ALGEBRA I

Žikica Perović
Univerzitet u Nišu

SADRŽAJ

GLAVA I

TEORIJA BROJEVA

1.1. Relacija deljivosti

1.1.1. Definicija. Neka su $a, b \in Z$, $b \neq 0$. $b|a$ akko postoji $m \in Z$ tako da je $a = mb$.

1.1.2. Tvrđenje. *Relacija | je refleksivna, tranzitivna relacija koja zadovoljava oslabljenu antisimetričnost:*

$$b|a \quad \& \quad a|b \Leftrightarrow b = \pm a.$$

Dokaz. **Refleksivnost.** Kako je za svaki $a \in Z$, $a = 1 \cdot a$, to je za $a \neq 0$, $a|a$.

"Antisimetričnost". Neka je $a, b \in Z \setminus \{0\}$, tako da $a|b$, $b|a$. Tada je, za neke $s, t \in Z$, $a = bs$ i $b = at$. Zamenom druge jednakosti u prvoj, dobijamo $a = ast$. Skraćivanjem dobijamo $st = 1$. Kako su s i t celi brojevi, $s = t = \pm 1$. Otuda je $b = at = \pm a$.

Tranzitivnost. Neka je $a, b, c \in Z$, tako da $a|b$, $b|c$. Tada je, za neke $s, t \in Z$, $b = as$ i $c = bt$. Zamenom prve jednakosti u drugoj, dobijamo $c = ast$. Dakle, $a|c$. □

1.1.3. Posledica. *Relacija | restrikovana na N^+ je relacija poretka.*

Dokaz. Kako u N, $b = \pm a$ akko $b = a$, to imamo da je | antisimetrična relacija. □

Na sledećoj slici predstavljen je graf ove relacije | na N^+.
SLIKA

1.1.4. Tvrđenje. *Neka su $a, b, c \in Z$.*
(i) $a|b \& a|c \Rightarrow a|b + c$.
(ii) $a|b \Rightarrow a|bc$.

Dokaz. Po definiciji relacije |, postoje s i t, tako da je $b = sa$ i $c = ta$. Sada imamo

$$b + c = sa + ta = (s + t)a.$$

$$bc = sta^2$$

Dakle, $a|b+c, bc$. □

1.1.5. Tvrđenje. *Neka je* $a, b \in Z$, $b \neq 0$. *Postoje jedinstveni brojevi* $q, r \in Z$ *tako da je*

$$a = bq + r \quad \& \quad 0 \leq r < |b|.$$

Dokaz. Dokažimo najpre postojanje. Razmatramo najpre slučaj $a \geq 0$. Neka je $S = \{m \in Z : m|b| > a\}$. Kako $a + 1 \in S$, to je S neprazan podskup od N, pa ima najmanji element. Neka je $s = minS$ i $q' = s - 1$. Tada $t \notin S$, pa je $q'|b| \leq a$. Otuda je $r = a - q'|b| \geq 0$. Sdruge strane, kako $s \in S$, $s|b| > a$. Otuda je

$$s|b| - q'|b| > a - q'|b|,$$

tj. $|b| > r$. Iz definicione jednakosti za r, imamo $a = q'b + r$. Kako je $|b| = b \cdot sgn(b)$, to je $a = qb + r$, za $q = q'sgn(b)$.

Neka je sada $a < 0$. Kako je $-a > 0$, to prema već dokazanom slučaju, postoje $s, r' \in Z$ tako da je $-a = s|b| + r'$, i $0 \leq r' < |b|$. Sada je $a = -s|b| + (-r')$, i $-|b| < -r' \leq 0$. Ako je $r' = 0$, onda je za $q = -s\,sgn(b)$ i $r = r' = 0$ tvrđenje zadovoljeno. Međutim, ako je $r' > 0$, onda $-r'$ ne zadovoljava tražene nejednakosti. Zato radimo popravku.

$$\begin{aligned} a &= -s|b| + (-r') \\ &= -s|b| - |b| + |b| - r' \\ &= (-s-1)|b| + (|b| - r'). \end{aligned}$$

Neka je $q' = -s-1$ i $r = |b| - r'$. Sada je $a = q'|b| + r$. Proverimo nejednakosti za r. Kako je $0 < r' < |b|$, množenjem sa -1 dobijamo $-|b| < -r' < 0$. Dodavanjem $|b|$, dobijamo $0 < |b| - r' < |b|$, tj. $0 < r < |b|$. Za $q = q'sgn(b)$, je $a = bq + r$ i $0 < r < |b|$.

Ostaje da pokažemo jedinstvenost. Dakle, neka je $a = bq + r = bq_1 + r_1$ i $0 \leq r, r_1 < |b|$. Bez gubljenja opštosti pretpostavimo da je $r \leq r_1$. Tada je $b(q - q_1) = r_1 - r$. Kako je $0 \leq r_1 - r < |b|$, to je $0 \leq |b(q - q_1)| < |b|$. Skraćivanjem sa $|b|$, dobijamo $0 \leq |q - q_1| < 1$. Kako je $|q - q_1|$ nenegativan ceo broj, to je $|q - q_1| = 0$. Otuda je $q = q_1$, pa je i $r = r_1$. □

1.1.6. Definicija. Neka je $a \in Z$, $n \in N_+$.

$rem_n(a)$ je ostatak pri deljenju a sa n.

1.1.7. Primer. Neka je $n \in N^+$. Funkcija rem_n ima n mogućih vrednosti: $0, 1, \ldots, n-1$. Sve te vrednost se realizuju jer je za $0 \leq a < n$, $rem_n(a) = a$. Tako funkcija rem_2 ima vrednosti 0 i 1, koje dobijaju parni odnosno neparni brojevi. rem_4 ima četiri vrednosti: 0,1,2 i 3. Za $i \in \{0, 1, 2, 3\}$ definišimo $C_i = \{a \in Z : rem_4(a) = i\}$. C_i, $i \in \{0, 1, 2, 3\}$ čine particiju skupa Z, tj. to su disjunktni skupovi i svaki ceo broj pripada jednom od njih. Primetimo da se sa ovim skupovima dosta pravilno računa. Pokazaćemo da je proizvod dvaju brojeva iz C_1 opet u C_1.

Neka su $a, b \in C_1$. Tada postoje brojevi $k, l \in Z$, tako da je $a = 4k + 1$ i $b = 4l + 1$. Tada je

$$\begin{aligned} a \cdot b &= (4k + 1) \cdot (4l + 1) \\ &= 16kl + 4k + 4l + 1 \\ &= 4(4kl + k + l) + 1. \end{aligned}$$

Dakle, $ab \in C_1$. Slično se pokazuje da je za $a \in C_1$ i $b \in C_3$, $a \cdot b \in C_3$.

1.1.8. Definicija. Neka je $a \in Z$. $D(a) = \{t \in Z^+ : t|a\}$. Ako je $a > 1$ i $D(a) = \{1, a\}$ kažemo da je a prost broj.

U nastavku za proste brojeve rezervišemo slovo p. Primetimo da se u grafu relacije $|$, prosti brojevi nalaze na drugom nivou. Ako restrikujemo $|$ na $N_2 = N^+ \setminus \{1\}$, onda su prosti brojevi minimalni elementi uređenja $(N_2, |)$. Prirodno se u matematici nastoji da se svi elementi strukture predstave pomoću minimalnih. To ćemo i ovde uspeti, u narednom odeljku.

1.1.9. Definicija. Neka su $a, b \in Z$, $a, b \neq 0$. $D(a, b) = D(a) \cap D(b)$. Najveći zajednički delilac brojeva a i b, u oznaci (a, b) je $max D(a, b)$. Ako je $(a, b) = 1$ kažemo da su a i b uzajamno prosti.

Pokažimo da je definicija korektna, tj. da za svaka dva broja $a, b \in Z$ postoji (a, b). Kako $1|a, b$, to je skup $D(a, b)$ neprazan. Kako je za svaki $t \in D(a, b)$, $t \leq |a|$, to je $D(a, b)$ ograničen neprazan skup prirodnih brojeva, pa ima maksimum prema ??. Primetimo takođe da je za $(a, b) \in Z$, $(a, b) = (|a|, |b|)$. Zato u nastavku uvek pretpostavljamo da je u oznaci (a, b), $a, b \in N^+$.

1.2. Euklidov algoritam

1.2.1. Lema. *Neka su $a, b, q, r \in Z$, .*

(i) *Ako je $a = qb$, tada je $(a, b) = b$,*

(ii) *Ako je* $a = qb + r$, *tada je* $(a, b) = (b, r)$.

Dokaz. (i) Neka je $(a, b) = d$. Kako $|b| \in D(a, b)$, to $|b| \leq d$. Kako $d \in D(a, b)$, to $d|b$, pa je $|d| \leq |b|$. Dakle, $d = |b|$.

(ii) Dokazaćemo da je $D(a, b) = D(b, r)$. Neka je $t \in D(a, b)$. Tada $t|a$ i $t|b$, pa $t|a - bq = r$. Dakle, $t \in D(r, b)$. Slično, ako je $t \in D(b, r)$, to $t|b$ i $t|r$. Otuda $t|qb + r$ tj. $t|a$. Dakle, $t \in D(a, b)$. Odavde je $maxD(a, b) = maxD(b, r)$ tj. $(a, b) = (b, r)$.

1.2.2. Definicija. Neka su $a, b \in Z$, $b \neq 0$. Neka je $r_0 = b$. Niz jednakosti

$$
\begin{array}{ll}
a = bq_1 + r_1 & 0 < r_1 < |b| \\
b = r_1 q_2 + r_2 & 0 < r_2 < r_1 \\
r_1 = r_2 q_3 + r_3 & 0 < r_3 < r_2 \\
\ldots & \ldots \\
r_{n-2} = r_{n-1} q_n + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = r_n q_{n+1} &
\end{array} \qquad (*)
$$

nazivamo Euklidovim algoritmom dužine n za a i b. Reč algoritam podrazumeva konačnu automatsku proceduru za izračunavanje nekog objekta. U sledećoj teoremi pokazujemo da Euklidov algoritam zadovoljava sve te uslove.

1.2.3. Teorema. *Neka su* $a, b \in Z$, $b \neq 0$. *Postoji jedinstven Euklidov algoritam za* a *i* b. $(a, b) = r_n$.

Dokaz. Prema prethodnom tvrđenju postoje jedinstveni celi brojevi q_1 i r_1 tako da je $a = bq_1 + r_1$. Ako je $r_1 = 0$, onda je ta jednakost Euklidov algoritam dužine 0. Ako je $r_1 \neq 0$, tada se isto tvrđenje može primeniti na brojeve b i r_1. Proceduru nastavljamo na jedinstven način dokgod je ostatak različit od 0. Dakle, r_{i+2} je ostatak pri deljenju r_{i+1} sa r_i tj. $r_{i-1} = r_i q_{i+1} + r_{i+1}$. Ako bi za svako $i \in N$ imali $r_i \neq 0$, tada bi imali beskonačan opadajući niz prirodnih brojeva $\cdots < r_{i+1} < r_i < \cdots < r_1 < b$, suprotno činjenici da je $(N, \leq)$ dobro uređenje. Dakle, za neko $i \in N$ je $r_i = 0$. Otuda, za $n = i - 1$, imamo $r_{n-1} = r_n q_{n+1} + 0$.

Ostaje da pokažemo da je $(a, b) = r_n$. Dokaz izvodimo indukcijom po n, dužini Euklidovog algoritma. Za $n = 0$ imamo $a = bq_1$ i $(a, b) = b = r_0$. Pretpostavimo da je tvrđenje dokazano za Euklidove algoritme dužine $n - 1$, i neka je (a, b) par brojeva koji ima Euklidov algoritam dužine n. Ako u $(*)$ zanemarimo prvu jednakost, dobijamo Euklidov algoritam za brojeve b i r_1, dužine $n - 1$. Prema indukcijskoj hipotezi $(b, r_1) = r_n$. Kako je $a = bq_1 + r_1$, to je, prema Lemi 1.2.1.(ii), $(a, b) = (b, r_1) = r_n$. □

1.2.4. Primer. Euklidov algoritam za 77 i 16 je

$$\begin{aligned} 77 &= 4 \cdot 16 + 13 \\ 16 &= 1 \cdot 13 + 3 \\ 13 &= 4 \cdot 3 + 1 \\ 3 &= 3 \cdot 1. \end{aligned}$$

Dakle, $(77, 16) = 1$.

1.2.5. Posledica. *(Bezu-ova teorema) Neka su $a, b \in Z$, $a, b \neq 0$, i $d = (a, b)$. Postoje celi brojevi $u, v \in Z$ tako da je $d = au + bv$.*

Dokaz. Prema Teoremi 1.2.3., postoji Euklidov algoritam za brojeve a i b. Dokaz izvodimo indukcijom po dužini tog Euklidovog algoritma. Neka je najpre dužina Euklidovog algoritma za a i b jednaka 0. Tada je $a = qb$, pa je $b = (a, b)$. Kako je $b = 0 \cdot a + 1 \cdot b$, to $u = 0$ i $v = 1$ zadovoljavaju uslove teoreme. Pretpostavimo da je tvrđenje dokazano za sve parove brojeva (a, b) koji imaju Euklidov algoritam dužine $n - 1$. Neka je sada (a, b) par brojeva koji ima Euklidov algoritam dužine n. Dakle, imamo sledeći niz jednakosti

$$(*) \qquad \begin{aligned} a &= bq_1 + r_1 && 0 < r_1 < |b| \\ b &= r_1 q_2 + r_2 && 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 && 0 < r_3 < r_2 \\ &\dots && \dots \\ r_{n-2} &= r_{n-1} q_n + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

Analizirajmo niz jednakosti koji se dobija kada odstranimo prvu jednakost. To je Euklidov algoritam za b i r_1, dužine $n - 1$. Prema Teoremi 1.2.3., $(b, r_1) = r_n$. Prema indukcijskoj hipotezi, postoje celi brojevi $t, w \in Z$, tako da je $(b, r_1) = r_n = bt + r_1 w$. Kako je prema prvoj jednakosti $r_1 = a - bq_1$, zamenom dobijamo $r_n = bt + (a - bq_1)w = aw + (t - q_1)b$. Kako je, prema Teoremi 1.2.3., $(a, b) = r_n$, to imamo $(a, b) = au + bv$, za $u = w$ i $v = t - q_1$. □

1.2.6. Primer. Iz Euklidovog algoritma za 77 i 16 iz Primera 1.2.4., dobijamo

$$\begin{aligned} 1 &= 13 - 4 \cdot 3 \\ &= 13 - 4 \cdot (16 - 13) \\ &= 5 \cdot 13 - 4 \cdot 16 \\ &= 5 \cdot (77 - 4 \cdot 16) - 4 \cdot 16 \\ &= 5 \cdot 77 - 24 \cdot 16. \end{aligned}$$

1.2.7. Posledica. *Neka su* $a, b, c \in N^+$ *i* $d = (a, b)$.

(i) *Za svako* $t \in D(a, b)$, $t|d$.

(ii) $(ac, bc) = dc$.

(iii) *Ako* $c|a, b$ *tada* $(\frac{a}{c}, \frac{b}{c}) = \frac{d}{c}$.

Dokaz. (i) Neka je (∗) Euklidov algoritam za a, b. Neka je $t \in D(a, b)$. Prema dokazu Leme 1.2.1, $D(a, b) = D(b, r_1) = D(r_1, r_2) = \cdots = D(r_{n-1}, r_n)$. Kako $t \in D(a, b)$, to $t \in D(r_{n-1}, r_n)$. Kako je $r_n = d$, to $t|d$.

(ii) Neka je (∗) Euklidov algoritam za a, b. Prema Teoremi 1.2.3., $d = r_n$. Množenjem svih jednakosti i nejednakosti sa c, dobijamo

$$\begin{aligned}
ac &= bcq_1 + cr_1 && 0 < cr_1 < bc \\
cb &= cr_1q_2 + cr_2 && 0 < cr_2 < cr_1 \\
cr_1 &= cr_2q_3 + cr_3 && 0 < cr_3 < cr_2 \\
&\cdots && \cdots \\
cr_{n-2} &= cr_{n-1}q_n + cr_n && 0 < cr_n < cr_{n-1} \\
cr_{n-1} &= cr_nq_{n+1}\,. &&
\end{aligned}$$

To je po definiciji Euklidovog algoritma, Euklidov algoritam za ac i bc. Prema Teoremi 1.2.3., $(ac, bc) = cr_n$. Kako je $d = r_n$, $(ac, bc) = dc$.

(iii) Dokaz izvodimo na isti način kao i u (ii), stim što se sve jednakosti i nejednakosti Euklidovog algoritma za a i b delc sa c. □

1.2.8. Primer. Primetimo da za $a, b, c \in N^+$, iz $c|ab$ ne sledi da $c|a$ ili $c|b$. Zaista, $6|2 \cdot 3$, ali $6 \nmid 2$ i $6 \nmid 3$.

Kako je situacija iz prethodnog primera veoma važna pri rešavanju jednačina, od velikog je značaja da nađemo one specijalne slučajeve u kojima implikacija važi.

1.2.9. Posledica. *Neka su* $a, b, c \in N^+$.

(i) *Ako* $c|ab$ *i* c *i* a *su uzajamno prosti, tada* $c|b$.

(ii) *Ako je* $c = p$ *prost broj i* $p|ab$, *onda* $p|a$ *ili* $p|b$.

(iii) *Ako je* $(a, c) = 1$ *i* $(b, c) = 1$ *onda je* $(ab, c) = 1$.

(iv) *Ako je* $(a, b) = 1$ *i* $a, b|c$ *onda* $ab|c$.

Dokaz. (i) Kako je $(a, b) = 1$, to, prema Bezu-ovoj teoremi, postoje $u, v \in Z$, tako da je

$$1 = au + cv.$$

Pomnožimo jednakost sa b. Tada imamo

$$b = abu + bcv.$$

Kako $c|ab$, to $c|abu$. Otuda, i iz $c|bcv$, dobijamo $c|b$.

(ii) Ako je $c = p$ prost broj, tada je $D(p) = \{1, p\}$. Kako je $D(a, p) \subset D(p)$, to je $D(a, p) = \{1, p\}$ ili $D(a, p) = \{1\}$. U prvom slučaju $p|a$. U drugom slučaju je $(a, p) = 1$, pa , prema (i), $p|b$.

(iii) Sledi direktno iz (i). Neka je $d = (ab, c)$. Kako je $(c, a) = 1$ i $d|c$, to je $(d, a) = 1$. Kako $d|ab$, prema tački (i), imamo $d|b$. Otuda $d|(b, c) = 1$, pa je $d = 1$.

(iv) Kako $a|c$, to je $c = as$, za neki $s \in Z$. Kako $b|c$, to $b|as$. Kako je $(a, b) = 1$, prema tački (i) ovog tvrđenja, $b|s$. Dakle, $s = bt$, za neki $t \in Z$. Kako je sada $c = as = abt$, to $ab|c$. □

Definicija 1.1.9., se prirodno generalizuje za ma kojih k brojeva iz N^+.

1.2.10. Definicija. Neka je $(a_k)_{k\in N}$ niz u N^+. Za $k \in N_2$ rekurzivno definišemo najveći zajednički delilac $(a_1, \ldots, a_k)$ brojeva $a_1, \ldots, a_k$.

$$(a_1, a_2) = max D(a_1, a_2)$$
$$(a_1, \ldots, a_{k+1}) = ((a_1, \ldots, a_k), a_{k+1}).$$

Ako je $(a_1, \ldots, a_k) = 1$ kažemo da su $a_1, \ldots, a_k$ uzajamno prosti. Ako je za proizvoljne $1 \leq i < j \leq k$, $(a_i, a_j) = 1$ kažemo da su $a_1, \ldots, a_k$ dva po dva uzajamno prosti.

1.2.11. Definicija. Neka je $k \in N^+$, i $a_1, \ldots, a_k \in N^+$. $D(a_1, \ldots a_k) = D(a_1) \cap \cdots \cap D(a_k)$.

1.2.12. Tvrđenje. *Neka su oznake kao u Definiciji 1.2.10.*

(i) *Za svako $t \in N^+$, $t \in D(a_1, \ldots, a_k)$, akko $t|(a_1, \ldots, a_k)$.*

(i) $(a_1, \ldots, a_k) = max D(a_1, \ldots, a_k)$.

(ii) Ako su $a_1, \ldots, a_k$ dva po dva uzajamno prosti, onda su $a_1, \ldots, a_k$ uzajamno prosti.

Dokaz. (i) Dokaz izvodimo indukcijom po $k \geq 2$. Za $k = 2$ Tvrđenje je trivijalno zadovoljeno. Pretpostavimo da je tvrđenje dokazano za najveći zajednički delilac k brojeva. Dokazujemo da je zadovoljeno i za najveći zajednički delilac $k + 1$ brojeva. Dakle, neka je $a_1, \ldots, a_k, a_{k+1} \in N^+$, $d = (a_1, \ldots, a_{k+1})$ i neka je $t \in N^+$.

$$\begin{aligned} t \in D(a_1, \ldots, a_{k+1}) &\Leftrightarrow (t|a_1 \& \ldots \& t|a_k) \& t|a_{k+1} \\ &\Leftrightarrow t \in D(a_1, \ldots, a_k) \& t \in D(a_{k+1}) \\ &\Leftrightarrow t|(a_1, \ldots, a_k) \& t|a_{k+1}, \text{ (Indukcijska hipoteza)} \\ &\Leftrightarrow t|((a_1, \ldots, a_k), a_k), \text{ (Tvrđenje 1.2.7. (i))} \\ &\Leftrightarrow t|(a_1, \ldots, a_k, a_{k+1}). \text{ (Po definiciji)} \end{aligned}$$

(ii) Neposredno sledi iz prethodnog dela. Dakle, neka je $a_1, \ldots, a_k \in N^+$, $d = (a_1, \ldots, a_{k+1})$. Prema (i), $d \in D(a_1, \ldots, a_k)$, i za svaki $t \in D(a_1, \ldots, a_k)$, $t|d$ pa je i $t \leq d$. Dakle, $d = maxD(a_1, \ldots, a_k)$.

(iii) Neka je $1 \leq i < j \leq k$. Tada je

$$\begin{aligned} D(a_1, \ldots, a_k) &= \bigcap_{s \leq k} D(a_s) \\ &\subset D(a_i) \cap D(a_j) \\ &= D(a_i, a_j). \end{aligned}$$

Kako su $a_1, \ldots, a_k$ dva po dva uzajamno prosti, to je $D(a_i, a_j) = \{1\}$. Zbog prethodne inkluzije je i $D(a_1, \ldots, a_k) = \{1\}$, dakle $(a_1, \ldots, a_k)$ su uzajamno prosti. □

1.2.13. Primer. Pokazaćemo da u tački (iii) ne mora da važi obrat tvrđenja. $D(6, 10, 15) = 1$, pa su $6, 10, 15$ uzajamno prosti. Sdruge strane nikoja dva od njih nisu uzajamno prosti. $(6, 10) = 2$, $(6, 15) = 3$ i $(10, 15) = 5$.

1.3. Neprekidni razlomci

Analizirajmo Euklidov algoritam za 93 i 16.

$$\begin{aligned} 93 &= 5 \cdot 16 + 13 \\ 16 &= 1 \cdot 13 + 3 \\ 13 &= 4 \cdot 3 + 1 \\ 3 &= 3 \cdot 1. \end{aligned}$$

Napišimo svaku od ovih jednakosti u obliku razlomka.

$$\begin{aligned} \frac{93}{16} &= 5 + \frac{13}{16} \\ \frac{16}{13} &= 1 + \frac{3}{13} \\ \frac{13}{3} &= 4 + \frac{1}{3} \end{aligned}$$

U svakoj jednakosti je razlomak na desnoj strani recipročna vrednost razlomka na levoj strani sledeće jednačine. Zato zamenom dobijamo razlomak $\frac{93}{16}$ u obliku

$$5 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{3}}}.$$

Dobijeni izraz nazivamo neprekidnim razlomkom. Primetimo da se pojavljuju redom količnici iz Euklidovog algoritma.

1.3.1. Definicija. Neka je $q_0 \in Z$, $q_1, \ldots, q_n \in N^+$. Izraz

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_n}}}$$

je neprekidni razlomak $s(q_0, q_1, \ldots, q_n)$.

Iz jedinstvenosti Euklidovog algoritma sledi jedinstvenost razvoja svakog racionalnog broja u neprekidni razlomak.

Posmatrajmo sada $s(q_0, q_1, \ldots, q_n)$ kao izraz od promenljivih $q_0, \ldots, q_n$. $[q_0, q_1, \ldots, q_n]$ označava brojilac sređenog izraza $s(q_0, q_1, \ldots, q_n)$. Kako je

$$s(q_0, q_1, \ldots, q_n) = q_0 + \frac{1}{s(q_1, \ldots, q_n)},$$

to je imenilac od $s(q_0, q_1, \ldots, q_n)$ jednak brojiocu razlomka $s(q_1, \ldots, q_n)$, dakle, $[q_1, \ldots, q_n]$. Otuda imamo

$$s(q_0, q_1, \ldots, q_n) = \frac{[q_0, q_1, \ldots, q_n]}{[q_1, \ldots, q_n]} \tag{1}$$

Otuda imamo

$$\begin{aligned} s(q_0, q_1, \ldots, q_n) &= q_0 + \frac{1}{s(q_1, \ldots, q_n)} \\ &= q_0 + \frac{1}{\frac{[q_1, q_2, \ldots, q_n]}{[q_2, \ldots, q_n]}} \\ &= \frac{q_0[q_1, q_2, \ldots, q_n] + [q_2, \ldots, q_n]}{[q_1, \ldots, q_n]}. \end{aligned}$$

Odavde, i iz (1), dobijamo, za $n \geq 2$

$$[q_0, q_1, \ldots, q_n] = q_0[q_1, q_2 \ldots, q_n] + [q_2, q_3, \ldots, q_n]. \tag{2}$$

Ako po konvenciji uvedemo da je prazan neprekidni razlomak $[\,] = 1$, ova rekurentna relacija važi i za $n = 1$.

1.3.2. Tvrđenje. *(Ojlerovo pravilo)Neka je $n \geq 1$. Neka je za $0 \leq 2k \leq n+1$, T_k familija svih $(n+1-2k)$-torki dobijenih tako što je u $n+1$-orci $(0, 1, \ldots, n)$ ispušteno k disjunknih parova uzastopnih brojeva, i neka je*

$$S_k = \sum_{I \in T_k} \prod_{i \in I} q_i.$$

Tada je $[q_0, q, \ldots, q_n] = \sum_{0 \leq 2k \leq n+1} S_k$.

Dokaz. Napomenimo da se u definiciji za n neparno i $k = n+1$, dobija S_{k+1} kao suma jednog proizvoda, po praznom skupu, koji je po konvenciji jednak 1. Dokaz izvodimo transfinitnom indukcijom po n. Za $n = 1$, dobijamo $[q_0, q_1] = q_0 q_1 + 1$ što je korektna jednakost. Sada pretpostavimo da je $n \geq 2$ i da je tvrđenje dokazano za sve brojeve manje od n, a dokažimo tvrđenje za n. Prema formuli (2), imamo

$$[q_0, q_1, \ldots, q_n] = q_0[q_1, q_2 \ldots, q_n] + [q_2, q_3, \ldots, q_n]$$

Prema indukcijskoj hipotezi $[q_1, q_2, \ldots, q_n]$ je jednak zbiru svih proizvoda brojeva $q_1, q_2, \ldots, q_n$ kod kojih je, za $0 \leq 2k \leq n$, ispušteno k disjunktnih parova uzastopnih elemenata iz $(q_1, q_2, \ldots, q_n)$. Kako se taj zbir množi sa q_0, dobijamo opet zbir proizvoda kod kojih je ispušteno k disjunktnih parova uzastopnih brojeva iz niza $(q_0, q_1, q_2, \ldots, q_n)$, ali tako da nije ispušten par (q_0, q_1) . S druge strane, opet po indukcijskoj hipotezi, $[q_2, q_3, \ldots, q_n]$ jednak je zbiru svih proizvoda brojeva $q_2, q_3, \ldots, q_n$, kod kojih je, za $0 \leq 2k \leq n-1$, ispušteno k disjunktnih parova uzastopnih elemenata iz $(q_2, q_3, \ldots, q_n)$. Međutim taj zbir možemo smatrati zbirom svih proizvoda brojeva $q_0, q_1, q_2, q_3, \ldots, q_n$ kod kojih je, za $2 \leq k+1 \leq 2n+1$ ispušten $k+1$ disjunktan par uzastopnih bojeva od kojih je jedan ispušteni par obavezno (q_0, q_1). Kako je pri svakom ispuštanju par (q_0, q_1) ili ispušten ili nije, $[q_0, q_1, \ldots, q_n]$ jednak je zbiru svih proizvoda brojeva $q_0, q_1, \ldots, q_n$ kod kojih je, za $0 \leq 2k \leq n+1$, ispušteno k disjunktnih parova uzastopnih elemenata iz $(q_0, q_1, \ldots, q_n)$. □

1.3.3. Posledica. $[q_0, q_1, \ldots, q_n] = [q_n, q_{n-1}, \ldots, q_0]$.

Dokaz. Kako se pri invertovanju redosleda ne menjaju parovi uzastopnih članova, suma iz prethodnog tvrđenja ostaje nepromenjena. □

Primenjujući invertovanje dobijamo rekurentnu relaciju (2) u pogodnijoj formi

$$[q_n, q_{n-1}, \ldots, q_0] = q_n[q_{n-1}, \ldots, q_0] + [q_{n-2}, \ldots, q_0].$$

Ako u prethodnoj relaciji opet primenimo invertovanje dobijamo

$$[q_0, q_1, \ldots, q_n] = q_n[q_0, q_1 \ldots, q_{n-1}] + [q_0, q_1, \ldots, q_{n-2}]. \tag{3}$$

Ova relacija pogodnija je jer na desnoj strani ne vršimo promene na početku neprekidnog razlomka već na njegovom kraju.

Sada opet razmatramo $s(q_0, q_1, \ldots, q_n)$ gde su $q_0, q_1, \ldots, q_n \in N^+$. Neka je za $0 \leq m \leq n$, $A_m = [q_0, \ldots, q_m]$ i $B_m = [q_1, \ldots, q_m]$. Tada je, prema (1),

$$s(q_0, \ldots, q_m) = \frac{A_m}{B_m}.$$

Na osnovu Ojlerovog pravila $A_m, B_m \in N^+$. Rekurentna veza (3), za $m \geq 2$ dobija oblik

$$\begin{aligned} A_m &= q_m A_{m-1} + A_{m-2} \\ B_m &= q_m B_{m-1} + B_{m-2}. \end{aligned} \tag{4}$$

Kako je $s(q_0) = q_0 = \frac{q_0}{1}$, to je $A_0 = q_0$ i $B_0 = 1$. Takođe iz $s(q_0, q_1) = \frac{q_0 q_1 + 1}{q_1}$, imamo $A_1 = q_0 q_1 + 1$ i $B_1 = q_1$. Ove jednakosti, zajedno sa (4) u potpunosti određuju A_k, B_k, za $k \leq n$. Kako je $s(q_0, q_1, \ldots, q_n) = \frac{A_n}{B_n}$, na taj način dobijamo vrednost neprekidnog razlomka.

1.3.4. Tvrđenje. *Za $1 \leq m \leq n$ je*

$$A_m B_{m-1} - B_m A_{m-1} = (-1)^{m-1}. \tag{5}$$

Dokaz. Indukcijom po m. Za $m = 1$ imamo $A_1 B_0 - B_1 A_0 = (q_0 q_1 + 1) \cdot 1 - q_1 q_0 = 1$. Pretpostavimo da je tvrđenje tačno za $m < n$ i dokažimo ga za $m + 1$.

$$\begin{aligned} A_{m+1} B_m - B_{m+1} A_m &= (q_{m+1} A_m + A_{m-1}) B_m - (q_{m+1} B_m + B_{m-1}) A_m \\ &= B_m A_{m-1} - A_m B_{m-1} \\ &= -(A_m B_{m-1} - B_m A_{m-1}) \\ &= (-1) \cdot (-1)^{m-1} \\ &= (-1)^m. \quad \square \end{aligned}$$

1.3.5. Posledica. *Neka je $\frac{a}{b} = s(q_0, \ldots, q_n)$. Tada se niz $\frac{A_m}{B_m}$, $0 \leq m \leq n$, alternativno odozdo pa odozgo približava broju $\frac{a}{b}$.*

Dokaz. Iz (5), dobijamo deljenjem sa $B_m B_{m-1}$,

$$\frac{A_m}{B_m} - \frac{A_{m-1}}{B_{m-1}} = (-1)^{m-1} \frac{1}{B_m B_{m-1}}. \tag{6}$$

Otuda je ta razlika za m neparno pozitivna, a za m parno negativna. Kako , prema (4), B_m raste, ta je razlika po apsolutnoj vrednosti sve manja. Otuda je niz sa parnim indeksima rastući a niz sa neparnim indeksima opadajući. Između njih se kao poslednji (najveći u rastućem podnizu ako je n paran i najmanji u opadajućem ako je n neparan) nalazi razlomak $\frac{A_n}{B_n} = \frac{a}{b}$. $\square$

1.3.6. Primer. Kako je $\frac{93}{16} = s(5,1,4,3)$, to je prema formuli (4), $A_0 = 5$, $A_1 = 6$, $A_2 = 29$ i $A_3 = 93$; $B_0 = 1$, $B_1 = 1$, $B_2 = 5$ i $B_3 = 16$, tako da imamo

$$\frac{5}{1} < \frac{29}{5} < \frac{93}{16} < \frac{6}{1}$$

1.4. Prosti brojevi

U ovom odeljku pokazujemo da su prosti brojevi gradivni materijal za izgradnju svih celih brojeva. Takode pokazujemo da ih ima dovoljno za tu ulogu, dakle beskonačno mnogo. Ovde nalazimo i lep primer situacije koja se ponavlja još od antičkog doba: Kada mislimo da je neko pitanje u matematici potpuno razrešeno, ispostavi se da to nije slučaj.

1.4.1. Tvrđenje. *Neka je $n \in N_2$. Postoji prost broj p tako da $p|n$.*

Dokaz. Tvrđenje dokazujemo transfinitnom indukcijom. Dakle, neka je $n \in N_2$ i neka je tvrđenje dokazano za sve brojeve manje od n. Razlikujemo dva slučaja.

Slučaj 1. n je prost. Tada je n prost broj koji deli n.

Slučaj 2. n je složen. Dakle, $D(n) \neq \{1, n\}$. Neka je $k \in D(n) \setminus \{1, n\}$. Tada je $1 < k < n$. Prema indukcijskoj hipotezi postoji prost broj p tako da $p|k$. Otuda i $p|n$, pa je tvrđenje dokazano. □

1.4.2. Tvrđenje. *Neka je $n \in N_2$ složen broj. Postoji prost broj $p \leq [\sqrt{n}]$ tako da $p|n$.*

Dokaz. Neka je n složen broj. Dakle, $D(n) \neq \{1, n\}$. Neka je $k \in D(n) \setminus \{1, n\}$. Kako $k|n$, to postoji $l \in N$ tako da je $n = kl$. Iz $1 < k < n$, sledi $1 < l < n$. Kako je $k \leq l$ ili $l \leq k$, bez gubljenja opštosti pretpostavimo da je $l \leq k$. Prema prethodnom tvrđenju, postoji prost broj p tako da $p|l$. Otuda je $p \leq l$, a time i $p \leq k$. Otuda je

$$p^2 \leq k \cdot l = n \text{ tj. } p \leq [\sqrt{n}]. \quad \square$$

1.4.3. Primer (Eratostenovo sito). Nalazimo sve proste brojeve manje od 100. Kako je $\sqrt{100} = 10$, dovoljno je, kao složene, odstraniti brojeve deljive sa 2,3,5 i 7, osim njih samih. Preostali brojevi su prosti. Na taj način dobijamo listu

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

1.4.4. Teorema. *Prostih brojeva ima beskonačno mnogo.*

Dokaz. Dokaz izvodimo svođenjem na kontradikciju. Dakle, pretpostavimo da je skup P prostih brojeva konačan. Dakle, $P = \{p_1, \ldots, p_k\}$, za neko $k \in N$. Neka je

$$M = p_1 \cdot \ldots \cdot p_k + 1.$$

Kako $M \in N_2$, to postoji prost broj p tako da $p|M$. Kako $p \in P$, to postoji $i \leq k$, tako da je $p = p_i$. Dakle, $p_i|M$. Sdruge strane, kako je $M - 1 = ps$, za $s = p_1 \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_k$, to $p_i|M - 1$. Otuda $p_i|M - (M - 1)$ tj. $p_i|1$. Kontradikcija. Kako nas je pretpostavka da prostih brojeva ima konačno mnogo dovela do kontradikcije, prostih brojeva ima beskonačno mnogo. □

Značaj naredne teoreme vidi se i iz njenog tradicionalnog imena: Osnovna teorema aritmetike. Napomenimo da u formulaciji teoreme koristimo konvenciju da je proizvod po praznom skupu jednak 1.

1.4.5. Teorema. *Za svaki prirodan broj $n \in N_+$, postoje jedinstveni $k \in N$, prosti brojevi $p_1 < p_2 < \cdots < p_k$ i $\alpha_1, \ldots, \alpha_k \in N^+$, tako da je*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Izraz $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ nazivamo prostom faktorizacijom broja n.

Dokaz. Teoremu dokazujemo transfinitnom indukcijom po $n \in N_+$. Za $n = 1$ imamo za $k = 0$ da je 1 proizvod po praznom skupu. Neka je $n \geq 2$ i pretpostavimo da je za $s < n$, tvrđenje dokazano. Najpre dokažimo postojanje faktorizacije za n.

Prema Tvrđenju 1.4.1., postoji prost broj p tako da $p|n$. Neka je $n = pt$, za $t \in N_+$. Kako je $p > 1$, to je $t < n$. Na osnovu indukcijske hipoteze, postoji prosta faktorizacija broja n. Dakle, postoji $l \in N$, prosti brojevi $q_1 < q_2 < \cdots < q_l$ i $\beta_1, \ldots, \beta_k \in N^+$, tako da je

$$t = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}.$$

Sada je $n = p \cdot t = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}$. Razlikujemo dva slučaja.

Slučaj 1. $p \in \{q_1, \ldots, q_l\}$. Neka je $i \leq l$, tako da je $p = q_i$. Tada je $n = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_i^{\beta_i + 1} \cdot \ldots \cdot q_l^{\beta_l}$.

Slučaj 2. $p \notin \{q_1, \ldots, q_l\}$. Mogu nastupiti tri mogućnosti: Da je p manji od svih elemenata skupa $\{q_1, \ldots, q_l\}$, veća od svih njih ili da postoji $i \leq l$ tako da $q_i < p < q_{i+1}$. Analiziraćemo samo treću mogućnost. Ostale dve se analizaraju analogno. Neka je

$$\begin{cases} p_j = q_j, \alpha_j = \beta_j, \text{ za } j \leq i \\ p_j = p, \alpha_j = 1 \text{ za } j = i + 1 \\ p_j = q_{j-1}, \alpha_j = \beta_{j-1}, \text{ za } j > i + 1 \end{cases}.$$

Sada je za $k = l + 1$, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$.

Ostaje da pokažemo da je ova faktorizacija jedinstvena. Neka je

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = s_1^{\gamma_1} \cdot s_2^{\gamma_2} \cdot \ldots \cdot s_l^{\gamma_l}.$$

Dokazaćemo najpre da je $p_1 = s_i$, za neko $i \leq l$. Pretpostavimo suprotno, da je za svako $i \leq l$, $p_1 \neq s_i$. Otuda je za svako $i \leq l$, $(p_1, s_i^{\gamma_i}) = 1$. Prema Posledici 1.2.9. (iii), $(p_1, n) = 1$, što je u kontradikciji sa $p_1 | n$. Na isti način pokazuje se da postoji $j \leq k$, tako da je $s_1 = p_j$. Sada imamo

$$p_j = s_1 \leq s_i = p_1.$$

Kako je po definiciji $p_1 \leq p_j$, to je $p_j = p_1$, dakle, $s_1 = p_1$. Podelimo obe strane jednakosti sa $p_1 = s_1$. Dobijamo

$$(*) \qquad \frac{n}{p_1} = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = s_1^{\gamma_1 - 1} \cdot s_2^{\gamma_2} \cdot \ldots \cdot s_l^{\gamma_l}.$$

Razlikujemo dva slučaja.

Slučaj 1. $\alpha_1 = 1$ ili $\gamma_1 = 1$. Ako je $\alpha_1 = 1$, tada imamo faktorizaciju $\frac{n}{p_1} = p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. Kako je $\frac{n}{p_1} < n$, prema indukcijskoj hipotezi $\frac{n}{p_1}$ ima jedinstvenu faktorizaciju. Zato, ako bi imali $\gamma_1 > 1$, tada bi $s_1^{\gamma_1 - 1} \cdot s_2^{\gamma_2} \cdot \ldots \cdot s_l^{\gamma_l}$, bila takođe faktorizacija broja $\frac{n}{p_1}$. Na osnovu jedinstvenosti faktorizacije imali bi $s_1 = p_2$, suprotno činjenici $s_1 = p_1$ i $p_1 < p_2$. Dakle, $\gamma_1 = 1$, pa je $s_2^{\gamma_2} \cdot \ldots \cdot s_l^{\gamma_l}$ faktorizacija broja $\frac{n}{p_1}$. Na osnovu jedinstvenosti faktorizacije broja $\frac{n}{p_1}$, je $k - 1 = l - 1$ i za svako $2 \leq i \leq k$, je $p_i = q_i$ i $\alpha_i = \gamma_i$. Kako je već pokazano da je $p_1 = s_1$ i $\alpha_1 = \gamma_1 = 1$, dokazana je jedinstvenost faktorizacije. Do iste situacije dolazimo i ako najpre pretpostavimo $\gamma_1 = 1$.

Slučaj 2. $\alpha_1, \gamma_1 > 1$. Tada u jednakosti (*) imamo faktorizacije broja $\frac{n}{p_1}$. Kako je $\frac{n}{p_1} < n$, to prema indukcijskoj hipotezi $\frac{n}{p_1}$ ima jedinstvenu faktorizaciju. Zato je $k = l$ i

$$\alpha_1 - 1 = \gamma_1 - 1$$
$$\alpha_i = \gamma_i, \; 2 \leq i \leq k$$

Time je dokazana jedinstvenost faktorizacije broja n. □

Prethodna teorema predstavlja osnovu za kodiranje konačnih nizova prirodnih brojeva prirodnim brojevima. Najpre objasnimo ideju kodiranja. Dakle, u manipulaciji sa nekom klasom objekata $\mathcal{A}$ veliko pojednostavljenje može se postići ako svakom od objekata $A \in \mathcal{A}$ pridružimo kod (etiketu) a iz klase $\mathcal{B}$. Manipulacija se onda vrši sa kodovima umesto s objektima. Na kraju se

rezultantni kod nazad prevodi u objekat, što je proces dekodiranja. Tipični primeri su pridruživanje broja knjigama u biblioteci, ili klijentima videokluba. Knjige se onda lakše nalaze, a uprava biblioteke ne mora klijente da drži u kartoteci. Neka ograničenja očigledno postoje. Pre svega, važno je da i kodiranje i dekodiranje budu jednoznačni. Time se izbegava da neko uzima knjigu , kada već duguje jednu (na drugu člansku kartu), a takođe i da se ne zna koji od dva člana duguje knjigu.

1.4.6. Posledica. *Neka je $(p_n)_{n\in N}$, skup prostih brojeva poređanih u rastući niz. Preslikavanje $f : N^{<\omega} \to N$, definisano sa*

$$f(\alpha_1, \ldots, \alpha_k) = p_1^{\alpha_1+1} \ldots p_k^{\alpha_k+1}$$

je $1-1$ preslikavanje.

Dokaz. Neka je za $k, l \in N^+$, i $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_l) \in N$

$$f(\alpha_1, \ldots, \alpha_k) = f(\beta_1, \ldots, \beta_l) = n.$$

Tada su $p_1^{\alpha_1+1} \ldots p_k^{\alpha_k+1}$ i $p_1^{\alpha_1+1} \ldots p_k^{\alpha_k+1}$ faktorizacije broja n. Kako n ima jedinstvenu faktorizaciju, to je $k = l$, i za $i \leq k$ je $\alpha_i + 1 = \beta_i + 1$, dakle i $\alpha_i = \beta_i$. Time smo pokazali da je $(\alpha_1, \ldots, \alpha_k) = (\beta_1, \ldots, \beta_l)$. Dakle, f je $1-1$ preslikavanje.

Kao posledicu dobijamo i to da je skup $N^{<\omega}$ prebrojiv.

1.4.7. Posledica. *Prirodan broj je kvadrat akko u prostoj faktorizaciji ima sve izložioce parne.*

Dokaz. Neka je $n \in N_2$ i neka je $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ prosta faktorizacija broja n. ($\Rightarrow$) Neka je $n = m^2$, i neka je $m = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}$ prosta faktorizacija broja m. Odavde je,

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} = q_1^{2\beta_1} \cdot q_2^{2\beta_2} \cdot \ldots \cdot q_l^{2\beta_l}.$$

Kako je faktorizacija broja n jedinstvena, $l = k$, i za $i \leq k$, $q_i = p_i$ i $\alpha_i = 2\beta_i$.

($\Leftarrow$) Pretpostavimo da n ima sve parne izložioce u faktorizaciji. Dakle, $n = p_1^{2\beta_1} \cdot p_2^{2\beta_2} \cdot \ldots \cdot p_k^{2\beta_k}$, za neke $k \in N^+$, proste brojeve p_i i prirodne brojeve $\beta_i \in N^+$, $i \leq k$. Za $m = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ je $n = m^2$. □

1.4.8. Posledica. *Neka su $a, b, c \in N^+$, $(a, b) = 1$ i $ab = c^2$. Tada postoje $k, l \in N$ tako da je $a = k^2$ i $b = l^2$.*

Dokaz. Neka je $a = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ i $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}$. Kako je $(a, b) = 1$, to je $p_i \neq q_j$, za svaki $i \leq k$ i $j \leq l$. Otuda je

$$c^2 = a \cdot b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}.$$

Kako je izraz na desnoj strani, do na uređivanje po veličini osnova, prosta faktorizacija broja c^2, prema prethodnom tvrđenju, imamo da je za svako $i \leq k$, α_i paran broj i za svako $j \leq l$, β_j je paran broj. Prema prethodnom tvrđenju, a i b su kvadrati. □

1.4.9. Definicija. Funkcija $f : N^+ \to N$ je multiplikativna, ako za svaki $a, b \in N^+$,

$$(a, b) = 1 \Rightarrow f(ab) = f(a)f(b).$$

1.4.10. Lema. *Ako je p prost broj i $k \in N^+$, tada je $D(p^k) = \{p^i : 0 \leq i \leq k\}$.*

Dokaz. Dokaz izvodimo indukcijom po k. Za $k = 1$ je, po definiciji prostog broja, $D(p^1) = \{1, p\} = \{p^0, p^1\}$. Pretpostavimo da je tvrđenje dokazano za k i dokažimo ga za $k + 1$. Neka je $d \in D(p^k)$ tj. $d|p^{k+1}$. Pretpostavimo najpre da je $(d, p) = 1$. Tada iz $d|p^k \cdot p$ i $(d, p) = 1$ imamo $d|p^k$. Prema indukcijskoj hipotezi $d = p^i$, za neko $i \leq k$. Međutim za $i > 0$ bi imali $p|d$, suprotno pretpostavci $(d, p) = 1$, dakle $i = 0$ i $d = p^0 = 1$. Pretpostavimo sada da je $(d, p) > 1$. Kako je $D(p) = \{1, p\}$, to je $(d, p) = p$, dakle $p|d$. Neka je $c = \frac{d}{p}$. Tada iz $cp|p^{k+1}$ skraćivanjem dobijamo $c|p^k$. Prema indukcijskoj hipotezi $c = p^i$, za $i \leq k$. Otuda je $d = pc = p^{i+1}$, gde je $i + 1 \leq k + 1$. Time je tvrđenje dokazano. □

1.4.11. Definicija. Neka je $n \in N^+$. $\tau(n) = |D(n)|$.

1.4.12. Tvrđenje. (i) *τ je multiplikativna funkcija.*

(ii) *Neka je $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, gde je $k \in N^+$, $p_1 < \ldots, < p_k$ prosti brojevi i $\alpha_1, \ldots, \alpha_k \in N^+$ prosta fakrorizacija broja $n \in N_2$. Tada je*

$$\tau(n) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1).$$

Dokaz. (i) Neka je $a, b \in N^+$, $(a, b) = 1$. Tada $d|ab$ akko $d = d_a d_b$, $d_a|a$ i $d_b|b$. Dakle, pridruživanje $d \mapsto (d_a, d_b)$ je bijekcija iz $D(ab)$ u $D(a) \times D(b)$. Dakle, $\tau(ab) = \tau(a) \cdot \tau(b)$.

(ii) Prema prethodnoj lemi, za $i \leq k$, $\tau((p_i)^{\alpha_i}) = \alpha_i + 1$. Kako su $p_i^{\alpha_i}$, za $i \leq k$, dva po dva uzajamano prosti, tvrđenje sledi iz (i). □

1.4.13. Definicija. Neka je $n \in N^+$. $\sigma(n) = \sum_{d \in D(n)} d$.

Analogno prethodnom tvrđenju može se pokazati,

1.4.14. Tvrđenje. (i) *σ je multiplikativna funkcija.*

(ii) *Neka je* $n = p_1^{\alpha_1} \cdot p_k^{\alpha_k}$, *gde je* $k \in N^+$, $p_1 < \ldots, < p_k$ *prosti brojevi i* $\alpha_1, \ldots, \alpha_k \in N^+$ *prosta fakrorizacija broja* $n \in N_2$. *Tada je*

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Dokaz. Dokaz ostavljamo čitaocu kao vežbu. □

1.4.15. Primer. Posmatrajmo ostatke pri deljenju sa 4. Kako C_i, $0 \leq i \leq 3$, čine particiju skupa Z, postavlja se pitanje kako je beskonačni skup P raspoređen u odnosu na njih. U C_0, nema prostih brojeva jer za $a \in C_0$, $\{1, 2, 4\} \subset D(a)$. Kako su svi brojevi iz C_2 parni, to za svaki $a \in C_2$, $\{1, 2\} \subset D(a)$. Otuda je jedini prost broj u C_2 broj 2. Dakle, svi prosti brojevi osim 2 su raspoređeni u C_1 i C_3. Da li obe klase sadrže po beskonačno mnogo brojeva? Imitirajući dokaz Teoreme 1.4.4., dokazaćemo da C_3 sadrži beskonačno mnogo prostih brojeva. Dakle, pretpostavimo suprotno, da je $P \cap C_3$ konačan skup. Dakle $P \cap C_3 = \{p_1, \ldots, p_k\}$, za neko $k \in N$. Neka je $M = 4p_1 \ldots p_k - 1$. Očigledno $M \in C_3$. Neka je $M = q_1^{\alpha_1} \ldots q_s^{\alpha_s}$ prosta faktorizacija broja M. Kako je M neparan broj, za svako $i \leq s$, $q_i \in C_1$ ili $q_i \in C_3$. Ako bi za svaki $i \leq s$, imali $q_i \in C_1$, onda bi, na osnovu Primera 1.1.7., imali $M \in C_1$. Kako $M \in C_3$, to postoji $i \leq s$, tako da $q_i \in C_3$. Dakle, $q_i \in P \cap C_3$. Otuda je $q_i = p_j$, za neki $j \leq k$. Tada imamo, kao u dokazu teoreme, da $p_j | M$ i $p_j | M + 1$, pa imamo $p_j | 1$. Kontradikcija.

Dokaz da i u C_1 ima beskonačno mnogo prostih brojeva ne može se izvesti na ovaj način. Problem je što broj u C_1 može imati sve proste faktore iz C_3, kao na primer broj 9. Dokaz odlažemo za odeljak 1.12.

Bez dokaza navodimo teoremu koja uopštava prethodni primer.

1.4.15. Teorema (Dirišle). *Neka je* $n \in N^+$, $a \in Z_n$ *i neka za* $i \in Z_n$, $C_i = \{m \in Z : rem_n(m) = i\}$. C_i *sadrži beskonačno mnogo prostih brojeva akko* $(i, n) = 1$.

1.4.16. Definicija. Za $n \in N$, $\pi(n) = |\{i \leq n : i \text{ je prost broj }\}|$.

Funkcija π je očigledno neopadajuća. Prirodno se postavlja pitanje njenog asimptotskog ponašanja. Opet bez dokaza navodimo teoremu koja daje tu procenu kada $n \to \infty$.

1.4.17. Teorema(Hadamard, de la Vallée Poussin).

$$\pi_n \approx \frac{n}{ln(n)}.$$

1.4.18. Primer. Prethodna teorema nam daje grubu ideju o funkciji $\pi(n)$ bez dugog računanja. Na primer, za $n = 10^6$, dobijamo procenu $\pi(n) \approx \frac{10^6}{6ln(10)} \approx 72.382$, dok je $\pi(n) = 78.498$.

1.5. Ojlerova funkcija

1.5.1. Definicija. Neka je $n \in N_2$. $\Phi_n = \{a \leq n : (a,n) = 1\}$. Ojlerova funkcija je funkcija $\varphi : N^+ \to N$ definisana tako da je za $n \in N_2$, $\varphi(n) = |\Phi_n|$.

Kako je za svaki $n \in N_2$, $(n,1) = 1$, to $1 \in \Phi_n$, dakle $\varphi(n) \geq 1$. S druge strane kako je $\Phi_n \subset Z_n^+$, to je $\varphi(n) < n$.

1.5.2. Primer. Kako je $\Phi_7 = \{1,2,3,4,5,6\}$, to je $\varphi(7) = 6$. Slično je $\Phi_{12} = \{1,5,7,11\}$, pa je $\varphi(12) = 4$.

1.5.3. Tvrđenje. (i) *Ako je p prost broj i $k \in N^+$, $\varphi(p^k) = p^k - p^{k-1}$.*

(ii) *φ je multiplikativn funkcija.*

(iii) *Neka je $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, gde je $k \in N^+$, $p_1 < \ldots, < p_k$ prosti brojevi i $\alpha_1, \ldots, \alpha_k \in N^+$ prosta faktorizacija broja $n \in N_2$. Tada je*

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Dokaz. (i) Neka je $S = \{a \leq p^k : (a,p^k) > 1\}$. Neka je za $a \in S$, $(a,p^k) = d$. Kako $d|p^k$, to je, prema Lemi 1.4.10., $d = p^i$, za neko $i \leq k$. Kako je $d > 1$, to je $i > 0$. Otuda $p|d$. Kako $d|a$, to $p|a$. Dakle,

$$\begin{aligned} S = \{a \leq p^k : p|a\} &= \{a \leq p^k : a = pb \text{ za neki } b\} \\ &= \{pb : pb \leq p^k\} \\ &= \{pb : b \leq p^{k-1}\}. \end{aligned}$$

Otuda je $|S| = p^{k-1}$. Kako je $Z_{p^k}^+ = S \cup \Phi_{p^k}$, to je $\varphi(p^k) = |\Phi_{p^k}| = p^k - p^{k-1}$.

(ii)Neka je $f : \Phi_{kl} \to \Phi_k \times \Phi_l$ definisano tako da je $f(a)$ uređeni par $(rem_k(a), rem_l(a))$. Pokažimo najpre da je f dobro definisano tj. da za $a \in \Phi_{kl}$, $rem_k(a) \in \Phi_k$ i $rem_l(a) \in \Phi_l$. Neka je $rem_k(a) = r$ i $(r,k) = d$. Kako $k|a - r$, to $d|a - r$. Kako $d|r$, to $d|a$. Kako $d|k$, to $d|kl$. Dakle, $d \in D(a,kl)$. Kako je $a \in \Phi_{kl}$, $d = 1$, dakle $r \in \Phi_k$. Slično pokazujemo $rem_l(a) \in \Phi_l$.

Pokažimo da je f 1-1 preslikavanje. Dakle, neka je za $a,b \in \Phi_{kl}$, $f(a) = f(b)$. Tada je $rem_k(a) = rem_k(b)$ i $rem_l(a) = rem_l(b)$. Otuda $k|b - a$ i $l|b - a$. Kako je $(k,l) = 1$, prema Tvrđenju 1.2.9.(iv), $kl|b - a$. Kako je $1 \leq a,b \leq kl$, to je $|b - a| < kl$ pa je $a = b$.

Ostaje da dokažemo da je f preslikavanje na. Neka je $s \in \Phi_k$ i $t \in \Phi_l$. Prema Bezu-ovoj teoremi, postoje $u,v \in Z$ tako da je $1 = uk + vl$. Neka je $a = rem_{kl}(vls + ukt)$. Pokažimo da je $a \in \Phi_{kl}$. Po definiciji a imamo

$0 \leq a < kl$. Neka je $d = (a, kl) > 1$. Prema Tvrđenju 1.4.1., postoji prost broj p tako da $p|d$, dakle $p|a$ i $p|kl$. Kako je $(k, l) = 1$, prema Tvrđenju 1.2.9, $p|k$ ili $p|l$. Bez gubljenja opštosti pretpostavimo da $p|k$. Kako je $(k, l) = 1$, $p \nmid l$. Iz $1 = uk + vl$ i $p|uk$, imamo $p \nmid vl$, jer bi u suprotnom dobili $p|1$. Prema Tvrđenju 1.2.1., $d = (vls + ukt, kl)$, pa $p|vls + ukt$. Kako $p|k$, to $p|ukt$ pa imamo $p|vls$. Kako $p \nmid vl$, to imamo $p|s$. Sada imamo $p|s$ i $p|k$, suprotno pretpostavci $s \in \Phi_k$. Iz dobijene kontradikcije zaključujemo da je $(a, kl) = 1$.

Ostaje da dokažemo da je $f(a) = (s, t)$. Kako je $a = rem_{kl}(uls + vkl)$, to je $a = qkl + ukt + vls$, za neki $q \in Z$. Zamenom $vl = 1 - uk$ dobijamo

$$a = qkl + ukt + (1 - uk)s = k(ql + ut - us) + s.$$

Kako je $0 \leq s < k$, po definiciji je $rem_k(a) = s$.

Dualno se pokazuje da je $rem_l(a) = t$. Dakle, $f(a) = (s, t)$. Time je pokazano da je f "na" preslikavanje, dakle bijekcija.

Otuda je $|\Phi_{kl}| = |\Phi_k| \cdot |\Phi_l|$ tj. $\varphi(kl) = \varphi(k) \cdot \varphi(l)$.

(iii) Kako su $p_i^{\alpha_i}$, $i \leq k$, uzajamno prosti brojevi to je

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).\end{aligned}$$

1.5.4. Primer. Kako je $360 = 2^3 \cdot 3^2 \cdot 5$, to je $\varphi(360) = (2^3 - 2^2)(3^2 - 3)(5 - 1) = 96$.

1.6. Relacija kongruencije po modulu

1.6.1. Definicija. Neka je $m \in N^+$. Relacija $\equiv_m$ definiše se tako da je za $a, b \in Z$,

$$a \equiv_m b \Leftrightarrow m|b - a.$$

1.6.2. Tvrđenje. *Neka je $m \in Z$ i $a, b \in Z$. $a \equiv_m b$ akko $rem_m(a) = rem_m(b)$.*

Dokaz. Neka je $rem_m(a) = r$ i $rem_m(b) = s$, $0 \leq r, s < m$. Tada je za neke brojeve $q, q' \in Z$, $a = mq + r$ i $b = mq' + s$. Bez gubljenja opštosti pretpostavimo da je $r \leq s$ Tada je $b - a = m(q' - q) + (s - r)$. Kako je $0 \leq s - r < m$, to $m|s - r$ akko $s - r = 0$ tj. $s = r$. Kako $m|b - a$ akko $m|s - r$, to $m|b - a$ akko $s = r$.

1.6.3. Tvrđenje. *Neka je* $m \in N^+$.

(i) $\equiv_m$ *je relacija ekvivalencije skupa* Z.

(ii) $Z/\equiv_m = \{i/\equiv_m : 0 \leq i < n\}$.

(iii) *Za* $0 \leq i < n$, $i/\equiv_m = mZ + i$.

Dokaz. (i) Sledi trivijalno iz prethodnog tvrđenja, jer je $\equiv_m$ svedena na jednakost ostataka.

(ii) Neka je $a \in Z$ i neka je $rem_m(a) = i$, $0 \leq i < n$. Kako je $rem_m(a) = rem_m(i) = i$, to je $a \equiv_m i$, dakle $a/\equiv_m = i/\equiv_m$. Otuda je $Z/\equiv_m = \{i/\equiv_m : 0 \leq i < n\}$. Sve navedene klase su različite među sobom. Zaista, ako je $0 \leq i < j < n$, tada je $rem_m(i) = i \neq j = rem_m(j)$, dakle $i \not\equiv_m j$, pa je $i/\equiv_m \neq j/\equiv_m$.

(iii) Neka je $0 \leq i < n$. Tada je

$$\begin{aligned} a \in i/\equiv_m &\Leftrightarrow a \equiv_m i \\ &\Leftrightarrow rem_m(a) = i \\ &\Leftrightarrow \exists q(a = mq + i) \\ &\Leftrightarrow a \in mZ + i. \end{aligned}$$

1.6.4. Primer. U Primeru 1.1.7., C_0, C_1, C_2 i C_3 su klase ekvivalencije za $\equiv_4$.

1.6.5. Tvrđenje. *Neka je* $m, n \in N^+$ *i* $a, b, c, d \in Z$.

(i) $a \equiv_m b \,\&\, c \equiv_m d \Rightarrow a + c \equiv_m b + d$.

(ii) $a \equiv_m b \Rightarrow ac \equiv_m bc$.

(iii) $a \equiv_m b \,\&\, c \equiv_m d \Rightarrow a \cdot c \equiv_m b \cdot d$.

(iv) $a \equiv_m b \Rightarrow a^n \equiv b^n$.

Dokaz. (i) Prema definiciji relacije $\equiv_m$, $m|b-a$ i $m|d-c$. Prema Tvrđenju 1.1.4.(i), $m|(b-a)+(d-c)$, tj. $m|(b+d)-(a+c)$. Otuda je $a+c \equiv_m b+d$.

(ii) Opet imamo $m|b-a$. Prema Tvrđenju 1.1.4.(ii), $m|c(b-a)$ tj. $m|bc-ac$. Po definiciji je $ac \equiv_m bc$.

(iii) Neka je $a \equiv_m b$ i $c \equiv_m d$. Prema prethodnom delu, imamo $ac \equiv_m bc$ i $bc \equiv_m bd$. Kako je $\equiv_m$ tranzitivna, $ac \equiv_m bd$.

(iv) Neka je $a \equiv_m b$. Dokaz da je $a^n \equiv_m b^n$ izvodimo indukcijom po n, pri čemu za indukcijski korak koristimo (iii). Dakle, za $n = 1$ tvrđenje je trivijalno zadovoljeno. Pretpostavimo da je tvrđenje dokazano za $n \in N^+$, dakle $a^n \equiv_m b^n$. Dokažimo tvrđenje za $n+1$. Kako je $a^n \equiv_m b^n$ i $a \equiv_m b$, prema (iii), dobijamo $a^n \cdot a \equiv_m b^n \cdot b$, tj. $a^{n+1} \equiv_m b^{n+1}$. Time je tvrđenje dokazano.

Iz prethodnog tvrđenja zaključujemo da se relacija $\equiv_m$ ponaša kao jednakost u odnosu na operacije sabiranja i množenja. To nam omogućuje da izračunavamo ostatke nekih brojeva bez njihovog efektivnog izračunavanja.

1.6.6. Primer. Izračunaćemo ostatak broja 6^{1998} pri deljenju sa 7. Kako je $6 \equiv_7 -1$, to je prema tački (iv) prethodnog tvrđenja,

$$6^{1998} \equiv_7 (-1)^{1998} = 1.$$

Dakle, razmatrani broj daje ostatak 1 pri deljenju sa 7.

Pojednostavljenje se ne postiže uvek u jednom koraku. Izračunajmo ostatak pri deljenju 3^{1999} sa 11. Sada je

$$\begin{aligned} 3^{1999} &\equiv_{11} 3 \cdot 3^{1998} \\ &\equiv_{11} 3 \cdot (3^2)^{999} \\ &\equiv_{11} 3 \cdot (-2)^{999} \\ &\equiv_{11} -3 \cdot 2^4 \cdot 2^{995} \\ &\equiv_{11} -3 \cdot 5 \cdot (2^5)^{199} \\ &\equiv_{11} -15 \cdot (-1)^{199} \\ &\equiv_{11} -15 \cdot (-1) \\ &\equiv_{11} 4 \end{aligned}$$

1.6.7. Primer. Izvešćemo testove za deljivost sa 3,9 i 11. Neka je $n = a_k \cdot 10^k + \cdots + a_1 \cdot 10 + a_0$ dekadni zapis broja n. Kako je $10 \equiv_3 1$ i $10 \equiv_9 1$, to je

$$n \equiv_9 a_k \cdot 1^k + \cdots + a_1 \cdot 1 + a_0.$$

Dakle, broj je pri deljenju sa 9(3) daje isti ostatak kao i njegov zbir njegovih cifara.

Slično, koristeći da je $10 \equiv_{11} -1$, dobijamo da n pri deljenju sa 11 daje isti ostatak kao broj $a_0 - a_1 + a_2 + \cdots + (-1)^k a_k$.

U odnosu na relaciju $\equiv_m$ jednačine se mogu rešavati kao i kod obične jednakosti. Međutim, kod skraćivanja relacija $\equiv_m$ ima neka ograničenja.

1.6.8. Tvrđenje. *Neka je $m, n \in N^+$ i $a, b, c, d \in Z$.*

(i) *Ako $d|a$, $d|b$ i $(d, m) = 1$, tada $a \equiv_m b \Leftrightarrow \frac{a}{d} \equiv_m \frac{b}{d}$.*

(ii) *Ako $d|a$, $d|b$ i $d|m$, tada $a \equiv_m b \Leftrightarrow \frac{a}{d} \equiv_{\frac{m}{d}} \frac{b}{d}$.*

Dokaz. (i) Neka je $d|a$, $d|b$, $(d, m) = 1$, i $a \equiv_m b$. Neka je $a_1 = \frac{a}{d}$ i $b_1 = \frac{b}{d}$. Kako $m|b - a$, to imamo $m|d(b_1 - a_1)$. Kako je $(m, d) = 1$, prema Tvrđenju 1.2.9. (i), imamo $m|b_1 - a_1$. Dakle, $a_1 \equiv_m b_1$ tj. $\frac{a}{d} \equiv_m \frac{b}{d}$.

(ii) Neka je $a = a_1 d$, $b = b_1 d$, $m = m_1 d$ i $a \equiv_m b$. Sada imamo $m|b - a$ tj. $b - a = mt$, za neki $t \in Z$. Zamenom vrednosti za a, b i m dobijamo

$b_1 d - a_1 d = m_1 dt$. Skraćivanjem jednakosti sa d, dobijamo $b_1 - a_1 = m_1 t$. Otuda imamo $m_1 | b_1 - a_1$ tj. $a_1 \equiv_{m_1} b_1$. Kako je $a_1 = \frac{a}{d}$ i $b_1 = \frac{b}{d}$, tvrđenje je dokazano.

1.6.9. Primer. Pokazaćemo da skraćivanje može biti nekorektno ako nisu zadovoljeni uslovi prethodnog tvrđenja.

Ako relaciju $8 \equiv_6 20$ skratimo sa 4 dobijamo $2 \equiv_6 10$, što nije tačno jer $6 \nmid (10 - 2)$.

1.7. Sistemi ostataka

1.7.1. Definicija. Neka je $m \in N_2$. Potpuni sistem ostataka modulo m, u oznaci PSO_m, je transverzala faktor skupa $Z/\equiv_m$.

1.7.2. Primer. $A = \{6, 5, 19, 90, 24, 33, 100, 55\}$ je PSO_8. Zaista $24 \in 0/\equiv_8$, $33 \in 1/\equiv_8$, $90 \in 2/\equiv_8$, $19 \in 3/\equiv_8$, $100 \in 4/\equiv_8$, $5 \in 5/\equiv_8$, $6 \in 6/\equiv_8$ i $55 \in 7/\equiv_8$.

1.7.3. Tvrđenje. *Neka je A potpuni sistem ostataka modulo m. Tada,*

(i) *Za proizvoljne $a, b \in A$, ako je $a \neq b$ onda je $a \not\equiv_m b$.*

(ii) *Neka je $s \in Z$. Postoji $a \in A$, tako da je $a \equiv_m s$.*

(iii) $|A| = m$.

(i) Neka su $a, b \in A$, $a \neq b$. Kako je A transverzala skupa $Z/\equiv_m$, i $a \in a/\equiv_m$, $b \in b/\equiv_m$, to je $a/\equiv_m \neq b/\equiv_m$. Otuda imamo $a \not\equiv_m b$.

(ii) Neka je $s \in Z$. Kako je A transverzala skupa $A/\equiv_m$ i $s/\equiv_m \in A/\equiv_m$, to postoji $a \in A$, tako da $a \in s/\equiv_m$. Po definiciji klase ekvivalencije je $a \equiv_m s$.

(iii) Neka je $f : A \to Z/\equiv_m$ definisano sa $f(a) = a/\equiv_m$, $a \in A$. Kako je A transverzala skupa $Z/\equiv_m$, dakle iz svake klase ekvivalencije sadrži po tačno jedan element, f je bijekcija. Otuda je $|A| = |Z/\equiv_m|$. Prema Tvrđenju 1.6.3. (ii), $|Z/\equiv_m| = m$, dakle $|A| = m$.

Ma koja dva od tri uslova iz prethodnog tvrđenja definišu A kao PSO_m. Mi formulišemo i dokazujemo jedno od tih tvrđenja.

1.7.4. Tvrđenje. *Neka je $m \in N^+$. Ma kojih m nekongruentnih celih brojeva nekongruentnih po modulu m čini PSO_m.*

Dokaz. Neka je A skup od m brojeva koji zadovoljavaju uslove tvrđenja. Neka je, kao u tački (iii) prethodnog tvrđenja, $f : A \to Z/\equiv_m$ definisano sa $f(a) = a/\equiv_m$, $a \in A$. Neka je $a, b \in A$, $a \neq b$. Po pretpostavci tvrđenja je $a \not\equiv_m b$, pa je $a/\equiv_m \neq b/\equiv_m$. Dakle, A iz svake klase ekvivalencije sadrži

najviše jedan element. S druge strane, dokazali smo da je $f(a) \neq f(b)$, za $a \neq b$. Time smo pokazali da je f 1-1 preslikavanje istobrojnih konačnih skupova A i $Z/\equiv_m$. Prema Tvrdenju ??, f je bijekcija. Otuda za svaki $C \in Z/\equiv_m$, postoji $a \in A$, tako da je $f(a) = C$, tj. $a/\equiv_m = C$, odnosno $a \in C$. Dakle, A iz svake klase ekvivalencije sadrži po bar jedan element. Kako smo već pokazali da A iz svake klase sadrži najviše jedan element, A je transverzala skupa $Z/\equiv_m$.

1.7.5. Posledica. *Ma kojih m uzastopnih brojeva čini PSO_m.*

Dokaz. Kako je razlika ma koja dva člana tog skupa po apsolutnojvrednosti manja od m, to su oni nekongruentni pa, prema prethodnom tvrđenju, čine PSO_m.

1.7.6. Primer. $Z_m = \{0, 1, \ldots, m-1\}$ je PSO_m. Ovde smo iz svake klase izabrali najmanji pozitivni element. Ako iz svake klase izaberemo element sa najmanjom apsolutnom vrednošću dobijamo PSO_m. Ako je $m = 2k$ paran broj, onda taj PSO_m ima oblik $0, \pm 1, \ldots, \pm(k-1), k$. Ako je $m = 2k+1$, tada taj PSO_m ima oblik $0, \pm 1, \ldots, \pm k$.

1.7.7. Tvrđenje. *Neka je A PSO_m i $c \in Z$, tako da je $(c, m) = 1$. Tada je za ma koji $d \in Z$, $cA + d = \{cx + d : x \in A\}$ PSO_m.*

Dokaz. Neka je $S = cA + d$. Dokazaćemo da je S skup od m nekongruentnih (po modulu m) brojeva. Neka je $f : A \to S$, definisano sa $f(x) = cx + d$. f je po definiciji skupa S na preslikavanje. Neka je $a, b \in A$ tako da je $a \neq b$. Dokazaćemo da je $f(a) \not\equiv_m f(b)$. Pretpostavimo suprotno, da je $f(a) \equiv_m f(b)$. Sada imamo

$$ca + d \equiv_m cb + d.$$

Dodavanjem $-d$ obema stranama relacije dobijamo $ca \equiv_m cb$. Kako je $(c, m) = 1$, prema Tvrdenju 1.6.8. (i), skraćivanjem sa c dobijamo $a \equiv_m b$. To je u kontradikciji sa činjenicom da su a i b različiti elementi PSO_m, naime A. Iz dobijene kontradikcije zaključujemo da je $f(a) \not\equiv_m f(b)$. Odatle zaključujemo da je f bijekcija i da je S skup nekongruentnih brojeva. Kako je $|A| = m$, to je i $|S| = m$. Dobili smo da je S skup od m nekongruentnih celih brojeva, pa tvrđenje sledi iz prethodnog.

Primetimo da se klase ekvivalencije po modulu m ponašaju uniformno po pitanju uzajamne prostosti sa m.

1.7.8. Tvrđenje. *Neka je $m \in N_2$, $a \in Z$ i $(a, m) = 1$. Za svaki $b \in a/\equiv_m$, $(b, m) = 1$.*

Dokaz. Neka je $b \in a/\equiv_m$ tj. $a \equiv_m b$, i neka je $d = (b, m)$. Kako $m|b-a$, to postoji $t \in Z$, tako da je $b - a = mt$. Kako $d|b$ i $d|mt$, to $d|a$. Dakle, $d \in D(a, m)$. Kako je $(a, m) = 1$, to je $d = 1$. $(a, m) = (b, m) = 1$.

Na osnovu toga kazaćemo da je klasa ekvivalencije $a/\equiv_m$ uzajamno prosta sa m ako je a (a time i ostali predstavnici klase) uzajamno prost sa m. Skup klasa ekvivalencije uzajamno prostih sa m označićemo sa R_m.

1.7.9. Definicija. Neka je $m \in N_2$. $F \subset Z$ je redukovani sistem ostataka modulo m, skraćeno RSO_m, akko je transverzala skupa R_m.

1.7.10. Primer. Kako je $Z/\equiv_6 = \{0/\equiv_6, \ldots, 5/\equiv_6\}$, i samo su 1 i 5 uzajamno prosti sa 6, to je $\{1, 5\}$ RSO_6.

1.7.11. Tvrđenje. *Neka je $m \in N_2$, A PSO_m i $F = \{a \in A : (a, m) = 1\}$. F je RSO_m.*

Dokaz. Kako je $Z/\equiv_m = \{a/\equiv_m : a \in A\}$, to je $R_m = \{a/\equiv_m : a \in F\}$. Dakle, F je RSO_m.

1.7.12. Posledica. *Neka je $m \in N_2$.*
(i) *Φ_m je RSO_m*
(ii) $|R_m| = \varphi(m)$.

Dokaz. (i) Kako je Z_m PSO_m, tvrđenje sledi iz prethodnog.
(ii) Kako je Φ_m transverzala skupa R_m, to je preslikavanje $f : \Phi_m \to R_m$ definisano sa $f(a) = a/\equiv_m$ bijekcija. Otuda je $|R_m| = |\Phi_m| = \varphi(m)$.

1.7.13. Tvrđenje. *Neka je F redukovani sistem ostataka modulo m.*
(i) *Za proizvoljne $a, b \in F$, ako je $a \neq b$ onda je $a \not\equiv_m b$.*
(ii) *Neka je $s \in Z$ tako da $(s, m) = 1$. Postoji $a \in F$, tako da je $a \equiv_m s$.*
(iii) $|F| = \varphi(m)$.

(i) Neka su $a, b \in F$, $a \neq b$. Kako je A transverzala skupa R_m, i $a \in a/\equiv_m$, $b \in b/\equiv_m$, to je $a/\equiv_m \neq b/\equiv_m$. Otuda imamo $a \not\equiv_m b$.

(ii) Neka je $s \in Z$ i $(s, m) = 1$. Kako je A transverzala skupa R_m, , kome pripada $s/\equiv_m$, to postoji $a \in A$, tako da $a \in s/\equiv_m$. Po definiciji klase ekvivalencije je $a \equiv_m s$.

(iii) Neka je $f : F \to R_m$ definisano sa $f(a) = a/\equiv_m$, $a \in F$. Kako je F transverzala skupa R_m, dakle iz svake klase ekvivalencije sadrži po tačno jedan element, f je bijekcija. Otuda je $|F| = |R_m|$. Prema Posledici 1.7.12.(ii), $|R_m| = \varphi(m)$, dakle $|F| = \varphi(m)$.

Ako je F skup brojeva uzajamno prostih sa m, onda ma koja dva od tri uslova iz prethodnog tvrđenja definišu F kao RSO_m. Mi formulišemo i dokazujemo jedno od tih tvrđenja.

1.7.14. Tvrđenje. *Ma kojih $\varphi(m)$ celih brojeva nekongruentnih po modulu m, uzajamno prostih sa m čini PSO_m.*

Dokaz. Neka je F skup od $\varphi(m)$ brojeva koji zadovoljavaju uslove tvrđenja. Neka je, kao u tački (iii) prethodnog tvrđenja, $f : F \to R_m$ definisano sa $f(a) = a/\equiv_m$, $a \in A$. Kako je $(a, m) = 1$, to je $f(a) \in R_m$, dakle preslikavanje je korektno definisano. Neka je $a, b \in A$, $a \neq b$. Po pretpostavci tvrđenja je $a \not\equiv_m b$, pa je $a/\equiv_m \neq b/\equiv_m$. Dakle, F iz svake klase ekvivalencije iz R_m sadrži najviše jedan element. S druge strane, dokazali smo da je $f(a) \neq f(b)$, za $a \neq b$. Time smo pokazali da je f 1-1 preslikavanje istobrojnih konačnih skupova F i R_m. Prema Tvrđenju ??, f je bijekcija. Otuda za svaki $C \in R_m$, postoji $a \in F$, tako da je $f(a) = C$, tj. $a/\equiv_m = C$, odnosno $a \in C$. Dakle, A iz svake klase ekvivalencije iz R_m sadrži po bar jedan element. Kako smo već pokazali da A iz svake klase sadrži najviše jedan element, F je transverzala skupa R_m.

1.7.15. Tvrđenje. *Neka je F RSO_m i $c \in Z$, tako da je $(c, m) = 1$. Tada je $cF = \{cx : x \in F\}$ RSO_m.*

Dokaz. Neka je $S = cF$. Neka je $s \in S$. Po definiciji skupa S, $s = ca$ za neki $a \in F$. Kako je $(c, m) = 1$ i $(c, a) = 1$, to je i $(c, s) = 1$. Dakle, S je skup brojeva uzajamno prostih sa m. Dokazaćemo da je S skup od $\varphi(m)$ nekongruentnih (po modulu m) brojeva. Neka je $f : A \to S$, definisano sa $f(x) = cx$. f je po definiciji skupa S "na" preslikavanje. Neka je $a, b \in A$ tako da je $a \neq b$. Dokazaćemo da je $f(a) \not\equiv_m f(b)$. Pretpostavimo suprotno, da je $f(a) \equiv_m f(b)$. Sada imamo

$$ca \equiv_m cb.$$

Kako je $(c, m) = 1$, prema Tvrđenju 1.6.8.(i), skraćivanjem sa c dobijamo $a \equiv_m b$. To je u kontradikciji sa činjenicom da su a i b različiti elementi RSO_m, naime F. Iz dobijene kontradikcije zaključujemo da je $f(a) \neq f(b)$. Odatle zaključujemo da je f bijekcija i da je S skup nekongruentnih brojeva. Kako je $|F| = \varphi(m)$, to je i $|S| = \varphi(m)$. Dobili smo da je S skup od m nekongruentnih celih brojeva uzajamno prostih sa m, pa tvrđenje sledi iz prethodnog.

1.7.16. Posledica. *Neka je $m \in n_2$ i $c \in Z$, tako da $(c, m) = 1$. Postoji $b \in Z$, tako da je $c \cdot b \equiv_m 1$.*

Dokaz. Neka je F RSO_m i $S = cF$. Prema prethodnom tvrđenju, S je RSO_m. Kako je $(1, m) = 1$, prema Tvrđenju 1.7.13. (ii), postoji $s \in S$ tako da je $s \equiv_m 1$. Po definiciji skupa S, $s = ca$, za neki $a \in F$. Otuda je $ca \equiv_m 1$. □

Kao jednostavne posledice dobijenih rezultata imamo velike teoreme Teorije brojeva.

1.7.17. Teorema (Ojlerova teorema). *Neka je $m \in N_2$ i $c \in Z$ tako da je $(c, m) = 1$.*

$$c^{\varphi(m)} \equiv_m 1.$$

Dokaz. Neka je F RSO_m i $S = cF = \{cx | x \in F\}$. Prema Tvrđenju 1.7.15, S je RSO_m. Kako, na osnovu Tvrđenja 1.7.13, za svaki broj iz S postoji tačno jedan broj iz F koji je sa njim kongruentan, to je $\prod S \equiv_m \prod F$. Kako su svi brojevi iz S uzajamno prosti sa m, to je i $\prod S$ uzajamno prost sa m. Kako je

$$\begin{aligned}\prod S &= \prod \{cx : x \in F\} \\ &= c^{\varphi(m)} \prod \{x : x \in F\} \\ &= c^{\varphi(m)} \prod F \\ &\equiv_m c^{\varphi(m)} \prod S.\end{aligned}$$

Kako je $\prod S$ uzajamno prost sa m, skraćivanjem sa $\prod S$ dobijamo traženu jednakost. □

1.7.18. Posledica (Mala Fermaova teorema). *Neka je p prost broj i $a \in Z$, tako da $p \nmid a$. Tada je*

$$a^{p-1} \equiv_m 1.$$

Dokaz. Kako $p \nmid a$, to je $(a, p) = 1$. Kako je $\varphi(p) = p - 1$, tvrđenje sledi iz prethodnoh. □

Mala Fermaova teorema iskazuje se i u drugom obliku.

1.7.19. Posledica. *Neka je p prost broj i $a \in Z$. Tada je*

$$a^p \equiv_m a.$$

Dokaz. Ako $p \nmid a$, onda prema prethodnoj posledici imamo $a^{p-1} \equiv_m 1$. Množenjem te jednakosti sa a dobijamo željenu jednakost.

Ako $p|a$, tada je $a \equiv_p 0$, pa je $a^p \equiv_m a \equiv_m 0$. □

Dokažimo jednu lemu koju koristimo u dokazu sledeće teoreme.

1.7.20. Primer. Prethodne teoreme omogućuju nam da brže računamo ostatke stepena po nekom modulu. Kako je $\varphi(14) = 6$, to je $3^6 \equiv_{14} 1$. Otuda je

$$\begin{aligned} 3^{2000} &\equiv_{14} 3^{6\cdot 333+2} \\ &\equiv_{14} (3^6)^{333} \cdot 9 \\ &\equiv_{14} 9. \end{aligned}$$

1.7.21. Lema. *Neka je p prost broj i $a \in Z$. $a^2 \equiv_p 1$ akko $a \equiv_p \pm 1$.*

Dokaz.

$$\begin{aligned} a^2 \equiv_p 1 &\Leftrightarrow p|(a^2-1) \\ &\Leftrightarrow p|(a-1)(a+1) \\ &\Leftrightarrow p|a-1 \vee p|a+1 \\ &\Leftrightarrow a \equiv_p 1 \vee a \equiv_p -1. \quad \square \end{aligned}$$

1.7.22. Teorema. *(Vilsonova teorema) Neka je $n \in N_2$. n je prost broj akko $(n-1)! \equiv_n -1$.*

Dokaz. ($\Leftarrow$) Dokazujemo kontrapoziciju te implikacije. Dakle, neka je n složen broj. Tada je $n = kl$, za $1 < k, l < n$. Ako je $k \neq l$, tada $(n-1)! = 1 \cdot 2 \cdot \ldots \cdot k \cdot \ldots \cdot l \cdot \ldots (n-1)$. Otuda $n = kl|(n-1)!$, tj. $(n-1)! \equiv_n 0$, dakle $(n-1)! \not\equiv_n -1$. Ako je $k = l > 2$, tj. $n = k^2$, onda iz $k > 2$, imamo $2k < n$. Otuda je $(n-1)! = 1 \cdot 2 \cdot \ldots \cdot k \cdot \ldots \cdot 2k \cdot \ldots (n-1)$. Otuda $n = k^2|(n-1)!$ tj. $(n-1)! \equiv_n 0$, dakle $(n-1)! \not\equiv_n -1$. Ako je,konačno $n = k^2$ i $k = 2$, onda je $(n-1)! = 3! = 6 \equiv_4 2$, dakle $(n-1)! \not\equiv_n -1$.

($\Rightarrow$) Neka je $n = p$ prost broj. Tada je $F = \{1, 2, \ldots, p-1\}$ RSO_p. Prema Tvrđenju 1.7.16., za svaki $a \in F$, postoji $b \in F$ tako da je $ab \equiv_p 1$. Pri tome $a = b$ akko $a = \pm 1$. Dakle, $F \setminus \{-1, 1\}$ se može podeliti u parove brojeva čiji su proizvodi kongruentni sa 1. Otuda je

$$(p-1)! \equiv_p (-1) \cdot 1 \cdot 1^{\frac{p-1}{2}} \equiv_p -1$$

$\square$

1.8. Jednačine po modulu m

1.8.1. Definicija. Neka je $n \in N$ i $(a_i)_{i \leq n}$ niz celih brojeva takav da je $a_n \neq 0$. Izraz $p(x) = \sum_{i \leq n} a_i x^i$ nazivamo polinomom stepena n sa celobrojnim koeficijentima. Skup polinoma sa celobrojnim koeficijentima označavamo sa $Z[x]$.

1.8.2. Definicija. Neka je $p \in Z[x]$. Formulu oblika $p(x) \equiv_m 0$ nazivamo jednačinom po modulu m.

Primetimo da ako je za neki $c \in Z$, $p(c) \equiv_m 0$, da je onda za svaki $a \in c/\equiv_m$, takođe $p(a) \equiv_m 0$. Dakle, brojevi iz iste klase ekvivalencije ili svi zadovoljavaju jednačinu ili nijedan. Zato se rešenje jednačine traži iz nekog PSO_m, recimo Z_m. Otuda jednačinu modulo m možemo smatrati i jednačinom u Z_m gde su koeficijenti polinoma svedeni modulo m.

1.8.3. Definicija. Neka je A PSO_m. Rešenje jednačine $p(x) \equiv_m 0$ je svaki broj $a \in A$ tako da je $p(a) \equiv_m 0$.

1.8.4. Teorema. *(Lagranžova teorema) Neka je $p \in Z[x]$, $p \neq 0$ polinom stepena $n \in N$. Tada jednačina $p(x) = 0$ ima najviše n rešenja.*

Dokaz. Dokaz izvodimo indukcijom po stepenu polinoma p. Neka je najpre p konstantan polinom (stepena 0). Tada je p ne-nula konstanta, pa p nema nijednu nulu. Pretpostavimo da je tvrđenje dokazano za sve polinome stepena n i dokažimo ga za polinome stepena $n+1$. Dakle, neka je p polinom stepena $n+1$. Ako p nema nijednu nulu, tada je tvrđenje trivijalno zadovoljeno jer je $0 \leq n+1$. Pretpostavimo sada da p ima bar jednu nulu, i neka je a jedna od njih. Tada je, prema Bezuovoj teoremi, $p = (x-a)q$, za neki polinom q. Kako se koeficijenti polinoma q mogu dobiti Hornerovom šemom, to i $q \in Z[x]$. q je polinom stepena n. Prema indukcijskoj hipotezi, q ima najviše n nula. Neka je sada $b \in Z$.

$$\begin{aligned} p(b) = 0 &\Leftrightarrow (b-a)q(b) = 0 \\ &\Leftrightarrow b = a \vee q(b) = 0. \end{aligned}$$

Dakle, p ima nule polinoma q i još jednu nulu, naime a, pa je taj broj ukupno najviše $n+1$. □

Jednačine po složenim modulima mogu se razložiti na sistem jednačina po manjim modulima.

1.8.5. Tvrđenje. *Neka je $m = q_1^{\alpha_1} \cdot \ldots \cdot q_k^{\alpha_k}$ prosta faktorizacija broja $m \in N_2$. Tada je jednačina $p(x) \equiv_m 0$ ekvivalentna sistemu jednačina*

$$\begin{aligned} p(x) &\equiv_{q_1^{\alpha_1}} 0 \\ &\vdots \\ p(x) &\equiv_{q_k^{\alpha_k}} 0. \end{aligned}$$

Dokaz. Neka je $m_i = q_i^{\alpha_i}$, $i \leq k$. Kako su brojevi m_i, $i \leq k$, uzajamno prosti, to za proizvoljni $a \in Z$ imamo da $m|P(a)$ akko $m_i|p(a)$, za svaki $i \leq k$. Otuda imamo da je $p(a) \equiv_m 0$ akko $p(a) \equiv_{m_i} 0$, za svako $i \leq k$. □

1.8.6. Primer. Rešavamo jednačinu

$$p(x) = x^4 + 2x^3 + 8x + 9 \equiv_{35} 0.$$

Ona je ekvivalentna sistemu $p(x) \equiv_5 0$ i $p(x) \equiv_7 0$. Probanjem utvrđujemo da prva jednačina ima skup rešenja 1,4, a druga 3,5,6. Zadatak ćemo završiti kasnije, kada vidimo kako se rade sistemi jednačina po različitim modulima.

1.9. Primitivni ostatak po prostom modulu

1.9.1. Primer. Posmatrajmo $\Phi_7 = \{1,2,3,4,5,6\}$. Prema Maloj Fermaovoj teoremi, za svaki od njih važi $x^6 \equiv_7 1$. Da li oni tek na šestom stepenu postaju jednaki 1 ili se nekima to događa ranije? Probanjem nalazimo najmanji stepen na koji oni postaju kongruentni sa 1: $1^1 \equiv_7 1$, $2^3 \equiv_7 1$, $3^6 \equiv_7 1$, $4^3 \equiv_7 1$, $5^6 \equiv_7 1$ i $6^2 \equiv_7 1$. Najmanji stepen na koji ostatak postaje kongruentan sa 1 u velikoj meri karakteriše taj ostatak. Posebno su važni oni ostaci koji postaju kongruentni sa 1 tek kad ih na to primora Fermaova teorema, dakle kada se podignu na stepen $p-1$. To su upravo primitivni ostaci. U ovom primeru to su 3 i 5.

1.9.2. Definicija. Neka je p prost broj i $a \in Z$. Red od a po modulu p je $r(a) = min\{i \in N^+ : a^i \equiv_p 1\}$. a je primitivni ostatak po modulu p ako je $r(a) = p-1$.

Kako je u prethodnoj definiciji $a^{p-1} \equiv_p 1$, to je skup na desnoj strani definicije $r(a)$ neprazan, pa je definicija korektna.

1.9.3. Tvrđenje. *Neka je p prost broj i $a \in Z$, $i \in N^+$.*

$$a^i \equiv_p 1 \Leftrightarrow r(a)|i\,.$$

Dokaz. Neka je $r(a) = k$, dakle $a^k \equiv_p 1$.

($\Leftarrow$) Neka je $a^i \equiv_p 1$. Neka je dalje $i = qk + r$ za $0 \leq r < k$. Tada je $1 \equiv_p a^i = a^{qk+r} = (a^k)^q \cdot a^r \equiv_p a^r$. Dakle, $0 \leq r < k$ i $a^r \equiv_p 1$. Zbog minimalnosti broja k u N^+, $r \notin N^+$, dakle $r = 0$, tj. $k|m$.

($\Rightarrow$) Neka je $i = qk$ za neki $q \in Z$. Tada je $a^i = (a^k)^q \equiv_p 1$. □

Iz ovog tvrđenja i Fermaove teoreme, dobijamo,

1.9.4. Posledica. *Neka je p prost broj i $a \in Z$. $r(a)|p-1$.*

Dakle, nije slučajno što su u Primeru 1.9.1., redovi svih elemenata bili delioci broja 6.

1.9.5. Lema. *Neka je p prost broj, $a, b \in Z$, $r(a) = k$, $r(b) = l$, i $(k, l) = 1$. Tada je $r(ab) = kl$.*

Dokaz. Kako je $a^k \equiv_p 1$ i $b^l \equiv_p 1$, to je

$$(ab)^{kl} = (a^k)^l \cdot (b^l)^k \equiv_p 1.$$

Otuda $r(ab)|kl$, pa je $r(ab) = k_1 l_1$, za neke $k_1, l_1 \in N^+$ tako da $k_1|k$ i $l_1|l$. Otuda je $(ab)^{k_1 l_1} \equiv_p 1$, a kako $k_1 l_1 | k_1 l$, to je i $(ab)^{k_1 l} \equiv_p 1$. Dalje je

$$\begin{aligned} 1 &\equiv_p (ab)^{k_1 l} \\ &\equiv_p a^{k_1 l} (b^l)^{k_1} \\ &\equiv_p a^{k_1 l} \cdot 1. \end{aligned}$$

Prema Tvrđenju 1.9.3., $r(a) = k|k_1 l$. Kako je $(k, l) = 1$, to $k|k_1$. Ranije smo pokazali da $k_1|k$, pa je $k_1 = k$. Analogno se pokazuje da je $l_1 = l$, dakle $r(ab) = kl$. □

1.9.6. Tvrđenje. *Neka je p prost broj i $d|p-1$. Jednačina $x^d = 1$ ima tačno d rešenja.*

Dokaz. Označimo sa $Z(p)$ skup nula polinoma p. Prema Lagranžovoj teoremi jednačina ima najviše d rešenja. Pokazaćemo da ona ima tačno d rešenja. Neka je $p - 1 = dq$, za $q \in N^+$. Sada je, prema formuli za razliku stepena,

$$x^{p-1} - 1 = (x^d)^q - 1 = (x^d - 1)((x^d)^{q-1} + \cdots + x^d + 1)$$

Označimo polinome na desnoj strani sa $s(x)$ i $t(x)$. Kako je

$$Z(x^{p-1} - 1) = Z(s) \cup Z(t),$$

to je $|Z(x^{p-1})| \leq |Z(s)| + Z(t)|$. Prema Fermaovoj teoremi svi brojevi iz redukovanog sistema ostataka su rešenja jednačine $x^{p-1} - 1 \equiv_p 1$, dakle $|Z(x^{p-1})| = p - 1$. Otuda je $|Z(s)| + |Z(t)| = p - 1 = dq$. Kako je, prema Lagranžovoj teoremi, $|Z(t)| \leq d(q-1)$, množeći sa -1 i dodajući prethodnoj jednčini, dobijamo $|Z(s)| \geq dq - d(q-1) = d$. □

1.9.7. Lema. *Neka su p, q prosti brojevi i $k \in N^+$ tako da $q^k|(p-1)$. Postoji $q^k - q^{k-1}$ elemenata reda q^k.*

Dokaz. Prema prethodnom tvrđenju, jednačina $x^{q^k} \equiv_p 1$ ima q^k rešenja. Označimo taj skup rešenja sa A. Neka je $B = \{a \in A : r(a) = q^k\}$ i

$C = \{a \in A : r(a) < q^k\}$. Dakle, A je disjunktna unija skupova B i C. Označimo sa D skup rešenja jednačine $x^{q^{k-1}} \equiv_p 1$. Prema prethodnom tvrđenju, $|D| = q^{k-1}$. Pokazaćemo da je $D = C$. Kako je $x^{q^k} = (x^{q^{k-1}})^q$ to svaki element iz D pripada A. Iz definicione jednakosti za D vidimo da je njihov red ne veći od q^{k-1}, dakle manji od q^k. Zato je $D \subset C$. Neka je sada $c \in C$. Tada $r(c)|q^k$, pa je $r(c) = q^i$, za $i < k$. Kako je $k - 1 - i \geq 0$, i $c^{q^i} \equiv_p 1$, sada imamo

$$c^{q^{k-1}} = (c^{q^i})^{q^{k-1-i}} \equiv_p 1.$$

Dakle, $c \in D$. Kako je c proizvoljni element iz C, to je $C \subset D$, pa imamo $C = D$. Otuda je $|C| = q^{k-1}$. Sada imamo $|B| = |A| - |C| = q^k - q^{k-1}$. □

1.9.8. Teorema. *Neka je p prost broj. Postoji primitivni ostatak modulo p.*

Dokaz. Neka je $p - 1 = q_1^{\alpha_1} \dots q_s^{\alpha_s}$ prosta faktorizacija broja $p - 1$. Neka je, za $i \leq k$, a_i ostatak takav da je $r(a_i) = q_i^{\alpha_i}$. Takvi ostaci postoje prema prethodnoj lemi. Neka je $a = a_1 \cdot a_2 \cdot \dots \cdot a_k$. Kako su redovi elemenata a_i, $i \leq k$, uzajamno prosti, prema Lemi 1.9.5.,

$$r(a) = q_1^{\alpha_1} \cdot \dots \cdot q_k^{\alpha_k} = p - 1.$$

Dakle, a je primitivni ostatak. □

U prethodnoj teoremi mogli smo dokazati da postoji tačno $\varphi(p-1)$ primitivnih ostataka ali taj rezultat dobijamo u Glavi 3, kao usputnu posledicu.

1.9.9. Posledica. *Neka je p prost broj i a primitivni ostatak modulo p.* $Z_p \setminus \{0\} = \{rem_p(a^i) : 0 \leq i \leq p - 2\}$.

Dokaz. Pretpostavimo da je za $0 \leq i < j \leq p - 2$, $a^i \not\equiv_p a^j$. Kako je $(a^i, p) = 1$, skraćivanjem sa a^i, dobijamo $a^{j-i} \equiv_p 1$. Kako je $0 < j - i < p - 1$, to je kontradikcija sa $r(a) = p - 1$. Dakle, svi elementi navedenog skupa su nekongruentni i uzjamno prosti sa p pa čine redukovani sistem ostataka. Zato je skup njihovih ostataka $Z_p \setminus \{0\}$.

1.9.10. Primer. Kako je u Z_7, broj 3 primitivni ostatak, to imamo da je $Z_7 = \{1, 3^1, 3^2, 3^3, 3^4, 3^5\} \equiv_7 \{1, 3, 2, 6, 4, 5\}$. To nam omogućuje da u Z_7 definišemo logaritmovanje za osnovu 3, tako da je $log_3 i = j$ akko $3^j \equiv_7 3$. Tako dobijamo $log_3 2 = 2$ jer je $3^2 \equiv_7 2$. To možemo primeniti i za svođenje proizvoda na zbir. Naime, $log_3 5 = 5$ i $log_3 6 = 3$, pa je

$$log_3(5 \cdot 6) = 5 +_6 3 = 2.$$

Otuda je $5 \cdot 6 \equiv_7 3^2 = 2$.

1.10. Linearne jednačine u Z_n

1.10.1. Definicija. Neka su $a, b \in N$, $m \in N_2$. Jednačina $ax \equiv_m b$ naziva se linearnom jednačinom modulo m.

1.10.2. Tvrđenje. *Neka su $a, b \in N$, $(a, m) = 1$. Jednačina $ax \equiv_m b$ ima jedinstveno rešenje.*

Dokaz. Kako je $(a, m) = 1$, postoje $u, v \in Z$ tako da je $1 = au + mv$. Množenjem jednakosti sa b dobijamo, $b = abu + mbv$. Odavde je $abu = \equiv equiv_m b$, dakle bu zadovoljava jednačinu iz formulacije tvrđenja. Pokažimo jedinstvenost: Neka su s, t rešenja jednačine. Tada je $as \equiv_m b$ i $at \equiv_m b$. Otuda je $as \equiv_m at$. Skraćivanjem sa a dobijamo $s \equiv_m t$. Kako su s i t iz nekog PSO_m, to je $s = t$. □

Prethodno tvrđenje može se dokazati neposredno pozivanjem na Tvrđenje 1.7.7.

1.10.3. Primer. Jednačina $3x \equiv_{10} 4$ ima jedinstveno rešenje $x = 8$. Našli smo ga probanjem brojeva iz skupa $\{0, 1, \ldots, 9\}$. Da bi se spremili za glavnu teoremu treba da rešimo problem privikavanja na promenu modula. Primetimo da je, na osnovu Tvrđenja 1.6.8.(ii), za svaki ceo broj x,

$$2x \equiv_4 0 \Leftrightarrow x \equiv_2 0.$$

Iako su to ekvivalentne jednačine, prva ima dva rešenja, 0 i 2, a druga samo jedno 0. Kako je to moguće? Stvar je u našoj definiciji rešenja. Za prvu jednačinu rešenja tražimo iz PSO_4, $\{0, 1, 2, 3\}$, a za drugi iz PSO_2, 0,1. Ako pogledamo klase ekvivalencije, tu su se klase 0 i 2, po modulu 4, stopile u klasu 0, po modulu 2.

1.10.4. Teorema. *Neka su $a, b \in N$, $(a, m) = d$. Jednačina $ax \equiv_m b$ ima rešenja akko $d|b$. Tada ona ima tačno d rešenja.*

Dokaz. Neka je s proizvoljno rešenje ove jednačine u Z_m. Tada je $as \equiv_m b$ tj. $m|as - b$. Kako $d|m$ i $d|as$, to $d|b$. Time smo pokazali neophodnost uslova $d|b$ za postojanje rešenja jednačine.

Pretpostavimo sada da $d|b$. Neka je $a = a_1 d$, $b = b_1 d$, $m = m_1 d$ i $(a_1, m_1) = 1$. Tada, prema Tvrđenju 1.6.8.(ii), imamo da je za svaki $x \in Z$,

$$ax \equiv_m b \Leftrightarrow a_1 x \equiv_{m_1} b_1. \tag{1}$$

Prema prethodnom tvrđenju jednačina na desnoj strani ima rešenje, jedinstveno u Z_{m_1}. Neka je to c. Pokazćemo da je $R = \{c + im_1 : 0 \leq i < d\}$

skup svih rešenja polazne jednačine. Kako svi elementi skupa R zadovoljavaju desnu jednačinu u (1), oni zadovoljavaju i levu jednačinu, dakle, jesu njena rešenja. Pokažimo da su svi u Z_m, a time nekongruentni. Zaista, kako je $0 \leq c < m_1$, to je, za $0 \leq i < d$,

$$0 \leq c + im_1 < m_1 + (d-1)m_1 = dm_1 = m.$$

Ostaje da pokažemo da drugih rešenja nema u Z_m. Međutim, ako je s rešenje jednačine, prema (1), mora biti $s \equiv_{m_1} c$. Otuda je $s = c + im_1$. Kako je po pretpostavci $0 \leq s < m$, to je $0 \leq i < d$, dakle $s \in R$. Time smo pokazali da je R skup rešenja polazne jednačine. □

1.10.5. Primer. Rešavamo jednačinu $9x \equiv_{15} 12$.

Korak 1. (9,15)=3. 3|12, dakle jednačina ima 3 rešenja.

Korak 2. Kratimo sa 3. Dobijamo jednačinu

$$3x \equiv_5 4.$$

Korak 3. Rešavamo jednačinu probanjem, na osnovu Bezuove teoreme ili neki drugi način. Dobijamo jedinstveno rešenje $c = 3$.

Korak 4.Rešenja su: 3,3+5,3+10 tj. 3,8 i 13.

1.10.6. Primer. U rešavanju linearnih kongruencija možemo primeniti rezultate iz 1.3. Rešavamo jednačinu $ax \equiv_m b$, $(a, m) = 1$. Bez gubljenja opštosti pretpostavimo $a, b \in N$. Neka je $\frac{m}{a} = s(q_0, q_1, \ldots, q_n)$. Kako je $\frac{A_n}{B_n} = \frac{a}{m}$, i oba razlomka su skraćena, to jednakost (5) možemo pisati u obliku

$$mB_{n-1} - aA_{n-1} = (-1)^{n-1}.$$

Otuda je

$$aA_{n-1} \equiv_m (-1)^n.$$

Otuda je $x = (-1)^n A_{n-1} b$ rešenje kongruencije. Pokažimo to na primeru jednačine $30 \equiv_{43} 7$. Pomoću Euklidovog algoritma, dobijamo da je $\frac{43}{30} = s(1, 2, 3, 4)$. Otuda su konveregenti $1, \frac{3}{2}, \frac{10}{7}$ i $\frac{43}{30}$. Kako je $n = 3$, i $A_2 = 10$, to je rešenje $x = -70 \equiv_{43} 16$.

1.11. Kineska teorema o ostacima

1.11.1. Teorema. *Neka je $\{m_1, \ldots, m_k\}$ skup dva po dva uzajamno prostih brojeva. Sistem jednačina*

$$x \equiv_{m_1} a_1$$

$$\vdots$$

$$x \equiv_{m_k} a_k,$$

ima jedinstveno rešenje po modulu $M = \prod_{i \leq k} m_i$.

Dokaz. Neka je za $i \leq k$, $M_i = \frac{M}{m_i}$, dakle proizvod svih modula osim i-tog. Neka je M_i' rešenje jednačine $M_i x \equiv_{m_i} 1$. Kako je, prema Tvrđenju 1.2.9.(iii), $(M_i, m_i) = 1$, takvo rešenje postoji. Tada je

$$x_0 = M_1 M_1' a_1 + \cdots + M_k M_k' a_k$$

rešenje datog sistema jednačina. Zaista, neka je $i \leq k$.

$$x_0 = \sum_{j \leq m, j \neq i} M_j M_j' a_j + M_i M_i' a_i.$$

U sumi u svakom od sabiraka M_j sadrži m_i, jer je u njemu ispušten m_j, pa je čitava suma deljiva sa m_i. Dakle, $x_0 \equiv_{m_i} M_i M_i' a_i$. Kako je $M_i M_i' \equiv_{m_i} 1$, to je $x_0 \equiv_{m_i} a_i$. Kako je i proizvoljno, x_0 je rešenje sistema.

Ostaje da pokažemo jedinstvenost modulo M. Neka je x_1 drugo rešenje sistema. Tada je $x_0 \equiv_{m_i} x_1$, za $i \leq k$. Otuda $m_i | x_1 - x_0$, za $i \leq k$. Kako su m_i, $i \leq k$, dva po dva uzajamno prosti, to prema Tvrđenju 1.2.9.(iv), $M = \prod_{i \leq k} m_i | x_1 - x_0$. Dakle, $x_1 \equiv_M x_0$. □

1.11.2. Primer. Završimo rešavanje jednačine iz Primera 1.8.6. Stali smo kod nalaženja brojeva koji zadovoljavaju $x \equiv_5 1 \vee x \equiv_5 4$ i $x \equiv_7 3 \vee x \equiv_7 5 \vee x \equiv_5 6$. Dobijamo šest sistema jednačina. Rešimo jedan od njih.

$$x \equiv_5 4$$
$$x \equiv_7 3$$

Sada imamo $M = 35$, $M_1 = 7$, $M_2 = 5$, $M_1' = 3$, $M_2' = 3$, pa je

$$x_0 = 7 \cdot 3 \cdot 4 + 5 \cdot 3 \cdot 3 = 129 \equiv_{35} 24.$$

1.12. Kvadratni ostaci po prostom modulu

1.12.1. Definicija. Neka je $p > 2$ prost broj. $a \in Z_p \setminus \{0\}$ je kvadratni ostatak po modulu p, ako jednačina

$$x^2 \equiv_p a$$

ima rešenja.

1.12.2. Primer. Koji su kvadratni ostaci modulo 11? Kako je $S_{11} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$potpuni sistem ostataka iz koga je odstranjena 0, to su kvadrati ovih brojeva kvadratni ostaci modulo 11. Dakle, to su $1^2, 2^2, 3^2, 4^2, 5^2$ odnosno $1, 4, 9, 5, 3$. Primećujemo da su od 10 brojeva iz RSO_{11}, tačno polovina njih kvadrati.

1.12.3. Tvrđenje. *Postoji* $\frac{p-1}{2}$ *kvdrata i* $\frac{p-1}{2}$ *nekvadrata.*

Dokaz. Neka je za $1 \leq i \leq \frac{p-1}{2}$, $b_i = rem_p(\pm i)^2$. $\{b_i : 1 \leq i \leq \frac{p-1}{2}\}$ je skup međusobno nekongruentih kvadrata. Zaista, ako bi imali za $i \neq j$, $b_i \equiv_p b_j$, tada bi jednačina $x^2 = b_i$ imala četiri rešenja, naime $\pm i, \pm j$. Kako su svi brojevi iz $Z \setminus \{0\}$ iscrpljeni, za preostalih $\frac{p-1}{2}$ brojeva nema rešenja odgovarajućih kvadratnih jednačina, dakle oni nisu kvadrati. □

1.12.4. Definicija. Za $a \in Z_p \setminus \{0\}$, Ležandrov simbol definiše se tako da

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ako je } a \text{ kvadrat modulo } p \\ -1, & \text{ako } a \text{ nije kvadrat modulo } p. \end{cases}$$

1.12.5. Tvrđenje. *Neka je* $a \in Z_p \setminus \{0\}$.

$$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}.$$

Dokaz. Neka je $a \in Z_p \setminus \{0\}$, i neka je $b = a^{\frac{p-1}{2}}$. Prema Maloj Fermaovoj teoremi, $b^2 \equiv_p a^{p-1} \equiv_p 1$. Kako jednačina $x^2 \equiv_p 1$ ima tačno dva rešenja, naime ± 1, to je $b \equiv_p \pm 1$. Dakle, za svaki $a \in Z_p \setminus \{0\}$, imamo $a^{\frac{p-1}{2}} \equiv_p \pm 1$. Pretpostavimo sada da je a kvadrat, dakle $\left(\frac{a}{p}\right) = 1$. Tada postoji $s \in Z_p \setminus \{0\}$, tako da je $a \equiv_p s^2$. Otuda je,

$$a^{\frac{p-1}{2}} \equiv_p (s^2)^{\frac{p-1}{2}} = s^{p-1} \equiv_p 1.$$

Poslednja jednakost sledi iz Male Fermaove teoreme. Dakle, $\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}$. Usput primetimo da $\frac{p-1}{2}$ kvadrata zadovoljava jednačinu $x^{\frac{p-1}{2}} \equiv_p 1$. Prema Lagranžovoj teoremi ova jednačina drugih rešenja nema. Dakle, ako a nije kvadrat $a^{\frac{p-1}{2}} \neq 1$. Kako $a^{\frac{p-1}{2}} \equiv_p \pm 1$, dobijamo da ako a nije kvadrat, tada je $a^{\frac{p-1}{2}} \equiv_p -1 = \left(\frac{a}{p}\right)$. □

1.12.6. Posledica. *-1 je kvadrat po modulu p akko je p oblika $4k+1$.*

Dokaz. Na osnovu prethodnog tvrđenja, -1 je kvadrat akko $(-1)^{\frac{p-1}{2}} \equiv_p 1$. To je slučaj akko je broj $\frac{p-1}{2}$ paran, tj p oblika $4k+1$. □

1.12.7. Posledica. *Postoji beskonačno mnogo prostih brojeva oblika $4k+1$.*

Dokaz. Pretpostavimo suprotno, da ih ima konačno mnogo. Neka je $P = \{p_1, \ldots, p_n\}$ lista svih prostih brojeva oblika $4k+1$. Neka je

$$M = 4p_1^2 \cdot \ldots \cdot p_n^2 + 1.$$

Prema Tvrđenju 1.4.1, M sadrži prost faktor. Neka je q jedan od njih. Kako je M neparan, $q \neq 2$. Pokazaćemo da je q oblika $4k+1$. Pretpostavimo suprotno da je q oblika $4k+3$. Tada iz $q|M$ dobijamo

$$4p_1^2 \cdot \ldots \cdot p_n^2 \equiv_p -1.$$

Otuda je

$$(2p_1 \cdot \ldots \cdot p_n)^2 \equiv_p -1.$$

Dakle, -1 je kvadrat modulo q. Kako je q oblika $4k+3$, to je u kontradikciji sa prethodnom posledicom. Iz dobijene kontradikcije zaključujemo da je q oblika $4k+1$. Kraj je standardan. Imamo $q \in P$, dakle $q = p_i$, za neko $i \leq n$. Otuda $q|M - 1 = 4p_1^2 \cdot \ldots \cdot p_n^2$. Kako $q|M$, to $q|M - (M-1) = 1$. Kontradikcija. □

1.12.8. Posledica. *Neka je $a, b \in Z_p \setminus \{0\}$.*

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Dokaz. Tvrđenje sledi neposredno iz Tvrđenja 1.12.5., i relacije $a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}}$. □

1.12.9. Tvrđenje (Gausova lema). *Neka je $p > 2$ prost broj i $s = \frac{p-1}{2}$. Neka je za $1 \leq i \leq s$, $s \cdot i \equiv_p b_i$, gde $b_i \in \{\pm 1, \pm 2, \ldots, \pm s\}$ redukovanom sistemu ostataka najamanjih po apsolutnoj vrednosti. Ako je ν broj negativnih elemenata skupa $\{b_1, \ldots, b_s\}$, onda je*

$$\left(\frac{a}{p}\right) = (-1)^{\nu}.$$

Dokaz. Pokazaćemo najpre da je $\{|b_1|, \ldots, |b_s|\} = \{1, \ldots, s\}$. Neka je $1 \leq i \leq s$. Kako $b_i \in \{\pm 1, \ldots, \pm s\}$, to $|b_i| \in \{1, \ldots, s\}$. Dakle,

$$\{|b_1|, \ldots, |b_s|\} \subset \{1, \ldots, s\}.$$

Pokažimo da je za $1 \leq i \neq j \leq s$, $|b_i| \neq |b_j|$. Pretpostavimo suprotno da je $|b_i| = |b_j|$, za $1 \leq i < j \leq s$. Otuda je $b_i = \pm b_j$. Po definiciji b_i, odavde dobijamo $a \cdot i \equiv_p \pm a \cdot j$. Kako je $(a, p) = 1$, skraćivanjem kongruencije dobijamo $i \equiv_p \pm j$. Odatle $p|j - i$ ili $p|i + j$. Kako je $1 \leq i < j \leq s$, to je $2 \leq i + j \leq 2s = p - 1$, i $0 < i - j < s < p$. Otuda nijedan od tih brojeva nije deljiv sa p. Kontradikcija. Dakle $\{|b_1|, \ldots, |b_s|\}$ je skup od s različitih brojeva. Kako i njegov nadskup $\{1, \ldots, s\}$ ima s elemenata, oni su jednaki.

Odavde imamo da je $\prod_{i \leq s} |b_i| = \prod_{i \leq s} i$. Sada je

$$\begin{aligned} a^s \cdot \prod_{i \leq s} i &= \prod_{i \leq s} ai \\ &\equiv_p \prod_{i \leq s} b_i \\ &\equiv_p \prod_{i \leq s} sgn(b_i)|b_i| \\ &= \prod_{i \leq s} sgn(b_i) \cdot \prod_{i \leq s} |b_i| \\ &= (-1)^\nu \prod_{i \leq s} i. \end{aligned}$$

Skraćivanjem $\prod_{i \leq s} i$, na levoj i desnoj strani jednakosti, dobijamo $a^s \equiv_p (-1)^\nu$. Kako je $s = \frac{p-1}{2}$, dobijamo, prema Tvrdenju 1.12.5., $\left(\frac{a}{p}\right) = (-1)^\nu$. □

1.12.10. Primer. Odredimo za koje proste brojeve p je 2 kvadrat modulo p. Neka je $s = \frac{p-1}{2}$. Sada svodimo skup $\{2 \cdot 1, 2 \cdot 2, \ldots, 2 \cdot s\}$ na sistem najmanjih po apsolutnoj vrednosti. Ako je $2i < \frac{p}{2}$ onda je $b_i = 2i > 0$, a ako je $2i > \frac{p}{2}$, onda je $b_i = 2i - p < 0$. Sada treba da izbrojimo koliko ima i-ova takvih da je $b_i < 0$, tj. da je $2i > \frac{p}{2}$. Razlikovaćemo dva slučaja.

p = 4k + 1. Sada je $s = 2k$. Kako je prvi ceo broj manji od $\frac{p}{2}$ jednak $2k$, to je $2i > \frac{p}{2}$ ekvivalentno sa $2i > 2k$. Zato je

$$\begin{aligned} \nu &= |\{i : 1 \leq i \leq s, 2k < 2i\}| \\ &= |\{i : 2k < 2i \leq 2s\}| \\ &= |\{i : k < i \leq s\}| \\ &= |\{i : k < i \leq 2k\}| \\ &= k. \end{aligned}$$

Dakle, 2 je kvadrat modulo p akko je k paran broj, tj. oblika $2l$. Tada je $p = 8l + 1$.

p = 4k + 3. Sada je $s = 2k + 1$. Kako je prvi ceo broj manji od $\frac{p}{2}$ jednak $2k + 1$, to je $2i > \frac{p}{2}$ ekvivalentno sa $2i > 2k + 1$. Zato je

$$\begin{aligned}\nu &= |\{i : 1 \leq i \leq s, 2k + 1 < 2i\}| \\ &= |\{i : 2k + 1 < 2i \leq 2s\}| \\ &= |\{i : 2k + 2 \leq 2i \leq 2s\}| \\ &= |\{i : k + 1 \leq i \leq s\}| \\ &= |\{i : k < i \leq 2k + 1\}| \\ &= k + 1.\end{aligned}$$

Dakle, 2 je kvadrat modulo p akko je k neparan broj, tj. oblika $2l + 1$. Tada je $p = 4(2l + 1) + 3 = 8l + 7$.

Konačan odgovor je da je 2 kvadrat modulo p akko je $p = 8k \pm 1$.

1.13. Diofantske jednačine

1.13.1. Definicija. Neka je $p(x_1, \ldots, x_n) \in Z[x]$. Jednačina

$$p(x_1, \ldots, x_n) = 0,$$

je Diofantska jednačina. Rešenje ove Diofantske jednačine je n-torka $(a_1, \ldots, a_n) \in Z^n$, koja zadovoljava jednačinu.

Jedan od najvećih problema matematike 20. veka bio je 10. Hilbertov problem: Da li postoji algoritam kojim se za svaku Diofantsku jednačinu može odrediti da li ima rešenja. Na problem je 1970. negativan odgovor dao Matijaševič. U terminima Teorije rekurzija, ovaj problem je rekurzivno nabrojiv ali nije rekurzivan. Mi se u nastavku interesujemo za neke jednostavne primere Diofantskih jednačina.

Linearna Diofantska jednačina.

1.13.2. Definicija. Neka su $a, b, c \in Z$. Jednačina $ax + by = c$ je linearna Diofantska jednačina.

1.13.3. Tvrđenje. *Neka je $a, b, c \in Z$, $(a, b) = 1$. Linearna Diofantska jednačina $ax + by = c$ ima rešenja. Ako je (x_0, y_0) jedno rešenje jednačine, onda su sva rešenja oblika*

$$(x_0 + bt, y_0 - at).$$

Dokaz. Prema Bezu-ovoj teoremi postoje $u, v \in Z$, tako da je $1 = au + bv$. Množenjem sa c dobijamo $c = a(uc) + b(vc)$. Dakle, $(x_0, y_0) = (uc, vc)$ je rešenje jednačine.

Opisaćemo sva rešenja ove jednačine. Neka je (x_1, y_1) rešenje jednačine. Tada imamo

$$ax_1 + by_1 = c = ax_0 + by_0, \text{ dakle,}$$
$$a(x_1 - x_0) = b(y_1 - y_0). \tag{1}$$

Kako je $(a, b) = 1$, to $b|x_1 - x_0$. Zato postoji $t \in Z$, tako da je $x_1 - x_0 = bt$. Zamenom u (1) dobijamo $y_1 - y_0 = at$. Dakle, sva rešenja su traženog oblika. Zamenom (x_1, y_1) u jednačini, i uzimanjem u obzir da je (x_0, y_0) rešenje jednačine, proveravamo da su svi parovi tog oblika rešenja jednačine.

1.13.4. Teorema. *Neka su $a, b, c \in Z$ i $(a, b) = d$. Jednačina $ax + by = c$ ima rešenja akko $d|c$. Ako $d|c$ jednačina je ekvivalentna jednačini $a_1x + b_1y = c_1$, gde je $a_1 = \frac{a}{d}, b_1 = \frac{b}{d}$, $c_1 = \frac{c}{d}$, kod koje je $(a_1, b_1) = 1$.*

Dokaz. ($\Rightarrow$) Neka je (k, l) rešenje jednačine. Dakle, $ak + bl = c$. Kako $d|ak, bl$, to $d|c$.

($\Leftarrow$). Neka su oznake kao u formulaciji teoreme. Kako je $d \neq 0$,

$$ax + by = c \Leftrightarrow da_1x + db_1y = dc_1$$
$$\Leftrightarrow a_1x + b_1y = c_1$$

Poslednja jednačina se rešava po proceduri iz prethodnog tvrdenja. □

Pitagorine trojke. Razmatramo Diofantsku jednačinu $x^2 + y^2 = z^2$. Kako su pozitivna rešenja ove jednačine merni brojevi stranica pravouglog trougla, ta rešenja nazivamo Pitagorinim trojkama. Mi se ograničavamo na rešenja oblika (a, b, c), gde $a, b, c \in N^+$ jer su onda automatski rešenja i sve trojke oblika $(\pm a, \pm b, \pm c)$. Rešenje (a, b, c) je primitivna Pitagorina trojka ako je $(a, b, c) = 1$.

1.13.5. Teorema. *Skup svih Pitagorinih trojki je*

$$P = \{2kld, d(l^2 - k^2), d(l^2 + k^2) : k, l, d \in N^+, k < l\}.$$

Dokaz. Jednostavnom zamenom proveravamo da su svi elementi skupa P Pitagorine trojke. Pokažimo sada da drugih Pitagorinih trojki nema. Pokažimo najpre da sve primitivne Pitagorine trojke pripadaju skupu P.

Dakle, neka je (a, b, c) primitivna Pitagorina trojka. Tada je

$$a^2 + b^2 = c^2.$$

Neka je $(a,b)=d$. Kako $d|a,b$, to $d^2|c^2$, pa $d|c$. Kako je $(a,b,c)=1$, to je $d=1$. Dakle, $(a,b)=1$. Slično zaključujemo i da je $(b,c)=1$ i $(a,c)=1$. Otuda odmah imamo da a,b ne mogu biti oba parni brojevi. a i b ne mogu biti ni oba neparni brojevi. Zaista, ako je $a=2k+1$ i $b=2l+1$, tada je $c^2=a^2+b^2=4(k^2+l^2+k+l)+2$. Dakle, $c^2\equiv_4 2$. Međutim kvadrati neparnih brojeva daju ostatak 1 po modulu 4, a kvadrati parnih ostatak 0. Kontradikcija. Dakle, jedan od brojeva a,b je paran a drugi neparan. Bez gubljenja opštosti neka je a paran i b neparan broj. Tada imamo da je c neparan broj. Neka je $a=2m$, za neki $m\in N$. Tada je

$$4m^2=(c-b)(c+b).$$

Kako su b i c neparni brojevi $c-b$ i $c+b$ su parni brojevi, dakle postoje $u,v\in N$ tako da je $c-b=2u$ i $c+b=2v$. Neka je $(u,v)=d$. Kako je $c=u+v$ i $b=v-u$, to $d|b,c$. Kako je $(b,c)=1$, to je $d=1$. Dakle, u i v su uzajamno prosti. Zamenom u jednačini dobijamo

$$4m^2=4uv \text{ tj. } m^2=uv.$$

Kako je $(u,v)=1$ i njihov proizvod je kvadrat, prema Posledici 1.4.8., u i v su kvadrati. Dakle, postoje k i l tako da $u=k^2$ i $v=l^2$. Sada imamo

$$m^2=k^2\cdot l^2,$$

dakle, $m=kl$. Otuda je $a=2m=kl$, $b=v-u=l^2-k^2$ i $c=v+u=l^2+k^2$. Time smo pokazali da $(a,b,c)\in P$. Neka je sada (a,b,c) proizvoljna Pitagorina trojka, i neka je njihov najveći zajednički delilac $(a,b,c)=d$. Tada je

$$\left(\frac{a}{d}\right)^2+\left(\frac{b}{d}\right)^2=\left(\frac{c}{d}\right)^2.$$

Kako su $a_1=\frac{a}{d}$, $b_1=\frac{b}{d}$ i $c_1=\frac{c}{d}$ uzajamno prosti, (a_1,b_1,c_1) je primitivna Pitagorina trojka, pa postoje $k,l\in N$ tako da je $a_1=2kl$, $b_1=l^2-k^2$ i $c_1=l^2+k^2$. Otuda je $a=2dkl$, $b=d(l^2-k^2)$ i $c=d(l^2+k^2)$. Dakle, $(a,b,c)\in P$. □

$x^3=y^2+2$. Ova jednačina ima rešenje $(3,5)$. Da li ima drugih rešenja? Na to pitanje odgovorićemo u trećoj glavi.

1.14. Otvoreni problemi

1. *Fermaov problem* Na margini svoje kopije Diofantove knjige *Aritmetika*, pored jednačine $x^2+y^2 = z^2$, pravnik Pjer Ferma napisao je:"Međutim, nemoguće je napisati kub kao zbir dva kuba, četvrti stepen kao zbri dva četvrta stepena, i uopšte ma koji stepen veći od drugog kao zbir sličnih stepena. Za to sam otkrio zaista sjajan dokaz, ali je margina premala da on stane." To je Velika (Poslednja) Fermaova teorema. Dakle, ne postoje $x, y, z \in N^+$ i $n > 2$ tako da je

$$x^n + y^n = z^n.$$

U zaostavštini ovog matematičara nije naden dokaz ove teoreme. Matematičari su sledećih 300 godina pokušavali da nadu dokaz. U neuspešnim pokušajima nalaženja dokaza došlo je do mnogih važnih otkrića u matematici. Jedan od najpoznatijih je pojam ideala. Nemački matematičar Kumer (1810-1893) je verovao da je našao dokaz Fermaove teoreme. Dirišle mu je skrenuo pažnju na grešku u dokazu. Nastojeći da popravi dokaz Kumer je došao do pojma ideala.

Problem je konačno rešio Engleski matematičar Howie, 1992. godine. Dokaz je izveden metodima algebarske geometrije i toliko je komplikovan da "ne bi stao na marginu knjige čak i da je bila milju dugačka".

2. *Goldbahova hipoteza.* To je hipoteza koju je 1742. godine Goldbah formulisao u pismu Ojleru 1742. godine:

Goldbahova hipoteza. *Svaki paran broj ≥ 6 je zbir dva prosta broja.*

Bilo koji paran broj za koji je hipoteza proveravana je zadovoljava. Na primer,

$$6 = 3 + 3,\ 8 = 5 + 3,\ 10 = 7 + 3,\ 12 = 7 + 5\ \ldots.$$

Problem je još uvek otvoren. Značajan progres prema rešenju problema učinio je Vinogradov 1937. godine. On je pokazao da je svaki neparan broj, od nekog dovoljno velikog broja nadalje, zbir tri prosta broja. Kako je za svaki takav neparn broj $n - 3$, paran, to je svaki dovoljno veliki paran broj zbir četiri prosta broja.

Rénjai je takođe dao doprinos rešavanju ovog problema pokazajući je svaki dovoljno veliki paran broj predstavljiv u obliku zbira dva broja, od kojih je jedan prost a drugi ima uniformno ograničen broj prostih faktora.

3. *Mersenovi brojevi.*

1.14.1. Definicija. Neka je p prost broj. Ako je broj $n = 2^p - 1$ prost, onda je n Mersenov broj.

Otvoreno je pitanje da li postoji beskonačno mnogo Mersenovih brojeva. Prirodno je što je u izrazu $2^k - 1$, k ograničen na proste brojeve. Ako je

$k = st$, onda je za $m = 2^s$,

$$2^{st} - 1 = m^t - 1 = (m-1)(m^{t-1} + \cdots + m + 1),$$

dakle, složen broj.

Dugo se mislilo da ako je $p$prost broj, onda su svi brojevi oblika $2^p - 1$ prosti. Hudalricus Regius je 1536. godine pokazao da broj $2^{11} - 1 = 2047 = 23 \cdot 89$ nije prost. Marin Mersenne (1588-1648) je u predgovoru svoje knjige *Cogitata Physica-Mathematica* napisao da su brojevi oblika $2^p - 1$ prosti za

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127i257,$$

a da su složeni za sve druge brojeve $p < 257$.

Do sada je nađeno 37 Mersenovih brojva. Neka je M_k, k-ti Mersenov broj. Danas se Mersenovi brojevi nalaze uz pomoć računara. Mersenov broj M_35 otkriven je 1996., (Armegaund, Waltman, ...) za $p = 1398269$ i ima 420921 cifru. Utvrđeno je i da se za $p = 2976221$ i $p = 3021377$ dobijaju Mersenovi brojevi, ali se ne zna koji su po redu. Poslednji Mersenovi brojevi otkriveni su ne na super-računarima kao njihovi prethodnici, već u okviru projekta koji vodi George Waltman, na kome radi veliki broj PC-ja povezanih paralelno. Danas se testiranje velikih Meresenovih brojeva preporučuje i kao test za kvalitet računara.

Na kraju pitamo s zašto je to uopšte problem, kada imamo algoritam (Eratostenovo sito) za ispitivanje da li je broj prost. Problem je u tome što je taj algoritam eksponencijalni, a ne polinomski. Dakle, kada broj raste potrebno je enormno mnogo vremena za izvođenje ovog testa. Na primer, za ispitivanje Eratostenovim metodom da li je broj sa 50 cifara prost, potrebno je 10^{11} godina rada računara koji izvodi 10^6 operacija u sekundi.

Zato su iznalaženi brži algoritmi za ovu namenu. Jedna od mogućnosti je da se iskoristi obrat Male Fermaove teoreme. Dakle, kazaćemo da je za $2 \leq a < n$, broj n pseudo-prost za bazu a ako je $a^{n-1} \equiv_n 1$. Po Maloj Fermaovoj teoremi, svaki prost broj je pseudo-prost za sve pomenute baze. Da li važi obrat. To bi omogućilo veliko ubrzanje jer se račun izvodi samo po modulu n. Odgovor je ne. Postoje brojevi (Karmichael-ovi brojevi) koji su pseudo-prosti za sve baze a nisu prosti, na primer 561, 1729, ... Oni su međutim dosta retki. Izračunato je (Bohman) da postoji 882.206.716 prostih brojeva manjih od $20 \cdot 10^9$, dok je u istom intervalu 19865 pseudoprostih za bazu 2. Dakle, ako za takav broj pretpostavite da je prost pogrešićete sa verovatnoćom oko 10^{-6}. Varijacija ovog pokušaja je Lucas-ov test iz 1876. godine.

Lukasov test. *Ako je* $a^{n-1} \equiv_n 1$ *i* $b^{\frac{n-1}{p}} \not\equiv_n 1$, *za neki prost faktor* p *broja* $n-1$, n *je prost broj.*

Poboljšanje iste ideje dali su Adleman i Rumely, 1980. godine. Evo poređenja brzine tih testova na računaru koji izvodi 10^6 operacija u sekundi.

	20 cif	50 cif	100 cif	200 cif	1000 cif
Eratosten	2h	10^{11}god.	10^{36}god.	10^{86}god.	10^{486}god.
Lucas	5"	10h	100 god.	10^9god.	10^{44}god.
Adleman	10"	15"	40"	10'	1 nedelja

Brzina testiranja povećava se i ubrzanjem računara ali ni blizu tako rapidno, za nekoliko decimalnih mesta.

Naravno da i pitanje brze faktorizacije broja postaje otvoreno. Taj proces je još sporiji od ispitivanja primalnosti. Pomenimo i praktičnu primenu ovih rezultata u teoriji kriptosistema, zaštite prenosa podataka. Pitanje je kako preneti poruku tako da neovlašćena lica ne mogu da joj pristupe. Ideja je sledeća.

Kako se svaki niz reči može shvatiti kao niz brojeva, reči se mogu kodirati prirodnim brojevima (Posledica 1.4.6.). Dakle, dobijamo broj M kao kod naše poruke. Taj broj M mogu da faktorišu i osoba kojoj šaljemo poruku, kao i neovlašćena osoba. Zato M množimo sa velikim brojem K koji zna osoba kojoj šaljemo poruku, koji smo joj poslali sigurnom poštom, i koji je dogovorena konstanta za neki period. K se bira i tako da je proizvod MK veći od granica mogućnosti faktorizacije za savremene računare. Zato neovlašćena osoba, iako zna metod kodiranja, ne može naći poruku M. Osoba kojoj se poruka šalje dobijeni broj podeli konstantom K, a onda dobijeni broj, koji je u granicama moguće faktorizacije, faktoriše i vrši proces dekodiranja.

4. Savršeni brojevi.

1.14. Definicija. Prirodan broj n je savršen akko je $\sigma(n) = 2n$.

Kako je $\sigma(n)$ definisan kao zbir svih prirodnih delilaca broja n, a najveći među njima je sam n, to je n savršen broj akko je jednak zbiru svih svojih delilaca manjih od njega.

1.14. Primer. Kako je

$$6 = 1 + 2 + 3, \quad 28 = 1 + 2 + 4 + 7 + 14,$$

to su 6 i 28 savršeni brojevi.

1.14. Tvrđenje. *Neka je $2^p - 1$ Mersenov broj. Tada je $2^{p-1}(2^p - 1)$ savršen broj.*

Dokaz. Neka je $q = 2^p - 1$ i $n = 2^{p-1}(2^p - 1) = 2^{p-1} \cdot q$. Kako je q neparan broj, $(2^{p-1}, q) = 1$. Kako je σ multiplikativna funkcija, prema Tvrđenju 1.4.14., imamo da je

$$\begin{aligned}\sigma(n) &= \sigma(q) \cdot \sigma(2^{p-1}) \\ &= (q+1) \cdot (2^p - 1) \\ &= 2^p \cdot q \\ &= 2 \cdot 2^{p-1} \cdot q \\ &= 2n. \quad \square\end{aligned}$$

Iz Tvrđenja se vidi da su to brojevi koji u binarnom zapisu imaju p jedinica i $p - 1$ nulu.

Dokazano je da su svi parni savršeni brojevi ovog oblika. Dakle, poznato je onoliko savršenih brojeva koliko i Mersenovih. Pitanje da li postoji neparan savršen broj je još uvek otvoreno. Pokazano je da ako takav broj postoji on je oblika $k^2 \cdot p$, gde je p prost broj, ima bar 29 prostih faktora od kojih je bar 8 različito, ima barem 300 cifara, i ima prost faktor veći od 1020.

GLAVA II

POLINOMI

2.1. Definicija i prve osobine

Neka je $\{\mathrm{r} : r \in R\}$ skup simbola konstanti indeksiranih skupom realnih brojeva. Polinomi su termi jezika $\{\mathrm{r} : r \in R\} \cup \{+, \cdot\}$ sa samo jednom promenljivom. Ipak polinomi se uglavnom definišu u svom kanoničnom obliku. Najpre definišimo $N_1 = N \cup \{-\infty\}$, gde je $-\infty$ novi objekat. Uredenje na N_1 definišemo kao ekstenziju uredenja na N stim što je ∞ najmanji element. Takode dodefinišemo *max* funkciju na N, tako da je maksimum praznog skupa $-\infty$. Operacija sabiranja na N_1 je ekstenzija operacije $+$ na N tako da $-\infty + x = -\infty$.

2.1.1. Definicija. Neka je $n \in N_1$ i $(a_i)_{i \in N}$ niz realnih brojeva takav da je $n = max\{i : a_i \neq 0\}$. Izraz $p(x) = \sum_{i \leq n} a_i x^i$ nazivamo polinomom stepena n sa nizom koeficijenata $(a_i)_{i \in N}$. Koeficijent a_n nazivamo vodećim koeficijentom polinoma $p(x)$. 0 je polinom stepena $-\infty$, sa nizom koeficijenata $(0)_{i \in N}$. 0 i polinome stepena 0 nazivamo konstantnim polinomima (konstantama). Izraz je polinom ako je polinom stepena n za neko $n \in N_1$. Skup polinoma označavamo sa $R[x]$. Funkcija $st : R[x] \to N_1$ definisana je tako da je st (p) jednak stepenu polinoma p. Koficijent a_n nazivamo vodećim koeficijentom polinoma p. Za polinom čiji je vodeći član 1 kažemo da je moničan.

Uzimajući u definiciji da su koeficijenti iz Z, Q ili C analogno se definišu Z[x], Q[x] i C[x].

Napomenimo činjenicu koja direktno sledi iz definicije.

2.1.2. Posledica. *Dva polinoma su jednaka ako su im jednaki nizovi koeficijenata.*

U nastavku definišemo sabiranje i množenje polinoma.

2.1.3. Definicija. Neka je $p(x) = \sum_{i \leq n} a_i x^i$ i $q(x) = \sum_{i \leq m} b_i x^i$. Tada je

$$p(x) + q(x) = \sum_{i \leq k} (a_i + b_i) x^i, \text{ gde je } k = max\{i \in N : a_i + b_i \neq 0\}$$

$$-p(x) = \sum_{i \leq n} (-a_i) x^i$$

$$p(x) \cdot q(x) = \sum_{i \leq m+n} c_i x^i, \text{ gde je za } i \in N, c_i = \sum_{j+s=i} a_j b_s \, .$$

2.1.4. Tvrđenje. *Neka su su oznake kao u prethodnoj definiciji.*

(i) $st(p(x) + q(x)) \leq max\{\mathrm{st}\,(p(x)), \mathrm{st}\,(q(x))\}$.

(ii) $c_i = 0$, *za* $i > m + n$ *i* $c_{mn} \neq 0$.

(iii) $st(p(x) \cdot q(x)) = \mathrm{st}\,(p(x)) + \mathrm{st}\,(q(x))$.

Dokaz. (i) Kako je za $i > max\{m, n\}$, $a_i = 0$ i $b_i = 0$, to je $a_i + b_i = 0$, za $i > max\{\mathrm{st}\,(p), \mathrm{st}\,(q)\}$. Otuda je $k \leq max\{\mathrm{st}\,(p), \mathrm{st}\,(q)\}$.

(ii) Pretpostavimo da je najpre $p, q \neq 0$. Kako je $c_i = \sum_{j+s=i} a_j b_s$, to je za $i > m + n$, u svakom od sabiraka $a_j b_s$, $j + s = i > m + n$, te je $j > n$ ili $s > m$. Otuda je $a_j = 0$ ili $b_s = 0$, dakle $a_j b_s = 0$. Zato je i $c_i = 0$. Dalje je, $c_{mn} = \sum_{j+s=m+n} a_j b_s$. Analizirajmo proizvoljni sabirak $a_j b_s$, $j+s = m+n$. Ako je $j < n$, tada je $s > m$, pa je $b_s = 0$ a time i $a_j b_s = 0$. Ako je $j > n$ tada je $a_j = 0$ pa je i $a_j b_s = 0$. Dakle, svi sabirci su jednaki nuli osim sabirka za koji je $j = n$ i $s = m$. Taj sabirak je $a_n b_m \neq 0$. Dakle $c_{m+n} = a_n b_m \neq 0$ je vodeći koeficijent polinoma pq. Ostaje slučaj kada je jedan od polinoma p i q jednak 0. Neka je najpre $p = 0$. Tada je $a_j = 0$, za svako $j \in N$, pa je $c_i = \sum_{j+s=i} a_j b_s = 0$, za svaki $i \in N$. Slično se analizira slučaj $q = 0$.

(iii) Prema (ii), ako je $p, q \neq 0$ tada je $\mathrm{st}\,(pq) = m + n$, dakle $\mathrm{st}\,(pq) = \mathrm{st}\,(p) + \mathrm{st}\,(q)$. Neka je sada $st(p) = 0$. Tada je, prema (ii), $p \cdot q = 0$ i $\mathrm{st}\,(pq) = -\infty$. Kako je $\mathrm{st}\,(p) = -\infty$, to je i $\mathrm{st}\,(p) + st(q) = -\infty = st(pq)$, prema definiciji sabiranja u N_1. Slično se analizira slučaj $q = 0$. □

U sledećem tvrđenju nabrajamo algebarske osobine definisanih operacija.

2.1.5. Tvrđenje. *Neka su* $p, q, r \in R[x]$.

(i) $(p + q) + r = p + (q + r)$

(ii) $p + q = q + p$

(ii) $p + 0 = p$

(iv) $p + (-p) = 0$

(v) $(p \cdot q) \cdot r = p \cdot (q \cdot r)$

(vi) $p \cdot q = q \cdot p$

(vii) $p \cdot 1 = p$

(viii) $p \cdot (q + r) = p \cdot q + p \cdot r$.

Dokaz. Dokaz ostavljamo čitaocu kao računsku vežbu. □

2.2. Euklidov algoritam

U $R[x]$ se kao i u Z može definisati deljenje sa ostatkom.

2.2.1. Tvrđenje. *Neka je $p, s \in R[x]$, $s \neq 0$. Postoje jedinstveni polinomi $q, r \in R[x]$ tako da je*

$$p = sq + r \quad \& \quad \mathrm{st}\,(r) < \mathrm{st}\,(s).$$

Dokaz. Dokažimo najpre postojanje. Dokaz izvodimo transfinitnom indukcijom po $\mathrm{st}\,(p)$. Pretpostavimo da je tvrđenje dokazano za polinome stepena manjeg od n. Dokažimo tvrđenje za polinom p stepena n. Neka je $\mathrm{st}\,(p) < \mathrm{st}\,(s)$. Tada je $p = 0 \cdot s + p$ i $\mathrm{st}\,(p) < st(s)$, dakle $q = 0$ i $r = s$ ispunjavaju uslove tvrđenja. Neka je sada $\mathrm{st}\,(p) \geq \mathrm{st}\,(s)$, i neka je $p(x) = \sum_{i \leq n} a_i x^i$ i $s(x) = \sum_{i \leq m} b_i x^i$. Neka je $u = \frac{a_n}{b_m} x^{n-m} \cdot s$. Prema formuli za stepen proizvoda, $\mathrm{st}\,(u) = (n - m) + m = n$. Takođe imamo i da je vodeći koeficijent polinoma u jednak $\frac{a_n}{b_m} \cdot b_m = a_n$. Dakle, $st(p-u) < n$. Zato, prema indukcijskoj hipotezi, postoje polinomi q_1 i r tako da je $p - u = s \cdot q_1 + r$ i $\mathrm{st}\,(r) < \mathrm{st}\,(s)$. Otuda je

$$p = u + (p - u) = (\frac{a_n}{b_m} x^{n-m}) \cdot s + q_1 s + r = (\frac{a_n}{b_m} x^{n-m} + q_1) \cdot s + r = qs + r.$$

Polinomi $q = \frac{a_n}{b_m} x^{n-m} + q_1$ i r zadovoljavaju uslove tvrđenja.

Ostaje da pokažemo jedinstvenost. Dakle, neka je $p = sq + r = sq_1 + r_1$ i $0 \leq \mathrm{st}\,(r), \mathrm{st}\,(r_1) < st(s)$. Tada je $s(q - q_1) = r_1 - r$. Kako je $st(r_1 - r) \leq max\{\mathrm{st}\,(r), \mathrm{st}\,(r_1)\} < st(s)$, to je $st(s(q - q_1)) < st(s)$. Dalje je, prema formuli za stepen proizvoda, $\mathrm{st}\,(s) + st(q - q_1) < \mathrm{st}\,(s)$. Skraćivanjem $\mathrm{st}\,(s)$ sa obe strane nejednakosti dobijamo $\mathrm{st}\,(q - q_1) < 0$. Dakle, $\mathrm{st}\,(q - q_1) = -\infty$ tj. $q - q_1 = 0$. Kako je $q = q_1$, to je i $r = r_1$. □

Analogno definiciji kod celih brojeva definišemo relaciju deljivosti.

2.2.2. Definicija. Neka su $p, s \in R[x]$, $s \neq 0$. $s|p$ akko postoji $q \in R[x]$ tako da je $sq = p$.

2.2.3. Primer. Neka je a ne-nula konstanta i $p \in R[x]$. Tada je $\frac{1}{a}$ takođe ne-nula konstanta. Neka je $s = \frac{1}{a} \cdot p$. Tada $p = a \cdot s$, dakle $a|p$. Zaključujemo da se polinom stepena 0 sadrži u svakom polinomu.

2.2.4. Tvrđenje. *Relacija* $|$ *je refleksivna, tranzitivna relacija koja zadovoljava oslabljenu antisimetričnost:*

$$p|q \quad \& \quad q|p \Leftrightarrow \exists s \in R[x](\ s \text{ je ne-nula konstanta} \quad \& \quad q = sp).$$

Dokaz. Neka je za $p, q \in R[x]$, $p|q$ i $q|p$. Tada je, za neke $s, t \in R[x]$, $p = qs$ i $q = pt$. Zamenom druge jednakosti u prvoj, dobijamo $p = pst$. Na osnovu formule za stepen proizvoda, dobijamo $\mathrm{st}(p) = \mathrm{st}(p) + \mathrm{st}(s) + \mathrm{st}(t)$. Skraćivanjem $\mathrm{st}(p)$, dobijamo $\mathrm{st}(s) + \mathrm{st}(t) = 0$. Dakle, s i t su ne-nula konstante. □

2.2.5. Definicija. Neka su $p, s \in R[x]$, $p, s \neq 0$. $D(p, s) = \{t \in R[x] : t|p, t|q\}$. $d \in R[x]$ je najveći zajednički delilac polinoma p i s ako $d \in D(p, s)$ i za svako $t \in D(p, s)$, $t|d$.

Kako iz $t|d$, sledi $t|ad$, za ma koju ne-nula konstantu a, najveći zajednički delilac nije jedinstven. Međutim, kako se oni sadrže jedan u drugom, razlikuju se do na množenje konstantom. Jednoznačnosti radi najveći zajednički delilac se može definisati kao monični polinom iz te klase polinoma.

2.2.6. Lema. *Neka su* $p, s, q, r \in R[x]$.

(i) *Ako je* $p = qs$, *tada je* $(p, s) = s$

(ii) *Ako je* $p = qs + r$, *tada je* $(p, s) = (r, s)$.

Dokaz. (i) Neka je $(p, s) = d$. Kako $s \in D(p, s)$, to $s|d$. Kako $d \in D(p, s)$, to $d|s$. Prema Tvrđenju 2.2.4., $d = as$ za neku konstantu a.

(ii) Dokazaćemo da je $D(p, s) = D(s, r)$. Neka je $d \in D(p, s)$. Tada $d|p$ i $d|s$, pa $d|p - sq = r$. Dakle, $d \in D(r, s)$. Slično, ako je $d \in D(s, r)$, onda $d|s$ i $d|r$. Otuda $d|qs + r$ tj. $d|p$. Dakle, $d \in D(p, s)$.

2.2.7. Definicija. Neka su $p, s \in R[x]$, $s \neq 0$. Neka je $r_0 = s$. Niz jednakosti

$$(*) \qquad \begin{array}{ll} p = sq_1 + r_1 & 0 < \mathrm{st}(r_1) < \mathrm{st}(s) \\ s = r_1 q_2 + r_2 & 0 < \mathrm{st}(r_2) < \mathrm{st}(r_1) \\ r_1 = r_2 q_3 + r_3 & 0 < \mathrm{st}(r_3) < \mathrm{st}(r_2) \\ \ldots & \ldots \\ r_{n-2} = r_{n-1} q_n + r_n & 0 < \mathrm{st}(r_n) < \mathrm{st}(r_{n-1}) \\ r_{n-1} = r_n q_{n+1} & \end{array}$$

nazivamo Euklidovim algoritmom dužine n za polinome p i s.

2.2.8. Teorema. *Neka su $p, s \in R[x]$, $s \neq 0$. Postoji jedinstven Euklidov algoritam za polinome p i s. $(p, q) = r_n$.*

Dokaz. Prema prethodnom tvrdenju postoje jedinstveni polinomi q_1 i r_1 tako da je $p = sq_1 + r_1$. Ako je $r_1 = 0$. onda je ta jednakost Euklidov algoritam dužine 0. Ako je $r_1 \neq 0$, tada se isto tvrđenje može primeniti na polinome s i r_1. Proceduru nastavljamo na jedinstven način dokgod je ostatak različit od 0. Dakle, r_{i+1} je ostatak pri deljenju r_i sa r_{i-1} tj. $r_{i-1} = r_i q_{i+1} + r_{i+1}$. Ako bi za svako $i \in N$ imali $r_i \neq 0$, tada bi imali beskonačan opadajući niz prirodnih brojeva $\cdots < r_{i+1} < r_i < \cdots < r_1 < s$, suprotno činjenici da je $(N, \leq)$ dobro uređenje. Dakle, za neko $i \in N$ je $r_i = 0$. Otuda, za $n = i - 1$, imamo $r_{n-1} = r_n q_{n+1} + 0$.

Ostaje da pokažemo da je $(p, s) = r_n$. Dokaz izvodimo indukcijom po n, dužini Euklidovog algoritma. Za $n = 0$ imamo $p = sq_1$ i $(p, s) = s = r_0$. Pretpostavimo da je tvrđenje dokazano za Euklidove algoritme dužine $n - 1$, i neka je (p, s) par polinoma koji ima Euklidov algoritam dužine n. Ako u $(*)$ zanemarimo prvu jednakost dobijamo Euklidov algoritam za polinome s i r_1, dužine $n - 1$. Prema indukcijskoj hipotezi $(s, r_1) = r_n$. Kako je $p = sq_1 + r_1$, to je, prema Lemi 2.2.6.(iii), $(p, s) = (s, r_1) = r_n$. □

2.2.9. Posledica. *(Bezu-ova teorema) Neka su $p, s \in R[x]$, $p, s \neq 0$, i $d = (p, s)$. Postoje polinomi $u, v \in R[x]$ tako da je $d = pu + sv$.*

Dokaz. Prema Teoremi 2.2.8., postoji Euklidov algoritam za polinome p i s. Dokaz izvodimo indukcijom po dužini tog Euklidovog algoritma. Neka je najpre dužina Euklidovog algoritma za p i s jednaka 0. Tada je $p = qs$, pa je $s = (p, s)$. Kako je $s = 0 \cdot p + 1 \cdot s$, to $u = 0$ i $v = 1$ zadovoljavaju uslove teoreme. Pretpostavimo da je tvrđenje dokazano za sve parove polinoma (p, s) koji imaju Euklidov algoritam dužine $n - 1$. Neka je sada (p, s) par polinoma koji ima Euklidov algoritam dužine n. Dakle, imamo sledeći niz jednakosti

$$\begin{aligned}
p &= sq_1 + r_1 && 0 < \mathrm{st}(r_1) < \mathrm{st}(s) \\
s &= r_1 q_2 + r_2 && 0 < \mathrm{st}(r_2) < \mathrm{st}(r_1) \\
r_1 &= r_2 q_3 + r_3 && 0 < \mathrm{st}(r_3) < \mathrm{st}(r_2) \\
&\cdots && \cdots \\
r_{n-2} &= r_{n-1} q_n + r_n && 0 < \mathrm{st}(r_n) < \mathrm{st}(r_{n-1}) \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}$$

Analizirajmo niz jednakosti koji se dobija kada odstranimo prvu jednakost. To je Euklidov algoritam za s i r_1, dužine $n - 1$. Prema Teoremi 2.2.8.,

$(s, r_1) = r_n$. Prema indukcijskoj hipotezi, postoje polinomi $t, w \in R[x]$, tako da je $(s, r_1) = r_n = st + r_1 w$. Kako je prema prvoj jednakosti $r_1 = p - sq_1$, zamenom dobijamo $r_n = st + (p - sq_1)w = pw + (t - q_1)s$. Kako je, prema Teoremi 2.2.8., $(p, s) = r_n$, to imamo $(p, s) = pu + sv$, za $u = w$ i $v = t - q_1$. □

2.3. Ireducibilni polinomi

Ireducibilni polinomi imaju ulogu prostih brojeva u $R[x]$.

2.3.1. Definicija. Polinom $p \in R[x]$ je ireducibilan (nesvodljiv) ako je $\mathrm{st}(p) \geq 1$, i za proizvoljne polinime $u, v \in R[x]$,

$$p = u \cdot v \Rightarrow \mathrm{st}(u) = 0 \vee \mathrm{st}(v) = 0$$

2.3.2. Primer. Neka je $p = ax + b$ linearan polinom. p je ireducibilan. Zaista, neka je $p = u \cdot v$. Prema formuli za stepen proizvoda, $1 = \mathrm{st}(u) + \mathrm{st}(v)$, $\mathrm{st}(u), \mathrm{st}(v) \geq 0$. Otuda je $\mathrm{st}(u) = 0$ ili $\mathrm{st}(v) = 0$.

Kvadratni polinom $x^2 + 1$ je takode ireducibilan. Da bi to pokazali pretpostavimo da je $p = u \cdot v$. Tada je $2 = \mathrm{st}(u) + \mathrm{st}(v)$. Pretpostavimo najpre da je $\mathrm{st}(u) = 1$ i $\mathrm{st}(v) = 1$. Dakle, $u = ax + b$ i $v = cx + d$, za neke $a, b, c, d \in R$, $a \neq 0$, $c \neq 0$. Tada je $x^2 + 1 = (ax + b)(cx + d) = acx^2 + (ad + bc)x + bd$. Otuda je $ac = 1$, $bd = 1$ i $ad + bc = 0$. Zamenjujući $c = \frac{1}{a}$ i $d = \frac{1}{b}$ u poslednjoj jednakosti, dobijamo $\frac{a}{b} + \frac{b}{a} = 0$. Otuda je $a^2 + b^2 = 0$, dakle, $a = 0$. Kontradikcija. Kako je $0 \leq \mathrm{st}(u) \leq 2$, to je $\mathrm{st}(u) = 0$ ili $\mathrm{st}(u) = 2$. Kako je u drugom slučaju $\mathrm{st}(v) = 0$, $x^2 + 1$ je ireducibilan. □

U nastavku razmatramo pojam ireducibilnosti u $Z[x]$ i $Q[x]$.

2.3.3. Definicija. Neka je $p \in Z[x]$. p je primitivan ako su njegovi koeficijenti uzajamno prosti.

2.3.4. Tvrđenje. *(Gausova lema) Proizvod primitivnih polinoma je primitivan polinom.*

Dokaz. Neka su $u = \sum_{i \leq n} a_i x^i$ i $v = \sum_{i \leq m} b_i x^i$ primitivni polinomi. Pretpostavimo da $p = uv = \sum_{i \leq m+n} c_i x^i$ nije primitivan. Dakle, neka je $d \in N$ prost broj takav da $d | c_i$, za $i \leq (m + n)$. Kako su u i v primitivni, postoje $k, l \in N$, tako da $d \nmid a_k$ i $d \nmid b_l$. Pretpostavimo da su k i l najmanji takvi brojevi. Dakle $d | a_i$ za $i < k$, i $d \nmid a_k$, $d | b_i$ za $i < l$, a $d \nmid a_l$. Tada je

$$c_{k+l} = \sum_{i+j=k+l} a_i b_j = a_k b_l + \sum_{i+j=k+l, i<k} a_i b_j + \sum_{i+j=k+l, j<l} a_i b_j.$$

Posmatrajmo dve sume na desnoj strani. U prvoj od njih svaki sabirak ima činilac a_i, $i < k$, pa je po pretpostavci deljiv sa d. Slično u drugoj sumi svaki sabirak sadrži b_j, $j < l$, pa je i on deljiv sa d. Kako d deli obe sume, i po pretpostavci $d|c_{k+l}$, to imamo $d|a_k b_l$. Kako je d prost broj, $d|a_k$ ili $d|b_l$. Kontradikcija. Na osnovu dobijene kontradikcije zaključujemo da je p primitivan polinom. □

Za polinome sa racionalnim koeficijentima problem se može svesti na polinome sa celim koeficijentima. Ako je $p \in Q[x]$, dovođenjem koeficijenata na zajednički imenilac a zatim izvlačenjem najvećeg zajedničkog delioca brojilaca, dobijamo $p = \frac{a}{b}s$, gde je $s \in Z[x]$ primitivan polinom, $a, b \in Z$, $(a, b) = 1$. Ovakvo predstavljanje je jedinstveno.

2.3.5. Tvrđenje. *Neka je* $\frac{a}{b}s = \frac{c}{d}t$, $a, b, c, d \in Z$, $(a, b) = 1$, $(c, d) = 1$, $s, t \in Z[x]$, *si* t *primitivni polinomi. Tada je* $t = \pm s$, $\frac{a}{b} = \pm\frac{c}{d}$.

Dokaz. Neka je $s = \sum_{i \leq m} a_i x^i$ i $t = \sum_{i \leq m} a_i x^i$. Množenjem jednakosti sa bd, dobijamo $ads = bct$. Kako jednaki polinomi imaju jednake stepene, $m = n$. Dokazaćemo da $a|c$. Neka je p prost broj takav da $p^k|a$. p^k deli sve koeficijente polinoma na levoj strani, pa zato deli i sve koeficijente polinoma na desnoj strani jednakosti. Kako je s ireducibilan polinom, postoji $i \leq n$ tako da $p \nmid c_i$. Kako $p^k|bcc_i$, $p \nmid b$, jer je $(a, b) = 1$, i $p \nmid c_i$, to $p^k|c$. Kako svaki činilac u prostoj faktorizaciji od a deli c, to $a|c$. Na isti način pokazujemo $c|a$. Otuda je $c = \pm a$. Slično se pokazuje da je $d = \pm b$. Otuda je $ad = \pm bc$, pa je i $t = \pm s$. □

2.3.6. Teorema. *Neka je* $p \in Z[x]$. *Ako je* p *ireducibilan u* $Z[x]$ *onda je* p *ireducibilan i u* $Q[x]$.

Dokaz. Pretpostavimo suprotno da je $p = u \cdot v$, $u, v \in Q[x]$, $\mathrm{st}(u), \mathrm{st}(v) > 0$. Tada je $u = \frac{a}{b}s$, $v = \frac{c}{d}t$, $a, b, c, d \in Z$, $(a, b) = 1$, $(c, d) = 1$, s, t su primitivni polinomi u $Z[x]$. Tada imamo

$$p = \frac{a}{b}s\frac{c}{d}t$$
$$1 \cdot p = \frac{ac}{bd}st.$$

Kako je, prema Gausovoj lemi, st primitivan polinom ovo su dva kanonična predstavljanja polinoma $p \in Q[x]$. Prema prethodnom tvrđenju, imamo $p = \pm st$. To je u kontradikciji sa pretpostavkom o ireducibilnosti polinoma p u $Z[x]$. □

Za utvrđivanje ireducibilnosti u $Z[x]$ može nam pomoći sledeći kriterijum.

2.3.7. Teorema (Ajzenštajnov kriterijum). *Neka je* $s = \sum_{i \leq n} a_i x^i \in Z[x]$, *i* p *prost broj takav da* $p|a_i$, *za* $i < n$, $p \nmid a_n$, *i* $p^2 \nmid a_0$. s *je ireducibilan polinom.*

Dokaz. Pretpostavimo da je $s = uv$, $u, v \in Z[x]$, $\mathrm{st}(u) > 0$, $\mathrm{st}(v) > 0$. Neka je $u = \sum_{i \leq m} a_i x^i$, $v = \sum_{i \leq l} b_i x^i$, $m + l = n$. Kako je $a_0 = c_0 d_0$, to iz $p|a_0$, sledi $p|c_0$ ili $p|d_0$. Kako $p^2 \nmid a_0$, to p ne deli oba ta broja. Bez gubljenja opštosti pretpostavimo da $p|c_0$ i $p \nmid d_0$. Dokazaćemo transfinitnom indukcijom da $p|c_i$, za svako $i \leq m$. Pretpostavimo da za $i < m < n$, $p|c_j$ za svako $j < i$. Dokažimo da $p|c_i$. Kako je $a_i = \sum_{j+k=i} c_j d_k = c_i d_0 + \sum_{j+k=i, j<i} c_j d_k$. Kako u poslednjoj sumi, za svako $j < i$, $p|c_j$, to je čitava suma deljiva sa p. Kako $p|a_i$, to $p|c_i d_0$. Kako $p \nmid d_0$, to $p|c_i$. Time smo pokazali da $p|c_i$, za svako $i \leq m$. Kako $p|c_m$ i $a_n = c_m d_l$, to $p|a_n$, suprotno pretpostavci teoreme. Pretpostavka o reducibilnosti polinoma s dovela je do kontradikcije. Dakle, s je ireducibilan. □

2.3.8. Primer. Polinom $x^3 + 3x^2 + 9x + 3$ je ireducibilan, jer prost broj 3 deli sve koeficijente osim vodećeg, i $3^2 \nmid 3$.

2.3.9. Primer. Neka je p prost broj. Pokažimo da je $s = x^{p-1} + \cdots + x + 1$ ireducibilan. Na prvi pogled se ne vidi kako bi primenili Ajzenštajnov kriterijum. Pomnožimo najpre obe strane jednakosti sa $x - 1$. Dobijamo

$$(x-1)s = x^p + \cdots + x^2 + x - x^{p-1} - \cdots - x - 1.$$

Na desnoj starni se potiranjem jednakih izraza dobija $x^p - 1$, dakle,

$$(x-1)s = x^p - 1.$$

Uvedimo smenu $x = y + 1$, i označimo sa $t(y)$ polinom $s(y+1)$. Tada jednakost dobija oblik

$$\begin{aligned} yt(y) = s(y+1) &= (y+1)^p - 1 \\ &= y^p + \binom{p}{p-1} y^{p-1} + \cdots + \binom{p}{1} y + 1 - 1 \\ &= y^p + \binom{p}{p-1} y^{p-1} + \cdots + \binom{p}{1} y. \end{aligned}$$

Skraćivanjem sa y dobijamo,

$$t(y) = y^{p-1} + \binom{p}{p-1} y^{p-2} + \cdots + \binom{p}{1}.$$

Kako p deli sve binomne koeficijente $\binom{p}{p-1}, \ldots \binom{p}{1}$, primenom Ajzenštajnovog kriterijuma sledi ireducibilnost polinoma $t(y)$. Odavde jednostavno sledi ireducibilnost polinoma $s(x)$. Zaista, pretpostavimo da je $s(x) = u(x) \cdot v(x)$, $u(x), v(x) \in Z[x]$, $\mathrm{st}(u), \mathrm{st}(v) > 0$. Smenom $x = y + 1$ dobijamo $t(y) = s(y+1) = u(y+1)v(y+1) = q(y)r(y)$, gde su $q, r \in R[y]$ i $\mathrm{st}(q), \mathrm{st}(r) > 0$. Kontradikcija sa ireducibilnošću polinoma $t(y)$. Dakle, $s(x)$je ireducibilan polinom.

2.4. Nule polinoma

U dosadašnjim delovima ove glave polinome smo tretirali na strogo sintaksni način. Sada uvodimo semantiku polinoma - davanje vrednosti polinomu. U nastavku ove glave uradićemo inverziju uređanju koeficijenata, tako da polinom $p(x) = \sum_{i \leq n} a_i x^i \in R[x]$ nadalje pišemo u obliku $p(x) = \sum_{i \leq n} a_i x^{n-i}$ i $a \in R$. Na taj način a_0 označava najstariji koeficijent, a a_n slobodan član.

2.4.1. Definicija. Neka je $p(x) = \sum_{i \leq n} a_i x^{n-i} \in R[x]$ i $a \in R$.

$$p(a) = \sum_{i \leq n} a_i a^{n-i}.$$

Ako je $p(a) = 0$ kažemo da je a nula polinoma $p(x)$.

Na ovaj način svakom polinomu p pridružena je realna funkcija f_p tako da je za $a \in R$,

$$f_p(a) = p(a).$$

Funkciju f_p zovemo polinomskom funkcijom pridruženom polinomu p. Prirodno se postavlja sledeće pitanje: Da li je ovo pridruživanje jednoznačno. Da li su različitim polinomima pridružene različite polinomske funkcije?

Sledeća teorema povezuje sintaksni i semantički aspekt polinoma.

2.4.2. Teorema. *(Bezuova teorema) Neka je $p(x) \in R[x]$ i $a \in R$.*

$$p(a) = 0 \Leftrightarrow (x - a) | p(x).$$

Dokaz. Neka je $p(x) = (x-a)q(x) + r$, gde je r konstanta. Zamenom $x = a$, dobijamo $p(a) = (a - a)q(a) + r = r$. Dakle, $p(a) = 0$ akko $r = 0$ tj. $x - a | p(x)$. □

Sada navodimo jedan vrlo koristan i brz algoritam za deljenje polinoma linearnim polinomom.

2.4.3. Tvrđenje. *Neka je* $p(x) = \sum_{i\leq n} a_i x^{n-i} \in R[x]$ *i* $p = (x-c)q + r$. *Ako je* $q(x) = \sum_{i\leq n-1} b_i x^{n-1-i}$, *tada je*

$$b_0 = a_0$$
$$b_i = cb_{i-1} + a_i, \text{ za } 1 \leq i \leq n-1$$
$$r = cb_{n-1} + a_n$$

Dokaz. Kako je $p = (x-a)q + r$, to imamo

$$\sum_{i\leq n} a_i x^{n-i} = (x-c) \sum_{i\leq n-1} b_i x^{n-1-i} + r.$$

Uvedimo u drugoj sumi smenu $j = i+1$. Dobijamo

$$\begin{aligned}\sum_{i\leq n} a_i x^{n-i} &= \sum_{i\leq n-1} b_i x^{n-i} - c \sum_{1\leq j\leq n} b_{j-1} x^{n-j} + r \\ &= \sum_{i\leq n-1} b_i x^{n-i} - \sum_{1\leq i\leq n} cb_{i-1} x^{n-i} \\ &= b_0 x^n + \sum_{1\leq i\leq n-1} (b_i - ab_{i-1}) x^{n-i} + r - cb_{n-1}\end{aligned}$$

Izjednačavanjem koeficijenata na levoj i desnoj strani dobijamo

$$a_0 = b_0$$
$$a_i = b_i + cb_{i-1}, \text{ za } 1 \leq i \leq n-1$$
$$a_n = r - cb_{n-1}.$$

Rešavajući ove jednačine po b_i i r dobijamo

$$b_0 = a_0$$
$$b_i = cb_{i-1} + a_i, \text{ za } 1 \leq i \leq n-1$$
$$r = cb_{n-1} + a_n.$$

Prethodno tvrdenje se koristi u obliku Hornerove šeme.

2.4.5. Primer. Hornerova šema.

Podelićemo polinom $x^5 - 2x^3 + 3x^2 - 5x + 3$ sa $x - 2$.

2	1	0	−2	3	−5	3
		2	4	4	14	18
	1	2	2	7	9	21

Dakle količnik je $x^4 + 2x^3 + 2x^2 + 7x + 9$, a ostatak je 21.

2.4.6. Primer. Iako nam računanje vrednosti polinoma izgleda kao bliži pojam, a deljenje polinoma kao komplikovaniji pojam, Hornerova šema se, na osnovu Bezuove teoreme, često koristi i za brzo nalaženje vrednosti polinoma.

2.4.7. Primer. Posmatrajmo polinome $p = x^3 - 6x^2 + 12x - 8 = (x-2)^3$ i $s = x^3 - x^2 - 4x + 4 = (x-2)(x^2 + x - 2)$. Oba polinoma imaju nulu $x = 2$. Međutim kod p se član $x - 2$ u faktorizaciji pojavljuje tri puta, a kod q samo jednom. Očigledno je da $x - 2$ mnogo više utiče na ponašanje polinoma p nego u slučaju polinoma q.

2.4.8. Definicija. Neka je $p \in R[x]$, $a \in R$ i $k \in N$. a je nula višestrukosti k polinoma p, u oznaci $m_p(a) = k$, ako $(x-a)^k | p$ i $(x-a)^{k+1} \nmid p$.

Primetimo da smo u definiciji dozvolili i nule višestrukosti nula, koje uopšte nisu nule polinoma. Nule višestrukosti 1 nazivamo jednostrukim, a nule višestrukosti > 1, višestrukim.

2.4.9. Tvrđenje. *Neka je $p \in R[x]$, $a \in R$ i $k \in N$. a je nula višestrukosti k polinoma p, akko postoji polinom q tako da*

$$p = (x-a)^k q \quad \& \quad q(a) \neq 0.$$

Dokaz. ($\Rightarrow$) Pretpostavimo da je a nula višestrukosti k. Dakle, $(x-a)^k | p$ i $(x-a)^{k+1} \nmid p$. Dakle, $p = (x-a)^k q$ za neki polinom q. Ako bi $x - a | q$ imali bi $(x-a)^{k+1} \mid p$, suprotno pretpostavci. Dakle, $x - a \nmid q$, pa je prema Bezuovoj teoremi $q(a) \neq 0$.

($\Leftarrow$) Neka je sada $p = (x-a)^k q$ i $q(a) \neq 0$. Očigledno $(x-a)^k | p$. Ako bi imali $(x-a)^{k+1} | p$, tada $x - a | q$, suprotno pretpostavci $q(a) \neq 0$. Dakle, $(x-a)^{k+1} \nmid p$, pa je a nula višestrukosti k polinoma p. □

Kako je nula polinoma semantički pojam, prirodno bi bilo nastojati da pojam višestrukosti karakterišemo semantički. Za to nam je potreban pojam izvoda polinoma.

2.4.10. Definicija. Neka je $p(x) = \sum_{i \leq n} a_i x^{n-i} \in R[x]$. Izvod polinoma p je polinom

$$p'(x) = \sum_{i \leq n-1} (n-i) a_i x^{n-i-1}.$$

2.4.11. Tvrđenje. *Operacija izvoda polinoma ima sledeće osobine*

(i) $(p+q)' = p' + q'$

(ii) $(pq)' = p'q + pq'$

Dokaz. Dokazuje se direktno po definiciji. □

Rekurzivno se definišu izvodi višeg reda.

2.4.11. Definicija. Neka je $p(x) \in R[x]$.

$$p^{(0)}(x) = p(x)$$
$$p^{(n+1)} = (p^{(n)}(x))'.$$

2.4.12. Teorema. *Neka je $p(x) \in R[x]$, $a \in R$, $k \in N$. a je nula višestrukosti k polinoma p akko*

$$p(a) = 0 \quad \& \quad p'(a) = 0 \ldots \quad \& \quad p^{(k-1)}(a) = 0 \quad \& \quad p^{(k)}(a) \neq 0.$$

Dokaz. Neka je $l(p) = min\{i : p^{(i)}(a) \neq 0\}$. Indukcijom po k dokazaćemo da je $l(p) = k$.

Dokažimo tvrđenje za $k = 0$. Tada je a nula višestrukosti 0 polinoma p pa otuda $x - a \nmid p$, što je ekvivalentno sa $p^{(0)}(a) = p(a) \neq 0$. Dakle $l(p) = 0$.

Sada pretpostavimo da je tvrđenje dokazano za sve polinome i sve njihove eventualne nule višestrukosti k.

Neka je sada p polinom i a nula višestrukosti $k+1$. Dakle, $p = (x-a)^{k+1}q$, gde je $q(a) \neq 0$. Tada je $p' = (k+1)(x-a)^k q + (x-a)^{k+1}q' = (x-a)^k((k+1)q + (x-a)q') = (x-a)^k s$, gde je $s = (k+1)q + (x-a)q'$. Kako je $s(a) = (k+1)q(a) + (a-a)q' = (k+1)q(a)$, to je $s(a) \neq 0$. Dakle, a je nula višestrukosti k polinoma p'. Prema indukcijakoj hipotezi, $l(p') = k$. Dakle, $p'(a) = 0, (p')'(a) = 0, \ldots, (p')^{(k-1)}(a) = 0, (p')^{(k)} \neq 0$. Kako je $(p')^{(i)} = p^{(i+1)}$, imamo $p'(a) = 0$, $p''(a) = 0, \ldots, p^{(k)}(a) = 0$, $p^{(k+1)}(a) \neq 0$. Otuda je $l(p) = k + 1$, što je i trebalo dokazati. □

2.4.13. Posledica. *a je višestruka nula polinoma p akko je a nula polinoma (p, p').*

Dokaz. a je višestruka nula polinoma p, akko $p(a) = 0$ i $p'(a) = 0$. Po Bezuovoj teoremi to je ekvivalentnu uslovu $x - a | p, p'$ tj. $x - a | (p, p')$. □

2.5. Polinomi i polinomske funkcije

Vraćamo se problemu odnosa polinoma i polinomskih funkcija. Navedimo najpre teoremu koja ograničava broj nula polinoma.

2.5.1. Definicija. Neka je $p \in R[x]$. $Z(p) = \{a \in R : p(a) = 0\}$. $z(p) = |Z(p)|$ ako je taj broj konačan. U suprotnom je $z(p) = \infty$.

2.5.2. Tvrđenje. *Neka je $p \in R[x]$, $p \neq 0$. Tada je $z(p)$ konačan broj i $z(p) \leq \mathrm{st}(p)$.*

Dokaz. Dokaz izvodimo indukcijom po $\mathrm{st}(p)$. Neka je najpre $\mathrm{st}(p) = 0$. Tada je p ne-nula konstanta, pa p nema nijednu nulu. Dakle, $Z(p) = \emptyset$, i $z(p) = 0$. Zato imamo $z(p) = \mathrm{st}(p) = 0$. Pretpostavimo da je tvrđenje dokazano za sve polinome stepena n i dokažimo ga za polinome stepena $n+1$. Dakle, neka je p polinom stepena $n+1$. Ako p nema nijednu nulu, tada je $z(p) = 0$. Kako je $0 \leq n+1$, tvrđenje je trivijalno zadovoljeno. Pretpostavimo sada da p ima bar jednu nulu, i neka je a jedna od njih. Tada je, prema Bezuovoj teoremi, $p = (x-a)q$, za neki polinom q. Prema formuli za stepen proizvoda, $\mathrm{st}(q) = n$. Prema indukcijskoj hipotezi, $z(q) \leq n$. Neka je sada $b \in R$.

$$\begin{aligned} p(b) = 0 &\Leftrightarrow (b-a)q(b) = 0 \\ &\Leftrightarrow b = a \vee q(b) = 0. \end{aligned}$$

Dakle, $Z(p) = \{a\} \cup Z(q)$. Otuda je $z(p) \leq 1 + z(q) \leq n+1 = \mathrm{st}(p)$. □

Sledeće tvrđenje je kontrapozicija teoreme.

2.5.3. Posledica. *Neka je $p \in R[x]$. $z(p) \geq \mathrm{st}(p) \Rightarrow p = 0$.*

Međutim iz teoreme lako sledi i odgovor na naše početno pitanje.

2.5.4. Posledica. *Neka su $p, q \in R[x]$ i $k = max\{\mathrm{st}(p), \mathrm{st}(q)\}$. Ako postoji $k+1$ različitih realnih brojeva u kojima p i q imaju jednake vrednosti, onda je $p = q$.*

Dokaz. Neka je $EQ(p,q) = \{a \in R : p(a) = q(a)\}$, i neka je $s = p - q$. Prema formuli za stepen zbira, $\mathrm{st}(s) \leq k$. Po pretpostavci je $|EQ(p,q)| \geq k+1$. Kako je za proizvoljni $a \in R$, $s(a) = p(a) - q(a)$, to je $s(a) = 0$ akko $p(a) = q(a)$. Dakle, $a \in Z(s)$ akko $a \in EQ(p,q)$. Otuda je $Z(s) = EQ(p,q)$. Otuda je $z(s) \geq k+1$, tj. $z(s) > \mathrm{st}(s)$. Prema prethodnoj posledici, $s = 0$, tj. $p = q$. □

2.5.5. Posledica. *Neka su $p, q \in R[x]$. $p = q \Leftrightarrow f_p = f_q$*

Dokaz. Implikacija sleva u desno sledi direktno iz definicije vrednosti polinoma. Dokažimo drugu implikaciju. Neka je dakle, $f_p = f_q$. Otuda je $EQ(p,q) = R$. Neka je $k = max\{\mathrm{st}(p), \mathrm{st}(q)\}$. Kako p i q imaju jednake vrednosti u ma kojih $k+1$ različitih realnih brojeva, prema prethodnoj posledici, $p = q$. □

Zahvaljujući ovoj jednoznačnoj korespondenciji u nastavku ne pravimo razliku između polinoma i polinomske funkcije. Iz konteksta se vidi o kojem

se od ta dva objekta radi. Iz prethodnih posledica vidimo da za zadatih $n+1$ vrednosti u $n+1$ različitih tačaka, postoji najviše jedan polinom stepena $\leq n$ koji u tim tačkama uzima zadate vrednosti. Da li uvek postoji takav polinom? Odgovor nam daje sledeća Kineska teorema o ostacima.

2.5.6. Teorema. *Neka su $a_0, \ldots, a_n \in R$ različiti brojevi i $A_0, \ldots, A_n \in R$. Postoji polinom $p \in R[x]$ takav da $\mathrm{st}(p) \leq n$ i $p(a_i) = A_i$, $i \leq n$.*

Dokaz. Najpre da objasnimo zašto je ovo Kineska teorema o ostacima. Uslov $p(a_i) = A_i$, je ekvivalentan uslovu da $p(x)$ pri deljenju sa $x - a_i$ daje ostatak A_i, tj. $p(x) \equiv A_i \pmod{(x - a_i)}$. Dakle, traži se rešenje ovog sistema kongruencija. Takođe imamo da iz $a_i \neq a_j$ sledi $(x - a_i, x - a_j) = 1$. Dakle, pretpostavke i zahtev su identični onima u Kineskoj teoremi o ostacima. I rešenje se postiže na identičan način.

Neka je $M = \prod_{i \leq n}(x - a_i)$, $M_i(x) = \frac{M}{x - a_i}$, $i \leq n$. Neka je dalje M_i' rešenje kongruencije $M_i(x)y \cong 1 (mod x - a_i)$, koje nalazimo na sledeći način. Zamenom $x = a_i$ dobijamo $M_i' = \frac{1}{M_i(a_i)}$. Otuda je traženo rešenje sistema $p = \sum_{i \leq n} M_i M_i' A_i$ odnosno,

$$p = \sum_{i \leq n} A_i \frac{(x - a_0) \ldots (x - a_{i-1})(x - a_{i+1}) \ldots (x - a_n)}{(a_i - a_0) \ldots (a_i - a_{i-1})(a_i - a_{i+1}) \ldots (a_i - a_n)}. \qquad \square$$

Polinom dobijen u dokazu prethodne teoreme naziva se Lagranžov interpolacioni polinom.

2.6. Jednačine trećeg i četvrtog stepena

U ovom delu izvodimo obrazac za rešavanje jednačina trećeg stepena analogno poznatom obrascu za rešavanje kvadratnih jednačina. Dakle, rešavamo jednačinu $ax^3 + bx^2 + cx + d = 0$, $a, b, c, d \in C$. Jednačina u opštem slučaju ima kompleksne koeficijente. Deljenjem sa a dobijamo ekvivalentnu jednačinu kod koje je vodeći koeficijent 1. Dakle, analiziramo jednačinu $x^3 + bx^2 + cx + d = 0$. Ona se dalje pojednostavljuje smenom $x = y - \frac{b}{3}$. Posle sređivanja jednačina dobija oblik $y^3 + py + q = 0$. U tom obliku i rešavamo jednačinu.

Dakle, razmatramo jednačinu $x^3 + px + q = 0$. Potražimo rešenje u obliku $x_0 = \alpha + \beta$, gde ćemo drugi uslov za α i β odrediti naknadno. Zamenom u jednačini dobijamo

$$(\alpha + \beta)^3 + p(\alpha + \beta) + q = 0$$
$$\alpha^3 + \beta^3 + 3\alpha\beta(\alpha + \beta) + p(\alpha + \beta) + q = 0$$
$$\alpha^3 + \beta^3 + (3\alpha\beta + p)(\alpha + \beta) + q = 0.$$

Sada vidimo da se jednačina drastično pojednostavljuje uslovom $\alpha\beta = -\frac{p}{3}$. Jednačina dobija oblik

$$\alpha^3 + \beta^3 = -q$$

$$(*) \qquad \alpha\beta = -\frac{p}{3}.$$

Dakle, ako α i β zadovoljavaju uslov $(*)$, onda je $\alpha + \beta$ rešenje jednačine. Podizanjem drugog uslova na treći stepen dobijamo

$$\alpha^3 + \beta^3 = -q$$

$$\alpha^3\beta^3 = -\frac{p^3}{27}.$$

Na osnovu Vijetovih pravila za kvadratne jednačine su α^3 i β^3 rešenja kvadratne jednačine $z^2 + qz - \frac{p^3}{27} = 0$. Prema formuli za rešavanje kvadratnih jednačina dobijamo

$$(**) \qquad \alpha^3 = \frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

$$\beta^3 = \frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

α i *beta* su treći koreni izraza na desnoj strani jednakosti. Međutim na taj način dobijamo tri vrednosti za α i tri vrednosti za β. Da li to znači da jednačina ima devet rešenja. Naravno da ne. Znamo da ona ima najviše 3 rešenja. Redukciju vrši kontrolni uslov $\alpha\beta = -\frac{p}{3}$, tako da svakom od tri izbora za α pridružuje $\beta = \frac{-p}{3\alpha}$. Dakle, rešenja biramo na sledeći način. Najpre za α biramo jedan treći koren α_1. Ostala dva imaju oblik $\alpha_2 = \alpha_1\epsilon$ i $\alpha_3 = \alpha_1\epsilon^2$, gde su $\epsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2}$ i $\epsilon^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2} = \bar{\epsilon}$ treći koreni iz 1. $\beta_1 = \frac{-p}{3\alpha_1}$. Tada je $\beta_2 = \frac{-p}{3\alpha_2} = \frac{-p}{3\alpha_1\epsilon} = \frac{-p}{3\alpha}\epsilon^2 = \beta_1\epsilon^2$. Slično dobijamo $\beta_3 = \beta_1\epsilon$. Rešenja jednačine su dakle,

$$\alpha_1 + \beta_1$$

$$\alpha_1\epsilon + \beta_1\epsilon^2$$

$$\alpha_1\epsilon^2 + \beta_1\epsilon.$$

Upravo izvedene formule, Kardanovi obrasci, validne su za polinome u $C[x]$, i rešenja su kompleksni brojevi. Sada redukujemo pažnju na jednačine sa realnim koeficijentima. Izvešćemo diskusiju rešenja jednačine. Najpre uvedimo analogno kvadratnim jednačinama diskriminantu polinoma trećeg stepena

$$D = -4p^3 - 27q^2.$$

Primetimo da je to potkorena veličina u izrazu za α^3 i β^3, pomnožena sa -108. Zbog toga je potkorena veličina suprotnog znaka od diskriminante.

2.6.1. Tvrđenje. *Neka je* $x^3 + px + q \in R[x]$.

(i) *Ako je* $D < 0$, *onda jednačina ima jedno realno i dva konjugovano kompleksna rešenja.*

(ii) *Ako je* $D = 0$, *onda jednačina ima tri realna rešenja od kojih su dva jednaka.*

(iii) *Ako je* $D > 0$, *onda jednačina ima sva tri rešenja realna i različita.*

Dokaz. (i) $D > 0$. Tada je potkorena veličina u $(**)$ pozitivna, pa je α^3 realan broj. Neka je α_1 realni treći koren tog realnog broja. Primetimo da je i $\beta^3 \in R$ i $\beta^3 \neq \alpha^3$. Kako je $\frac{-p}{3} \in R$, to je i $\beta_1 \in R$. Kako je $\alpha_1^3 \neq \beta_1^3$, to je $\alpha_1 \neq \beta_1$. Zato je prvo rešenje $x_1 = \alpha_1 + \beta_1 \in R$. Pokazaćemo da su preostala dva rešenja konjugovano-kompleksna. Primetimo najpre da je

$$\overline{x_2} = \alpha_1\overline{\epsilon} + \beta_1\overline{\epsilon^2} = \alpha_1\epsilon^2 + \beta_1\epsilon = x_3.$$

Pretpostavimo da je $x_2 = \alpha_1\epsilon + \beta_1\epsilon^2 \in R$. Tada je i $x_3 = \overline{x_2} \in R$. Otuda je i $x_2 - x_3 \in R$. Međutim,

$$\begin{aligned} x_2 - x_3 &= \alpha_1\epsilon + \beta_1\epsilon^2 - \alpha_1\epsilon^2 - \beta_1\epsilon \\ &= (\alpha_1 - \beta_1)(\epsilon - \epsilon^2) \\ &= i\sqrt{3}(\alpha_1 - \beta_1). \end{aligned}$$

Kako je $\sqrt{3}(\alpha_1 - \beta_1) \in R$, sledi da je i $i \in R$. Kontradikcija. Dakle $x_2, x_3 \notin R$.

(ii) $D = 0$. Tada je $\alpha^3 = \beta^3$, pa je otuda $\alpha_1 = \beta_1$. dakle, $x_1 = 2\alpha_1$. Dalje je

$$\begin{aligned} x_2 &= \alpha_1\epsilon + \alpha_1\epsilon^2 = \alpha_1(\epsilon + \epsilon^2) = -\alpha_1 \\ x_3 &= \alpha_1\epsilon^2 + \alpha_1\epsilon = \alpha_1(\epsilon^2 + \epsilon) = -\alpha_1. \end{aligned}$$

Dakle, $x_2 = x_3 \in R$.

(iii) $D > 0$. Kako je potkorena veličina u $(**)$ negativna, α^3 i β^3 , a time i njihovi treći koreni, ne pripadaju R i različiti su. Sada koristimo jedno tvrđenje koje ćemo dokazati kasnije: Jednačina neparnog stepena sa realnim koeficijentima ima bar jedno realno rešenje. Dakle, neka je baš $x_1 = \alpha_1 + \beta_1 \in R$, $\alpha_1, \beta_1 \notin R$. Kako je, prema uslovu $(*)$, $\alpha_1\beta_1 = \frac{-p}{3} \in R$, to su, po Vijetovim pravilima, α_1 i β_1 konjugovano kompleksna rešenja kvadratne jednačine sa realnim koeficijentima. Dakle, $\beta_1 = \overline{\alpha_1}$. Sada imamo

$$\begin{aligned} x_2 &= \alpha_1\epsilon + \overline{\alpha_1}\epsilon^2 = \alpha_1\epsilon + +\overline{\alpha_1\epsilon} \in R \\ x_3 &= \alpha_1\epsilon^2 + \overline{\alpha_1}\epsilon = \alpha_1\epsilon^2 + +\overline{\alpha_1\epsilon^2} \in R \end{aligned}$$

Ostaje da dokažemo da su rešenja različita. Kako je bilo koje rešenje (jer su sva tri realna) moglo biti uzeto za x_1, dovoljno je dokazati $x_2 \neq x_3$.

$$\begin{aligned} x_2 - x_3 &= \alpha_1\epsilon + \beta_1\epsilon^2 - \alpha_1\epsilon^2 - \beta_1\epsilon \\ &= (\alpha_1 - \beta_1)(\epsilon - \epsilon^2) \\ &= i\sqrt{3}(\alpha_1 - \beta_1). \end{aligned}$$

Kako je $\alpha_1 \neq \beta_1$, to je $x_2 - x_3 \neq 0$ tj. $x_2 \neq x_3$. □

Jednačine četvrtog stepena. Jednačina $x^4 + ax^3 + bx^2 + cx + d = 0$ smenom $x = y - \frac{a}{4}$ dobija oblik $y^4 + b_1y^2 + c_1x + d_1 = 0$. Zato u nastavku rešavamo jednačinu $x^4 + bx^2 + cx + d = 0$. Transformišemo jednačinu uvođenjem parametra t, čiju vrednsot odredujemo naknadno.

$$x^4 + bx^2 + cx + d = (x^2 + \frac{b}{2} + t)^2 - t^2 - 2tx^2 - bt - \frac{b^2}{4} + cx + d$$

$$=(x^2 + \frac{b}{2} + t)^2 - [2tx^2 - cx + (t^2 + bt - d + \frac{b^2}{4})] = 0.$$

Sada biramo t tako da izraz u srednjim zagradama, kao kvadratni plinom po x, bude potpun kvadrat. Poznato je da je to ispunjeno za kvadratni trinom akko je diskriminanta trinoma jednaka nuli. To i jeste naš uslov za t. Dakle, t biramo iz uslova

$$c^2 - 8t(t^2 + bt - d + \frac{b^2}{4}) = 0, \text{ tj.}$$

$$(*) \qquad t^3 + bt^2 + (\frac{b^2}{4} - d)t - \frac{c^2}{8} = 0.$$

Dakle, da bi dobili pogodnu vrednost za t treba da rešimo jednačinu trećeg stepena.

Neka je t_0 jedno rešenje jednačine $(*)$. Početna jednačina dobija oblik

$$(x^2 + \frac{b}{2} + t_0)^2 - 2t_0(x - \frac{c}{4t_0})^2 = 0.$$

Formulom za razliku kvadrata, ova jednačina se razlaže u dve kvadratne jednačine. Njihova rešenja su rešenja polazne jednačine četvrtog stepena.

Dugi niz godina činjeni su pokušaji da se slični obrasci nađu za jednačine višeg stepena. Sredinom 19. veka dokazano je da za jednačine stepena $n \geq 5$ takvi obrasci ne postoje. Dokazano je i jače tvrđenje da za svako $n \geq 5$ postoji polinom čije se nule ne mogu izraziti u kvadraturama (sabiranjem, množenjem i korenovanjem).

2.7. Racionalni koreni polinoma u $Z[x]$

Nepostojanje opštih obrazaca za rešavanje jednačina višeg stepena, i ne baš jednostavni obrasci za jednačine trećeg i četvrtog stepena, primoravaju nas da nalazimo druge metode njihovog rešavanja. Jednačine trećeg stepena se recimo prirodno pojavljuju u elementarnoj matematici pri rešavanju zadataka u vezi sa zapreminama. Jedan od korisnih i jednostavnih metoda je sledeći: Ako je polinom u $Z[x]$, možemo naći sve njegove eventualne racionalne nule vrlo jednostavnim postupkom. Polinome iz $Q[x]$ i ne analiziramo posebno, jer se jednačine množenjem sa celim brojem koji sadrži imenioce koeficijenata svodi na ekvivalentnu jednačinu sa celim koeficijentima.

2.7.1. Tvrđenje. *Neka je* $p(x) = \sum_{i \leq n} a_i x^{n-i} \in Z[x]$. *Ako je* $\frac{a}{b}$, $(a,b) = 1$, *nula polinoma* p, *onda* $a|a_n$ *i* $b|a_0$.

Dokaz. Pretpostavimo da je $\frac{a}{b}$ nula polinoma p. Zamenom $x = \frac{a}{b}$ i množenjem obe strane jednačine sa b^n dobijamo

$$a_0 a^n + a_1 a^{n-1} b + a_2 a^{n-2} b^2 + \cdots + a_{n-1} a b^2 + a_n b^n = 0.$$

Kako u sumi na levoj strani jednakosti b deli sve sabirke osim prvog, b deli i prvi sabirak. Dakle, $b|a_0 a^n$. Kako je $(a,b) = 1$, to $b|a_0$. Slično, a deli sve sabirke osim poslednjeg pa deli i njega. Dakle, $a|a_n b^n$. Kako je $(a,b) = 1$, to $a|a_n$. □

2.7.2. Primer. Rešavamo jednačinu

$$6x^4 + 37x^3 + 22x^2 - 9x - 6 = 0.$$

Neka je $\frac{a}{b}$ racionalno rešenje ove jednačine. Prema prethodnom tvrđenju $a|6$ i $b|6$. Otuda $a \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ i $b \in \{1, 2, 3, 6\}$. Otuda $\frac{a}{b} \in \{\pm 1, \pm 2, \pm 3, \pm 6, \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{1}{6}\}$. Zamenom ovih 18 vrednosti u polinomu utvrđujemo da su $\frac{1}{2}$ i $-\frac{2}{3}$ nule polinoma. Zamenjivanje 18 razlomlenih vrednosti nije nimalo prijatno. Može nam pomoći Hornerova šema, jer je α nula polinoma akko je ostatak pri deljenju sa $x - \alpha$ jednak 0. Pogodnost je i u tome što u slučaju kada α jeste nula, odmah imamo i količnik i dalje radimo sa njim. Dakle,

$\frac{1}{2}$	6	37	22	−9	−6
		3	20	21	6
	6	40	42	12	0

Sada dobijeni količnik delimo sa $x + \frac{2}{3}$.

$-\frac{2}{3}$	6	40	42	12
		-4	-16	-12
	6	36	18	0

Dakle, polazna jednačina je ekvivalentna jednačini

$$(x - \frac{1}{2})(x + \frac{2}{3})(6x^2 + 36x + 18) = 0.$$

Rešavajući preostalu kvadratnu jednačinu dobijamo ipreostala dva rešenja, $x = -3 \pm \sqrt{6}$.

Čak se i ispitivanje racionalnih nula može svesti na ispitivanje celih nula nekog drugog polinoma u $Z[x]$.

2.7.3. Tvrđenje. *Neka je* $p(x) = \sum_{i \leq n} a_i x^{n-i} \in Z[x]$. $r \in Q$ *je nula polinoma* p *akko je* ra_0 *celobrojna nula polinoma*

$$q = 1 + \sum_{1 \leq i \leq n} a_i a_0^{i-1} x^{n-i} \in Z[x].$$

Dokaz. Pomnožimo jednačinu $p(x) = 0$, sa a_0^{n-1}. Jednačina dobija oblik

$$\begin{aligned} a_0^n p(x) &= \sum_{i \leq n} a_i a_0^{n-1} x^{n-i} \\ &= 1 + \sum_{1 \leq i \leq n} a_i a_0^{i-1} (a_0 x)^{n-i} = 0 \end{aligned}$$

Uvedimo smenu $a_0 x = y$. Time dobijamo jednačinu

$$q(y) = 1 + \sum_{1 \leq i \leq n} a_i a_0^{i-1} y^{n-i} = 0.$$

Broj $s \in Z$ je rešenje ove jednačine akko je $\frac{s}{a_0} \in Q$ rešenje polazne jednačine. □

Zato na značaju dobija sledeći test.

2.7.4. Tvrđenje. *Neka je* $p(x) \in Z[x]$. *Ako je* $a \in Z$ *nula polinoma* p, *onda*

$$1 - a|p(1) \ \& \ 1 + a|p(-1).$$

Dokaz. Neka je $a \in Z$ nula polinoma p. Tada je $p = (x - a)q(x)$, za neki polinom $q \in R[x]$. Kako se koeficijenti polinoma q mogu dobiti Hornerovom šemom, dakle množenjem i sabiranjem celog broja a i celobrojnih koeficijenata polinoma p, to je $q \in Z[x]$. Zamenom $x = 1$ u jednakosti, dobijamo $p(1) = (1 - a)q(a)$. Kako je $q(a) \in Z$, to $1 - a|p(a)$. Analognom zamenom $x = -1$ dobijamo $1 + a|p(-1)$. □

2.7.5. Primer. Primenimo prethodno tvrdenja za rešvanje jednačine $x^4 + x^3 - 4x^2 + 2x - 12 = 0$. Kako je polinom moničan, sva racionalna rešenja su cela. Prema Tvrđenju 2.7.1., jedina moguća racionalna rešenja su iz skupa $\{\pm 1, \pm 2, \pm 3, \pm 6, \pm 12\}$. Kako je $p(1) = -12$ i $p(-1) = -18$, 1 i -1 nisu rešenja jednačine. Međutim, prema prethodnom tvđenju nijedan od brojeva ± 6, ± 12 nije rešenje jednačine, jer na rastojanju 1 po apsolutnoj vrednsoti imaju brojeve 5 i 7, odnosno 11 i 13 koji ne dele niti $p(1)$ niti $p(-1)$. Takode i $1 + 3 \nmid -18$, pa ni 3 nije rešenje. Dakle, dovoljno je isprobati brojeve ± 2 i -3. Posle kratke provere dobijamo da su $x = -3$ i $x = 2$ rešenja jednačine. Deljenjem polinoma sa $x + 3$ i $x - 2$, dobijamo polinom $x^2 + 2$. Zato supreostala dva rešenja, $x = \pm i\sqrt{2}$.

2.8. Osnovna teorema algebre

Iz pretencioznog naslova vidimo da se radi o veoma važnoj teoremi. Kako je rešavanje polinomskih jednačina bilo osnovno pitanje algebre sve do sredine 19. veka, ona je u to vreme i zaluživala svoje ime. Danas je ono zadržano iz tradicionalnih razloga. Mi nećemo dati dokaz ove teoreme jer algebarski dokaz zahteva razvijenu teoriju ekstenzija polja. Dokazi koji koriste aparat analize su ili računski komplikovani ili nisu predmet našeg rada. Zato ovde dokazujemo specijalni slučaj ove teoreme, i analiziramo neke njene posledice. Najpre se pozivamo na dve teoreme iz analize.

2.8.1. Teorema. *Polinomska funkcija je neprekidna*

2.8.2. Teorema. *(Teorema o međuvrednosti) Neka je* $f : R \to R$ *funkcija neprekidna na intervalu* $[a, b]$, *tako da je* $f(a) < 0$ *i* $f(b) > 0$. *Postoji* $c \in (a, b)$, *tako da je* $f(c) = 0$.

2.8.3. Lema. *(Lema o najstarijem članu) Neka je* $p(x) = \sum_{i \leq n} a_i x^{n-i} \in R[x]$ *i* $s(x) = \sum_{1 \leq i \leq n} a_i x^{n-i}$. *Neka je* $A = max\{|a_1|, \ldots, |a_n|\}$ *i* $M =$

$1 + \frac{A}{|a_0|}$. *Tada je za* $|x| > M$,

$$|a_0 x^n| > |s(x)|.$$

Dokaz. Neka je $|x| > M$. Kako je $|x| > 1$, imamo da je $\frac{A}{|x|-1} < |a_0|$. Sada je

$$\begin{aligned} |s(x)| &\leq \sum_{1 \leq i \leq n} |a_i||x|^{n-i} \\ &\leq A \sum_{1 \leq i \leq n} |x|^{n-i} \\ &= A \frac{|x|^n - 1}{|x| - 1} \\ &\leq \frac{A}{|x| - 1} |x|^n \\ &\leq |a_0 x^n|. \quad \square \end{aligned}$$

2.8.4. Posledica. *Neka su oznake kao u prethodnoj lemi. Sve realne nule polinoma* p *su u intervalu* $[-M, M]$.

Dokaz. Neka je $|x| > M$. Kako je $|a_0 x^n| > |s(x)|$, to je $p(x) = a_0 x^n + s(x) \neq 0$. Dakle, van intervala $[-M, M]$ nema nula polinoma p. $\square$

2.8.5. Teorema. *Neka je* $p \in R[x]$, $\mathrm{st}\,(p) = n$, n *neparan. Tada* p *ima bar jednu realnu nulu.*

Dokaz. Neka su oznake kao u lemi o najstarijem članu. Bez gubljenja opštosti možemo pretpostaviti da je $a_0 > 0$. U suprotnom razmatramo polinom $-p$. Neka je $a > M$. Tada je $p(a) = a_0 a^n > 0$. Kako je n neparan, to je $p(-a) = a_0(-a)^n < 0$. Prema teoremi o međuvrednosti, postoji $c \in (-a, a)$ tako da je $p(c) = 0$. $\square$

Navodimo bez dokaza najvažniju teoremu ove glave. Ona se odnosi na polinome sa kompleksnim koeficijentima.

2.8.6. Teorema. *Neka je* $p \in C[x]$, $\mathrm{st}\,(p) \geq 1$. *Tada* p *ima bar jednu (kompleksnu) nulu.*

Naredna posledica deluje mnogo jače od teoreme ali iz nje trivijalno sledi. Ona pokazuje da se granica ustanovljena Lagranžovom teoremom dostiže (ako računamo nule sa njihovom višestrukošću). Najpre fiksirajmo neke oznake.

2.8.7. Definicija. Neka je p polinom. $z_m(p) = \sum_{a \in Z(p)} m_p(a)$.

2.8.8. Posledica. *Neka je $p \in C[x]$ i $\mathrm{st}\,(p) = n \geq 0$. Tada p ima tačno n nula, tj. $z_m(p) = n$.*

Dokaz. Dokaz izvodimo indukcijom po n. za $n = 0$ tvrdenje je trivijalno zadovoljeno. Pretpostavimo da tvrđenje važi za polinome stepena n. Neka je sada $\mathrm{st}\,(p) = n + 1$. Prema osnovnoj teoremi algebre, postoji $a \in C$ tako da je $p(a) = 0$. Nastavak je kao kod dokaza Lagranžove teoreme. Dakle, postoji $q \in C[x]$, tako da je $p = (x - a)q$ i $\mathrm{st}\,(q) = n$. Prema Indukcijskoj hipotezi, $z_m(q) = n$. Kako je $Z(p) = \{a\} \cup Z(q)$, to je a ili nova nula ili povećava višestrukost za 1, pa je $z_m(p) = z_m(q) + 1 = n + 1$. □

Naredna posledica pokazuje da su jedini ireducibilni polinomi u $C[x]$ linearni polinomi.

2.8.9. Posledica. *Neka je $p(x) = \sum_{i \leq n} a_i x^{n-i} \in C[x]$, $n \geq 0$. Postoje $\alpha_1, \ldots, \alpha_n \in C$ tako da je*

$$p(x) = a_0 \prod_{i \leq n} (x - \alpha_i).$$

Dokaz. Indukcijom po n. Za $n = 0$, tvrdenje je trivijalno zadovoljeno (prazan proizvod jednak je 1). Pretpostavimo da je tvrdenje dokazano za polinome stepena n. Neka je sada $\mathrm{st}\,(p) = n + 1$. Prema osnovnoj teoremi algebre, postoji $a \in C$ tako da je $p(a) = 0$. Dakle, postoji $q \in C[x]$, tako da je $p = (x - a)q$ i $\mathrm{st}\,(q) = n$. Vodeći koeficijent od q je takođe a_0. Prema Indukcijskoj hipotezi, $q(x) = a_0 \prod_{i \leq n}(x - \alpha_i)$. Otuda je, za $\alpha_{n+1} = \alpha$, $p(x) = a_0 \prod_{i \leq n+1}(x - \alpha_i)$. □

2.8.10. Posledica. *Neka je $p(x) = \sum_{i \leq n} a_i x^{n-i} = a_0 \prod_{i \leq n}(x - \alpha_i)$. Tada je*

$$\sum_{i \leq n} \alpha_i = -\frac{a_1}{a_0}$$

$$\sum_{i < j \leq n} \alpha_i \alpha_j = -\frac{a_2}{a_0}$$

$$\vdots$$

$$\sum_{i_1 < \cdots < i_k \leq n} \prod_{s \leq k} \alpha_{i_s} = (-1)^k \frac{a_k}{a_0}$$

$$\vdots$$

$$\prod_{i \leq n} \alpha_i = (-1)^n \frac{a_n}{a_0}$$

Dokaz. Množenjem izraza na desnoj strani i izjednačavnjem koeficijenata dobijamo navedene jednakosti. □

Jednakosti iz prethodne posledice nazivaju se Vijetovim formulama. Sada se vraćamo polinomima sa realnim koeficijentima. Pre toga navodimo poznate osobine konjugovanja kompleksnog broja.

2.8.11. Tvrđenje. *Neka su* z, z_1 *kompleksni brojevi,* $p(x) \in R[x]$.

(i) $\overline{z + z_1} = \overline{z} + \overline{z_1}$

(ii) $\overline{z \cdot z_1} = \overline{z} \cdot \overline{z_1}$

(iii) $\overline{z^n} = (\overline{z})^n$.

(iv) $\overline{p(z)} = p(\overline{z})$

Dokaz. . Prve dve jednakosti dokazuju se po definiciji. Osobina (iii) dokazuje se indukcijom, gde se indukcijski korak zasniva na osobini (ii).

(iv) Neka je $p(x) = \sum_{i \leq n} a_i x^{n-i}$.

$$\begin{aligned}
\overline{p(z)} &= \overline{\sum_{i \leq n} a_i z^{n-i}} \\
&= \sum_{i \leq n} \overline{a_i z^{n-i}} \\
&= \sum_{i \leq n} a_i \overline{z}^{n-i}, \text{ jer je } a_i \in R \\
&= p(\overline{z}).
\end{aligned}$$

2.8.12. Lema. *Neka je* $p \in R[x]$ *i* $z \in C$. $m_p(z) = m_p(\overline{z})$.

Dokaz. Najpre pokazujemo da ako je z nula polinoma p, onda je i $\overline{z}$ nula polinoma p. Zaista

$$\begin{aligned}
p(z) = 0 &\Rightarrow \overline{p(z)} = 0 \\
&\Rightarrow p(\overline{z}) = 0.
\end{aligned}$$

Sada pokazujemo da z i $\overline{z}$ imaju istu višestrukost. Neka je $m_p(z) = k$ i $m_p(\overline{z}) = l$. Bez gubljenja opštosti možmo pretpostaviti da je $k \geq l$. Prema definiciji višestrukosti nule polinoma,

$$p = (x - z)^k (x - \overline{z})^l s(x),$$

gde je $s(z) \neq 0$ i $s(\overline{z}) \neq 0$. Kako je $(x - z)(x - \overline{z}) = x^2 - (z + \overline{z})x + z\overline{z}$, i $z + \overline{z}, z\overline{z} \in R$, to je $q(x) = \frac{p}{(x-z)^l (x-\overline{z})^l} \in R[x]$. S druge strane,

$$q(x) = \frac{(x - z)^k (x - \overline{z})^l s(x)}{(x - z)^l (x - \overline{z})^l} = (x - z)^{k-l} s(x).$$

Ako bi imali $k - l > 0$, tada bi z bio nula polinoma $q \in R[x]$, a $\overline{z}$ ne bi bio nula tog polinoma, suprotno činjenici dokazanoj u prvom delu dokaza. Kako je $k - l \geq 0$, ostaje $k - l = 0$, tj. $k = l$. □

2.8.13. Teorema. *Svaki polinom p, $\mathrm{st}(p) > 0$, može se predstaviti kao proizvod linearnih i kvadratnih ireducibilnih polinoma.*

Dokaz. Neka je $p(x) = \sum_{i \leq n} a_i x^{n-i} \in R[x]$. prema Posledici 2.8.8., p ima (računato sa višestrukošću), n (kompleksnih) nula. Neka je među njima k realnih i $n - k$ nula iz $C \setminus R$. Neka su $\alpha_1, \ldots, \alpha_n$ realne nule i $\beta_1, \ldots, \beta_{n-k}$ nule koje nisu u R. Prema prethodnoj lemi, za svaki β_i, $i \leq n - k$, postoji β_j, $j \neq i$, tako da je $\beta_j = \overline{\beta_i}$. To pridruživanje može se definisati tako da je različitim β_i pridružen različit β_j, jer kadgod se β_i ponovi sa nekim drugim indeksom, prema prethodnoj lemi, isto toliko puta ponavlja se i β_j sa nekim drugim indeksom. Dakle, za $l = \frac{n-k}{2}$, $\{\beta_1, \ldots, \beta_{n-k}\}$ može se predstaviti u obliku $\{\gamma_1, \overline{\gamma}_1, \ldots, \gamma_l, \overline{\gamma}_l\}$. Neka je za $i \leq l$, $q_i = (x - \gamma_i)(x - \overline{\gamma_i})$. Kako je $q_i = x^2 - (\gamma_i + \overline{\gamma_i})x + \gamma_i\overline{\gamma_i}$, i $\gamma_i + \overline{\gamma_i}, \gamma_i\overline{\gamma_i} \in R$, to je $q_i \in R[x]$. Kako nule polinoma q_i nisu u R, to je q_i, $i \leq l$, kvadratni ireducibilan polinom u $R[x]$. Prema Posledici 2.8.9., imamo

$$\begin{aligned} p &= a_0 \prod_{i \leq k} (x - \alpha_i) \cdot \prod_{j \leq l} (x - \gamma_i)(x - \overline{\gamma_i}) \\ &= a_0 \prod_{i \leq k} (x - \alpha_i) \cdot \prod_{j \leq l} q_j. \end{aligned}$$

Time je tvrđenje dokazano. □

2.8.14. Posledica. *U $R[x]$ skup ireducibilnih polinoma čine linearni polinomi i neki kvadratni polinomi.*

2.9. Granice korena polinoma

U situaciji kada ne možemo u kvadraturama da rešimo polinomske jednačine, nastojaćemo da približno odredimo nule polinoma. Osnovnu pomoć nam predstavlja teorema o međuvrednosti. Nastojimo da odredimo intervale u kojima polinom menja znak. U tim intervalima se, prema teoremi o međuvrednosti, nalaze nule polinoma. Da bi te intervale efikasno tražili, treba da rešimo dva problema:

Problem 1. Odrediti intervale u kojima se mogu naći nule polinoma.

Problem 2. Odrediti broj realnih nula polinoma.

Problem 1 analiziramo u ovoj sekciji, a Problem 2 u narednoj. Metode ilustrujemo na polinomu

$$p = x^5 + 2x^4 - 7x^3 + 2x^2 + x - 5.$$

Prema Teoremi 2.8.13., p ima jednu, tri ili svih pet realnih nula. Prema Lemi 2.8.3., $M = 1 + \frac{7}{1} = 8$. Dakle, sve realne nule su u intervalu $(-8, 8)$. Nalaženjem nekih vrednosti iz tog intervala dobijamo tabelu vrednsoti.

x	-4	-3	-2	-1	0	1	2
y	-41	118	57	4	-5	-6	13

Iz tabele, na osnovu teoreme o međuvrednosti, dobijamo da p ima realne nule u intervalima $(-4, -3)$, $(-1, 0)$ i $(1, 2)$. Deleći ove intervale na sitnije, i nalazeći one od njih u kojima p menja znak, možemo te nule približn odrediti sa tačnošću željeng broja decimala. Pitanje je koliko će to biti brzo, i razvoj tih efikasnih algoritama je važno pitanje Numeričke analize. Mi još uvek ne znamo broj realnih nula polinoma p. Taj broj je 3 ili 5. Zar nije jasno da je taj broj 3? Ne. Koliko god sitnu podelu napravili, nikada nismo sigurni da, iako polinom na krajevima nekog od tih intervala ima isti znak, on nije unutar njega dva puta promenio znak, i vratio se na polazni. To bi rezultiralo sa 2 dodatne nule. Dakle, naš Problem 2, moramo rešavati na drugi način.

2.9.1. Definicija. Neka je $p \in R[x]$.

(i) Broj $a \in R^+$ je gornja granica pozitivnih nula polinoma p, u oznaci $GGP_p(a)$, ako za $x > a$, $p(x) \neq 0$.

(ii) Broj $a \in R^+$ je donja granica pozitivnih nula polinoma p, u oznaci $DGP_p(a)$, ako za $0 < x < a$, $p(x) \neq 0$.

(iii) Broj $a \in R^-$ je gornja granica negativnih nula polinoma p, u oznaci $GGN_p(a)$, ako za $a < x < 0$, $p(x) \neq 0$.

(iv) Broj $a \in R^-$ je donja granica negativnih nula polinoma p, u oznaci $DGN_p(a)$, ako za $x < a$, $p(x) \neq 0$.

Sledeće tvrđenje omogućuje nam da nalaženje svih granica svedemo na nalaženje GGP. Umesto da menjamo algoritam, mi menjamo polinom.

2.9.2. Tvrđenje. *Neka je* $p = \sum_{i \leq n} a_i x^{n-i} \in R[x]$

(i) *Za* $p_1 = \sum_{i \leq n} a_i x^i \in R[x]$, *ako je* N_1 *GGP za* p_1 *onda je* $\frac{1}{N_1}$ *DGP za* p.

(ii) *Za* $p_2 = \sum_{i \leq n} -a_n x^{n-i} \in R[x]$, *ako je* N_2 *GGP za* p_2, *onda je* $-N_1$ *DGN za* p.

(i) *Za* $p_3 = \sum_{i\leq n} a_i x^i \in R[x]$, *ako je* N_3 *GGP za* p_3 *onda je* $-\frac{1}{N_3}$ *GGN za* p.

Dokaz. (i) Neka je N_1 GGP za p_1. Tada imamo

$$x > N_1 \Rightarrow \sum_{i\leq n} a_n x^n \neq 0, \text{ smenom } y = \frac{1}{x} \text{ dobijamo}$$

$$\frac{1}{y} > N_1 \Rightarrow \sum_{i\leq n} a_i \left(\frac{1}{y}\right)^i \neq 0. \text{ Kako je } y > 0, \text{ imamo}$$

$$0 < y < \frac{1}{N_1} \Rightarrow \frac{1}{y^n} \sum_{i\leq n} a_i y^{n-i} \neq 0.$$

$$0 < y < \frac{1}{N_1} \Rightarrow \sum_{i\leq n} a_i y^{n-i} \neq 0.$$

Dakle, $\frac{1}{N_1}$ je DGP za p.

(ii) Analogno prethodnom dokazu. Smena je $y = -x$.

(iii) Analogno (i). Smena je $y = -\frac{1}{x}$. □

U nastavku razvijamo samo algoritme za GGP. Jedan od njih već imamo iz Leme o najstarijem članu.

2.9.3. Tvrđenje. *Neka je* $p = \sum_{i\leq n} a_i x^{n-i}$, $A = max\{|a_i| : 1 \leq i \leq n\}$, $M = 1 + \frac{A}{a_0}$. *M je GGP polinoma p.*

Ako malo pogledamo dokaz te leme, vidimo da majoriranje nismo izvršili najštedljivije. Očigledno je da članove sa pozitivnim koeficijentima nije trebalo stavljati u tabor koji a_0 treba da nadvisi po apsolutnoj vrednosti. Zato preciznijim majoriranjem dobijamo bolju GGP polinoma.

2.9.4. Tvrđenje. *Neka je* $p(x) = \sum_{i\leq n} a_i x^{n-i} \in R[x]$, *tako da je* $a_0 > 0$, *i označimo sa* $s(x) = \sum_{1\leq i\leq n} a_i x^{n-i}$. *Neka je* $S = \{i \leq n : a_i < 0\}$, $k = minS$, $A = max\{|a_i| : i \in S\}$ *i* $M = 1 + \sqrt[k]{\frac{A}{|a_0|}}$. *Tada je M GGP za p.*

Dokaz. Neka je $|x| > M$. Kako je $|x| > 1$, imamo da je $\frac{A}{|x|-1^k} < |a_0|$. Neka

je $s(x) = \sum_{i \in S} a_i x^{n-i}$ Sada je

$$\begin{aligned}
|s(x)| &\leq \sum_{i \in S} |a_i||x|^{n-i} \\
&\leq A \sum_{i \in S} |x|^{n-i} \\
&\leq A \sum_{k \leq i \leq n} |x|^{n-i} \\
&= A \sum_{0 \leq j \leq n-k} |x|^j \\
&= A \frac{|x|^{n+k-1} - 1}{|x| - 1} \\
&\leq A \frac{|x|^{n+k-1}}{|x| - 1} \\
&= \frac{A}{(|x| - 1)|x|^{k-1}} |x|^n \\
&\leq \frac{A}{(|x| - 1)^k} |x|^n \\
&\leq |a_0 x^n|.
\end{aligned}$$

Neka je $T = \{i \leq n : i \geq 1, a_i > 0\}$. Dakle,

$$p(x) = a_0 x^n + \sum_{i \in T} a_i x^{n-i} + \sum_{i \in S} a_i x^{n-i}.$$

Kako je za $x > M$, $|a_0 x^n + \sum_{i \in T} a_i x^{n-i}| \geq |a_0 x^n| > |\sum_{i \in S} a_i x^{n-i}|$, to je za $x > M$, $p(x) \neq 0$. Dakle, M je GGP polinoma p. □

Imamo još jedan metod za određivanje GGP, baziran na Maklorenovoj formuli.

2.9.5. Tvrđenje. *Neka je* $p(x) = \sum_{i \leq n} a_i x^{n-i} \in R[x]$, $a_0 > 0$ *i neka je* $c \in R$ *tako da*

$$p(c) = 0, p'(c) > 0, \ldots, p^{(n)}(0) > 0.$$

Tada je c *GGP za* p.

Dokaz. Prema Maklorenovoj formuli,

$$p(x) = \sum_{i \leq n} \frac{p^{(i)}(c)}{i!} (x - c)^i.$$

Neka je $x > c$. Tada su svi sabirci pozitivni, pa je $p(x) > 0$. Dakle, c je GGP za p. □

2.9.5. Primer. Tvrđenje 2.9.4. primenjeno na polinom p daje GGP $1+\sqrt{7} \leq 3,7$. Da bi našli DGP, treba da promenimo polinom. DAkle, analiziramo polinom

$$q = x^5 p(\frac{1}{x}) = -3x^5 - 7x^4 + 8x^3 - 5x^2 + 2x - 1$$

$$= -(3x^5 + 7x^4 - 8x^3 + 5x^2 - 2x + 1.$$

Posmatramo polinom u zagradama, zbog uslova da je vodeći koeficijent pozitivan (a ima iste nule kao q). Za njega je $A = 8$, pa je $M = 1 + \sqrt{\frac{8}{3}} \geq 2,6\}$, pa je 0,38 DGN polinoma polinoma p.

Jednostavnom zamenom se takođe proverava da je za $x = 2$, $p(x) > 0$,$p'(x) > 0$, $p''(x) > 0$, $p'''(x) > 0$, $p^{(iv)}(x) > 0$, $p^{(v)}(x) > 0$. Otuda je prema prethodnom tvrđenju 2 GGP za polinom p.

2.10. Šturmov algoritam

Neka je $f : R \to R$ realna funkcija i $\alpha \in R$. Kazaćemo da f menja znak pri prolasku kroz α, ako postoji $\epsilon > 0$, tako da f ima jedan znak u intervalu $(\alpha - \epsilon, \alpha)$, a suprotan znak u $(\alpha, \alpha + \epsilon)$. Teorema o međuvrednosti može se interpretirati tako da ako neprekidna funkcija menja znak pri prolasku kroz α, onda je α nula te funkcije. Koristićemo i sledeću osobinu neprekidnih funkcija, formulisanu za polinome, koja sledi direktno iz definicije neprekidnosti.

2.10.1. Tvrđenje. *Neka je $p \in R[x]$ i $\alpha \in R$. Ako je $p(\alpha) > 0$, tada postoji $\epsilon > 0$, tako da je za svako $x \in (\alpha - \epsilon, \alpha + \epsilon)$, $p(x) > 0$. Analogno tvrđenje važi ako zanak $>$ zamenimo znakom $<$.*

2.10.2. Definicija. Neka je $p \in R[x]$ polinom čije su sve realne nule jednostruke. Niz polinoma $(p_i)_{i \leq k}$ nazivamo Šturmovim nizom za polinom $p = p_0$, ako je

(i) $Z(p_k) = \emptyset$ tj. p_k nema realnih nula.

(ii) Za $i \geq 0$, p_i i p_{i+1} nemaju zajedničkih nula.

(iii) Ako je za $1 \leq i < k$ i $\alpha \in R$, $p_i(\alpha) = 0$, onda je $p_{i-1}(\alpha)p_{i+1}(\alpha) < 0$.

(iv) Ako je za $\alpha \in R$, $p(\alpha) = 0$, onda $p_0 p_1$ menja znak sa $-$ na $+$, pri prolasku kroz α.

2.10.3. Definicija. Neka je $p \in R[x]$ i $(p_i)_{i \leq k}$ Šturmov niz za p. Funkciju $W : R \to N$, definišemo tako da je za $a \in R$, $W(a)$ broj promena znaka u nizu $(p_i(a))_{i \leq k}$, ili preciznije

$$W(a) = |\{i \leq k : p_i(a)p_{i+1}(a) < 0\}|.$$

2.10.4. Teorema. *Neka je $p \in R[x]$, $(p_i)_{i \leq k}$ Šturmov niz za p, i $a, b \in R$, $a < b$. Broj nula polinoma p u intervalu (a, b) jednak je $W(a) - W(b)$.*

Dokaz. Neka je $\alpha \in (a, b)$. Za α postoje tri mogućnosti:

1^0. Za svako $i \leq k$, $p_i(\alpha) \neq 0$.

2^0. Postoji $1 \leq i < k$, tako da je $p_i(\alpha) = 0$.

3^0. $p(\alpha) = 0$.

Pokazaćemo da u prva dva slučaja funkcija W ne menja vrednost pri prolasku kroz α, a u trećem slučaju W se smanji za jedan. Time će biti dokazano, da se W od a do b smanjila za onaj broj koliko je bilo nula polinoma p u intervalu (a, b).

1^0. Prema Tvrđenju 2.10.1., za svako $i \leq k$, postoji $\epsilon_i > 0$, tako da p_i ne menja znak u okolini $(\alpha - \epsilon_i, \alpha + \epsilon_i)$. Neka je $\epsilon = min\{\epsilon_i : i \leq k\}$. Tada u okolini $(\alpha - \epsilon, \alpha + \epsilon)$, nijedan od polinoma Šturmovog niza ne menja znak, pa se ni vrednost W funkcije ne menja.

2^0. Neka je $1 \leq i < k$, i neka je $p_i(\alpha) = 0$. Ovde smo iskoristili uslov (i) jer smo isključili mogućnost $i = k$. Prema uslovu (iii), $p_{i-1}(\alpha) \cdot p_{i+1}(\alpha) < 0$. Mi ćemo analizirati slučaj $p_{i-1}(\alpha) < 0$ i $p_{i+1}(\alpha) > 0$. Tada postoji $\epsilon > 0$, tako da je $p_{i-1}(x) < 0$ i $p_{i+1}(x) > 0$, za svako $x \in I = (\alpha - \epsilon, \alpha + \epsilon)$. Bez obzira na vrednost $p_i(\alpha - \epsilon)$, u nizu $p_{i-1}(\alpha - \epsilon)$, $p_i(\alpha - \epsilon)$, $p_{i+1}(\alpha - \epsilon)$ ima jedna promena. Bez obzira na vrednost $p_i(\alpha + \epsilon)$, u nizu $p_{i-1}(\alpha + \epsilon)$, $p_i(\alpha + \epsilon)$, $p_{i+1}(\alpha + \epsilon)$ ima jedna promena. Dakle, W funkcija ne menja vrednost pri prolasku kroz α.

3^0. Neka je $p_(\alpha) = 0$. Prema uslovu (ii), $p_1(\alpha) \neq 0$. Mi ćemo razmotriti slučaj $p_1(\alpha) > 0$. Drugi slučaj analizira se analogno. Prema prethodnom tvrđenju, postoji $\epsilon > 0$ tako da je $p_1(x) > 0$ za $x \in (\alpha - \epsilon, \alpha + \epsilon)$.

Prema uslovu (iv), postoji $\epsilon > 0$, tako da je $pp_1(x) < 0$, za $x \in (\alpha - \epsilon, \alpha)$ i $pp_1(x) > 0$, za svako $x \in (\alpha, \alpha + \epsilon)$. Otuda je $p(x) < 0$, za $x \in (\alpha - \epsilon, \alpha)$, i $p(x) > 0$ za $x \in (\alpha, \alpha + \epsilon)$. Otuda u $\alpha - \epsilon$ niz p, p_1 ima jednu promenu, a u $\alpha + \epsilon$ nema nijednu. Dakle, pri prolasku kroz α gubi se jedna promena, tj. $W(\alpha)$ se smanji za 1. To je i trebalo dokazati. □

Iz prethodne teoreme zaključujemo da bi naše pitanje 2. bilo rešeno, kada bi znali kako da napravimo Šturmov niz za dati polinom. Algoritam nam daje sledeće tvrđenje.

2.10.5. Tvrđenje. *Neka je $p \in R[x]$ polinom koji nema višestrukih nula.*

Niz polinoma $(p_i)_{i\leq k}$ *definisan tako da je:*

$$\begin{aligned} p_0 &= p \\ p_1 &= p' \\ p_{i-1} &= p_i q_i - p_{i+1}, \qquad \mathrm{st}\,(p_{i+1} < st(p_i) \\ &\vdots \\ p_{k-1} &= p_k q_k. \end{aligned}$$

je Šturmov niz za polinom p.

Dokaz. Najpre, evidentno je da ovaj niz jednakosti podseća na Euklidov algoritam za polinome p, p', stim što je u svakom koraku ostatku promenjen znak. Na isti način kao kod Euklidovog algoritma pokazuje se da je postupak konačan, i da se na kraju dobija deljenje bez ostatka, kao i da je $p_k = (p, p') = (p_i, p_{i+1})$, za $1 \leq i < k$.

(i) Otuda odmah sledi zadovoljenje uslova (i). Zaista, ako bi p_k imao realnu nulu, to bi bila nula i za p i za p', dakle p bi imao višestruku nulu, suprotno pretpostavci.

(ii) Neka je sada $i < k$, i pretpostavimo da p_i i p_{i+1} imaju zajedničku nulu α. Tada bi imali $x - \alpha \mid (p_i, p_{i+1})$, dakle $x - \alpha \mid p_n$, suprotno pokazanoj osobini (i).

(iii) Neka je za $1 \leq i < k$ i $\alpha \in R$, $p_i(\alpha) = 0$. Zamenom u jednakosti $p_{i-1} = p_i q_i - p_{i+1}$, $x = \alpha$, dobijamo $p_{i-1}(\alpha) = -p_{i+1}(\alpha)$. Kako su ti brojevi, prema (ii), različiti od nule, to je $p_{i-1}(\alpha)p_{i+1}(\alpha) < 0$.

(iv) Ako je za $\alpha \in R$, $p(\alpha) = 0$. Kako je α jednostruka nula polinoma p, to $p$menja znak pri prolasku kroz α. Analiziraćemo slučaj kada je to promena sa $-$ na $+$. Drugi slučaj analizira se analogno. Dakle, za neko $\epsilon > 0$, $p(x) < 0$ za $x \in (\alpha - \epsilon, \alpha)$, i $p(x) > 0$ za $x \in (\alpha, \alpha + \epsilon)$. Dakle, p je u α rastuća funkcija, pa je $p'(\alpha) > 0$. Otuda je za $x \in (\alpha - \epsilon, \alpha + \epsilon)$, $p'(x) > 0$. Dakle, za $x \in (\alpha - \epsilon, \alpha)$, $p_0(x)p_1(x) < 0$, a za $x \in (\alpha, \alpha + \epsilon)$, $p_0(x)p_1(x) > 0$. Time smo pokazali da $p_0 p_1$ menja znak sa $-$na $+$ pri prolasku kroz α . □

2.10.5. Primer. Računamo Šturmov niz za polinom $p = x^5 + 2x^4 - 7x^3 + 2x^2 + x - 5$. Dobijamo niz

$$\begin{aligned} p_0 &= x^5 + 2x^4 - 7x^3 + 2x^2 + x - 5 \\ p_1 &= p' = 5x^4 + 8x^3 - 21x^2 + 4x + 1 \\ p_2 &= 86x^3 - 72x^2 - 12x + 127 \\ p_3 &= 1494x^2 + 249x + 2514 \\ p_4 &= 63651621x + 6798696 \\ p_5 &= 1. \end{aligned}$$

Kako su sve nule polinoma realnih polinoma p. Međutim računski je jednostavnije ako postupimo na sledeći način: Svaki od polinoma iz Šturmovog niza ima granicu M_i,$i \leq p$, tako da za $|x| > M_i$ najstariji čla određuje znak polinoma. Označimo sa ∞ maximum tih granica. Sada u takozvanim $-\infty$ i ∞ ne moramo računati vrednosti polinoma, već samo gledamo znak najstarijeg člana. TAko dobijamo,

	p_0	p_1	p_2	p_3	p_4	W
$-\infty$	$-$	$+$	$-$	$+$	$-$	4
∞	$+$	$+$	$+$	$+$	$-$	1

Dakle, p ima $4 - 1 = 3$ realne nule.

2.11. Polinomi više promenljivih

Polinomi više promenljivih predstavljaju prirodnu generalizaciju polinoma jedne promenljive.

2.11.1. Definicija. Neka je $n \in N$. $D_n = (-\infty \cup N^n, \leq)$, gde je $\leq$ leksikografsko uređenje i $-\infty$ je najmanji element uređenja.

2.11.2. Tvrđenje. *$(D_n, \leq)$ je prebrojivo, linearno i dobro uređenje.*

2.11.3. Definicija. Neka je $n \in N$, $d \in N^n$ i $(a_s)_{s \in N^n}$ niz realnih brojeva, indeksiran skupom N^n, takav da je $d = max\{s : a_s \neq 0\}$. Izraz $p(x_1, \ldots, x_n) = \sum_{s \leq d} a_s \prod_{i \in s} x_i$ nazivamo polinomom stepena d od promenljivih $x_1, \ldots, x_n$, sa nizom koeficijenata $(a_i)_{i \in N}$. Koeficijent a_d nazivamo vodećim koeficijentom polinoma $p(x_1, \ldots, x_n)$. 0 je polinom stepena $-\infty$, sa nizom koeficijenata $(0)_{s \in N^n}$. Izraz je polinom ako je polinom stepena d za neko $d \in D_n$. Skup polinoma od promenljivih $x_1, \ldots, x_n$ označavamo sa $R[x_1, \ldots, x_n]$. Funkcija $st : R[x_1, \ldots, x_n] \to D_n$ definisana je tako da je st (p) jednak stepenu polinoma p. Koficijent a_d nazivamo vodećim koeficijentom polinoma p.

Jednakost polinoma, operacije sabiranja i množenja definišu se kao kod polinoma jedne promenljive. I ovde važe teoreme o stepenu zbira i proizvoda, kao i tvrđenje analogno Tvrđenju 2.1.5., o osobinama operacija $+$ i $\cdot$.

Često se promenljive polinoma pišu kao $x, y, z, \ldots, u, \ldots$, pri čemu se podrazumva da je $x = x_1$, $y = x_2$, $z = x_3$, $\ldots$. Mi ćemo sada posebnu pažnju posvetiti jednoj važnoj specijalnoj klasi polinoma - simetričnim polinomima više promenljivih.

2.11.4. Definicija. Neka je $p \in R[x_1, \ldots, x_n]$. Polinom p je simetričan polinom ako je

$$p(x_{\tau(1)}, \ldots, x_{\tau(n)}) = p(x_1, \ldots, x_n),$$

za svaku permutaciju τ skupa $\{1, \ldots, n\}$.

2.11.5. Definicija. Neka je $n \in N$. Elementarni simetrični polinomi od promenljivih $x_1, \ldots, x_n$ su:

$$\sigma_1(x_1, \ldots, x_n) = \sum_{i \leq n} x_i$$

$$\sigma_2(x_1, \ldots, x_n) = \sum_{i<j \leq n} x_i x_j$$

$$\vdots$$

$$\sigma_k(x_1, \ldots, x_n) = \sum_{i_1 < \ldots i_k \leq n} \prod_{s \leq k} x_{i_s}$$

$$\vdots$$

$$\sigma_n(x_1, \ldots, x_n) = \prod_{i \leq n} x_i$$

Primetimo da se pomoću elementarnih simetričnih polinoma Vijetove formule mogu predstaviti u obliku

$$\sigma_1(\alpha_1, \ldots, \alpha_n) = -\frac{a_1}{a_0}$$

$$\sigma_2(\alpha_1, \ldots, \alpha_n) = \frac{a_2}{a_0}$$

$$\vdots$$

$$\sigma_k(\alpha_1, \ldots, \alpha_n) = (-1)^k \frac{a_k}{a_0}$$

$$\vdots$$

$$\sigma_n(\alpha_1, \ldots, \alpha_n) = (-1)^n \frac{a_n}{a_0}.$$

Dakle, koeficijenti polinoma jedne promenljive p, do na množenje sa (-1) i a_0, su vrednosti elementarnih simetričnih polinoma u korenima tog polinoma.

2.11.6. Primer. Podsetimo se jednog standardnog zadatka u vezi sa kvadratnim jednačinama. Zadatak je da se odredi vrednost nekog izraza od korena kvadratne jednačine, bez njenog rešavanja. Recimo: Data je kvadratana

jednačina $x^2 + 23x + 59$, treba odrediti vrednost izraza $\alpha^2 + \beta^2$, ako su α i β koreni jednačine. Zadatak se onda varira tako da se traži vrednost izraza $\alpha^3 + \beta^3$, ili $\alpha^2\beta + \alpha\beta^2$. Međutim, to su uvek izrazi simetrični po α i β. Postupak rešavanja je takav da se taj simetrični polinom napiše pomoću elementarnih simetričnih polinoma, čije se vrednosti u α i β čitaju iz Vijetovih pravila. Dakle, ako se traži vrednost $\alpha^2 + \beta^2$, onda imamo

$$\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = (\sigma_1(\alpha, \beta))^2 - 2\sigma_2(\alpha, \beta) = (-23)^2 - 59 = 470.$$

□

Ovaj postupak možemo izvesti i za jednačinu proizvoljnog stepena. To je kod njih još značajnije jer za jednačine viših stepena nemamo postupak za njihovo rešavanje. Postupak se bazira na mogućnosti predstavljanja proizvoljnog simetričnog polinoma kao "kombinacije" elementarnih simetričnih polinoma. Pojasnimo o kakvoj se "kombinaciji" radi.

2.11.7. Tvrđenje. *Neka je* $q \in R[x_1, \ldots, x_n]$. *Polinom* $p(x_1, \ldots, x_n) = q(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n))$ *je simetričan polinom.*

Dokaz. Dakle, polinom p je dobijen tako što je u q_i umesto x_i zamenjeno σ_i. Dakle, gledano kao funkcija, p je kompozicija funkcije q i funkcija σ_i, $i \leq n$. Dokaz izvodimo po definiciji. Svodi se na to da σ_i, kao simetrični, apsorbuju efekte permutacije, tako da njih više nema kada dođe na red da se računa nesimetrični polinom q. Dakle, neka je τ permutacija skupa $\{1, \ldots, n\}$. Tada je

$$\begin{aligned} p(x_{\tau(1)}, \ldots, x_{\tau(n)}) &= q(\sigma_1(x_{\tau(1)}, \ldots, x_{\tau(n)}), \ldots, \sigma_n(x_{\tau(1)}, \ldots, x_{\tau(n)}) \\ &= q(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)) \\ &= p(x_1, \ldots, x_n). \quad \square \end{aligned}$$

Nama je mnogo važniji obrat prethodnog tvrđenja. Pre nego ga formulišemo i dokažemo, dokažimo najpre jednu lemu.

2.11.8. Lema. *Neka je* $p \in R[x_1, \ldots, x_n]$ *simetričan polinom sa najstarijim članom* $ax_1^{m_1} \ldots x_n^{m_n}$. *Tada je* $m_1 \geq \cdots \geq m_n$.

Dokaz. Pretpostavimo suprotno da je za neke $i, j \leq n$, $i < j$ i $m_i < m_j$. Neka je τ permutacija skupa $\{1, \ldots, n\}$ definisana tako da je $\tau(i) = j$, $\tau(j) = i$, i $\tau(k) = k$, za $k \neq i, j$. Tada na osnovu simetričnosti polinoma p, p sadrži i član

$$ax_{\tau(1)}^{m_1} \ldots x_{\tau(i)}^{m_i} \ldots x_{\tau(j)}^{m_j} \ldots x_{\tau(n)}^{m_n} = ax_1^{m_1} \ldots x_i^{m_j} \ldots x_j^{m_i} \ldots x_n.$$

Međutim, u leksikografskom poretku na N^n, $(m_1, \ldots m_j \ldots m_i \ldots m_n) > (m_1, \ldots m_i \ldots m_j \ldots m_n)$, jer na prvoj koordinati na kojoj se razlikuju, naime i-toj, prva n-torka ima koordinatu m_j a druga m_i, i $m_j > m_i$. To je u suprotnosti sa pretpostavkom da je $ax_1 \ldots x_n$ najstariji član polinoma p. □

2.11.9. Teorema. *Svaki simetrični polinom je polinom od elementarnih simetričnih polinoma.*

Dokaz. Transfinitnom indukcijom po stepenu polinoma. Neka je $n \in N^+$, $d \in D_n$ i pretpostavimo da je tvrđenje dokazano za sve simtrične polinome stepena $< d$, iz $R[x_1, \ldots, x_n]$. Neka je $p \in R[x_1, \ldots, x_n]$ polinom stepena $d = (m_1, \ldots, m_n)$. Tada je $p = a_d x_1^{m_1} \ldots x_n^{m_n} + s(x_1, \ldots, x_n)$, gde je $\mathrm{st}(s) < d$. Prema prethodnoj lemi, $m_1 \geq m_2 \cdots \geq m_n$. Neka je $t = a_d {\sigma_1}^{m_1 - m_2} {\sigma_2}^{m_2 - m_3} \ldots {\sigma_n}^{m_n}$. Najstariji član polinoma t jednak je proizvodu broja a_d i najstarijih članova činilaca proizvoda. Kako je najstariji član polnoma σ_i jednak $x_1 \ldots x_i$, to je najstariji član polinoma t

$$a_d {x_1}^{m_1 - m_2} (x_1 x_2)^{m_2 - m_3} \ldots (x_1 x_2 \ldots x_n)^{m_n} = a_d \prod_{i \leq n} x_i^{\sum_{j \geq i} m_j - m_{j+1}}$$
$$= a_d \prod_{i \leq n} x_i^{m_i}$$

Radi lakšeg pisanja sume, u prethodnom računu smo fiktivno dodefinisali $m_{n+1} = 0$. Dakle, $t = a_d x_1^{m_1} \ldots x_n^{m_n} + u(x_1, \ldots, x_n)$, gde je $\mathrm{st}(u) < d$. Tada je $p - t = s - u$, i $\mathrm{st}(p - t) = \mathrm{st}(s - u) < max\{\mathrm{st}(s), \mathrm{st}(u)\} < d$. Dakle, za $p - t$ važi indukcijska hipoteza. Zato postoji polinom $q \in R[x_1, \ldots, x_n]$, tako da je $p - t = q(\sigma_1, \ldots, \sigma_n)$. Tada je $p = t + q(\sigma_1, \ldots, \sigma_n) = a_d {\sigma_1}^{m_1 - m_2} {\sigma_2}^{m_2 - m_3} \ldots {\sigma_n}^{m_n} + q(\sigma_1, \ldots, \sigma_n)$. Dakle, p je polinom od elementarnih simetričnih polinoma $\sigma_1, \ldots, \sigma_n$. □

2.11.10. Primer. Neka je

$$S(x_1, x_2, \ldots, x_n) = \sum_{i \neq j} x_i^3 x_j.$$

S je očigledno simetričan polinom. Umesto da kao u dokazu teoreme snižavamo red polinoma, mi odjednom tražimo sve polinome koji se mogu u svim tim koracima pojaviti u ulozi polinoma p iz prethodnog dokaza ili u ulozi polinoma q u poslednjem koraku. Ako je $ax_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ vodeći član jednog od tih polinoma, onda on zadovoljava sledeće uslove:

1) Zbir izložilaca $\sum_{i \leq n} \alpha_i$, jednak je 4, kao i kod vodećeg, i svih ostalih članova, polaznog polinoma.

2) $(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n) \leq (3, 1, 0 \ldots, 0)$.

3) Niz $(\alpha_i)_{i\leq n}$ je neopadajući.

Odavde zaključujemo da vodeći članovi tih polinoma imaju sledeće stepene: $(3,1,0,\ldots)$, $(2,2,0,\ldots)$, $(2,1,1,0,\ldots)$ i $(1,1,1,1,0,\ldots)$. Otuda se u ulozi polinoma t, i poslednjeg redukovanog p, mogu pojaviti $\sigma_1^2\sigma_2$, σ_2^2, $\sigma_1\sigma_3$i σ_4. Dakle,

$$S = A\sigma_1^2\sigma_2 + B\sigma_2^2 + C\sigma_1\sigma_3 + \sigma_4.$$

Da bi odredili konstante izjednačavamo vrednosti polinoma na levoj i desnoj strani u četiri tačke. Pri tome, zbog lakšeg računa, biramo valuacije sa što većim brojem nula. Međutim valuacije koje imaju najviše jednu vrednost različitu od nule, daju na obe strane trivijalnu jednačinu $0 = 0$. Zato izračunajmo obe strane u $(1,1,0,\ldots)$. Kako je $S = x_1^3x_2 + x_2^3x_1 + \ldots$, $\sigma_1 = x_1 + x_2 + \ldots$, $\sigma_2 = x_1x_2 + \ldots$ i σ_3, σ_4 u svakom sabirku imaju jedan činilac koji dobija vrednost 0, dobijamo jednačinu

$$2 = 4A + 2B.$$

Slično, zamenom $(1,-1,0,\ldots,)$, dobijamo jednačinu $0 = -4A + B$. Rešavajući ovaj sistem, dobijamo $A = \frac{1}{4}$ i $B = 1$.

Zamenom $(1,1,1,0,\ldots)$ dobijamo jednačinu $3 = 27A + 9B + 3C$, odakle je $C = \frac{-17}{4}$.

Konačno, zamenom $(1,1,1,1,0,\ldots)$ dobijamo $6 = 96A + 36B + 16C + D$. Odatle je $D = 14$. Dakle,

$$S = \frac{1}{4}\sigma_1^2\sigma_2 + \sigma_2^2 - \frac{17}{4}\sigma_1\sigma_3 + 14\sigma_4.$$

2.11.11 Primer. Neka su α,β, γ, δ koreni polinoma

$$p = x^4 - x^3 + 3x^2 - x + 1.$$

Naći vrednost izraza $\alpha^3 + \beta^3 + \gamma^3 + \delta^3$. Dakle, ovaj zadatak je analogan zadatku u Primeru 2.11.6., samo za polinom višeg stepena.

Neka je $S(x_1,x_2,x_3,x_4) = x_1^3 + x_2^3 + x_3^3 + x_4^3$, simetričan polinom od četiri promenljive. Na isti način kao i u prethodnom primeru, zaključujemo da su mogući stepeni pomoćnih polinoma $(3,0,\ldots)$, $(2,1,0,\ldots)$ i $(1,1,1,0,\ldots)$. Otuda je

$$S = A\sigma_1^3 + B\sigma_1\sigma_2 + C\sigma_3.$$

Zamenom vrednosti $(1,0,\ldots)$, $(1,1,0,\ldots)$ i $(1,1,1,0,\ldots)$, dobijamo

$$1 = A$$
$$2 = 2^3A + B\cdot 2\cdot 1$$
$$3 = 3^3A + B\cdot 3\cdot 3 + C.$$

Otuda je $A = 1$, $B = -3$ i $C = 3$. Dakle, $S = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$. Prema Vijetovim pravilima imamo da je $\sigma_1(\alpha,\beta,\gamma,\delta) = 1$, $\sigma_2(\alpha,\beta,\gamma,\delta) = -3$ i $\sigma_3(\alpha,\beta,\gamma,\delta) = -1$. Otuda je

$$S(\alpha,\beta,\gamma,\delta) = 7.$$

2.12. Rezultanta dva polinoma

Ovu sekciju možemo da shvatimo i kao ilustraciju prethodne. U situaciji kada ne možemo da nađemo nule polinoma, možemo da nađemo vrednosti simetričnih funkcija od nula polinoma. Rezultanta dva polinoma je jedna od njih.

2.12.1. Definicija. Neka su $p = \sum_{i\le n} a_i x^{n-i} = a_0 \prod_{i\le n}(x-\alpha_i)$ i $q = \sum_{j\le s} b_j x^{s-j} = b_0 \prod_{j\le s}(x-\beta_j)$. Rezultanta polinoma p i q je broj

$$R(p,q) = a_0^s b_0^n \prod_{i\le n}\prod_{j\le s}(\alpha_i - \beta_j).$$

2.12.2. Tvrđenje. *(i) $R(p,q)=0$ akko p i q imaju zajedničkih nula.*
(ii) $R(q,p) = (-1)^{ns} R(p,q)$.
(iii) $R(p,q) = a_0^s \prod_{i\le n} q(\alpha_i)$.
(iv) $R(p,q) = (-1)^{ns} b_0^n \prod_{j\le s} p(\beta_j)$.

Dokaz. (i) $R(p,q) = 0$, akko postoje $i \le n$, $j \le s$, tako da je $\alpha_i - \beta_j = 0$, što je i trebalo pokazati.

(ii) Po definiciji rezultante imamo

$$\begin{aligned}
R(q,p) &= a_0^s b_0^n \prod_{i\le n}\prod_{j\le s}(\beta_j - \alpha_i) \\
&= a_0^s b_0^n \prod_{i\le n}\prod_{j\le s}(-1)(\alpha_i - \beta_j) \\
&= a_0^s b_0^n \prod_{i\le n}(-1)^s \prod_{j\le s}(\alpha_i - \beta_j) \\
&= a_0^s b_0^n (-1)^{ns} \prod_{i\le n}\prod_{j\le s}(\alpha_i - \beta_j) \\
&= (-1)^{ns} R(p,q)
\end{aligned}$$

(iii) Zamenom $x = \alpha_i$ u jednakosti $q = b_0 \prod_{j \le s}(x - \beta_j)$, dobijamo $q(\alpha_i) = b_0 \prod_{j \le s}(\alpha_i - \beta_j)$. Množenjem ovih jednakosti za $i \le n$, i množenjem obe strane sa ${a_0}^s$ dobijamo traženu jednakost.

(iv) Primenom (ii), i (iii) na $R(q, p)$ (zamenjena mesta p i q, odnosno α i β),dobijamo

$$R(p, q) = (-1)^{ns} R(q, p) = (-1)^{ns} b_0^n \prod_{j \le s} p(\beta_j).$$

Dakle, iz vrednosti $R(p, q)$ vidimo da li pilinomi p i q imaju zajedničkih nula. To je ipak beskorisno tvrđenje. Zašto bi pravili taj ogromni proizvod, kad možemo da samo uporedimo spiskove nula za dva polinoma i vidimo da li ima zajedničkih članova. Ideja je ta da je $R(p, q)$ simetrična funkcija i od korena prvog i od korena drugog polinoma. To nam omogućuje da $R(p, q)$ predstavimo kao vrednost nekog polinoma više promenljivih u koeficijentima dvaju polinoma. Upravo to izvodimo u sledećoj teoremi. Pre formulacije podsetimo se jednog pojma iz Linearne algebre.

2.12.3. Definicija. Neka su $\gamma_1, \ldots, \gamma_k \in R$. Vandermondova determinanta je

$$W(\gamma_1, \ldots, \gamma_k) = \begin{vmatrix} {\gamma_1}^{k-1} & {\gamma_2}^{k-1} & \ldots & {\gamma_k}^{k-1} \\ {\gamma_1}^{k-2} & {\gamma_2}^{k-2} & \ldots & {\gamma_k}^{k-2} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_1 & \gamma_2 & \ldots & \gamma_k \\ 1 & 1 & \ldots & 1. \end{vmatrix}$$

2.12.4. Tvrđenje. $W(\gamma_1, \ldots, \gamma_k) = \prod_{1 \le i < j \le k}(\gamma_i - \gamma_j)$.

2.12.5. Teorema. *Neka su oznake kao u Definiciji 2.12.1. Tada je*

$$R(p, q) = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & 0 & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_n & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_n \\ b_0 & b_1 & \ldots & b_s & 0 & 0 & \ldots & 0 \\ 0 & b_0 & b_1 & \ldots & b_s & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_s \end{vmatrix}.$$

Dokaz. U dokazu koristimo Vandermondovu determinantu reda $s + n$, $W = W(\beta_1, \ldots, \beta_s, \alpha_1, \ldots, \alpha_n)$. Primetimo da u $(\beta_1, \ldots, \beta_s, \alpha_1, \ldots, \alpha_n)$, β_i prethodi β_j, za $1 \le i < j \le s$, α_i prethodi α_j, za $1 \le i < j \le n$, i β_i prethodi

α_j, za svako $i \leq s$ i $j \leq n$. Prema Tvrdenju 2.12.4.,

$$a_0^s b_0^n \cdot W(\beta_1, \ldots, \beta_s, \alpha_1, \ldots, \alpha_n) =$$

$$= \prod_{1 \leq i < j \leq s} (\beta_i - \beta_j) \cdot \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \cdot a_0^s b_0^n \prod_{j \leq s, i \leq n} (\beta_j - \alpha_i)$$

$$(*) \qquad = W(\beta_1, \ldots, \beta_s) \cdot W(\alpha_1, \ldots, \alpha_n) \cdot R(q, p).$$

Sdruge strane množenjem determinanti D i $W(\beta_1, \ldots, \beta_s, \alpha_1, \ldots, \alpha_n)$ po pravilu za množenje matrica, dobijamo da je determinanta $D \cdot W$ jednaka determinanti

$$\begin{vmatrix}
\sum\limits_{i \leq n} a_i \beta_1^{n+s-i-1} & \ldots & \sum\limits_{i \leq n} a_i \beta_s^{n+s-i-1} & \sum\limits_{i \leq n} a^i \alpha_1^{n+s-i-1} & \ldots & \sum\limits_{i \leq n} a^i \alpha_n^{n+s-i-1} \\
\sum\limits_{i \leq n} a_i \beta_1^{n+s-i-2} & \ldots & \sum\limits_{i \leq n} a_i \beta_s^{n+s-i-2} & \sum\limits_{i \leq n} a_i \alpha_1^{n+s-i-2} & \ldots & \sum\limits_{i \leq n} a_i \alpha_n^{n+s-i-2} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\sum\limits_{i \leq n} a_i \beta_1^{n-i} & \ldots & \sum\limits_{i \leq n} a_i \beta_s^{n-i} & \sum\limits_{i \leq n} a_i \alpha_1^{n-i} & \ldots & \sum\limits_{i \leq n} a_i \alpha_n^{n-i} \\
\sum\limits_{i \leq s} b_i \beta_1^{n+s-i-1} & \ldots & \sum\limits_{i \leq s} b_i \beta_n^{n+s-i-1} & \sum\limits_{i \leq s} a^i \alpha_1^{n+s-i-1} & \ldots & \sum\limits_{i \leq s} a^i \alpha_s^{n+s-i-1} \\
\sum\limits_{i \leq s} b_i \beta_1^{n+s-i-2} & \ldots & \sum\limits_{i \leq s} b_i \beta_n^{n+s-i-2} & \sum\limits_{i \leq s} b_i \alpha_1^{n+s-i-2} & \ldots & \sum\limits_{i \leq s} b_i \alpha_s^{n+s-i-2} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\sum\limits_{i \leq s} b_i \beta_1^{s-i} & \ldots & \sum\limits_{i \leq s} b_i \beta_n^{s-i} & \sum\limits_{i \leq s} b_i \alpha_1^{s-i} & \ldots & \sum\limits_{i \leq s} b_i \alpha_s^{s-i}
\end{vmatrix}$$

Izvlačeći zajedničke faktore sabiraka ispred suma dobijamo, da je $D \cdot W$ jednaka determinanti

$$\begin{vmatrix}
\beta_1^{s-1} \sum\limits_{i \leq n} a_i \beta_1^{n-i} & \ldots & \beta_s^{s-1} \sum\limits_{i \leq n} a_i \beta_s^{n-i} & \alpha_1^{s-1} \sum\limits_{i \leq n} a_i \alpha_1^{n-i} & \ldots & \alpha_n^{s-1} \sum\limits_{i \leq n} a_i \alpha_n^{n-i} \\
\beta_1^{s-2} \sum\limits_{i \leq n} a_i \beta_1^{n-i} & \ldots & \beta_s^{s-2} \sum\limits_{i \leq n} a_i \beta_s^{n-i} & \alpha_1^{s-2} \sum\limits_{i \leq n} a_i \alpha_1^{n-i} & \ldots & \alpha_n^{s-2} \sum\limits_{i \leq n} a_i \alpha_n^{n-i} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\sum\limits_{i \leq n} a_i \beta_1^{n-i} & \ldots & \sum\limits_{i \leq n} a_i \beta_s^{n-i} & \sum\limits_{i \leq n} a_i \alpha_1^{n-i} & \ldots & \sum\limits_{i \leq n} a_i \alpha_n^{n-i} \\
\beta_1^{n-1} \sum\limits_{i \leq n} b_i \beta_1^{s-i} & \ldots & \beta_s^{n-1} \sum\limits_{i \leq n} b_i \beta_s^{s-i} & \alpha_1^{n-1} \sum\limits_{i \leq n} b_i \alpha_1^{s-i} & \ldots & \alpha_n^{n-1} \sum\limits_{i \leq s} b_i \alpha_n^{s-i} \\
\beta_1^{n-2} \sum\limits_{i \leq n} b_i \beta_1^{s-i} & \ldots & \beta_s^{n-2} \sum\limits_{i \leq n} b_i \beta_s^{s-i} & \alpha_1^{n-2} \sum\limits_{i \leq n} b_i \alpha_1^{s-i} & \ldots & \alpha_n^{n-2} \sum\limits_{i \leq s} b_i \alpha_n^{s-i} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\sum\limits_{i \leq s} b_i \beta_1^{s-i} & \ldots & \sum\limits_{i \leq n} b_i \beta_s^{s-i} & \sum\limits_{i \leq s} b_i \alpha_1^{s-i} & \ldots & \sum\limits_{i \leq s} b_i \alpha_n^{s-i}
\end{vmatrix}$$

Očigledno su izrazi u sumama jednaki vrednostima polinoma p i q u α_i i β_i.

Zato je

$$D\cdot W=\begin{vmatrix} \beta_1^{s-1}p(\beta_1) & \dots & \beta_s^{s-1}p(\beta_s) & \alpha_1^{s-1}p(\alpha_1) & \dots & \alpha_n^{s-1}p(\alpha_n)\\ \beta_1^{s-2}p(\beta_1) & \dots & \beta_s^{s-2}p(\beta_s) & \alpha_1^{s-2}p(\alpha_1) & \dots & \alpha_n^{s-2}p(\alpha_n)\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ p(\beta_1) & \dots & p(\beta_s) & p(\alpha_1) & \dots & p(\alpha_n)\\ \beta_1^{n-1}q(\beta_1) & \dots & \beta_s^{n-1}q(\beta_s) & \alpha_1^{n-1}q(\alpha_1) & \dots & \alpha_n^{n-1}q(\alpha_n)\\ \beta_1^{n-2}q(\beta_1) & \dots & \beta_s^{n-2}q(\beta_s) & \alpha_1^{n-2}q(\alpha_1) & \dots & \alpha_n^{n-2}q(\alpha_n)\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ q(\beta_1) & \dots & q(\beta_s) & q(\alpha_1) & \dots & q(\alpha_n) \end{vmatrix}.$$

Kako je $q(\beta_i)=0$, za $i\le s$, i $p(\alpha_i)=0$, za $i\le n$, to dobijamo

$$D\cdot W=\begin{vmatrix} \beta_1^{s-1}p(\beta_1) & \dots & \beta_s^{s-1}p(\beta_s) & 0 & \dots & 0\\ \beta_1^{s-2}p(\beta_1) & \dots & \beta_s^{s-2}p(\beta_s) & 0 & \dots & 0\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ p(\beta_1) & \dots & p(\beta_s) & 0 & \dots & 0\\ 0 & \dots & 0 & \alpha_1^{n-1}q(\alpha_1) & \dots & \alpha_n^{n-1}q(\alpha_n)\\ 0 & \dots & 0 & \alpha_1^{n-2}q(\alpha_1) & \dots & \alpha_n^{n-2}q(\alpha_n)\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 0 & \dots & 0 & q(\alpha_1) & \dots & q(\alpha_n) \end{vmatrix}.$$

Iz i-te od prvih s kolona možemo izvući zajednički faktor $p(\beta_i)$, $i\le s$, a iz i-te od preostalih n kolona, zajednički faktor $q(\alpha_i)$, $i\le n$.

$$D\cdot W=\prod_{i\le s}p(\beta_i)\cdot\prod_{i\le n}q(\alpha_i)\cdot\begin{vmatrix} \beta_1^{s-1} & \dots & \beta_s^{s-1} & 0 & \dots & 0\\ \beta_1^{s-2} & \dots & \beta_s^{s-2} & 0 & \dots & 0\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 1 & \dots & 1 & 0 & \dots & 0\\ 0 & \dots & 0 & \alpha_1^{n-1} & \dots & \alpha_n^{n-1}\\ 0 & \dots & 0 & \alpha_1^{n-2} & \dots & \alpha_n^{n-2}\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ 0 & \dots & 0 & 1 & \dots & 1 \end{vmatrix}.$$

Kako detreminanta ima blok dijagonalni oblik, ona je jednaka proizvodu blokova. Svaki od tih blokova je Vandermondova determinanta, pa dobijamo

$$D\cdot W=\prod_{i\le s}p(\beta_i)\cdot\prod_{i\le n}q(\alpha_i)\cdot W(\beta_1,\dots,\beta_s)\cdot W(\alpha_1,\dots,\alpha_s)$$

Množeći obe strane jednakosti sa $a_0^s b_0^n$ i zamenjujući vrednost za $a_0^s b_0^n W$ iz (*), dobijamo

$$DW(\alpha_1, \ldots, \alpha_n)W(\beta_1, \ldots, \beta_s)R(q,p) = b_0^n \prod_{i \le s} p(\beta_i) \cdot a_0^s \prod_{i \le n} q(\alpha_i) \cdot W(\beta_1, \ldots, \beta_s) \cdot W(\alpha_1, \ldots, \alpha_s).$$

Prema Tvrđenju 2.12.2., $R(q,p) = b_0^n \prod_{i \le s} p(\beta_i)$ i $R(p,q) = a_0^s \prod_{i \le n} q(\alpha_i)$. Posle zamene, na osnovu ovih jednakosti, posle skraćivanja jednakih izraza na obema stranama, dobijamo

$$DR(q,p) = R(q,p)R(p,q).$$

Posle skraćivanja dobijamo $D = R(p,q)$. □

Diskriminanta

2.12.6. Definicija. Neka je $p = \sum_{i \le n} a_i x^{n-i} = a_0 \prod_{i \le n}(x - \alpha_i)$. Diskriminanta polinoma p je broj

$$D(p) = a_0^{2n-2} \prod_{i<j} (\alpha_j - \alpha_i)^2.$$

2.12.7. Tvrđenje. *$D(p) = 0$ akko p ima višestrukih nula.*

Dokaz. $D(p) = 0$ akko je jedan od činilaca u proizvodu jednak 0, tj. $\alpha_i = \alpha_j$ za neke $1 \le i < j \le n$. □

Kao u prethodnom delu, da bi diskriminanta bila od koristi treba da je izračunamo u funkciji koeficijenata polinoma.

2.12.8. Teorema. *Neka je $p = \sum_{i \le n} a_i x^{n-i}$, i p' izvod polinoma p.*

$$R(p,p') = (-1)^{\binom{n}{2}} a_0 D(p).$$

Dokaz. Kako je $\mathrm{st}(p') = n - 1$, prema Tvrđenju 2.12.2.,

$$R(p,p') = a_0^{n-1} \prod_{i \le n} p'(\alpha_i).$$

Zato izračunajmo vrednosti $p'(\alpha_i)$, $i \leq n$.

$$p'(x) = a_0 \sum_{k \leq n} \prod_{j \neq k} (x - \alpha_j)$$

$$p'(\alpha_i) = a_0 \sum_{k \leq n} \prod_{j \neq k} (\alpha_i - \alpha_j).$$

U poslednjoj sumi, za $k \neq i$, $\prod_{j \neq k}(\alpha_i - \alpha_j)$ sadrži činilac $\alpha_i - \alpha_i = 0$. Dakle, jedini sabirak u sumi različit od nule dobija se za $k = i$. Zato je

$$p'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j).$$

Otuda je, prema Tvrđenju 2.12.2.,

$$\begin{aligned} R(p, p') &= a_0^{n-1} \prod_{i \leq n} p'(\alpha_i) \\ &= a_0^{n-1} \prod_{i \leq n} a_0 \prod_{j \neq i} (\alpha_i - \alpha_j) \\ &= a_0^{2n-1} \prod_{i \leq n} \prod_{j \neq i} (\alpha_i - \alpha_j). \\ &= a_0^{2n-1} \prod_{1 \leq i \neq j \leq n} (\alpha_i - \alpha_j). \end{aligned}$$

Neka je $D = \{(i, j) : 1 \leq i < j \leq n\}$, i $E = \{(i, j) : 1 \leq j < i \leq n\}$. Tada imamo

$$R(p, p') = a_0^{2n-1} \prod_{D} (\alpha_i - \alpha_j) \prod_{E} (\alpha_i - \alpha_j).$$

Ako u drugom proizvodu zamenimo promenljive i i j, tada $(i, j) \in D$. Zatim u prvom proizvodu iz svakog činioca izvučemo -1, pa dobijamo

$$\begin{aligned} R(p, p') &= a_0^{2n-1} \prod_{D} (\alpha_i - \alpha_j) \prod_{D} (\alpha_j - \alpha_i) \\ &= a_0^{2n-1} (-1)^{\binom{n}{2}} \prod_{D} (\alpha_j - \alpha_i) \prod_{D} (\alpha_j - \alpha_i) \\ &= a_0^{2n-1} (-1)^{\binom{n}{2}} \prod_{D} (\alpha_j - \alpha_i)^2 \\ &= a_0 (-1)^{\binom{n}{2}} D(p). \end{aligned}$$

Time je tvrđenje dokazano. □

2.12.9. Primer. Neka je $p = ax^2 + bx + c$. Tada je $p' = 2ax + b$.

$$R(p, p') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix}$$

Izračunavanjem determinante dobijamo $R(p, p') = 4a^2c - ab^2$. Zato je $D(p) = -\frac{R(p,p')}{a} = b^2 - 4ac$.

2.12.10. Primer. Neka je $p = x^3 + px + q$. Tada je $p' = 3x^2 + p$, pa imamo

$$R(p, p') = \begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix}.$$

Izračunavanjem determinante dobijamo $R(p, p') = 4p^3 + 27q^2$. Zato je $D(p) = -R(p, p') = -4p^3 - 27q^2$.

2.14 Racionalne funkcije

2.14.1. Definicija. Neka su $p, q \in R[x]$, $q \neq 0$. Racionalna funkcija je izraz $\frac{p}{q}$. Skup racionalnih funkcija označavamo sa $R(x)$. $\frac{p}{q}$ je prava racionalna funkcija ako je $\mathrm{st}\,(p) < \mathrm{st}\,(q)$.

Polinome smatramo racionalnim funkcijama tako što polinom p identifikujemo sa racionalnom funkcijom $\frac{p}{1}$. Odmah na početku definišimo jednakost dveju racionalnih funkcija.

$$\frac{p}{q} = \frac{s}{t} \Leftrightarrow pt = qs$$

Operacije sabiranja i množenja definišemo po koordinatama. Dakle,

$$\frac{p}{q} + \frac{s}{t} = \frac{pt + qs}{qt}$$
$$\frac{p}{q} \cdot \frac{s}{t} = \frac{ps}{qt}.$$

Obe operacije su komutativne i asocijativne. Važi i distributivnost $\cdot$ prema $+$.

2.14.2. Tvrđenje. *Svaka racionalna funkcija je zbir polinoma i prave racionalne funkcije.*

Dokaz. Dokaz sledi direktno iz Tvrđenja 2.2.1. Dakle, neka je $\frac{p}{q} \in R(x)$. Neka su $t, r \in R[x]$, tako da je $p = qt + r$, $\mathrm{st}(r) < \mathrm{st}(q)$. Tada je prema definiciji jednakosti racionalnih funkcija $\frac{p}{q} = \frac{tq+r}{q} = t + \frac{r}{q}$. Kako je $\mathrm{st}(r) < \mathrm{st}(q)$, to je $\frac{r}{q}$ prava racionalna funkcija.

2.14.3. Lema. *Neka je $\frac{p}{uv}$ prava racionalna funkcija i $(u, v) = 1$. Postoje $r, t \in R[x]$, tako da je $\mathrm{st}(t) < \mathrm{st}(u)$, $\mathrm{st}(r) < \mathrm{st}(v)$, i*

$$\frac{p}{uv} = \frac{t}{u} + \frac{r}{v}.$$

Dokaz. Prema Bezu-ovoj teoremi, kako je $(u, v) = 1$, to postoje $q, w \in R[x]$, tako da je $p = qu + vw$. Podelimo polinom q sa v. Dakle, $q = vs + r$, gde je $\mathrm{st}(r) < \mathrm{st}(v)$. Ako vrednost za q zamenimo u izrazu za p, dobijamo

$$p = (vs + r)u + vw = ru + (su + w)v.$$

Označimo $su + w$ sa t. Tada je $p = ru + tv$, pa je na osnovu definicije jednakosti, $\frac{p}{uv} = \frac{r}{v} + \frac{t}{u}$. Već smo pokazali da je $\mathrm{st}(r) < \mathrm{st}(v)$. Ostaje da pokažemo da je $\mathrm{st}(t) < \mathrm{st}(u)$. To pokazujemo ne na osnovu sastavnih delova od t, već na osnovu veze $p = ru + tv$, odnosno $tv = p - ru$. Dakle, kako je $\mathrm{st}(r) < \mathrm{st}(v)$, to je $\mathrm{st}(ru) < \mathrm{st}(uv)$. Kako je po pretpostavci $\mathrm{st}(p) < \mathrm{st}(uv)$, to je na osnovu nejednakosti za stepen zbira (razlike) polinoma $\mathrm{st}(tv) = \mathrm{st}(p - ru) < \mathrm{st}(uv)$. Na osnovu formule za stepen proizvoda dobijamo $\mathrm{st}(t) + \mathrm{st}(v) < \mathrm{st}(u) + \mathrm{st}(v)$. Skraćivanjem jednakih brojeva sa raznih strana nejednakosti, dobijamo $\mathrm{st}(t) < \mathrm{st}(u)$. □

Neka je $\frac{p}{q} \in R(x)$ prava racionalna funkcija. Prema Tvrđenju 2.8.13., je $q(x) = q_1^{m_1} \cdot \ldots \cdot q_k^{m_k}$, za neke različite ireducibilne polinome $q_1, \ldots, q_k$, i $m_1, \ldots, m_k \in N^+$. Kako su $q_1, \ldots, q_k$, dva po dva uzajamno prosti polinomi, to prema prethodnoj lemi postoje polinomi $p_1, \ldots, p_k$, takvi da je $\mathrm{st}(p_i) < \mathrm{st}(q_i^{m_i})$, $i \leq k$, i

$$(*) \qquad \frac{p}{q} = \frac{p_1}{q_1} + \ldots \frac{p_k}{q_k}.$$

Prednost oblika na desnoj strani jednakosti je u tome što imamo jednostavnije racionalne funkcije od funkcije na levoj strani, u smislu da imaju imenilac manjeg stepena i bolje majoriran brojilac. Cena za taj dobitak je što umesto jedne, imamo k racionalnih funkcija. Međutim u situacijama

gde na racionalne funkcije primenjujemo operatore koji se "dobro slažu" sa zbirom, a loše sa količnikom, to je ogromno poboljšanje. Tipičan primer je integracija racionalnih funkcija.

Racionalne funkcije na desnoj strani jednakosti mogu se i dalje pojednostaviti, tako da za brojilac imamo još bolje majoriranje stepena. Najpre uvedimo jednu definiciju.

2.14.4. Definicija. Neka je $m \in N^+$. Prava racionalna funkcija $\frac{p}{q^m}$ je elementarna racionalna funkcija, ako je q ireducibilan polinom i $\mathrm{st}(p) < \mathrm{st}(q)$.

Primetimo da je uslov drastično pojačan u odnosu na zahtev da je ta racionalna funkcija prava racionalna funkcija. Zaista, uslov da je $\frac{p}{q^m}$ prava racionalna funkcija je ekvivalentan uslovu $\mathrm{st}(p) < \mathrm{st}(q^m) = m \cdot \mathrm{st}(q)$. Kod elementarne racionalne funkcije zahteva se da je $\mathrm{st}(p) < \mathrm{st}(q)$, dakle od stepena osnove imenioca.

2.14.5. Teorema. *Svaka prava racionalna funkcija je zbir elementarnih ravionalnih funkcija.*

Dokaz. Prema formuli (*), tvrđenje je dovoljno dokazati za racionalne funkcije oblika $\frac{p}{q^m}$, gde je $m \in N^+$, q ireducibilan polinom i $\mathrm{st}(p) < m \cdot \mathrm{st}(q)$. To izvodimo tako što p delimo najpre sa q^{m-1}, zatim ostatak sa q^{m-2}, i tako redom. Dakle,

$$
\begin{aligned}
& p = s_1 q^{m-1} + p_1 && \mathrm{st}(p_1) < (m-1)\,\mathrm{st}(q) \\
& p_1 = s_2 q^{m-2} + p_2 && \mathrm{st}(p_2) < (m-2)\,\mathrm{st}(q) \\
(**) \qquad & p_2 = s_3 q^{m-3} + p_3 && \mathrm{st}(p_3) < (m-3)\,\mathrm{st}(q) \\
& \vdots && \vdots \\
& p_{m-2} = s_{m-1} q + p_{m-1} && \mathrm{st}(p_{m-1}) < \mathrm{st}(q).
\end{aligned}
$$

Dokazaćemo da je $\mathrm{st}(s_i) < stq$, za $i \leq m-1$. Kako je $s_i q^{m-i} = p_{i-1} - p_i$ i $\mathrm{st}(p_{i-1}), \mathrm{st}(p_i) < (m-i+1)\,\mathrm{st}(q)$, to je $\mathrm{st}(s_i q^{m-i}) < (m-i+1)\,\mathrm{st}(q)$. Koristeći formulu za stepen proizvoda polinoma, dobijamo

$$\mathrm{st}(s_i) + (m-i)\,\mathrm{st}(q) < (m-i+1)st(q)\,,$$

odnosno $\mathrm{st}(s_i) < \mathrm{st}(q)$, za $i \leq m-1$. Ako sve jednakosti u (**), podelimo sa q^m a zatim saberemo leve i desne strane, posle potiranja jednakih izraza na levoj i desnoj strani dobijamo

$$\frac{p}{q^m} = \frac{s_1}{q} + \frac{s_2}{q^2} + \cdots + \frac{s_{m-1}}{q^{m-1}} + \frac{p_{m-1}}{q}.$$

Kako je $\mathrm{st}\,(s_i) < \mathrm{st}\,(q)$, za $i \leq m-1$, i $\mathrm{st}\,(p_{m-1}) < \mathrm{st}\,(q)$, sve racionalne funkcije na desnoj strani jednakosti su elementarne racionalne funkcije. □

2.14.6. Primer. Razložićemo racionalnu funkciju

$$\frac{p}{q} = \frac{3x^4 - 13x^3 + 17x^2 - 4x + 1}{x^5 - 5x^4 + 9x^3 - 9x^2 + 8x - 4}.$$

Korak 1. Ako je $\mathrm{st}\,(p) \geq \mathrm{st}\,(q)$, delimo polinome p i q, tako da je $p = sq + r$ i $\mathrm{st}\,(r) < \mathrm{st}\,(q)$. Sada sa r radimo kao da je polinom p, i na samom kraju dodajemo dobijenom rezultatu polinom s. Kako to ovde nije slučaj prelazimo na Korak 2.

Korak 2. Rastavljamo q na proizvod ireducibilnih faktora. Ovaj korak nije algoritamski, niti se uvek može izvesti. U našem primeru to se može izvesti, recimo traženjem racionalnih nula, tako da imamo

$$q = (x-1)(x-2)^2(x^2+1).$$

Korak 3. Rastavljamo $\frac{p}{q}$ u zbir elementarnih racionalnih funkcija. Prema dokazu teoreme, za svaki ireducibilni polinom q_i u faktorizaciji od q, na desnoj strani imamo zbir racionalnih funkcija sa opadajućim izložiocima počevši od izložioca koji se pojavljuje u q_i. Ako je q_i linearni polinom, brojioci racionalnih funkcija koje odgovaraju q_i su konstante. Ako je q_i kvadratni polinom, brojioci racionalnih funkcija koje odgovaraju q_i su linearni polinomi. Dakle,

$$\frac{p}{q} = \frac{A}{x-1} + \frac{B}{(x-2)^2} + \frac{C}{x-2} + \frac{Dx+E}{x^2+1}.$$

Korak 4. Određujemo nepoznate brojioce. Množenjem obeju strana jednakosti sa q, dobijamo

$$\begin{aligned} p = {} & A(x-2)^2(x^2+1) + B(x-1)(x^2+1) + C(x-2)(x-1)(x^2+1) \\ & + (Dx+E)(x-1)(x-2)^2. \end{aligned}$$

Sređivanjem desne strane, i ujednačavanjem koeficijenata uz jednake stepene, dobijamo sistem od 5 jednačina sa 5 nepoznatih. Teorema garantuje da sistem ima rešenja. Ovaj metod je dosta neefikasan, jer sređivanje polinoma i rešavanje sistema nije nimalo prijatno. Mi primenjujemo drugu ideju. Umesto sređivanja polinoma na desnoj strani, dovoljno je obezbediti jednakost u 5 proizvoljno izabranih različitih tačaka. Račun se posebno pojednostavljuje ako zamenjujemo baš nule ireducibilnih polinoma q_i, u našem

primeru $\{1, 2, \pm i\}$. Zaista zamenom $x = 1$ svi sabirci na desnoj strani, osim prvog, imaju vrednost 0 jer sadrže faktor $x - 1$. Zato dobijamo

$$p(1) = 4 = A \cdot (1-2)^2(1^2+1) = 2A.$$

Otuda je odmah $A = 2$. Na isti način, zamenom $x = 2$, dobijamo $B = 1$. Zamenom $x = i$ dobijamo

$$\begin{aligned} p(i) = -13 + 9i &= (Di + E)(i-1)(i-2)^2 \\ &= (Di + E)(7i + 1) \\ &= (E - 7D) + (D + 7E)i. \end{aligned}$$

Izjednačavanjem realnih i imaginarnih delova, dobijamo sistem jednačina čije je rešenje $D = 2$, $E = 1$. Jedino je ostalo da nađemo C. To je tipičan slučaj kada imamo višestruke nule u imeniocu: Samo se najviši stepen dobija direktno zamenom. Problem možemo rešiti tako da zamenimo ma koji broj, recimo $x = 0$. Tada nema nestajanja sabiraka na desnoj strani, ali su nam preostale konstante već poznate.

$$\begin{aligned} p(0) = 1 &= A \cdot 4 \cdot 1 + B \cdot (-1) \cdot 1 + C \cdot -2 \cdot -1 \cdot 1 + E \cdot -1 \cdot (-2)^2 \\ &= 4A - B + 2C - 4E \\ &= 3 + 2C. \end{aligned}$$

Odavde je $C = -1$.

Postoji i za C način sa "nestajanjem", ali najpre treba naći izvod obe strane a zatim zameniti $x = 2$. Svi sabirci koji sadrže $(x-2)^2$, imaju prvi izvod deljiv sa $x - 2$, pa zato postaju jednaki 0 prilikom zamene $x = 2$. Takođe među sabircima u $[(x-1)(x-2)(x^2+1)]'$ za $x = 2$ postaju jednaki nuli svi sem onoga gde je izvod baš uzet od $x - 2$. Zato imamo

$$p'(x) = B(x^2+1) + B(x-1) \cdot 2x + C(x-1)(x^2+1) + \ldots,$$

gde je tačkicama označen deo koji je jednak 0 za $x = 2$. Zato imamo

$$p'(2) = 4 = 5 + 4 + 5C.$$

Otuda je $C = -1$. Dakle

$$\frac{p}{q} = \frac{2}{x-1} + \frac{1}{(x-2)^2} - \frac{1}{x-2} + \frac{2x+1}{x^2+1}.$$

3. ALGEBARSKE STRUKTURE

U prve dve glave videli smo primere nekih važnih konkretnih algebraskih struktura. Videli smo da se celi brojevi i polinomi umnogome slično ponašaju. Postavlja se prirodno pitanje : Iz čega proizilazi ta sličnost. Time prirodno dolazimo do ideje da lociramo izvestan skup zajedničkih osobina koji je "odgovoran za to", a da potom vidimo koje su logičke posledice tih osobina. Strukture koje zadovoljavaju izabrane osobine obuhvataju one strukture od kojih smo pošli (standardne modele) ali i neke druge (nestandardne modele). Na taj način zajedničke osobine standardnih modela mogu se dokazivati istovremeno. Drugi plod ovog pristupa je što nestandardni modeli, iako nusproizvod, ponekad postaju važne matematičke strukture. Izabrane osobine su najčešće rečenice u jeziku prvog reda, i uglavnom su u obliku jednakosti dva terma.

Apstraktne algebarske strukture nastaju ne samo aksiomatizacijom konkretnih objekata već i algebarskim konstrukcijama. Od posebnog su značaja tri algebarske konstrukcije: podalgebra, homomorfna slika i Dekartov proizvod. Kadgod uvedemo novu strukturu, ispitivaćemo kako se ona ponaša u odnosu na ove tri algebarske konstrukcije.

3.1. Grupoidi

U ovoj glavi razmatramo algebarske strukture koje su modeli jezika prvog reda koji sadrži samo konstante (operacijske simbole dužine nula) i operacijske simbole. U najvećem delu ove glave razmatramo modele jezika koji se sastoji iz samo jednog operacijskog znaka dužine 2.

3.1.1. Definicija. *Grupoid je struktura* $\mathcal{G} = (G, *)$, *gde je* $*$ *operacija dužine* 2 *skupa* G.

3.1.2. Primer. Navešćemo primere grupoida iz raznih oblasti matematike, kao i neke "veštačke" koji treba da pokažu veliku slobodu koju imamo u njihovom formiranju. Pri proveri da je neka struktura grupoid treba samo obratiti pažnju da li je operacija dobro definisana tj. da li je ono što nam se

čini da je operacija zaista operacija.
(i) $(N, +)$ gde je N skup prirodnih brojeva, a $+$ operacija sabiranja.
(ii) $(N, \dot{-})$ gde je N skup prirodnih brojeva, a $\dot{-}$ operacija definisana sa:

$$m \dot{-} n = \begin{cases} m - n, & \text{za } m \geq n \\ 0, & \text{za } m < n. \end{cases}$$

Jasno je da smo u slučaju $m < n$ operaciju veštački definisali tek da imamo rezultat u okviru skupa N. Ovo oduzimanje nema mnoge uobičajne osobine oduzimanja. Recimo, ne važi $(m \dot{-} n) + n = m$.
(iii) $(Z, +)$ gde je Z skup celih brojeva, a $+$ operacija sabiranja.
(iv) $(Z_n, +_n)$ gde je $Z_n = \{0, 1, \ldots, n-1\}$, $+_n$ operacija sabiranja po modulu n.
(v) $(Q, +)$, $(R, +)$, $(C, +)$, gde je Q skup racionalnih brojeva, R skup realnih brojeva i C skup kompleksnih brojeva.
(vi) $(R[x], +)$ gde je $R[x]$ skup polinoma sa realnim koeficijentima.
(vii) $(M_{m\times n}, +)$ gde je $M_{m\times n}$ skup matrica tipa $m \times n$.
(viii) $(M_{n\times n}, \cdot)$. Na skupu $M_{m\times n}$ za $m \neq n$ nije definisano množenje matrica, tako da ne postoji grupoid proizvoljnih matrica datog tipa sa operacijom množenja.
(ix) Neka je S fiksirani skup i neka je $P(S)$ partitivni skup od S. Tada je $(P(S), \cap)$ grupoid. Slično se može definisati i grupoid u odnosu na operacije $\cup$ i Δ unije i simetrične diferencije.
(x) Neka je S skup i S^S skup svih preslikavanja skupa S u sebe samog. S^S je grupoid u odnosu na operaciju kompozicije preslikavanja.
(xi) Neka je $W(L)$ skup reči (konačnih nizova simbola) alfabeta L. $W(L)$ čini grupoid u odnosu na operaciju dopisivanja $\smile$ definisanu sa $u \smile v = uv$.

Konačni grupoidi mogu se zadati i tablicom. Grupoid sa n elemenata dobija se tako što se kvadaratna tablica $n \times n$ popuni elementima skupa. Na taj način dobija se n^{n^2} različitih operacija a time i grupoida. U nastavku razmatramo tri osnovne algebarske konstrukcije i njihove osobine.

Podgrupoid.

3.1.3. Definicija. Neka je $\mathcal{G} = (G, *)$ grupoid i $S \subset G$ tako da je $\mathcal{S} = (S, * \restriction S \times S)$ grupoid. Tada kažemo da je *$\mathcal{S}$ podgrupoid od $\mathcal{G}$ određen podskupom S i pišemo $\mathcal{S} < \mathcal{G}$.*

Iz definicije podgrupoida očigledno je da $S \subset G$ određuje podgrupoid od $\mathcal{G}$ akko je zatvoren za operaciju $*$ tj. za svaka dva elementa $a, b \in S$, $a * b \in S$.

3.1.4. Primer. (i) $(N, +) < (Z, +) < (Q, +) < (R, +) < (R[x], +) < (R(x), +)$.

(ii) $(N, \dot{-})$ nije podgrupoid od $(Z, -)$ jer $\dot{-}$ nije restrikcija operacije $-$ na N. Situacija se ne može popraviti predefinisanjem operacije $\dot{-}$; N ne određuje podgrupoid od $(Z, -)$ jer nije zatvoren za operaciju $-$.

(iii) Iz istog razloga $(Z_n, +_n)$ nije podgrupoid od $(Z, +)$. $(n-1)+1 = n \notin Z_n$. On jeste kongruentan modulo n sa 0 koja je u Z_n ali to ne obezbeđuje jednakost u Z.

(iv) Neka je $T \subset S$. $(P(T), \cap) < (P(S), \cap)$.

Homomorfna slika grupoida. Kao što samo ime kaže homomorfizmi su preslikavanja koja čuvaju oblik. Oblik je u algebri način računanja, dakle to su preslikavanja kod kojih se sa slikama računa slično kao sa njihovim originalima. Malo preciznije: Isti se rezultat dobija kada izvršimo računanje u originalu pa preslikamao izlaz, i kada najpre preslikamo ulaze pa računamo sa njihovim slikama. Ipak je to najpreciznije u matematičkom jeziku.

3.1.5. Definicija. Neka su $\mathcal{G}$ i $\mathcal{S}$ grupodi. Preslikavanje $f : G \to S$ je *homomorfizam grupoida* $\mathcal{G}$ *i* $\mathcal{S}$, *u oznaci* $f : \mathcal{G} \to \mathcal{S}$, *ako je za svaki* $a, b \in G$

$$f(a * b) = f(a) * f(b).$$

Ako je f *preslikavanje na, kažemo da je* f *epimorfizam a* $\mathcal{S}$ *homomorfna slika od* $\mathcal{G}$. *Injektivni* $(1-1)$ *homomorfizam je monomorfizam. Bijektivni homomorfizam je izomorfizam. Izomorfizam grupoida u sebe samog je automorfizam.*

3.1.6. Primer. (i) Preslikavanje $f : Z \to Z_n$ definisano sa $f(x) = rem_n(x)$ je epimorfizam. Zaista, neka su $x, y \in Z$ i r i r' njihovi ostaci pri deljenju sa n. Po definiciji je $0 \leq r, r' < n$, i za neke $q, q' \in Z$,

$$x = qn + k$$
$$y = q'n + k\,.$$

Tada je $x + y = (q + q')n + (r + r')$. Ako je $r + r' < n$, tada je $rem_n(x + y) = r + r' = rem_n(x) +_n rem_n(y)$. Ako je $r + r' \geq n$, tada zbog $r + r' < 2n$ imamo da je $r + r' = n + s$, gde je $0 < s < n$. Dakle, $x + y = (q + q' + 1)n + s$ tj. $rem_n(x + y) = s$. Kako je $r +_n r' = s$, to opet imamo $rem_n(x + y) = rem_n(x) +_n rem_n(y)$.

(ii) Neka je S skup i $T \subset S$. Preslikavanje $f : P(S) \to P(T)$ definisano sa $f(A) = A \cap T$ je homomorfizam grupoida $(P(S), \cap)$ i $(P(T), \cap)$. Zaista,

$$f(A \cap B) = (A \cap B) \cap T = A \cap B \cap T = (A \cap T) \cap (B \cap T) = f(A) \cap f(B)\,.$$

Interesantno je da je $P(T)$ istovremeno i podgrupoid i homomorfna slika grupoida $P(S)$. Kada naidu na takvu neobičnu situaciju istraživači u matematici se automatski pitaju: Kako opisati sve podgrupoide od $P(S)$ sa tom

osobinom. Ili još opštije: U kakvim se sve strukturama to može desiti. Nama nije namera da ovde razmatramo taj problem. Samo smo hteli da čitaocu ukažemo na jedan jako čest način iniciranja matematičkih istraživanja.

(iii) Neka je $(R^3, +)$ trodimenzionalni vektorski prostor i $(S, +)$ njegov potprostor koji se sastoji iz vektora koji imaju treću koordinatu 0. Jednostavno se proverava da je preslikavanje $f : R^3 \to S$ definisano sa $f(x, y, z) = (x, y, 0)$ homomorfizam. Opet imamo situaciju kao u tački (ii) ovog primera. Geometrijski ovo preslikavanje predstavlja projekciju prostora R^3 na ravan Oxy.

3.1.7. Tvrđenje. *Neka su $\mathcal{G}$ i $\mathcal{S}$ grupodi i $f : \mathcal{G} \to \mathcal{S}$. $Im(f)$ određuje podgrupoid od $\mathcal{S}$.*

Dokaz. Neka je $\mathcal{G} = (G, *)$ i $\mathcal{S} = (S, \cdot)$. Treba dokazati da je $Im(f)$ zatvoren za operaciju $\cdot$. Dakle, neka je $c, d \in Im(f)$. Tada postoje elementi iz G čiji su oni f slike. Izaberimo $a, b \in G$ tako da je $c = f(a)$ i $d = f(b)$. Tada je

$$\begin{aligned} c \cdot d &= f(a) \cdot f(b) \\ &= f(a * b) \quad \text{(po definiciji homomorfizma)}. \end{aligned}$$

Dakle, $a \cdot b$ je slika elementa $a * b \in G$, te pripada $Im(f)$. □

Dekartov proizvod grupoida.

3.1.8. Definicija. Neka su $\mathcal{G} = (G, *)$ i $\mathcal{S} = (S, \cdot)$ grupoidi. Dekartov proizvod grupoida $\mathcal{G}$ i $\mathcal{S}$, u oznaci $\mathcal{G} \times \mathcal{S}$, je grupoid $(G \times S, \circ)$, gde je operacija $\circ$ definisana tako da je za $(a, b), (a_1, b_1) \in G \times S$,

$$(a, b) \circ (a_1, b_1) = (a * a_1, b \cdot b_1)\,.$$

Primetimo da je u prethodnoj definiciji operacija $\circ$ korektno definisana tako da je rezultat operacije opet element skupa $G \times S$.

U sledećem tvrđenju uočava se jaka veza između Dekartovih proizvoda i homomorfizama.

3.1.9. Tvrđenje. *Neka su oznake kao u prethodnoj definiciji. Preslikavanje $\pi_1 : G \times S \to G$ definisano tako da je za $(a, b) \in G \times S$,*

$$\pi_1((a, b)) = a$$

je epimorfizam, koji nazivamo projekcijom na prvu koordinatu.

Analogno preslikavanje na drugu koordinatu je takođe epimorfizam.

Dokaz. Preslikavanje je *na* jer za proizvoljni element $s \in A$, $\pi_1(t, s) = t$, gde je s proizvoljni element iz S. Proverimo da je π_1 homomorfizam. Neka su

$(a,b),(a_1,b_1) \in G \times S$. Tada je

$$\begin{aligned}\pi_1((a,b) \circ (a_1,b_1)) &= \pi_1((a * a_1, b \cdot b_1)), \text{ (po definiciji operacije } \circ) \\ &= a * a_1, \text{ (po definiciji preslikavanja } \pi_1) \\ &= \pi_1((a,b)) * \pi_1((a_1,b_1)) \quad \square\end{aligned}$$

Slično se može definisati i proizvod proizvoljne familije grupoida.

3.1.10. Definicija. Neka je $\{\mathcal{G}_i : i \in I\}$ indeksirana familija grupoida, gde je za $i \in I$, $\mathcal{G}_i = (G_i, *_i)$. Proizvod ove indeksirane familije grupoida je grupoid $\prod_{i\in I} \mathcal{G}_i = (\prod_{i\in I} G_i, *)$, gde je operacija $*$ definisana tako da je za $f,g : I \to \bigcup_{i\in I} G_i$, $f * g = h$, gde je $h : I \to \bigcup_{i\in I} G_i$ definisano sa

$$h(i) = f(i) *_i g(i).$$

Ako uređeni par grupoida shvatimo kao familiju indeksiranu uređenim parom $(1,2)$, onda je definicija proizvoda dva grupoida specijalni slučaj proizvoda indeksirane familije grupoida. Za Dekartove proizvode proizvoljnih indeksiranih familija grupoida može se lako dokazati tvrđenje analogno Tvrđenju 3.1.9.

3.1.11. Definicija. Neka je $\mathcal{G} = (G,*)$ grupoid. Element $e \in G$ je levi (desni) neutral od $\mathcal{G}$ ako za proizvoljni $x \in G$ važi $e * x = x$ ($x * e = x$). Element koji je istovremeno i levi i desni neutral je neutral (jedinica) grupoida $\mathcal{G}$.

3.1.12. Tvrđenje. *U grupodu je neutral, ako postoji, jedinstven.*

Dokaz. Neka su e i e' dva jedinična elementa grupoida $\mathcal{G} = (G,*)$. Tada je,

$$\begin{aligned}e * e' &= e, \text{ jer je } e' \text{ desna jedinica} \\ &= e', \text{ jer je } e \text{ leva jedinica.} \quad \square\end{aligned}$$

3.1.13. Primer. Razmotrimo koji grupoidi u Primeru 3.1.2. imaju neutral. U primerima (i)-(vi) 0 je neutral.
(vii) U $(M_{m\times n}, +)$ neutral je nula matrica (čiji su svi ulazi jednaki 0).
(viii) U $(M_{n\times n}, \cdot)$ neutral je jedinična matrica koja na dijagonali ima jedinice a na ostalim mestima 0.
(ix) U $(P(S), \cap)$ neutral je element S.
(x) U $(S^S, \circ)$ neutral je identičko preslikavanje id_S definisano sa $id_S(x) = x$, za svaki $x \in S$.
(xi) U $(W(L), \smile)$ neutral je prazna reč.

Iz naših primera bi se moglo zaključiti da svaki grupoid ima neutral. To nije tačno. Grupoid $(N^+, +)$ nema netrual.

3.2. Semigrupe

U nastavku se interesujemo za grupoide koji imaju neke unapred propisane osobine. Njih uglavnom zadajemo u obliku algebarskih zakona.

3.2.1. Definicija. Algebarski zakon jezika L je formula oblika $t_1 = t_2$, gde su t_1 i t_2 termi jezika L.

Dakle, algebarski zakoni su atomične formule. Oni ne uključuju logičke veznike niti kvantore. Doduše kako je zadovoljenje otvorene formule na datom modelu ekvivalentno zadovoljenju njenog zatvorenja (Pravilo generalizacije), to se može reći i da su algebarski zakoni rečenice koje su univerzalna zatvorenja formula oblika $t_1 = t_2$.

3.2.2. Primer. $x*y = y*x$ je primer algebarskog zakona koji nazivamo zakonom komutativnosti. Iako je većina struktura sa kojima se radi u elementarnoj matematici komutativna, ne možemo u svakoj strukturi proizvoljno menjati redosled elemenata, i treba da se naviknemo da je to dozvoljeno samo ako je to navedeno u aksiomama ili ako smo za datu strukturu to dokazali. U Primeru 3.1.2 nekomutativni su grupoidi (ii), (viii), (x) i (xi).

Jedan od najvažnijih algebarskih zakona je zakon asocijativnosti. Mada se u algebri razmatraju i neasocijatiovne strukture, u njima je rad vrlo nekomforan.

3.2.3 Definicija. Asocijativni zakon je formula

$$x * (y * z) = (x * y) * z.$$

Grupoid koji zadovoljava asocijativni zakon je semigrupa. Semigrupa sa jedinicom naziva se monoid. Svi grupoidi navedeni u Primeru 3.1.2., osim grupoida (ii), su semigrupe.

Sledeće tvrđenje nam pokazuje da vrednost terma u semigrupi ne zavisi od rasporeda zagrada, tako da u semigrupi zagrade možemo izostaviti, pretpostavljajući da su raspoređene na proizvoljan način. Pre toga fiksirajmo nekoliko oznaka.

3.2.4. Definicija. Neka je za $k > 1$, $(z_1, \ldots, z_k)$ niz promenljivih (ne obavezno različitih). Term $l(z_1, \ldots, z_k)$ definišemo na sledeći način,

$$\begin{aligned} l_1(z_1, \ldots, z_k) &= z_1 \\ l_{i+1}(z_1, \ldots, z_k) &= (l_i(z_1, \ldots, z_k) * z_{i+1}), \text{ za } i < k-1 \\ l(z_1, \ldots, z_k) &= l_{k-1}(z_1, \ldots, z_k) * z_k. \end{aligned}$$

Prethodna definicija može se shvatiti tako da je između svake dve promenljive upisan po jedan operacijski znak $*$, pre svih promenljivih upisano

$k-2$ zagrada, a zatim posle svake promenljive osim prve i poslednje upisana po jedna desna zagrada. Recimo $l(z_1, \ldots, z_5) = (((z_1 * z_2) * z_3) * z_4) * z_5$.

3.2.5. Definicija. Neka je t term jezika $\{*\}$ i $(z_1, \ldots, z_k)$ niz promenljivih dobijen brisanjem zagrada u t. Sa $\hat{t}$ označavamo $l(z_1, \ldots, z_k)$.

3.2.6. Tvrđenje. *Neka je S semigrupa i t term jezika $\{*\}$. Na S važi $t = \hat{t}$.*

Dokaz. Dokaz izvodimo indukcijom po $d(t)$, dužini (broju operacijskih simbola) terma t.

Neka je $d(t) = 0$. Tada je $t = z$, za neku promenljivu z. Kako u t nema zagrada, to je i $\hat{t} = z$, pa je $t = \hat{t}$.

Pretpostavimo da je tvrđenje dokazano za sve terme t takve da je $d(t) < n$, i dokažimo ga za $d(t) = n$. Dakle, neka je t term takav da je $d(t) = n$. Neka je z poslednje pojavljivanje promenljivih u termu t. Po definiciji terma, t je oblika $(u) * z$, za neki term u dužine $< n$ ili oblika $(u) * (v)$ za neke terme u i v dužine veće od 0 i manje od n. U prvom slučaju, na osnovu indukcijske hipoteze, na S važi $u = \hat{u}$, a kako je $\hat{t} = (\hat{u}) * z$, to na S važi $t = (u) * z = (\hat{u}) * z = \hat{t}$. Razmotrimo drugi slučaj. Dakle t je oblika $(u) * (v)$, za neke terme u i v, i z se pojavljuje u v. Kako je $d(v) < n$ to za v važi indukcijska hipoteza, te na S važi $v = \hat{v}$. Otuda na S važi $t = (u) * (\hat{v})$. Sdruge strane, $\hat{v} = (v_1) * z$, za neki term v_1, pa na S važi $t = (u) * ((v_1) * z)$. Kako na S važi asocijativni zakon, to na S važi i $t = ((u) * (v_1)) * z$. Označimo sa w term $(u) * (v)$. Dakle, $t = (w) * z$. Iz definicije operacije $\hat{}$, očigledno je $\hat{t} = (\hat{w}) * z$. Kako je w term dužine manje od n, to za w važi indukcijska hipoteza pa na S važi $w = \hat{w}$. Otuda na S važi $t = (\hat{w}) * z$ tj. $t = \hat{t}$. □

3.2.7. Posledica. *Neka su t i t_1 termi jezika $\{*\}$ koji se razlikuju samo po rasporedu zagrada i $S = (S, *)$ semigrupa. Na S važi $t = t_1$.*

Dokaz. Kako se t i t_1 razlikuju samo po rasporedu zagrada, to je $\hat{t} = \hat{t}_1$. Dokaz sada neposredno sledi iz prehodnog tvrđenja. □

Sada definišemo stepen pozitivnim prirodnim eksponentom . Definisaćemo ga tako da odgovara intuitivnoj ideji o proizvodu elementa sa samim sobom određeni broj puta. Takođe želimo da stepeni imaju osobine poznate iz elementarne matematike. Upravo to je razlog zašto stepen definišemo u semigrupama. U proizvoljnom grupoidu se stepeni mogu definisati, ali bi imali različite varijante stepena, zavisno od rasporeda zagrada. U semigrupi stepen definišemo rekurzivno.

3.2.8. Definicija. Neka je $(S, *)$ semigrupa i $a \in S$.

$$a^1 = a$$

$$a^{n+1} = a^n * a$$

Dokažimo da ovako definisan stepen ima željene osobine.

3.2.9. Teorema. *Neka je* $(S, *)$ *semigrupa,* $a \in S$, $m, n \in N^+$.
(i) $a^m * a^n = a^{m+n}$,
(ii) $(a^m)^n = a^{mn}$.

Dokaz. Dokaze izvodimo indukcijom po n.
(i) Za $n = 1$ jednakost sledi iz definicije stepena.
Pretpostavimo da je tvrđenje dokazano za prirodan broj n. Dokažimo jednakost za $n + 1$.

$$\begin{aligned} a^m * a^{n+1} &= a^m * (a^n * a), \text{ po definiciji stepena} \\ &= (a^m * a^n) * a \text{ , asocijativnost} \\ &= a^{m+n} * a \text{ , induktivna hipoteza} \\ &= a^{m+n+1} \text{ , po definiciji stepena.} \end{aligned}$$

(ii) Za $n = 1$ jednakost je trivijalno zadovoljena.
Pretpostavimo da je tvrđenje zadovoljeno za prirodan broj n. Dokažimo jednakost za $n + 1$.

$$\begin{aligned} (a^m)^{n+1} &= (a^m)^n * a^m \text{ , po definiciji stepena} \\ &= a^{mn} * a^m \text{ , induktivna hipoteza} \\ &= a^{mn+m} \text{ , na osnovu tačke (i) ovog tvrđenja} \\ &= a^{m(n+1)} \quad \square \end{aligned}$$

3.2.10. Definicija. Neka je $\mathcal{G} = (G, \cdot)$ semigrupa i $a \in G$. a je idempotentan ako je $a^2 = a$.

Iz definicije stepena lako se indukcijom dokazuje da za idempotenatan element a važi $a^n = a$ za svaki $n \in N$ kao što i ime kaže.

Stepen elementa je specijalan slučaj konačnog proizvoda elemenata.

3.2.11. Definicija. Neka je S semigrupa i $(a_i)_{i \in N}$ niz u S.

$$\prod_{i=1}^{1} a_i = a_1$$

$$\prod_{i=1}^{n+1} a_i = (\prod_{i=1}^{n} a_i) * a_{n+1}.$$

U sledećoj teoremi pokazuje se da sve tri osnovne algebarske konstrukcije očuvavaju zakon asocijativnosti.

3.2.12. Teorema. *(i) Podgrupoid semigrupe je semigrupa.*
(ii) Homomorfna slika semigrupe je semigrupa.
(iii) Dekartov proizvod semigrupa je semigrupa.

Dokaz. (i) Neka je $\mathcal{S} = (S, *)$ semigrupa i $\mathcal{T} = (T, \cdot)$ podgrupoid od $\mathcal{S}$. Tada je za proizvoljne $a, b, c \in T$,

$$\begin{aligned}(a \cdot b) \cdot c &= (a * b) * c \text{ , jer je } \cdot \text{ restrikcija } * \\ &= a * (b * c) \text{ , jer je } \mathcal{S} \text{ semigrupa} \\ &= a \cdot (b \cdot c) \text{ , jer je } \cdot \text{ resrikcija } *\end{aligned}$$

(ii) Neka je $\mathcal{S} = (S, *)$ semigrupa, $\mathcal{T} = (T, \cdot)$ grupoid i $f : \mathcal{S} \to \mathcal{T}$ epimorfizam. Za proizvoljne elemente $d, s, t \in T$, neka su a, b, c respektivno njihovi originali. Tada je

$$\begin{aligned}(d \cdot s) \cdot t &= (f(a) \cdot f(b)) \cdot f(c) \\ &= f(a * b) \cdot f(c) \text{ , jer je } f \text{ homomorfizam} \\ &= f((a * b) * c) \\ &= f(a * (b * c)) \text{ , jer je } \mathcal{S} \text{ semigrupa} \\ &= f(a) \cdot f(b * c) \text{ , jer je } f \text{ homomorfizam} \\ &= f(a) \cdot (f(b) \cdot f(c)) \text{ , jer je } f \text{ homomorfizam} \\ &= d \cdot (s \cdot t)\end{aligned}$$

(iii) Neka su $\mathcal{S} = (S, *)$ i $\mathcal{T} = (T, \cdot)$ semigrupe, $(S \times T, \circ)$ njihov Dekartov proizvod i $(a, d), (b, s), (c, t) \in S \times T$. Tada je

$$\begin{aligned}((a, d) \circ (b, s)) \circ (c, t) &= ((a * b) * c, (d \cdot s) \cdot t) \\ &= ((a * (b * c), d \cdot (s \cdot t)) \\ &= (a, d) \circ ((b, s) \circ (c, t)).\end{aligned}$$ □

Videli smo da je grupoid iz Primera 3.1.2.(x) semigrupa. Ta semigrupa ima poseban značaj zbog svoje univerzalnosti.

3.2.13. Lema. *Neka je $\mathcal{S}$ semigrupa sa jedinicom. Tada se $\mathcal{S}$ može potopiti u $(S^S, \circ)$.*

Dokaz. Neka je e neutral u $\mathcal{S}$. Za fiksirani element $a \in S$ definišimo preslikavanje $\tau_a : S \to S$ tako da je za $x \in S$, $\tau_a(x) = a * x$.

Neka je sada $f : S \to S^S$ definisano sa $f(a) = \tau_a$. Pokazaćemo da je f injektivni homomorfizam.

$1-1$ Neka je za $a, b \in S$, $f(a) = f(b)$, tj. $\tau_a = \tau_b$. Tada je $\tau_a(e) = \tau_b(e)$, tj. $a * e = b * e$, odnosno $a = b$.
Homomorfizam. Za $a, b \in S$ treba pokazati da je $f(a * b) = f(a) \circ f(b)$ tj. $\tau_{a*b} = \tau_a \circ \tau_b$. Neka je $x \in S$. Tada imamo

$$\begin{aligned} \tau_{a*b}(x) &= (a * b) * x \\ &= a * (b * x) \\ &= \tau_a(b * x) \\ &= \tau_a(\tau_b(x)) \\ &= \tau_a \circ \tau_b(x). \end{aligned}$$

Dakle, $\tau_{a*b} = \tau_a \circ \tau_b$. □

Preslikavanje τ_a često zovemo levom translacijom elementom a. Razlog je očigledan iz sledećeg primera. Napomenimo još da se dualno može definisati i desna translacija.

3.2.14. Primer. Posmatrajmo levu translaciju τ_3 definisanu u grupoidu $(Z, +)$. Ona je definisana tako da je $\tau_3(x) = 3 + x$. Time se svaki element u Z povećava za 3, tj. čitav skup Z transliran je za $+3$ (udesno). Kako je razmatrani grupoid komutativan, desna translacija definisana sa $\sigma_3(x) = x + 3$ se poklapa sa levom. Ove dve translacije se očigledno ne moraju poklapati u nekomutativnim strukturama.

3.2.15. Teorema. *Svaka semigrupa izomorfna je nekoj semigrupi preslikavanja.*

Dokaz. Neka je $\mathcal{S} = (S, *)$ semigrupa. Ako je S semigrupa sa jedinicom tvrđenje sledi iz prethodne leme. Ako S nema jedinicu dodajmo je. Dakle, neka je e novi element koji ne pripada S, i $S_1 = S \cup \{e\}$. Definišimo na S_1 operaciju $\cdot$ na sledeći način. Neka su $a, b \in S_1$.

$$a \cdot b = \begin{cases} a * b, & \text{za } a, b \in S \\ a, & \text{za } b = e \\ b, & \text{za } a = e. \end{cases}$$

$\mathcal{S}_1 = (S_1, \cdot)$ je očigledno semigrupa. Ako su u proizvodu sva tri elementa iz S to se svodi na asocijativnost u S, a ako je bar jedan od elemenata e onda su oba proizvoda jednaka proizvodu preostala dva elementa. Takođe je $\mathcal{S}$ podgrupoid od $\mathcal{S}_1$. $\mathcal{S}_1$ je semigrupa sa jedinicom, pa prema prethodnoj lemi postoji potapanje $f : S_1 \to (S_1^{S_1}, \circ)$ u semigrupu preslikavanja. Preslikavanje $g = f \restriction S$ je potapanje $\mathcal{S}$ u semigrupu preslikavanja. $Im(g)$ je podgrupoid semigrupe $(S_1^{S_1}, \circ)$, dakle i sam semigrupa. Dakle, toj semigrupi preslikavanja izomorfna je polazna semigrupa $\mathcal{S}$. □

3.3. Kvazigrupe. Skrativi elementi

U Primeru 3.1.2. većina struktura je asocijativna. U nastavku razmatramo jednu vrstu struktura koje su interesantne upravo onda kada nisu asocijativne.

3.3.1. Definicija. Grupoid $\mathcal{G} = (G, \cdot)$ je kvazigrupa ako u njemu svaka linearna jednačina ima jedinstveno rešenje tj. za proizvoljne elemente $a, b \in G$ postoje jedinstveni elementi $c, d \in G$ tako da je

$$a \cdot c = b$$
$$d \cdot a = b$$

Kvazigrupa sa jedinicom naziva se petljom.

Ako imamo tablicu grupoida onda se jednostavno proverava da li je on grupoid.

3.3.2. Tvrđenje. *Konačan grupoid je kvazigrupa akko se svaki element pojavljuje po tačno jednom u svakom redu i koloni njegove tablice.*

Dokaz. Za date $a, b \in G$, postoji tačno jedan c koji zadovoljava $a \cdot c = b$ akko se b pojavljuje tačno jednom u a-toj vrsti tablice grupoida. Slično, postoji samo jedan d koji zadovoljava $d \cdot a = b$ akko se b pojavljuje tačno jednom u a-toj koloni tablice grupoida. □

Primetimo da je konačnost važna samo zbog mogućnosti ispisivanja tablice. Za proizvoljni grupoid važi da je kvazigrupa akko su leve i desne translacije tog grupoida bijekcije.

3.3.3. Definicija. Latinski kvadrat reda n je $n \times n$ matrica elemenata nekog skupa A od n elemenata, takva da se svaki element od A u svakoj vrsti i koloni pojavljuje po tačno jednom.

U svetlu prethodne definicije i prethodnog tvrdenja možemo reći da su konačne kvazigrupe grupoidi čije su tablice latinski kvadrati. Na slici možemo videti primer jednog latinskog kvadrata tipa 4×4.

	a	b	c	d
	d	c	a	b
	b	a	d	c
	c	d	b	a

Poseban značaj imaju ortogonalni latinski kvadrati.

3.3.4. Definicija. Neka su (a_{ij}) i (b_{ij}) dva Latinska kvadrata reda n sa ulazima iz skupa A i osobinom da za svaki $(a, b) \in A \times A$ postoji tačno jedan indeks ij takav da $(a, b) = (a_{ij}, b_{ij})$. Tada kažemo da su (a_{ij}) i (b_{ij}) ortogonalni Latinski kvadrati.

1782. godine Ojlera su pitali, u formi nekog rasporeda vojnika, da li postoje ortogonalni Latinski kvadrati reda 6. On je formulisao hipotezu da ako je $n \cong 2(mod\, 4)$ tada ne postoje ortogonalni Latinski kvadrati reda n. Krajem šezdesetih godina ovog veka pokazano je da za svaki $n \neq 2, 6$ postoje ortogonalni Latinski kvadrati reda n. Na slici su navedeni primeri Latinskih kvadrata reda 3.

	a	b	c
	b	c	a
	c	a	b

	a	b	c
	c	a	b
	b	c	a

Vratimo se našoj analizi grupoida. U kvazigrupi iz jedinstvenosti rešenja linearnih jednačina sledi da se jednačine mogu skraćivati. Elemente grupoida koji imaju tu osobinu nazivamo skrativim.

3.3.5. Definicija. Neka je $\mathcal{G} = (G, \cdot)$ grupoid. Element $a \in G$ je levo skrativ ako za svako $x, y \in G$ važi

$$a \cdot x = a \cdot y \Rightarrow x = y$$

Dualno se definišu desno skrativi elementi.

Ova osobina omogućuje da se pojam $1-1$ i *na* preslikavanja definišu algebarski.

3.3.6. Tvrđenje. *Neka je A skup sa bar dva elementa i $f : A \to A$.*

(i) f je levo skrativ u $(A^A, \circ)$ akko je $1-1$ preslikavanje.

(ii) f je desno skrativ u $(A^A, \circ)$ akko je na preslikavanje.

Dokaz. (i) ($\Leftarrow$) Neka je f $1-1$ preslikavanje, i neka je za preslikavanja $g, h \in A^A$ ispunjeno $f \circ g = f \circ h$. Tada je za proizvoljni $a \in A$ ispunjeno

$$f \circ g(a) = f \circ h(a)$$
$$f(g(a)) = f(h(a))$$
$$g(a) = h(a), \text{ jer je } f \text{ } 1-1.$$

Kako je a proizvoljni element skupa A, to je $g = h$.

($\Rightarrow$) Dokaz izvodimo kontrapozicijom. Pretpostavimo da f nije $1-1$. Neka su a, b, c elementi iz A takvi da je $a \neq b$, $f(a) = f(b) = c$. Neka su $g, h \in A^A$ konstantna preslikavanja takva da je $g[A] = \{a\}$ i $h[A] = \{b\}$. Tada je $f \circ g[A] = \{c\}$ i $f \circ h[A] = \{c\}$. Dakle $f \circ g = f \circ h$ ali $g \neq h$, pa f nije levo skrativ.

(ii) ($\Leftarrow$) Neka je f *na* preslikavanje, i neka je za preslikavanja $g, h \in A^A$ ispunjeno $g \circ f = h \circ f$. Neka je a proizvoljni element iz A. Kako je f preslikavanje *na*, to postoji $b \in a$ tako da je $a = f(b)$. Iz $g \circ f = h \circ f$ sledi da je $g \circ f(b) = h \circ f(b)$, tj. $g(f(b)) = h(f(b))$, tj. $g(a) = f(a)$. Kako je a proizvoljni element iz A, $g = h$.

($\Rightarrow$) Dokaz izvodimo kontrapozicijom. Pretpostavimo da f nije *na*. Neka je $c \in A \setminus Im(f)$.Neka su $g, h \in A^A$ preslikavanja koja se razlikuju u tački c a poklapaju se u svim ostalim elementima skupa A. Naprimer može se uzeti da je g identičko preslikavanje, a h preslikavanje koje se od njega razlikuje samo po tome što je $h(c) = d$, gde je $d \neq c$. Neka je a proizvoljni element iz A. Tada je $f(a) \neq c$, pa je $g(f(a)) = h(f(a)) = f(a)$. Dakle $g \circ f = h \circ f$, dok je $g \neq h$. dakle, f nije desno skrativ. □

U proizvoljnom grupoidu skrativost je u vezi sa osobinama translacija uvedenih u dokazu Leme 3.2.13.

3.3.7. Tvrđenje. *Neka je $\mathcal{G} = (G, \cdot)$ grupoid i $a \in G$. a je levo (desno) skrativ akko je τ_a (σ_a) $1-1$ preslikavanje.*

Dokaz. Dokazaćemo tvrđenje za levo skrative elemente. Tvrđenje za desno skrative elemente dokazuje se dualno. Neka je $a \in G$.

$\forall x, y(a \cdot x = a \cdot y \Rightarrow x = y)$ je ekvivalentno sa
$\forall x, y(\tau_a(x) = \tau_a(y) \Rightarrow x = y)$ je ekvivalentno sa
τ_a je $1-1$ □

Sada definišemo još jednu važnu klasu elemenata u grupoidu sa jedinicom.

3.3.8. Definicija. Neka je $\mathcal{G} = (G, \cdot)$ grupoid sa jedinicom e. Element $a \in G$ je levo (desno) invertibilan ako postoji $c \in G$ tako da je $c \cdot a = e$ ($a \cdot c = e$). Za svaki takav element c kažemo da je levi (desni) inverz od a. a je invertibilan ako je i desno i levo invertibilan.

3.3.9. Tvrđenje. *Neka je $\mathcal{G} = (G, \cdot)$ semigrupa sa jedinicom e i $a \in G$. Ako je a invertibilan, onda postoji $c \in G$ tako da je*

$$c \cdot a = a \cdot c = e.$$

Taj element je jedini desni i jedini levi inverz elementa a.

Dokaz. Kako je a invertibilan, to postoje $c, d \in G$ tako da je $c * a = a * d = e$. Tada je

$$\begin{aligned} d &= e \cdot d \\ &= (c \cdot a) \cdot d \\ &= c \cdot (a \cdot d) \\ &= c \cdot e \\ &= c \quad \square \end{aligned}$$

U sledećem tvrđenju pokazaćemo da u semigrupi sa jedinicom invertibilni elementi čine podgrupoid.

3.3.10. Tvrđenje. *Neka je $\mathcal{G} = (G, \cdot)$ semigrupa sa jedinicom i S skup invertibilnih elemenata u $\mathcal{G}$. S određuje podgrupod od $\mathcal{G}$.*

Dokaz. Neka su $a, b \in S$ i neka je c inverz za a i d inverz za b. Tada imamo

$$\begin{aligned} (d \cdot c) \cdot (a \cdot b) &= d \cdot (c \cdot a) \cdot b \\ &= d \cdot e \cdot b \\ &= d \cdot b \\ &= e. \end{aligned}$$

Analogno je

$$\begin{aligned} (a \cdot b) \cdot (d \cdot c) &= a \cdot (b \cdot d) \cdot c \\ &= a \cdot e \cdot c \\ &= a \cdot c \\ &= e. \end{aligned}$$

Dakle, $d \cdot e$ je inverzni element za $a \cdot b$ pa $a \cdot b \in S$. Primetimo da je inverzni element proizvoda jednak proizvodu inverznih elemenata, ali u obrnutom redosledu. $\square$

I invertibilnost elementa semigrupe sa jedinicom u vezi je sa osobinama translacija koje određuje.

3.3.11. Tvrđenje. *Neka je $\mathcal{G} = (G, \cdot)$ semigrupa sa jedinicom i $a \in G$. a je levo (desno) invertibilan akko je σ_a (τ_a) na preslikavanje.*

Dokaz. Dokazaćemo tvrdenje za levo invertibilne elemente. Tvrdenje za desno invertibilne elemente dokazuje se dualno. Neka je $a \in G$.

($\Rightarrow$) Pretpostavimo da je a levo invertibilan i neka je c njegov levi inverz. Neka je b proizvoljni element iz G.

$$\begin{aligned}\sigma_a(b \cdot c) &= (b \cdot c) \cdot a \\ &= b \cdot (c \cdot a) \\ &= b \cdot e \\ &= b\end{aligned}$$

($\Leftarrow$) Ova strana tvrđenja očigledno važi u proizvoljnom grupoidu sa jedinicom. Neka je τ_a *na* preslikavanje. Tada postoji $c \in G$ tako da je $\sigma_a(c) = e$, tj. $c \cdot a = e$. □

Iz poznate osobine da je preslikavanje konačnog skupa $1-1$ akko je *na*, kao posledicu dobijamo sledeće tvrđenje.

3.3.12. Posledica. *Neka je G semigrupa sa jedinicom. Svaki invertibilni element je skrativ. Ako je G konačna semigrupa važi i obrat.*

Dokaz. Neka je $a \in G$. Pretpostavimo da je a levo invertibilan i neka je $c \in G$ tako da je $c \cdot a = e$. Pretpostavimo da je za neke $x, y \in G$, $a \cdot x = a \cdot y$. Tada je

$$\begin{aligned}ax &= ay \\ cax &= cay \\ ex &= ey \\ x &= y.\end{aligned}$$

Dakle, a je levo skrativ. Analogno se dokazuje implikacija za desnu invertibilnost i desnu skrativost. Dakle, ako je element invertibilan onda je i skrativ.

Neka je G konačna semigrupa i $a \in G$ skrativ element. Tada su τ_a i σ_a, $1-1$ preslikavanja konačnog skupa u sebe samog. Kako su $1-1$ preslikavanja istobrojnih skupova bijekcije, to su τ_a i σ_a *na* preslikavanja, te je a invertibilan. □

3.4. Grupe. Definicija i osobine

Grupe su semigrupe sa jedinicom u kojima je svaki element invertibilan. Videli smo (Tvrđenje 3.3.9.) da je pretpostavka ekvivalentna postojanju elementa koji je istovremno (jedinstveni) levo i desni inverz datog elementa grupe.

3.4.1. Definicija. Grupid $\mathcal{G} = (G, *)$ je grupa ako zadovoljava sledeće formule:

$$\text{(i)} \quad (x * y) * z = x * (y * z)$$
$$\text{(ii)} \quad \exists y \forall x \, (x * y = y * x = x \& \exists z (x * z = z * x = y)).$$

Aksioma (ii) se u jeziku $\{*\}$ ne može odvojiti u dve aksiome, jer egzistencijalni kvantor nije saglasan sa konjunkcijom, mada se po mnogim knjigama mogu naći takve pogrešne aksiomatizacije grupa. Primećujemo da aksioma (ii) nema oblik algebarskog zakona. Situacija se može popraviti proširenjem jezika, tj. skolemizacijom aksiome (ii).

Zato dajemo još dve definicije grupa.

3.4.2. Definicija. Struktura $\mathcal{G}_1 = (G, *, \hat{e})$ jezika $\{*, e, ^{-1}\}$ koja zadovoljava aksiome:

$$\text{(i)} \quad (x * y) * z = x * (y * z)$$
$$\text{(ii)} \quad x * e = e * x = x$$
$$\text{(iii)} \quad \forall x \exists z (x * z = z * x = e).$$

je grupa.

3.4.3. Definicija. Struktura $\mathcal{G}_1 = (G, *, e, ^{-1})$ jezika $\{*, e, ^{-1}\}$ koja zadovoljava aksiome:

$$\text{(i)} \quad (x * y) * z = x * (y * z)$$
$$\text{(ii)} \quad x * e = e * x = x$$
$$\text{(iii)} \quad \forall x (x * x^{-1} = x^{-1} * x = e).$$

je grupa.

Pokazaćemo da ovakvom trostrukom definicijom istog pojma nije uvedena nikakva konfuzija. Kad god je grupa zadana u jednom od ova tri jezika, iz nje se može na jedinstven način preći na strukturu u bilo kom od preostala dva jezika. Dakle,neka je $\mathcal{G} = (G, *)$ grupa. Kako je postojeći neutralni element $\hat{e}$ jedinstven (Tvrdenje 3.1.12.) model $\mathcal{G}$ može se proširiti do modela jezika $\{*, e\}$ gde je e simbol konstante koji se interpretira baš kao taj jedinstveni neutral $\hat{e}$. Obrnuto, svaki model jezika $\{*, e\}$ koji zadovoljava ove tri aksiome, posmatran u jeziku $\{*\}$ postaje grupa u smislu Definicije 3.4.1.. Zbog ove jednoznačne korespondencije mi u nastavku teksta ne pravimo razliku između grupe u jeziku $\{*\}$ i u jeziku $\{*, e\}$. Takođe ne pravimo razliku

između simbola konstante e i njegove interpretacije $\hat{e}$. Međutim ni u jeziku $\{*, e\}$ aksiome nemaju oblik algebarskih zakona. Rešili smo se konjunkcije, ali ne i egzistencijalnog kvantora.

Izvršimo još jednu skolemizaciju. Dakle neka je $\mathcal{G}_1 = (G, *, e)$ grupa u jeziku $\{*, e\}$. Kako aksioma (iii) znači da je svaki element invertibilan, a znamo da u grupoidu svaki invertibilni element ima jedinstven inverz (Tvrđenje 3.3.9), time je na jedinstven način određeno preslikavanje koje svakom elementu pridružuje njegov inverz. Zato se $\mathcal{G}_1 = (G, *, e)$ može proširiti (ne skupovno) do modela $\mathcal{G}_2 = (G, *, e, ^{-1})$ jezika $\{*, e, ^{-1}\}$, gde je $^{-1}$ operacijski simbol dužine 1, koji zadovoljava Definiciju 3.4.3. Obrnuto, grupa u jeziku $\{*, e, ^{-1}\}$ osiromašenjem jezika postaje grupa u smislu Definicije 3.4.2.

3.4.4. Primer. Navešćemo neke važne primere grupa u jeziku $\{*, e, ^{-1}\}$. Grupoidi iz primera 3.1.2. koji nisu ovde navedeni nisu grupe.
(i) $\mathcal{Z} = (Z, +, 0, -)$ gde je Z skup celih brojeva, $+$ operacija sabiranja, a $-$ operacija koja celom broju pridružuje broj sa suprotnim znakom.
(ii) $\mathcal{Z}_n = (Z_n, +_n, 0, -_n)$ gde je $Z_n = \{0, 1, \ldots, n-1\}$, $+_n$ operacija sabiranja po modulu n, a $-_n$ operacija definisana sa $-_n(k) = n - k$, za $k > 0$ i $-_n(0) = 0$.
(iii) $\mathcal{Q} = (Q, +, 0, -)$, $\mathcal{R} = (R, +, 0, -)$, $\mathcal{C} = (C, +, 0, -)$, gde je Q skup racionalnih brojeva, R skup realnih brojeva i C skup kompleksnih brojeva.
(iv) $(R[x], +, 0, -)$ gde je $R[x]$ skup polinoma sa realnim koeficijentima.
(v) $(M_{m\times n}, +, 0, -)$ gde je $M_{m\times n}$ skup matrica tipa $m \times n$, 0 matrica čiji su svi ulazi jednaki 0, a $-$ operacija koja menja znak svim ulazima matrice.
(vi) $(R_{n\times n}, \cdot, E, ^{-1})$ skup regularnih matrica tipa $n \times n$, tj. matrica sa osobinom $det(A) \neq 0$. E je jedinična matrica koja na dijagonali ima ulaze jednake 1 dok su svi ostali ulazi jednaki nuli. Operacija $^{-1}$ je operacija invertovanja matrice. Ova grupa je određena skupom invertibilnih elemenata grupoida iz Primera 3.1.2.(viii).
(vii) $(P(S), \Delta, \emptyset, id)$. Interesantno je da je u ovoj grupi svaki element sam sebi inverzni.
(viii) Neka je A skup i $S(A)$ skup svih permutacija (bijekcija) skupa A $(S(A), \circ, id, ^{-1}$ gde je $\circ$ operacija kompozicije preslikavanja, id identičko preslikavanje a $^{-1}$ operacija koja bijekciji pridružuje inverzno preslikavanje, je grupa. Ova grupa je određena skupom invertibilnih elemenata grupoida iz Primera 3.1.2.(x).
Grupe se mogu zadati i slabijim (jednostavnijim za proveru) aksiomama.

3.4.5. Tvrđenje. (i) *Neka je $\mathcal{G} = (G, \cdot)$ semigrupa u kojoj postoji leva (desna) jedinica i u kojoj je svaki element levo (desno) invertibilan u odnosu na tu levu (desnu) jedinicu. $\mathcal{G}$ je grupa.*

(ii) *Asocijativna kvazigrupa je grupa.*

Dokaz. Neka je e leva jedinica, i neka za svaki element a iz G, a' označava jedan njegov levi inverz, a a" levi inverz od a'. Pokažimo da je a' istovremeno i desni inverz od a . $(a' \cdot a) \cdot a' = e \cdot a' = a'$, pa množenje ove jednaksoti sleva sa a" daje

$$\begin{aligned}(a" \cdot a') \cdot (a \cdot a') &= a"a' \\ e \cdot (a \cdot a') &= e \\ a \cdot a' &= e.\end{aligned}$$

Pokažimo sada da je e i desna jedinica.

$$\begin{aligned}a \cdot e &= a \cdot (a' \cdot a) \\ &= (a \cdot a') \cdot a \\ &= e \cdot a \\ &= a.\end{aligned}$$

Dakle, $\mathcal{G}$ je semigrupa sa jedinicom u kojoj su svi elementi invertibilni, dakle $\mathcal{G}$ je grupa.

(ii) Neka je $\mathcal{G} = (G, \cdot)$ asocijativna kvazigrupa. Fiksirajmo proizvoljni element $a \in G$. Označimo sa e_a jedinstveno rešenje jednačine $x \cdot a = a$ (to rešenje postoji na osnovu definicije kvazigrupe). e_a se u odnosu na a ponaša kao lokalna leva jedinica, tj. da bi pokazali postojanje (univerzalne) leve jedinice treba da pokažemo da se e_a za bilo koji drugi element ponaša kao leva jedinica (a ne samo za element a za koji je dizajnirana). Dakle, neka je $b \in G$ i neka je s_b jedinstveno rešenje jednačine $ay = b$. Dakle, $a \cdot s_b = b$. Tada imamo

$$\begin{aligned}e_a \cdot b &= e_a \cdot (a \cdot s_b) \\ &= (e_a \cdot a) \cdot s_b \\ &= a \cdot s_b \\ &= b.\end{aligned}$$

Dakle, e_a je leva jedinica. Zato taj element nadalje označavamo samo sa e. Kako za proizvoljno $b \in G$ jednačina $x \cdot b = e$ ima (jedinstveno) rešenje, to je svaki element iz G levo invertibilan. Tvrđenje sada neposredno sledi iz tačke (i) ovog tvrđenja. □

U sledećem tvrđenju navodimo neke osnovne osobine grupa. One su uglavnom ranije dokazane, ali je dobro da ih napišemo na jednom mestu.

3.4.6. Tvrđenje. *Neka je* $\mathcal{G} = (G, *, e, ^{-1})$ *i* $a, b \in G$.

(i) $(a^{-1})^{-1} = a$.

(ii) $(a * b)^{-1} = b^{-1} * a^{-1}$

(iii) $ax = ay \Rightarrow x = y$ *dakle u grupi se jednakosti mogu skraćivati.*

(iv) *Jednačina* $ax = b$ *ima jedinstveno rešenje* $x = a^{-1} * b$, *a jednačina* $ya = b$ *ima jedinstveno rešenje* $y = b * a^{-1}$. (v) *Leva translacija* σ_a *i desna translacija* τ_a *su bijekcije.*

Dokaz. (i) Iz $a \cdot a^{-1} = e$ sledi da je a levi inverz od a^{-1}. Slično iz $a^{-1} \cdot a = e$ sledi da je a desni inverz od a^{-1}. Dakle, a je inverz od a^{-1}.

(ii) Videti dokaz Tvrđenja 3.3.10.

(iii) Sledi iz Tvrđenja 3.3.12.

(iv) Jednostavnom zamenom se proverava da su navedeni elementi rešenja datih jednačina. Njihova jedinstvenost sledi iz prethodne tačke ovog istog tvrđenja. □

(v) Sledi iz invertibilnosti elementa a (Tvrđenja 3.3.11., 3.3.12. i 3.3.7.). □

U grupi se definicija stepena može proširiti na stepenovanje celim izložiocem, tako da i dalje ima poznate osobine.

3.4.7. Definicija. Neka je $\mathcal{G} = (G, \cdot, e, ^{-1})$ grupa, $a \in G$, $m \in Z$.

$$a^m = \begin{cases} a^m, \text{ za } m > 0 \\ e, \text{ za m=0} \\ (a^{-m})^{-1}, \text{ za } m < 0 \end{cases}$$

3.4.8. Tvrđenje. *Neka je* $\mathcal{G} = (G, \cdot, e, ^{-1})$ *grupa,* $a \in G$, $m, n \in Z$.

(i) $a^{-m} = (a^m)^{-1}$.

(ii) $a^{m+n} = a^m \cdot a^n$.

(iii) $(a^m)^{-1} = (a^{-1})^m$.

(iv) $(a^m)^n = a^{mn}$.

Dokaz. (i) Za $m > 0$ to je ispunjeno na osnovu definicije. Za $m = 0$ obe strane su jednake e. Za $m < 0$ po definiciji je $a^m = a^{-m})^{-1}$. Invertovanjem obe strane dobijamo $(a^m)^{-1} = ((a^{-m})^{-1})^{-1} = a^{-m}$.

(ii) U dokazu treba razmotriti devet slučajeva (i za m i za n po tri). Neki od njih se mogu simultano dokazati. Dakle, pretpostavimo najpre da je $m = 0$ ili $n = 0$. Označimo prvi (u redosledu (m, n)) od njih koji je jednak 0 sa s a onaj drugi sa t. Tada je leva strana jednakosti jednaka $a^{s+t} = a^t$, a desna $a^0 \cdot a^t$ ili $a^t \cdot a^0$. Kako je $a^0 = e$, desna strana je uoba slučaja jednaka a^t, dakle jednaka levoj strani.

Razmatramo preostala četiri slučaja, kada je $m \neq 0$ i $n \neq 0$.

A) $m > 0$ i $n > 0$. Tvrđenje je već dokazano kao Tvrđenje 3.2.9.

B) $m < 0$ i $n < 0$. Tada je $m = -k$ i $n = -l$ za $k, l \in N^+$. Tada imamo

$$\begin{aligned} a^m \cdot a^n &= (a^k)^{-1} \cdot (a^l)^{-1} \\ &= (a^l \cdot a^k)^{-1} \\ &= (a^{l+k})^{-1} \\ &= a^{-(l+k)} \\ &= a^{m+n}. \end{aligned}$$

C) $m > 0$ i $n < 0$. Tada je $n = -k$ za $k = |n|$. Neka je najpre $m \geq k$ tj. $m = t + k$ za neko $t \in N$. Primetimo da je $t = m - k = m + n$. Tada je $a^{t+k} = a^t \cdot a^k$, prema već dokazanim slučajevima. Otuda imamo

$$\begin{aligned} a^m \cdot a^n &= a^{k+t} \cdot (a^k)^{-1} \\ &= a^t \cdot a^k \cdot (a^k)^{-1} \\ &= a^t \cdot e \\ &= a^t \\ &= a^{m+n} \end{aligned}$$

Razmotrimo sada podslučaj kada je $m < k$ tj. $k = t + m$ za neko $t \in N^+$. Primetimo da je $-t = m - k = m + n$. Tada je $a^k = a^{t+m} = a^t \cdot a^m$, prema već dokazanim slučajevima. Otuda imamo

$$\begin{aligned} a^m \cdot a^n &= a^m \cdot (a^k)^{-1} \\ &= a^m \cdot (a^t \cdot a^m)^{-1} \\ &= a^m \cdot (a^m)^{-1} \cdot (a^t)^{-1} \\ &= (a^t)^{-1} \\ &= a^{-t} \\ &= a^{m+n}. \end{aligned}$$

D) $m < 0$ i $n > 0$. Neka je $m = -k$. Prema dokazanim slučajevima (izložilac prvog činioca je pozitivan) imamo $a^n \cdot a^{k-n} = a^k$. Množeći obe strane jednakosti sa a^{-k} sleva i a^{n-k} sdesna imamo,

$$\begin{aligned} a^{-k} \cdot a^n \cdot a^{k-n} \cdot a^{n-k} &= a^{n-k} \\ a^{-k} \cdot a^n &= a^{n-k} \\ a^m \cdot a^n &= a^{m+n} \end{aligned}$$

(iii) Za $m = 0$ tvrđenje je trivijalno zadovoljeno. Razmotrimo slučaj $m > 0$. Tada je prema ranije dokazanoj teoremi za pozitivne eksponente

$$\begin{aligned} a^m \cdot (a^{-1})^m &= (a \cdot a^{-1})^m \\ &= e^m \\ &= e \end{aligned}$$

Dakle, $(a^{-1})^m$ je $(a^m)^{-1}$. Ostaje slučaj $m < 0$. Kako je $-m > 0$, to je prema dokazanom slučaju

$$(a^{-m})^{-1} = (a^{-1})^{-m}.$$

Uzimajući inverze leve i desne strane dobijamo

$$a^{-m} = ((a^{-1})^{-m})^{-1}.$$

Otuda prema tački (i) ovog tvrđenja dobijamo

$$(a^m)^{-1} = ((a^{-1})^m.$$

(iv) Tvrđenje se trivijalno dokazuje kada je jedan od brojeva m, n jednak 0. Kada su oba broja pozitivna tvrđenje je ranije dokazano. Razmotrimo preostale slučajeve.

A) $m > 0$ i $n < 0$. Neka je $n = -k$, $k \in N^+$. Tada je

$$\begin{aligned} (a^m)^n &= ((a^m)^k)^{-1} \\ &= (a^{mk})^{-1} \\ &= a^{-mk} \\ &= a^{mn}. \end{aligned}$$

Dakle, tvrđenje je dokazano za $m > 0$ nezavisno od znaka od n.

B) $m < 0$. Neka je $m = -k$. Tada je

$$\begin{aligned} (a^m)^n &= (a^{-k})^n \\ &= ((a^{-1})^k)^n \\ &= (a^{-1})^{kn} \\ &= a^{-kn} \\ &= a^{mn}. \quad \square \end{aligned}$$

Dosada nismo analizirali zadovoljenje komutativnog zakona na grupama. U Primeru 3.4.4 grupe komutativne su sve grupe osim (vi) i (vili).

3.4.9. Definicija. Komutativne grupe nazivamo Abelovim grupama.

U komutativnim grupama često se koristi aditivna notacija umesto generalne multiplikativne, tako da se piše

$$\begin{aligned} + &\quad \text{umesto} \quad \cdot \\ 0 &\quad \text{umesto} \quad e \\ -a &\quad \text{umesto} \quad a^{-1} \\ na &\quad \text{umesto} \quad a^n. \end{aligned}$$

Oznaka na asocira na množenje ali to nije operacija množenja elemenata grupe i prirodnih brojeva, već operacija koja predstavlja zbir n jednakih sabiraka. Kod aditivnih grupa definiše se i operacija oduzimanja:

$$a - b = a + (-b).$$

Navedimo još neke važne primere nekomutativnih grupa.

3.4.10. Primer. Neka je D_4 skup simetrija kvadrata, tj. izometrijskih transformacija ravni koje dati kvadrat preslikavaju u sebe samog. Iz geometrije znamo da je $D_4 = \{id, \rho, \rho^2, \rho^3, \sigma, \sigma_1, \sigma_2, \sigma_3\}$. Kako je kompozicija dve simetrije kvadrata opet simetrija kvadrata $(D_4, \circ)$ je grupod. Kako je operacija kompozicije preslikavanja asocijativna, $(D_4, \circ)$ je semigrupa. id je očigledno neutralni element. Svaki element je invertibilan. Zaista, elementi $\{id, \rho^2, \sigma, \sigma_1, \sigma_2, \sigma_3\}$ su sami sebi inverzi, dok je $\rho^{-1} = \rho^3$. Dakle D_4 je grupa, poznata kao Dijedarska grupa.

	e	ρ	ρ^2	ρ^3	σ	σ_1	σ_2	σ_3
e	e	ρ	ρ^2	ρ^3	σ	σ_1	σ_2	σ_3
ρ	ρ	ρ^2	ρ^3	e	σ_3	σ	σ_1	σ_2
ρ^2	ρ^2	ρ^3	e	ρ	σ_2	σ_3	σ	σ_1
ρ^3	ρ^3	e	ρ	ρ^2	σ_1	σ_2	σ_3	σ
σ	σ	σ_1	σ_2	σ_3	e	ρ	ρ^2	ρ^3
σ_1	σ_1	σ_2	σ_3	σ	ρ^3	e	ρ	ρ^2
σ_2	σ_2	σ_3	σ	σ_1	ρ^2	ρ^3	e	ρ
σ_3	σ_3	σ	σ_1	σ_2	ρ	ρ^2	ρ^3	e

Sada kada smo dobili tablicu možemo zaboraviti geometrijsku strukturu elemenata grupe. Sve algebarske osobine ove grupe i zadovoljenja zakona zavise samo od ove tablice. Čak se možemo pitati i zašto smo se mučili sa geometrijskom pričom i nismo samo naveli gotovu tablicu. Takav pristup bi najpre imao problem sa proverom asocijativnosti. Za proveru tablice trebalo bi proveriti 8^3 jednakosti. Ovako smo asocijativnost dobili usput iz osobina kompozicije preslikavanja. Sledeći razlog je taj što se tablica teže memoriše od geometrijskog opisa. Možemo li naći način prezentacije ove grupe koji ima prednosti oba pristupa?

Koristimo sledeću osobinu izometrijskih transformacija:

Neka su σ i τ osne simetrije čije se ose s i t seku u tački O i neka je $\varphi = \angle sOt$. Tada je $\tau \circ \sigma$ rotacija sa centrom O za ugao 2φ.

Otuda je ρ može predstaviti kao kompozicija bilo koje dve osne simetrije čije ose zaklapaju ugao od $45°$, a ρ^{-1} kao kompozicija bilo koje dve simetrije koje zaklapaju ugao od $-45°$.

Tako je naprimer $\rho = \sigma \circ \sigma_1$, pa imamo

$$\begin{aligned} \sigma \circ \rho &= \sigma \circ \sigma \circ \sigma_1 \\ &= \sigma_1 \end{aligned}$$

Slično je $\rho = \sigma_3 \circ \sigma$, pa imamo

$$\begin{aligned} \rho \circ \sigma &= \sigma_3 \circ \sigma \circ \sigma \\ &= \sigma_3 \end{aligned}$$

Odavde se vidi da D_4 nije Abelova grupa. Izvedimo još jedan račun.

$$\begin{aligned} \sigma \circ \rho^{-1} &= \sigma^{-1} \circ \rho^{-1} \\ &= (\rho \circ \sigma)^{-1} \\ &= (\sigma_3)^{-1} \\ &= \sigma_3 \end{aligned}$$

Iz prethodna dva računa može se videti da je $\rho \circ \sigma = \sigma \circ \rho^{-1}$. Primetimo i da je $\sigma \circ \sigma_2 = \rho^2$ pa množenjem sleva sa σ dobijamo $\sigma_2 = \sigma \circ \rho^2$.

Dakle, sada vidimo da se svaki element grupe D_4 može predstaviti u obliku $\sigma^i \circ \rho^j$ gde $i \in \{0, 1\}$ a $j \in \{0, 1, 2, 3\}$. Čitava tablica može se izvesti

iz sledeće tri jednakosti:

$$\rho^4 = id$$
$$\sigma^2 = id$$
$$\rho^\sigma = \sigma\rho^{-1}.$$

Zaista,

$$\sigma^i \circ \rho^j \circ \sigma^k \circ \rho^l = \sigma^i\sigma^k \circ \rho^{(-1)^k j} \circ \rho^l$$
$$= \sigma^{i+2k} \circ \rho^{(-1)^k j + l}.$$

Dakle, tri navedene jednakosti određuju strukturu grupe pa se i zovu strukturne jednakosti.

Napomenimo da se slično grupa D_n definiše za svako $n \geq 3$, kao grupa simetrija pravilnog n-tougla. $D_n = \{\rho^i : 0 \leq i < n\} \cup \{\sigma \circ \rho^i : 0 \leq i < n\}$. $|D_n| = 2n$ a strukturne jednakosti su $\{\rho^n = id, \sigma^2 = id, \rho \circ \sigma = \sigma \circ \rho^{-1}\}$.

3.4.11. Primer. Neka je $K = \{\pm 1, \pm i, \pm j, \pm k\}$. Definišimo operaciju $\cdot$ na K tako da je za proizvojne $x, y \in K$,

$$-(-x) = x,$$
$$1 \cdot x = x \cdot 1 = x,$$
$$(*) \qquad (-y) \cdot x = x \cdot (-y) = -(x \cdot y),$$
$$i^2 = j^2 = k^2 = -1,$$
$$i \cdot j = k, \quad j \cdot k = i, \quad k \cdot i = j,$$
$$j \cdot i = -k, \quad k \cdot j = -i, \quad i \cdot k = -j.$$

Dakle, i, j, k ponašaju se kao tri imaginarne jedinice, koje u cikličnom redosledu (i, j, k), kada su dva elementa susedi u pozitivnom smeru (smeru suprotnom kazaljkama na satu), onda im je proizvod onaj treći, a ako su susedi u negativnom smeru (smeru kazaljki), suprotni element od onog trećeg. Jednostavno se proverava da je 1 neutral, da su ± 1 sami sebi inverzi, a za ostale elemente je $-$ operacija invertovanja. Jedino je problem provera asocijativnosti. Da bi izbegli $2 \cdot 8^3$ izračunavanja, proveru radimo po karakteristiv cnim slučjevima. Dakle, proveravamo da li je za proizvoljne $a, b, c \in K$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Ako neki od brojeva a, b, c ima u sebi $-$, onda se svi ti minusi izvlače ispred zagrada, prema $(*)$. I na levoj i na desnoj strani je jednak broj $-$, dakle

ostaje da dokažemo jednakost "pozitivnih delova". Ako je neki od brojeva a, b, c jednak 1 oba proizvoda su jednaka proizvodu preostala dva člana. Dakle, ostaje slučaj $a, b, c \in \{1, i, j, k\}$. Ako su a, b, c različiti, onda ako su a, b u pozitivnom redosledu onda su i b, c u pozitivnom redosledu pa je $(a \cdot b) \cdot c = c \cdot c = -1$, i $a \cdot (b \cdot c) = a \cdot a = -1$. Ako su b i a u negativnom redosledu, onda su i b i c u negativnom redosledu, pa su oba proizvoda jednaka 1. Kada je $a = b = c$ oba proizvoda su jednaka $-a$. Ostaje slučaj kada su dva elementa jednaka a treći različit od njih. Najpre neka je $a = b \neq c$. Tada je $a \cdot (a \cdot c) = -c$ jer je jedan od redosleda a, b, a, c pozitivan a drugi negativan. Takođe i $(a \cdot a) \cdot c = -c$. Ako je $b = c$, zamenom mesta u najstarijem proizvodu na obe strane, i izvlačenjem $-$ na obe strane, slučaj se svodi na prethodni. Ostaje slučaj kada je $a = c$. Tada je $(a \cdot b) \cdot a = -a \cdot (a \cdot b) = a \cdot (b \cdot a)$. Asocijativnost je dokazana. Dakle, $(K) = (K, \cdot, 1)$ je nekomutativna grupa.

3.5. Podgrupe

3.5.1. Definicija. Neka je $\mathcal{G} = (G, \cdot)$ grupa i $H \subset G$. Ako je $\mathcal{H} = (H, \cdot \restriction H \times H)$ grupa tada kažemo da je $\mathcal{H}$ podgrupa od $\mathcal{G}$ određena podskupom H.

Pre nego dokažemo neke ekvivalente ovog pojma dokazaćemo jednu lemu.

3.5.2. Lema. *Neutral je jedini idempotent u grupi.*

Dokaz. Neka je $\mathcal{G} = (G, \cdot, e)$ grupa. e je očigledno idempotent. Obrnuto, neka je a idempotent. Tada je

$$\begin{aligned} a^2 &= a \\ a \cdot a &= a \cdot e, \text{ i skraćivanjem sa } a \text{ dobijamo} \\ a &= e \end{aligned}$$ □

3.5.3. Tvrđenje. *Neka je $\mathcal{G} = (G, \cdot)$ grupa sa jedinicom e i operacijom inverznog elementa $^{-1}$ i $H \subset G$. Sledeća tvrđenja su ekvivalentna:*

(i) *H određuje podgrupu od $\mathcal{G}$.*
(ii) *H je zatvoren za $\cdot$, $e \in H$ i H je zatvoren za operaciju $^{-1}$.*
(iii) *Za svako $a, b \in H$, $a \cdot b^{-1} \in H$.*

Dokaz. (i)$\Rightarrow$ (ii) Neka je $(H, *)$ grupa, za $* = \cdot \restriction H \times H$.

Kako je H grupoid, za proizvoljne $a, b \in H$, $a * b \in H$. Kako je $* = \cdot \restriction H \times H$, to je $a \cdot b = a * b \in H$.

Takođe $(H, *)$ ima neutral, označimo ga sa f. f je idempotent u H, dakle $f * f = f$. Kako je $* = \cdot \restriction H \times H$, to je i $f \cdot f = f$. Dakle, f je idempotent i u $\mathcal{G}$, pa je prema prethodnoj lemi $f = e$ tj. $e \in H$.

I na kraju pokažimo zatvorenost za operaciju $^{-1}$. Neka je $a \in H$ i neka je $b \in H$ inverzni element od a u $\mathcal{H}$ (u odnosu na operaciju $*$). Dakle, $a * b = b * a = e$. Kako je $* = \cdot \restriction H \times H$, to je i $b \cdot a = a \cdot b = e$, dakle $b = a^{-1}$, pa $a^{-1} \in H$.

(ii)$\Rightarrow$ (iii) Neka su $a, b \in H$. Tada, prema (ii), $a, b^{-1} \in H$ a time i $a \cdot b^{-1} \in H$.

(iii)$\Rightarrow$(i) Neka je $a, a \in H$. Tada je, prema (iii), $a \cdot a^{-1} \in H$, tj $e \in H$. Dakle, sada imamo $e, a \in H$. Otuda je, prema (iii), $e \cdot a^{-1} \in H$ tj. $a^{-1} \in H$. Dakle, H je zatvoren za $^{-1}$.

Neka je sada $a, b \in H$. Tada je, prema prethodnom delu dokaza, $a, b^{-1} \in H$. Primenom (iii) dobijamo $a \cdot (b^{-1})^{-1} \in H$ tj. $a \cdot b \in H$. Dakle, H sadrži neutral i zatvoren je za operacije $\cdot$ i $^{-1}$, pa je $(H, \cdot \restriction H \times H)$ grupa a time i podgrupa od $\mathcal{G}$.

Primetimo da je ekvivalent (iii) najjednostavniji za proveru. Napomenimo i to da taj ekvivalent u aditivnoj notaciji glasi

$$\forall a, b \in H (a - b \in H).$$

3.5.4. Posledica. *Neka je $\mathcal{G}$ grupa i neka H određuje podgrupu od $\mathcal{G}$ i $a \in H$. Tada je za svaki $m \in Z$, $a^m \in Z$.*

Dokaz. Za $m = 0$ je $a^m = e$, pa tvrđenje sledi iz tačke (ii) prethodnog tvrđenja. Ako je $m \in N^+$, tvrđenje se jednostavno dokazuje indukcijom po m. Za $m < 0$, tvrđenje sledi iz definicije stepena sa negativnim eksponentom i tačke (ii) prethodnog tvrđenja.

3.5.5. Primer. (i) Neka je $n \in N^+$. Kako je razlika dva broja deljiva sa n i sama deljiva sa n, nZ određuje podgrupu od $\mathcal{Z}$.

(ii) $\mathcal{Z} < \mathcal{Q} < \mathcal{R} < \mathcal{C}$. To se jdnostavno pokazuje time što je svaka od njih zatvorena za oduzimanje u sledećoj.

(iii) $\mathcal{R} < \mathcal{R}[x]$, jer je razlika dva relna broja (polinoma stepena 0 ili $-\infty$) opet realan broj.

(iii) Kako u $\mathcal{P}(S) = (P(S), \Delta, \emptyset, id)$ važi $a - b = a\Delta(-b) = a\Delta b$, to, prema Primeru 3.1.6.(ii), za svako $T \subset S$, $P(T)$ određuje podgrupu od $\mathcal{P}(S)$.

(iv) Neka je S_4 grupa permutacija četvoroelementnog skupa temena kvadrata. Svaka simetrija kvadrata određuje jednu permutaciju njegovih temena. Poznato je da je svaka izometrijska transformacija određena svojim vrednostima u trima različitiom tačkama ravni. Otuda je svaka simetrija kvadrata

jednoznačno određena tom permutacijom temena koju određuje. Otuda se grupa D_4 može i definisati kao grupa nekih permutacija četvoroelementnog skupa u odnosu na operaciju kompozicije. Tako posmatrana grupa $\mathcal{D}_4$ je podgrupa od $\mathcal{S}_4$. Uopšte je $\mathcal{D}_n < \mathcal{S}_n$, za $n \geq 3$. Kako D_3 i S_3 imaju obe po šest elemanata, to je $D_3 = S_3$.

3.5.6. Tvrđenje. *Neka je $\mathcal{G} = (G, \cdot)$ grupa i neka je familija podskupova od $\mathcal{G}$ koji određuju podgrupe u $\mathcal{G}$. Tada i $\bigcap$ određuje podgrupu od $\mathcal{G}$.*

Dokaz. Neka je $a, b \in \bigcap$. Tada je za svako $H \in$, $a, b \in H$. Kako $\mathcal{H}$ određuje podgrupu od $\mathcal{G}$, to je $a \cdot b^{-1} \in H$. Kako je to ispunjeno za svaki $H \in$, to $a \cdot b^{-1} \in \bigcap$. Prema Tvrđenju 3.5.3., $\bigcap$ određuje podgrupu od $\mathcal{G}$. □

U nastavku razmatramo jednu važnu konstrukciju. Neka je dat poskup grupe koji je nepravilan u smislu da ne određuje podgrupu. Mi hoćemo da ga proširimo da postane pravilan, tj. da određuje podgrupu date grupe. Naravno hoćmo da to bude najmanja (ako postoji) takva podgrupa da bi što više odražavala osobine elemenata tog skupa.

3.5.7. Definicija. Neka je $\mathcal{G}$ grupa i $K \subset G$. Podgrupa od $\mathcal{G}$ generisana skupom K je najmanja podgrupa od $\mathcal{G}$ koja sadrži K, u oznaci $\langle K \rangle$.

Jednostavnosti radi mi ćemo sa $\langle K \rangle$ označavat i podgrupu generisanu podskupom K i skup koji je određuje. Iz konteksta se može videti na koje se od ta dva značenja misli.

3.5.8. Tvrđenje. *Neka je $\mathcal{G}$ grupa. Za svaki $K \subset G$ postoji $\langle K \rangle$.*

Dokaz. Neka je familija podskupova H od G koji imaju sledeće osobine:
1) H određuje podgrupu od $\mathcal{G}$.
2) $K \subset H$.
Ova familija je neprazna jer $G \in$. Neka je $S = \bigcap$. Prema prethodnom tvrđenju, S određuje podgrupu od $\mathcal{G}$. Kako je K, prema osobini 2), sadržano u svim elementima familije , to je $K \subset S$. Dakle, i S ispunjava uslove 1) i 2), tj. $S \in$. Kako je S presek te familije, on je sadržan u svim elementima familije tj. S je najmanji član familije . Po definiciji S određuje $\langle K \rangle$. □

Ma kako bili zadovoljni ovako kratkim i jednostavnim dokazom on nema veliku praktičnu korist. Da bi generisali podgrupu čak i najmanjim skupom mi treba da učitamo u memoriju možda ogromnu familiju nekih skupova koji ga sadrže. Mnogo korisniju internalnu karakterizaciju podgrupe generisane podskupom daje nam sledeće tvrđenje.

3.5.9. Tvrđenje. *Neka su oznake kao u prethodnoj definiciji.*

$$\langle K \rangle = \{u_1^{m_1} \cdot u_2^{m_2} \cdot \ldots \cdot u_k^{m_k} : k \in N, \forall i \leq k \, (u_i \in K, \, m_i \in Z)\}$$

Dokaz. Označimo skup na desnoj strani sa S. Pokazaćemo da S ima osobine 1) i 2) iz prethodnog tvrđenja.

1) Treba pokazati da je za proizvoljne $a, b \in S$, $a \cdot b^{-1} \in S$. Dakle, neka je $a = u_1^{m_1} \cdot u_2^{m_2} \cdot \ldots \cdot u_k^{m_k}$ i $b = v_1^{n_1} \cdot v_2^{n_2} \cdot \ldots \cdot v_l^{n_l}$, za neke $k, l \in N$, tako da je za svako $i \leq k$ i $j \leq l$, $u_i, v_j \in K$ a $m_i, n_j \in Z$. Tada je

$$\begin{aligned} a \cdot b^{-1} &= u_1^{m_1} \cdot u_2^{m_2} \cdot \ldots \cdot u_k^{m_k} \cdot (v_1^{n_1} \cdot v_2^{n_2} \cdot \ldots \cdot v_l^{n_l})^{-1} \\ &= u_1^{m_1} \cdot u_2^{m_2} \cdot \ldots \cdot u_k^{m_k} \cdot v_l^{-n_l} \cdot \ldots \cdot v_2^{-n_2} \cdot v_1^{-n_1} \end{aligned}$$

Vidimo da je $a \cdot b^{-1}$ jednak proizvodu stepena čije su osnove u K a izložioci celi, dakle $a \cdot b^{-1} \in S$.

2) Neka je $u \in K$. Tada je $u = u^1$, pa po definiciji skupa S, $u \in S$. Kako je $u$proizvoljni element skupa K, $K \subset S$.

Pokažimo na kraju da je S najmanji skup koji ima osobine 1)i 2). Neka je dakle, $H \subset G$ skup koji zadovoljava osobine 1) i 2). Neka je g proizvoljni element iz S. $g = u_1^{m_1} \cdot u_2^{m_2} \cdot \ldots \cdot u_k^{m_k}$, za neki $k \in N$, i neke $u_i \in K$, $m_i \in Z$, $i \leq k$. Kako je $K \subset H$, to je $u_i \in H$, za $i \leq k$. Kako H određuje podgrupu od $\mathcal{G}$, to je H zatvoren za stepenovanje, i za svako $i \leq k$ je $u_i^{m_i} \in H$. Na kraju je $g \in H$ kao konačan proizvod elemenata iz H. Dakle $S \subset H$. Time je pokazano da je S najmanji skup sa osobinama 1) i 2), dakle $S = \langle K \rangle$.

3.5.10. Posledica. *Neka je $(A, +)$ Abelova grupa i $K \subset A$.*

$$\begin{aligned} \langle K \rangle = \{ & m_1 u_1 + m_2 u_2 + \cdots + m_k u_k : k \in N, \forall i \leq k \, (m_i \in Z), \\ & u_1, \ldots, u_k \text{ su različiti elementi iz } K \}. \end{aligned}$$

Dokaz. To je prethodno tvrđenje, samo u aditivnoj notaciji. Pojačanje je samo u pretpostavci da su osnove različite. Opšti izraz se može svesti na ovaj oblik zahvaljujući komutativnosti. Ako se pojavljuje više stepena sa istom osnovom oni se mogu zahvaljujući komutativnosti rasporediti jedan pored drugog, a zatim se iskoristi teorema o množenju stepena istih osnova. □

Ukoliko je skup K konačan, recimo $K = \{u_1, \ldots, u_k\}$, onda umesto $\langle \{u_1, \ldots, u_k\} \rangle$ pišemo $\langle u_1, \ldots, u_k \rangle$.

3.5.11. Posledica. *Neka je $\mathcal{G}$ grupa i $a \in G$. Tada je $\langle a \rangle = \{a^i : i \in Z\}$.*

3.5.12. Primer. U $\mathcal{Z}$ je $\langle 1 \rangle = \{m1 : m \in Z\} = Z$. Dakle, sama $\mathcal{Z}$ je jedina podgrupa od $\mathcal{Z}$ koja sadrži 1.

Slično je $\langle 3 \rangle = \{m3 : m \in Z\} = 3Z$

$\langle 6, 15 \rangle = \{m6 + n15 : m, n \in Z\} = \{k : \exists m, n \, (k = 6m + 15n)\} = 3Z$. Poslednja jednakost sledi iz Bezu-ove teoreme. Detaljnije, na osnovu

Bezuove teoreme postoje $m, n \in Z$ tako da je $3 = 6m + 15n$. Otuda je $3 \in \langle 6, 15\rangle$. Kako je $3Z$ najmanja podgrupa koja sadrži 3, to je $3Z < \langle 6, 15\rangle$. S druge strane, kako je svaki broj oblika $6m + 15n \in 3Z$, to je $3Z < \langle 6, 15\rangle$.

Na isti način može se, indukcijom po k, dokazati da je $\langle m_1, \ldots, m_k\rangle = dZ$, gde je $d = (m_1, \ldots, m_k)$ njihov najveći zajednički delilac.

U Posledici 3.5. opisane su podgrupe generisane jednim elementom. Međutim ne moraju svi nabrojani elementi biti različiti među sobom. Može se desiti da su mnogi elementi u navedenom opisu jednaki, pa se iz tog opisa ne vidi dobro izgled podgrupe. Sada želimo da elemente podgrupe generisane jednim elementom nabrojimo u listi bez ponavljanja.

3.5.13. Definicija. Neka je $\mathcal{G}$ grupa i $a \in G$. Red elementa a u oznaci $r(a)$ definišemo na sledeći način:

$$r(a) = \begin{cases} min\{k \in N^+ : a^k = e\}, & \text{ako je taj skup neprazan} \\ \infty, & \text{ako je taj skup prazan.} \end{cases}$$

3.5.14. Primer. (i) U $\mathcal{Z}$ je $r(6) = \infty$, jer je za svako $k \in N^+$, $k6 = 6k \neq 0$. U stvari $r(0) = 1$ a svi ostali elementi imaju red ∞.

(ii) U $\mathcal{D}_4$ je $r(\rho) = 4$, jer je $\rho, \rho^2, \rho^3 \neq id$, a $\rho^4 = id$. Slično je $r(\rho^3) = 4$. Naravno, $r(id) = 1$, a svi ostali elementi su reda 2 (jer su sami sebi inverzni).

(iii) U svakoj grupi je $r(a) = r(a^{-1})$, jer $(a^{-1})^k = e$ akko $(a^k)^{-1} = e$ odnosno $a^k = e$.

3.5.15. Tvrđenje. *Neka je $\mathcal{G}$ grupa i $a \in G$.*

(i) Ako je $r(a) = k$, onda je $\langle a\rangle = \{a^i : 0 \leq i < k\}$, gde je za svako $0 \leq i \neq j < n$, $a^i \neq a^j$. Zato je $|\langle a\rangle| = r(a)$.

(ii) Ako je $r(a) = \infty$, onda je $\langle a\rangle = \{a^i : i \in Z\}$, gde je za svako $i \neq j$, $a^i \neq a^j$. Zato je $\langle a\rangle$ beskonačan prebrojiv skup.

Dokaz. (i) Dokazaćemo najpre da za svaki $j \in Z$ postoji $0 \leq r < k$, tako da je $a^j = a^i$. Neka je $j = qk + r$ gde je $0 \leq r < k$. Tada je

$$\begin{aligned} a^j &= a^{qk} \cdot a^r \\ &= (a^k)^q \cdot a^r \\ &= e \cdot a^r \\ &= a^r. \end{aligned}$$

Ostaje da pokažemo da je za $0 \leq i \neq j < k$, $a^i \neq a^j$. Bez gubljenja opštosti možemo pretpostaviti da je $0 \leq i < j < n$. Tada je $0 < j - i < k$.

Pretpostavimo da je $a^i = a^j$. Tada je

$$a^i = a^j$$
$$a^i \cdot a^{-i} = a^j \cdot a^{-i}$$
$$e = a^{j-i}$$

što je u kontradikciji sa minimalnošću broja k.

(ii) Neka je $r(a) = \infty$. To znači da je za svako $n \in N^+$ $a^n \neq e$. Dakle, neka je $i \neq j$. Bez gubljenja opštosti možemo pretpostaviti da je $i < j$, tj. $j - i > 0$. Iz pretpostavke $a^i = a^j$ se na isti način kao u prethodnom delu dokaza pokazuje da je $a^{j-i} = e$. Kako je $j-i \in N^+$, dobili smo kontradikciju. Dakle, za $i \neq j$ je $a^i \neq a^j$. □

3.5.16. Definicija. Neka je $\mathcal{G}$ grupa. Red grupe, u oznaci $|G|$, definišemo kao kardinalnost skupa G, ako je on konačan. U suprotnom kažemo da je red od G beskonačan.

3.5.17. Posledica. *Neka je $\mathcal{G}$ grup konačnog reda i $a \in G$. Tada je $r(a)$ konačan i $r(a) \leq |G|$.*

Dokaz. Kako je $\langle a \rangle \subset G$, to je $\langle a \rangle$ konačan skup i $|\langle a \rangle| \leq |G|$. Kako je $r(a) = |\langle a \rangle|$, to je $r(a)$ konačan i $r(a) \leq |G|$. □

U nastavku nastojimo da opišemo brojeve koji se mogu pojaviti kao red elementa grupe, i uticaj reda elementa na njegovo ponašanje.

3.5.18. Tvrđenje. *Neka je $\mathcal{G}$ grupa i $a \in G$. Tada za svaki ceo broj važi*

$$a^m = e \Leftrightarrow r(a) | m .$$

Dokaz. ($\Rightarrow$) Neka je $r(a) = k$ i $a^m = e$. Neka je dalje $m = qk + r$ za $0 \leq r < k$. Tada je $e = a^m = a^{qk+r} = (a^k)^q \cdot a^r = a^r$. Dakle, $0 \leq r < k$ i $a^r = e$. Zbog minimalnosti broja k u N^+, $r \notin N^+$, dakle $r = 0$, tj. $k|m$.

($\Leftarrow$) Neka je $m = qk$ za neki $q \in Z$. Tada je $a^m = (a^k)^m = e$. □

Na kraju ovog dela navodimo jednu teoremu koja je vrlo moćno oruđe u analizi konačnih grupa.

3.5.19. Definicija. Neka je $\mathcal{G} = (G, \cdot)$ grupa i $a \in G$; $J, K \subset G$.

$$aK = \{a \cdot g : g \in K\}$$
$$Ja = \{g \cdot a : g \in K\}$$
$$KL = \{g \cdot s : g \in K, s \in L\}$$
$$LK = \{s \cdot g : g \in K, s \in L\}$$

Primetimo da se u prethodnoj definiciji ne radi o operaciji množenja skupova, već je to samo oznaka za određeni skup. Skup aH (Ha) zovemo desnim (levim) H-kosetom ili pomerajem određenim elementom a. Razlog je taj što je $aH = \sigma_a[H]$, dakle slika od H levom translacijom (pomerajem). Dualno je Ha pomeraj od H desnom translacijom.

3.5.20. Definicija. Neka je $\mathcal{G}$ grupa i $\mathcal{H} < \mathcal{G}$. Relacije $\sim_{LH}$ i $\sim_{DH}$ na G definišu se na sledeći način. Za $a, b \in G$

$$a \sim_{LH} b \Leftrightarrow a^{-1} \cdot b \in H$$
$$a \sim_{LH} b \Leftrightarrow b \cdot a^{-1} \in H.$$

3.5.21. Tvrđenje. *Neka su oznake kao u prethodnoj definiciji.*

(i) $\sim_{LH}$ ($\sim_{LH}$) *je relacija ekvivalencije skupa* G.

(ii) *Za* $a \in G$, *klasa ekvivalencije* $a/\sim_{LH} = aH$ *i* $a/\sim_{DH} = Ha$.

(iii) *Za* $a \in H$, $|aH| = |H|$.

Dokaz. Dokaz izvodimo za $\sim_{LH}$. Dokaz za $\sim_{DH}$ izvodi se dualno.

(i) Neka je $a, b \in G$.

Refleksivost. Kako je $a^{-1} \cdot a = e \in H$, to je $a \sim_{LH} a$.

Simetričnost. Neka je $a \sim_{LH} b$. To znači da je $a^{-1} \cdot b \in H$. Kako je H zatvoren za operaciju $^{-1}$, to je $(a^{-1} \cdot b)^{-1} = b^{-1} \cdot a \in H$. Dakle, $b \sim_{LH} a$.

Tranzitivnost. Neka je $a \sim_{LH} b$ i $b \sim_{LH} c$. Otuda imamo $a^{-1} \cdot b \in H$ i $b^{-1} \cdot c \in H$. Kako je H zatvoren za proizvode, $a^{-1} \cdot b \cdot b^{-1} \cdot c = a^{-1} \cdot c \in H$. Dakle, $a \sim_{LH} c$.

(ii) Neka je $a \in G$.

$$\begin{aligned} b \in a/\sim_{LH} &\Leftrightarrow a \sim_{LH} b \\ &\Leftrightarrow a^{-1} \cdot b \in H \\ &\Leftrightarrow a^{-1} \cdot b = h, \quad \text{za neki } h \in H \\ &\Leftrightarrow b = a \cdot h, \quad \text{za neki } h \in H \\ &\Leftrightarrow b \in aH. \end{aligned}$$

(iii) Preslikavanje σ_a je bijekcija, pa je $|H| = |\sigma_a[H]| = |aH|$. □

3.5.22. Teorema (Lagranž). *Neka je* $\mathcal{G}$ *konačna grupa i* $\mathcal{H} < \mathcal{G}$. *Tada*

$$|H| \,|\, |G|.$$

Dokaz. Neka je $G/\sim_{LH}$ faktor skup, skup klasa ekvivalencije relacije $\sim_{LH}$. Neka je dalje, T transverzala faktor skupa tj. $T \subset G$ koji iz svake klase ekvivalencije sadrži po tačno jedan element. Tada je $G/\sim_{LH} = \bigcup_{a \in T} a/\sim_{LH}$

disjunktna unija različitih klasa ekvivalencije. Otuda je po definiciji zbira kardinala

$$\begin{aligned} |G| &= |\bigcup_{a\in T} a/\sim_{LH}| \\ &= \sum_{a\in T} |a/\sim_{LH}| \\ &= \sum_{a\in T} |aH| \\ &= \sum_{a\in T} |H| \\ &= |T|\cdot|H| \\ &= |G/\sim_{LH}|\cdot|H|. \end{aligned}$$

Iz poslednje jednakosti očigledno $|H|\,|\,|G|$. Dokaz se mogao izvesti i sa $\sim_{DH}$. Kako je

$$|G/\sim_{LH}| = \frac{|G|}{|H|}$$

$$|G/\sim_{DH}| = \frac{|G|}{|H|},$$

to imamo i da je $|G/\sim_{LH}| = |G/\sim_{DH}|$. □

3.5.23. Definicija. Neka je $\mathcal{G}$ grupa i $\mathcal{H} < \mathcal{G}$. Ako je $|G\sim_{LH}|$ konačan broj, $|G\sim_{LH}|$ nazivamo indeksom podgrupe $\mathcal{H}$ u grupi $\mathcal{G}$ u oznaci $[G:H]$. U suprotnom je $[G:H]=\infty$.

3.5.24. Posledica. *Neka je $\mathcal{G}$ grupa konačnog reda i $\mathcal{H} < \mathcal{G}$.*

$$[G:H] = \frac{|G|}{|H|}.$$

Dokaz. Tvrdnje je dokazano u okviru prethodnog. □

Lagranžova teorema ima važne posledice i na red elementa.

3.5.25. Posledica. *Neka je $\mathcal{G}$ grupa konačnog reda i $a \in G$. $r(a)\,|\,|G|$.*

Dokaz. Kako je $r(a) = |\langle a\rangle|$ i prema Lagranžovoj teoremi $|\langle a\rangle|\,|\,|G|$, to $r(a)\,|\,|G|$. □

3.5.26. Posledica. *Neka je $\mathcal{G} = (G,\cdot,e)$ grupa konačnog reda i $a \in G$. $a^{|G|} = e$.*

Dokaz. Neposredno sledi iz prethodne posledice i Tvrđenja 3.5.18. □

3.6. Kongruencije. Homomorfizmi.

Relacije ekvivalencije nastale su uopštenjem jednakosti (njenih RST osobina) i predstavljaju strogo skupovnu konstrukciju jer su u uzajamno jednoznačnoj korespondenciji sa particijama. U slučaju algebre one ni na koji način ne zavise od operacija. Međutim jednakost ima u algebarskim strukturama i osobinu saglasnosti sa operacijama. Uopštenjem te osobine dolazimo do pojma kongruencija, algebarskih relacija ekvivalencije.

3.6.1. Definicija. Neka je $\mathcal{G} = (G, *)$ grupoid i $\sim$ relacija ekvivalencije skupa G. $\sim$ je relacija kongruencije ako je za proizvoljne $a, b, c, d \in G$

$$\text{(S)} \qquad a \sim b \,\&\, c \sim d \Rightarrow a * c \sim b * d\,.$$

3.6.2. Tvrđenje. *Neka su oznake kao u prethodnoj definiciji.* $\sim$ *je relacija kongruencije akko za proizvoljne* $a, b, c \in G$

$$a \sim b \Rightarrow c * a \sim c * b \,\&\, a * c \sim b * c\,.$$

Dokaz. ($\Rightarrow$) Neka je $\sim$ relacija kongruencije i $a, b, c \in G$. Tada iz $a \sim b$ i $c \sim c$ sledi $c * a \sim c * b$ i $a * c \sim b * c$.

($\Leftarrow$) Pretpostavimo da $\sim$ zadovoljava uslov (S). Neka je $a \sim b$ i $c \sim d$. Tada je prema (S), $a * c \sim b * c$ i $b * c \sim b * d$. Na osnovu tranzitivnosti je $a * c \sim b * d$. □

3.6.3. Primer. Relacija $\equiv_m$ je relacija kongruencije grupe $\mathcal{Z}$.

Ukoliko je $\sim$ relacija kongruencije grupoida $\mathcal{G} = (G, *)$, onda $*$ indukuje strukturu grupoida na faktor skupu $G/\sim$. Zaista na $G/\sim$ može se uvesti operacija $*_\sim$ tako da je za $a/\sim, b/\sim \in G/\sim$

$$a/\sim *_\sim b/\sim = a * b/\sim\,.$$

Primetimo da je operacija korektno definisana tj. da ne zavisi od izbora predtavnika klase. Zaista, za $c \in a/\sim$ i $d \in b/\sim$ imamo $a \sim c$ i $b \sim d$. Kako je $\sim$ relacija kongruencije, to je $a * b \sim c * d$, pa je $a * b/\sim = c * d/\sim$ odnosno $a/\sim *_\sim b/\sim = c/\sim *_\sim d/\sim$.

3.6.4. Definicija. Neka je $\sim$ relacija kongruencije grupoida $\mathcal{G} = (G, *)$. Grupoid $(G/\sim, *_\sim)$ nazivamo faktor grupoidom grupoida $\mathcal{G}$, u oznaci $\mathcal{G}/\sim$.

3.6.5. Tvrđenje. *Neka je $\mathcal{G}$ grupa i $\mathcal{G}/\sim$ faktor grupoid od $\mathcal{G}$. Tada je i $\mathcal{G}/\sim$ grupa.*

Dokaz. Asocijativnost. Neka je $a/\sim, b/\sim, c/\sim \in G$. Tada je

$$\begin{aligned}(a/\sim *_\sim b/\sim) *_\sim c/\sim &= (a*b)*c/\sim \\ &= a*(b*c)/\sim \\ &= a/\sim *_\sim (b/\sim *_\sim c/\sim).\end{aligned}$$

Lako se proverava da je $e/\sim$ neutral i da je inverzni element od $a/\sim$ jednak $a^{-1}/\sim$. Dakle, $\mathcal{G}/\sim$ je grupa. □

U nastavku razmatramo homomorfizme grupa.

3.6.6. Tvrđenje. *Neka je $f : \mathcal{G} \to \mathcal{S}$ epimorfizam grupoida. Ako je $\mathcal{G}$ grupa, onda je $\mathcal{S}$ takođe grupa.*

Dokaz. Pokažimo najpre asocijativnost. Neka je $s, t, u \in S$. Kako je f preslikavanje *na*, to postoje $a, b, c \in G$ tako da je $f(a) = s$, $f(b) = t$ i $f(c) = u$. Tada je

$$\begin{aligned}(s\cdot t)\cdot v &= (f(a)\cdot f(b))\cdot f(c) \\ &= f((a*b)*c) \\ &= f(a*(b*c)) \\ &= f(a)\cdot(f(b)\cdot f(c)) \\ &= s\cdot(t\cdot v).\end{aligned}$$

Slično se proverava da je $f(e_G)$ neutral u $\mathcal{S}$ i da je inverzni element od $c = f(a)$ element $f(a^{-1})$. Te provere su ustvari izvedene u dokazu sledećeg tvrđenja. □

3.6.7. Tvrđenje. *Neka je $f : \mathcal{G} \to \mathcal{S}$ homomorfizam grupa $\mathcal{G} = (G, *)$ i $\mathcal{S} = (S, \cdot)$ i neka su e_G i e_S neutrali tih grupa a $^{-1_G}$ i $^{-1_S}$ operacije invertovanja. Neka je a proizvoljni element iz G.*

(i) $f(e_G) = e_S$.
(ii) $f(a^{-1_G}) = (f(a))^{-1_S}$.
(iii) $f(a^m = (f(a))^m$.
(iv) $Im(f) < \mathcal{S}$.
(v) *Ako je $r(a)$ konačan onda $r(f(a))|r(a)$.*

Dokaz. (i) Kako je $e_G * e_G = e_G$, to je $f(e_G) = f(e_G)\cdot f(e_G)$. Dakle, $f(e_G)$ je idempotent. Kako je prema Lemi 3.5.2., e_S jedini idempotent u $\mathcal{S}$, to je $f(e_G) = e_S$.

(ii) Kako je

$$\begin{aligned} e_H &= f(e_G) \\ &= f(a^{-1_G} * a) \\ &= f(a^{-1_G}) \cdot f(a), \end{aligned}$$

to je $f(a^{-1_G})$ levi inverz za $f(a)$. Dualno se pokazuje da je to i levi inverz, dakle i inverz za $f(a)$. Dakle, $f(a^{-1_G}) = (f(a))^{-1_S}$.

(iii) Za $n = 0$ tvrdenje se svodi na tačku (i) ovog tvrdenja. Za $n > 0$ tvrđenje dokazujemo indukcijom po n. Za $n = 1$ je to trivijalni identitet. Pretpostavimo da je $f(a^n) = f(a)^n$. Tada je

$$\begin{aligned} f(a^{n+1}) &= f(a^n * a) \\ &= f(a^n) \cdot f(a) \\ &= f(a)^n \cdot f(a) \\ &= f(a)^{n+1}. \end{aligned}$$

Ostaje slučaj kada je $n < 0$. Tada imamo

$$\begin{aligned} f(a^n) &= f((a^{-n})^{-1}) \\ &= (f(a^{-n}))^{-1} \\ &= (f(a)^{-n})^{-1}, \text{ jer je } -n > 0 \\ &= f(a)^n. \end{aligned}$$

(iv) Neka je $c, d \in Im(f)$. Dakle, postoje $a, b \in G$ tako da je $f(a) = c$ i $f(b) = d$. Tada je

$$\begin{aligned} c * d^{-1} &= f(a) \cdot f(b)^{-1} \\ &= f(a * b^{-1}). \end{aligned}$$

Dakle, $c \cdot d^{-1} \in Im(f)$. Prema Tvrđenju 3.5.3., $Im(f) < S$.

(v) Neka je $r(a) = k$. Kako je $a^k = e_G$, to je $f(a^k) = f(a)^k = e_S$. Prema Tvrđenju 3.5.18., $r(f(a))|k$. □

3.6.8. Primer. Opisati sve homomorfizme grupe $\mathcal{Z}_{24}$ u grupu $\mathcal{Z}_5$. Očigledno postoji trivijalni homomorfizam koji sve elemente iz Z_{24} preslikava u neutral 0. Da li ima netrivijalnih homomorfizama. Neka je $a \in G$, $r(a) = k$. Tada prema Posledici 3.5.25., $k|24$ i $r(f(a))|5$. Prema prethodnom tvrđenju, tačka (v), $r(f(a)|k$ pa imamo i $r(f(a))|24$. Kako $r(f(a))|24$ i $r(f(a))|5$, to je $r(f(a) = 1$ tj. $f(a) = e$. Kako je a proizvoljni element iz Z_{24}, f je trivijalni homomorfizam.

3.6.9. Primer. Neka je $\mathcal{G}$ grupa i $a \in G$. Definišimo preslikavanje $\varphi_a : G \to G$ tako da je $\varphi = \sigma_{a^{-1}} \circ \tau_a$, tj. $\varphi_a(x) = a^{-1} \cdot x \cdot a$. φ je bijekcija kao kompozicija dve bijekcije (jedne leve i jedne desne translacije). Pokazaćemo da je φ_a homomorfizam. Dakle, za $x, y \in G$ je

$$\begin{aligned}\varphi_a(x \cdot y) &= a^{-1} \cdot (x \cdot y) \cdot a \\ &= a^{-1} \cdot x \cdot a^{-1} \cdot a \cdot y \cdot a \\ &= \varphi_a(x)\varphi_a(y).\end{aligned}$$

3.6.10. Definicija. Automorfizam φ_a konstruisan u prethodnom primeru nazivamo unutrašnjim automorfizmom grupe $\mathcal{G}$ određenim elementom a. $Inn(\mathcal{G})$ označava skup unutrašnjih automorfizama grupe $\mathcal{G}$.

U sledećoj teoremi uspostavlja se veza između homomorfizama i kongruencija.

3.6.11. Teorema. *Neka su $\mathcal{G} = (G, *)$ i $\mathcal{S} = (S, \cdot)$ grupe.*

(i) *Neka je $f : \mathcal{G} \to \mathcal{S}$ i $\sim_f$ relacija na G definisana tako da je za $a, b \in G$*

$$a \sim_f b \Leftrightarrow f(a) = f(b).$$

Tada je $\sim_f$ relacija kongruencije grupe $\mathcal{G}$.

(ii) *Neka je $\sim$ relacija kongruencije grupe $\mathcal{G}$ i $f_\sim : G \to G/\sim$ preslikavanje definisano sa*

$$f_\sim(a) = a/\sim .$$

Tada je $f_\sim$ epimorfizam.

Takođe je $\sim_{f_\sim} = \sim$ i $f_{\sim_f} = f$.

Dokaz. (i) Trivijalno se proverava da je $\sim_f$ relacija ekvivalencije. Proverimo da je $\sim_f$ saglasna sa operacijom $*$. Neka je za $a, b, c \in G$, $a \sim_f b$ tj. $f(a) = f(b)$. Tada je $f(c) \cdot f(a) = f(c) \cdot f(b)$ tj. $f(c * a) = f(c * b)$. Otuda je $c * a \sim_f c * b$. Dualno se pokazuje da je i $a * c \sim_f b * c$.

(ii) Kako je $f_\sim(a) = a/\sim$, to je $f_\sim$ preslikavanje *na*. Ostaje da proverimo da je $f_\sim$ homomorfizam. Neka je $a, b \in G$.

$$\begin{aligned}f_\sim(a * b) &= a * b/\sim \\ &= a/\sim *_\sim b/\sim \\ &= f_\sim(a) *_\sim f_\sim(b).\end{aligned}$$

Ostaje da dokažemo da su ova pridruživanja inverzi jedan drugome. Neka je $a, b \in G$.

$$\begin{aligned}a \sim_{f_\sim} b &\Leftrightarrow f_\sim(a) = f_\sim(b) \\ &\Leftrightarrow a/\sim = b/\sim \\ &\Leftrightarrow a \sim b.\end{aligned}$$

Dakle, $\sim_{f_\sim} = \sim$. Druga jednakost pokazuje se slično. □

3.7. Normalne podgrupe

U nastavku razmatramo važan pojam normalnih podgrupa koji je u bliskoj vezi sa pojmom homomorfizma.

3.7.1. Definicija. Neka je $\mathcal{G}$ grupa i $\mathcal{H} < \mathcal{G}$. $\mathcal{H}$ je normalna podgrupa od G, u oznaci $\mathcal{H} \lhd \mathcal{G}$, ako je za svaki $g \in G$, $gH = Hg$.

Činjenicu da je H normalna grupa tehnički često koristimo kao neku vrstu komutiranja sa elementima iz H. U proizvodu gh, gde je $h \in H$, činioci mogu da komutiraju stim što element h ne mora biti isti, ali je neki element iz H. Dakle, $g \cdot h = h_1 \cdot g$ za neki $h_1 \in H$.

3.7.2. Tvrđenje. *Neka su oznake kao u prethodnoj definiciji. Sledeća tvrđenja su ekvivalentna.*

(i) $\mathcal{H} \lhd \mathcal{G}$.

(ii) *Za svaki* $g \in G$, $\varphi_g[H] = H$.

(iii) *Za svaki* $g \in G$, H *je invarijantni podskup unutrašnjeg automorfizma* φ_g *tj.* $\varphi_g[H] \subset H$.

(iv) *Za svaki* $g \in G$, $Hg \subset gH$.

(v) $\sim_{LH} = \sim_{DH}$

(vi) $\sim_{LH}$ *je relacija kongruencije.*

Dokaz. $(i) \Rightarrow (ii)$ Neka je $a \in G$. Kako je $H \lhd G$, to je $Ha = aH$. Množenjem ove skupovne jednakosti sa a^{-1} sleva, dobijamo $a^{-1}Ha = H$.

$(ii) \Rightarrow (iii)$ Trivijalno.

$(iii) \Rightarrow (iv)$ Neka je $a \in G$. Tada je, prema (iii), $a^{-1}Ha \subset H$. Množenjem ove nejednakosti sa a sleva dobijamo $Ha \subset aH$.

$(iv) \Rightarrow (i)$ Pretpostavimo $\forall g(g^{-1}Hg \subset H)$. Neka je a proizvoljni element iz G. Tada je $a^{-1}Ha \subset H$. Zamenom $g = a^{-1}$, dobijamo $(a^{-1})^{-1}Ha^{-1} \subset H$. Množenjem ove nejednakosti sa a^{-1} sleva i sa a sdesna dobijamo $H \subset a^{-1}Ha$, pa otuda i $H = a^{-1}Ha$.

$(i) \Leftrightarrow (v)$ Neka je $a, b \in G$

$$\begin{aligned} \sim_{LH} = \sim_{DH} &\Leftrightarrow \forall g\,(g/\sim_{DH} = g/\sim_{LH}) \\ &\Leftrightarrow \forall g\,(Hg = gH) \\ &\Leftrightarrow \mathcal{H} \lhd \mathcal{G} \end{aligned}$$

$(v) \Rightarrow (vi)$ Neka je za $a, b \in G$, $a \sim_{LH} b$. Tada je $a/\sim = b/\sim$ tj. $aH = bH$. Neka je $c \in G$. Množenjem sa c sleva dobijamo $caH = cbH$, tj. $ca \sim cb$.

Prema (v) je i $a \sim_{DH} b$, pa je $Ha = Hb$. Množenjem sa c sdesna dobijamo $Hac = Hbc$, dakle $ac \sim_{DH} bc$. Kako je $\sim_D H = \sim_L H$, to je i $ac \sim_{LH} bc$. Dakle, $\sim_{LH}$ je relacija kongruencije.

$(vi) \Rightarrow (v)$ Neka je $\sim_{LH}$ relacija kongruencije i neka je $a \sim_{LH} b$. Množenjem sa a^{-1} sdesna, dobijamo $e \sim_{LH} b \cdot a^{-1}$. Po definiciji relacije $\sim_{LH}$ je $e^{-1}ba^{-1} \in H$, tj. $ba^{-1} \in H$. Otuda je $a \sim_{DH} b$. Ovaj isti niz jednakosti, samo u obrnutom redosledu, je dokaz da iz $a \sim_{DH} b$ sledi $a \sim_{LH} b$. □

3.7.3. Definicija. Neka je $\mathcal{H} \lhd \mathcal{G}$. Tada relaciju kongruencije $\sim_{LH} = \sim_{DH}$ označavamo sa $\sim_H$, a faktor grupu $G/\sim_H$ sa $\mathcal{G}/\mathcal{H}$.

U prethodnoj teoremi je pokazano da je svakoj normalnoj podgrupi $\mathcal{H}$ pridružena relacija kongruencije $\sim_H$. U sledećem tvrđenju se između ova dva pojma uspostavlja veza slična onoj između kongruencija i epimorfizama.

3.7.4. Teorema. *Neka je $\sim$ relacija kongruencije grupe $\mathcal{G} = (G, \cdot, e)$. Tada je $N_\sim = e/\sim \lhd \mathcal{G}$. Pri tome je $\sim_{N_\sim} = \sim$ i $N_{\sim_N} = N$.*

Dokaz. Neka je $a \in G$. Pokazaćemo da je $a^{-1}N_\sim a \subset N_\sim$. Neka je $b \in a^{-1}N_\sim a$. Postoji $h \in N_\sim$ tako da je $b = a^{-1}ha$. Kako je $h \in N_\sim$, to je $h \sim e$. Množenjem ove relacije sleva sa a^{-1} i sdesna sa a dobijamo $a^{-1}ha \sim e$. Dakle $b \in N_\sim$, što je i trebalo dokazati.

Neka su $a, b \in G$.

$$\begin{aligned} a \sim_{N_\sim} b &\Leftrightarrow a^{-1}b \in N_\sim \\ &\Leftrightarrow a^{-1}b \sim e \\ &\Leftrightarrow b \sim a \\ &\Leftrightarrow a \sim b. \end{aligned}$$

Dakle, $\sim_{N_\sim} = \sim$.

Neka je $a \in G$.

$$\begin{aligned} a \in N_{\sim_N} &\Leftrightarrow a \sim_N e \\ &\Leftrightarrow ae^{-1} \in N \\ &\Leftrightarrow a \in N. \end{aligned}$$

Dakle, $N_{\sim_N} = N$. □

Sledeća teorema nam obezbeđuje bogat izbor primera normalnih podgrupa.

3.7.5. Tvrđenje. *(i) U svakoj grupi $\mathcal{G} = (G, \cdot, e)$, imamo da je $\{e\}, \mathcal{G} \lhd \mathcal{G}$.*

(ii) *Svaka podgrupa komutativne grupe je komutativna.*

(iii) *Centar grupe je normalna podgrupa te grupe.*

(iv) *Neka je $\mathcal{G}$ grupa i $\mathcal{H}$ podgrupa od $\mathcal{G}$ indeksa 2. Tada je $\mathcal{H} \lhd \mathcal{G}$.*

Dokaz. (i) Za svaki $g \in G$ je $g\{e\} = \{e\}g = \{g\}$. Kako je φ_g automorfizam od $\mathcal{G}$, $\varphi_g[G] = G$.

(ii) Neka je $\mathcal{G}$ Abelova grupa i $\mathcal{H} < \mathcal{G}$. Neka je $a \in G$. Kako je $\mathcal{G}$ komutativna grupa, to je za svaki $h \in H$ $ah = ha$, pa je $aH = Ha$. Dakle, $\mathcal{H} \lhd \mathcal{G}$.

(iii) Neka je $a \in G$. Za svaki $h \in Z(G)$, po definiciji centra, $ah = ha$, pa je $aZ(G) = Z(G)a$. Dakle $\mathcal{Z}(G) \lhd \mathcal{G}$.

(iv) Kako je $[G : H] = 2$, to se $G/\sim_{LH}$ sastoji iz dva koseta. Zbog osobine da klase ekvivalencije čine particiju oni su komplementarni. Jedan od njih je $e/\sim = H$, pa drugi možemo označiti sa H^c. Iz istog razloga su i koseti relacije $\sim_{DH}$ takođe H i H^c. Kako $\sim_{LH}$ i $\sim_{DH}$ određuju istu particiju, to je $\sim_{LH} = \sim_{DH}$, pa je $\mathcal{H} \lhd \mathcal{G}$. □

3.7.6. Primer. (i) $6\mathcal{Z} \lhd \mathcal{Z}$ jer je $\mathcal{Z}$ Abelova grupa.

(ii) U D_4 je $P = \{id, \rho, \rho^2, \rho^3\} \lhd D_4$ jer je indeksa 2. To se vidi na osnovu Posledice 3.5.24.: $[D_4 : P] = \frac{|D_4|}{|P|} = \frac{8}{4} = 2$. Iz istog razloga je i $\{id, \sigma, \rho^2, \sigma\rho^2\} \lhd D_4$.

Kako je $Z(D_4) = \{id, \rho^2\}$, to je $\{e, \rho^2\} \lhd D_4$. Međutim $S = \{id, \sigma\} \not\lhd D_4$. Zaista, $S\rho = \{\sigma, \sigma\rho\}$, dok je $\rho S = \{\sigma, \rho\sigma\} = \{\sigma, \sigma\rho^3\}$.

(iii) U grupi kvaterniona K svaka podgrupa je normalna. Proverimo tu činjenicu. $\{-1, 1\} = Z(K)$, pa je normalna podgrupa od K. Neka je $\mathcal{H} < \mathcal{K}$, netrivijalna podgrupa od $\mathcal{K}$ različita od podgrupe $\mathcal{Z}(K)$. H mora sadržati element iz skupa $\{\pm i, \pm j, \pm k\}$. Kako je svaki od tih elemenata reda 4, $|H| \geq 4$. H je netrivijalana podgrupa pa je $|H| < 8$. Po Lagranžovoj teoremi $|H| | 8$. dakle, $|H| = 4$. Zato je $[K : H] = 2$, pa je $H \lhd K$. Dakle, sve podgrupe od K su normalne, iako K nije Abelova grupa.

3.7.7. Tvrđenje. *Neka je $\mathcal{G}$ grupa i $\mathcal{H}, \mathcal{K} < \mathcal{G}$.*

(i) *Neka je $\mathcal{K} < \mathcal{H} < \mathcal{G}$ i $\mathcal{K} \lhd \mathcal{G}$. Tada je $K \lhd H$.*

(ii) *Ako je $K \lhd G$, tada je $HK < G$ i $KH < G$.*

(iii) *Ako je $H, K \lhd G$, tada je $HK \lhd G$.*

Dokaz. (i) Sledi direktno iz definicije. Kako je za svaki $g \in G$, $gK = Kg$, i $H \subset G$, to je za svaki $g \in H$, $gK = Kg$. Dakle, $K \lhd H$.

(ii) Neka je $a, b \in HK$. Tada postoje $h_1, h_2 \in H$ i $k_1, k_2 \in K$ tako da je $a = h_1k_1$ i $b = h_2k_2$. Tada je $a^{-1}b = k_1^{-1}h_1^{-1}h_2k_2$. Neka je $h = h_1^{-1}h_2$. Kako je H zatvorena za $\cdot$, $h \in H$. Kako je $K \lhd G$, to je $hk_2 = k_3h$ za neki $k_3 \in K$ (videti komentar iza Definicije 3.7.1.). Otuda je $a^{-1}b = k_1^{-1}hk_2 = k_1^{-1}k_3h$. Neka je $k_1^{-1}k_3 = k$. Kako je K zatvoren za operaciju $\cdot$, $k \in K$. Dakle, $a^{-1}b = hk \in HK$. Prema Tvrđenju 3.5.3., $HK < G$. Slično se dokazuje i da je $KH < G$.

(iii) Neka je $g \in G$. Kako je $K, H \lhd G$, to je $Hg = gH$ i $Kg = gK$. Otuda je $g(HK) = (gH)K = (Hg)K = H(gK) = H(Kg) = (HK)g$. Kako je g proizvoljni element iz G, $HK \lhd G$. □

3.7.8. Primer. i) Relacija $\lhd$ među podgrupama date grupe nije tranzitivna, iako je relacija $<$ tranzitivna. Zaista, $\{id, \sigma\} \lhd S = \{id, \sigma, \rho^2, \sigma\rho^2\}$ jer je indeksa 2. Iz istog razloga $S \lhd D_4$, ali $\{id, \sigma\} \not\lhd D_4$.

ii) Normalnost jedne od podgrupa u dokazu tačke (ii) prethodnog tvrđenja je zaista neophodna, što pokazuje sledeći primer. Neka je $H = \{id, \sigma\} < D_4$, $K = \{id, \sigma\rho\} < D_4$, ali $HK = \{id, \sigma, \sigma\rho, \rho\} \not< D_4$.

iii) Da je normalnost obe podgrupe u dokazu tačke (iii) prethodnog tvrđenja neophodna pokazuje sledeći primer. Neka je $H = \{id\}$, $K = \{id, \sigma\}$. $H \lhd G$, $K < G$, ali $HK = K \not\lhd G$.

3.8. Teoreme o izomorfizmu

Teoreme o izomorfizmu su važno oruđe u konstrukciji novih izomorfizama iz već poznatih homomorfizama i izomorfizama. Osnovu predstavlja prva od njih koja je globalni koncept, dok su druge dve teoreme njene posledice. U prvoj teoremi je zatvoren trougao veza između kongruencija, homomorfizama i normalnih podgrupa. Ubuduće dakle, kadgod je dat jedan od tih objekata treba imati na umu da imamo jednoznačno određena i druga dva objekta, koji su možda zgodniji za rad.

3.8.1. Definicija. Neka je $f : \mathcal{G} \to \mathcal{S}$ homomorfizam grupa. Jezgro homomorfizma f je $Ker(f) = \{g \in G : f(g) = e\}$.

3.8.2. Teorema (I Teorema o izomorfizmu). *Neka je $f : \mathcal{G} \to \mathcal{S}$ epimorfizam grupa.*

(i) $Ker(f) \lhd G$.

(ii) $\mathcal{G}/Ker(f) \cong \mathcal{S}$.

Dokaz. (i) Pokažimo najpre da je $Ker(f) < G$. Dakle, neka je $a, b \in Ker(f)$. To znači da je $f(a) = f(b) = e$. Sada je

$$\begin{aligned} f(a^{-1}b) &= f(a)^{-1}f(b) \\ &= e^{-1}e \\ &= e. \end{aligned}$$

Dakle, $a^{-1}b \in Ker(f)$.

(ii) Označimo $Ker(f)$ sa N. Definišimo preslikavanje $g : G/N \to S$ tako da je

$$g(x/N) = f(x).$$

Dokazaćemo da je g traženi izomorfizam.

Najpre proverimo da je g dobro definisan tj. da ne zavisi od izbora predstavnika. Dakle, neka je $g(a/N) = s$ i neka je $b/N = a/N$ tj. $a \sim_N b$. Tada je $a^{-1}b \in N = Ker(f)$. Po definiciji $Ker(f)$ je

$$\begin{aligned} f(a^{-1})b) &= e \\ f(a)^{-1}f(b) &= e \\ f(b) &= f(a) \quad \text{(množenje sa } f(a) \text{ sleva)} \\ g(a/N) &= g(b/N). \end{aligned}$$

Činjenica da je g preslikavanje $1-1$ pokazuje se istim nizom jednakosti samo obrnutim redosledom.

g je očigledno *na* preslikavanje. Neka je $s \in S$. Kako je f preslikavanje *na*, postoji $a \in G$ tako da je $f(a) = s$. Tada je $g(a/N) = f(a) = s$.

Ostaje provera da je g homomorfizam. Neka su $a/N, b/N \in G/N$. Tada imamo

$$\begin{aligned} g(a/N \cdot b/N) &= g(ab/N), \text{ (po definiciji množenja klasa)} \\ &= f(ab) \\ &= f(a)f(b) \text{ (jer je } f \text{ homomorfizam)} \\ &= g(a/N)g(b/N). \quad \square \end{aligned}$$

3.8.3. Primer. Neka je $f : Z \to Z_n$ preslikavanje definisano sa $f(i) = rem_n(i)$. U Primeru 3.1.6.(i), pokazano je da je f epimorfizam grupoida. Kako je Z grupa, to je i Z_n grupa (lep način da izbegnemo neprijatnu proveru asocijativnosti). $Ker(f) = \{i : rem_n(i) = 0\} = nZ$. Dakle,

$$Z/nZ \cong Z_n.$$

3.8.4. II Teorema o izomorfizmu. *Neka je G grupa, $K, H < G$, $K \lhd G$. Tada je*

(i) $HK < G$ *i* $K \lhd HK$,

(ii) $H \cap K \lhd H$, *i*

$$HK/K \cong H/H \cap K.$$

Dokaz. (i) Dokazano je u Tvrđenju 3.7.7.

(ii) Neka je $H \cap K = N$, i $h \in H$ proizvoljni element. Kako je $K \lhd G$, to je $hK = Kh$. Sada imamo

$$\begin{aligned} hN &= h(H \cap K) \\ &= hH \cap hK \\ &= H \cap Kh \\ &= Hh \cap Kh \\ &= (H \cap K)h \\ &= hN \end{aligned}$$

(iii) Neka je $f : G \to G/K$ kanonski epimorfizam definisan sa $f(a) = a/K$. Zatim restrikujmo ovo preslikavanje na H. Tu restrikciju označimo sa f_1. Odredimo $Im(f_1)$.

$$\begin{aligned} Im(f_1) &= \{gK : f_1(h) = gK, \text{ za neki } h \in H\} \\ &= \{gK : hK = gK, \text{ za neki } h \in H\} \\ &= \{hK : h \in H\} \\ &= \{hkK : h \in H, k \in K\}, \text{ (jer je za proizvoljni } k \in K,\ kK = K) \\ &= HK/K. \end{aligned}$$

Kao restrikcija homomorfizma f_1 je homomorfizam. Neka je sada $f_2 : H \to HK/K$ preslikavanje f_1 sa kodomenom restrikovanim na $Im(f_1)$. Sada je f_2 epimorfizam. Odredimo $Ker(f_2)$.

$$\begin{aligned} Ker f_2 &= \{h \in H : hK = eK\} \\ &= \{h \in H : e^{-1}h \in K\} \\ &= \{h \in H : h \in K\} \\ &= H \cap K. \end{aligned}$$

Primenom prve teoreme o izomorfizmu na f_2 dobijamo željeno tvrđenje. □

3.8.5. Primer. Neka je $H = 6Z$ i $K = 15Z$. Tada je, u aditivnoj notaciji,

$$\begin{aligned} H + K &= \{h + k : h \in H, k \in K\} \\ &= \{6m + 15n : m, n \in Z\} \\ &= \langle 6, 15 \rangle \\ &= \langle 3 \rangle \\ &= 3Z. \end{aligned}$$

S druge strane, $H \cap K = 30Z$. Prema prethodnoj teoremi imamo,

$$3Z/15Z \cong 6Z/30Z.$$

3.8.6. III Teorema o izomorfizmu. *Neka je G grupa, $K < H < G$, $K, H \triangleleft G$. Tada je*

$$G/H \cong G/K/H/K.$$

Dokaz. Neka je $f : G/K \to G/H$ preslikavanje definisano sa

$$f(a/K) = a/H.$$

Dokazaćemo da je f epimorfizam a zatim jednostavnom primenom I teoreme o izomorfizmu dobiti željeno tvrđenje.

Najpre pokazujemo da je f dobro definisano. Neka je za $a, b \in G$, $a/K = b/K$. Tada je, po definiciji, $a^{-1}b \in K$. Kako je $K \subset H$, to $a^{-1}b \in H$, pa je $a/H = b/H$, odnosno $f(a/K) = f(b/K)$.

Preslikavanje je očigledno *na*, jer je za proizvoljni element $a/H \in G/H$, $f(a/K) = a/H$.

Ostaje da pokažemo da je f homomorfizam.

$$\begin{aligned} f(a/Kb/K) &= f(ab/K) \text{ (po definiciji množenja klasa)} \\ &= ab/H \\ &= a/H \cdot b/H \\ &= f(a/K) \cdot f(b/K). \end{aligned}$$

Izračunajmo jezgro od f.

$$\begin{aligned} Ker(f) &= \{a/K : f(a/K) = e/H\} \\ &= \{a/K : a/H = e/H\} \\ &= \{a/K : e^{-1}a \in H\} \\ &= \{a/K : a \in H\} \\ &= H/K. \end{aligned}$$

Dakle, $Ker(f) = H/K$. Primenom prve teoreme o izomorfizmu dobijamo $G/K/H/K. \cong G/H$. □

3.8.7. Primer. Neka je u Z, $H = 6Z$ a $K = 30Z$. Kako je $30Z, 6Z \triangleleft Z$, prema prethodnoj teoremi imamo

$$Z/6Z \cong (Z/30Z)/(6Z/30Z).$$

Dakle, teoreme o izomorfizmu su sjajno oruđe. One su kao čarobni štapić jer dobijamo izomorfizme bez obaveze da ih konstruišemo. Međutim u situacijama koje ne kontrolišemo korak po korak lako s naprave i greške (kao kod kalkulatora). Hajde da nastavimo zaključivanje iz ovog primera na sledeći način. Kako je $Z/30Z \cong Z_{30}$ i $6Z/30Z \cong Z/5Z \cong Z_5$, to je $Z/6Z \cong Z_{30}/Z_5$. Zaključak je pogrešan. Izraz Z_{30}/Z_5 nema smisla jer $Z_5 \not< Z_{30}$. Gde smo pogrešili? Iz $G \cong S$ i $G_1 \cong S_1$ sledi $G/G_1 \cong S/S_1$ samo ako je $G_1 < G$ i $S_1 < S$.

3.9. Dekartov proizvodi grupa

3.9.1. Tvrđenje. *Dekartov prozvod grupa je grupa.*

Dokaz. Mi tvrđenje dokazujemo samo za proizvod dve grupe, da čitaocu pažnju ne bi odvukle oznake. Dakle, neka su $\mathcal{G} = (G, *, e_G, {}^{-1_G})$ i $\mathcal{S} = (S, \cdot, e_S, {}^{-1_S})$ grupe. Ranije smo videli da je $\mathcal{G} \times \mathcal{S}$ semigrupa. Neka je $(g, s) \in G \times S$. Tada je

$$(e_G, e_S) \circ (g, s) = (e_G * g, e_S \cdot s) = (g, s)$$
$$(g^{-1_G}, s^{-1_S}) \circ (g, s) = (g^{-1_G} * g\,,\ s^{-1_S} \cdot s) = (e_G, e_S).$$

Prema Tvrđenju 3.4.5. (i), $\mathcal{G} \times \mathcal{S}$ je grupa.

3.9.2. Primer. Neka je $\mathcal{P}(S)$ grupa iz Primera 3.1.2.(ix), za S skup kardinalnosti n, $n \in N$. Neka je za svaki $A \subset S$ funkcija $\chi_A : S \to \{0, 1\}$ definisana tako da je za $i \in S$, $\chi_A(i) = 1$ akko $i \in A$.

Neka je $\mathcal{P}(U)$ isti tip grupe pri čemu je U jednoelementni podskup od S. $P(U) = \{\emptyset, U\}$. Ova struktura je očigledno izomorfna sa $(\{\top, \bot\}, \wedge)$, a takođe i sa $(Z_2, \cdot)$. Zato označimo redom elemente skupa $\mathcal{P}(U)$ sa 0 i 1. $\mathcal{P}(U)$ je očigledno podgrupa od $\mathcal{P}(S)$. Sdruge strane, ako sa $\mathcal{P}(U)^n$ označimo Dekartov proizvod n kopija grupe $\mathcal{P}(U)$, onda je

$$\mathcal{P}(S) \cong \mathcal{P}(U)^n.$$

Zaista, preslikavanje $f : P(S) \to P(U)^n$ definisano tako da za $A \subset S$ $f(S) = \chi_A$ je izomorfizam.

Kako S iz prethodnog primera ima n jednoelementnih podskupova koji imaju zajednički samo neutral, zaključujemo da je S izomorfan proizvodu svojih skorodisjunktnih podgrupa. To je specijalna situacija za jednu generalnu konstrukciju. Ona se jednostavno uopštava za ma kakve proizvode, ali mi je opet formulišemo za dve podgrupe.

3.9.3. Definicija. Grupa $\mathcal{G} = (G, \cdot, e, {}^{-1})$ je unutrašnji direktan proizvod svojih podgrupa $\mathcal{H}$ i $\mathcal{K}$ akko su ispunjeni sledeći uslovi:

(i) $G = \langle H \cup K \rangle$.
(ii) $\mathcal{K}, \mathcal{H} \lhd \mathcal{G}$.
(iii) $H \cap K = \{e\}$.

3.9.4. Tvrđenje. *Grupa $\mathcal{G} = (G, \cdot, e, {}^{-1})$ je unutrašnji direktan proizvod svojih podgrupa $|CalH$ i $\mathcal{K}$, akko za proizvoljne $h \in H$ i $k \in K$,*

$$h \cdot k = k \cdot h,$$

i za svaki $g \in G$ postoje jedinstveni $h \in H$ i $k \in K$ tako da je $g = hk$.

Dokaz. ($\Leftarrow$) Neka je $g \in G$. Kako je $g = hk$, za neke $h \in H$, $g \in G$, to je $\langle H \cup K \rangle = G$.

Neka je sada $g \in G$. Prema pretpostavci, postoje $h \in H$, $k \in K$, tako da je $g = hk$. Prema prvoj pretpostavci, imamo da je $kH = Hk$. Sada je

$$g = hkH = khH = kH = Hk = Hhk = Hg.$$

Dakle, $\mathcal{H} \lhd \mathcal{G}$. Slično se pokazuje da je $\mathcal{K} \lhd \mathcal{G}$. Neka je $g \in H \cap K$. Kako je $g = eg = ge$, gde prvi proizvod tretiramo kao $e \in H$, $g \in K$, a drugi kao $g \in H$, $e \in K$, to je na osnovu jedinstvenosti predstavljanja, $g = e$.

($\Rightarrow$) Neka je $h \in H$ i $k \in K$. Neka je $d = h^{-1}k^{-1}hk$. Kako je $H \lhd G$, to je $k^{-1}Hk = H$, pa je $k^{-1}hk = h_1 \in H$ dakle i $d = h^{-1}h_1 \in H$. Slično je $h^{-1}k^{-1}h = k_1 \in K$, pa je $d \in H \cap K = \{e\}$. Dakle $h^{-1}k^{-1}hk = e$. Množenjem obe strane jednakosti sa kh dobijamo $hk = kh$.

Neka je $g \in G$. Kako je $G = \langle H \cup K \rangle$, to prema Tvrđenju 3.5.9., $g = u_1^{m_1} \cdot u_2^{m_2} \cdot \ldots \cdot u_k^{m_k}$ za neke $k \in N$, $u_i \in H \cup K$, $m_i \in Z$, $i \leq k$. Kako su elementi iz H permutabilni sa elementima iz K, u navedenom proizvodu se činioci mogu permutovati tako da najpre dođu činioci iz H a zatim činioci iz K. Neka je h proizvod činilaca iz H a k proizvodčinilaca iz K. Dobili smo $g = hk$. Ostaje da pokažemo jedinstvenost. Neka je $g = hk = h_1k_1$. Množeći sdesna sa k^{-1} i sleva sa h_1^{-1}, dobijamo $h_1^{-1}h = h_1h^{-1}$. Kako je izraz na levoj strani jednakosti u H a izraz na desnoj strani iz K, to je $h_1^{-1}h = h_1h^{-1} = e$. Otuda je $h = h_1$ i $k = k_1$, što je i trebalo dokazati. □

3.9.4. Teorema. *(i) Neka je $\mathcal{G}$ grupa. Ako je $\mathcal{G}$ unutrašnji direktni proizvod podgrupa $\mathcal{H}$ i $\mathcal{K}$, onda je $\mathcal{G} \cong \mathcal{H} \times \mathcal{K}$.*

(ii) Ako je $\mathcal{G} = \mathcal{U} \times \mathcal{V}$, za neke grupe $\mathcal{U}, \mathcal{V}$, onda je $\mathcal{G}$ unutrašnji direktan proizvod svojih podgrupa $\mathcal{H} = (U, e_V)$ i $\mathcal{K} = (e_U, V)$.

Dokaz. (i) Prema prethodnoj lemi, za svaki $g \in G$ postoje jedinstveni $h_g \in H$ i $k_g \in K$ takoda je $g = h_g \cdot k_g$. Preslikavanje $f : G \to H \times K$ definisano tako da je $f(g) = (h_g, k_g)$, je traženi izomorfizam.

(ii) Jednostavno se proveravaju uslovi iz definicije unutrašnjeg direktnog proizvoda. Dokaz ostavljamo čitaocu. □

3.10. Ciklične grupe

3.10.1. Definicija. Grupa $\mathcal{G}$ je ciklična ako postoji $a \in G$ tako da je $G = \langle a \rangle$. Element a zovemo generatorom ciklične grupe.

3.10.2. Primer. Kako je $\mathcal{Z} = \langle 1 \rangle$, to je $\mathcal{Z}$ beskonačna ciklična grupa. Slično je $\mathcal{Z}_n = \langle 1 \rangle$, i to je ciklična grupa reda n.

3.10.3. Tvrđenje. *$\mathcal{G}$ grupa konačnog reda je ciklična akko postoji $a \in G$ tako da je $r(a) = |G|$. Element $b \in G$ je generator te grupe akko $r(b) = |G|$.*

Dokaz. Neka je G konačna ciklična grupa. Neka je $a \in G$ tako da $G = \langle a \rangle$. Otuda je $|G| = |\langle a \rangle|$. Kako je, prema Tvrđenju 3.5.15., $|\langle a \rangle| = r(a)$, to je $|G| = r(a)$ i a je traženi element.

Obrnuto, neka je $a \in G$ tako da $r(a) = |G|$. Tada je $|\langle a \rangle| = |G|$. Kako je $\langle a \rangle \subset G$ i oba imaju istu, konačnu kardinalnost, $\langle a \rangle = G$.

Što se drugog dela tvrđenja tiče, upravo smo dokazali da je bilo koji element reda $|G|$ generator grupe $\mathcal{G}$. Obrnuto, neka je b generator, tj. $\langle b \rangle = G$. Tada je $r(b) = |\langle b \rangle| = |G|$. □

3.10.4. Posledica. *Svaka grupa prostog reda je ciklična.*

Dokaz. Neka je $\mathcal{G}$ grupa prostog reda p. Neka je $a \in G$, $a \neq e$. Otuda je $r(a) > 1$. Prema Tvrđenju 3.5.25., $r(a)|p$. Kako je $r(a) > 1$ i p prost broj, $r(a) = p$. Tvrđenje sada sledi iz prethodnog tvrđenja. □

U sledećem tvrđenju pokazuje se da su ciklične grupe iz Primera 3.10.2., do na izomorfizam, jedine ciklične grupe.

3.10.5. Tvrđenje. *(i) Konačna ciklična grupa reda n izomorfna je sa $\mathcal{Z}_n$.*
(ii) Beskonačna ciklična grupa izomorfna je sa $\mathcal{Z}$.

Dokaz. (i) Neka je C konačna ciklična grupa reda n, i neka je $G = \langle a \rangle$. Tada je, prema Tvrđenju 3.5.15. (i), $G = \{a^i : 0 \leq i < n\}$ i $r(a) = n$. Definišimo preslikavanje $f : C \to Z_n$ takoda je $f(a^i) = i$. Preslikavanje je očigledno *na* i $1 - 1$. Proverimo da li je f homomorfizam. Za i, j koji zadovoljavaju $0 \leq i, j < n$ je $0 \leq i + j < 2n$. Zato u C imamo da ako je $i + j < n$, $a^i \cdot a^j = a^{i+j} = a^{i+_n j}$, a ako je $n \leq i + j < 2n$, onda je $a^i \cdot a^j = a^{i+j} = a^{i+j-n} \cdot a^n = a^{i+_n j} \cdot e = a^{i+_n j}$. Zato je

$$\begin{aligned} f(a^i \cdot a^j) &= f(a^{i+j}) \\ &= f(a^{i+_n j}) \\ &= i +_n j \\ &= f(a^i) +_n f(a^j). \end{aligned}$$

(ii) Neka je C beskonačna ciklična grupa i neka je $C = \langle a \rangle$. Prema Tvrđenju 3.5.15.(ii), $C = \langle a \rangle = \{a^i : i \in Z\}$. Jednostavno se proverava da je preslikavanje $f : C \to Z$ definisano sa $f(a^i) = i$ izomorfizam. □

3.10.6. Lema. *Neka je $\mathcal{G}$ ciklična grupa konačnog reda k, generisana elementom a i neka je $b \in G$. Postoji $i < k$ tako da je $b = a^i$. b je generator grupe $\mathcal{G}$ akko $(i,k) = 1$.*

Dokaz. Dakle, $G = \langle a \rangle$. Neka je $|G| = k$. Tada je, prema Tvrđenju 3.5.15.(i), $r(a) = k$ i $G = \langle a \rangle = \{a^i : 0 \leq i < k\}$. Kako $b \in G$, $b = a^i$, za neki i, $0 \leq i < k$. Prema Tvrđenju 3.10.3., b je generator od G akko je $r(b) = k$. Pretpostavimo da je $(i,k) = 1$. Tada je

$$\begin{aligned} b^s = e &\Leftrightarrow (a^i)^s = e \\ &\Leftrightarrow a^{si} = e \\ &\Leftrightarrow k | si \\ &\Leftrightarrow k | s. \end{aligned}$$

Dakle, $r(b) = k$, pa je b generator od G.

Obratnu implikaciju dokazujemo kontrapozicijom. Dakle, neka je $(i,k) = d > 1$. Tada je

$$\begin{aligned} b^{\frac{k}{d}} &= (a^i)^{\frac{k}{d}} \\ &= (a^k)^{\frac{i}{d}} \\ &= e. \end{aligned}$$

Dakle, $r(b) \leq \frac{k}{d} < k$, pa b nije generator. □

3.10.7. Tvrđenje. (i) *Podgrupa ciklične grupe je ciklična.*

(ii) *Homomorfna slika ciklične grupe je ciklična.*

(iii) *Dekartov proizvod cikličnih grupa C_k i C_l je ciklična grupa akko $(k,l) = 1$.*

Dokaz. (i) Neka je $G = \langle a \rangle$ i $H < G$. Neka je dalje $k = min\{i \in N^+ : a^i \in H\}$, i $c = a^k$. Dokazaćemo da je $H = \langle c \rangle$.

Kako je $c \in H$, a $\langle c \rangle$ najmanja podgrupa koja sadrži c, to je $\langle c \rangle \subset H$. Dokažimo $H \subset \langle c \rangle$. Zaista, neka je najpre $b \in H$. Prema Tvrđenju 3.5.11., $b = a^i$ za neko $i \in Z$. Neka je $i = qk + r$, za $0 \leq r < k$. Tada je $a^i = a^{qk}a^r \in H$. Otuda je $a^r = a^i(a^k)^{-q} = a^i c^{-q}$. Kako su oba elementa na desnoj strani iz H to je i $a^r \in H$. Kako je k minimalan u N^+ sa tom osobinom, to $r \notin N^+$. Kako je $r \geq 0$, to je $r = 0$. Kako je $c = a^k \in H$, to je i $b = a^{qk} = c^q \in H$. Kako je b proizvoljni element iz H to je $H < \langle c \rangle$. Dakle, $H = \langle c \rangle$, pa je otuda ciklična.

(ii) Neka je $G = \langle a \rangle$ ciklična grupa generisana elementom a, $f : \mathcal{G} \to \mathcal{S}$ epimorfizam i $c = f(a)$. Dokazaćemo da je $\mathcal{S} = \langle c \rangle$. Neka je d proizvoljni

element iz S. Kako je f epimorfizam, postoji $b \in G$ tako da je $f(b) = d$. Kako je $G = \langle a \rangle$, to postoji $i \in Z$ tako da je $b = a^i$. Tada je

$$\begin{aligned} d &= f(b) \\ &= f(a^i) \\ &= (f(a))^i \\ &= c^i. \end{aligned}$$

Dakle, $d \in \langle c \rangle$. Kako je d proizvoljni element iz S, to je $S = \langle c \rangle$. Time je pokazano da je S ciklična grupa.

(iii) Na osnovu definicije množenja kardinala, $|C_k \times C_l| = kl$.

($\Rightarrow$) Ovu stranu implikacije dokazujemo kontrapozicijom. Dakle, neka je $(k, l) = d > 1$. Neka je (a, b) proizvoljni element iz $C_k \times C_l$. Kako je $a \in C_k$ i $b \in C_l$, to je $a^k = e$ i $b^l = e$. Tada je

$$\begin{aligned} (a, b)^{\frac{kl}{d}} &= (a^{\frac{kl}{d}}, b^{\frac{kl}{d}}) \\ &= ((a^k)^{\frac{l}{d}}, (b^l)^{\frac{k}{d}}) \\ &= (e, e). \end{aligned}$$

Otuda je $r((a, b)) \leq \frac{kl}{d} < kl$. Kako u $C_k \times C_l$ nema elementa reda kl, $C_k \times C_l$ nije ciklična grupa.

($\Leftarrow$) Neka je $(k, l) = 1$. Za $n \in N^+$ imamo

$$\begin{aligned} (a, b)^n = (e, e) &\Leftrightarrow (a^n, b^n) = (e, e) \\ &\Leftrightarrow a^n = e \ \& \ b^n = e \\ &\Leftrightarrow k|n \ \& \ l|n \\ &\Leftrightarrow kl|n \text{ (jer je } (k, l) = 1 \text{).} \end{aligned}$$

Dakle, $r((a, b)) = kl$, pa je (a, b) generator grupe $C_k \times C_l$. Dakle, $C_k \times C_l$ je ciklična grupa. Kako su sve ciklične grupe istog reda izomorfne imamo i $C_k \times C_l \cong C_{kl}$. $\square$

3.11. Opis nekih konačnih grupa

Sa tehnikom koju smo do sada razvili možemo opisati grupe reda $n \leq 8$.

n=2,3,5,7 Kako su to prosti brojevi, postoji , do na izomorfizam, samo jedna grupa tog reda $\mathcal{Z}_n$.

n=4 Znamo već dve neizomorfne grupe reda 4. To su Z_4 koja je ciklična i $Z_2 \times Z_2$, Klajnova grupa, koja nije ciklična. Pokazaćemo da su to i jedine grupe reda 4. Dakle, neka je $|G| = 4$. Ako G ima element reda 4 ona je izomorfna sa Z_4. Zato pretpostavimo da G nema element reda 4. Kako su redovi elemenata iz G faktori broja 4, i e je jedini element u grupi koji ima red 1, to je $G = \{e, a, b, c\}$, i $a^2 = b^2 = c^2 = e$. Kako su svi elementi (sem e) reda 2, to je G komutativna. Iz $ab = e$ sledi da je b inverz od a, suprotno činjenici da je a samoinvertovan. Iz $a \cdot b = a$ skraćivanjem sa a dobijamo $a = e$. Iz istog razloga $a \cdot b \neq b$. Dakle, $a \cdot b = c$. Zbog komutativnosti je $b \cdot a = c$. Time je potpuno određena tablica grupe G. Preslikavanje f definisano sa: $f((0,1)) = a$, $f((1,0)) = b$ određuje izomorfizam G i $Z_2 \times Z_2$.

n=6 Znamo dve neizomorfne grupe reda 6: Z_6 i $D_3 \cong S_3$. Pokazaćemo da su to jedine grupe reda 6. Ako G ima element reda 6, $G \cong Z_6$. Zato pretpostavimo da su svi elementi reda 2 ili 3. Pretpostavimo najpre da su svi elementi reda 2. Tada je G komutativna. Neka je $a, b \in G\{e\}$, $a \neq b$ i $c = a \cdot b$. Tada je, iz istog razloga kao u slučaju $n = 4$, $c \notin \{e, a, b\}$. Tada je $H = \{e, a, b, c\} < G$. Prema Lagranžovoj teoremi $|H| | |G|$, tj. $4|6$. Kontradikcija. Dakle, G ima element reda 3. Označimo ga sa ρ. Tada je $N = \{e, \rho, \rho^2\} < G$. Kako je $[G : N] = 2$, $N \lhd G$. Neka je $\sigma \in G \setminus N$. Kako $\sigma \notin N$, $\sigma N \neq N$. Dakle, $\sigma N = N^c = \{\sigma, \sigma\rho, \sigma\rho^2\}$. Koliko je σ^2? Pretpostavimo najpre da je $r(\sigma) = 3$. Tada je $\sigma^2 \neq e$. Pretpostavka da $\sigma^2 \in N^c$, skraćivanjem daje kontradikciju $\sigma \in \{e, \rho, \rho^2\}$. Dakle, $\sigma \in \{\rho, \rho^2\}$. Međutim iz $\sigma^2 = \rho$ kvadriranjem sledi $\sigma = \sigma^4 = \rho^2$, a $\sigma^2 = \rho^2$ kvadriranjem daje $\sigma = \sigma^4 = \rho^4 = \rho$. Kontradikcija. Dakle, $r(\sigma) = 2$. Ostaje još da odredimo $\rho \cdot \sigma$. Jednostavnom eliminacijom se zaključuje da $\rho \cdot \sigma \in \{\sigma \cdot \rho, \sigma \cdot \rho^2\}$. Međutim, iz $\rho \cdot \sigma = \sigma \cdot \rho$ bi sledilo da je $\sigma \cdot \rho$ element reda 6. Kontradikcija. Dakle, $\rho \cdot \sigma = \sigma \cdot \rho^2$. Dakle, $G \cong D_3$.

n=8 Znamo 5 neizomorfnih grupa reda 8: Z_8, $Z_2 \times Z_4$, $Z_2 \times Z_2 \times Z_2$, D_4 i K. Prve tri su Abelove dok su poslednje dve nekomutativne. Prve tri su međusobno neizomorfne jer prva ima element reda 8, druga ima element najvišeg reda 4, a u trećoj su svi elementi reda 2. Poslednje dve su neizomorfne jer D_4 ima 5 elemenata reda 2, a K samo jedan. Svaka grupa reda 8 je izomorfna jednoj od ovih pet grupa. Dokaz se izvodi analogno dokazu za $n = 6$ i ostavljamo ga čitaocu kao vežbu.

3.12. Grupa permutacija S_n.

3.12.1. Definicija. Neka je X skup i $S(X)$ skup svih bijekcija (permutacija). Grupu $\mathcal{S}_x = (S(X), \circ)$ nazivamo grupom permutacija skupa X. Za $X = I_n = \{1, \ldots, n\}$, $\mathcal{S}_X$ označavamo sa $\mathcal{S}_n$.

Kako svaka bijekcija skupova indukuje izomorfizam njihovih grupa permutacija, to $\mathcal{S}_X$ ne zavisi od elemenata skupa X već od njegove kardinalnosti. Značaj ove grupe jasno se vidi iz sledeće teoreme.

3.12.2. Teorema (Kejli). *Svaka grupa je izomorfna nekoj grupi permutacija.*

Dokaz. Iskoristićemo Lemu 3.2.13. Neka je $f : G \to G^G$ preslikavanje iz Leme 3.2.13. Kako je homomorfna slika grupe grupa, $Im(f)$ je grupa. Kako su svi elementi iz Imf invertibilni, svi su bijekcije. Dakle, $Imf < S(G)$. Otuda je $G \cong Imf$ tj. G je izomorfna grupi permutacija (ali ne grupi $S(G)$).

Posle ovog tvrđenja, mi možemo za bilo koju grupu smatrati da su njeni elementi permutacije nekog skupa, ako nam ta konkretizacija apstraktnog objekta znači u psihološkom smislu. Ova teorema međutim znači i da grupe S_X imaju dosta komplikovanu strukturu jer "u njih može svašta da stane".

Kako smo videli već u $S_3 = D_3$, S_n za $n \geq 2$ nije Abelova grupa. Ipak u nekim situacijama permutacije komutiraju.

3.12.3. Definicija. Neka su $\sigma, \tau \in S_n$. Kažemo da su σ i τ disjunktne permutacije ako za svaki $i \leq n$ $\sigma(i) = i$ ili $\tau(i) = i$.

3.12.4. Tvrđenje. *Disjunktne permutacije komutiraju među sobom.*

Dokaz. Neka su $\sigma, \tau \in S_n$ i $i \leq n$. Prema definiciji disjunktnosti permutacija, jedna od ove dve permutacije ostavlja i fiksnim. Neka je to σ. Dakle, $\sigma(i) = i$. Razlikujemo dva slučaja. Neka je najpre $\tau(i) = i$. Tada je $\tau \circ \sigma(i) = \sigma \circ \tau(i) = i$. Ostaje slučaj kada je $\tau(i) = j$ i $j \neq i$. Kako je τ bijekcija, $\tau(j) \neq j$ (j je već slika od i). Po definiciji disjunktnosti permutacija $\sigma(j) = j$. Sada imamo $\sigma \circ \tau(i) = \sigma(j) = j$ i $\tau \circ \sigma(i) = \tau(i) = j$. Dakle, u oba slučaja je $\tau \circ \sigma(i) = \sigma \circ \tau(i)$. Kako je $i \leq n$ proizvoljan $\tau \circ \sigma = \sigma \circ \tau$.

3.12.5. Definicija. Nekaje $k \geq 2$ i $C = (i_1, \ldots, i_k)$ niz različitih elemenata skupa I_n. Permutacija σ definisana tako da je $\sigma(i_s) = i_{s+_k 1}$ naziva se ciklom dužine k, u oznaci $(i_1\, i_2\, \ldots i_k)$. Ciklovi dužine 2 nazivaju se transpozicijama.

3.12.6. Tvrđenje. *Svaka permutacija iz S_n može se predstaviti kao proizvod disjunktnih ciklova.*

Dokaz. Neka je $\sigma \in S_n$. Definišimo relaciju ekvivalencije na I_n tako da

$$i \sim j \Leftrightarrow \exists m \in Z\, (\sigma^m(i) = j).$$

Lako se proverava da je $\sim$ relacija ekvivalencije. Opišimo klase ekvivalencije. Neka je $i \in I_n$. $i/\sim = \{j \in I_n : i \sim j\} = \{\sigma^m(i) : m \in Z\}$. Kako je

$i/\sim = \{\sigma^j(i) : j \in N\} \subset I_n$, dakle konačan skup, postoje $j, l \in N^+$ tako da je $j < l$ i $\sigma^j(i) = \sigma^l(i)$. Tada je $\sigma^{l-j}(i) = i$, za $l - j \in N^+$. Neka je $k_i = min\{j \in N^+ : \sigma^j(i) = i\}$. Tada je $i/\sim = \{\sigma^m(i) : 0 \leq m < k_i\}$. Zaista, neka je $s \in Z$ i $s = k_i q + r$, $0 \leq r < k_i$. Tada je $\sigma^s(i) = \sigma^r(\sigma^{k_i q}(i)) = \sigma^r(i)$. Pri tome je za $0 \leq j < l < k_i$, $\sigma^j(i) \neq \sigma^l(i)$ zbog minimalnosti k_i. Dakle, $i/\sim$ određuje cikl $c_i = (i, \sigma(i), \ldots \sigma_{k-1}(i))$ dužine k_i.

Izaberimo sada transverzalu količničkog skupa $I_n/\sim$. Dokazaćemo da je $\sigma = \prod_{t \in T} c_t$. Kako su ciklovi c_t, $t \in T$, disjunktne permutacije, redosled kompozicije nije bitan.

Neka je $j \in I_n$. Kako klase ekvivalencije čine particiju skupa I_n i T je transverzala faktor skupa, postoji $t \in T$, tako da je $j \sim t$. Tada je $j \in t/\sim$, dakle postoji $0 \leq m < k_t$, tako da je $j = \sigma^m(t)$. Otuda je $c_t(j) = c_t(\sigma^m(t)) = \sigma^{m+k_t-1}(t) = \sigma(\sigma^m(t)) = \sigma(j)$. Kako ostali ciklovi ostavljaju j nepromenjenim, to je $\prod_{t \in T} c_t(j) = \sigma(j)$. Kako je j prozvoljan, $\prod_{t \in T} c_t = \sigma$.

3.12.7. Primer. Ilustrovaćemo prethodno tvrđenje na primeru. Polazimo od 1 i pratimo njegov trag dokgod se ne vratimo opet u 1. Sada nastavljamo na isti način sa prvim elementom koji nije uključen u prvi cikl, itd.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 7 & 5 & 4 & 6 & 1 & 2 \end{pmatrix} = (137)(28)(45)(6).$$

Naravno (6) nije cikl (mada se može dodefinisati kao cikl dužine 1) ali smo pomenuli i (6) da ne bi nedostajao na desnoj strani. Inače $(6) = id$.

Sledeće tvrđenje je važno oruđe u manipulaciji ciklovima.

3.12.8. Tvrđenje. *Neka je $c = (i_1 \ldots i_k)$ cikl dužine k iz S_n, i τ proizvoljna permutacija iz S_n. Tada je $\tau \circ c \circ \tau^{-1} = (\tau(i_1), \ldots, \tau(i_k))$.*

Dokaz. Neka je za $s \leq k$, $\tau(i_s) = j_s$. Prema definiciji cikla $c(i_s) = i_{s+k1}$, $s \leq k$. Treba da pokažemo da ako je $j = j_s$, za neko $j \leq k$, onda je $\tau \circ c \circ \tau^{-1}(j) = \tau \circ c \circ \tau^{-1}(j_s) = j_{s+1}$, a za $j \notin \{j_1, \ldots, j_k)\}$, $\tau \circ c \circ \tau^{-1}(j) = j$.

Zaista, neka je najpre $j = j_s$, za neko $s \leq k$. Tada je

$$\begin{aligned} \tau \circ c \circ \tau^{-1}(j) \tau \circ c \circ \tau^{-1}(j_s) &= \tau \circ c \circ \tau^{-1}(\tau(i_s)) \\ &= \tau \circ c(i_s) \\ &= \tau(i_{s+1}) \\ &= j_{s+1}. \end{aligned}$$

Neka je sada $j \notin \{j_1, \ldots, j_k\}$. Odavde, i iz činjenice da je je τ bijekcija, imamo da $\tau^{-1}(j) \notin \{\tau^{-1}(j_1), \ldots, \tau - 1(j_k)\}$ tj. $\tau^{-1}(j) \notin \{i_1, \ldots, i_k\}$. Po definiciji cikla c, $c(\tau^{-1}(j)) = \tau^{-1}(j)$. Zato imamo

$$\begin{aligned} \tau \circ c \circ \tau^{-1}(j) &= \tau(c(\tau^{-1}(j_s))) \\ &= \tau(\tau^{-1}(i_s)) \\ &= i_s \\ &= j. \quad \square \end{aligned}$$

3.12.9. Posledica. *Svaka permutacija iz S_n može se predstaviti kao kompozicija transpozicija.*

Dokaz Prema Tvrđenju 3.12.6. , dovoljno je dokazati da je svaki cikl kompozicija transpozicija. Neka je $(1\,2 \ldots k)$ cikl dužine k. Tada je $(1\,2 \ldots k) = (1\,k) \ldots (1\,3)\,(1\,2)$. Zaista, neka je τ kompozicija na desnoj strani jednakosti. Tada je za $1 \leq i < k$,

$$\begin{aligned} \tau(i) &= (1\,k) \ldots (1\,i+1)(1\,i)(i) \\ &= (1\,k) \ldots (1\,i+1)(1) \\ &= (1\,k) \ldots (i+1) \\ &= i+1. \end{aligned}$$

Takođe je $\tau(k) = (1\,k)(k) = 1$.

Kako je $(1\,2 \ldots k) = (k\,1\,2 \ldots k-1)$ to imamo i dekompoziciju $(1\,2 \ldots k) = (k\,k-1) \ldots (k\,2) \ldots (k\,1)$. $\square$

Dakle, grupa S_n reda $n!$ generisana je skupom transpozicija koji ima $\frac{n(n-1)}{2}$ članova. Možemo naći i manje generatorne skupove.

3.12.10. Primer. Skup $\{(n\,1), (n\,2) \ldots, (n\,n-1)\}$ je generatorni skup grupe S_n. Dovoljno je pokazati da ovaj skup generiše sve transpozicije. Neka je $(i\,j)$ proizvoljna transpozicija u S_n. Tada je za $\tau = (n\,i)$,

$$\begin{aligned} (n\,i)(n\,j)(n\,i) &= (n\,i)^{-1}(n\,j)(n\,i) \\ &= (\tau(n)\,\tau(j)) \\ &= (i\,j). \end{aligned}$$

Dakle, grupa S_n generisana je sa samo $n-1$ transpozicijom.

3.12.11. Primer. Neka je $\tau = (1 \ldots n-1)$ i $\sigma = (n-1\, n)\}$. Dvočlani skup permutacija $\{\sigma, \tau\}$ generiše S_n. Da bi to pokazali, dovoljno je pokazati da taj skup generiše sve transpozicije iz prethodnog primera.

$$\begin{aligned}\tau^{-i}\sigma\tau^i &= (\tau^i(n-1)\,\tau^i(n)) \\ &= (i\,n).\end{aligned}$$

Dakle, S_n je generisana sa samo 2 permutacije. Manji skup generatora nije moguće naći. Ako bi S_n bila generisana sa samo jednim elementom, bila bi ciklična, dakle komutativna, a mi znamo da S_n, za $n \geq 3$, nije komutativna.

U nastavku razmatramo jedan važan epimorfizam grupe S_n na grupu $(\{1,-1\},\cdot)$.

3.12.12. Definicija. Neka je $\pi : S_n \to Q$ preslikavanje definisano tako da je za $\sigma \in S_n$,

$$\pi(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}.$$

3.12.13. Primer. Prema definiciji očigledno je $\pi(id) = 1$. Pokazaćemo da ako je σ transpozicija $(1\,k)$, onda je $\pi(\sigma) = -1$. Iz definicije je očigledno da je za $i, j \notin \{1,k\}$, $\sigma(i) = i$ i $\sigma(j) = j$, pa su svi ti činioci jednaki 1. Za razmatranje ostaju samo slučajevi: $i = 1$ i $j = k$; $i = 1$ i $j \notin \{1,k\}$; $i = k$ i $j > k$; $i \notin \{1,k\}$ i $j = k$. Zato imamo

$$\begin{aligned}\pi(\sigma) &= \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i} \\ &= \frac{\sigma(k)-\sigma(1)}{k-1} \prod_{j\notin\{1,k\}} \frac{\sigma(j)-\sigma(1)}{j-1} \cdot \prod_{j>k} \frac{\sigma(j)-\sigma(k)}{j-k} \cdot \prod_{1<i<k} \frac{\sigma(k)-\sigma(i)}{k-i} \\ &= \frac{1-k}{k-1} \prod_{j\notin\{1,k\}} \frac{j-k}{j-1} \cdot \prod_{j>k} \frac{j-1}{j-k} \cdot \prod_{1<i<k} \frac{1-i}{k-i} \\ &= (-1) \prod_{j\notin\{1,k\}} \frac{j-k}{j-1} \cdot \prod_{j>k} \frac{j-1}{j-k} \cdot \prod_{1<j<k} \frac{1-j}{k-j}, \text{ (smena } i=j) \\ &= (-1) \prod_{j\notin\{1,k\}} \frac{j-k}{j-1} \cdot \prod_{j\notin\{1,k\}} \frac{j-1}{j-k} \\ &= -1.\end{aligned}$$

3.12.14 Tvrđenje. *Neka je Q skup racionalnih brojeva.*

(i) *Preslikavanje $\pi : S_n \to Q$ je homomorfizam.*

(ii) *$Im(\pi) = \{-1, 1\}$.*

Dakle, π je epimorfizam grupe S_n na grupu $(\{1, -1\}, \cdot)$.

Dokaz. Neka su $\sigma, \tau \in S_n$. $T = \{((\tau(i), \tau(j)) : i < j \& \tau(i) < \tau(j)\}$ i $U = \{(\tau(i), \tau(j)) : i < j \& \tau(i) > \tau(j)\}$. Kako je τ bijekcija, za svaki $(k, l) \in I_n \times I_n$, ako je $k < l$ onda $(k, l) \in T$ ili $(l, k) \in U$. Ako je $U' = \{(l, k) : (k, l) \in U$, onda je $\{(k, l) : k < l\} = T \cup U'$. Sada imamo,

$$\pi(\sigma \circ \tau) = \prod_{i<j} \frac{\sigma \circ \tau(j) - \sigma \circ \tau(i)}{j - i}$$

$$= \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i}.$$

Kako je drugi proizvod po definiciji jednak $\pi(\tau)$, ostaje da pokažemo da je prvi proizvod jednak $\pi(\sigma)$.

$$\prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} = \prod_{(\tau(i),\tau(j)) \in T} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{(\tau(i),\tau(j)) \in U} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}$$

$$= \prod_{(\tau(i),\tau(j)) \in T} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{(\tau(j),\tau(i)) \in U'} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}$$

Uvedimo u prvom proizvodu smenu $\tau(i) = k$ i $\tau(j) = l$, a u drugom $\tau(i) = l$ i $\tau(j) = k$. Sada imamo,

$$\prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} = \prod_{(k,l) \in T} \frac{\sigma(l) - \sigma(k)}{l - k} \cdot \prod_{(k,l) \in U'} \frac{\sigma(k) - \sigma(l)}{k - l}$$

$$= \prod_{(k,l) \in T} \frac{\sigma(l) - \sigma(k)}{l - k} \cdot \prod_{(k,l) \in U'} \frac{\sigma(l) - \sigma(k)}{l - k}$$

$$= \prod_{k<l} \frac{\sigma(l) - \sigma(k)}{l - k}$$

$$= \pi(\sigma).$$

Dakle, $\pi(\sigma \circ \tau) = \pi(\sigma) \cdot \pi(\tau)$. Kako je svaka permutacija proizvod transpozicija oblika $(1\ k)$, postoje transpozicije $c_1, \ldots c_s$, tako da je $\sigma = c_1 \circ \ldots c_s$. U prethodnom primeru videli smo da je $\pi(c_i) = -1$, za $i \leq s$. Otuda je

$$\pi(\sigma) = \pi(c_1 \circ \ldots c_s) = \pi(c_1) \cdot \ldots \cdot \pi(c_s) = (-1)^s \in \{-1, 1\}.$$

Dakle, $Im(\pi) = \{-1, 1\}$. □

3.12.15. Definicija. Skup parnih permutacija u S_n je $A_n = Ker(\pi)$. Permutacije iz $S_n \setminus A_n$ nazivamo neparnim.

Prema prvoj teoremi o izomorfizmu, $A_n \lhd S_n$ i kako je $\frac{S_n}{A_n} \cong \{-1, 1\}$, to je $[S_n : A_n] = 2$. Otuda je, prema posledici Lagranžove teoreme, $|A_n| = \frac{n!}{2}$.

3.12.16. Posledica. *Neka je $c = (1 \ldots k)$ cikl dužine k. $\pi(c) = (-1)^{k-1}$.*

Dokaz. Kako je $c = (1\,k) \circ \ldots (1\,2)$, to je $\pi(c) = (-1)^{k-1}$. □

3.12.17. Posledica. *Neka je $\sigma = c_1 \ldots c_l$, predstavljanje permutacije σ kao proizvoda disjunktnih ciklova, i s broj invarijantnih elemenata permutacije σ. Tada je*

$$\pi(\sigma) = (-1)^{n-l-s}.$$

Dokaz. Neka je k_i dužina i-tog cikla. Kako je svaki element iz I_n sadržan u jednom i samo jednom ciklu ili je invarijantan, to je $n = \sum_{i \leq l} k_i + s$, pa imamo

$$\begin{aligned}
\pi(\sigma) &= \prod_{i \leq l} \pi(c_i) \\
&= \prod_{i \leq l} (-1)^{k_i - 1} \\
&= (-1)^{\sum_{i \leq l} (k_i - 1)} \\
&= (-1)^{\sum_{i \leq l} k_i - l} \\
&= (-1)^{n-s-l)}.
\end{aligned}$$

3.12.18. Primer. Nalazimo parne permutacije u S_4. koristićemo terminologiju u kojoj invarijantni elementi određuju cikl dužine 1. Kako je $n = 4$ paran, prema prethodnom tvrđenju, $\sigma \in S_4$ je parna ako je predstavljiva kao proizvod parnog broja ciklova. Ako su to četiri disjunktna cikla, dužine 1, onda je $\sigma = id$. Preostaje slučaj kada je σ proizvod dva disjunktna cikla. Oni mogu biti oba dužine 2 ili je jedan dužine 3, a drugi dužine 1 tj. imamo jedan invarijantan element, pa je σ cikl dužine 3. Otuda je skup parnih permutacija u S_4, skup

$$A_4 = \{id, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}.$$

Primetimo da je $B = \{id, (12)(34), (13)(24), (14)(23)\} \lhd S_4$. Kako su svi elementi iz B reda najviše dva, oni su samoinvertovani. Jednostavno se

proverava da je proizvod dva elementa iz B opet u B, pa je $B < A_4$. Proverimo da je B normalna podgrupa od S_4. Neka je $\tau \in S_n$ i $\sigma = c_1c_2 \in B$, gde su c_1 i c_2 transpozicije. Tada je,

$$\tau\sigma\tau^{-1} = \tau c_1 c_2 \tau^{-1} = (\tau c_1 \tau^{-1})(\tau c_2 \tau^{-1}) = \tau_1\tau_2.$$

Prema Tvrđenju 3.12.8., τ_1 i τ_2 su disjunktne transpozicije, pa imamo $\tau\sigma\tau^{-1} \in B$. Dakle, $B \lhd S_4$. Otuda je i $B \lhd A_4$. Kako je i $C = \{id, (12)(34)\} \lhd B$, to imamo lanac normalnih podgrupa:

$$\{e\} \lhd C \lhd B \lhd A_4 \lhd S_4.$$

Interesantno je da su sve faktor grupe susednih članova niza reda 2 ili 3, pa su kao takve ciklične i komutativne.

U sledećem tvrđenju pokazujemo da takav niz ne postoji za $n \geq 5$, ali najpre dokažimo jednu lemu.

3.12.19. Lema. *Neka je $n \geq 5$ i $H \lhd A_n$. Ako H sadrži cikl dužine 3, onda je $H = A_n$.*

Dokaz. Neka je $c = (i_1, i_2, i_3)$ cikl dužine 3 u A_n. Pokazaćemo da H sadrži sve ciklove dužine 3. Zaista neka je $c' = (j_1, j_2, j - 3)$, proizvoljni cikl dužine 3 u A_n, i neka je $\tau \in A_n$ permutacija takva da je $\tau(i_s) = j_s$, $s \leq 3$. Ako je τ izabrana tako da nije u A_n, onda se permutovanjem vrednosti u dvema tačkama različitim od i_1, i_2, i_3 obezbeđuje $\tau \in A_n$. Tada je, prema Tvrđenju 3.12.8. $\tau c \tau^{-1} = c'$. Kako je $c \in H$ i $H \lhd A_n$, to je $c' \in H$. Neka je $\sigma \in A_n$. Prema Tvrđenju 3.12.9., σ je proizvod transpozicija, a kako je σ u A_n, taj broj je paran. Dakle, σ je proizvod parova transpozicija. Kako je za proizvoljni par transpozicija (ij) i (kl), $(ij)(kl) = (ilk)(ijk)$, i H sadrži sve ciklove dužine 3, $\sigma \in H$. Kako je σ proizvoljan, $H = A_n$. □

3.12.20. Tvrđenje. *A_n, $n \geq 5$ nema netrivijalnih normalnih podgrupa.*

Dokaz. Neka je $H \lhd A_n$, $H \neq \{e\}$. Prema prethodnoj lemi, dovoljno je dokazati da H sadrži cikl dužine 3 pa da imamo $H = A_n$. Razlikujemo nekoliko slučajeva.

(A) Postoji $\sigma \in H$ tako da σ u svojoj dekompoziciji sadrži cikl c dužine $k \geq 4$. Neka je $c = (1234\ldots)$. Primetimo da je $c^{-1} = (\ldots 4321)$. Tada je $\sigma = \tau c$ za neku permutaciju τ. Neka je $\nu = (123)$. Kako su ν i τ disjunktne, one komutiraju. Otuda je

$$\begin{aligned}\nu\sigma\nu^{-1}\sigma^{-1} &= \nu c\tau\nu^{-1}\tau^{-1}c^{-1} \\ &= (\nu c\nu^{-1})c^{-1}\tau\tau^{-1} \\ &= (2314\ldots)c^{-1} = (2314\ldots)(\ldots 4321) = (124) \in H.\end{aligned}$$

Dakle, u svim preostalim slučajevima su svi ciklovi koji se pojavljuju u permutacijama iz H, dužine 2 ili 3.

(B) Postoji permutacija u H koja sadrži bar jedan cikl dužine 3.

B1 Postoji permutacija $\sigma \in H$ koja sadrži tačno jedan cikl dužine 3. Tada je $\sigma = c \circ \tau$, gde je τ kompozicija trnspozicija, dakle element reda 2. Tada je

$$\sigma^2 = c^2 \circ \tau^2 = c^2 = c \in H.$$

(B2) Sve permutacije iz H koje sadrže ciklove dužine 3 sadrže bar po dva takva cikla. Neka je $\sigma = c_1 c_2 \tau$, gde je $c_1 = (123)$, $c_2 = (3,4,5)$ i $\tau \in A_n$. Neka je $c = (234)$. Tada je

$$\begin{aligned} c\sigma c^{-1}\sigma &= cc_1c_2\tau c^{-1}c_1c_2\tau \\ &= (cc_1c^{-1})(cc_2c^{-1})c_1c_2\tau\tau \\ &= (134)(425)(123)(345) \\ &= (15324) \in H. \end{aligned}$$

Time je ovaj slučaj sveden na (A).

(C) Sve permutacije iz H u svojoj dekompoziciji sadrže samo transpozicije. (C1) Postoji permutacija iz H koja sadrži samo dve transpozicije. Neka je to $\sigma = c_1 c_2$, gde je $c_1 = (12)$ i $c_2 = (34)$. Neka je $c = (152)$. Tada je

$$(c\sigma c^{-1})\sigma = (51)(34)(12)(34) = (51)(12) = (125) \in H.$$

(C2) Sve permutacije iz H sadrže bar po tri transpozicije. Neka je $\sigma = c_1 c_2 c_3 \tau$, gde je $c_1 = (12)$, $c_2 = (34)$, $c_3 = (56)$, i $\tau \in S_n$, jedna od njih. Nek je $\nu = (23)(45)$. Tada je

$$(\nu\sigma\nu)\sigma = (13)(25)(46)(12)(34)(56) = (541)(623) \in H.$$

Time je ovaj slučaj sveden na slučaj (B). □

3.12.21. Posledica. *Za $n \geq 5$, jedina netrivijalna normalna podgrupa od S_n je A_n.*

Dokaz. Neka je $n \geq 5$ i $K \triangleleft S_n$. Tada je $K \cap A_n \triangleleft A_n$. Kako A_n nema netrivijalnih normalnih podgrupa, $K \cap A_n = \{e\}$ ili $K \cap A_n = A_n$. U drugom slučaju je $K = A_n$ ili $K = S_n$, jer je A_n indeksa dva, pa ne postoji prava podgrupa od S_n koja je sadrži i različita je od nje. Ostaje slučaj kada je $K \cap A_n = \{e\}$. Dokazaćemo da je $K = \{e\}$. Pretpostavimo suprotno, da je K netrivijalna podgrupa od S_n. Neka je $\sigma \in K \setminus A_n$. Neka je τ takođe iz $K \setminus A_n$. Kako je proizvod neparnih permutacija parna permutacija, $\tau\sigma^{-1} \in$

$K \cap A_n = \{e\}$. Otuda je $\tau = \sigma$. Dakle, $K \setminus A_n$ sadrži samo jedan element, pa je $K = \{e, \sigma\}$. Primetimo da je za ma koju permutaciju $\nu \in S_n \setminus A_n$, $\nu^{-1}\sigma\nu \in K$. Kako je taj proizvod neparna permutacija, to je $\nu^{-1}\sigma\nu = \sigma\}$. Odatle je $\sigma\nu = \nu\sigma$. Dakle, σ komutira sa svim transpozicijama. Kako je σ reda 2, ona je proizvod transpozicija. Dakle, postoji transpozicija (ij) tako da je $\sigma = \tau \circ (ij)$, za neku permutaciju $\tau \in A_n$. Neka je $k \neq i, j$. Tada je $\sigma \circ (ik) \neq (ik) \circ \sigma$. Zaista, kako su i i j invarijntni za τ, $\sigma \circ (ik) = \tau(ij)(ik)$ preslikava k u j, a $(ik) \circ \sigma = (ik)\tau(ij)$ preslikava k u i. To je u kontrdikciji sa pokazanom činjenicom da σ komutira sa svim transpozicijama. □

3.13. Prsteni. Euklidski domeni

U nastavku ove glave razmatramo strukture sa dve operacije.

3.13.1. Definicija. Struktura $(S, +, 0, -, \cdot)$ je prsten ako zadovoljava sledeće zahteve:

(i) $(S, +, 0, -)$ je Abelova grupa,
(ii) $(S, \cdot)$ je semigrupa,
(iii) Zakone distributivnosti

$$(x + y) \cdot z = x \cdot z + y \cdot z$$
$$z \cdot (x + y) = z \cdot x + z \cdot y.$$

Ukoliko je $(S, \cdot)$ komutativna semigrupa kažemo da je $\mathcal{S}$ komutativan prsten. Ako je $(S, \cdot)$ semigrupa sa jedinicom, kažemo da je $\mathcal{S}$ prsten sa jedinicom.

U prstenu, zbog razlikovanja, inverzni element u odnosu na operaciju $+$ nazivamo suprotnim, a operaciju skraćivanja u odnosu na $+$, potiranjem. Kako se svakoj semigrupi može dodati neutral, videti Teoremu 3.2.15., to se često u definiciji prstena pretpostavlja da prsten ima jedinicu.

3.13.2. Primer. Navešćemo nekoliko poznatih primera prstena.
(i) $\mathcal{Z} = (Z, +, 0, -, \cdot)$ gde je Z skup celih brojeva, $+$ operacija sabiranja, a $\cdot$ operacija množenja, je komutativni prsten sa jedinicom.
(ii) $\mathcal{Z}_n = (Z_n, +_n, 0, -_n, \cdot_n)$ gde je $Z_n = \{0, 1, \ldots, n-1\}$, $+_n$ operacija sabiranja po modulu n, a $\cdot_n$ množenje po modulu n, je komutativni prsten sa jedinicom.
(iii) $\mathcal{Q} = (Q, +, 0, -, \cdot)$, $\mathcal{R} = (R, +, 0, -, \cdot)$, $\mathcal{C} = (C, +, 0, -, \cdot)$, gde je Q skup racionalnih brojeva, R skup realnih brojeva i C skup kompleksnih brojeva. Sve su ovo primeri komutativnih prstenova sa jedinicom.
(iv) $(R[x], +, 0, -, \cdot)$ gde je $R[x]$ skup polinoma sa realnim koeficijentima. Jednostavno se proverava da se definicija može proširiti tako da umesto

R uzmemo na koji prsten S, tako da opet dobijemo prsten polinoma sa koeficijentima iz prstena S.
(v) $(M_{n\times n}, +, 0, -, \cdot)$ gde je $M_{n\times n}$ skup matrica tipa $n \times n$, a $\cdot$ množenje matrica. Ovaj prsten sa jedinicom nije komutativan.
(vi) $(P(S), \Delta, \emptyset, id, \cap)$, gde je $P(S)$ partitivni skup proizvoljnog skupa S. Ovaj komutativni prsten sa jedinicom S je primer Bulovog prstena. Bulov prsten je prsten sa jedinicom koji zadovoljava zakon $x^2 = x$. Svaki Bulov prsten je komutativan jer

$$\begin{aligned} x + y &= (x + y)^2 \\ &= (x + y) \cdot (x + y) \\ &= x \cdot (x + y) + y \cdot (x + y) \\ &= x \cdot x + x \cdot y + y \cdot x + y \cdot y \\ &= x^2 + x \cdot y + y \cdot x + y^2 \\ &= x + x \cdot y + y \cdot x + y. \end{aligned}$$

Potirući (u odnosu na operaciju $+$), x i y, dobijamo $0 = x \cdot y + y \cdot x$, dakle, $y \cdot x = -(x \cdot y)$. Ako zamenimo $y = x$, dobijamo $x^2 = -x^2$ tj. $x = -x$. Dakle, svaki element je sam sebi suprotni. Kako je $y \cdot x$ suprotni element za $x \cdot y$, a i on je sam sebi suprotni, to je $y \cdot x = x \cdot y$. Usput smo dokazali i da je svaki element Bulovog prstena sam sebi suprotni. Može se pokazati da se svaki Bulov prsten može predstaviti u obliku $(P(S), \Delta, \emptyset, id, \cap)$.
vii) Neka je $(A, +, 0, -)$ proizvoljna Abelova grupa. Ako $\cdot$ definišemo tako da je za svaki $a, b \in A$, $a \cdot b = 0$, tada je $\mathcal{A} = (A, +, 0, -, \cdot)$ prsten. Uloga ovog primera je da pokaže da je svaka Abelova grupa, grupa sabiranja nekog prstena.

U sledećem tvrđenju pokazaćemo da se neka računanja u prstenima izvode onako kako smo navikli kod realnih brojeva.

3.13.3. Tvrđenje. *Neka je S prsten. Tada u S važi*
(i) $x \cdot 0 = 0 \cdot x = 0$.
(ii) $x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$.
(iii) $x \cdot y - x \cdot z = x \cdot (y - z)$.

Dokaz. (i) Neka je $a \in S$ proizvoljni element prstena S. Tada je,

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Potirući izraz $a \cdot 0$ na levoj i desnoj strani jednakosti dobijamo $0 = a \cdot 0$. Analogno se dokazuje druga jednakost.

(ii) Neka je $a, b \in S$. Tada je

$$a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0.$$

Dakle, $(-a) \cdot b$ je suprotni element od $a \cdot b$, tj. $(-a) \cdot b = -(a \cdot b)$. Analogno se dokazuje druga jednakost.

(iii) Neka su $a, b, c \in S$. Tada je

$$\begin{aligned} a \cdot b - a \cdot c &= a \cdot b + -(a \cdot c) \\ &= a \cdot b + a \cdot (-c) \\ &= a \cdot (b + -c) \\ &= a \cdot (b - c). \end{aligned}$$

□

3.13.4. Definicija. Element $a \neq 0$ komutativnog prstena S je delilac 0, ako postoji $b \neq 0$, tako da je $a \cdot b = 0$. Komutativni prsten sa jedinicom u kome nema delitelja 0 nazivamo integralnim domenom.

3.13.5. Tvrđenje. *U integralnom demenu važi formula (nije zakon),*

$$x \cdot y = 0 \Leftrightarrow x = 0 \vee y = 0.$$

Dokaz. Tvrđenje je logička transformacija definicije.

$$\begin{aligned} \neg\exists x \exists y\,(x \neq 0 \wedge y \neq 0 \wedge x \cdot y = 0) &\Leftrightarrow \forall x \forall y\,(\neg(x \cdot y = 0) \vee (x = 0 \vee y = 0)) \\ &\Leftrightarrow \forall x \forall y\,(x \cdot y = 0 \Rightarrow (x = 0 \vee y = 0)). \end{aligned}$$

Druga strana implikacije je posledica Tvrđenja 3.13.3.

3.13.6. Primer. (i) $\mathcal{Z}$ je integralni domen, po kome je ovaj pojam i dobio ime.

(ii) $\mathcal{Z}_n$ je integralni domen akko je n prost broj. Zaista, neka je n složen broj. Tada je $n = kl$, za neke $1 < k, l < n$. Tada je $k, l \neq 0$, a $k \cdot_n l = 0$. Sdruge strane, ako je $n = p$, prost broj, tada za proizvoljne $k, l \in Z_p$ imamo

$$\begin{aligned} k \cdot_p l = 0 &\Leftrightarrow p | kl \\ &\Leftrightarrow p | k \vee p | l \\ &\Leftrightarrow k = 0 \vee l = 0. \end{aligned}$$

(iii) $\mathcal{R}[x]$ je integralni domen. Zaista, neka su $p, q \in R[x]$, tako da je $p \cdot q = 0$. Tada je, po formuli za stepen proizvoda, $st(p) + st(q) = -\infty$, pa je $st(p) = -\infty$ ili $st(q) = -\infty$ tj. $p = 0$ ili $q = 0$.

3.13.7. Tvrđenje. *U integralnom domenu je svaki element različit od* 0 *skrativ.*

Dokaz. Neka je $\mathcal{S}$ integralni domen i $a \in S$, $a \neq 0$. Neka je za $b, c \in S$, $a \cdot b = a \cdot c$. Tada je,

$$\begin{aligned} a \cdot b = a \cdot c &\Rightarrow a \cdot b - a \cdot c = 0 \\ &\Rightarrow a \cdot (b - c) = 0 \\ &\Rightarrow a = 0 \vee b - c = 0 \\ &\Rightarrow b = c, \text{ jer je } a \neq 0. \quad \square \end{aligned}$$

3.14. Domeni glavnih ideala

U prve dve glave videli smo da postoji velika sličnost između celih brojeva i polinoma u pogledu teorije deljivosti. Videli smo u prethodnom odeljku da su obe strukture intgralni domeni. Međutim ne može se analogna teorija deljivosti izvesti u svim integralnim domenima. Zato nastojimo da opišemo strukture koje zadovoljavaju neki dodatni uslov, iz koga bi sledila teorija deljivosti. Ako analiziramo prve dve glave prirodno se nameću dva kandidata: Postojanje jedinstvene faktorizacije u proste brojeve i Euklidov algoritam. U ovom odeljku ispitujemo apstraktne strukture tog tipa. Na kraju dobijamo i nagradu, rešenje Diofantove jednačine $y^2 = x^3 - 2$.

3.14.1. Definicija. Neka je $\mathcal{S}$ integralni domen i $J \subset S$. J je ideal u $\mathcal{S}$ ako je $(J, +) < (S, +)$ i $JS = S$ tj. ako za proizvoljne $a, b \in J$ i $s \in S$,

$$b - a, s \cdot a \in J.$$

3.14.2. Primer. nZ je ideal u $\mathcal{Z}$, jer je zbir ma koja dva broja iz nZ takođe u nZ, i proizvod bilo kog celog broja iz Z sa brojem iz nZ je opet u nZ. Analogno je u proizvoljnom integralnom domenu S, za proizvoljni element $a \in S$, aS ideal u $\mathcal{S}$. On se obično označava sa (a).

3.14.3. Definicija. Ideal iz prethodnog primera naziva se glavnim idealom.

Primetimo da ako je J ideal u $\mathcal{S}$ i $1 \in J$, tada je $J = S$. Zaista, za proizvoljni $a \in S$ i $1 \in J$ je $1 \cot a = a \in J$. Dakle, $S \subset J$, tj. $J = S$.

3.14.4. Tvrđenje. *Neka je $\mathcal{S}$ integralni domen, $n \in N^+$ i $a_1, \ldots, a_n \in S$.*

$$(a_1, \ldots, a_n) = Sa_1 + \cdots + Sa_n = \{\sum_{i=1}^{n} s_i a_i : s_i \in S\},$$

je ideal u S.

Dokaz. Prema Posledici 3.5.10., $(a_1, \ldots, a_n)$ određuje podgrupu od $(S, +)$. Neka je $s \in S$ i $a = \sum_{i=1}^{n} s_i a_i \in J$. Tada je

$$s \cdot \sum_{i=1}^{n} s_i a_i = \sum_{i=1}^{n} (ss_i) a_i \in (a_1, \ldots, a_n).$$

Dakle, $(a_1, \ldots, a_n)$ je ideal u $\mathcal{S}$. □

3.14.5. Definicija. Ideal iz prethodnog tvrđenja naziva se konačno generisanim idealom.

Primetimo da je glavni ideal specijalni slučaj konačno generisanog ideala.

3.14.6. Definicija. Integralni domen $\mathcal{S}$ je domen glavnih ideala (DGI) ako je svaki ideal u $\mathcal{S}$ glavni.

3.14.7. Primer. Pokazaćemo da je $\mathcal{Z}$ DGI. Dakle, neka je $J \subset Z$ ideal u $\mathcal{Z}$. Kako je $(J, +) < (Z, +)$, to je $(J, +)$, prema Tvrđenju 3.10.7.(i), ciklična grupa. Neka je $a \in J$ generator te grupe. Tada je, prema Posledici 3.5.11., $J = aZ$. Dakle, $J = (a)$.

Relacija dljivosti definiše se kao i u $\mathcal{Z}$.

3.14.8. Definicija. Neka je $\mathcal{S}$ integralni domen i $a, b \in S$. $a|b$ akko postoji $s \in S$ tako da je $b = as$. $D(a, b) = \{t \in S : t|a, t|b\}$.

Pre nego razvijemo teoriju deljivosti razmotrimo jedan pojam koji je trivijalizovan u Z.

3.14.9. Definicija. Neka je $\mathcal{S}$ DGI i $u \in S$. u je junit u $\mathcal{S}$ ako $u|1$. $U(\mathcal{S})$ je skup junita u $\mathcal{S}$. Elementi $a, b \in S$ su pridruženi ako je $a = bu$ za neki junit u.

Juniti u $\mathcal{Z}$ su ± 1, a u $R[x]$ svi nenula konstantni polinomi. Setite se da u $R[x]$ nismo imali jedinstven najveći zajednički delilac. Primetimo da ako je u unit, onda za svako $a \in S$, iz $u|1$ i $1|a$ sledi $u|a$. dakle, juniti dele sve elemente DGI. Analogno komentaru posle Definicije 3.14.3., pokazuje se da ako je u junit, J ideal, i $u \in J$, tada je $J = S$.

Primetimo da je relacija pridruženosti simetrična. Zaista, neka je $a = bu$, za neki junit u. Neka je $v \in S$ tako da $uv = 1$. Množenjem jednakosti $a = bu$ sa v dobijamo $av = buv = b$. Kako je v junit, to su i b, a pridruženi. Kako je 1 junit i proizvod junita je junit, relacija pridruženosti je relacija ekvivalencije.

I u $\mathcal{S}$ možemo definisati pojam prostog broja, ali postoje dve njegove varijante.

3.14.10. Definicija. Ne-nula element $p \in S \setminus U(S)$ je ireducibilan ako za svaki $a \in S$, iz $a|p$ sledi da je a junit ili je pridružen a.

p je prost ako za svaki $a, b \in S$, iz $p|ab$ sledi $p|a$ ili $p|b$.

Prvi pojam odgovara našoj definiciji prostog broja u $\mathcal{Z}$, a druga osobini prostih brojeva iz Tvrđenja 1.2.9. (ii).

3.14.11. Definicija. Neka je $\mathcal{S}$ DGI, $a, b \in S$. $d \in S$ je najveći zajednički delilac za a i b ako $d \in D(a, b)$ i za svaki $t \in D(a, b)$, $t|d$.

3.14.12. Tvrđenje. *Neka je $\mathcal{S}$ DGI, $a, b \in S$. Postoji najveći zajednički delilac d za a i b, i $(d) = (a, b)$.*

Dokaz. Kako je $\mathcal{S}$ DGI, postoji $d \in S$ tako da je ideal $(a, b) = (d)$. d je očigledno najveći zajednički delilac za a i b. □

3.14.13. Definicija. Neka je $\mathcal{S}$ DGI, $a, b \in S$. a i b su uzajamno prosti ako je $D(a, b) = U(S)$.

Iz prethodnog tvrđenja i komentara posle Definicije 3.14.3., direktno imamo

3.14.14. Posledica. *Neka je $\mathcal{S}$ DGI, $a, b \in S$. Ako su a i b uzajamno prosti, onda je $(a, b) = S$.*

3.14.15. Posledica. *Neka je $\mathcal{S}$ DGI, i $p \in S$. p je ireducibilan element akko je p prost.*

Dokaz. ($\Rightarrow$) Pretpostavimo da za $a, b \in S$, $p|ab$ i $p \nmid a$. Kako $p \nmid a$, ne dele ga ni njemu pridruženi elementi. Kako p drugih faktora osim junita nema, to je $D(a, p) = U(S)$. Prema Posledici 3.14.14., $(a, p) = S$. Po definiciji konačno generisanog ideala je $(ap, bp) = (b)$. Kako $p|ab$ i $p|pb$, to je $ab \in (p)$ i $pb \in (p)$, pa je i $(b) \subset (p)$. Dakle, $p|b$.

($\Leftarrow$) Pretpostavimo da je p prost i neka je $p = kl$. Pokazaćemo da $k \in U(S)$ ili $l \in U(S)$. Kako $p|kl$, prema definiciji prostog broja, $p|k$ ili $p|l$. Bez gubljenja opštosti pretpostavimo da $p|k$. Tada je $k = ps$, za neki $s \in S$. Zamenom u $p = kl$, dobijamo $p = psl$. Skraćivanjem sa p dobijamo $1 = sl$. Dakle, $l|1$ tj. $l \in U(S)$. □

U daljem tekstu ne razlikujemo pojmove prost i ireducibilan.

3.14.16. Lema. *Neka je $\mathcal{S}$ DGI, i $(a_i)_{i \in N^+}$ niz elemanata u S tako da je*

$$(a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \ldots.$$

Postoji $k \in N^+$, tako da je $(a_i) = (a_k)$, za $i \geq k$.

Dokaz. Neka je $I = \bigcup_{i \in N^+} (a_i)$. Jednostavno se proverava da je J ideal u $\mathcal{S}$. Kako je $\mathcal{S}$ DGI, postoji $a \in S$, tako da je $J = (a)$. Kako $a \in J = \bigcup_{i \in N^+} (a_i)$,

postoji $k \in N^+$, tako da $a \in (a_k)$. Otuda je $(a) \subset (a_k)$. Kako je $(a_k) \subset J = (a)$, to je $(a_k) = (a)$. Kako za $i \geq k$, $(a_i) \subset (a) = (a_k)$, i $(a_k) \subset (a_i)$, to je $(a_i) = (a_k)$. □

Analogno definiciji kod monoida, usvajamo konvenciju da je proizvod po praznom skupu bilo koji junit.

3.14.17. Tvrđenje. *Neka je S DGI. Svaki ne-nula element iz S može se predstaviti kao proizvod prostih elemenata.*

Dokaz. Dokaz izvodimo po ugledu na dokaz za $\mathcal{Z}$. Neka je $a \in S$. Pokažimo najpre da postoji prost element $p \in S$ tako da $p|a$. Prethodna lema omogućuje indukciju. Dakle, ako je a prost tvrđenje trivijalno sledi. Neka a nije prost. Tada je $a = a_1 b_1$, gde a_1 i b nisu juniti. Ako je a_1 prost, tvrđenje je dokazano. U suprotnom je $a_1 = a_2 b_2$ za neke a_2, b_2 koji nisu juniti. Proces nastavljamo rekurzivno. Ako a ne sadrži prost element, onda se proces nastavlja za svko $n \in N^+$. Na taj način dobijamo niz $(a) \subset (a_1) \subset \cdots \subset (a_n) \subset \ldots$. Prema prethodnoj lemi, postoji $k \in N^+$, tako da je $(a_k) = (a_{k+1})$. Odatle sledi da su a_k i a_{k+1} pridruženi. Kako je $a_k = a_{k+1} b_{k+1}$, to je b_{k+1} junit suprotno konstrukciji. Iz dobijene kontradikcije sledi da a sadrži prost faktor.

Dokažimo sada postojanje faktorizacije. Neka je $a \in S$ i p_1 prost element tako da $p_1|a$. Tada postoji $b_1 \in S$ tako da $a = p_1 b_1$. Ako je b_1 junit tvrđenje je dokazano. U suprotnom, neka je p_2 prost element koji deli b_1. Tada postoji $b_2 \in S$ tako da $b_1 = p_2 b_2$. Tada je $a = p_1 p_2 b_2$. Ako je b_2 junit, tvrđenje je dokazano. U suprotnom nastavljamo postupak rekurzivno. Na taj način dobijamo niz glavnih ideala $(a) \subset (b_1) \subset (b_2) \subset \ldots$. Na osnovu prethodne leme, ovaj niz ne može beskonačno da raste. Dakle, postoji $k \in N^+$, tako da je $a = p_1 p_2 \ldots p_k b_k$, gde je b_k junit. Kako je $p_k b_k$prost, tvrđenje je dokazano. □

3.14.18. Lema. *Neka je p prost element i $a \neq 0$. Postoji $k \in N$, tako da $p^k|a$ i $p^{k+1} \nmid a$.*

Dokaz. Neka je $T = \{n \in N : p^n \nmid a$. Pokažimo da je T neprazan. Pretpostavimo suprotno. Tada za svaki $n \in N$ postoji $b_n \in S$, tako da je $a = p^n b_n$. Kako je $p b_{m+1} = b_m$, to je $(b_n)_{n \in N}$ strogo rastući niz glavnih ideala, suprotno Tvrđenju 3.14.16. Iz dobijene kontradikcije zaključujemo da je T neprazan skup. $k = (min\, T) - 1$. □

3.14.19. Definicija. Neka su oznake kao u prethodnoj lemi. Broj k označavamo sa $ord_p(a)$.

Verovatno primećujete da je ovaj pojam analogan pojmu višestrukosti nule polinoma.

3.14.20. Lema. *Neka je $a, b \in S$ i $a, b \neq 0$. Tada je*

$$ord_p(ab) = ord_p(a) + ord_p(b).$$

Dokaz. Neka je $ord_p(a) = k$ i $ord_p(b) = l$. Tada je $a = p^k c$ i $b = p^l d$, gde $p \nmid c, d$. Tada je $ab = p^{k+l}cd$, pri čemu $p \nmid cd$, dakle $ord_p(ab) = k + l$ □

Neka je P skup prostih elemenata u DGI S i T transverzala faktor skupa $S/\sim$ gde je $\sim$ relacija pridruženosti na P. Dakle iz svake klase pridruženih prostih elemenata izabran je po tačno jedan predstavnik. To je slično situaciji kada smo u $\mathcal{Z}$ birali n iz skupa $\{-n, n\}$, a u $R[x]$ iz svake klase birali moničan polinom.

3.14.21. Teorema. *Neka je S DGI, i T transverzala klasa pridruženosti prostih elemenata. Svaki $a \in S$, $a \neq 0$ može se na jedinstven način (do na raspored) predstaviti u obliku*

$$a = u \prod_{p \in T} p^{\alpha(p)}, \tag{1}$$

gde je u junit.

Dokaz. Postojanje faktorizacije dokazano je u Tvrđenju 3.14.17. Za dokaz jednoznačnosti koristimo Lemu 3.4.20. Dakle, neka je $q \in T$ prost element. Primenjujući ord_q na obe strane jednakosti (1), dobijamo

$$ord_q(a) = ord_q u + \sum_{p \in T} \alpha(p) ord_q(p).$$

Po definiciji funkcije ord_q je $ord_q(u) = 0$, $ord_q(p) = 0$, i $ord_q(p^{\alpha(p)}) = \alpha(q)$, za $p = q$. Dakle, $ord_q(a) = \alpha(q)$. Dakle, broj a jednoznačno određuje izložioce $\alpha(q)$. Otuda je, zbog postojanja skraćivanja u S, jednoznačno (u T) određen i junit u. □

Do sada osim primera koji su i bili motivacija čitave apstrakcije nismo ni imali drugih primera DGI. Umesto primera, evo još jedne apstrakcije, domena u kojima postoji Euklidov algoritam.

3.14.22. Definicija. Integralni domen S je Euklidski domen ako postoji funkcija $\lambda : S \setminus \{0\} \to N$ sa svojstvom da za svaki $a, b \in S$, $b \neq 0$, postoje $q, r \in S$ tako da je

$$a = bq + r, \text{ i ili je } r = 0 \text{ ili je } \lambda(r) < \lambda(b).$$

Nadam se da prepoznajete zahtev ispunjenosti pripremne leme za Euklidov algoritam. Situacija naročito podseća na onu kod polinoma. Odvajanje uslova $r = 0$ je urađeno da ne bi uvodili $-\infty = \lambda(0)$. Dakle, kod celih brojeva je $\lambda(a) = |a|$ a kod polinoma je $\lambda(p) = \mathrm{st}\,(p)$.

3.14.23. Tvrđenje. *Svaki Euklidski domen je DGI.*

Dokaz. Neka je$S$ Euklidski domen i J ideal u S. Neka je $k = \{mini \in N^+ : \exists a \in J\,(\lambda(a) = i)\}$, i neka je $b \in J$ tako da $\lambda(a) = k$. Dokazaćemo da je $J = (b)$. Neka je $a \in J$. Prema definiciji postoje $q, r \in S$ tako da je $a = bq + r$ i $r = 0$ ili $\lambda(r) < \lambda(b)$. Kako $a \in J$ i $bq \in J$, to $r \in J$. Ako bi imali da je $\lambda(r) < \lambda(b) = k$, to bi bilo u suprotnostisa minimalnošću broja k. Dakle, $r = 0$, tj. $a \in (b)$. Kako je a proizvoljni element iz J, $J \subset (a)$. Iz $b \in J$ sledi $(b) \subset J$, pa je $J = (b)$. □

Sad možemo da navedemonove primere DGI koji su preciznije Euklidski domeni.

3.14.24. Primer. Neka je i imaginarna jedinica. $Z[i] = \{k + li : k, l \in Z\}$. $Z[i]$ je očigledno zatvoren za operacije sabiranja i množenja i on je podstruktura integralnog domena C kompleksnih brojeva. Pokazaćemo da je $Z[i]$ Euklidski domen, dakle i DGI.

Neka je za $k + li \in Z[i] \setminus \{0\}$, $\lambda(k + li) = k^2 + l^2$. Funkcija λ je definisana za svaki kompleksni broj (kvadrat modula) i poznato je da ima osobinu $\lambda(zz_1) = \lambda(z)\lambda(z_1)$. Pokažimo da su zadovoljeni uslovi iz definicije. Neka je $a = k + li$, $b = m + ni$, $b \neq 0$. Neka je $\frac{a}{b} = s + ti$, za $s, t \in Q$. Neka su $u, v \in Z$ tako da je $|s - u| \leq \frac{1}{2}$ i $|t - v| \leq \frac{1}{2}$. Neka je $q = u + vi \in Z[i]$ i $r = a - bq$. Sada imamo, za proširenu funkciju λ,

$$\begin{aligned}\lambda(\frac{a}{b} - q) &= \lambda((s + ti) - (u + vi)) \\ &= (s - u)^2 + (t - v)^2 \\ &\leq \frac{1}{2}.\end{aligned}$$

Kako je $r = (\frac{a}{b} - q) \cdot b$, to je $\lambda(r) \leq \frac{1}{2}\lambda(b)$. Otuda je ili $\lambda(r) < \lambda(b)$ ili $\lambda(r) = 0$ (u proširenom smislu) pa za r funkcija λ u užem smislu nije ni definisana. U svakom slučaju zadovoljeni su uslovi iz definicije za λ.

3.14.25. Primer. Na isti način pokazuje se da je $Z[\sqrt{-2}]$ Euklidski domen. Funkcija λ definiše se tako da je $\lambda(k + l\sqrt{-2}) = k^2 + 2l^2$, dakle opet kao kvadrat modula kompleksnog broja. Primetimo da iz osobine $\lambda(ab) = \lambda(a)\lambda(b)$ sledi da ako $a|c$ onda $\lambda(a)|\lambda(c)$. Primetimo takođe da ako je $k, l \neq 0$, onda je $k^2, l^2 \geq 1$, pa je $\lambda(k + l\sqrt{-2}) \geq 3$.

Dokazaćemo da je $\sqrt{-2}$ prost element. Dakle, neka je $a = k + l\sqrt{-2}$ i $a|\sqrt{-2}$. Sada imamo $\lambda(a)|2$, pa je $\lambda(a) < 3$. Prema prethodnom pasusu, $k = 0$ ili $l = 0$. Ako je $k = 0$, onda je $a = l\sqrt{-2}$, pa imamo $\sqrt{-2}|a$. Kako smo pretpostavili $a|\sqrt{-2}$ to su a i $\sqrt{-2}$ pridruženi. Ako je $l = 0$, onda je

$a = k$. Tada $\lambda(a) = k^2|2$ pa je $k = 1$. Dakle, a je ili 1 ili je pridružen $\sqrt{-2}$. Po definiciji je $\sqrt{-2}$ prost.

U ovom DGI rešavaćemo Diofantsku jednačinu iz 1.14, tražeći rešenja samo u $Z \subset Z[\sqrt{-2}]$.

$$y^2 = x^3 - 2.$$

Transformišimo jednačinu u oblik $y^2 - (-2) = x^3$, a zatim u $Z[\sqrt{-2}]$ kao razliku kvadrata

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3.$$

Pokažimo najpre da su $y + \sqrt{-2}$ i $y - \sqrt{-2}$ uzajmano prosti. Zaista, neka je p prost element koji deli oba ta broja. Tada p deli i njihovu razliku, dakle $p|2\sqrt{-2} = (-\sqrt{-2})^3$. Kako je p prost, to $p|\sqrt{-2}$. Kako je $\sqrt{-2}$ prost i p nije junit, p i $\sqrt{-2}$ su pridruženi, pa imamo i $\sqrt{-2}|p$. Kako p deli levu stranu jednav cine, p deli i desnu stranu, dakle, $p|x^3$. Kako je p prost, to $p|x$. Zajedno sa $\sqrt{-2}|p$ to daje $\sqrt{-2}|x$. Uzimanjem normi, dobijamo da $2|x$. Zamenom u polaznoj jednačini dobijamo da je $y^2 \equiv_4 2$. Kontradikcija. Dakle, $y + \sqrt{-2}$ i $y - \sqrt{-2}$ uzajmano prosti.

Na isti način kao u Posledici 1.4.8., pokazuje se da su i $y + \sqrt{-2}$ i $y - \sqrt{-2}$ kubovi u $Z[\sqrt{-2}]$. Dakle, postoje $k, l \in Z$ tako da je

$$y + \sqrt{-2} = (k + l\sqrt{-2})^3.$$

Podiznjem binoma na kub, posle sređivanja i izjednačavanja dela uz $\sqrt{-2}$ i slobodnog dela, dobijamo

$$y = k^3 - 6kl^2 \tag{1}$$

$$1 = 3k^2l - 2l^3 = l(3k^2 - 2l^2). \tag{2}$$

Iz (2) imamo da $l|1$, pa je $l = \pm 1$. Za $l = 1$ dobijamo $3k^2 = 2$, što je nemoguće. Za $l = -1$ dobijamo $3a^2 = 3$, dakle $a = \pm 1$. Zamenom u (1) dobijamo $y = \pm 5$. Otuda je rešenje naše Diofantske jednačine u Z par $(3, \pm 5)$.

3.15 Polja

3.15.1. Definicija. Prsten $(S, +, 0, -, \cdot)$ je telo, ako je $(S \setminus \{0\}, \cdot)$ grupa. Komutativno telo je polje.

3.15.2. Primer. (i) $\mathcal{Z}$ nije polje jer nijedan element osim -1 i 1 nije invertibilan. Zaista, za $m \in Z \setminus \{0\}$, $m \neq -1, 1$, i svaki $n \in Z \setminus \{0\}$, je $|mn| \geq 2$, dakle nije jednako 1.
(ii) $\mathcal{Q}$, $\mathcal{R}$, $\mathcal{C}$ su polja.
(iii) $\mathcal{R}[x]$ nije polje. Jednostavni argument sa stepenima proizvoda pokazuje da nijedan nekonstantan polinom nije invertibilan koeficijentima.
(iv) $\mathcal{R}(x)$ skup racionalnih funkcija, u odnosu na uobičajne operacije sabiranja i množenja, je polje.
(v) Neka je $K = \{a + bi + cj + dk : a, b, c, d \in R\}$, skup uopštenih kompleksnih brojeva - kvaterniona. Definišimo operaciju sabiranja po koordinatama a množenje koristeći pravila iz grupe kvaterniona $\mathcal{K}$ iz Primera 3.4.11. Neka je $z = a + bi + cj + dk$ i $u = a_1 + b_1 i + c_1 j + d_1 k$. Tada je

$$\begin{aligned} z + u &= (a + a_1) + (b + b_1)i + (c + c_1)j + (d + d_1)k \\ z \cdot u &= (aa_1 - bb_1 - cc_1 - dd_1) + (ab_1 + ba_1 + cd_1 - dc_1)i \\ &\quad + (ac_1 - bd_1 + ca_1 + cd_1)j + (ad_1 + bc_1 - cb_1 + da_1)k. \end{aligned}$$

Očigledno je 0 neutral za sabiranje i $-(a + bi + cj + dk) = (-a) + (-b)i + (-c)j + (-d)k$. $(K, +, 0, -, \cdot)$ je telo. Neprijatnu proveru asocijativnosti ostavljamo čitaocu kao računsku vežbu. Neutral za množenje je 1. Neka je $z \in K$, $z = a + bi + cj + dk$, i neka je $M = a^2 + b^2 + c^2 + d^2 \in R$. Tada je

$$(a + bi + cj + dk) \cdot (a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2 = M.$$

Zato je $\frac{a}{M} - \frac{b}{M}i - \frac{c}{M}j - \frac{d}{M}k$ inverzni element od z u odnosu na množenje. Dakle, $\mathcal{K}$ je telo. $\mathcal{K}$ nije polje jer je $i \cdot j = k$ a $j \cdot i = -k$.

Kao i kod grupa, jezik polja može se proširiti tako da je $(S, +, 0, -, 1, ^{-1})$ polje u proširenom jeziku, ako je $(S, +, 0, -, \cdot)$ polje u kome je 1 jedinica za množenje a $^{-1}$ inverzni element. Korespondencija je uzajamno jednoznačna i u nastavku ne pravimo razliku između ove dve notacije.

Iz definicije polja jasno je da je svako polje integralni domen. Zahtev da je $(S \setminus \{0\}, \cdot)$ grupa podrazumeva da je taj skup zatvoren za $\cdot$, odnosno

$$\begin{aligned} a \in S \setminus \{0\} \,\&\, b \in S \setminus \{0\} \Rightarrow a \cdot b \in S \setminus \{0\} \text{ tj.} \\ a \neq 0 \;\&\; b \neq 0 \Rightarrow a \cdot b \neq 0, \end{aligned}$$

što je kontrapozicija uslova 3.13.5. U konačnom slučaju važi i obrat.

3.15.3. Tvrđenje. *Konačan integralni domen je polje.*

Dokaz. Neka je S konačan integralni domen. Kako je svaki element u $(S \setminus \{0\}, \cdot)$ skrativ i $S \setminus \{0\}$ je konačan, tvrđenje sledi iz Tvrđenja 3.3.12.

3.16. Konstrukcija celih i racionalnih bojeva

Evo nas na početku. Podsetimo se da smo na početku podrazumevali intuitivno poznavanje prirodnih, celih, racionalnih i realnih brojeva. Mi ipak preferiramo situaciju kada je objekat precizno definisan kako bi mogli da dokazujemo njegove osobine i izbegnemo eventualne kontradikcije. U nastavku pokazujemo kako se celi i racionalni brojevi mogu konstruisati iz prirodnih.

Neka je $\mathcal{N} = (N, +, 0, \cdot, 1, \leq)$ (standardni) model prirodnih brojeva sa uobičajnim operacijama $+, \cdot$ i relacijom linearnog uređenja $\leq$. $(N, +, 0)$ je komutativni monoid u kome su svi elementi skrativi. Otuda je i njegov Dekartov kvadrat $(N^2, +, (0,0))$ komutativni monoid. Slično je i $(N, \cdot, 1)$ komutativni monoid. Neka je $\sim$ relacija skupa N^2 definisana tako da za $(k,l),(s,t) \in N^2$,

$$(k,l) \sim (s,t) \Leftrightarrow k + t = l + s.$$

3.16.1. Tvrđenje. *Relacija $\sim$ je relacija kongruencije monoida $(N^2, +)$.*

Dokaz. Pokažimo najpre da je $\sim$ relacija ekvivalencije.

Refleksivnost. Kako je $k + l = k + l$, to je $(k,l) \sim (k,l)$.

Simetričnost. Neka je $(k,l) \sim (s,t)$. Tada je $k + t = l + s$, pa je i $s + l = k + t$, što po definiciji znači da je $(s,t) \sim (k,l)$.

Tranzitivnost. Neka je $(k,l) \sim (s,t)$ i $(s,t) \sim (u,v)$. Tada je $k+t = l+s$ i $s+v = t+u$. Sabiranjem ovih jednakosti i potiranjem s i t dobijamo $k+v = u+l$, tj. $(k,l) \sim (u,v)$. Ostaje da pokažemo da je $\sim$ relacija kongruencije. Neka je $(k,l) \sim (s,t)$ i $(k_1,l_1) \sim (s_1,t_1)$. Tada je $k+t = l+s$ i $k_1+t_1 = l_1+s_1$. Sabiranjem jednakosti dobijamo $(k+k_1)+(t+t_1) = (l+l_1)+(s+s_1)$, tj. $(k,t)+(k_1,t_1) \sim (l,s)+(l_1,s_1)$. □

Primetimo da je $N^2/\sim = \{(0,n)/\sim : n \in N^+\} \cup \{(0,0)/\sim\} \cup \{(n,0)/\sim : n \in N^+\}$ i da su sve nabrojane klase međusobno različite. Najpre neka je $(k,l) \in N^2$, tako da je $k < l$. Tada je $(k,l) \sim (0, l-k)$, $l-k \in N^+$. Ako je $k = l$, tada je $(k,k) \sim (0,0)$. I na kraju, ako je $k > l$, tada je $(k,l) \sim (k-l, 0)$, $k-l \in N^+$. Trivijalno se razmatranjem slučajeva proverava da su sve nabrojane klase različite.

Definišimo na količničkom skupu $N^2/\sim$ operacije sabiranja i množenja tako da je

$$(k,l)/\sim + (u,v)/\sim = (k+u, l+v)/\sim$$
$$(k,l)/\sim \cdot (s,t)/\sim = (ks+lt, kt+ls)/\sim .$$

Kako je $\sim$ relacija kongruencije monoida $(N^2, +, (0,0))$, to je operacija $+$ dobro definisana. Proverimo da li je operacija množenja dobro definisana,

tj. da ne zavisi od izbora predstavnika. Dakle, neka je $(k,l) \sim (s,t)$ i $(k_1,l_1) \sim (s_1,t_1)$. Tada je $k+t = l+s$ i $k_1+t_1 = l_1+s_1$. Množenjem prve jednakosti najpre sa k_1 a zatima sa l_1 i druge jednakosti sa s i t, dobijamo

$$kk_1 + tk_1 = lk_1 + sk_1$$
$$ll_1 + sl_1 = kl_1 + tl_1$$
$$k_1s + t_1s = l_1s + ss_1$$
$$l_1t + s_1t = k_1t + t_1t.$$

Sabiranjm jednakosti i potiranjem jednakih izraza dobijamo

$$kk_1 + ll_1 + st_1 + s_1t = ss_1 + tt_1 + k_1l + kl_1, \text{odnosno}$$
$$(kk_1 + ll_1, k_1l + kl_1) \sim (ss_1 + tt_1, s_1t + st_1).$$

3.16.2. Lema. $(N^2, +, (0,0)/\sim)$ *je Abelova grupa.*

Dokaz. Asocijativnost i komutativnost se prenose kroz Dekartove proizvode i homomorfne slike (faktor strukture kongruencija) pa je $(N^2,+)$, komutativna semigrupa sa neutralom $(0,0)/\sim$. Ostaje da pokažemo postojanje suprotnog elementa. Međutim,

$$(k,l)/\sim + (l,k)/\sim = (k+l, l+k)/\sim = (0,0)/\sim .$$

Dakle, $(l,k)/\sim = -(k,l)/\sim$. □

3.16.3. Teorema. $\mathcal{Z} = (N^2/\sim, +, (0,0)/\sim, -, \cdot)$ *je integralni domen.*

Dokaz. Jednostavno se proverava da je operacija $\cdot$ komutativna. Da bi pokazali da je $\mathcal{Z}$ prsten, ostaje da proverimo da je operacija $\cdot$ asocijativna i da važi distributivnost. Asocijativnost po već ustaljenoj praksi ostavljamo kao računsku vežbu čitaocu. Proverimo distributivnost. Kako je množenje komutativno, dovoljno je proveriti levu distributivnost. Neka je $(k,l),(s,t),(u,v) \in N^2$. Tada je,

$$(k,l)/\sim \cdot((s,t)/\sim + (u,v)/\sim) = (k(s+u) + l(t+v), k(t+v) + l(s+u))/\sim$$
$$(k,l)/\sim \cdot(s,t)/\sim + (k,l)/\sim \cdot(u,v)/\sim = (ks + lt + ku + lv, kt + ls + kv + lu)/\sim .$$

Izrazi na desnoj strani očigledno su jednaki.

Jedinica u $\mathcal{Z}$ je očigledno $(1,0)/\sim = \{(k+1,k) : k \in N\}$. Ostaje da pokažemo da $\mathcal{Z}$ nema delitelja 0. Dakle, neka je $(k,l)/\sim \cdot(s,t)/\sim = (0,0)/\sim$. Tada je $ks + lt = kt + ls$. Bez gubljenja opštosti možemo pretpostaviti da je $k \geq l$ a time i $ks \geq ls$ i $kt \geq lt$. Sada imamo $ks - ls = kt - lt$, odnosno $s(k-l) = t(k-l)$. Ako je $k - l \neq 0$, tada skraćivanjem dobijamo $s = t$. Dakle, $k - l = 0$ ili $s = t$. Otuda je $k = l$ ili $s = t$, odnosno $(k,l)/\sim = (0,0)/\sim$ ili $(s,t)/\sim = (0,0)/\sim$. Time je tvrđenje dokazano. □

3.16.4. Tvrđenje. *Preslikavanje* $f : N \to Z$ *definisano sa* $f(k) = (k,0)/\sim$ *je monomorfizam u jeziku* $\{+,\cdot\}$. $Im(f) = \{(k,0)/\sim : k \in N\}$.

Dokaz. $f(k+l) = (k+l,0)/\sim = (k,0)/\sim + (l,0)/\sim = f(k) + f(l)$. Drugi deo tvrđenja je očigledan. □

Neka je $\check{N} = Im(f)$, gde je f homomorfizam iz prethodnog tvrđenja, i $\check{\mathcal{N}} = (\check{N}, +, \cdot)$. Tada je $\mathcal{N} \cong \check{\mathcal{N}}$. Dakle, $\mathcal{Z}$ sadrži u sebi izomorfnu kopiju prirodnih brojeva. Prema reprezentaciji klasa ustanovljenoj u tekstu iza Tvrđenja 3.16.1, proizvoljni element $m \in Z$ je oblika $(k,0)/\sim$ ili $(0,k)/\sim$, za $k \in N$. Kako je $(0,k)/\sim = -(k,0)/\sim$, to $m \in \check{N}$ ili $m = -n$, za $n \in \check{N}$. Dakle, svaki ceo broj je ili prirodan broj ili njemu suprotan broj. Ako sa $-\check{N}$ označimo skup $\{(0,k)/\sim : k \in N^+\}$, onda imamo $Z = -\check{N} \cup \check{N}$.

Razmotrimo na kraju kako se prenosi uređenje.

3.16.5. Definicija. Neka je $\leq$ relacija skupa Z definisana sa

$$(k,l)/\sim \leq (s,t)/\sim \Leftrightarrow k + t \leq s + l.$$

3.16.6. Lema. *Neka je* $\leq$ *relacija uvedena u prethodnoj definiciji.*

(i) $(Z, \leq)$ *je linearno uređenje.*

(ii) *Preslikavanje* f *definisano u Tvrđenju 3.16.4., je izotono preslikavanje* $(N, \leq)$ *u* $(Z, \leq)$.

(iii) *Za* $m, n \in Z$, $m \leq n \Leftrightarrow \exists u \in \check{N}(n = m + u)$.

(iv) *Neka je* $m = -k$ *i* $n = -l$, $k, l \in \check{N}$. $m \leq n \Leftrightarrow l \leq k$.

(v) *Relacija* $\leq$ *je saglasna sa operacijama sabiranja i množenja nenegativnim brojem.*

Dokaz. (i) Sledi direktno iz činjenice da je $\leq$ na N linearno uređenje.

(ii) Neka je $k \leq l$, $k, l \in N$. Tada je $k + 0 \leq l + 0$, pa je po definiciji $(k,0)/\sim \leq (l,0)/\sim$, tj. $f(k) \leq f(l)$.

(iii) Neka je $m = (k,l)/\sim$ i $n = (s,t)/\sim$. Po definiciji je

$$\begin{aligned}(k,l)/\sim \leq (s,t)/\sim &\Leftrightarrow k + t \leq s + l \\ &\Leftrightarrow \exists u \in N\,(k + t + u = l + s) \\ &\Leftrightarrow \exists u \in N\,((k+t,l)/\sim = (u,v)/\sim) \\ &\Leftrightarrow \exists u \in N\,((k,l)/\sim + (t,0)/\sim = (u,v)/\sim) \\ &\Leftrightarrow \exists u \in \check{N}\,(m + u = n).\end{aligned}$$

(iv) Neka je $k = (s,0)/\sim$ i $l = (t,0)/\sim$. Tada je

$$\begin{aligned}m \leq n &\Leftrightarrow (0,s) \leq (0,t) \\ &\Leftrightarrow 0 + t \leq 0 + s \\ &\Leftrightarrow (t,0)/\sim \leq (s,0) \\ &\Leftrightarrow l \leq k.\end{aligned}$$

(v) Neka je $m \leq n$. Tada je, prema (iii), $n = m + t$, za neki $t \in \check{N}$. Tada je $n + u = m + u + t$, pa je, opet prema (iii), $m + u \leq n + u$. Slično se pokazuje da je za $u \geq 0$, $u \cdot m \leq u \cdot n$.

3.16.7. Teorema. *$(Z, \leq)$ je leksikografska suma uređenja $(-\check{N}, \leq)$ i $(\check{N}, \leq)$ pri čemu su ova uređenja izomorfna redom sa $(N, \geq)$ i $(N, \leq)$.*

Dokaz. Kako je Z disjunktna unija $-\check{N}$ i $\check{N}$, dovoljno je dokazati da je za $m \in -\check{N}$ i $n \in \check{N}$, $m < n$. Zaita, neka je $m = (0, k)/\sim$, $k \in N^+$, i $n = (l, 0)/\sim$, $l \in N$. Tada je $0 + 0 < k + l$, pa je $(0, k)/\sim < (l, 0)/\sim$. Mi smo već pokazali da je $(\check{N}, \leq) \cong (N, \leq)$. Preslikavanje $f : N \to -\check{N}$ definisano sa $f(k) = (0, k + 1)$ je, prema tački iv) prethodne leme, izomorfizam $(N, \geq)$ i $(-\check{N}, \leq)$. □

Dakle, i uređenje na $\mathcal{Z}$ ima osobine koje očekujemo od strukture koja pretenduje da predstavlja cele brojeve.

Na sličan način se od $\mathcal{Z}$ može izgraditi struktura racionalnih brojeva.

Neka je $\mathcal{Z} = (Z, +, 0, -, \cdot, 1, \leq)$ upravo izgrađeni model celih brojeva. Neka je $D = Z \times Z \setminus \{0\}$. Neka je $\sim$ relacija skupa D definisana tako da za $(k, l), (s, t) \in D$,

$$(k, l) \sim (s, t) \Leftrightarrow k \cdot t = l \cdot s.$$

3.16.8. Tvrđenje. *Relacija $\sim$ je relacija ekvivalencije skupa D.*

Dokaz. Pokazuje se na isti način kao kod izgradnje celih brojeva. □

Kako je $(m, s) \sim (-m, -s)$, bez gubljenja opštosti možemo pretpostaviti da je predstavnik klase izabran tako da je $s > 0$. Definišimo na količničkom skupu $D/\sim$ operacije sabiranja i množenja tako da je

$$(k, l)/\sim + (u, v)/\sim = (kv + lu, lv)/\sim$$
$$(k, l)/\sim \cdot (s, t)/\sim = (ks, lt)/\sim .$$

Pokažimo da su operacije dobro definisane, tj. da ne zavise od izbora predstavnika. Dakle, neka je $(k, l) \sim (s, t)$ i $(k_1, l_1) \sim (s_1, t_1)$. Tada je $k \cdot t = l \cdot s$ i $k_1 \cdot t_1 = l_1 \cdot s_1$. Množenjem ovih jednakosti trivijalno se pokazuje da $\cdot$ ne zavisi od izbora predstavnika klasa. Množenjem prve jednakosti najpre sa sa $l_1 t_1$ i druge jednakosti sa lt, i sabiranjem dobijenih jednakosti imamo,

$$kl_1tt_1 + lk_1ltt_1 = slt_1l_1 + lts_1l_1$$
$$(kl_1 + k_1l, ll_1) \sim (st_1 + s_1t, tt_1).$$

Dakle, ni sabiranje ne zavisi od izbora predstavnika.

3.16.9. Teorema. $Q = (Z^2/\sim, +, (0,1)/\sim, \cdot, (1,1)/\sim)$ *je polje.*

Dokaz. Pokazaćemo samo da je $Q \setminus \{0\}$ zatvoren za množenje, da svaki element u Q ima suprotni element i da svaki element u $Q \setminus \{0\}$ ima inverz. Proveru ostalih aksioma ostavljamo čitaocu.

Neka je $(k,l)/\sim \neq (0,1)/\sim$ i $(s,t)/\sim \neq (0,1)/\sim$. Tada je $k \cdot 0 \neq l \cdot 1$ i $s \cdot 0 \neq t \cdot 1$, odnosno $k \neq 0$ i $s \neq 0$. Otuda je $ks \neq 0$, pa je $(ks, lt)/\sim \neq (0,1)/\sim$.

Suprotni element od $(k,l)/\sim$ je $(-k,l)/\sim$. Zaista, $(k,l)/\sim + (-k,l)/\sim = (kl - kl, l^2)/\sim = (0,l^2)/\sim = (0,1)\sim$.

Neka je $(k,l)/\sim \neq (0,1)/\sim$ odnosno $k \neq 0$. Tada je $(l,k) \in Q$ i $(k,l)/\sim \cdot (l,k)/\sim = (kl, lk)/\sim = (1,1)/\sim$. □

3.16.10. Tvrđenje. *Preslikavanje* $f : Z \to Q$ *definisano sa* $f(m) = (m,1)/\sim$ *je monomorfizam u jeziku* $\{+, \cdot\}$. $Im(f) = \{(m,1)/\sim : m \in Z\}$.

Dokaz. $f(m+s) = (m+s,1)/\sim = (m,1)/\sim + (s,1)/\sim = f(m) + f(s)$. Slično je $f(ms) = (ms,1)/\sim = (m,1)/\sim \cdot (s,1)/\sim = f(m) \cdot f(s)$. Drugi deo tvrđenja je očigledan. □

Dakle, Q sadrži izomorfnu kopiju $\check{Z}$ celih brojeva. Kako je $(m,s)/\sim = (m,1)/\sim \cdot (1,s)/\sim = (m,1)/\sim \cdot ((s,1)/\sim)^{-1}$ to se svaki element $r \in Q$ može predstaviti u obliku $m \cdot s^{-1} = \frac{m}{s}$, gde su $m, s \in \check{Z}$.

Razmotrimo na kraju kako se prenosi uređenje.

3.16.11. Definicija. Neka je $\leq$ relacija skupa Z definisana tako da za $(k,l)/\sim, (s,t)/\sim \in Q$, ali tako da je $l, t > 0$.

$$(k,l)/\sim \leq (s,t)/\sim \Leftrightarrow kt \leq sl.$$

Jednostavno se proverava da ovako definisano uređenje ne zavisi od izbora predstavnika.

3.16.12. Lema. *Neka je* $\leq$ *relacija uvedena u prethodnoj definiciji.*

(i) $(Q, \leq)$ *je linearno uređenje.*

(ii) *Preslikavanje* f *definisano u Tvrđenju 3.16.10., je izotono preslikavanje* $(Z, \leq)$ *u* $(Q, \leq)$.

(iii) *Ako je* $r \geq u$ *onda je* $-r \leq -u$.

(iv) *Relacija* $\leq$ *je saglasna sa sabiranjem i množenjem nenegativnim brojem.*

(v) $(Q, \leq)$ *je prebrojivo, gusto linearno uređenje bez krajeva.*

Dokaz. (i) Sledi direktno iz činjenice da je $\leq$ na Z linearno uređenje.

(ii) Neka je $m \leq s$, $m, s \in Z$. Tada je $m \cdot 1 \leq s \cdot 1$, pa je po definiciji $(m,1)/\sim \leq (s,1)/\sim$, tj. $f(m) \leq f(s)$.

(iii) Neka je $r = (m,n)/\sim$ i $u = (s,k)/\sim$, $n,k > 0$. Po definiciji je

$$\begin{aligned}(m,n)/\sim \geq (s,k)/\sim &\Leftrightarrow mk \geq sn \\ &\Leftrightarrow -mk \leq -sn \\ &\Leftrightarrow (-m,n)/\sim \leq (-s,k)/\sim \\ &\Leftrightarrow -r \leq -u.\end{aligned}$$

(iv) Neka je $r = (m,n)/\sim$, $u = (s,k)/\sim$, $v = (t,l)/\sim$, $n,k,l > 0$, i neka je $u \leq v$. Tada je

$$\begin{aligned}u \leq v &\Leftrightarrow sl \leq kt \\ &\Leftrightarrow sln^2 \leq ktn^2 \\ &\Leftrightarrow mkln + sln^2 \leq mkln + ktn^2 \\ &\Leftrightarrow (mk + sn)ln \leq (ml + tn)kn \\ &\Leftrightarrow r + u \leq r + v.\end{aligned}$$

Neka je sada $r \geq 0$, tj. $m \geq 0$. Sada imamo

$$\begin{aligned}u \leq v &\Leftrightarrow sl \leq kt \\ &\Rightarrow msnl \leq nktm \\ &\Rightarrow (ms,nk)/\sim \leq (mt,nl) \\ &\Rightarrow ru \leq rv. \quad \square\end{aligned}$$

Dakle, $\mathcal{Q}$ je uređeno polje koje sadrži cele brojeve i u kome je svaki element količnik dva cela broja.

(v) U (i) smo pokazali da je uređenje linearno. Kako je skup celih brojeva prebrojiv, a time i Z^2, to je i Q koji je određen parovima celih brojeva prebrojiv. Neka je $r = (m,n)/\sim$, $n > 0$, proizvoljni element iz Q. Ako je $k = |m|$, onda je $(-k,1)/\sim \leq r \leq (k,1)/\sim$. Kako je $\mathcal{Z}$ neograničen, to je i $\mathcal{Q}$ neograničen, tj. nema ni najmanji ni najveći element. Ostaje da pokažemo da je $\mathcal{Q}$ gust.

Neka je $r,u \in Q$, $r < u$. Tada je $r < \frac{r+u}{2} < u$, dakle postoji element u otvorenom intervalu (r,u). $\square$

Sada očekujete da iz $\mathcal{Q}$ izgradimo $\mathcal{R}$. Međutim to se ne može izvesti konstrukcijama ovog tipa. Zato je $\mathcal{R}$ glavni objekat druge grane matematike - Analize.