehanički način.

Arhimed je sistematski izučavao duljine crta, ploštine i zapremine raznih tjelesa, pa je s tim u vezi imao velik uspjeh jer je taj problem riješio za razne skupove (npr. kugla, cilindar, rotacione površine 2. stepena, odrezak parabole itd.), a s druge strane na tom putu došao do novih metoda i novih činjenica (primjer beskonačnih redova, razlomljenih potencija).

6.4.1. U djelu *O kugli i valjku* I, II našao je pravilo kako zapremina tih tijela zavisi od r i visine, posebno ispituje kako kuglu treba razrezati ravninom na dva dijela pa da im se zapremine odnose kao zadani brojevi a, b; odnosno, kako se zadana veličina a treba podijeliti na dva dijela x, $a-x$ pa da bude

$$x : m = n^2 : (a-x)^2; \tag{1}$$

tu se radi o *kubnoj jednadžbi* a Arhimed je rješava uklapanjem dviju geometrijskih sredina između dvije zadane veličine.

U današnjoj simbolici, dovoljno je tražiti sjecište parabole

$$(a-x)^2 = \frac{n^2}{a} y$$

i hiperbole $xy = am$, pa da se nađe i rješenje kubne jednadžbe (1).

6.4.2. Istom metodom Arhimed rješava problem da se zadanoj kružnici upiše pravilan 7-kut (Arhimedovo djelo »*O 7-kutu*« nije nađeno u originalu, a arapski prevod je odgonetnut 1927).

6.4.3. U teoremu 8 drugoga dijela govori o potenciji s razlomljenim eksponentom dokazujući da je omjer većeg segmenta kugle i manjeg segmenta kugle manji od $a^2 : b^2$ a veći od $a^{3/2} : b^{3/2}$, pri čemu je a ploština veće kapice, a b ploština manje kapice,

6.4.4. U djelu *Pješčanik* (ψαμμιτης) nastoji Arhimed na zgodan način prikazati vrlo velike brojeve $\left((\text{do } 10^{8\cdot 10^{16}}\right)$ i radi implicitno s današnjim pravilom $10^m \cdot 10^n = 10^{m+n}$; dolazi do zaključka da bi broj zrna pijeska u kugli koja bi obuhvatala zvijezde stajačice bio ispod 10^{63}.

6.4.5. *Heliosovo stado.* Sa velikim brojevima je vezan i Arhimedov problem o *Heliosovu stadu* krava i bikova. Stado se sastojalo od krava i bikova boje ili bijele ili sive ili mrke ili šarene; neka je B broj bijelih bikova a b broj bijelih krava; analogno imamo S, s za sivu boju, $Š$, $š$ za šarenu boju te M, m za mrku boju; tada je prema uslovima zadatka bilo:

$$B - Š = \frac{5}{6} S$$

$$S - Š = \frac{9}{20} M$$

$$M - Š = \frac{13}{42} B$$

$$b = \frac{7}{12}(S+s), \qquad s = \frac{9}{20}(M+m), \qquad m = \frac{11}{30}(Š+š)$$

$$š = \frac{13}{42}(B+b).$$

Odrediti sastav stada (najmanje pozitivno rješenje).
Izlazi

b=7 206 360, B=10 366 482, m=3 515 820, M=7 358 060

s=4 893 246, S= 7 460 514, $š$ =5 439 213, $Š$ =4 149 387.

6.4.6. Arhimed u mnogo navrata traži *približna i praktična rješenja*; tako npr. nalazi da je broj π smješten između $3\frac{10}{71}$ i $3\frac{10}{70}$, što znači grešku $<\frac{1}{500}$.

6.5. *Diofant* (3. st.). Jedini »čisti« algebrista u Grčkoj i osnivač prave algebre bio je veliki Diofant (3. st. n. e.); njegova *Aritmetika* je najbolja algebra starog doba. On je odijelio algebru od geometrije, znatno unapredio simboliku, rješava kvadratne jednadžbe $a x^2 + b x + c = 0$ u svakom slučaju osim ako su a, b, c negativni brojevi, no promatra samo pozitivno rješenje i to jedno jedino čak i onda ako su oba rješenja pozitivna. Rješava i kubnu jednadžbu $x^3 - 3x^2 + 3x - 1 = x^2 + 2x + 3$. Nije imao slijedbenika sve do 17. stoljeća (Bachet, Fermat).

7. POZICIONI, MJESTOVNI, SISTEM SA NULOM

7.1. *Pozicioni sistem u Maja.* Pozicioni sistem sa nulom nastao je najprije u Srednjoj Americi (poluotok Jukatan u Meksikanskom zalivu) a razvili su ga indijci Maja u vremenu od preko 2000 godina sve do španjolskog osvajanja tih oblasti u 16. vijeku. Već u 4. stoljeću prije naše ere narod Maja — narod pronalazač kukuruza — imao je pozicioni sistem sa nulom za prikazivanje brojeva. Baza računanja je bio broj 20; znak za nulu je bila slika školjke (poput zatvorena oka), a cifre 1—19 su se gradile pomoću tačkica i horizontalnih paralelnih crtica; npr. 15= $\equiv$, 16 = $\dot{\equiv}$, 17 = $\ddot{\equiv}$, 18 = $\dddot{\equiv}$, 19 = $\ddddot{\equiv}$ (Maja su pisali u stupcima, odozdo prema gore; i zdesna nalijevo).

7.2. *Indija.* Nezavisno od Maja pozicioni sistem i to decimalni sistem sa nulom razvio se u Indiji, u Aziji; posebno ga je poznavao Hindus Aryabhata (r. 476. na gornjem Gangesu) početkom 6. stoljeća, no dosad prvi pisani dokaz o decimalnim ciframa i nuli potječe iz 595. godine (odnosno godine 346. razdoblja »cedi«); sam oblik nule nam nije poznat sve do 9. vijeka: bio je oblika tačke pa kruga; 738. se prvi put javlja nula u obliku kružnice na jednoj bakrenoj ploči u Indiji.

Današnji decimalni sustav i njegovi znakovi razvili su se u Indiji vjerojatno u vezi s računanjem na abaku posutu pijeskom ili prašinom tim prije što u sanskrtu ima nezavisnih posebnih riječi za potencije 10, $10^2, \ldots 10^9, 10^{10}$; sistem se toliko razvio da ga Ariabhata (5/6 st.) i Brahmagupta (6. st.) ni ne tumače u svojim djelima. U Siriji se sistem spominje 666. g., a Arapi su ga primili i raširili u 7. i 8. stoljeću.

7.3. *Arapi. Perzijci. Naziv Al gebr.* Prvu arapsku matematiku u indijskom sustavu napisao je perzijski matematičar Mohamed ibn Musa zvan Al Kowarizmi[1]; živio je u Bagdadu oko 825. godine kao knjižničar na dvoru halifa al Mamuna, sina Harum al Rašida (i otac i sin mu bili su zaštitnici matematike); rođen je pod imenom Muhamed ibn Musa u današnjoj Hivi; njegova algebra se zvala *Al-gebr w'al muqabalah* a napisana je oko 825. godine. To djelo i njen pisac su vrlo znatni u historiji matematike, pa će Bagdad — nov grad osnovan oko 762. — biti preko pet stoljeća jako matematičko središte, u kojem uz muhamedance djeluju i hebrejski i kršćanski matematičari. *Iz naslova toga djela nastao je naziv »algebra«* te nove matematičke discipline; inače, sama riječ *Al-gebr* (lat. restauratio) značila je *uspostavljanje* (restauriranje), a operacija je na jednadžbi služila tome da se prenošenjem članova zadana jednadžba tako ekvivalentno preinači da dolaze samo pozitivni članovi. Onaj drugi izraz u naslovu *Al muqabalah* (lat. oppositio) iskazivao je operaciju da se uoče dva istoimena člana na raznim stranama jednadžbe, pa se manji član ispusti a veći zamijeni razlikom između toga većeg i onog manjeg člana na suprotnoj strani jednadžbe.

Al-Kowarizmova algebra je imala velik uticaj na razvoj matematičke misli; djelo je bazirano na Brahmaguptinoj algebri kao i uopće na indijskoj matematici kao i na grčkoj matematici. Djelo sadrži razrađen dekadski brojevni sistem sa nulom pa je u tom pogledu odigralo presudnu ulogu. Prevedeno je na latinski u 12. v.

7.4. *Algoritmisti. Abakisti.* Po Al Kowarizmu, nazivani su u Evropi 12—14. stoljeća pristaše dekadskog sistema *algoritmistima* za razliku od njihovih protivnika tzv. *abakista* koje je predvodio papa Silvestar II (rođen Gerbert, 950—1003), a koji su se služili rimskim brojevnim sistemom i abakom usavršenim time što su za »kuglice« i »marke« uzimali žetone, »apices« — brojke 1, 2, . . . 9 (bez nule!).

Knjiga Al gebr . . . je stavljana u protivutežu sa poznatom školskom knjigom Aritmetika (Quadrivium) što ju je napisao Rimljanin Boethius (475—526), a koja je bazirana na udžbeniku Aritmetici koju je oko 100. godine napisao Nikomah; te dvije aritmetike su u srednjem vijeku bili priznati udžbenici matematike.

7.5. *Kršćanska matematika.* Arapska matematika imala je uticaja na kršćansku matematiku u Španiji, Italiji, Francuskoj. Najpoznatija algebra srednjeg vijeka

---

1) Iskrivljavanjem nastala je odatle i riječ *algoritam* (postupak); isp. niže § 7.5.

bilo je djelo Leonardo Fibonacci: *Liber abaci* (Računica) 1202. (prerađeno 1228).[1] Po naslovu bi se moglo zaključiti da je knjiga pisana u stilu abacista; međutim, djelo je pisano u drugom duhu, posebno na bazi dekadskog pozicionog sistema koji je autor izučio u Alžiru gdje mu je otac bio carinski činovnik. Leonardo je rođen u Italiji, Pisa, pa se osim pravog prezimena Fibonacci vrlo često govori naprosto o Leonardu Pisano ili Leonardu iz Pize (1175—1250).

8. RENESANSA (PREPOROD). KULMINACIJA

8.1. *Kulminacija talijanskih matematičara.* U poznoj renesansi vrlo velik i samostalan uspjeh postigli su talijanski matematičari riješivši opći oblik algebarske jednadžbe stepena 3. ili 4. Scipione del Ferro (1465—1526) koji je kao prvi matematičar djelovao na Sveučilištu u Bologni riješio je 1515. jednadžbu

$$x^3+a\,x=b. \tag{1}$$

N. Tartaglia je riješio jednadžbe oblika $x^3+p\,x^2=q$, i svoje rješenje saopćio Cardanu; Cardano je 1545. u djelu *Ars magna*, štampano u Nürnbergu, to rješenje razradio i 1545. objavio. U istoj knjizi je objavljeno i rješenje algebarskih jednadžbi stepena 4 koje je našao Ferrari oko 1540.

Vrhunac talijanskih istraživanja u algebri čini djelo Rafaello Bombelli, *Algebra, parte maggiore dell'aritmetica, divisa in tre libri*, Bologna 1572. To djelo sadrži sve što je dotada bilo dostignuto u algebri a posebno se odlikuje time što inženjer Bombelli *slobodno radi s imaginarnim brojevima* dokazujući da pri tzv. *nesvodljivu slučaju* kubne jednadžbe jednadžba ima tri realna rješenja (isp. 5 § 6.5.2). Dokazuje da se problem trisekcije kuta svodi na rješavanje kubne jednadžbe (v. 5. § 8.7.). Potencije nepoznanice $\underset{\smile}{1} = x$ označuje pomoću indeksa pa mu $\underset{\smile}{2}, \underset{\smile}{3}, \ldots$ označuje današnje $x^2, x^3, \ldots$ slično kao što je 1586. Stevin pisao ①, ②, ③, . . .

8.2. *Stevinova sinteza.* Simon Stevin (1548—1620), flamanski matematičar i inženjer u svojem djelu *Arithmétique* (Leyden 1585) razradio je decimalne razlomke pokazujući koliko su oni u primjenama praktičniji nego obični razlomci, zatim slobodno radi s negativnim brojevima i prvi put u historiji matematike dolazi do spoznaje *da oduzeti pozitivan broj znači isto što dodati negativan broj.* On kao statičar i tvorac trokuta sila svakako je do te spoznaje morao doći. Ipak, nije prihvatao imaginarne brojeve ali je prihvatao kao brojeve i iracionalne brojeve i jedinicu.

8.3. *François Viète* (1540—1603) (lat. oblik *Vieta*) — otac simboličke algebre. Premda su talijanski matematičari Ferro, Cardano, Tartaglia, Ferrari, Bombelli riješili jednadžbe 3. odnosno 4. stepena, ipak su oni to još radili više po receptu nego svijesno imajući jasno pred očima koje operacije treba izvoditi sa *općim koeficijentima* pa da se dođe do rješenja; oni su više radili s *pojedinim proizvoljnim primjerima* jednadžbi nego s *općim oblikom jednadžbe.* Oni naime još nisu bili došli

[1]) U tom djelu se nalazi i tzv. *Fibonacciev identitet*

$$(a^2+b^2)(c^2+d^2)=(ac\pm bd)^2+(ad\mp bc)^2$$

koji ji vezan s trigonometrijom, teorijom brojeva itd.

do pojma i oznake općeg broja. *Taj korak učinio je upravo Viète i tako od sinkoptičke algebre i numeričke algebre prešao na simboličku algebru,* na algebru sa slovima ili kako kaže sam Viète: učinjen je prelaz *logistica numerosa* → *logistica speciosa.* Dok su se prije Viète-a veličine x, x^2, x^3 smatrale samostalnima i nepovezanima, Viète je uočio da su te veličine međusobno povezane pa je zato i prirodno da u svojoj oznaci imaju i nešto zajedničko.

Važno je da je F. Vièta *označivao i koeficijente i nepoznanice slovima* i time uočio koliko je algebra nad aritmetikom — upravo time je algebra stvorena kao nadgradnja aritmetike (Vieta je koeficijente označivao suglasnicima B, C, D,... a nepoznanice samoglasnicima: A, E, I,...; današnje označavanje koeficijenata početnim slovima $a, b, c,\ldots$ abecede a nepoznanica pomoću završnih slova $x, y, z,\ldots$ abecede uveo je Descartes 1637.). Vieta nije bio matematičar po struci nego se njome bavio kao amater, a zanimljivo je da je u službi kralja Henri IV pokazao izvrsne osobine u odgonetavanju ratnih šifara (za vrijeme francusko-španjolskih ratova). Najglavnija su mu djela iz algebre: *In artem analyticam isagoge* (Uvod u umijeće analize), Tours 1591 (sa dodatkom: *Logistica Speciosa*), *De aequationum recognitione et emendatione* (posmrtno djelo, 1615). Viète je sistematski primjenjivao algebru i algebarske metode u trigonometriji i geometriji pa je on znatan preteča analitičke geometrije isto kao što je to bio njegov prijatelj Dubrovčanin Marin Getaldić.

Posebno je Vièta znao da se zadaća o trisekciji kuta odnosno zadaća o udvostručenju kocke, svode na kubne jednadžbe. Poslije će Descartes (Géometrie 1637) na osnovu toga izvesti zaključak da se *ta dva problema ne mogu riješiti elementarno* (pomoću ravnala i šestara) (isp. 5 § 8).

8.4. *Albert Girard* (1595 Lorraine — 1632) u djelu *Invention nouvelle en algèbre*, Amsterdam 1629 (*Nov izum u algebri*) stavlja se na Stevinovo i Vieteovo stanovište, dopušta negativne koeficijente i negativna rješenja pa tvrdi da svaka algebarska jednadžba $a(x)=0$ stepena n ima upravo n rješenja s tim da se uračunavaju i kompleksna rješenja. Bila su potrebna skoro dva stoljeća da se ta istina i dokaže.

Time se završava renesansna algebra otvarajući put analitičkoj geometriji, infinitezimalnom računu i drugim matematičkim disciplinama.

9. ALGEBRA U 17. 18. I 19. STOLJEĆU

9.1. Nakon što je u preporodu nađeno rješenje jednadžbi 3. i 4. stupnja i nakon što je zaslugom Viètea stvorena algebra kao samostalna nauka, nezavisna od aritmetike, bio je utrt put kasnijim istraživanjima: rješavati jednadžbe stepena >4, nalaziti numerička rješenja danih posebnih jednadžbi, itd.

Specijalno je 1770. Euler riješio jednadžbu 4. stupnja na način koji se razlikovao od Ferrarijeva načina a 1786. je E. S. Bring (1736—1798) sveo opću algebarsku jednadžbu 5. stepena na oblik $x^5+ax+b=0$.

Znatne priloge u teoriji jednadžbi dali su: R. Descartes (1596—1650), P. Fermat (1601—1665), I. Newton (1642—1727), G. W. Leibniz (1646—1716), E. W. Tschirnhaus (en) (1651—1708), M. Rolle (1652—1719) (isp. 29 § 3.2), G. Cramer (1704—1752), L. Euler (1707—1783), A. T. Vandermonde (1735—1796), E. Bézout (1730—1783), isp. 20 § 6.2), E. Waring (1734—1798), P. S. Laplace (1749—1827).

Cilj tih istraživanja bio je da se riješi opća jednadžba n-tog stepena, posebno da se dokaže Girardova slutnja (v. § 8.4), da se riješe sistemi jednadžbi uopće a linearnih posebno. U tom pogledu posebno mjesto zauzima nastajanje i razvijanje pojma *determinante* koju su nezavisno izumili: Japanac Seki Kowa (1642—1708), Leibniz i Cramer, a naročito razvili: Vandermonde, Cauchy, Jacobi i dr.

9.2. *Osnovni stavak algebre* (isp. 7 § 13.1, 29 § 6.5—6.7). Već 1608. je Peter Rothe (★ 1617) izrekao misao da svaka algebarska jednadžba stepena n ima n rješenja (v. 29 § 6.5); tu su misao kasnije sve jasnije izricali razni matematičari kao: Girard 1629, Descartes 1637, Newton 1685, Euler 1742. a u zavisnosti od toga koliko su se dopuštala kompleksna rješenja i kako se određivala kratnost rješenja; činjeni su ozbiljni pokušaji da se ta tvrdnja i dokaže (d'Alembert (1746), Euler (1751), no potpun dokaz je pošao za rukom tek Gaussu 1799. odnosno 1849; dosad je poznato preko 50 dokaza toga stavka.

9.3. *Determinante.* Rješavajući sisteme linearnih jednadžbi determinante su otkrili: Leibniz (1693), C. Cramer (1750) a posebno su ih mnogo upotrebljavali E. Bézout i A. T. Vandermonde (formalna pravila!); 1772. je Laplace našao teorem o razvoju determinante; 1812. J. P. M. Binet (1786 Rennes — 1856 Paris) je našao teorem o množenju determinanata; u 19. stoljeću determinante su izučavali specijalno: Cauchy (osamostaljenje teorije), Jacobi, Cayley (oznaka iz 1841: pravokutna tablica među uspravnim zagradama!), Weierstrass: naziv »determinanta« potječe iz 1812. (Cauchy), premda je 1801. Gauss u *Disquisitiones arithmeticae,* § 154, taj izraz upotrebio za diskriminantu forme. U 20. stoljeću determinante su izučavane u vezi s matricama i postale su jedno poglavlje teorije matrica; posebno su izučavane determinante matrica iz proizvoljna tijela, kao i determinante beskonačna formata, odnosno determinante nekvadratnih matrica.

T. Muir (1844—1934) napisao je historiju determinanata u pet knjiga (ukupno oko 2500 stranica).

9.4. *Lagrangeovo rješenje jednadžbi. Nagovještaj grupa* (isp. 32 § 5.7). Glasovit je način kako je 1770. L. Lagrange riješio algebarske jednadžbe $a(x)=0$ stepena $n < 5$; bilo je veliko iznenađenje kad se vidjelo da analogna metoda primijenjena na $a(x)=0$ stepena $n=5$ umjesto da dovodi do »rezolvente« koja bi bila stupnja $< n$ dovodi naprotiv do rezolvente stupnja $6 > n$ i dakle ne može dovesti do cilja — riješiti jednadžbu $a(x)=0$. Međutim, Lagrangeova metoda i ispitivanja bazirana su na novim principima: upotrebljene su permutacije i grupe permutacija Odatle su proizašla dva rezultata: 1) dokaz da se opća jednadžba $a(x)=0$ stepena $n=5$ (odnosno $n > 4$) ne može riješiti pomoću radikala (1798—1813. P. Ruffini) (1765—1822)[1], 1824. N. H. Abel (1802—1829); 2) razvila se teorija grupa i posebno se problem rješivosti jednadžbi $a(x)=0$ sveo na određenu problematiku o grupama permutacija; a na tome raširenom polju lako se dokazuje da općenito pri $n > 4$ jednadžba zaista nije rješiva algebarski (rješiva je onda i samo onda ako je rješiva pripadna grupa te jednadžbe; E. Galois; isp. 32 § 5).

Vandermonde je 1771. izrazio radikalima rješenja od $x^{11}=1$; Gauss je 1801. to učinio za proizvoljno $x^n=1$; Abel je 1829. našao važan razred ireducibilnih

---

[1]) Isp. knjigu Paolo Ruffini, *Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebrica delle equazioni generali di grado superiore al quarto,* 2 v. Bologna 1798 (str. 522). (Opća teorija jednadžbi u kojoj se dokazuje nemogućnost algebarskog rješavanja opće jednadžbe stepena >4).

jednadžbi $a(x)=0$ koje su rješive algebarski (to su tzv. *Abelove jednadžbe*, tj. one kojima je Galoisova grupa komutativna ili Abelova).

9.5. *Teorija grupa.* U vezi s pitanjem o rješivosti algebarskih jednadžbi $a(x)=0$ u radikalima nastala je teorija grupa permutacija (E. Galois).

Sam termin »*grupa*« uveo je Galois. Postulate grupe dao je 1854. Cayley, a opsežna istraživanja o grupama permutacija vršio je Cauchy već 1814. g; također Gaussova istraživanja o jednadžbi dijeljenja kruga (7. poglavlje u Disquisitiones arithmeticae, 1801) imaju dosta dodira s teorijom grupa.

Standardno djelo o grupama napisao je C. Jordan (1838—1922): *Traité des substitutions et des équations algébriques*, Paris 1870; to djelo je pravi spomenik Galoisu. Već u tome djelu ima pogleda i na beskonačne grupe kao i na probleme o predstavljanju grupa. A istraživanja matematičara kao što su: F. Klein (1849—1925) S. Lie (1842—1899), H. Poincaré (1854—1912), G. Frobenius (1849—1917), W. Burnside (1852—1927), L. Sylow (1832—1918), E. Picard (1856—1941), L. E. Dickson (1873—1945), I. Schur (1875—1941), A. G. Kuroš (20. st.), A. S. Pontrjagin (20 st.), H. Wielandt (★ 1910), R. Baer (20. st.), M. Hall (20. st.) sa sve novim oblastima i problemima u vezi s teorijom grupa pokazuju kako je pojam grupe važan i kako se svuda može primijeniti. Posebno je često grupa vezana uz raznovrsna razmatranja o simetriji (figura, skupova, pojava itd); tu treba spomenuti grupovne klasifikacije geometrija (F. Klein, Erlanger Program 1872) svih mogućih prostornih rešetki i kristala, pa primjene grupa u kvantnoj mehanici, itd. To su svjesna dostignuća matematičara iz konca 19. stoljeća i iz 20. stoljeća; sa druge strane vrlo je zanimljivo spomenuti da se već u primitivnijim uzorcima ornamenata, vezova i slika koji datiraju još iz 1500. godine prije naše ere (npr. u Egiptu za vrijeme 18. dinastije) nalaze lijepe pravilnosti u vezi s grupama.

Savremena matematika radi vrlo mnogo o grupama i raznim nadgradnjama i podgradnjama grupa (grupoidi, polugrupe, dualne grupe ili mreže, prsteni, ideali, tijela, vektorski prostori, A-moduli, algebre, itd.). Posebno mjesto zauzima pitanje o reprezentaciji grupa i drugih algebarskih struktura pomoću matrica, odnosno pomoću linearnih operatora.

9.6. *Približna rješavanja jednadžbi.* Približna rješavanja jednadžbi poznata su još iz davnina, iz staroegipatske, kineske i arapske matematike (*metoda lažnog položaja*). Specijalno se tako razvila tzv. metoda sekante (31 § 1.3). Vieta je našao jednu metodu približnog rješavanja koju je razvio Newton i koja se danas zove *metoda tangente* ili *Newtonova metoda*; metodu je L. V. Kantorović (★ 1912.) (Trudi mat. inst. Steklova Moskva 28 (1949) 104—144) prenio i na polinome s kompleksnim koeficijentima. Metoda Dandelin-Lobačevski-Graeffe iz 19. st. opisana je u 31 § 2.

Metoda iteracije (isp. 31. § 1) potječe od Legendrea i Cauchy-a (isp. Cauchy, *Analyse algébrique* 1821, Oeuvres (2) 3,381); to je vrlo opća metoda i razvija se sve više; upotrebljava se i u izučavanju jednadžbe stepena n kao i u izučavanju sistema jednadžbi. Posebno je prikladna za rješavanje pomoću matematičkih strojeva jer joj se lako određuje program. Metoda iteracije specijalno se mnogo upotrebljava za rješavanje sistema linearnih jednadžbi i matričnih jednadžbi.

U vezi s numeričkim rješavanjem jednadžbi važna su među ostalim još ova imena s naznačenom godinom kad je rezultat postignut: M. Rolle (u njegovoj Traité d'algebre 1690. kao i u Newtonovoj *Arithmetica universalis* 1707. nalaze se međe koje zatvaraju svako realno rješenje date alg. jednadžbe $a(x)=0$), D. Bernoulli (Akad. Petrograd, 3 (1728) 92) navodi postupak koji su dotjerali Euler i Fourier kako se razvijanjem u rekurentne redove mogu dobiti sva rješenja od $a(x)=0$; B. Bolzano (29 § 2.5), Lagrange 1798, Ch. Fourier 1831, Sturm 1829, 1835, Dandelin 1826, Lobačevski 1834, Graeffe 1837.

9.7. *Uloga raznih vrsta funkcija pri rješavanju jednadžbi.* Kad se već saznalo da se svaka jednadžba $a(x)=0$ ne može riješiti radikalima, pitalo se kakve funkcije koeficijenata treba uzeti pa da se nađu rješenja x. Ako je st $a=5$, Hermite je 1858. dokazao da je dovoljno promatrati *eliptičke funkcije* pa da se iz $x^5+ax+b=0$ izrazi x pomoću a, b; ako je st $a > 5$, tada Poincaréove automorfne funkcije vode na cilj[1] (isp. slučaj st $a=3$ i Vieteovo rješenje pomoću trigonometrijskih funkcija u 5 § 6.5). S historijskog stajališta zanimljiva je knjiga F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom 5. Grade*, Leipzig 1884, VIII+261 str. jer se u njoj s grupovnog stajališta osvjetljavaju razni problemi u vezi s jednadžbom 5. stepena.

9.8. *Teorija brojeva. Preraštanje u modernu algebru.*

9.8.1. Već su starogrčki matematičari znali za parne i neparne brojeve, za proste i složene brojeve, za savršene brojeve, znali su cjelobrojno rješavati jednadžbu $x^2+y^2=z^2$; posebno se u Euklidovim elementima (— 3 st). nalaze važni teoremi o djeljivosti brojeva i najvećem kratniku dvojke prirodnih brojeva. Za teoriju brojeva je važna Diofantova *Aritmetika.*

9.8.2. Snažan impuls novovjekoj teoriji brojeva (kao i raznim drugim matematičkim oblastima: infinitezimalnom računu, koordinatnoj geometriji, višedimenzionalnoj geometriji, računu vjerojatnosti) dao je francuski pravnik i matematičar Pierre de Fermat (1601—1665); kao amater u matematici, nije skoro ništa objavio za života no poslije je nađeno mnogo njegovih rezultata od kojih još i danas ima nedokazanih.

Veliki matematičari L. Euler i L. Lagrange (1736—1813) dali su važnih priloga teoriji brojeva. Wilson (1741—1793) je oko 1760. našao da je $1+(p-1)!$ kratnik od p za svako prosto p. A. M. Legendre (1752 Toulouse — 1833 Paris) svojim djelom *Théorie des nombres* (Paris 1798, s dodacima 1816, 1825) je znatno unapredio teoriju brojeva; u tom se djelu nalazi i kvadratni zakon recipročnosti (22 § 7.12).

Kubni zakon recipročnosti našao je Jacobi (i Gauss ali nije objavio). Bikvadratni zakon recipročnosti našao je Gauss ali tek pošto je 1828—1832 razvio teoriju kola $D+iD$ (*Gaussovi brojevi*).

Recipročni zakoni razreda >4 vrlo su mnogo izučavani od raznih matematičara.

9.8.3. Epohalno djelo u teoriji brojeva čini Gaussovo *Disquisitiones Arithmeticae* 1821 (*Istraživanja o aritmetici*); u tom djelu Gauss je definirao relaciju kongruencije, odredio broj razreda binarnih kvadratnih formi s datom determinantom, razradio teoriju kongruencija, binomskih jednadžbi, pravilnih poligona (već 30.3.

[1]) Monumentalno djelo o tim funkcijama je F. Klein-R. Fricke: *Vorlesungen über die Theorie der automorphen Funktionen*, Leipzig, I, 1897, II_1 1901, II_2 1912.

1796. u svojem dnevniku nadničarski sin 19-godišnji Gauss zapisuje da je našao konstrukciju pravilna 17-kuta pomoću lineara i šestara).

Učenik, komentator i nastavljač Gaussovih ideja bio je P. Lejeune — Dirichlet (1805— Gottingen 1859); Euleru i njemu dugujemo zahvat analitičkih, graničnih metoda u teoriju brojeva (1839), čime je osnovana tzv. *Analitička teorija brojeva*; jedan od velikih uspjeha u tom pravcu bila su istraživanja o raspodjeli i ulozi prostih brojeva (Hermite, Riemann, Čebišev, Hadamard, De la Vallée Poussin, Hilbert, Vinogradov, itd.).

9.8.4. *Ideali.* Kummer (1810—1893) je 1849. nastojao dokazati nemogućnost, nad D, Fermatove relacije $x^p+y^p=z^p$, $x\,y\,z \neq 0$, $p>2$ pa je promatrao tijelo $R(\alpha)$ što ga proizvodi nulište α polinoma $x^{p-1}+x^{p-2}+\ldots+x+1$; mislio je da je dokazao rastav $x^p+y^p=(x+y)\,(x+\alpha\,y)+\ldots(x+\alpha^{p1}-y)$. No, pri tom je učinio grešku jer je radio kao da u tijelu $R(\alpha)$ za cijele članove vrijedi jednoznačna faktorizacija; a stvarno je ona izuzetno na snazi. Da bi spasao iskaz o faktorizaciji, izmislio je *idealne faktore* (*Kummerovi ideali*).

Izučavanje općih algebarskih cijelih brojeva započeo je 1870. R. Dedekind uvodeći svoje *ideale* na posve nov način, onako kako se danas definira (isp. 32 § 3.3) i *zamjenjujući relaciju djeljivosti među brojevima relacijom inkluzije među idealima.* Time su se otkrile posve nove mogućnosti i velike sinteze u novim oblastima omogućujući izučavati s jedinstvenog stajališta razna aritmetička, algebarska i geometrijska pitanja. Specijalno se spoznalo da teorija algebarskih brojeva i Galoisova teorija jednadžbi imaju zajednički korijen u teoriji algebarskih tijela brojeva. Međutim, i to su još bila *brojena* tijela.

9.8.5. Naredni korak bio je da se krene na tijela koja nisu brojevna (isp. Galoisov korak) dakle na proizvoljna tijela; takav korak je 1910. učinio E. Steinitz (1871—1928). Premda se Steinitz ograničio na komutativna tijela[1], ipak je njegovim djelom započeta nova era algebre.

Prvu algebru napisanu u tom novom duhu napisao je Holanđanin B. L. van der Waerden, *Moderne Algebra* I Berlin 1930, II Berlin 1931.

Danas se algebra razvija kao teorija algebarskih struktura među kojima se posebno ističu: grupoidi, polugrupe, grupe, prsteni, oblasti cijelih, tijela, vektorski ili linearni prostori (uključujući tenzore), hiperkompleksni sistemi, A — moduli; vrlo usko područje zauzima pri tom klasična teorija cijelih racionalnih brojeva i klasična algebra (kao nauka o algebarskim jednadžbama). Ali zato pri tom važnu ulogu imaju međašnje i prelazne oblasti kao što su uređene strukture, topološke strukture, kategorije, razne geometrije itd. (isp. knjigu A. G. Kuroš [2]).

Za razvijanje pojedinih oblasti (topologija, funkcionalna analiza itd.) koje zajedno s algebrom dovode do sve novih saznanja, velikih zasluga su imali i imaju: H. Poincaré, D. Hilbert, St. Banach (1892—1945) M. Fréchet (1878—), braća Riesz, (F. 1880—1956i M. *1886), J. von Neumann (1903—1957) i dr.

U današnje doba oko (1965. godine) algebra je u punom cvatu i na njoj radi vrlo mnogo matematičara pa se govori čak o algebraizaciji matematike.

---

[1]) Pojam tijela dolazi već kod Abela (Oeuvres 1, 479; 2, 220) i Galoisa (Ouvres, p. 34); naziv *Körper* potječe od Dedekinda.

10. VEKTORI. MATRICE. LINEARNI OPERATORI

10.1. *Vektori.* Zbrajanje vektora kao komponiranje sila odnosno brzina dolazi u mehanici još od vremena Galileja (16/17 st.) i Stevina (16/17 st.); međutim, u algebri to nije imalo svojeg odraza sve dok se nije našla geometrijska interpretacija kompleksnih brojeva (preko dva stoljeća nakon otkrića tih brojeva od strane italijanskih matematičara 16. stoljeća). Tada se vidjelo kako se može direktno »računati« s geometrijskim tvorevinama — dužinama.

Specijalno se vidjelo kako se kretanja u ravnini mogu lako provesti u operacije s kompleksnim brojevima.

10.2. *Prvo nekomutativno tijelo.* Otuda zamisao da se slično postupi u prostoru i da se posebno rotacije u prostoru mogu prikazivati kao računanje s nekim brojevima sa 3 ili više dijelova. Tu ideju je ostvario 1843. irski astronom i matematičar Hamilton izumom *kvaterniona*; time je ujedno *prvi put ostvareno jedno nekomutativno matematičko tijelo*; rezultate je objavio u opsežnim knjigama: *Lectures on quaternions,* Dublin 1952, 64+736+LXXII te *Elements of quaternions* 1866 (LVII+762).

Naziv *vektor* (lat. *vehere* = vući) potječe od Hamiltona. Glavni zagovornik vektora bio je američki fizičar J. W. Gibbs (1839—1903) sa svojom knjigom *Vector Analysis,* New Haven 1881; 1884. dalje su ih primjenjivali i razrađivali: Englezi O. Heaviside (1850—1925), *Electromagnetic Theory* 1893; J. C. Maxwell (1831—1879) *Treatise on electricity and magnetism* 1873, Nijemac A. Föppl (1854—1924) *Geometrie der Wirbelfelder* 1897 (Geometrija vrtložnih polja).

10.3. *Tenzori.* Već je Leibniz iskazao potrebu da se provodi direktno računanje s raznim geometrijskim objektima. Tu Leibnizovu misao proveo je Hamilton za prostor R^3; Leibnizovu misao na vrlo širokim temeljima i u mnogo širim prostorima ostvario je njemački matematičar H. G. Grassman (1809—1877) u djelu *Ausdehnungslehre,*[1] Leipzig 1844 (prošireno 1862). To je djelo pisano na dosta težak način, puno je novih ideja, uključuje promatranje proizvoljno opsežnih prostora i daje za n-dimenzionalne prostore nešto od onog što Hamiltonovi kvaternioni daju za 3-dimenzionalni euklidski prostor. Specijalno je Grassmann došao — u današnjoj terminologiji — do pojma vektorskih prostora i vektora, do pojma vanjske algebre, polivektora i tenzora.

Inače, Cayley se je 1843. počeo služiti geometrijskim jezikom n-dimenzionalnih euklidskih prostora u izučavanju linearnih jednadžbi.

U izgradnji vektorskog i tenzorskog računa sudjelovali su znatno: B. Riemann (1826—1866), E. B. Christoffel (1829—1900), L. Kronecker (1823—1891), M. M. G. Ricci (1853—1925) (Delle derivazione covarijante e contravarijante, Padova 1888), T. Levi — Cività (1873—1941), H. Poincaré (1854—1912), E. Cartan (1869—1961), H. Weyl (1885—1955) i dr. Tenzorski račun je našao svoje primjene u Einsteinovoj općoj teoriji relativnosti (1915) kao njena važna aparatura; od tada su mu važnost i ugled neprestano rasli.

10.4. *Matrice.* Prvi put je matrice promatrao 1853. Hamilton, dakle matematičar koji je prvi dao formalnu aritmetičku definiciju kompleksnih brojeva i koji je otkrio kvaternione. Sam naziv »matrica« potječe od Cayleya 1854; on je 1858. razvio algebru matrica koju su nezavisno otkrili E. Laguerre 1867. i Frobenius 1878. U daljoj izgradnji matrica sudjelovao je vrlo velik broj matematičara kao: A. Cayley (1821—1895), Ch. Hermite (1822—1905), G. Frobenius (1849—1917),

[1] *Nauka o protezanju.*

L. Kronecker (1823—1891), H. Smith (1826—1883), J. H. H. Wedderburn (1882—1948).

Godine 1925. fizičar W. Heisenberg (*1901) upotrebio je matrice u izgradnji kvantne mehanike.

11. NEKOLIKO NAZIVA ZA ALGEBRU

Ahmes (Egipt, oko — 18. st.) »*Pravila o izučavanju prirode i za razumijevanje svega što postoji, svih nejasnih stvari i tajni*... »Papirus 20 m × 30 cm; zove se i *Rhindov papirus* (našao ga Rhind polovinom 19. st.) ili *Londonski papirus*.

Slične nazive s pridjevima nalazimo kod nekih japanskih matematičara i evropskih matematičara iz 16. i 17. stoljeća.

Aritmetika. To je opći naziv kod Grka za nauku o brojevima uključujući i algebru (specijalno je važna Diofantova Aritmetika, 3. st.).

Logistica (15. st.) (u staro-grčko doba tako se zvala vještina računanja).

Bija Ganita (Biža Ganita); traženje prvotnih elemenata

Lilavati (Prekrasna; ime preminule kćerke) — aritmetika; Baskara (12. st.)

Avyakta ganita

Ars rei et census

Regola de la cosa (tal.) 15. st., Die Regula Coss) (njem., 16. st.).

Cossike arte (engl.), Ars magna (Cardano, 16. st.), Arte maggiore (tal., 16. st.), Arte mayor (Juan Diez, 16. st. Meksiko); (Arte minore je naziv za trgovačku računicu).

Analiza (Viete 16. st.; Vieta je bio protiv arapskog naziva Algebra).

12. NAZIVI, ZNAKOVI I NEKI POJMOVI U ALGEBRI

12.1. *Nepoznanica*: *hau* (Ahmes, — 18. st.) znači: gomila, hrpa; *neodređen broj jedinica* (Diofant, 3. st.), *ša* — stvar (Arapi); *yen* (element), stvar.

Diofant označuje nepoznanicu sa ς (posljednje slovo riječi αριτμος): Vieta nepoznanice označuje slovima za vokale; današnja oznaka: x, y, z, t, u, w za nepoznanice potječe od Descartesa (17. st.).

12.2. *Koeficijent* (Vieta, 16. st.) (lat. *coefficiens* — koji djeluje zajedno). *Vieta je prvi matematičar koji i koeficijente i nepoznanice označuje slovima i s njima sistematski operira.*

12.3. *Znakovi* +, — J. Widman iz Češke (15. st.) u djelu: *Behennde und hüpsche Rechnung*, Leipzig 1489; znakovi za višak i manjak u paketima robe; kao znakovi za zbrajanje, odnosno oduzimanje, znakovi +, — dolaze prvi put 1514. kod holandskog matematičara Vander Hoecke-a.

12.4. *Znak množenja*: × (Oughtred, 1637); (Clavius 1583; Harriot, posmrtno 1631); Descartes izostavlja svaki znak za množenje.

12.5. *Znak za dijeljenje* : (znak za dijeljenje se vjerojatno javio prvi put poč. 17. st. u Engleskoj u djelu: Johnsons Arithmetick; in two Bookes (Džonsonova aritmetika u dvije knjige); Leibniz 1684. se služi istim simbolom.

12.6. = (jednakost) Recorde, The whetstone of witte (Brusilo oštroumnosti, London 1557); <, > Harriot 1631.

12.7. *Zagrade.* ( ) (okrugle zagrade): 16. st. (M. Stifel, Tartaglia i dr; { } Vieta 1593; [ ] Girard 1629.

Međutim u 17. stoljeću ulogu zagrade su imale crte iznad izraza; tako su radili Descartes, Newton i dr. Zagrade su učinili poznatima specijalno Leibniz, Euler i dr.

12.8. $\sqrt{\ }$ štampano prvi put u Chr. Rudolff: Die Coss 1525. (vjerojatno je $\sqrt{\ }$ u vezi s početnim slovom riječi radix = korijen).

12.9. ∞ (za beskonačno): Wallis, Arithmetica Infinitorum, 1655.

12.10. % je vjerojatno nastalo iz talijanske riječi *cento* (= *stotina*).

12.11. *Indeks.* Upotrebljava prvi Leibniz 1676. (pisao ga je lijevo od slova; Leibniz se služi dvostrukim indeksima 1693. u onom pismu De l'Hospitalu u kojem Leibniz govori o formiranju determinanata.

12.12. *Razmjer* (*proporcija*) $a : b = c : d$ (Leibniz 1693.). Još 1631. Englez Oughtred je umjesto toga pisao $a \cdot b : : c \cdot d$, a Descartes $a \mid b \mid c \mid d$.

12.13. *Nazivi većih brojeva.* Milijun: L. Pacioli (Summa, Venezia, 1494). prviput naštampano; bilijun (10^{18}), trilijun (10^{12}), kvadrilijun ($10^{4.6}$), . . . nonilijun (10^{81}) potječu od Francuza Chuquet-a (Le tryparty en la science des nombres, 1484; objavljeno istom 1880.); no trebalo je nekoliko stoljeća da se ti nazivi prihvate svuda.

Riječ milijun (10^6) nije nađena prije 13. stoljeća.

Milijarda (10^9) dolazi već u poč. 16. st.

12.14. *Eksponent* (Arhimed — 2. st.; prvi put razlomljen eksponent, kao pojam); Oresme (1360), Chuquet (1484.), Stifel (1544).), Descartes (današnji način pisanja), Girard 1629, Wallis 1665., Newton 1669. Riječ eksponent uveo M. Stifel (1487—1567) Arithmetica integra, Nürnberg 1544.

12.15. *Oznaka razlomka.* Razlomkovu crtu upotrebljavaju: Heron (1. st.) i Diofant; Indijci Brahmagupta (7. st.), Baskara (11. st.) pišu $\begin{matrix}2\\3\end{matrix}$ umjesto $\frac{2}{3} = 2/3$.
Arapi su se služili razlomkovom crtom; u Evropi je upoznata preko L. Fibonacci-a (1202.); u općoj je upotrebi od 17. st.

12.16. *Decimalni razlomci.* Imaju dugu povijest; proizašli su iz decimalnih mjera.

12.17. *Transcendentan broj* (naziv) dolazi izgleda prvi put kod Leibniza (razlikovanje: algebarske funkcije — transcendentne funkcije potječe od Johana Bernoullia iz godine 1730).

13. HISTORIJAT BROJEVA. NAZIVI. OZNAKE

13.1. *Decimalni razlomci ili decimalni brojevi.* Proizašli su iz decimalnih mjera (npr. u 10. st. u Kini su za težine imali: 1 *lan* = 10 *cen* = 10^2 *fen* = 10^3 *li* = 10^4 *hao* = 10^5 *si* = 10^6 *ho*). Po uzoru na heksagezimalne razlomke Babilonaca izgradio ih u Samarkandu al Kaši (*Ključ aritmetike*, 1427.); cijeli dio ispisuje jednom bojom a razlomljeni dio drugom bojom ili ta dva dijela odjeljuje vertikalnom crtom. N. Chuquet (1484) odjeljuje tačkom, S. Stevin (1585.) razvio teoriju u djelcu *La Disme*... (*Desetinka. Pouka kako se bez razlomka može sve lako izračunati*). Pelizzati (Torino 1492.): prvi put dolazi decimalna tačka štampana, a 1592. Bürgi uvodi decimalni zarez.[1] Izumom i upotrebom logaritama (Bürgi, Napier, Briggs raširila se i decimalna oznaka, a Stevinov prijedlog iz 1585. za uvođenje decimalnih mjera proveden je (bar djelomično) tek poslije francuske revolucije.

13.2. *Negativni brojevi.* Tragovi u staroj babilonskoj matematici; njihovi astronomi u — 4. st. ispravno množe relativne brojeve. Kinezi su bojom razlikovali pozitivne i negativne koeficijente jednadžbi (crveno: pozitivno, crno: negativno?). Diofant (?3. st.) ispravno izmnaža pozitivne diferencije $(a-b)(c-d) = ac - bc - ad + bd$; govori o *besmislenoj* (ἄλογος) jednadžbi $4x+20=4$ jer daje $x=-4$ (prvi spomen negativna broja u Evropi). Negativni brojevi (»negativne i pozitivne veličine«) promatraju Hindusi Brahmagupta (7. st.), Mahavira (9. st.) i dr; Baskara (oko 1150.) za naše — 6 piše $\dot{6}$ ili $\mathring{6}$ i govori *o dugu* 6. *Afirmativni — privativni brojevi* (Scheubel 1551.), *numeri veri — numeri ficti* (Cardano 1545.), Stifel 1544. govori o *apsurdnim brojevima*: oni su manji od 0, Bombelli: plus (p. 5), minus (m. 5); rade s njima ispravno. Znakovi +, — ne javljaju se (u vezi s relativnim brojevima) prije 15. stoljeća; štampani su prvo u Widmanovoj aritmetici iz 1489. Od kasne renesanse (Vieta, Harriot, Fermat, Descartes, Hudde Girard, Stevin) negativni brojevi su opća matematička tekovina. Negativni brojevi, odnosno cijeli racionalni brojevi kao uređeni parovi prirodnih brojeva izučavani su svijesno istom u 19. st. (zaslugom Hamiltona).

13.3. *Nula.* 0. Cifra (brojka) 0 (u sanskrtu *çunya* = *prazan, nezauzet* ili *kha* = *uzduh*, arapski *aş* — *şifr* — *prazan*, odakle *zefirum, zero, sifra cifra*; lat. *nulla* = *nulla figura*) zauzima osobit položaj među drugim ciframa. Znak za nulu zvali su Indijci *bindu* (*kap, kapljica*).

Možda znak 0 za nulu dolazi od slova O (omikron, poč. slovo riječi οὐθὲν (č. uden) — ništa. Tim su znakom grčki astronomi (služili su se babilonskom bazom 60) odjeljivali mjestovne vrijednosti heksagezimalnih razlomaka.

Broj nula mnogo je mlađeg datuma nego cifra 0; u vezi je s praznim skupom.

Nula kao neutralni član grupe koja je pisana aditivno vrlo je mladog datuma.

13.4. *Realni* (*stvarni*) *brojevi.* Naziv potječe od Descartesa (1637.), kao protuteža »imaginarnim« brojevima koji su se pojavili računanjem s antikvadratima negativnih brojeva. Razlikovanje racionalnih (ῥετά) veličina od iracionalnih neizrecivih, veličina, (ἄρρετα), inkommensurabilnih (ἄλογα) potječe od Pitagorovaca (—6. st.)

[1]) Zarez kao znak sastavljanja uveo je mletački tipograf Manuzzi (15/16 st.); izgleda da je on počeo knjigama dodavati i Sadržaj.

Platonov učitelj Teodor iz Kirene (—5. st.) zna da su veličine $n^{1/2}$ pri $n \in \{2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17\}$ iracionalne; on je uveo riječ ἄλογον; on je uveo i σύμμετρι — ἀσύμμετρι; tim se izrazima služio i Euklid (—3. st.; knjiga Elementi x ima 115 teorema o iracionalnim veličinama) pa još i Englez Bradwardinus (1290—1349.). Boecije (480—524) te izraze prevodi sa *commensurabilis* — *incommensurabilis*, što Cassiodor (5/6 st.) prevodi sa *rationalis* — *irrationalis*; Marcijan Capella (r. oko 470.) prevodi ἄλογος sa *irrationalis*.

Izrazivi — neizrazivi brojevi (Arapi i Hebreji); *razjašnjiv — nerazjašnjiv* (neki matematičari iz renesanse); *čujni* (*audibilni*) — *nečujni* (*inaudibilni*) *brojevi* (Muhamed ibn Musa) odakle *nijemi brojevi — surdi* (npr. Gherardo di Cremona, c. 1150).

Prelaz od nesumjerljivih veličina na iracionalne brojeve učinili su komentatori na arapskom među kojima se ističe Perzijanac Abul-Abbas ben Hatim el NAIRISI (? — 924). Inače, teorija omjera pravocrtnih odrezaka (Euklid, V knjiga) je određena geometrijska teorija realnih brojeva na visokom stupnju (premda Grci nisu smatrali te omjere brojevima; naprotiv npr. Newton, u *Arithmetica universalis* 1707, upravo definira realne brojeve kao omjere odrezaka).

Kad se jednom razvio decimalni prikaz brojeva (17. st.) *racionalno i iracionalno* je našlo svoj odraz u *periodsko-neperiodsko*.

Aritmetičku teoriju realnih brojeva dali su u 19/20. stoljeću 1865. Weierstrass (sume redova racionalnih brojeva), 1872. Méray i Cantor (pomoću nizova racionalnih brojeva) i 1872. Dedekind (pomoću rezova skupa racionalnih brojeva); 1946. Kolmogorov je definirao realne brojeve pomoću prirodnih brojeva (Realni brojevi mogu se definirati i kao uređene neprekidne lančasto uređene grupe odnosno kao uređene lančasto uređena potpuna tijela (isp. 32 § 8.9.11).

13.5. *Kompleksni brojevi.* Prvi kompleksan nerealan broj jest $(81-144)^{1/2}$ i javlja se kod Herona (—1. st.); pri obrađivanju krnje 4-strane pravilne piramide on daje nezgodne brojevne podatke za osnovne i pobočne bridove pa mu se u računanju pojavljuje izraz $(81-144)^{1/2}$; međutim, Heron se na to ne obazire pa radi dalje sa $(144-81)^{1/2}$ (v. Tropfke [1] 2 str. 103/4). Diofant (3. st.) određujući pravokutan trokut opsega 12 i ploštine 7 sveo je zadatak na jednadžbu $336x^2+24=$ $=172\,x$ i kaže da zadatak nema rješenja jer nije ispunjen uslov da $\left(\frac{172}{2}\right)^2-24\cdot 336$ bude kvadrat. Hindus Mahavira (c. 850) izričito kaže da negativan broj nije kvadrat. L. Pacioli (Summa 1494) izričito kaže da $x^2+c=b\,x$ ima rješenje samo ako je $\frac{1}{4}b^2 \geqq c$. Cardano se prvi služio nerealnim brojevima rastavljajući 10 na dva dijela x, y kojima je umnožak 40; našao je $x=5+\sqrt{-15}$, $y=5-\sqrt{-15}$. Girard 1629. priznaje kompleksne brojeve kako bi bio na snazi njegov iskaz o broju nulišta polinoma $a(x)$ (isp. § 8.4). Descartes 1635. govori o *realnim* brojevima i *imaginarnim* brojevima. Wallis, Leibniz, Cotes, J. Bernoulli, Euler s kompleksnim brojevima računaju i nalaze važne formule

$$ln\,(cos\,\varphi + i\,sin\,\varphi) = i\,\varphi \qquad \text{(Cotes, c. 1710)}$$

$$cos\,\varphi + i\,sin\,\varphi = e^{i\varphi} \qquad \text{(Euler)}$$

$$(cos\,\varphi = i\,sin\,\varphi)^n = cos\,n\,\varphi + i\,sin\,n\,\varphi$$

(De Moivre 1730., a možda i 1707.)

$$\cos\varphi=\frac{1}{2}(e^{i\varphi}+e^{-i\varphi}),\quad \sin\varphi=\frac{1}{2i}(e^{i\varphi}-e^{-i\varphi})$$

(Euler 1743, 1748).

Geometrijsku interpretaciju kompleksnih brojeva u brojevnoj ravnini (isp. 4 § 6. 2. 2.) dao je Danac (1797—1799) Wessel (1745—1818.); nezavisno su do tog rezultata došli Francuz J. R. Argand 1806. i Nijemac Gauss 1831.

Riječi realno-imaginarno (u smislu nerealno) uveo je 1637. Descartes; naziv kompleksan broj potječe od Gaussa (1832); oznaku $i=\sqrt{-1}$ uveo je 1748. Euler; $a-b\,i$ kao konjugirano od $a+b\,i$ uveo je Cauchy 1821.; normu a^2+b^2 od $a+b\,i$ uveo je 1832. Gauss; izraz $+\,(a^2+b^2)^{1/2}$ uveo je 1821. Cauchy i nazvao ga *modulom broja* $a+b\,i$ (Weierstrass umjesto o modulu govori o *apsolutnoj vrijednosti broja* $a+b\,i$).

Poopćenje kompleksnih brojeva jesu *kvaternioni* (Hamilton 1843.) i *oktave* (Cayley, 1821—1895) (isp. 32 § 6. 3.4).

13.6. *Algebarski brojevi — Transcendentni brojevi.* Bilo je veliko iznenađenje kad su otkrili iracionalne brojeve (Pitagorina škola; — 6. st.), tj. brojeve koji nisu rješenja linearne jednadžbe s cijelim koeficijentima. Zato nije moglo biti jasno da uopće ima *transcendentnih brojeva*, tj. brojeva koji ne bi zadovoljavali koju algebarsku jednadžbu $a(x)=0$ s *cijelim* koeficijentima. Postojanje transcendentnih brojeva dokazao je istom 1844. J. Liouville (1809—1882); prvi broj iz prakse koji se pokazao transcendentnim bio je broj e (Hermite 1873.) pa broj π (Lindemann 1872.); time je dokazana nemogućnost kvadrature kruga! Brojevi a^b (a je algebarsko $o \neq a \neq 1$, b iracionalno (npr. $b=2^{\sqrt{2}}$) su transcendentni (A. O. Geljfond, 1929—34.). Algebarskih brojeva ima $\aleph_0$, a transcendentnih $c=2^{\aleph_0}$ dakle $>\aleph_0$ (Cantor 1874.).

Riječ »transcendentan broj« javlja se izgleda prvi put kod Leibniza (Djela VII, 215), napominjući da je jednadžba $x^x+x=30$ zadovoljena brojem $x=3$ no da većinom takve jednadžbe osim uz pomoć *transcendenata* nisu rješive.

14. RAČUNSKE OPERACIJE. ZAKONI. NAZIVI

Istom oko 1870. godine bilo je posve raščišćeno pitanje o tome da imamo četiri *osnovne* računske operacije: zbrajanje, oduzimanje, množenje i dijeljenje s tim da je oduzimanje (dijeljenje) obrat od zbrajanja (množenja).

Još u 15. stoljeću razlikovalo se 8 osnovnih računskih operacija: numeratio, additio, subtractio, mediatio (raspolavljanje), duplatio (udvostručavanje), multiplicatio, divisio, progressio.

S tim u vezi sjetimo se kako se prije pronalaska logaritama produkte i kvocijente trigonometrijskih funkcija svodilo na sume i diferencije (od pronalaska logaritama do danas radi se obrnuto). Pitanje je da li se pronalaskom i širom upotrebom računskih strojeva neće koja zamršenija operacija smatrati osnovnom.

Izraz »komutativno« (Servois, 1814.); inače komutativnost $a\,b=b\,a$ za množenje dokazuje Euklid (—3. st.; Elementi VII (16)).

Izraz »*distributivno*« (Servois; 1814.); isp. Euklid, *Elementi* II, teor. 1, V: teor, 1, 2, 3.

Izraz »*asocijativno*« (Hamilton, 19. st.).

Zakon permanencije (Hankel, 1867.).

15. NEKE ALGEBRE OD INTERESA S HISTORIJSKOG STANOVIŠTA (KRONOLOŠKI)

1. STARI VIJEK

Ahmesova računica (—18. st.); Diofant: *Aritmetika* (3. st.) najbolja aritmetika, odnosno algebra starog vijeka (prevedeno na francuski: Les six livres mathématiques et le livre des nombres polygones, preveo P. Ver Eecke, Bruges 1926).

Euklid (—3. st.) ΣΤΟΙΧΕΙΑ (*Elementi*), knjige 2, 5, 7, 8, 9, 10 (preveo A. Bilimović, Beograd 1949—1957).

Vještina računanja; u 9 *poglavlja*. Kina (negdje u intervalu — 2 st. do + 2. st).

Nikomah iz Gerase (Grk iz Palestine, neopitagorovac, konac 1. st.) *Aritmetika*.

2. SREDNJI VIJEK

Boethius (ili Boetius) iz Rima (oko 510) *De institucione arthmetica*, I, II. Poznat udžbenik u srednjem vijeku i početkom novog vijeka.

Perzijsko-arapske algebre: Muhamed ibn Musa Al Kowarizmi: Algebr w'al-muqabalah (Bagdad, oko 825); al - Karkhi: Al Fakhri (11. st.) najdotjeranija arapsko-perzijska algebra.

Omar Hayam (1048—1123) *Algebra*. Najbolja algebra napisana od Perzijanaca; pisana je na arapskom (na francuskom u Parizu izdao 1851. F. Woepcke, a na engleskom 1931. D. S. Kasir).

Baskara (1114—?; Indija) *Lilavata* (*Prekrasna*), *Bija Ganita* (*Račun korijena ili prvotnih elemenata*). To su prva dva od četiri dijela iz astronomskog djela *Siddhanta çiromani* (Indija oko 1150) (*Ukras glave za rješavanja*).

Šu Šu Kien Čang: *Devet poglavlja o računanju*, 1247, Južna Kina.

Li Ye (1178—1265): *Mornarevo ogledalo izmjerenih krugova*.

Leonardo Fibonacci (Leonardo iz Pize) *Liber abaci*, 1202. Najglasovitija algebra srednjeg vijeka.

Jordanus Nemorarius ili Jordanus de Saxonia (? — 1236 ili 1237) *De numeris datis* (*O danim brojevima*); djelo se sastoji od 4 knjige. To je »apstraktna« algebra 13. stoljeća (pisac se služi slovima umjesto brojevima, mada na dosta nedosljedan način).

3. RENESANSA. NOVI VIJEK

Luca Pacioli, *Summa*, Venecija 1494; to je prva štampana algebra.

G. Cardano, *Ars magna*, Nürnberg, 1545.

R. Bombelli, *L'Algebra parte maggiore dell'aritmetica I, II, III* Bologna, 1572.

Franciscus Vieta (François Viète) *In artem analyticem isagoge* 1591 (*Uvod u umijeće analize*) (prva simbolička algebra).

Michel Rolle, *Traité d'algèbre*, Paris, 1690.

J.Wallis, *Treatise of algebra*, London 1585.

Isaac Newton, *Arithmetica universalis*, Cambridge 1707 (*opća aritmetika*).

L. Euler, Универзальная аритметика, Petrograd, 1768 (na njem. 1770; na francuskom s dodacima izdao Lagrange u Berlinu 1796—1797).

E. Bézout, Théorie générale des équations algébriques, Paris 1779, 471 p, 4°.

L. Lagrange, Traité de la résolution des équations numériques de tous les degrés; Paris, 1826.

A. M. Legendre, Essai sur la théorie des nombres, Paris 1798; 2. izd. *Théorie des nombres*, Paris 1808 (sa suplementima 1816, 1825); 3. izd. u dva sveska 1830; 1899_4 800 str. 4° (na njemačkom H. Maser, Leipzig 1893, I 18+442, II 12+453).

Odatle i današnji naziv *Teorija brojeva.*

F. K. Gauss, *Disquisitiones arithmeticae*, Lipsiae 1801 (na njem. H. Maser, Untersuchungen über höhere Arithmetik, Berlin 1889, 695 str. zajedno s nekim drugim Gaussovim člancima).

N. I. Lobačevski, Algebra, Kazan 1834.

Literatura:

Cantor M. [1]; Dickson [1]; Glejzer [1]; Juškevič [1], [2]; Kol'man [1]; Matvijevskaja [1]; Muir [1]; Smith [1]; Struik [1]; Taton [1]; Tropfke [1]; Vigodski [1]; Wieleitner [1].

TREĆI DIO

1. RJEŠENJA NEKIH ZADATAKA

POGLAVLJE 1.

str. 3. **3.3. Zadaci**

1. 1), 2), 4), 5): 1; 3) 0.

2. 1), 4), 5): 0; 3): 1.

str. 4. **4.3. Zadaci**

1. 3) 7): 0; ostali slučajevi: 1.

2. 1) 1; 2) 0, 1, 1, 0; 4) 1; 5) 1.

str. 5. **5.4. Zadaci**

2. 1) $vA=1$, $vB=1$, $vC=0$; 2) $v(A\vee B\vee C)=1$; 3) $v((A\vee B)\wedge C)=0$; 4) $v((A\wedge B)\wedge \neg C)=1$; 5) $v(\neg A\wedge \neg B\wedge \neg C)=0$; 6) $v(\neg A\vee \neg A\vee C)=1$; 7) $v(B\wedge \neg C)=1$.

5. 1) $x\vee \neg y$; 2) $x\wedge(y\vee z)$; 3) $x\wedge(y\vee z)$.

str. 8. **10. Zadaci**

1. 1), 2), 6) : 0; ostali slučajevi: 1.

10. 2) $\neg x=S(x,x)$; $x\vee y=S(S(x,x),\ S(y,y))$; $x\wedge y=S(S(x,y),\ S(x,y))$; $x\Rightarrow y=S(S(S(x,x),\ S(x,x)),\ S(y,y))$.

12. 2) $\neg x=L(x,x)$; $x\vee y=L(L(x,y),\ L(x,y))$; $x\wedge y=L(L(x,x),\ L(y,y))$; $x\Rightarrow y=L(L(L(x,x),y,\ L(L(x,x),y))$.

str. 15. **11.6. Zadaci**

1. 1), 3), 4), 7), 9), 10), 12), 16): istinito; ostali slučajevi: lažno.

3. 1) $\bigvee_x x+x\neq 2x$; 2) $\bigvee_x 2x\neq 6$; 3) $\bigwedge_x 2x\neq 6$; 4) $\bigwedge_x 2x=6$; 5) $\bigvee_x (2x=6)$;

6) $\bigvee_x x\neq -x$; 7) $\bigwedge_x x\neq -x$; 8) $\bigvee_x x\neq x+3$;

9) $\bigvee_x \bigvee_x (((x^2\neq y^2)\wedge((x=y)\vee(x=-y)))\vee((x^2=y^2)\wedge((x\neq y)\wedge(x\neq -y)))$;

10) $\bigvee_x (x^2=x)$; 11) $\bigvee_x (x-2)(x-3)\neq 0$; 12) $\bigvee_x \bigvee_y (x+y\neq y+x)$;

13) $\bigwedge_x \bigwedge_y \bigwedge_z (x<y)\wedge(y<z)\wedge(x\geqslant z)$;

14) $\bigvee_x ((\bigvee_{y_1} \bigvee_{y_2} (y_1\neq y_2)\wedge(x+y_1=x)\wedge(x+y_2=x))\vee(\bigwedge_y x+y\neq x))$;

15) $\bigvee_x ((x\neq 0)\wedge \bigwedge_y (xy\neq 1))$;

16) $\bigvee_x ((\bigvee_{y_1} \bigvee_{y_2} (y_1\neq y_2)\vee(x+y_1=x+y_2=0))\vee(\bigwedge_x x+y\neq 0))$.

5. 3), 8), 9): 1; ostali slučajevi: 0.

6. $\bigwedge_y \bigvee_x !$

7. $\bigwedge_a (a\geqslant 0)\Rightarrow(\bigvee_b \bigvee_c \bigvee_d \bigvee_e a=b^2+c^2+d^2+e^2)$

a, b, c, d, e znače cijele brojeve).

POGLAVLJE 2.

str. 30. **3.11. Zadaci**

9. 3) 34650; 6) $\prod_{\nu=1}^{m}\binom{u(m-\nu+1)}{u}$.

12. Na 126 500 načina.

2. $n^r!\geq(n!)^r$.

17. b) $\binom{n}{1}-3(n-2)$.

20. Na $\binom{13}{3}\binom{13}{1}\binom{13}{1}\binom{13}{1}=3770036$ načina

str. 34. **4.7. Zadaci**

2. Peti član u razvoju je 16 974,744 x^6y^{-7} ako je $n=5$; 152 772,696 x^8y^{-6} ako je $n=6$; 1 069 408,872 $x^{10}y^{-5}$ ako je $n=7$; $6{,}4165\cdot 10^6x^{12}y^{-4}$ ako je $n=8$.

3. $-99x^{-15}y^7$.

4. Središnji članovi su:
$9082,8x^8y^{-1}$ i $-17\,561,08x^7y^{-4}$ ako je $n=5$; $-105\,360,48x^9y^{-3}$ ako je $n=6$; $-553\,142,52x^{11}y^{-2}$ i $1\,069\,408,872x^{10}y^{-5}$ ako je $n=7$; $6\,416\,453,232x^{12}y^{-4}$ ako je $n=8$.

5. 70.

6. 1) 4 725 000; 2) 10.

7. 1) 90; 2) 0; 3) 1; 4) 3.

9. $(x+y-z)^2=x^2+2xy-2xz+y^2+z^2-2yz$;

$(x+y-z)^3=x^3+3x^2y-3x^2z+3xy^2-6xyz+3xz^2+y^3-3y^2z+3yz^2-z^3$;

$(x+y-z)^4=x^4+4x^3y-4x^3z+6x^2y^2-12x^2yz+6x^2z^2+4xy^3-12xy^2z+12xyz^2-$
$-4xz^3+y^4-4y^3z+6y^2z^2-4yz^3+z^4$;

$(x+y-z)^5=x^5+5x^4y-5x^4z+10x^3y^2-20x^3yz+10x^3z^2+10x^2y^3-30x^2y^2z+$
$+30x^2yz^2-10x^2z^3+5xy^4-20xy^3z+30xy^2z^2-20xyz^3+5xz^4+y^5-5y^4z+$
$+10y^3z^2-10y^2z^3+5yz^4-z^5$.

10. 12.

11. $\binom{8}{k}\cdot 0,02^k>10^{-5}$ onda i samo onda ako je $0\le k\le 4$. $1,02^8 \doteq 1,1718$.

POGLAVLJE 3.

str. 67. **9.6. Zadaci**

1. Ima 120 permutacija. Trideseti član je 21 543.
Susjedi permutacije 43 215 su 43 152 i 43 251.

8. 2) 12 parnih i 12 neparnih permutacija.

9. Ako je $n=4k$ odnosno $n=4k+1$), onda je $(-1)^{ip}=(-1)^{sp}$; ako je n oblika $4k+2$ ili $4k+3$, onda je $(-1)^{ip}=-(-1)^{sp}$, jer je $ip+sp=\binom{n}{2}$.

10. $\frac{1}{2}\cdot\binom{n}{2}n!$

17. 1) na 43 200 načina; 2) $(6\cdot5\cdot4\cdot3)\cdot4!+(6\cdot5\cdot4\cdot3\cdot2)-(4\cdot3\cdot2)+6!\,(4\cdot3)=34560$.

19. na 1 728 načina. **20.** $\frac{10!}{5!}=30240$.

21. na 378 načina.

22. na 1120 načina.

26. 1) 20 načina, 2) 42 načina.

27. na 1 820 načina, odnosno na 728 načina.

29. 1) $\binom{15}{8}=6435$ načina,

2) $\binom{15}{8}+\binom{15}{1}\binom{14}{6}+\binom{15}{2}\binom{13}{4}+\binom{15}{3}\binom{12}{2}+\binom{15}{4}=157950$ načina.

3) $\binom{22}{8}-15\cdot\binom{15}{2}-15\binom{14}{1}-15$ načina $=317\,970$ načina.

POGLAVLJE 4.

str. 105. **24. Zadaci**

3. Ako $\leq$ znači glavno uređenje kompleksnih brojeva (v. 6.5.) tada je $1-4i<5+0\cdot i<8+6i<19+17i$

dok je $10-5i$ neuporedljiv sa ostalim brojevima.

4. 1) $8+2i$; 2) $-2+6i$; 3) $23+14i$; 4) $\frac{1}{29}(7+26i)$;

5) $-28+44i$; 8) $2\,953+2\,554i$; 9) $-182+286i$; 13) 14; 14) $27-112i$.

11. 1) Kružnica sa središtem (1, 0) i polumjerom $r=4$;

2) kružnica sa središtem (5, —4) i polumjerom 5;

3) kružnica sa središtem $\left(-\frac{5}{3}, 0\right)$ i polumjerom $\frac{4}{3}$;

4) kružnica sa središtem $\left(-1, \frac{2}{3}\right)$ i polumjerom $\frac{\sqrt{97}}{3}=3{,}28\ldots$;

5) skup od dvije tačke.

12. 1) Na kružnici polumjera 1 sa središtem (5, 0);

2) na kružnici polumjera 1 sa središtem (5. —2);

3) na kružnici polumjera 1 sa središtem (5, 6).

13. $\left(Z^{\frac{1}{2}}\right)_{1,\,2}=\pm(2{,}53+i\cdot 1{,}18)$; $\left(Z^{\frac{1}{3}}\right)_1=1{,}90+i\cdot 0{,}57$;

$\left(Z^{\frac{1}{3}}\right)_2=-1{,}45+i\cdot 1{,}36$; $\left(Z^{\frac{1}{3}}\right)_3=-0{,}45-i\cdot 1{,}93$.

17. $\cos 4x=\cos^4 x-6\cos^2 x\sin^2 x+\sin^4 x$;

$\cos 5x=\cos^5 x-10\cos^3 x\sin^2 x+5\cos x\sin^4 x$;

$\sin 6x=6\sin^5 x\cos x-15\sin^3 x\cos^3 x+6\sin x\cos^5 x$.

18. $\operatorname{tg} 3x=\dfrac{3\operatorname{tg} x-\operatorname{tg}^3 x}{1-3\operatorname{tg}^2 x}$,

$\operatorname{tg} 6x=\dfrac{6\operatorname{tg} x-20\operatorname{tg}^3 x+6\operatorname{tg}^5 x}{1-15\operatorname{tg}^2 x+15\operatorname{tg}^4 x-\operatorname{tg}^9 x}$.

19. $\sin^3 x=\frac{1}{4}(3\sin x-\sin 3x)$,

$\cos^5 x=\frac{1}{16}(\cos 5x+5\cos 3x+10\cos x)$,

$\cos^6 x=\frac{1}{32}(\cos 6x+6\cos 4x+15\cos 2x+10)$.

23. 7) Tačke kruga sa središtem u ishodištu i polumjerom 1;

8) tačke na istostranoj hiperboli $x^2-y^2=1$;

9) tačke na istostranoj hiperboli $xy=\frac{1}{2}$;

10) tačke na krivulji $e^x\cos y=1$;

11) tačke na krivulji $e^x\sin y=1$;

12) tačke na osi y;

13) tačke na kružnici sa središtem $S\left(\frac{1+a^2}{1-a^2}, 0\right)$ i polumjerom $\left|\frac{2a}{1-a^2}\right|$ ako je $a \neq 1$, a ako je $a=1$, tačke na pravulli $x=0$; odnosno tačke na kružnici sa središtem $S\left(0, \frac{1}{\operatorname{tg} b}\right)$ i polumjerom $\left|\frac{1}{\sin b}\right|$ ako je $\operatorname{tg} b \neq 0$, a ako je $\operatorname{tg} b=0$, tačke pravulje $y=0$.

28. 1) $\frac{4}{3}$; 2; $\frac{6-10i}{17}$.

POGLAVLJE 5.

str. 115. **2.8. Zadaci**

4^+) 10,197, 0,0775; 4^-) 10,362, $-0{,}0761$;

7^+) $-1{,}16287$, $-0{,}12285$; 7^-) $-1{,}389$, 0,103;

8^+) 0,1228, 1,1629; 8^-) 1,3888, $-0{,}1031$; 12) $-2{,}884$, 0,245.

str. 122. **4.3. Zadaci**

1. 2) $0{,}62\,481\cdots \pm 0{,}30\,024\cdots i$ 4) $0{,}3077\cdots-0{,}4967\cdots i$; $0{,}3138\cdots-0{,}0585\cdots i$

2. 1) -5; $\frac{13}{3}$, 2) $-\frac{4}{3}$; $-\frac{4}{7}$; 3) $\frac{a^2+b^2}{a+b}$; $\frac{a^2+b^2}{a-b}$; 4) $2a-b$, $a-2b$;

7) 7,631; $-0{,}131$, 8) $\frac{a-b}{a+b}$; $\frac{a+b}{a-b}$; 9) $\frac{5\pm\sqrt{9439}}{276}$; 10) nema rješenja.

5. $m_1=\frac{7}{5}$, $x_1=2$; $m_2=\frac{1}{2}$, $x_2=\frac{1}{2}$.

6. 6) $\frac{3}{2}<x<\frac{11}{7}$, 7) $x<\frac{10}{9}$ ili $x>\frac{8}{7}$.

7. $m=4$ ili $m=-7$.

10. 1) $m\leq-\frac{2}{3}\sqrt{2}$ ili $m\geq\frac{2}{3}\sqrt{2}$; 2) $m\geqq\frac{2}{3}\sqrt{2}$;

3) $m\in\left[-1, -\frac{2}{3}\sqrt{2}\right]\cup\left[\frac{2}{3}\sqrt{2}, 1\right]$; 4) ne postoji takav m.

11. 1) $x<-3$ ili $x>5$; 2) $x\in R\left(-3, \frac{8}{5}\right)$, 3) $x\in R\left(-\frac{1}{6}, 1\right)$,

4) $-\frac{1}{6}<x<\frac{3}{4}$; 5) $\frac{3}{2}<x<\frac{5}{2}$; 6) $\frac{3}{2}<x<\frac{11}{7}$; 7) $x<\frac{10}{9}$ ili $x>\frac{8}{7}$; 8) $-8<x<5$; 9) $x<-8$ ili $-4<x<5$ ili $6<x$,

10) $2<x<\frac{22}{5}$ ili $8<x$, 11) $x<\frac{41}{9}$; 12) $x\in R(-\infty, -15)\cup$ $\cup R(-6,3)\cup R(6, \infty)$. 14 $R(-4; 2)\cup R(3,8)\cup R(38, \infty)$.

12. 18 cm, 80 cm.

17. Ili bi prva tvornica radila 45 a druga 36 dana, ili bi prva tvornica radila 41 a druga $\frac{352}{9}$ dana.

20. 1) $x_{1,2}=2\pm\sqrt{5}$, 2) $x=\frac{1}{2}(17-\sqrt{33})$ 3) $x=\frac{1}{2}(223-15\sqrt{221})$,

4) $x_{1,2}=\pm\frac{1}{\pi r}\sqrt{l^2-\pi^2 r^2}$; 5) $x=a$.

str. 137. **6.9. Zadaci**

6. 1) $-7,\ -1\pm i\sqrt{3}$; 2) $\pm 2^{1/2}$; 3; 3) $D=-147/8$;

$U=\left(-\frac{55}{216}+\frac{7}{24}\sqrt{2}\right)^{1/3}$, $V=\left(-\frac{55}{216}-\frac{7}{24}\sqrt{2}\right)^{1/3}$; 4) $\frac{1}{2}$, $-1\pm i\sqrt{3}$.

7. 1) $x^3-6x^2+11x-6=0$; 2) $x^3-2x^2+x=0$; 3) $x^3+6x+12x+8=0$; 4) $x^3-16x^2+73x-90=0$; 5) $x^3+2x^2-53x+90=0$; 6) $x^3-6x^2-37x+90=0$; 7) $x^3-12x^2+17x+90=0$; 8) $x^3+12x^2+17x-90=0$; 9) $x^3+6x^2-37x-90=0$; 10) $x^3-2x^2-53x-90=0$; 11) $x^3+16x^2+73x+90=0$; 12) $x^3-19x^2+85x-91=0$.

8. 1) -3; $\frac{1}{2}(3\pm i\sqrt{3})$; 2) -3; $\frac{1}{2}(3\pm 5i\sqrt{3})$;

3) -7; $-1\pm i\sqrt{3}$; 4) -1; $\frac{1}{2}(-5\pm 5i\sqrt{3})$; 5) 2; $-1\pm i\sqrt{3}$;

6) $x_1=\sqrt[3]{2}-\sqrt[3]{4}$, $x_{2,3}=\frac{\sqrt[3]{4}-\sqrt[3]{2}}{2}\pm\frac{i\sqrt{3}}{2}\left(\sqrt[3]{4}+\sqrt[3]{2}\right)$;

7) $\sqrt[3]{9}-2\sqrt[3]{3}$; $\frac{2\sqrt[3]{3}-\sqrt[3]{9}}{2}\pm\frac{i\sqrt{3}}{2}(\sqrt[3]{9}+2\sqrt[3]{3})$;

8) $1-\sqrt[3]{2}-\sqrt[3]{4}$; $\frac{2+\sqrt[3]{2}+\sqrt[3]{4}}{2}\pm\frac{i\sqrt{3}}{2}(\sqrt[3]{4}-\sqrt[3]{2})$,

9) $-(1+\sqrt[3]{3}+\sqrt[3]{9})$; $\frac{-2+\sqrt[3]{3}+\sqrt[3]{9}}{2}\pm i\frac{\sqrt{3}}{2}(\sqrt[3]{9}-\sqrt[3]{3})$;

10) 2; $-1\pm 2i\sqrt{3}$; 11) 2; $-1\pm 3i\sqrt{3}$; 12) 2; $-2\pm 4\sqrt{3}\,i$;

13) 1; $-2\pm\sqrt{3}$; 14) 4; $-1\pm 4i\sqrt{3}$;

17) $-(a+b)$; $\frac{a+b}{2}\pm i\frac{\sqrt{3}}{2}(a-b)$; 18) $-(a\sqrt[3]{f^2 g}+b\sqrt[3]{fg^2})$,

$\frac{a\sqrt[3]{f^2 g}+b\sqrt[3]{fg^2}}{2}\pm\frac{i\sqrt{3}}{2}(a\sqrt[3]{f^2 g}-b\sqrt[3]{fg^2})$;

19) 2,1149; $-0{,}2541$; $-1{,}8608$; 20) 1,5981; 0,5115; $-2{,}1007$.

9. 1) 1; $-\frac{1}{2}\pm i\frac{\sqrt{3}}{2}$; 2) 3,532; 0,121; 2,347.

10. 3) Realni korijen $y_0 = 4{,}75\cdots$.

11. $n(a) = 1$ za svaki realni broj a.

15. 6,355 cm.

16. Riješiti $x^3 - 3rx^2 + 2r^2 s = 0$.

18. $k_1 k_2 = \frac{1}{4}(a-b)^2$; $x_1 x_2 = c^2$;

21. 1) $x > -1{,}769$.

22. 1) Broju $y = 2$ odgovaraju: $x_1 = 1{,}1209\cdots$, $x_2 = -1{,}5888\cdots$, $x_3 = 0{,}46\,788\cdots$. 2) Broju $x_1 = 1{,}1209\cdots$ odgovaraju: $y_1 = 2$, $y_2 = -0{,}1152\cdots$. Broju $x_2 = -1{,}5888\cdots$ odgovaraju $y_1 = 2$, $y_2 = 1{,}79\cdots$. Broju $x_3 = 0{,}46\,7888\cdots$ odgovaraju $y_1 = 2$, $y_2 = -1{,}6715\cdots$, 3) Takvi x-ovi su rješenja ove jednadžbe: $9x^5 - 32x + 40 = 0$; 4) Takvi y-ovi su rješenja ove jednadžbe: $32y^6 + 192y^4 + 384y^2 - 2025y + 256 = 0$.

str. 142. **7.3. Zadaci**

4. 3) $x_{1,2} = 1{,}0654 \pm 3{,}13\,99\,i$; $x_{3,4} = -1{,}0654 \pm 1{,}1881\,i$;
4) $x_1 = -1{,}1687$; $x_2 = -1{,}7287$; $x_{3,4} = 1{,}4487 \pm 3{,}2072\,i$;
7) $x_1 = -2{,}245$; $x_2 = -0{,}861$; $x_{3,4} = 1{,}553 \pm 2{,}302\,i$;
8) $x_1 = 1{,}791$; $x_2 = 0{,}181$; $x_{3,4} = -0{,}985 \pm 0{,}481\,i$;
9) $x_{1,2} = 0{,}792 \pm 0{,}483\,i$; $x_{3,4} = -0{,}792 \pm 2{,}005\,i$;
11) $x_{1,2} = 0{,}256 \pm 2{,}844\,i$ $x_3 = 1{,}650$; $x_4 = -4{,}162$;
13) $x_1 = 1$; $x_2 = -0{,}2626$; $x_{3,4} = -0{,}3682 \pm 1{,}1255 \cdot \sqrt{3}\,i$;
14) $x_{1,2} = 1{,}0156 \pm 3{,}4730\,i$; $x_3 = 2{,}9845$; $x_4 = -5{,}0156$;
20) $x_1 = 1{,}3632$, $x_2 = 0{,}5180$; $x_{3,4} = -0{,}9406 \pm 1{,}3956\,i$.

5. 1) $x_{1,2} = -2{,}04 \pm 1{,}33\,i$; $x_{3,4} = 1{,}04 \pm 0{,}68\,i$;
3) $x_{1,2} = 0{,}399 \pm 2{,}709\,i$; $x_{3,4} = -1{,}399 \pm 1{,}333\,i$;
4) $x_1 = -0{,}999$; $x_2 = -2{,}658$; $x_{3,4} = 0{,}829 \pm 2{,}952\,i$.

7. 1, 1, $\frac{1}{3}(-1 \pm i\sqrt{2})$.

POGLAVLJE 6.

str. 159. **3.14. Zadaci**

2. 1) da; 2) ne; 3) ne; 4) da.

8. 1) $10^0 \in 10D + 1$, $10^n \in 10D$, $n = 1, 2, 3, 4, 5, 6, 7, 8, 9$;
2) $2^0 \in 10D + 1$; $2^1 \in 10D + 2$; $2^2 \in 10D + 4$; $2^3 \in 10D + 8$; $2^4 \in 10D + 6$; $2^5 \in 10D + 2$; $2^6 \in 10D + 4$; $2^7 \in 10D + 8$; $2^8 \in 10D + 6$; $2^9 \in 10D + 2$;
3) $18 \in 10D + 8$; $18^2 \in 10D + 4$; $18^3 \in 10D + 2$; $18^4 \in 10D + 6$; $18^5 \in 10D + 8$; $18^6 \in 10D + 4$; $18^7 \in 10D + 2$; $18^8 \in 10D + 6$; $18^9 \in 10D + 8$; $18^{10} \in 10D + 4$.

9. 1) $2D + 1$; 2) $4D + 2$; 3) $2D$; 4) $2D + 1$.

10. 1) $4D$; 2) $4D + 2$; 3) $12D + 4$.

12. Skupovi S_1, S_2, S_3, S_4, S_6, S_8, su potpuni predstavnici modulo 5, nijedan od skupova S_5, S_7, S_9 to nije.

13. 1) 6, −9, 2) 8, −10; 3) 280, −80; 4) 28, −8.

14. 2) da; 3) $2D+\frac{5}{6}$; 5) da; 6) npr. svi elementi skupa $Q[0, 2]$.

str. 184. **9.9. Zadaci**

1. 1) (6, 3); 2) (−6, 3); 3) (−7, 1); 4) (7, 1); 5) (3, 95); 6) 19, 0);
8) (120, 8); 9) (15, 5); 10) (−69, 22); 11) (129, 37); 13) (159; 0,973⋯).

3. 1) −0,64279; 2) 0,9654; 3) 0,9654.

5. 6) 0; 7) 248; 8) 907; 11) 1; 1; 0; 0; 0.

7. $s=97$.

str 193. **11.8. Zadaci**

1. 1—3) 6, 168; 4) 2, 3600; 5) 12, 26 588 016; 6) 4, 266 728 600;
7) 1, 1023; 8) 1, 29 928 163.

2. 1) 17; 2) 1.

str. 205. **14.9. Zadaci**

1. 3) $P(10^n)=\{2, 5\}$; 5) $P(10^5+1)=\{11,9091\}$.

2. 1) $10\,000=2^4\cdot 5^4$; 2) $35\,000=2^3\cdot 5^4\cdot 7$; 3) $(10^5-1)(10^3-1)=3\cdot 37\cdot 11\,111$;
4) $6!=2^4\cdot 3^5\cdot 5$; 5) $25!=2^{22}\cdot 3^{10}\cdot 5^6\cdot 7^3\cdot 11^2\cdot 13\cdot 17\cdot 19\cdot 23$;
6) $100!=2^{97}\cdot 3^{48}\cdot 5^{24}\cdot 7^{16}\cdot 11^9\cdot 13^7\cdot 17^5\cdot 19^5\cdot 23^4\cdot 29^3\cdot 31^3\cdot 37^2\cdot 41^2\cdot 43^2\cdot 47^2\cdot 53\cdot 61\cdot$
$\cdot 67\cdot 71\cdot 73\cdot 79\cdot 83\cdot 89\cdot 91\cdot 97$;
7) $200!=2^{197}\cdot 3^{88}\cdot 5^{49}\cdot 7^{32}\cdot 11^{19}\cdot 13^{16}\cdot 17^{11}\cdot 19^{10}\cdot 23^8\cdot 29^6\cdot 31^6\cdot 37^5\cdot 41^4\cdot 43^4\cdot 47^4\cdot$
$\cdot 53^3\cdot 61^3\cdot 67^2\cdot 71^2\cdot 73^2\cdot 79^2\cdot 83^2\cdot 89^2\cdot 91^2\cdot 97^2\cdot 101\cdot 103\cdot 107\cdot 109\cdot 113\cdot 127\cdot 131\cdot$
$\cdot 137\cdot 139\cdot 149\cdot 151\cdot 157\cdot 163\cdot 167\cdot 173\cdot 179\cdot 181\cdot 191\cdot 193\cdot 197\cdot 199$.

str. 213. **15.10. Zadaci**

4. 1) 1010, 1 100 100, 1 111 101 000, 10 011 100 010 000
11 000 011 010 100 000, 11 110 100 001 000 000,
2) 101, 10 201, 1 101 001, 111 201 101, 12 002 011 201, 1 212 210 202 001,
3) 20, 400, 13 000, 310 000, 11 200 000, 224 000 000,
4) 13, 202, 2 626, 41 104, 564 355, 11 333 311,
5) 12, 144, 1 750, 23 420, 303 240, 3 641 100,
6) 10, 84, $6\boxed{11}4$, 5 954, $49\boxed{10}54$, 402 854,
7) $\boxed{10}$, $1\boxed{40}$, $\boxed{16}\boxed{40}$, $2\boxed{46}\boxed{40}$, $\boxed{27}\boxed{46}\boxed{40}$, $4\boxed{37}\boxed{46}\boxed{40}$,
8) $\boxed{10}$, $\boxed{100}$, $2\boxed{280}$, $\boxed{27}\boxed{280}$, $\boxed{277}\boxed{280}$, $7\boxed{257}\boxed{280}$.

5. 1) 63; 2) 2 100; 3) 333.

6. $e<b<d<a<c$.

8. 1) 10,
2) 10 (to je oznaka za broj dva u sistemu sa bazom dva),
3) 10 (to je oznaka za broj tri u sistemu sa bazom tri),
4) 10, 5) 10, 6) 10.

10. 1) $34=(100\,010)_2$, $57=(111\,001)_2$, 2) $101=(1\,100\,101)_2$, $11=(1\,011)_2$,
3) $-28=(-11\,100)_2$, $4=(100)_2$, 4) $\frac{5}{3}=(1{,}10\,101\,010\ldots)_2$.
6) $\pi=(11{,}001\,001\,000\ldots)_2$, 7) $e=(10{,}101\,101\,111\ldots)_2$.

13. 1) 24 nule; 2) 97 nula; 3) 48 nula; 4) 24 nule; 5) 12 nula.

15. 1) 512; 2) 39 366; 3) 786 432; 4) 939 524 096.

str. 219. **16.6. Zadaci**

1. 1) $2^{50}=1\ (\mathrm{I}_3)$; 2) $2^{50}=4\ (\mathrm{I}_4)$; 3) $2^{50}=4\ (\mathrm{I}_{10})$.

4. 1) $x=0$; 2) nema rješenja; 3) $x=2$ ili $x=3$; 4) $x=3$ ili $x=7$.

5. 2) x^2+x+3; 3) x^4+4; 4) x^3+3; 5) za polinome-da, za brojeve-ne;
7) $x=3$; 8) nema rješenja.

str. 233. **17.7. Zadaci**

2. 1), 2), 5), 6): nema rješenja,

str. 236. **18.4. Zadaci**

1. 1) $x\equiv 97 \pmod{105}$; 2) $105\,D+97$;
3) najveće negativno rješenje je -8, a najmanje pozitivno 97.

POGLAVLJE 7.

str. 255. **1.10. Zadaci**

2. 1) ne; 2) ne; 3) da; 4) ne.

4. Polinom $x\in S_1$ je funkcionalno jednak polinomu $x^2\in S_2$,
polinom $x+1\in S_1$ je funkcionalno jednak polinomu $x^2+1\in S_2$.

8. 2) Jedino $1+x+x^2$.

12. 2^n.

str. 261. **3.8. Zadaci**

5. 1) $x^2-2=0$; 2) $x^2-3=0$; 3) $x^4-10x^2+1=0$; 4) $x^4-8=0$;
5) $x^3-9x^2+15x-11=0$.

str. 263. **4.5. Zadaci**

1. 1) $(x^2+x+1,\ 2)$; 2) $(x^2-2x+4,\ -7)$; 3) $(x^2+x,\ 1)$;

4) $\left(\frac{5}{2}x+\frac{3}{2},\ -\frac{1}{2}x+\frac{1}{2}\right)$; 5) $\left(\frac{5}{2}x+\frac{3}{2},\ -\frac{1}{2}x-\frac{5}{2}\right)$;

6) $\left(\frac{5}{2}x+\frac{3}{2},\ -\frac{9}{2}x-\frac{1}{2}\right)$; 7) $\left(\frac{5}{2}x-\frac{3}{2},\ -\frac{1}{2}x+\frac{5}{2}\right)$;

8) $\left(-\frac{5}{2}x+\frac{3}{2},\ \frac{9}{2}x-\frac{1}{2}\right)$; 9) $\left(\frac{5}{2}x+\frac{3}{2},\ -\frac{9}{2}x-\frac{5}{2}\right)$.

2. 1) $(x+8,\ 20x+20)$;

2) $(3t^3-3,5t^2-0,25t-1,875;\ \ 2,125t+2,875)$;

4) $(0,0066x^2-0,3322x-0,06636;\ 2,2938x+1,3318)$.

3. 1) —3) da.

4. 1) da, 2) da, 3) ne, 4) da.

5. 1) $a=-1,\ b=5$; 2) $a=-16,\ b=80$; 3) $a=-1,\ b=5$.

6. 2) $-20x+15$.

7. $-r^n \sin(n-1)\alpha$.

8. $m=4$.

str. 266. **6.7. Zadaci**

3. 2) x^2-2x+3; 4) 1, 5) 1.

5. 1) $X(t)=-\frac{1}{2}$; $Y(t)=\frac{1}{4}$.

6. $6n+1,\ 6n+5$.

str. 273. **10.8. Zadaci**

1. 3) $x^3-y^3=(x-y)(x^2+xy+y^2)$, 4) $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$,

5) $x^4-1\,000xy^3=x(x-10y)(x^2+10xy+100y^2)$,

6) $a^2-1-ab-b=(a+1)(a-b+1)$,

7) $x^5-x^3-x^2+1=(x+1)(x-1)^2(x^2+x+1)$,

8) $9-x^2+9x^3-x^5=(3-x)(3+x)(1+x)(1-x+x^2)$.

7. 1) $x^4-27x^3+268x^2-1152x+1792$, 2) $x^4-11x^3-36x^2+704x-1792$,

3) $x^4+5x^3-84x^2-256x+1792$, 4) $x^4+3x^3-92x^2-192x+1792$,

5′) $x^4+19x^3+84x^2-256x-1792$, 5″) $x^4+27x^3+268x^2+1152x+1792$,

6) $x^4-4x^3+49x^2-144x+468$, 7) $x^3-(4+6i)x^2+(13+24i)-78i$,

8) x^3+3x^2+3x+1, 9) $x^3-(2i+1)x^2+(2i-1)x+1$,

10) x^3-3x^2+3x-1, 11) $x^4-8x^3+24x^2-32x+16$,

12) $x^5-8x^4+25x^3-38x^2+28x-8$.

17. 5) $x^3+3y^3=(x+\sqrt[3]{3}\,y)(x^2-\sqrt[3]{3}\,xy+\sqrt[3]{9}\,y^2)$;

6) $x^3-3y^3=(x-\sqrt[3]{3}\,y)(x^2+\sqrt[3]{3}\,xy+\sqrt[3]{9}\,y^2)$.

POGLAVLJE 8.

str. 295. **2.8. Zadaci**

1. 1) $(x, y, z)=(1, 2, -3)$; 3) $(x_1, x_2, x_3, x_4)=(-2, -3, -4, -5)$;

5) $(x_1, x_2, x_3, x_4)=\left(\frac{54}{5}, \frac{22}{5}, -\frac{17}{5}, -\frac{34}{5}\right)$; 6) $(-1, 0, -1, 0)$;

7) 1, 0, 0, 0); 8) $\left(-\frac{5}{11}, 0, \frac{2}{11}, \frac{1}{22}\right)$; 9) $(2, -1, 0, 1)$;

10) $\left(1+\frac{n(n-1)}{2}, -1, -2, \dots, -(n-1)\right)$.

POGLAVLJE 9.

str. 302. **1.13. Zadaci**

1. 11) $m^4-4m^2n^2+n^4$; 12) $-50{,}321\,160$; 13) $x^n-(xy)^{n+1}+y^{n+1}$;
15) 1; 16) 0; 17) $1+x^2+y^2$.

str. 311. **2.10. Zadaci**

1. 1) -47, 2) 119, 3) 181, 4) -316, 5) 134 810, 6) 29 693 020,
7) $3abc-(a^3+b^3+c^3)$, 8) $-x_2x_3(x_2-x_3)-x_1x_3(x_1-x_3)-x_1x_2(x_1-x_2)$,
9) 0; 10) $adf-ae^2-b^2f+2bce-c^2d$, 11) $1+a^2+b^2+c^2$, 12) 1.

2. 1), 2) abc, rezultat ne zavisi o x, y, z.

3. $x=-\frac{119}{65}$, $y=-\frac{181}{65}$, $z=\frac{316}{65}$.

5. 1) $-2(a^3+b^3)$, 2) $\sin(c-a)\sin(c-b)\sin(a-b)$.

6. 1) $x^3+a_2x^2+a_1x+a_0$, 2) $2x^3-(a+b+c)x^2+abc$, 3) $x^2+y^2+z^2+1$.

9. $\det a=-38-90i$, $\det \bar{a}=-38+90i$.

10. 1) —4) 0; 5) 12; 6) 0; 7) 0; 8) —9) 12; 10) 2.

11. 4) $x_1[(x_3-x_2)\sin 2\alpha+(y_2-y_3)\cos 2\alpha]+x_3(y_1-y_2)$,
5) $(x_2y_3-x_3y_2)-(x_1y_3-x_3y_1)+(x_1y_2-x_2y_1)$.

str. 315. **3.5. Zadaci**

1. 0) —2): -23.

2. 1) -1; 2) -1; 3) $+1$, 12) 1.

3. 1) $-81\,549$; 2) $-117\,691$; 3) $-81\,549$; 4) $141\,491$.

4. $a_3x^3+a_2x^2+a_1x+a_0$.

5. $a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$.

8. 2) 0; 3) $(ad-eh)(bc-fg)$; 4) $(bg-ah)(jh-bi)$; 5) 0; 6) 0;
7) $ef(aj-dg)$; 8) 0; 9) 0; 10) $defg-aefj$.

10. 3 700.

14. $-(a^2+b^2+c^2+d^2)^2$.

15. 1) $x=0$; 2) $x_1=0$, $x_2=-1$; 3) $x_1=0$, $x_2=1$, $x_3=2$.

16. 1) a^2-b^2; 2) $3abc-a^3-b^3-c^3$; 3) $2a^2c^2+2abcd-a^4+b^4-c^4+d^4-4ab^2c-$
$-4acd^2-2b^2d^2+2a^2bd+4bc^2d$.

str. 318. **4.7. Zadaci**

10. 0.

11. 1) 0; 2) -3; 3) $-6x-3=\pm\sqrt{3}\,i$; 4) 0; 5) 0; 6) 0.

13. 1.

POGLAVLJE 10.

str. 328. **1.7. Zadaci**

11. $\det a=0$, $\det e=34\,560$, $\det(a\cdot e)=0$.

14. Matrica ishodnih jednadžbi glasi $\begin{bmatrix}3 & -2 & 2\\ 5 & 3 & 2\end{bmatrix}$, matrica dolaznih jednadžbi
$\begin{bmatrix}26 & -14 & 36\\ 37 & 2 & 22\end{bmatrix}$.

16. 512 različitih matrica, a 5 različitih vrijednosti determinante: 0, ± 1, ± 2,

$$2=\det\begin{bmatrix}1&1&0\\0&1&1\\1&0&1\end{bmatrix}.$$

17. 512 različitih matrica, a različite vrijednosti determinante 0, ± 4,

$$4=\det\begin{bmatrix}1&-1&1\\1&1&1\\-1&1&1\end{bmatrix}.$$

18. a) 6, b) 1, c) da.

str. 336. **2.10. Zadaci**

4. 2) $\binom{k}{r}\binom{n}{s}$.

5. 1) $2^{kn}-1$; 2) $\sum\limits_{r,s}\binom{k}{r}\binom{n}{s}$, $r=1, 2, \ldots, k$; $s=1, 2, \ldots, n$; 3) $4 \cdot \inf\{k, n\}-3$.

str. 351. **4.7. Zadaci**

6. $-a=\begin{bmatrix}-2, & -3\\-5, & 7\end{bmatrix}$, $a+b=\begin{bmatrix}1&6\\9&-9\end{bmatrix}$, $a-b=\begin{bmatrix}3&0\\1&-5\end{bmatrix}$,

$$ab=\begin{bmatrix}10&0\\-33&29\end{bmatrix},\quad ba=\begin{bmatrix}13&-24\\-2&26\end{bmatrix}.$$

$$ab-ba=\begin{bmatrix}-3&24\\-31&3\end{bmatrix},\quad a^2=\begin{bmatrix}29&-15\\-25&64\end{bmatrix}$$

$$b^2=\begin{bmatrix}13&-9\\-4&16\end{bmatrix},\quad 3a+2b=\begin{bmatrix}4&15\\23&-25\end{bmatrix},$$

$$\frac{1}{3}a^2+\frac{1}{4}b^2=\begin{bmatrix}\frac{77}{12}&\frac{-29}{4}\\\frac{-28}{5}&\frac{78}{3}\end{bmatrix},\quad 3(ab)=\begin{bmatrix}30&0\\-99&87\end{bmatrix},$$

$$3\cdot a=a\cdot 3=\begin{bmatrix}6&9\\15&-21\end{bmatrix},\quad (a+b)^2=\begin{bmatrix}55&-48\\-72&135\end{bmatrix},$$

$$(a+b)^3=\begin{bmatrix}-377&762\\1143&-1647\end{bmatrix}.$$

14. 1) $x=\frac{1}{97}\begin{bmatrix}63\\43\\47\end{bmatrix}$, 2) $x=\frac{1}{97}\begin{bmatrix}-6\\19\\111\end{bmatrix}$, 3) $x=\begin{bmatrix}7\\-6\\113\end{bmatrix}$,

4) $x=\frac{1}{97}\begin{bmatrix}63&-6&7\\43&19&-6\\47&111&113\end{bmatrix}$, 5) $x=\frac{1}{97}\begin{bmatrix}77&79&49\\33&87&-59\\21&48&31\end{bmatrix}$.

str. 357. **8.9. Zadaci**

4.
$$a=\begin{bmatrix} 3 & -\frac{3}{2} & \frac{5}{2} \\ -\frac{3}{2} & 1 & 4 \\ \frac{5}{2} & 4 & 4 \end{bmatrix}+\begin{bmatrix} 0 & -\frac{7}{2} & \frac{3}{2} \\ \frac{7}{2} & 0 & 1 \\ -\frac{3}{2} & -1 & 0 \end{bmatrix},$$

$$b=\begin{bmatrix} 2-i & -\frac{3}{2}+\frac{5}{2}i & \frac{1}{2}+2i \\ -\frac{3}{2}+\frac{5}{2}i & 2 & \frac{1}{2} \\ \frac{1}{2}+2i & \frac{1}{2} & 5 \end{bmatrix}+$$

$$+\begin{bmatrix} 0 & -\frac{3}{2}-\frac{5}{2}i & -\frac{1}{2}+2i \\ \frac{3}{2}+\frac{5}{2}i & 0 & \frac{7}{2} \\ \frac{1}{2}-2i & -\frac{7}{2} & 0 \end{bmatrix},$$

$$c=\begin{bmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & i \end{bmatrix}+\begin{bmatrix} 0 & 0 & \frac{1}{2} \\ 0 & 0 & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}.$$

6. Zadovoljavaju samo a, b. c, f, g.

POGLAVLJE 11.

str. 378. **8.8. Zadaci**

3. 1) $\det a=\det b=\det c=-14$,

4. 1) $\det a^T=-14$, 2) $a+a^T=\begin{bmatrix} 6 & 2 & 11 & 7 \\ 2 & 10 & 0 & 5 \\ 11 & 0 & 4 & 4 \\ 7 & 5 & 4 & 8 \end{bmatrix}$, $\det(a+a^T)=-2479$,

3) $a\cdot a^T=\begin{bmatrix} 99 & 27 & 47 & 47 \\ 27 & 54 & 1 & 12 \\ 47 & 1 & 50 & 13 \\ 47 & 12 & 13 & 26 \end{bmatrix}$, $\det(a\cdot a^T)=196$,

4) $a^T\cdot a=\begin{bmatrix} 49 & 28 & 21 & 19 \\ 28 & 51 & 14 & 55 \\ 21 & 14 & 47 & 37 \\ 19 & 55 & 37 & 82 \end{bmatrix}$, $\det(a^T\cdot a)=196$.

str. 396. **10.8. Zadaci**

5. 1) $(a^2+b^2+c^2+d^2)^2$; 2) $a^2+b^2+c^2+d^2+e^2+f^2+g^2+h^2)^4$.

6. 1) 0, ako je $n>2$; $(x_2-x_1)(y_2-y_1)$, ako je $n=2$;

2) 0, ako je $n>2$; $\sin^2(\alpha_1-\alpha_2)$, ako je $n=2$;

3) 0, ako je $n>2$; $-\sin^2(\alpha_1-\alpha_2)$, ako je $n=2$.

17. Pomnožiti $det\ a$ i $det\,[-a_{\cdot 2}\,a_{\cdot 1}-a_{\cdot 4}\,a_{\cdot 3}\cdots-a_{\cdot 2n}\,a_{\cdot 2n-1}]$.

POGLAVLJE 13.

str. 441. **3.8. Zadaci**

1. 1) 3) da.

2. 2) da.

3. da.

4. da.

str. 465. **8.9. Zadaci**

1. 1), 4), 5), 6): da! 2), 3): ne!

8. 1), 6): da; 2), 4) 5), 7): ne!

9. 1) Da! Dimenzija je n^2; sve (n, n)-matrice koje imaju jednu jedinu vrijednost 1, a ostale su vrijednosti 0 čine bazu; 2) Da! $d=\frac{n}{2}(n+1)$; 3) Ne!

10. k) Duljina najobuhvatnije regularne podmatrice matrice koeficijenata zadanih linearnih forama $f_{k1}, f_{k2}, \ldots (k=1, 2, 3, 4, 5)$.

11. 1) Prostor P_1 što ga rađaju $a_{1\cdot}, a_{2\cdot}$, tj. prostor $P_1=\{xa_{1\cdot}+ya_{2\cdot}=$ $=[x, 2x+y, 3x+2y];\ x, y\in R\}$. 2) Prostor P_2 što ga razapinju nizovi zapisani kao stupci $a_{\cdot 1}, a_{\cdot 2}$. Inače $a_{1\cdot}, a_{2\cdot}$ non $\in P_2$ kao i $a_{\cdot 1}, a_{\cdot 2}$ non $\in P_1$. Za svaku matricu a za koju je $det\ a\neq 0$ svaki redak $a_{i\cdot}$ (stupac $a_{\cdot i}$) je linearna kombinacija stupaca (redaka) matrice a.

13. 1) Dva. Npr. prvi i treći redić su linearno nezavisni dok za ostale rediće vrijedi: $a_{2\cdot}=10a_{1\cdot}-2a_{3\cdot}$, $a_{4\cdot}=5a_{1\cdot}-a_{3\cdot}$, $a_{5\cdot}=4a_{1\cdot}-2a_{3\cdot}$.

2) Dva. Npr. prvi i drugi stupac su linearno nezavisni dok za ostale vrijedi:

$$a_{\cdot 3}=\frac{3}{2}a_{\cdot 1}-a_{\cdot 2},\quad a_{\cdot 4}=2a_{\cdot 1}+a_{\cdot 2}.$$

3) Dva; 4) Dva; 5) Skup svih jednadžbi

$$2ax_1-2bx_2+(3a+2b)x_3+(4a-2b)x_4=0$$

gdje su a, b realni brojevi.

6) Skup svih jednadžbi

$$2ax_1+(20a+4b)x_2-2bx_3+(10a+2b)x_4+(8a+4b)x_5=0$$

gdje su a, b realni brojevi.

POGLAVLJE 14.

str. 481. **5. Zadaci**

9. 1) $x=\begin{bmatrix} -\frac{1}{2} & -\frac{1}{2} \\ \frac{4}{3} & \frac{5}{3} \end{bmatrix}$; 2) $x=\begin{bmatrix} -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{4} \\ \frac{4}{3} & \frac{5}{3} & \frac{5}{2} \end{bmatrix}$; 3) ne postoji.

9′. 1) $x=\begin{bmatrix} \frac{17}{12} & -\frac{1}{2} \\ -\frac{7}{4} & \frac{1}{4} \end{bmatrix}$; 2) —5) nema rješenja.

POGLAVLJE 15.

str. 495. **2.5. Zadaci**

4. 7) 0 jer je $a_{3\cdot}=2a_{1\cdot}+a_{2\cdot}$.

str. 517. **10.1. Zadaci**

5. ne.

POGLAVLJE 16.

str. 530. **1.13. Zadaci**

2. 1) jest kvadratna forma sa determinantom: $\begin{vmatrix} 2 & 0 \\ 0 & 1 \end{vmatrix}=2$; 2) nije;

3) jest; -1; 4) Jest; 31; 5) Jest; -4; 6) Jest; 0; 7) Jest; $-\frac{25}{4}$, 8) Jest; 0.

3. 1) $[x,y]\cdot\begin{bmatrix} 2x \\ y \end{bmatrix}$; 3) $[x,y]\cdot\begin{bmatrix} 38x-27y \\ -27x+20y \end{bmatrix}$;

4) $[u,v,x,y]\cdot\begin{bmatrix} u \\ v \\ y \\ x \end{bmatrix}$; 5) $[u,v]\cdot\begin{bmatrix} 2v \\ 2u \end{bmatrix}$; 6) $[x,y]\cdot\begin{bmatrix} 0 \\ 0 \end{bmatrix}$;

7) $[u_1,u_2,u_3]\cdot\begin{bmatrix} u_1 & -\frac{5}{2}u^2 \\ & -\frac{5}{2}u_1 \\ & u_4 \end{bmatrix}$; 8) $[x_0,x_1,x_2]\begin{bmatrix} 3x_0+\frac{5}{2}x_1+7x_2 \\ \frac{5}{2}x_0-2x_1+\frac{7}{2}x_2 \\ 7x_0+\frac{7}{2}x_1+15x_2 \end{bmatrix}$.

4. 1) x^2+2y^2; 3) $20x^2+54xy+38y^2$; 4) u^2-v^2-2xy; 5) $-4uv$;

6) $0\cdot x^2+0\cdot xy+0y^2$; 7) $u_2^2+5u_1u_2+\frac{25}{4}u_4^2$;

8) $-\frac{129}{4}x_0^2-4x_1^2-\frac{49}{4}x_2^2-54x_0x_1+\frac{71}{2}x_0x_2+26x_1x_2$.

7. Npr. $a=\begin{bmatrix} 3 & -3 \\ -3 & 1 \end{bmatrix}$, općenito $a=\begin{bmatrix} 3 & \delta \\ -6-\delta & 1 \end{bmatrix}$ gdje je δ realan broj.

Za zadano b takva realna matrica postoji samo ako je $b \geqslant -6$.

str. 537. **2.9. Zadaci**

1\. 2) $x'^2-y'^2$, $x'=x+\frac{3}{2}y$, $y=\frac{\sqrt{13}}{2}y$;

3) $x'^2-y'^2$, $x'=x-\frac{3}{2}y$, $y'=\frac{\sqrt{3}}{2}y$;

4) $-x'^2+y'^2$, $x'=x-\frac{3}{2}y$, $y'=\frac{\sqrt{13}}{2}y$;

6) $-x'^2+y'^2$, $x'=x-\frac{3}{2}y$, $y'=\frac{\sqrt{5}}{2}y$;

7) $-x'^2+y'^2$, $x'=x+\frac{3}{2}y$, $y'=\frac{\sqrt{5}}{2}y$;

8) $x'^2-y'^2-z'^2$, $x=x'-y+\frac{5}{2}z$, $y'=2y-\frac{5}{4}z$, $z'=\frac{\sqrt{43}}{4}z$;

11) $-x'^2+y'^2+z'^2$, $x'=\frac{1}{2}x+\frac{1}{2}y-z$, $y'=\frac{1}{2}x-\frac{1}{2}y$, $z'=z$.

str. 547. **5.4. Zadaci**

4\. Pozitivno-definitivna je forma 5).

9\. 1) $x_1=\frac{2}{3}y_1-\frac{1}{2}y_2+\frac{2}{3}y_3$, $x_2=\frac{2}{3}y_1+\frac{2}{3}y_2-\frac{1}{3}y_3$,

$x_3=-\frac{1}{3}y_1+\frac{2}{3}y_2+\frac{2}{3}y_3$; kanonski oblik: $3y_1^2+6y_2^2+9y_3^2$;

2) $x_1=\frac{2}{3}y_1+\frac{2}{3}y_2-\frac{1}{3}y_3$, $x_2=-\frac{1}{3}y_1+\frac{2}{3}y_2+\frac{2}{3}y_3$,

$x_3=\frac{2}{3}y_1-\frac{1}{3}y_2+\frac{2}{3}y_3$, kanonski oblik: $9y_1^2+18y_2^2-9y_3^2$;

3) $x_1=\frac{1}{\sqrt{3}}y_1+\frac{1}{\sqrt{6}}y_2+\frac{1}{\sqrt{2}}y_3$, $x_2=-\frac{1}{\sqrt{3}}y_1-\frac{1}{\sqrt{6}}y_2+\frac{1}{\sqrt{2}}y_3$,

$x_3=\frac{1}{\sqrt{3}}y_1-\frac{2}{\sqrt{6}}y_2$, kanonski oblik: $3y_1^2+6y_2^2-2y_3^2$;

4) $x_1=\frac{1}{\sqrt{3}}y_1+\frac{1}{\sqrt{6}}y_2+\frac{1}{\sqrt{2}}y_3$, $x_2=\frac{1}{\sqrt{3}}y_1+\frac{1}{\sqrt{6}}y_2-\frac{1}{\sqrt{2}}y_3$,

$x_3=\frac{1}{\sqrt{3}}y_1-\frac{2}{\sqrt{6}}y_2$, kanonski oblik: $5y_1^2-y_2^2-y_3^2$;

5) $x_1=\frac{1}{3}y_1-\frac{2}{3}y_2+\frac{2}{3}y_3$, $x_2=\frac{2}{3}y_1-\frac{1}{3}y_2-\frac{2}{3}y_3$,

$x_3=\frac{2}{3}y_1+\frac{2}{3}y_2+\frac{1}{3}y_3$, kanonski oblik: $9y_1^2+18y_2^2+18y_3^2$;

6) $x_1=\frac{2}{3}y_1+\frac{1}{6}\sqrt{2}y_2+\frac{1}{2}\sqrt{2}y_3,\quad x_2=\frac{1}{3}y_1-\frac{2}{3}\sqrt{2}y_2,$

$x_3=\frac{2}{3}y_1+\frac{1}{6}\sqrt{2}y_2-\frac{1}{2}\sqrt{2}y_3,$ kanonski oblik: $3y_1^2-6y_2^2$;

7) $x_1=\frac{2}{3}y_1+\frac{1}{2}\sqrt{2}y_2+\frac{1}{6}\sqrt{2}y_3,\quad x_2=\frac{1}{3}y_1-\frac{2}{3}\sqrt{2}y_3,$

$x_3=\frac{2}{3}y_1-\frac{1}{2}\sqrt{2}y_2+\frac{1}{6}\sqrt{2}y_3,$ kanonski oblik: $9y_1^2+9y_2^2-9y_3^3$;

8) $x_1=\frac{1}{2}(y_1+y_2+y_3+y_4)\quad x_2=\frac{1}{2}(-y_1+y_2+y_3-y_4),$

$x_3=\frac{1}{2}(-y_1-y_2+y_3+y_4),\quad x_4=\frac{1}{2}(y_1-y_2+y_3-y_4),$

kanonski oblik: $2y_1^2+4y_2^2-2y_3^2-4y_4^2$;

9) $x_1=\frac{1}{2}(y_1+y_2+y_3+y_4),\quad x_2=\frac{1}{2}(y_1-y_2-y_3+y_4),$

$x_3=\frac{1}{2}(y_1+y_2-y_3-y_4),\quad x_4=\frac{1}{2}(y_1-y_2+y_3-y_4);$

kanonski oblik: $4y_1^2+8y_2^2+12y_3^2-4y_4^2$;

10) $x_1=\frac{1}{5}\sqrt{5}(2y_1+y_2),\quad x_2=\frac{1}{5}\sqrt{5}(y_1-2y_2),\quad x_3=\frac{1}{5}\sqrt{5}(2y_3+y_4),$

$x_4=\frac{1}{5}\sqrt{5}(-y_3+2y_4),$ kanonski oblik: $5y_1^2-5y_2^2+5y_3^2$;

12) $x_1=y_1,\quad x_2=\frac{1}{3}(y_2+2y_3+2y_4),\quad x_3=\frac{1}{3}(2y_2+y_3-2y_4),$

$x_4=\frac{1}{3}(2y_2-2y_3+y_4),$ kanonski oblik: $9y_1^2+9y_2^3+9y_3^2$;

13) $x_1=\frac{1}{5}\sqrt{5}(2y_1+y_5),\quad x_2=\frac{1}{5}\sqrt{5}(-y_1+2y_5),\quad x_3=y_2,$

$x_4=\frac{1}{13}\sqrt{13}(2y_2+3y_4),\quad x_5=\frac{1}{13}\sqrt{13}(3y_2-2y_4),$

kanonski oblik: $5y_1^2+5y_2^2+5y_3^2-8y_4^2$;

14) $x_1=y_1,\quad x_2=\frac{1}{5}\sqrt{5}(y_2+2y_4),\quad x_3=\frac{1}{5}\sqrt{5}(-2y_2+y_4),$

$x_4=\frac{1}{10}\sqrt{10}(y_3+3y_5),\quad x_5=\frac{1}{10}\sqrt{10}(3y_3-y_5),$

kanonski oblik: $4y_1^2+4y_2^2+4y_3^3-6y_4^2-6y_5^2$;

15) $x_1=\frac{1}{5}\sqrt{5}(2y_1+y_2)$, $x_2=\frac{1}{5}\sqrt{5}(y_1-2y_2)$, $x_3=\frac{1}{10}\sqrt{10}(3y_3+y_4)$,

$x_4=\frac{1}{10}\sqrt{10}(-y_3+3y_4)$, $x_5=\frac{1}{5}\sqrt{5}(2y_5+y_6)$,

$x_6=\frac{1}{5}\sqrt{5}(y_5-2y_6)$, kanonski oblik: $5y_1^2-5y_2^2+5y_3^2-5y_4^2+5y_5^2$.

str. 591. **7.15. Zadaci**

3. 6) $5x_1\bar{x}_1+6x_2\bar{x}_2+(2+i)\bar{x}_1x_2+(2-i)x_1\bar{x}_2$,

7) $4x_1\bar{x}_1+(3+4i)\bar{x}_1x_2+(3-4i)x_1\bar{x}_2$.

str. 565. **9. Zadaci**

1. 1) $\left[3^{-\frac{1}{2}}(x+y)\right]^2+\left[3^{-\frac{1}{2}}(y+z)\right]^2+\left[3^{-\frac{1}{2}}(z+x)\right]^2$, $r=3$, $\sigma=3$;

2) $(x+y)^2+(y+2z)^2+z^2$; $r=3=\sigma$;

3) $\left[2^{-\frac{1}{2}}(x+z)\right]^2-\left[2^{-\frac{1}{2}}(t-y)\right]^2-\left(2^{-\frac{1}{2}}x\right)^2-\left(2^{-\frac{1}{2}}t\right)^2$, $r=4$, $\sigma=-2$.

2. 1) Matrica kvadratne forme $1_{(n)}+\delta$; $\sigma=n$;

2) Ako je $n=2$ normalni oblik je ovaj:

$$y_1^2+y_2^2,\quad y_1=\sqrt{2}\,x_1+\frac{\sqrt{2}}{2}x_2,\quad y_2=\sqrt{\frac{3}{2}}\,x_2.$$

Ako je $n=3$, normalni oblik te kvadratne forme je ovaj:

$$y_1^2+y_2^2+y_3^2,\quad y_1=\sqrt{2}\,x_1+\frac{\sqrt{2}}{2}x_2+\frac{\sqrt{2}}{2}x_3,\quad y_2=\sqrt{\frac{3}{2}}\,x_2+\frac{1}{\sqrt{6}}x_3,$$

$$y_3=\sqrt{\frac{4}{3}}\,x_3.$$

Slučaj n: forma je $=\sum_{i=2}^{n}\left\{\left(\frac{i}{i-1}\right)^{\frac{1}{2}}x_{i-1}+\frac{x_i+x_{i+1}+\cdots x_n}{\left[(i-1)i\right]^{\frac{1}{2}}}\right\}^2+\frac{n+1}{n}x_n^2$;

dokazuje se induktivno (isp. Obrešov [3], 170).

POGLAVLJE 18.

str. 686. **8. Zadaci**

1. Korijeni su jedinice:

reda 3: 1, $-0{,}50\,000\pm i\cdot 0{,}86\,603$,

reda 4: ± 1, $\pm i$,

reda 5: 1, $0{,}30\,902\pm i\,0{,}95\,106$, $-0{,}80\,902\pm i\cdot 0{,}58\,779$;

reda 6: ± 1, $0{,}50\,000\pm i\cdot 0{,}86\,603$, $-0{,}50\,000\pm i\cdot 0{,}86\,603$,

reda 7: 1, $0{,}62\,343\pm i\cdot 0{,}78\,188$, $-0{,}22\,240\pm i\,0{,}97\,496$, $-0{,}90\,095\pm i\cdot 0{,}43\,392$

reda 8: ± 1, $\pm i$, $\pm 0{,}70\,711\pm i\cdot 70\,711$,

reda 9: 1, $0{,}76\,604\pm i\cdot 0{,}64\,279$, $0{,}17\,365\pm i\cdot 0{,}98\,481$, —
$-0{,}50\,000\pm i\,0{,}86\,603$, $-0{,}93\,969\pm i\cdot 0{,}34\,202$,

reda 10: ± 1, $\pm 0{,}80\,902\pm i\,0{,}58\,779$, $\pm 0{,}30\,902\pm i\cdot 0{,}95\,106$.

U otvorenom prvom kvadrantu leže od tih korijena jedinice:
$0{,}30\,902+i\cdot 0{,}95\,106$, $0{,}50\,000+i\cdot 0{,}86\,603$, $0{,}62\,243+i\cdot 0{,}78\,188$, $0{,}70\,711+i\cdot 0{,}70\,711$, $0{,}76\,604+i\cdot 0{,}64\,279$, $0{,}17\,365+i\cdot 0{,}98\,481$.

U otvorenom drugom kvadrantu leže ovi od tih korijena jedinice:
$-0{,}50\,000+i\cdot 0{,}86\,603$, $-0{,}80\,902+i\cdot 0{,}58\,779$, $-0{,}22\,240+i\cdot 0{,}97\,496$, $-0{,}90\,095+i\cdot 0{,}43\,392$, $-0{,}70\,711+i\cdot 0{,}70\,711$, $-0{,}93\,969+i\cdot 0{,}34\,202$, $-0{,}30\,902+i\cdot 0{,}95\,106$.

2. Primitivni su korijeni jedinice

reda 3: $e^{i\frac{2\pi}{3}},\ e^{i\frac{4\pi}{3}}$;

reda 4: $i,\ -i$;

reda 5: $e^{i\frac{2\pi}{5}},\ e^{i\frac{4\pi}{5}},\ e^{i\frac{6\pi}{5}},\ e^{i\frac{8\pi}{5}}$;

reda 6: $e^{i\frac{\pi}{3}},\ e^{i\frac{5\pi}{3}}$;

reda 7: $e^{i\frac{2\pi}{7}},\ e^{i\frac{4\pi}{7}},\ e^{i\frac{6\pi}{7}},\ e^{i\frac{8\pi}{7}},\ e^{i\frac{10\pi}{7}},\ e^{i\frac{12\pi}{7}}$;

reda 8: $e^{i\frac{\pi}{4}},\ e^{i\frac{3\pi}{4}},\ e^{i\frac{5\pi}{4}},\ e^{i\frac{7\pi}{4}}$;

reda 9: $e^{i\frac{2\pi}{9}},\ e^{i\frac{4\pi}{9}},\ e^{i\frac{8\pi}{9}},\ e^{i\frac{10\pi}{9}},\ e^{i\frac{14\pi}{9}},\ e^{i\frac{16\pi}{9}}$;

reda 10: $e^{i\frac{\pi}{5}},\ e^{i\frac{3\pi}{5}},\ e^{i\frac{7\pi}{5}},\ e^{i\frac{9\pi}{5}}$;

reda 12: $e^{i\frac{\pi}{6}},\ e^{i\frac{5\pi}{6}},\ e^{i\frac{7\pi}{6}},\ e^{i\frac{11\pi}{6}}$;

reda 24: $e^{i\frac{\pi}{12}},\ e^{i\frac{5\pi}{12}},\ e^{i\frac{7\pi}{12}},\ e^{i\frac{11\pi}{12}},\ e^{i\frac{13\pi}{12}},\ e^{i\frac{17\pi}{12}},\ e^{i\frac{19\pi}{12}},\ e^{i\frac{23\pi}{12}}$.

3. 1 (stepen 1), -1 (stepen 2), $\cos 30^\circ + i\sin 30^\circ$ (stepen 12), $\cos\frac{2\pi}{17}+i\sin\frac{2\pi}{17}$ (stepen 17), $e^{i\frac{2\pi}{35}}$ (stepen 35)

4. 1) 0; 2) 0) pri $\varepsilon_n \neq 1$; 3) $\frac{2}{1-\varepsilon_n}$.

5. 1) $-\frac{n}{1-\varepsilon}$ ako je $\varepsilon \neq 1$,

$\frac{n(n+1)}{2}$ ako je $\varepsilon = 1$,

2) $-\frac{n^2(1-\varepsilon)+2n}{(1-\varepsilon)^2}$ ako je $\varepsilon \neq 1$,

$\frac{n(n+1)(2n+1)}{6}$ ako je $\varepsilon = 1$.

6. Jest!

13. 1) $0,\ e^{ik\frac{2\pi}{n}}$ $(k=0, 1, 2, \ldots, n-1)$;

2) $i \operatorname{ctg}\frac{k\pi}{n}$ $(k=1, 2, \ldots, n-1)$; 3) $\operatorname{ctg}\frac{k\pi}{n}$, $(k=1, 2, \ldots n-1)$.

15. $\Phi_3(x)=x^2+x+1$, $\Phi_4(x)=x^2+1$, $\Phi_5(x)=x^4+x^3+x^2+x+1$,

$\Phi_6(x)=x^2-x+1$, $\Phi_{12}(x)=x^4-x^2+1$, $\Phi_{20}(x)=x^8-x^6+x^4-x^2+1$.

16. 1) $\Phi_n(1)=1$,

2) $\Phi_2(-1)=0$, $\Phi_n(-1)=2$ ako je $n=2^k>1$,

$\Phi_n(-1)=p$ ako je $n=2p^\alpha$, p neparan prost broj,

$\Phi_n(-1)=1$ ako je $n=2n_1$, n_1 neparno,

$\Phi_n(-1)=1$ u ostalim slučajevima.

17. $\sqrt{n}$ ako je n neparno, $\sqrt{n\left(1+(-1^{\frac{n}{2}}\right)}$ ako je n parno.

18. $\frac{1}{2}\left[\mu(n)^2-\mu(n)\right]$ pri neparnom n; $\frac{1}{2}\left[\mu(n)^2+\mu(n)\right]$ pri $n=2(2m-1)$;

$\mu\left(\frac{n}{2}\right)$ pri $n=2^k(2m-1)$; $k>1$.

POGLAVLJE 19.

str. 703. **8. Zadaci**

1. 4) $\sigma_1=-13$, $\sigma_2=52$, $\sigma_3=-60$,

5) $\sigma_1=0$, $\sigma_2=-1$, $\sigma_3=0$,

6) $\sigma_1=-\frac{1}{2}n(n+1)$, $\sigma_2=\frac{1}{24}n(n+1)(n-1)(3n+2)$,

$\sigma_3=-\frac{1}{48}n^2(n+1)^2(n-1)(n-2), \ldots, \sigma_n=(-1)^n n!$

3. Polinom [2, 1] od n varijabla ima $n(n-1)$ članova.

3a. Polinom [1, 2, 3] od n varijabla ima $n(n-1)(n-2)$ članova.

4. 1) da, 2) ne, 3) ne, 4) da, 5) da, 6) da, 7) ne, 8) da, 9) da.

7. 1) $[1]=\sigma_1^2-2\sigma_2$, 2) $[3]=-\sigma_1^3+3\sigma_1\sigma_2+3\sigma_3$,

3) $[1, 2]=-\sigma_1\sigma_2+3\sigma_3$, 4) $[1,3]=\sigma_1^3\sigma_2-\sigma_1\sigma_3-2\sigma_2^2+4\sigma_4$.

5) $[1, 2, 3]=\sigma_1\sigma_2\sigma_3-3\sigma_1^2\sigma_4-3\sigma_3^2+4\sigma_2\sigma_4+7\sigma_1\sigma_5-12\sigma_6$,

6) $[2, 2, 1]=-\sigma_2\sigma_3+3\sigma_1\sigma_4-5\sigma_5$,

7) $[4. 1, 1]=\sigma_1^3\sigma_3-3\sigma_1\sigma_2\sigma_3-\sigma_1^2\sigma_4+3\sigma_3^2+2\sigma_2\sigma_4+\sigma_1\sigma_5-6\sigma_6$,

8) $[2, 2, 2]=\sigma_3^2-2\sigma_2\sigma_4+2\sigma_1\sigma_5-2\sigma_6$,

9) $[1, 5]=\sigma_1^4\sigma_2-4\sigma_1^2\sigma_2^2-\sigma_1^3\sigma_3+2\sigma_2^3+7\sigma_1\sigma_2\sigma_3+\sigma_1^2\sigma_4-$
$-3\sigma_3^2-6\sigma_2\sigma_4-\sigma_1\sigma_5+6\sigma_6$,

10) $[1,\ 1,\ 2,\ 2]=\sigma_2\sigma_4-4\sigma_1\sigma_5+9\sigma_6$.
Konkretizacijom $n=5$ dobivaju se jednakosti koje nastaju iz prethodnih uvrsti li se $\sigma_6=0$.

8. 1) $-\sigma_1^2+3\sigma_1\sigma_2$, 2) $\sigma_1^4-4\sigma_1^2\sigma_2+8\sigma_1\sigma_3$, 3) $-\sigma_1\sigma_2+\sigma_3$,
4) $\sigma_1^2\sigma_2^2-4\sigma_1^3\sigma_3-4\sigma_2^2+18\sigma_1\sigma_2\sigma_3-27\sigma_3^2$,

9. 1) $(n-)\,\sigma_1^2-2\,n\,\sigma_2$,
2) $(n-1)\,\sigma_1^4-4\,n\,\sigma_1^2\sigma_2+2\,(n+6)\,\sigma_2^2+4\,(n-3)\,\sigma_1\sigma_3-4\,n\,\sigma_4$,
3) $-(n-1)\,\sigma_1^3+3\,(n-2)\,\sigma_1\sigma_2-3\,(n-4)\,\sigma_3$,
4) $\dfrac{3\,(n-1)\,(n-2)}{2}\,\sigma_1^2-(3\,n-1)\,(n-2)\,\sigma_2$.

10. $$(n-1)!\sum_{i=1}^{n} z_i^2\sigma_1^2-2\,(n-2)!\left[n\sum_{i=1}^{n} z_i^2-\left(\sum_{i=1}^{n} a_i\right)^2\right]\sigma_2.$$

11. 1) $s_\nu=\begin{cases}(-1)^{\frac{\nu}{2}}\cdot 2 & \text{ako je } \nu \text{ paran broj}\\ 0 & \text{ako je } \nu \text{ neparan broj.}\end{cases}$

2) $s_\nu=\begin{cases}3 & \text{ako je } \nu \text{ kratnik od 3.}\\ 0 & \text{ako } \nu \text{ nije kratnik od 3.}\end{cases}$

12. $s_2=13$, $s_3=35$, $s_4=97$, $s_5=275$.

13. 1) 2, 2) 2, 3) 3, 4) 4, 5) 7, 6) 6, 7) 2, 8) 8, 9) $4\,n-4$ 10) $2\,n$.

14. 1) $[1,2]=30$, $[2,\ 3]=180$, 2) $[1,\ 2]=1$, $[1,\ 4]=\dfrac{25}{27}$,
3) $[3,\ 3]=\dfrac{131}{8}$, $[3,\ 4]=-\dfrac{25}{8}$.

15. 1) $a_1^2a_2^2-4\,a_1^3a_3-4\,a_2^3a_0+18\,a_0a_1a_2a_3-27\,a_0^2a_3^2$,
2) $a_1^3a_3-a_2^3a_0$, 3) $a_1^2a_2^2-a_1^3a_3-a_2^3a_0$,
4) $-\dfrac{2\,a_1^3a_2^2a_3}{a_0^5}+14\dfrac{a_1^3a_3^2}{a_0^5}+26\dfrac{a_2^3a_3}{a_0^4}-120\dfrac{a_1a_2a_3^2}{a_0^4}+135\dfrac{a_3^3}{a_0^2}$; 5) $\dfrac{a_1a_2}{a_0a_3}-9$,

u konkretnom je slučaja $a_0=3$, $a_1=-5$, $a_2=0$, $a_3=1$, tj.

1) -241, 2) -125, 3) 125, 4) $-\dfrac{535}{243}$, 5) -9.

16. 1) $m=-\dfrac{1}{5}$, 2) nije moguće, 3) $25\,m^2-20\,m-25=0$,
4) $a^3-4\,ab+8\,c=0$, 5) $2\,a^3-9\,ab+27\,c=0$,
6) $(b-c)^2+(a-1)^2\,c=0$, 7) $c\neq 0$, $a^3\,c=b^3$, 8) $q=-1$, 9) $m=\dfrac{21}{8}$,
10) $m=\dfrac{13}{4}$, 11) $a=\pm 4\lambda\mu$, $b=2\lambda^2\mu+\mu^2$.

17. 1) $s_3=0$, $s_5=0$, $s_7=0$, 2) $s_3=-3$, $s_5=-15$, $s_7=-63$.

24. 1) $-\dfrac{p^2}{q}$, 2) $\dfrac{2p-3q}{1+p-q}$, 3) $\dfrac{2p+3q}{q-p-1}$, 4) -3, 5) $\dfrac{3q}{1+p-q}$.

26. 2) $\sum_{k=1}^{n} \frac{\partial x_k}{\partial \sigma_i} = (-1)^{i-1}(u-1)\sigma_{i-1}$,

3) $det\ f = (-1)^{\nu} \prod_{\substack{k,j \\ 1 \leq k < j \leq n}} (x_k - x_j)$,

gdje je $\nu = \frac{n+1}{2}$ ako je n neparan a $\nu = \frac{n}{2}$ ako je n paran broj.

30. Ako je $a(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, tada je $\prod_i (1-x_i) = 1 + a_1 + \cdots + a_n$;
u specijalnom slučaju $a(x) = 1 + x + \cdots + x^{n-1}$, $\prod_i (1-x_i) = n$.

POGLAVLJE 20.

str. 722. **7. Zadaci**

1. 1) 33; 2) -21; 3) 1; 4) -1; 5) -11; 6) -7; 7) 243; 8) 0;
9) -59; 10) 4854; 11) $(b_0 a_2 - b_2 a_0)^2 - (b_0 a_1 - b_1 a_0)(b_1 a_2 - b_2 a_1)$,

12) $R(X_m, X_n) = \begin{cases} 0 & \text{ako je } m = n \\ p^{\varphi(n)} & \text{ako je } m = n p^{\lambda},\ p \text{ prost broj} \\ 1 \text{ u} & \text{ostalim slučajevima} \end{cases}$;

13) $R(X_n, x^m - 1) = \begin{cases} 0 \text{ ako je } \frac{n}{M(m,n)} = 1 \\ p^{\frac{\varphi(n)}{\varphi(n_1)}}, \quad n_1 = \frac{n}{M(m,n)} = p^{\lambda},\ p \text{ prost broj} \\ 1 \text{ u ostalim slučajevima} \end{cases}$.

2. 1) $i\sqrt{2}$ (ne postoji takav realan λ), 2) λ ne postoji.
3) $\lambda = -2{,}405\ldots$; 4) realno λ ne postoji; 5) $\lambda = -8$.
6) $\lambda = 3$ ili $\lambda = -1$, 7) $\lambda_1 = 1$, $\lambda_{2,3} = \frac{-2 + \sqrt{2} \pm \sqrt{4\sqrt{2} - 2}}{2}$,
8) $\lambda_{1,2} = \pm\sqrt{-2}$, $\lambda_{3,4} = \pm\sqrt{-12}$, (tj. λ nije realno). 9) $\lambda_1 = -6$, $\lambda_2 = -24$.

3. 1), 2): 1. Naime, definira se $D(ax+b) = 1$ pri $a \neq 0$, 3) -11, 4) -275,
5) -783, 6) 0, $9680 = D(x^4 + 3x^2 + 5)$, $29\,813 = D(x^4 + 3x + 5)$,
8) 49, 9) -107, 10) -843, 11) 725, 12) 2777, 13) $3125(b^2 - 4a^5)^2$,
14) $\lambda^4(4\lambda - 27)^3$, 15) $(b^2 - 3ab + 9a^2)^2$, 16) $(-1)^{\frac{n(n-1)}{2}} n^n a^{n-1}$,
17) $(-1)^{\frac{n(n-1)}{2}} n^n q^{n-1} + (-1)^{\frac{(n-1)(n-2)}{2}} (n-1)^{n-1} p^n$.

4. 1) $9y - 13 = 0$, 2) $13y^2 - 30y - 375 = 0$.
4) $y^6 - 4y^4 + 3y^2 - 12y + 12 = 0$, 6) $y^3 + 4y^2 - y - 4 = 0$,

5. 1) $x_1 = 1$, $x_2 = 2$, $x_3 = 0$, $x_4 = -2$,
$y_1 = 2$, $y_2 = 3$; $y_3 = -1$, $y_4 = 1$.

2) $x_1=0,\quad x_2=3,\quad x_3=2,\quad x_4=2,$
$y_1=1,\quad y_2=0,\quad y_3=2,\quad y_4=-1.$

3) $x_1=1,\quad x_2=1,\quad x_3=-1,\quad x_4=2.$
$y_1=-1,\quad y_2=-1,\quad y_3=1,\quad y_4=2.$

4) $x_1=0,\quad x_2=0,\quad x_3=1,\quad x_4=1,\quad x_{5,6}=2,$
$y_1=1;\quad y_2=3,\quad y_3=2;\quad y_4=3;\quad y_{5,6}=1\pm i\sqrt{2}.$

5) $x_1=0,\quad x_2=0,\quad x_3=2,\quad x_4=x_5=2,\quad x_6=-4,\quad x_7=4,\quad x_8=-6,\quad x_9=\frac{2}{3}.$
$y_1=2;\quad y_2=-2,\quad y_3=0,\quad y_4=y_5=2,\quad y_6=2,\quad y_7=6,\quad y_8=4,\quad y_9=\frac{4}{3}.$

6. 1) $\lambda=0$, 2) $\lambda=0$, 3) $\lambda=0$ (ako je $k>1$), 4) $\lambda=\pm\frac{10}{3}\sqrt{\frac{10}{3}}$,

5) $\lambda_1=3,\quad \lambda_{2,3}=3\left(-\frac{1}{2}\pm\frac{i\sqrt{3}}{2}\right)$, 6) $\lambda_1=0,\quad \lambda_2=-3,\quad \lambda_3=125,$

7) $\lambda_1=-1,\quad \lambda_2=-\frac{3}{2},\quad \lambda_{3,4}=\frac{7}{2}\pm i\frac{9}{2}\sqrt{3}.$

8) $\lambda_1=0,\quad \lambda_2=\frac{1}{4}$, 9) $\lambda_{1,2}=\pm 2{,}3507\ldots.$

8. 1) $(-1)^{\frac{n(n-1)}{2}}(n!)^n$; 2) $1\cdot 2^2\cdot 3^3\cdots(n-1)^{n-1}n^n$; 3) $1\cdot 2^3\cdot 3^5\cdots n^{2n-1}$;
4) $2^{n-1}n^n$; 5) $1\cdot 2^3\cdot 3^3\cdots n^{2n-1}\cdot 1^{2(n-1)}\cdot 3^{2(n-2)}\cdots(2n-3)^2$.

POGLAVLJE 21.

str. 740. **6. Zadaci**

1. 1) $x=t-\frac{5}{4}$, $16t^2-73=0$; 2) $x=t-\frac{2}{3}$, $27t^3+99t-236=0$.

2. 1) $2t^2+13t+12=0$; 2) $t^3+8t^2+25t+20=0$;
3) $t^3+9t^3+32t^2+57t+36=0$; 4) $t^4+9t^3+32t^2+57t+48=0$.

3. 1) Kvocijent $2x+15$ ostatak 69;
2) Kvocijent $x^2+7x+40$ ostatak 194;
3) Kvocijent $x^3+6x^2+32x+165$ ostatak 819;
4) Kvocijent $x^3+6x^2+32x+165$ ostatak 831;
5) Kvocijent $x^3+4x^2+18x+85$ ostatak 314;
6) Kvocijent $x^4+8x^3+40x^2+200x+1000$ ostatak 5000;
7) Kvocijent $x^7+11x^6+55x^5+275x^4+1375x^3+6875x^2$
$+34375x+171\,874$ ostatak 859 371.

POGLAVLJE 23

str. 810. **2,11. Zadaci**

10. 3) $\frac{(1,\ 2,\ 1,\ 3)}{\sqrt{15}},\quad \frac{(10,\ -1,\ 1,\ -3)}{\sqrt{111}},\quad \frac{(19,\ -87,\ -61,\ 72)}{\sqrt{15\,835}}.$

12. $\cos A=\frac{5}{\sqrt{39}},\quad \cos B=\frac{8}{\sqrt{78}},\quad \cos C=-\frac{\sqrt{2}}{3}.$

LITERATURA

Albert A. A.

[1] Structure of algebras, New York 1939, 12 + 210.

[2] Introduction to algebraic theories, Chicago 1941, 8 + 138.

Alendoerfer C. B. — Cletus Oakley

[1] Principi matematike (prevela Jelena Stojanović), Beograd 1961, XVI + 411 (gl. 1: logika).

Aljančić Slobodan

[1] Uvod u realnu i funkcionalnu analizu. Građevinska knjiga, Beograd 1968, 6+327.

Anđelić T. P.

[1] Teorija vektora, Beograd 1947, 8 + 408.

[2] Tenzorski račun, Beograd, 8 + 320.

[3] Matrice, Beograd 1962, 268 str.

Arow K. J. — Nurwitz L. N. — Uzawa H.

[1] Studies in linear and non-linear programming, Stanford 1958 (ruski, Moskva 1962, 334).

Bachmann P.

[1] Zahlentheorie. Versuch einer Gesamtdarstellung dieser Wissenschaft in ihren Hauptteilen. I - Die Elemente der Zahlentheorie, Leipzig 1892, 12 + 264; II - Die analytische Zahlentheorie; 1894, 18 + 494; III - Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie, 1872, 12 + 300; IV - Die Arithmetik der quadratischen Formen, 1. Abt. 1898, 16 + 668; V - Allgemeine Arithmetik der Zahlenkörper, 1905, 22 + 548.

[2] Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie, Leipzig 1872, 12 + 300.

Ball, W. W. Rouse

[1] A short account of the History of mathematics, London 1908_4, 24 + 522.

Barsov A. S.

[1] Čto takoe linejnoje programmirovanije, Moskva 1959, 104.

Behnke H. (sa saradnicima)

[1] Grundzüge der Mathematik, I Grundlagen. Arithmetik und Algebra; Göttingen 1962_2, 14 + 572.

Bell E. T.

[1] The development of mathematics, New York—London 1945_2, 12 + 638.

Berezin I. S. — Židkov N. P.

[1] Metodi vičislenij II, Moskva 1962_2, 639.

Bhagavantam S. — Venkatarayudu T.

[1] Theory of groups and its application to physical problems, Andhra Univ., Waltair 1951_2 (ruski, Moskva 1959, 301).

Bieberbach L. — Bauer G.

[1] Algebra, Leipzig—Berlin 1933_5, 10 + 358.

Bilimović Anton

[1] Geometrijske osnove Računa sa diodama I Dioda i afinor. Srpska akademija Nauka. Posebna izdanja 72 (1930) 14+232.

Birkhoff Garrett
[1] Lattice theory, New York, 1948_2, 14 + 283.
Birkhoff G. — Mac Lane S.
[1] A survey of modern algebra, New York 1953, 12 + 472.
Blanuša D.
[1] Viša matematika I dio; prvi svezak. Algebra i algebarska analiza, Zagreb I_1 1963, 483, I_2 (1965) s. 927; II_1 (1969) 403.
Bodewig E.
[1] Matrix Calculus, Amsterdam 1959_2, 12 + 452.
Boerner H.
[1] Darstellungen von Gruppen, Berlin — Göttingen — Heidelberg 1955. 12 + 287.
Boole George
[1] The mathematical analysis of logic, Cambridge 1847, 82.
Borevič Z. I. — Šafarevič I. R.
[1] Teorija čisel, Moskva 1964, 568.
Borůvka O.
[1] Uvod do teorie grup, Praha 1944_1, 1952_2.
[2] Grundlagen der Gruppoid — und Gruppentheorie, Berlin 1960, 12 + 198.
Bourbaki N.
[1] Éléments de Mathématiques, Livre II Algèbre: 1. Structures algébriques, Paris 1951_2, 4 + 176; 2. Algèbre linéaire, 134; 3. Algèbre multilinéaire Paris 1948, 158; 4. Polynomes et fractions rationnelles; 5. Corps commutatifs, Paris 1950, 222; 6. Groupes et corps ordonnés; 7. Modules sur les anneaux principaux, Paris 1952, 160 (ruski prevod 1-3 D. A. Rajkova, Moskva 1962, 516).
Buhštab A. A.
[1] Teorija čisel, Moskva 1966_2, 384.
Burnside W.
[1] Theory of groups of finite order, Cambridge 1897, 1911_2.
Cahen E.
[1] Élements de la théorie des nombres Paris 1899, 8 + 403.
Cantor Moritz
[1] Vorlesungen über Geschichte der Mathematik, I - Leipzig 1880_1, 8 + 804; II - Leipzig 1892, 10 + 963; III - Leipzig 1901_2, 10 + 923.
Cesarec Rudolf
[1] Analitička geometrija linearnog i kvadratnog područja. I - Analitička geometrija u ravnini, Zagreb 1957, 20 + 528.
Cohn P. M.
[1] Universal algebra, New York-London 1965 (ruski prevod 1968, 352).
Church A.
[1] Introduction to mathematical logic 1, Princeton 1956, IX + 376.
Curry Haskell B.
[1] Foundations of Mathematical logic, 1963 (ruski prevod: Osnovanija matematičeskoj logiki, Moskva, 1969, 568).
Demidovič B. P. — Maton I. A.
[1] Osnoví víčislitel' noj matematiki, Moskva 1963, 660.
Denis-Papin M., Kaufmann A.
[1] Cours de calcul matriciel appliqué, Paris 1951, 304.
Deuring Max
[1] Algebren, Ergebnisse der Mathematik und ihrer Grensgebiete, Bd. 4, fasc. 1,
Devidé Vladimir
[1] Matematička logika. Prvi dio (klasična logika sudova), Beograd 1964 (Mat. inst. knj. 3), 288.

Dickson Leonard Eugene
[1] History of the theory of numbers, Washington 1919—20—23, 3 sveska.
[2] Modern elementary theory of numbers, Chicago 1939, 7 + 309.
Dubreil Paul
[1] Algèbre I, Équivalences, operations, groupes, anneaux, corps, Paris 1946, 10 + 306, 1954_2, 467 pp.
Dubreil Paul, Dubreil — Jacotin M. L.
[1] Leçons d'algèbre moderne, Paris 1964_2, 7 + 401.
Dubreil — Jacotin M. L., Groisot R.
[1] Leçons sur la théorie des treillis ordonnés et des treillis géométriques, Paris 1958, 8 + 385
Galois E.
[1] Écrits et Mémoires mathématiques d'Evariste Galois. Édition critique intégrale de ses manuscrits et publicatons par Robert Bourgne et J. P. Azra, Préface de J. Dieudonné, Paris 1962, Gauthier—Villars, 22 + 542.
* * *
[1] Encyklopädie der math. Wissenschaften (red. W. F. Meyer), I - Arythmetik und Algebra, Leipzig 1898—1904, 38 + 1197. Drugo izdanje: I Algebra und Zahlentheorie, 1. A -- - Grundlagen, B - Algebra, 1939.
* * *
[2] Enciklopedija elementarnoj matematiki (pod redakcijej P. S. Aleksandrova, A. I. Mar kuševiča i J. J. Hinčina), II - Algebra, Moskva—Lenjingrad 1961, 424.
Faddejev D. K. — Faddejeva V. N.
[1] Vičislitel'nie metodi linejnoj algebri, Moskva—Lenjingrad 1963, 736. (popis literature ispunio je str. 677—734).
Faddeev D. K. — Sominskij I. S.
[1] Sbornik zadač po višej algebre, Moskva 1953_2, 308.
Gantmaher F. R.
[1] Teorija matric, Moskva 1954, 492, odnosno 1966_2, 576.
Gavrilović Bogdan
[1] Teorija determinanata, Beograd 1899, 12 + 278.
Gel'fond A. O.
[1] Transcendentnije i algebraičeskije čisla, Moskva 1952, 224.
Glejzer G. I.
[1] Istorija matematiki v škole, Moskva 1964, 376.
Gribanov V. U. — Titov P. I.
[1] Sbornik upražnenij po teoriji čisel, Moskva 1964, 144.
Greub Werner H.
[1] Linear Algebra, Berlin-Göttingen—Heidelberg, Springer Verlag 1963_2 12 + 338.
Hadley G.
[1] Linear programming, London 1962, 12 + 520.
Hall M. jr.
[1] The theory of groups, New York 1959 (na ruskom: Moskva 1962, 468).
Hasse Helmut — Klobe W.
[1] Aufgabensammlung zur höheren Algebra (Sammlung Göschen, 1082), Berlin 1961_3, 183.
Hasse H.
[1] Vorlesungen über Zahlentheorie, Grundl. d. math. Wiss. 61, Springer V. 1950, 12 + 474.
[2] Zahlentheorie. Akademie-Verlag, Berlin 1963; pp. 611.
[3] Höhere Algebra I - 1963_5, II - 1958_4 (Sammlung Göschen, 931, 932), 150, odn. 158 str.
Hilbert D. — Ackermann W.
[1] Grundzüge der theoretischen Logik, Berlin 1938_2, 8 + 134.
Jacobson Nathan
[3] Structure of rings, Amer. Math. Soc., Prov. 1956, 7 + 263 (ruski, Moskva 1961, 392 s).

Juškevič A. P.

[1] Istorija matematiki v srednije vjeka, Moskva 1961, 448.

(pod uredništvom Juškeviča)

[2] Istorija matematiki 1, 2 Moskva 1970.

Karamata J.

[1] Algebra I, Prvi deo, Beograd 1949, 140; Drugi deo, Beograd 1950, 184.

Karlin S.

[1] Mathematical methods and theory in games, programming and economics, London-Paris Vol I 10 + 433, Vol. II 11 + 386 (ruski, Moskva 1964, 838).

Kašanin R.

[1] Viša matematika, Beograd I (1949_3 7 + 847, II_1 (1949) 8 + 624, II_2 (1950) 7 + 679.

Kočin N. E.

[1] Vektornoje iščislenije i načala tenzornogo iščislenija, Moskva 1951_7, 428.

Kol'man E.

[1] Istorija matematiki v drevnosti, Moskva 1961, 236.

Kowalewski G.

[1] Determinantentheorie, Berlin—Leipzig 1925_2, 4 + 304.

Kraitschik M.

Recherches sur la théorie des nombres 1924. T. 1, 1929, str. 16 + 272; T. 2, Factorisation, 1924, str. 15 + 184; Théorie des nombres, Paris, I - 1922; II - 1929.

Krečmar V. A.

[1] Zadačnik po algebre, Moskva—Leningrad 1950, 440.

Križanič France

[1] Vektorji, matrike, tenzorji, Ljubljana 1962, 272.

Krull W.

[1] Elementare und klassische Algebra vom modernen Standpunkt I (Sammlung Göschen, 930), Berlin 1963_3, 148 str.; II (S. G. 933), Berlin 1959, 132.

[2] Allgemeine Modul-, Ring- und Idealtheorie . . . (Enzykl. d. math. Wiss.) Leipzig-Berlin 1939, Bd I 1. Teil, 11, 1—54 12, 1—53.

Kurepa Đuro

[1] Teorija skupova, Zagreb, 1951, 22 + 444.

[2] Šta su skupovi i kakva im je uloga. Zagred, 1960, 11+190; 1967_2, 4+203; 1970_3, 4+215.

Kurepa Svetozar

[1] Konačno dimenzionalni vektorski prostori i primjene, Zagreb, Tehn. knj. 1967, 788.

[2] Uvod u matematiku. Skupovi. Strukture. Brojevi. Zagreb, Tehn. knj. 1970, 252.

Kuroš A. G.

[1] Kurs višej algebri, Moskva—Leningrad 1952_3, 336.

[2] Teorija grupp, Moskva 1953_2, 468; 1967_3 648.

[3] Lekciji po obščej algebre, Moskva 1962, 396.

Landau E.

[1] Vorlesungen über Zahlentheorie. I - Aus der elementaren und additiven Zahlentheorie, 12 + 360; II - Aus der anal. und geom. Zahlentheorie, 8 + 308; III - Aus der alg. Zahlentheorie und über die Fermatsche Vermutung, 8 + 342 Leipzig 1927.

Lang Serge

[1] Algebra, Reading Mass. 1965 (r. Moskva, 1968, 564).

Lejeune — Dirichlet P. G.

Vorlesungen über Zahlentheorie (redigirao i dopunio R. Dedekind 1863_1, 1871_2, 1879_3, 1894_4, 17 + 657 str.). Isp. Dedekindova Djela (Gesammelte mathematische Werke, Braunschweig III, 508 str.).

Lichnerowicz A.

[1] Algèbre et Analyse linéaires, Paris 1947, 316 (njem. prevod. Berlin 1956,1 2 + 304).

Lomont J. S.

[1] Applications of finite groups, New York—London 1959, 10 + 346.

Lugowski H. — Weinert H. J.

[1] Grundzüge der Algebra, Leipzig. I - Allgemeine Gruppentheorio, 1957, 5 + 234; II - Allgemeine Ring- und Körper-Theorie 1958; III - Auflösungstheorie algebraischer Gleichungen, 1960, 274.

L'ubarskij G. Ja.

Teorija grupp i jijo primenjenije v fizike, Moskva 1958, 354 (na engl. preveo Dedijer).

Mac Duffee C. C.

[1] The theory of matrices (Ergebnisse d. Math. 2), Berlin 1933, 6 + 110.

[2] An introduction to abstract algebra, London 1940, 8 + 304.

Mal'cev A. I.

[1] Osnoví linejnoj algebri, Moskva, 1956_2, 340.

Marković Željko

[4] Uvod u višu analizu; I - 1947_2, 8 + 618; II - 1952, 12 + 640.

Matvijevskaja E. M.

[1] Učenije o čisle na sredn'evjekovom bližn'em i sredn'em vostoke Taškent, 1967, 344.

Miličić Pavle — Uščumlić Momčilo

[1] Zbirka zadataka iz Više matematike I, Građevinska knj., Beograd, 1969_3, 6 + 633; II 1971, 6 + 792.

Mitrinović D. S. sa saradnicima

[4] Zbornik matematičkih problema. I - Beograd 1958_2, 6 + 352; II - Beograd 1958_2, 16 + 408; III - Beograd 1960, 16 + 336.

Mitrinović D. S. — Mihailović D.

[1] Linearna algebra. Analitička geometrija. Polinomi. Beograd 1959, 16 + 414.

Mostowski Andrzej

[1] Logika matematyczna, Warszawa—Wrocław 1948, VIII + 388.

Muir Thomas

[1] The theory of determinants in the historical order of development, Vol. 1, London 1906_2, 11 + 491; Vol. 2 (period 1841—1860), London 1911, 16 + 475.

Najmark M. A.

[1] Normirovanníje kol'ca, Moskva 1956, 488.

Nešić Dimitrije

[1] Algebarska analiza, 1 - Beograd 1883; 2 - Beograd (1883), 12 + 670.

Obreškov N.

[1] Visša algebra, Sofija 1947_2, 10 + 524.

[2] — — II, 1935, 12 + 480.

[3] Sbornik ot zadači i teoremi po visša algebra, Sofija 1932, 8 + 488.

[4] Verteilung und Berechnung der Nullstellen reeller Polynome, Berlin 1963, 8 + 298 (navedena je opsežna bibliografija).

Ostrowski A. M.

[1] Solution of equations and systems of equations. Acad. Press, New York—London, 1960 (ruski: Moskva, 1963, 219).

Perron O.

[1] Algebra. I - Die Grundlagen, Berlin—Leipzig 1932_2, 8 + 302; II - Theorie der algebraischen Gleichungen, 1933_2, 8 + 262.

Pickert G.

[1] Einführung in die höhere Algebra, Göttingen 1951, 298.

Plemelj J.

[1] Algebra in teorija števil, Ljubljana 1962, 16 + 280.

Postnikov M. M.

[1] Teorija Galua, Moskva 1963, 218.

Prachar Karl

[1] Primzahlverteilung, Berlin—Göttingen—Heidelberg, 1957 (ruski, Moskva 1967, 511).

Prijatelj Niko

[1] Uvod v matematično logiko, Ljubljana 1960, 150.

Proskurjakov I. V.

[1] Sbornik zadač po linejnoj algebri, Moskva 1957, 368.

Rašajski Borivoje

[1] Analitička geometrija, Beograd, Građevinska knjiga, 1968_2, 6 + 320.

Rudeanu Sergiŭ

[1] Axiomele laticilor şi ale algebeler booleene, Bucuresti 1963, 159.

Scholz A. — Schoeneberg B.

[1] Einführung in die Zahlentheorie (S. G. 1131), Berlin 1961, 128.

Scorza G.

[1] Gruppi astratti, Roma 1942, 8 + 242.

Sedmak V.

[1] Uvod u algebru, Zagreb 1961, 16 + 240.

Serre Jean Pierre

[1] Représentations linéaires des groupes finis, Paris 1967 (ruski: Moskva, 1970, 132).

Serret J. A.

[1] Cours d'algèbre supérieure. I - Paris 1928_7, 648; II - Paris 1928_7, 696 (njem. Leipzig 1868_2, 528, 574).

Sierpiński Waclaw

[1] Teoria liczb. I - Warszawa 1950, 8 + 544; II - Warszawa 1959, 488.

[2] Zasady algebry wyzszej z przypisem A. Mostowskiego Zarys teorii Galois, Warszawa—Wroclaw 1951_2, 8 + 436.

[3] Algèbre des ensembles, Warszawa—Wroclaw 1951, 205.

Sikorski Roman

[1] Boolean algebras (Ergebnisse der Math.), Berlin—Gottingen—Heidelberg 1960, 10 + 176.

Simonart F.

[1] Leçons d'algèbre supérieure, Louvain—Paris 1934, 11 + 327.

Smirnov V. I.

[1] Kurs višej matematiki III_1, Moskva—Leningrad, 1949_4, 335.

Smith D. E.

[1] History of mathematics. I - New York 1958, 22 + 596; II - New York 1958, 12 + 725.

Specht W.

[1] Gruppentheorie, Berlin—Göttingen—Heidelberg 1956, 4 + 458.

Speiser A.

[1] Theorie der Gruppen von endlicher Ordnung, Berlin 1937_3, 10 + 262.

Steinitz E.

[1] Algebraische Theorie der Körper: a) Journal für die reine und angew. Mathematik; b) kao knjigu izdali Baer R. — Hasse H, Berlin—Leipzig 1930.

Stojaković Mirko

Teorija jednačina, Naučna knjiga, Beograd 1966, 155.

Stone M. H.

[1] Linear transformations in Hilbert space, New York 1932, 8 + 622.

Struik, Dirk J.

[1] A concise history of Mathematics, Dover Publ. New York (na srpskohrvatski preveo Milenko Nikolić, Beograd, Zavod za izdavanje udžbenika SRS, 1969, 372).

Szász Gabor
[1] Introduction to Lattice Theory, Budapest, 1963, 229.
Šilov G. E.
[1] Vvedenije v teoriju linejnih prostranstv, Moskva 1956, 303.
Taton R. (sa saradnicima)
[1] Histoire générale des Sciences. I - La science antique et médiévale, Paris 1957, 8 + 628; II - La science moderne (1450—1800), Paris 1958, 8 + 800.
Tropfke J.
[1] Geschichte der Elementar-Mathematik, Berlin—Leipzig. 1. Rechnen, 1930_3, 7 + 222; 2. Allgemeine Aritmetik, 1933_3, 266; 3. Proportionen. Gleichungen, 1937_3.
Vajda S.
[1] The theory of games and linear programming, London.
[2] Théorie des jeux et programmation linéaire (traduit et adapté par J. Bouzitat), Paris 1959, 14 + 256.
Vigodski M. Ja.
[1] Arifmetika i algebra v drevnem mirje, Moskva—Leningrad 1941, 252; Moskva 1967_2 (pripremio B. A. Rozenfel'd) 368.
Vilenkin N. Ja.
[1] Specijal'nie funkciji i teorija predstavlenij grupp, Moskva, 1965, 588.
Vidav Ivan
[1] Višja matematika, Ljubljana, I (1949) 334, II (1951) 442.
Vinogradov I. M.
[1] Osnovi teoriji čisel, Moskva—Leningrad 1949, 180.
van der Waerden Z. L.
[1] Moderne Algebra. I - (1930); 1960_5 8 + 292; II - (1931) 8 + 216 1959_4, 10 + 275.
Weber H.
[1] Lehrbuch der Algebra. I - Braunschweig 1895_1, 1898_2, 16 + 704; II - Braunschweig 1899_1, 1899_2, 16 + 885; III - Braunschweig 1908_2, 16 + 733.
Wedderburn J. H. M.
[1] Lectures on matrices, Amer. Math. Soc., New York 1934, 10 + 205 (kopija od 1949). Tu se nalazi popis literature o matricama prikazan po svakoj godini za razdoblje 1853—1936 (svega 661 djelo).
Weyl H.
[1] Gruppentheorie und Quantenmechanik, Leipzig 1928, 8 + 288.
[2] The classical groups. Their invariants and representations. Princeton 1953, 14 + 320.
Whittaker Edmund — Robinson G.
[1] Tečaj numeričke matematike; prevela Vojna Radojčić, Beograd 1951, 12 + 362 (original London 1948_4).
Wieleitner H.
[1] Istorija matematiki ot Dekarta do seredini XIX stoletija (ruski prevod s njemačkoga pod uredništvom A. P. Juškeviča) Moskva, Nauka, 1966, 508.
Wintner A.
[1] Spektraltheorie der unendlichen Matrizen, Leipzig 1929, 12 + 280.
Zariski O. — Samuel P.
[1] Commutative algebra. I - Princeton 1958, 11 + 329; II - 1960, 10 + 414 (ruski, Moskva 1963, I - 374 str., II - 440 str.).
Zassenhaus H.
[1] Lehrbuch der Gruppentheorie I, Leipzig—Berlin 1937, 152.
Zurmühl R.
[1] Matrizen, Berlin—Heidelberg 1950, 16 + 428 (odn. 1964_4, 12 + 452).

ABECEDNI POPIS IMENA

(brojevi označavaju stranice; mastan broj znači da se nalazi i slika)

ABECEDNI SADRŽAJ

(brojevi redom označavaju: poglavlje, paragraf itd.)

PREGLED OZNAKA

(brojevi označavaju redom: poglavlje, paragraf itd.)

o, O, $\ll$	6 § 7.14.31
$\vartheta(x)$	6 § 7.14.32
$P(x)$	6 § 7.14.30
$\zeta(s)$	6 § 7.14.33
$M(a, b)$, $a M b$, $\mathrm{W}(a, b)$, $a \mathrm{W} b$	6 § 8.3
$\Phi(m)$, $\varphi(m)$	6 § 17.16.2
$d_0 n$	6 § 19.4.6
σn	6 § 19.4.7. 1)
$d_r(n)$	6 § 19.4.8. 1)
Sp, σ_p	7 § 8.2.1; 24 § 2.5 (nota); 27 § 2.9
δ_{ij}, δ_j^i	10 § 3.6
$L(R, M)$	13 § 3.7.3
G/F	17 § 11.4
$G_1 \oplus G_2$	17 § 14.5.5
$[G, G]$	17 § 18.2
G'	17 § 18.3
$\Phi_n(x)$	18 § 5.1 (2)
$V_n(R)$	25 § 2
$x \ominus y$	25 § 3.1
$V^\star$	26 § 2.4
ZG	17 § 9.5
S_n	17 § 7.4

Ako je R dvočlana relacija, tada R_1 znači *prvi* a R_2 *drugi* dio (član) od R; tako npr. ako (5) znači jednadžbu, tada $(5)_1$ znači *lijevu* a $(5)_2$ znači *desnu* stranu od (5).

Ako S označuje skup, tada se svaki član iz S označuje sa $\dot{S}$ (tačka iznad S) ili $S^\cdot$; neka određena tačka iz S označuje se sa $\underset{\cdot}{S}$ (tačka ispod oznake za skup).

$\dot{n}$ ili $n^\cdot$ označuje *svaki* redni broj $<n$; $n^\cdot = \underbrace{0, 1, 2, \ldots}_{n}$

NERIJEŠENI PROBLEMI

P_1	6 § 6.12.8	P_{16}	6 § 7.14.19	P_{29}	6 § 7.14.36
P_2	6 § 6.12.9	P_{17}	6 § 7.14.20	P_{30}	6 § 14.9.11
P_3	6 § 7.5	P_{18}	6 § 7.14.21	P_{31}	6 § 17.7.18
P_4—P_5	6 § 7.12 (2 probl.)	P_{19}	6 § 7.14.22	P_{32}	6 § 17.7.19
P_6—P_7	6 § 7.14.3 (2 probl.)	P_{20}	6 § 7.14.23	P_{33}	6 § 19.3.10
P_8	6 § 7.14.10	P_{21}	6 § 7.14.25	P_{34}	6 § 19.4.3. 3).
P_9	6 § 7.14.11	P_{22}	6 § 7.14.26	P_{35}	6 § 19.4.7. 4).
P_{10}	6 § 7.14.12	P_{23}	6 § 7.14.27	P_{36}	6 § 19.4.12. 3).
P_{11}	6 § 7.14. 13.7).	P_{24}	6 § 7.14.28	P_{37}	6 § 19.4.12. 4).
P_{12}	6 § 7.14.14	P_{25}	6 § 7.14.29	P_{38}	6 § 19.4.13. 2).
P_{13}	6 § 7.14.16	P_{26}	6 § 7.14.33. 3).	P_{39}	6 § 19.4.13. 3).
P_{14}	6 § 7.14.17	P_{27}	6 § 7.14.34	P_{40}	17 § 20.11 3.4)
P_{15}	6 § 7.14.18	P_{28}	6 § 7.14.35	P_{41}	32 § 8.7.3.