Mathematical Faculty

University of Belgrade

Shadia Ali Shalandi

The Sylow's Theorems

Master thesis

Advisor:

Prof. Aleksandar Lipkovski, PhD.

Belgrade, 2010.

CONTENTS

Introduction

Symmetric objects are so singular in the natural world that our ancestors must have noticed them very early. Indeed, symmetrical structures were given special magical status. The Greeks' obsession with geometrical shapes led them to the enumeration of platonic solids, and to adorn their edifices with various symmetrical patterns. In the ancient world, symmetry was synonymous with perfection. What could be better than a circle or a sphere? The Sun and the planets were supposed to circle the Earth. It took a long time to get the apparently less than perfect ellipses.

Of course most shapes in the natural world display little or no symmetry, but many are almost symmetric. An orange is close to a perfect sphere; humans are almost symmetric about their vertical axis, but not quite, and ancient man must have been aware of this. Could this lack of exact symmetry have been viewed as a sign of imperfection, imperfection that humans need atone for?

It must have been clear that highly symmetric objects were special, but it is a curious fact that the mathematical structures which generate symmetrical patterns were not symmetrically studied until the nineteenth century. That is not to say that symmetry patterns were unknown or neglected, witness the Moors in Spain who displayed the seventeen different ways to tile a plane on the walls of their palaces.

Evariste Galois in his study of the roots of polynomials degree larger than four equated the problem to that of a set of substitutions which form that mathematical structure called a group. In physics, the study of crystals elicited wonderfully regular patterns which were described in terms of their symmetries have assumed a central role in the study of Nature.

The importance of symmetries is reinforced by the Standard Model of elementary particle physics, which indicates that Nature displays more symmetries in the small than in the large. In cosmological terms, this means that our Universe emerged from the Big Bang as a highly symmetrical structure, although most of its symmetries are no longer evident today.

Some symmetries of the natural world are so commonplace, that they are difficult to identify. The outcome of an experiment performed by undergraduates should not depend on the time and location of the bench on which it was performed. Their results should be impervious to shifts in time and space, as consequences of time and space translation invariances, respectively. But there are more subtle manifestations of symmetries.

According to Quantum Mechanics, physics takes place in Hilbert spaces. Bizarre as this notion might be, we have learned to live with it as it continues to be verified whenever experimentally tested. Surely, this abstract identification of a physical system with a state vector in Hilbert space will eventually be found to be incomplete, but in a presently unimaginable way, which will involve some other weird mathematical structure. That Nature uses the same mathematical structures invented by mathematicians is a profound mystery hinting at the way our brains are wired. Whatever the root cause, mathematical structures which find natural representations in Hilbert spaces have assumed enormous physical interest. Prominent among them are *groups* which, subject to specific axioms, describe transformations in these spaces.

In abstract algebra, as in the case of most twentieth-century developments, the basic concepts and goals were fixed in the nineteenth century. The fact that algebra can deal with collections of objects that are not necessarily real or complex numbers was demonstrated in a dozen nineteenth-century creations. Vectors, quaternions, matrices, forms such as $ax^2 + bxy + cy^2$, hypernumbers of various sorts, transformations, and substitutions or permutations are examples of objects that were combined under operations and laws of operation peculiar to the respective collections. Even the work on algebraic numbers, though it dealt with classes of complex numbers, brought to the fore the variety of algebras because it demonstrated that only some properties are applicable to these classes as opposed to the entire complex number system.

These various classes of objects were distinguished in accordance with the properties that the operations in them possessed; and we have seen that such

notions as group, ring, ideal, and field, and subordinate notions such as subgroup, invariant subgroup, and extension field were introduce to identify the sets of properties. However, nearly all of the nineteenth-century work on these various types of algebras dealt with the concrete systems mentioned above. It was only in the last decades of the nineteenth century that the mathematicians appreciated that they could move up to a new level of efficiency by integrating many separate algebras through abstraction of their common content. Thus permutation groups, the groups of classes of forms treated by Gauss, hypernumbers under addition, and transformation groups could all be treated in one swoop by speaking of a set of elements or things subject to an operation whose nature is specified only by certain abstract properties, the foremost of these being that the operation applied to two elements of the set produces a third element of the set. The same advantages could be achieved for the various collections that formed rings and fields. Though the idea of working with abstract collections preceded the axiomatics of Pasch, Peano, and Hilbert, the latter development undoubtedly accelerated the acceptance of the abstract approach to algebras.

Thus arose abstract algebra as the conscious study of entire classes of algebras, which individually were not only concrete but which served purposes in specific areas as substitution groups did in the theory of equations. The advantage of obtaining results that might be useful in many specific areas by considering abstract versions was soon lost sight of, and the study of abstract structures and the derivation of heir properties became an end in itself.

Abstract algebra has been one of the favored fields of the twentieth century and is now a vast area.

It is a favorite activity of historians, now that the abstract theory is in existence, to trace how many of the abstract ideas were foreshadowed by the concrete works of Gauss, Abel, Galois, Cauchy, Sylow and dozens of other men.

I. History of group theory

In this chapter we will present the main periods of finite group history and give the major problems that were solved during these periods.

There are four major sources in the evolution of group theory. They are (with the names of the originators and dates of origin):

1) Classical algebra (Lagrange, 1770)

2) Number theory (Gauss, 1801)

3) Geometry (Klein, 1874)

4) Analysis (Lie, 1874; Poincaré and Klein, 1876)

We shall deal with each of sources in turn.

1.1 Classical Algebra

The major problems in algebra at the time (1770) that Lagrange wrote his fundamental memoir "Reflections on the solution of algebraic equations" concerned polynomial equations. There were "theoretical" questions dealing with the existence and nature of the roots – for example, does every equation have a root? How many roots are there? Are they real, complex, positive, negative? And "practical" questions dealing with methods for finding the roots. In the latter instance there were exact methods and approximate methods. In what follows we mention exact methods. The Babylonians knew how to solve quadratic equations, essentially by the method of completing the square, around 1600. Algebraic methods for solving the cubic and the quartic were given around 1540. One of the major problems for the next two centuries was the algebraic solution of the quintic. This is the task Lagrange set for himself in his paper of 1770.

In this paper Lagrange first analyzed the various known methods, devised by Viète, Descartes, Euler, and Bezout, for solving cubic and quartic equations. He showed that the common feature of these methods is the reduction of such equations to auxiliary equations – the so-called *resolvent equations*. The latter are one degree lower than the original equations.

Lagrange next attempted a similar analysis of polynomial equations of arbitrary degree n. With each such equation he associated a resolvent equation, as follows: let $f(x)$ be the original equation, with roots $x_1, x_2, x_3, \ldots, x_n$. Pick a rational function $R(x_1, x_2, x_3, \ldots, x_n)$ of the roots and coefficients of $f(x)$. (Lagrange described methods for doing this.) Consider the different values which $R(x_1, x_2, x_3, \ldots, x_n)$ assumes under all the $n!$ permutations of the $x_1, x_2, x_3, \ldots, x_n$ of $f(x)$. If these are denoted by $y_1, y_2, y_3, \ldots, y_k$, then the resolvent equation is given by

$$g(x) = (x - y_1)(x - y_2) \cdots (x - y_k).$$

It is important to note that the coefficients of $g(x)$ are symmetric functions $x_1, x_2, x_3, \ldots, x_n$, hence they are polynomials in the elementary symmetric

functions of $x_1, x_2, x_3, \ldots, x_n$; that is, they are polynomials in the coefficients of the original equation $f(x)$. Lagrange showed that k divides $n!$ – the source of what we call Lagrange's theorem in group theory.

For example, if $f(x)$ is a quartic with roots x_1, x_2, x_3, x_4, then $R(x_1, x_2, x_3, x_4)$ may be taken to be $x_1x_2 + x_3x_4$, and this function assumes three distinct values under the twenty-four permutations of x_1, x_2, x_3, x_4. Thus the resolvent equation of a quartic is a cubic. However, in carrying over this analysis to the quintic Lagrange found that the resolvent equation is of degree six. Although Lagrange did not succeed in resolving the problem of the algebraic solvability of the quintic, his work was a milestone. It was the first time that an association was made between the solutions of a polynomial equation and the permutations of its roots. In fact, the study of the permutations of the roots of an equation was a cornerstone of Lagrange's general theory of algebraic equations. This, he speculated, formed "the true principles of the solution of equations." He was, of course, vindicated in this by Galois. Although Lagrange spoke of permutations without considering a "calculus" of permutations (e.g., there is no consideration of their composition or closure), it can be said that the germ of the group concept – as a group of permutations – is present in his work.

1.2 Number Theory

In the Disquisitiones Arithmeticae (Arithmetical Investigations) of 1801 Gauss summarized and unified much of the number theory that preceded him. The work also suggested new directions which kept mathematicians occupied for the entire century. As for its impact on group theory, the Disquisitiones may be said to have initiated the theory of finite abelian groups. In fact, Gauss established many of the significant properties of these groups without using any of the terminology of group theory. The groups appeared in four different guises: the additive group of integers modulo m, the multiplicative group of integers relatively prime to m, modulo m, the group of equivalence classes of binary quadratic forms, and the group of n-th roots of unity.

And although these examples turned up in number-theoretic contexts, it is as abelian groups that Gauss treated them, using what are clear prototypes of modern algebraic proofs. For example, considering the nonzero integers modulo p (p a prime), he showed that they are all powers of a single element; that is, that the group Z_p of such integers is cyclic.

Given any element of Z_p, he defined the order of the element (without using the terminology) and showed that the order of an element is a divisor of $p - 1$. He then used this result to prove Fermat's "little theorem," namely that $a^{p-1} \equiv 1 \pmod{p}$ if p does not divide a, thus employing group-theoretic ideas to prove number-theoretic results. Next he showed that if t is a positive integer which divides $p - 1$, then there exists an element in Z_p whose order is t – essentially the converse of Lagrange's theorem for cyclic groups.

Concerning the n-th roots of 1, which he considered in connection with the cyclotomic equation, he showed that they too form a cyclic group. In relation to this group he raised and answered many of the same questions he raised and answered in the case of Z_p. The problem of representing integers by binary quadratic forms goes back to Fermat in the early seventeenth century. (Recall his theorem that every prime of the form $4n + 1$ can be represented as a sum of two

squares $x^2 + y^2$.) Gauss devoted a large part of the Disquisitiones to an exhaustive study of binary quadratic forms and the representation of integers by such forms. A binary quadratic form is an expression of the form $ax^2 + bxy + cy^2$, with a, b, c integers. Gauss defined a composition on such forms, and remarked that if K_1 and K_2 are two such forms, one may denote their composition by $K_1 + K_2$. He then showed that this composition is associative and commutative, that there exists an identity, and that each form has an inverse, thus verifying all the properties of an abelian group. Despite these remarkable insights, one should not infer that Gauss had the concept of an abstract group, or even of a finite abelian group. Although the arguments in the Disquisitiones are quite general, each of the various types of "groups" he considered was dealt with separately – there was no unifying group-theoretic method which he applied to all cases.

1.3 Geometry

We are referring here to Klein's famous and influential lecture entitled "A Comparative Review of Recent Researches in Geometry," which he delivered in 1872 on the occasion of his admission to the faculty of the University of Erlangen. The aim of this so-called Erlangen Program was the classification of geometry as the study of invariants under various groups of transformations. Here there appear groups such as the projective group, the group of rigid motions, the group of similarities, the hyperbolic group, the elliptic groups, as well as the geometries associated with them. (The affine group was not mentioned by Klein.) Now for some background leading to Klein's Erlangen Program.

The nineteenth century witnessed an explosive growth in geometry, both in scope and in depth. New geometries emerged: projective geometry, non-Euclidean geometries, differential geometry, algebraic geometry, n-dimensional geometry, and Grassmann's geometry of extension. Various geometric methods competed for supremacy: the synthetic versus the analytic, the metric versus the projective. At mid-century a major problem had arisen, namely the classification of the relations and inner connections among the different geometries and geometric methods. This gave rise to the study of "geometric relations," focusing on the study of properties of figures invariant under transformations. Soon the focus shifted to a study of the transformations themselves. Thus the study of the geometric relations of figures became the study of the associated transformations.

Various types of transformations (e.g., collineations, circular transformations, inversive transformations, affinities) became the objects of specialized studies. Subsequently, the logical connections among transformations were investigated, and this led to the problem of classifying transformations, and eventually to Klein's group-theoretic synthesis of geometry.

Klein's use of groups in geometry was the final stage in bringing order to geometry. An intermediate stage was the founding of the first major theory of classification in geometry, beginning in the 1850s, the Cayley–Sylvester Invariant

Theory. Here the objective was to study invariants of "forms" under transformations of their variables. This theory of classification, the precursor of Klein's Erlangen Program, can be said to be implicitly group-theoretic. Klein's use of groups in geometry was, of course, explicit.

In the next section we will note the significance of Klein's Erlangen Program (and his other works) for the evolution of group theory. Since the Program originated a hundred years after Lagrange's work and eighty years after Gauss' work, its importance for group theory can best be appreciated after a discussion of the evolution of group theory beginning with the works of Lagrange and Gauss and ending with the period around 1870.

1.4 Analysis

In 1874 Lie introduced his general theory of continuous transformation groups – essentially what we call Lie groups today. Such a group is represented by the transformations $x_i' = f_i(x_1, x_2, \ldots, x_n, a_1, a_2, \ldots, a_n)$, $i = 1, 2, \ldots, n$, where the f_i are analytic functions in the x_i and a_i (the a_i are parameters, with both x_i and a_i real or complex). For example, the transformations given by

$x' = (ax + b)/(cx + d)$,

where a, b, c, d are real numbers and $ad - bc = 0$, define a continuous transformation group. Lie thought of himself as the successor of Abel and Galois, doing for differential equations what they had done for algebraic equations. His work was inspired by the observation that almost all the differential equations which had been integrated by the older methods remain invariant under continuous groups that can be easily constructed. He was then led to consider, in general, differential equations that remain invariant under a given continuous group and to investigate the possible simplifications in these equations which result from the known properties of the given group (cf. Galois theory). Although Lie did not succeed in the actual formulation of a "Galois theory of differential equations," his work was fundamental in the subsequent formulation of such a theory by Picard (1883-1887) and Vessiot (1892).

Poincaré and Klein began their work on "automorphic functions" and the groups associated with them around 1876. Automorphic functions (which are generalizations of the circular, hyperbolic, elliptic, and other functions of elementary analysis) are functions of a complex variable z, analytic in some domain D, which are invariant under the group of transformations

$x' = (ax + b)/(cx + d)$ (a, b, c, d real or complex and $ad - bc = 0$),

or under some subgroup of this group. Moreover, the group in question must be "discontinuous," that is, any compact domain contains only finitely many transforms of any point. Examples of such groups are the modular group (in which a, b, c, d are integers and $ad - bc = 1$), which is associated with the elliptic

modular functions, and Fuchsian groups (in which a, b, c, d are real and $ad - bc = 1$) associated with the Fuchsian automorphic functions.

1.5 Sylow's theorems

Among the methods of determining all finite groups, the approach of examining individual groups of certain orders can seem at times slow and methodical. Yet this task, begun in 1892 by Otto Holder, has proven fruitful in the advancement of group theory, if not always in the discovery of new simple groups. It has shed a great deal of light upon the structure of groups with given orders which allows one to understand the nature of simple groups, at least in so far as determining, what they are not. This particular problem, each aided by the work and discoveries of those who came before.

The range problem itself is not difficult to understand, in light of the search for simple groups. It is simply this: given a particular natural number, say n, what can we say about the structure of any group having n element? And in particular, can we determine if the group has any normal subgroups besides itself and the identity, i.e., can we show that the group is not simple? If the group is simple, is it unique? Through the history of this problem, there were two main methods used to explore the structure of groups with a given order. One was to use Sylow theorems and the other was to employ character theory.

"It would be of the greatest interest if it were possible to give an overview of the entire collection of finite simple groups." So begins an article by Otto Holder in *Mathematische Annalen* in 1982. Insofar as it is possible to give the birthyear of the program to classify the finite simple groups, this would be it. The first paper classifying an infinite family of finite simple groups, starting from a hypothesis on the structure of certain proper subgroups, was published by Burnside in 1899. As the final paper (the classification of quasithin simple groups of even characteristic by Aschbacher and S. D. Smith) in the first proof of the Classification Theorem for the Finite Simple Groups (henceforth to be called simply the Classification) will probably be published in the year 2001 or 2002, the classification endeavor comes very close to spanning precisely the 20^{th} century.

Of course there were some important pre-natal events. Galois introduced the concept of a normal subgroup in 1832, and Camille Jordan in the preface to his *Traite des substitutions et des equations algebriques* in 1870 flagged Galois' distinction between "groupes simples" and "groupes composees" as the most important dichotomy in the theory of permutation groups. Moreover, in the *Traite*, Jordan began to build a database of finite simple groups – the alternating groups of degree at least 5 and most of the classical projective linear groups over fields of prime cardinality. Finally, in 1872, Ludwig Sylow published his famous theorems on subgroups of prime power order.

Nevertheless Holder's paper is a landmark. Holder threw down a gauntlet which was rapidly taken up by Frank Cole, who in 1892 determined all simple groups of orders up to 500 (except for some uncertainties related to 360 and 432) and in 1893 extended this up to 660, discovering in the process a new simple group SL(2, 8). By the dawn of the 20th century Miller and Ling (1900) had pushed this frontier out to 2001. These results were achieved with the only available tools – Sylow's Theorems and the Pigeonhole Principle. Needless to say, the arsenal of weapons needed to be enlarged and the strategy of proceeding one integer at a time needed to be abandoned if any serious progress was to be made.

The abstract group concept spread rapidly during the 1880s and 1890s, although there still appeared a great many papers in the areas of permutation and transformation groups. The abstract viewpoint was manifested in two ways:

(a) Concepts and results introduced and proved in the setting of "concrete" groups were now reformulated and reproved in an abstract setting;

(b) Studies originating in, and based on, an abstract setting began to appear.

An interesting example of the former case is the reproving by Frobenius, in an abstract setting, of Sylow's theorem, which was proved by Sylow in 1872 for permutation groups. This was done in 1887, in a paper entitled "A new proof of Sylow's theorem." Although Frobenius admitted that the fact that every finite group can be represented by a group of permutations proves that Sylow's theorem must hold for all finite groups, he nevertheless wished to establish the theorem

abstractly: "Since the symmetric group, which is introduced into all these proofs, is totally alien to the context of Sylow's theorem, I have tried to find a new derivation of it".

II. Sylow theorems

For further presenting of Sylow theorems proofs, we should remind some necessary definitions and theorems and solve several essential lemmas.

Definition 1: Two subgroups S and T of a group G are called conjugate if there is a $g \in G$ such that $g^{-1}Sg = T$ ($g^{-1}Sg = T \Leftrightarrow g^{-1}Sg = \{g^{-1}Sg\ s \in S\}$).

Definition 2: Let A be a non-empty subset of a group G. The set $\{h\ h^{-1}Ah = A, h \in H\}$ is called the normalizer of A in H and is written $N_H(A)$.

Definition 3: Let A and B be non-empty subsets of G. B is said to be an *H-conjugate* of A if $h^{-1}Ah = B$ for some $h \in H$.

Definition 4: Suppose H is a subgroup of G of order a power of a prime p, and $|H|$ is the highest power of p that divides |G|. Then H is called a *Sylow p-subgroup* of G.

Lagrange's theorem

The order of a subgroup H of a finite group G divides the order of G, or in other words

$$|G| = |H| \cdot |G:H|$$

Lemmas 1, 2

1) If A is a subset of G, then $N(A)$ is a subgroup of G;

2) If A is a subgroup of G, then $A \lhd G$ if and only if $N(A) = G$.

Proof

1) $N(A) \neq 0$, since $1 \in N(A)$. Let $f, g \in N(A)$. Using $gA = Ag$ and $fA = Af$ implies $(fg^{-1})A = f(g^{-1}A) = f(Ag^{-1}) = (fA)g^{-1} = (Af)g^{-1} = A(fg^{-1})$. Hence $f, g \in N(A)$ implies $fg^{-1} \in N(A)$. Therefore $N(A)$ is a subgroup of G. Clearly, if A is a subgroup, $A \subseteq N(A)$ and $A \lhd N(A)$.

2) If A is a subgroup and $A \lhd G$, then for each $g \in G, gA = Ag$. Hence $g \in N(A)$ and so $G \subseteq N(A)$. Therefore $G = N(A)$. If A is a subgroup and $N(A) = G$, then since $A \lhd N(A)$, $A \lhd G$.

Lemma 3

If H is a subset of a group G and $g \in G$, then $|g^{-1}Hg| = |H|$, where $g^{-1}Hg = \{g^{-1}hg \, h \in H\}$.

Proof

We define a matching $\alpha : H \to g^{-1}Hg$ by $\alpha : h \to g^{-1}hg$ for $h \in H$. α is clearly an onto mapping. To show α is also one-to-one, we must prove $h_1 = h_2 (h_1, h_2 \in H)$ if and only if $g^{-1}h_1g = g^{-1}h_2g$. Let $h_1 = h_2$. Then by multiplying on the left by g^{-1} and on the right by g we get $g^{-1}h_1g = g^{-1}h_2g$. Similarly $g^{-1}h_1g = g^{-1}h_2g$ implies $h_1 = h_2$. Hence α is a matching and $|g^{-1}Hg| = |H|$.

Lemma 4

Let $|G| = p^r m (r \geq 1$ and $p \nmid m)$ and let P be a Sylow p-subgroup of G. Then if H is a p-group such that $P \subseteq H \subseteq G$, then $H = P$.

Proof

Suppose $|H| = p^t, t \geq 0$. By Lagrange's theorem, $p^t \mid p^r m$. Since p | m, $t \leq r$. But $P \subseteq H$ and $|P| = p^r$. Hence t = r and $|H| = |P|$, and so P = H.

Lemma 5

If H is a Sylow p-subgroup of G, then $g^{-1}Hg$ is also a Sylow p-subgroup of G.

Proof

Suppose $|G| = p^r m$ ($r \geq 0$ and $p \nmid m$); then $|H| = p^r$. But $|g^{-1}Hg| = |H|$ by Lemma 3. Hence $g^{-1}Hg$ is a Sylow p-subgroup of G if it is a subgroup. Now we have to prove that $g^{-1}Hg$ is a subgroup. According to well-known fact that if $f_1, f_2 \in H \subseteq G$ then H – subgroup $\Leftrightarrow$ $f_1 f_2^{-1} \in H$. Let us observe that $(g^{-1}h_1 g)(g^{-1}h_2 g)^{-1} = g^{-1}h_1 h_2^{-1} g \in g^{-1}Hg$.

$g^{-1}Hg$ is therefore a subgroup.

Lemma 6

$N_H(A) = N_G(A) \cap H$ for any non-empty subset A and subgroup H of a group G.

Proof

Let $n \in N_H(A)$; then $n \in H$ and $n^{-1}An = A$. But $H \subseteq G$, so that $n \in G$ and by definition $n \in N_G(A)$. Consequently $N_H(A) \subseteq N_G(A) \cap H$. If $n \in N_G(A) \cap H$, then $n^{-1}An = A$ and $n \in H$. Thus $N_G(A) \cap H \subseteq N_H(A)$ and the equality follows.

2.1 First Sylow Theorem

To prove Sylow's First Theorem yet two more lemmas will be needed.

Lemma 7

If G is a finite group with subgroup H and non-empty subset A, the number of distinct H-conjugates of A is the index of $N_H(A)$ in H, i.e. $[H : N_H(A)]$.

Proof:

Since $[H : N_H(A)]$ is the number of distinct right cosets of $N_H(A)$ in H, we need only define a one-to-one mapping, α, of the right cosets of $N_H(A)$ in H onto the distinct H-conjugates of A. Let α be defined by

$$\alpha : N_H(A)h \to h^{-1}Ah (h \in H)$$

To show that α is a one-to-one mapping, we must prove that for $h_1, h_2 \in H$,

$$N_H(A)h_1 = N_H(A)h_2 \text{ if and only if } h_1^{-1}Ah_1 = h_2^{-1}Ah_2$$

($\Leftarrow$) Let $h_1^{-1}Ah_1 = h_2^{-1}Ah_2$. Then $A = h_1h_2^{-1}Ah_2h_1^{-1} = (h_2h_1^{-1})^{-1}A(h_2h_1^{-1})$. Hence $h_2h_1^{-1} \in N_H(A)$ and so $h_2 \in N_H(A)h_1$. Since two right cosets are equal or disjoint, we conclude $N_H(A)h_1 = N_H(A)h_2$. Thus $h_1^{-1}Ah_1 = h_2^{-1}Ah_2$ implies $N_H(A)h_1 = N_H(A)h_2$.

($\Rightarrow$) If $N_H(A)h_1 = N_H(A)h_2$, then $h_1 \in N_H(A)h_2$, i.e. $h_1 = nh_2$ for some $n \in N_H(A)$. Therefore

$$h_1^{-1}Ah_1 = (nh_2)^{-1}Anh_2 = h_2^{-1}n^{-1}Anh_2 = h_2^{-1}Ah_2$$

because $n^{-1}An = A$ by definition of $N_H(A)$. Hence $N_H(A)h_1 = N_H(A)h_2$ implies $h_1^{-1}Ah_1 = h_2^{-1}Ah_2$ α is clearly onto, so the proof is complete.

We will make a few observations about ~, which follow because it is an equivalence relation on $\Im$. Recall that if $A \in \Im$, $A\sim = \{X \; X \in A \; and \; X \sim A\}$, i.e. $A\sim$ is the equivalence class containing A. Recall that the distinct equivalence classes are disjoint and that their union is $\Im$.

By a set *of representatives of the equivalence classes* we mean a set R which contains one and only one element from each of the distinct equivalence classes. It follows that $\Im$ is the disjoint union of the sets $R\sim$, $R \in \Re$. Hence

$$|\Im| = \sum_{R \in \Re} |R\sim|.$$

Lemma 8

Let $\Im$ ($\neq \emptyset$) be a set of subsets of G. Suppose that for each $A \in \Im$ and each $h \in H, h^{-1}Ah \in \Im$. Let ~ denote the equivalence relation defined by $A \sim B$ if B is an H-conjugate of A. Let $\Re$ be a set of representatives of the equivalence classes. Then $|\Im| = \sum_{R \in \Re} [H : N_H(R)]$

Proof:

We know from the remarks above that

$$|\Im| = \sum_{R \in \Re} |R\sim|$$

But $R\sim = \{X \; X = h^{-1}Rh \; for \; some \; h \in H\}$ since $h^{-1}Rh \in \Im$ for every $h \in H$. So $R\sim$ is the set of H-conjugates of R. The number of such H-conjugates is, by Lemma 7, $[H : N_H(A)]$. Hence $|\Im| = \sum_{R \in \Re} [H : N_H(R)]$, as claimed.

Corollary 1

Let P ($\neq \emptyset$) be a subset of G. Let $\Im = \{g^{-1}Pg \; g \in G\}$. Let $\Re$, H and ~ be as in Lemma 8. Then $|\Im| = \sum_{R \in \Re} [H : N_H(R)] = [G : N_G(P)]$

Corollary 2

Let $\Im$={ A| A is a subset of G and A has precisely one element}. Let ~ be the equivalence relation in $\Im$ when H = G, and let $\Re$ be a set of representatives of the equivalence classes. Let $\Re^* = \{R \; R \cap Z(G) = O, R \in \Re\}$. Then

$$|G| = |Z(G)| + \sum_{R \in \Re} [G : N_G(R)]$$

Proof:

Clearly $|\Im| = |G|$; hence

$$|G| = \sum_{R \in \Re} [G : N_G(R)] \qquad (*)$$

If $z \in Z(G)$, then $\{z\} \in \Im$ and the number of G-conjugates of {z} is one, namely {z} itself. Consequently $\{z\} \in \Re$ for each $z \in Z(G)$. Note that $N_G(\{z\}) = G$ if $z \in Z(G)$. Hence adding first the contribution made by all $R \in \Re$ with $R \cap Z(G) \neq 0$ in (*), we obtain $|Z(G)|$ and the result follows.

Note that as $R = \{r\}$,

$$N_G(R) = \{g \; g \in G \; and \; g^{-1}rg \in R\} = \{g \; g \in G \; and \; g^{-1}rg \in r\} = C(R)$$

Hence Corollary 2 takes the form

$$|G| = |Z(G)| + \sum_{R \in \Re^*} [G : C(R)] \qquad (**)$$

is called the *class equation of G.*

Firstly, we will prove a weak form of the first Sylow theorem.

Proposition 1

If G is a finite abelian group and p is a prime dividing the order of G, then G has an element of order p.

Proof:

We will prove the proposition by induction on the order of G. If |G| = 1 there is nothing to prove. Assume the proposition is true for all groups of order less than n, the order of G, where $n > 1$. If G is cyclic there is a subgroup of order

any integer that divides |G|. Thus if G is cyclic the theorem holds, and we may therefore assume G is not cyclic. If n is a prime, G is cyclic; hence n is not a prime.

Suppose $h(\neq 1) \in G$, h of order m. Clearly $m < n$. Let H be the cyclic group generated by h. H is a proper subgroup of G. Now if $p \mid m$, by the induction assumption, H has an element of order p. If $p \nmid m$, form the factor group G/H (every subgroup of an abelian group is a normal subgroup so $H \triangleleft G$). Since $|H| > 1$, $|G/H| < |G|$. As $|G/H| = |G|/|H|$, $p \mid |G|/|H|$. Therefore by the induction assumption, G/H has an element g of order p.

Let $\nu : G \to G/H$ be the natural homomorphism of a group onto its factor group and g be a preimage of g under ν. Now $(g^p)\nu = g^p =$ the identity of G/H, so $g^p \in H$. As H is of order m, $(g^m)^p = (g^p)^m = 1$. Therefore g^m has order p or $g^m = 1$. If $g^m = 1$, then $g^m\nu = g^m = 1$. Since g has order p this implies p divides m, contrary to our assumption. Therefore g^m is an element of G of order p.

First Sylow Theorem

Let G be a finite group, p a prime, and p^r the highest power of p dividing the order of G. Then there is a subgroup of G of order p^r.

Proof:

We will prove the theorem by induction on the order n of G. For $|G| = 1$ the theorem is trivial. Assume $n > 1$ and that the theorem is true for groups of order $< n$. Suppose $|Z(G)| = c$. We have two possibilities:

1) $p \mid c$;

$Z(G)$ is an abelian group. By Proposition 1, $Z(G)$ has an element of order p. Let N be a cyclic subgroup of $Z(G)$ generated by an element of order p. $N \triangleleft G$, since any subgroup of $Z(G)$ is normal in G. Consider G/N. Then $|G/N| = n/p$ by Lagrange's Theorem. Hence by our induction assumption, G/N has a subgroup H of order p^{r-1}.

There exists a subgroup H of G such that $H/N = H$. As $p^{r-1} = |H| = |H|/|N| = |H|/p$, we conclude that $|H| = p^r$. Thus in this case, G has a subgroup of order p^r.

(2) $p \nmid c$.

The class equation for G is (see equation (**) of Corollary 2):

$$|G| = |Z(G)| + \sum_{R \in \mathfrak{R}^*} [G : C(R)]$$

Since $p \mid |G|$ and $p \nmid c$, we have $p \nmid \sum_{R \in \mathfrak{R}^*} [G : C(R)]$. Therefore for at least one $R \in \mathfrak{R}^*$, $p \nmid [G : C(R)]$. But $|G| = [G : C(R)]|C(R)|$ by Lagrange's theorem. Hence $p^r \mid |C(R)|$, since $p^r \mid |G|$. Now $|C(R)| \neq |G|$; for if $|C(R)| = |G|$, then $C(R) = G$ and $R \cap Z(G) = R$, contrary to the assumption that $R \cap Z(G) = 0$. Thus by the induction assumption, *C(R)* has a subgroup H of order p^r. Consequently so does G.

In either case we have found a subgroup H of order p^r.

2.2 Second Sylow Theorem

Lemma 9 will help us to prove Second Sylow Theorem.

Lemma 9:

If G is a finite group, P a Sylow p-subgroup of G, and H is a subgroup of G of order a power of p, then

$$N_H(P) = H \cap P$$

Proof:

$P \cap H \subseteq N_H(P)$, as conjugation by an element of P sends P to itself. We show $N_H(P) \subseteq P \cap H$. $N_H(P) \subseteq N_G(P)$ and $P \lhd N_G(P)$ (see Lemma 2 and Lemma 6), so that by the subgroup isomorphism theorem we have: $N_H(P)P$ is a subgroup of G and

$$N_H(P)P / P \cong N_H(P) / N_H(P) \cap P$$

Consequently $[N_H(P)P : P] = [N_H(P) : N_H(P) \cap P]$. But $N_H(P)$ *is* a p-group, i.e. a group of order a power of p, since it is a subgroup of the p-group H. Thus $[N_H(P) : N_H(P) \cap P]$ is a power of p. $[N_H(P)P : P]$ is therefore also a power of p and, as P is a p-group, $|N_H(P)P|$ is a power of p. Accordingly, $N_H(P)P$ is a p-group. But $P \subseteq N_H(P)P$ and P is a Sylow p-subgroup. Hence $P = N_H(P)P$, for P cannot be a proper subgroup of any other p-subgroup of G (see Lemma 6). $N_H(P)$ is therefore a subgroup of P. As $N_H(P) \subseteq H$, we conclude $N_H(P) \subseteq P \cap H$.

Second Sylow Theorem

If H is a subgroup of a finite group G, and let P be a Sylow p-group of G. If H is a p-group, then H is contained in a G-conjugate of P.

Proof:

We apply Corollary 1, to $\Im = \{g^{-1}Pg \mid g \in G\}$ to conclude

$$|\Im| = \sum_{R \in \Re} [H : N_H(R)] = [G : N_G(P)]$$

By Lemma 9, $N_H(P) = H \cap P$ for each $R \in \Re$. Hence

$$[G : N_G(P)] = \sum_{R \in \Re} [H : H \cap R] \qquad (***)$$

If $H \cap R \neq H$ for all $R \in \Re$, as H is a p-group, the right-hand side of equation (***) is divisible by p. Hence $[G : N_G(P)]$ *is* divisible by p. But $P \subseteq N_G(P)$, so that p does not divide $[G : N_G(P)]$. This contradiction implies that $H \cap R = H$ for at least one $R \in \Re$. But as $R \in \Im$, R is a G-conjugate of P. The result follows.

Third Sylow Theorem

1) Any two Sylow p-subgroups of a finite group G are G-conjugate.

2) The number s_p of distinct Sylow p-subgroups of G is congruent to 1 modulo p.

3) s_p divides $|G|$.

Proof:

1) Let P and P' be two Sylow p-subgroups of G. By the second Sylow theorem, P', as a p-group, is contained in some G-conjugate R of P. But $|P'| = |R|$, by Lemma 3. Hence $P' = R$ and P' is conjugate to P under G.

2) Let P be any Sylow p-subgroup of G. Since any other Sylow p-subgroup is conjugate to P and any conjugate of a Sylow p-subgroup is a Sylow p-subgroup (Lemma 5), we conclude by Lemma 7 that

$$s_p = [G : N_G(P)]$$

But on putting $P = H$ in equation *(***)*, we have

$$s_p = \sum_{R \in \Re} [P : P \cap R]$$

Now for exactly one $R \in \Re$, $R = P$; for the only P-conjugate of P is P itself and so P is the only possible representative of its equivalence class. In all other cases, $P \cap R \neq P$. Therefore $[P : P \cap R]$ is a power of p for all $R \in \Re$ except one, and for this one $[P : P \cap R] = 1$. Hence

$$s_p = 1 + kp$$

3) By Lagrange's theorem, $|G| = [G : N_G(P)]\,|N_G(P)|$. Since $s_p = [G : N_G(P)]$, $s_p \,||\, G|$.

Corollary 3

If p and q are different prime factors of G and $n_p = 1$ and $n_q = 1$ then the elements of the p-Sylow subgroup commute with the elements of the q-Sylow subgroup.

Proof

Let P be the p-Sylow subgroup and Q be the q-Sylow subgroup. Since P and Q have relatively primes sizes, $P \cap Q = \{e\}$ by Lagrange. The subgroups P and Q are normal in G since $n_p = 1$ and $n_q = 1$ by hypothesis. For $a \in P$ and $b \in Q$,

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in P \cap Q = \{e\}$$

so $ab = ba$.

2.4 Alternative proof of Sylow theorems

In this chapter, we would like to present some historical proof of Sylow's Theorem.

Sylow's Theorem proof by Sylow

In modern language, here is Sylow's proof that his subgroups exist.

Pick a prime p dividing $|G|$. Let P be a p-subgroup of G which is as large as possible. We call P a maximal p-subgroup. We do not yet know its size is the biggest p-power in $|G|$. The goal is to show $[G:P]$ is not $\equiv 0 \bmod p$, so $|P|$ is the largest p-power dividing $|G|$.

Let $N = N(P)$ be the normalizer of P in G. Then all the elements of p-power order in N lie in P. Indeed, any element of N with p-power order which is not in P would give a non-identity element of p-power order in N/P. Then we could take inverse images through the projection $N \to N/P$ to find a p-subgroup inside N properly containing P, but this contradicts the maximality of P as a p-subgroup of G.

Since there are no non-trivial elements of p-power order in N/P, the index $[N:P]$ is not divisible by p by Cauchy's theorem.

Now let the p-group P act on G/N by left multiplication. Since $[G:P]$ is not $\equiv 0 \bmod p$, there must be a fixed point, say gN for some $g \in G$. For every $t \in P, tgN = gN$, so $g^{-1}Pg \subset N$. Because (as shown above) all elements of p-power order in N lie in P, $g^{-1}Pg \subset P$, and therefore $g^{-1}Pg = P$. Thus $g \in N(P) = N$, so $gN = N$.

Thus $N \in G/N$ is the only fixed point for left multiplication of P on G/N. Every other orbit has size divisible by p, so the fixed point congruence tells us $[G:N] \equiv 1 \bmod p$.

Therefore

$$[G:P]=[G:N][N:P]\equiv[N:P]\ is\ not\equiv 1 \bmod p$$

which proves P is a p-Sylow subgroup of G.

Sylow's Theorem by Frobenius

Here is Frobenius' first proof on the existence of Sylow subgroups. It takes for granted that there are Sylow subgroups of symmetric groups; this had been shown in a paper of Cauchy before Sylow's work.

By Cayley's theorem, every finite group can be embedded in a symmetric group. Given a finite group G, suppose we have $G \subset S_n$. Pick a prime p. By Cauchy's work, S_n has a p-Sylow subgroup, say P. Consider the *(G,P) double* coset decomposition of S_n:

$$S_n = \bigcup_i G\delta_i P$$

Each double coset $G\delta_i P$ has size $|G||P|/|(G\cap\delta_i^{-1}P\delta_i)|$, which is divisible by $|P|$. Therefore

$$\frac{|S_n|}{|P|}=\sum_i \frac{|G|}{|(G\cap\delta_i^{-1}P\delta_i)|}.$$

Since $|S_n|/|P|$ is not $\equiv 0 \bmod p$, one of the terms in the sum is not divisible by p. Let it be the *j-th* term. Then $G\cap\delta_j^{-1}P\delta_j$ is a p-group (since it's a subgroup of $\delta_j^{-1}P\delta_j$) with maximal p-power size inside of G (since its ratio with $|G|$ is not divisible by p). Thus $G\cap\delta_j^{-1}P\delta_j$ is a p-Sylow subgroup of G.

Modern alternative proof

Here we give an alternative proof, elementary and combinatoric in nature, due to Wielandt. There are many other proofs of this result. For a finite group G, Sylow's Theorems guarantee the existence of subgroups of all prime-power orders

dividing the order of G. This can be viewed as a kind of partial converse to Lagrange's Theorem.

Sylow's Theorem:

Let G be a finite group, p a prime, $|G| = p^{\alpha}m$, $(p;m) = 1$. Then:

1) every p-subgroup of G is contained in a subgroup of order p^{α} (and hence, since $\{1\}$ is a p-subgroup, Sylow p-subgroups exist)
2) if n_p denotes the number of Sylow p-subgroups, then $n_p \equiv 1 \pmod{p}$ and n_p divides m;
3) any two Sylow p-subgroups are conjugate in G (and hence also isomorphic).

Proof:

First we show existence of Sylow p-subgroups. Let S denote the set of all subsets of G with exactly p^{α} elements, and let G act on S by left multiplication.

Notice $|S| = \dfrac{(p^{\alpha}m)!}{p^{\alpha}!(p^{\alpha}m - p^{\alpha})!}$.

We claim that this is not divisible by p. We have

$$|S| = \frac{p^{\alpha}m(p^{\alpha}m-1)\cdots(p^{\alpha}m-p^{\alpha}+1)}{1\cdot 2\cdots(p^{\alpha}-1)p^{\alpha}} = m\prod_{i=1}^{p^{\alpha}-1}\left(\frac{p^{\alpha}m-i}{i}\right)$$

Consider $\dfrac{p^{\alpha}m-i}{i}$; $1 \le i < p^{\alpha}$. If p^{j} divides i then $j < \alpha$ and p^{j} divides $p^{\alpha}m - i$. Therefore p does not divide any of the factors $\dfrac{p^{\alpha}m-i}{i}$ and so does not divide $|S|$. This implies there is some orbit of S under the action of G which has order not divisible by p. Call it S_1. Let $X \in S_1$ and consider $[G : G_X] = |S_1|$. Then p does not divide this index, so p^{α} divides $|G_X|$. Now X is a subset of G with exactly p^{α} elements. Choose $x \in X$. Then $|\{gx | g \in G_X\}| = |G_X|$. Since G_X stabilizes X, we must have $gx \in X$ for all $g \in G_X$. Therefore $|G_X| \le p^{\alpha} = |X|$. Thus $|G_X| = p^{\alpha}$, and we have found a Sylow p-subgroup.

Now let ψ denote the set of all conjugates of some Sylow p-subgroup P in G. Then P acts on ψ by conjugation. The number of elements in an orbit must be a

power of p: $[P:P_x]=|O_x|$. We claim that P is the only element in ψ with a singleton orbit. If $O_{P_1}=P_1$, then $P_1 \lhd \langle P, P_1 \rangle$, so PP_1 is a subgroup of order $|P||P_1|/|P\cap P_1|=p^\alpha$, so $P=PP_1=P_1$. Thus $|\psi|\equiv 1 \pmod p$. Also $|\psi|=[G:N_G(P)]$ and $m=[G:P]=[G:N_G(P)][N_G(P):P]$, so $|\psi|$ divides m. We will be done if we can show that any p-subgroup of G is contained in some group in ψ (for then any Sylow p-subgroup will be conjugate to P, and every p-subgroup will be contained in a Sylow p-subgroup).

Let P' be a p-subgroup of G. Suppose P' is not contained in some conjugate of P. Let P' act on ψ by conjugation. Then there can be no singleton orbits or, as before, $P'P_1$ would be a subgroup of order greater than p^α, a contradiction. That says all P'-orbits in ψ have order a power of p, and are not 1. That implies $|\psi|\equiv 0 \pmod p$, a contradiction. Thus P' is contained in some $P_1 \in \psi$.

III. Applications

In the last chapter we would like to show you different applications of Sylow's theorems. Usually theorems are used for the classification of finite groups.

Also, the bulk of these applications use the Sylow's Theorems to show the existence of nontrivial proper normal subgroups, allowing one to show that a group of a given size is not simple and to proof theorems about cyclic groups,

3.1 Applications for theorems proving

Here is a nice application of First Sylow Theorem.

Theorem 1

If a finite group has at most one subgroup of any size, then it is a cyclic group.

Proof

Our argument has two steps: use Sylow I to reduce the theorem to the prime power case, and then settle the prime power case.

Step 1. Let G be a group with a unique subgroup of each size. In particular, for each prime p we obtain by Sylow I that G has one p-Sylow subgroup. Each Sylow subgroup is normal since $n_p = 1$. Then, for different primes p and q dividing $|G|$, the elements of the p-Sylow and q-Sylow subgroups commute with each other by Corollary 3.

Any subgroup of G has at most one subgroup of any size (otherwise G itself would have two subgroups of the same size). Suppose we knew the theorem for all groups with prime-power size. Then, for each prime p dividing $|G|$, the p-Sylow subgroup of G has to be cyclic. Choose a generator a_p of the p-Sylow subgroup of G. The order of a_p is the size of the p-Sylow subgroup of G. These a_p's commute as p varies and their orders are relatively prime, so the product of the a_p's has order equal to the product of the sizes of the Sylow subgroups of G. This product of sizes is $|G|$, so G is cyclic.

Step 2. We are now reduced to verifying our theorem for groups with prime-power size. The Sylow theorems will not be used further.

Let $|G| = p^k$ where p is prime, $k \geq 1$, and assume G has at most one subgroup of each size. To show G is cyclic, we argue by induction on k. If $k = 1$ then G has prime size so it is cyclic. We now suppose that $k \geq 2$ and the theorem is proved for all groups with p-power size less than p^k which have at most one subgroup of each size.

Since G is a nontrivial group with p-power size, it has a nontrivial center. Pick (by Cauchy) an element a of order p in the center of G. Then $\langle a \rangle$ is a subgroup of G with order p, so it is the unique such subgroup. Since every nontrivial subgroup of G contains a subgroup of size p by Cauchy, every nontrivial subgroup of G contains $\langle a \rangle$.

Since a lies in the center of G, $\langle a \rangle$ is a normal subgroup of G. We therefore can consider the group $G/\langle a \rangle$, whose size is p^{k-1}. Let's show $G/\langle a \rangle$ has at most one subgroup of any size. For any subgroup H of $G/\langle a \rangle$, let H' be the inverse image of H in G (all the elements of G which reduce to H). Then H' contains $\langle a \rangle$, has p times as many elements as H, and $H = H'/\langle a \rangle$. If K is a subgroup of $G/\langle a \rangle$ with the same size as H then $|K'| = |G'|$ (we define K' from K in the same way as H' is defined from H), so $H = K'$ since G is assumed to have at most one subgroup of any size. Reducing back modulo $\langle a \rangle$, we get $H = H'/\langle a \rangle = K'/\langle a \rangle = K$ in $G/\langle a \rangle$.

By induction, $G/\langle a \rangle$ is a cyclic group:

$$G/\langle a \rangle = \langle \bar{b} \rangle$$

Then every element of G has the form $b^i a^j$ for some i and j, and $b \neq e$ since $G/\langle a \rangle$ is nontrivial. Since $\langle b \rangle$ is a nontrivial subgroup of G, it must contain $\langle a \rangle$. Therefore $a \in \langle b \rangle$, so $b^i a^j$ is a power of b. This implies G is cyclic, which settles the theorem for groups of prime-power size.

□

Here is another application of First Sylow Theorem to prove a similar theorem.

Theorem 2

Let G be a finite group such that, for each n dividing $|G|$, the equation $x^n = 1$ in G has at most n solutions. Then G is cyclic.

Proof

We again argue in two steps: reduction to the prime power case using First Sylow Theorem and then the prime power case.

Step 1. Let p be a prime dividing $|G|$ and p^k be the largest power of p in $|G|$. Every $g \in G$ of p-power order in G has order dividing p^k (all orders divide $|G|$), so g is a solution to $x^{p^k} = 1$. Let P be a p-Sylow subgroup of G. It provides us with p^k solutions to this equation, so by assumption these are all the solutions. Therefore all elements of p-power order are in P, so P is the only p-Sylow subgroup.

The hypothesis on G passes to any of its subgroups, such as its Sylow subgroups. If we knew the theorem for groups of prime-power size then we get cyclicity of the Sylow subgroups, so G is cyclic by the same argument as in Step 1 of the proof of Theorem 1.

Step 2. We now verify the theorem for p-groups. The Sylow theorems are not going to be used. Let $|G| = p^k$, where $k \geq 2$. (The case $k=1$ is trivial.) Assume $x^n = 1$ has at most n solutions in G whenever $n \mid p^k$. We want to show G is cyclic. If $N \lhd G$ and $|(G/N)| > p$ then G/N has a nontrivial normal subgroup of order p (such as a subgroup of order p in its center). Lifting this subgroup of G/N back to G gives a normal subgroup $H \lhd G$ with $N \subset H \subset G$ and $[H:N]=p$. We can repeat this with H in place of N, and so on, so a maximal proper normal subgroup of G has index p in G. Let M be such a subgroup, so $|M| = p^{k-1}$. The equation $x^{p^{k-1}} = 1$ has p^{k-1} solutions in M, so by hypothesis these are the only solutions to this equation in G. Therefore any element of G - M does not have order dividing p^{k-1}, so its order must be p^k, which shows G is cyclic.

□

3.2 Applications to specific groups

Application 1

Let us prove that a group G of order $48 = 2^4 \cdot 3$ is not simple. Also we are going to show that G has either a normal subgroup of order 8 or 16.

Proof

If G is simple, $n_2 = 3$. Let $P \in Syl_2(G)$ and let G act by left multiplication on the left cosets of P; in this way, we get a nontrivial homomorphism $\rho : G \to S_3$. Since G is simple, Ker ρ is trivial, so 48 divides 6, which is absurd.

If $n_2 = 1$, then G has a Sylow 2_rsubgroup which is normal. Otherwise, assume $n_2 = 3$, so that there are 3 subgroups of order 16. Let H, K be any two of them. Then $H \cap K$ must be of order 8: for if $|H \cap K| \leq 4$ then $|HK| \geq \frac{16^2}{4} = 64$, impossible. It follows that $H \cap K$ is normal in both H and K since $H \cap K$ has index 2 in both H and K; this implies

$$H = N_H(H \cap K) := N_G(H \cap K) \cap H \Rightarrow H < N_G(H \cap K)$$

Thus $N_G(H \cap K)$ has order a multiple of 16 and a divisor of 48 so

$$|N_G(H \cap K)| = 48 = |G| \Rightarrow N_G(H \cap K) = G$$

so $H \cap K$ is a normal subgroup of G of order 8.

Application 2

Let us show that a group G of order $108 = 2^2 \cdot 3^3$ has a normal subgroup of order 9 or 27.

Proof

We have either $n_3 = 1$ or 4; if $n_3 = 1$, then G has a normal subgroup of order 27.

If $n_3 \neq 1$, let S be a Sylow 3-subgroup of G. Now, $|G : S| = 4$, so let G act by left multiplication on the left cosets of S. This action affords a permutation representation $\mu : G \to S_4$. Observe that $|\mu(G)|$ divides both 108 and 24, so it

must be a divisor of gcd(108,24) = 12. So $|\mu(G)| \leq 12 \Rightarrow |Ker\mu| \geq 9$. On the other hand, the kernel of this action is the largest normal subgroup of G contained in S, and this implies $|Ker\mu|$ must be a divisor of 27.

Since $|Ker\mu| \geq 9$, it follows that $|Ker\mu| = 9$ or 27.

Application 3

In this example we will prove that if N is a normal subgroup of G that contains a Sylow p-subgroup of G, then the number of Sylow p-subgroups of N is the same as that of G, i.e. $n_p(G) = n_p(N)$. Also we will use this to show that if G is a group of order 105, then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

Proof

Suppose that N contains the Sylow p-subgroup P. Then since N is normal it also contains all of the conjugates of P. But now N contains all of the Sylow p-subgroups of G, since they are all conjugate. Conclude that N and G have the same number of Sylow p-subgroups.

Next, $105 = 3 \cdot 5 \cdot 7$ and we have $n_3 = 1$ or 7; $n_5 = 1$ or 21, and $n_7 = 1$ or 15. Let $P \in Syl_5(G)$ and $Q \in Syl_7(G)$. Note that at least one of P, Q must be normal, since otherwise we would have 21(5−1)=48 e lements of order 5 and 15(7−1)=90 elements of order 7. Now, PQ is a subgroup, and it must be normal since its index is the smallest prime divisor of $|G|$. Since PQ is normal and contains a Sylow 5-subgroup, it contains all of the Sylow 5-subgroups of G. It follows that PQ and G have the same number of Sylow 5-subgroups, i.e. $n_5(PQ) = n_5(G)$. Similarly, $n_7(PQ) = n_7(G)$. It now follows $n_5(G) = n_7(G) = 1$.

Application 4

Let us show that a group of order p^2q, with p, q distinct primes, has either a normal Sylow p-subgroup, or a normal Sylow q-subgroup.

Proof

Suppose by way of contradiction $n_p > 1$ and $n_q >$. But n_p divides q so $n_p = q = 1 + kp$ for $k \neq 0$ so in particular, $q > p$.

Next n_q divides p^2 so either $n_q = p$ or $n_q = p^2$. But distinct Sylow q-subgroups intersect trivially, so there are $n_q(q-1)$ elements of order q in G.

Suppose first $n_q = p^2$. Then there are $p^2q - p^2(q-1)$ elements not of order q. But if $P \in Syl_p$, then P has no elements of order q, so P accounts for all the elements of G not of order q, so P must be the unique Sylow p-subgroup of G, i.e. $n_p = 1$, a contradiction. Therefore, $n_q = p$. But since $n_q \equiv 1 \bmod q$, we have $p>q$, a contradiction. Conclude that either $n_q = 1$ or $n_p = 1$.

Application 5

No group of order $36 = 2^2 \cdot 3^2$ is simple.

Proof

Suppose there is such a group G; then $n_3 = 4$. Let H, K be two distinct Sylow 3-subgroups, each of order 9. Notice that $H \cap K$ must have (at least) 3 elements, otherwise we would have $|HK| = 81$ elements in G, which is absurd. Also, $H \cap K$ is normal in both H and K. As before, $H < N_G(H \cap K)$ so $N_G(H \cap K)$ has order a multiple of 9 and a divisor of 36; that is, either $N_G(H \cap K)$ has order either 18 or 36. If it has order 18, then it has index 2 in G, so it is normal in G; if the order is 36, then $N_G(H \cap K) = G$ so $H \cap K$ is normal in G. Either way, no group of order 36 is simple.

Application 6

Every group G of order $255 = 3 \cdot 5 \cdot 17$ is abelian.

Proof

Let H be the unique Sylow 17-subgroup. Then G/H has order 15. Since H is a normal subgroup of G with abelian quotient, the commutator $G' < H$. Thus, G' has order 1 or 17 as a subgroup of H.

But now G has either 1 or 85 subgroups of order 3; either 1 or 51 subgroups of order 5. By order considerations (85 subgroups of order 3 and 51 of order 5 would require 375 elements of G, im possible), we must have either a subgroup K of order 3 or 5.

Then G/K has order either $5 \cdot 17$ or $3 \cdot 17$; in either case, G/K is abelian (pq, again). Thus $G' < K$ and this impli es G' has order either 1, 3 or 5. But $G' < H$ shows that G' has order either 1 or 17, so G' is trivial, hence G is abelian.

Application 7

Prove that a group of order 105 contains a subgroup of order 35.

Proof

Let G be a group of o rder $|G| = 105 = 3 \cdot 5 \cdot 7$. Then $n_5 = 1$ or 21; and $n_7 = 1$ or 15. If $n_5 = 21$ then there are $4 \times 21 = 84$ elements of order 5, and if $n_7 = 15$ there are $6 \times 15 = 90$ elements of order 3; but this implies G has at least 174 elements, which is absurd. So we must have $n_5 = 1$ or $n_7 = 1$. So let P be a Sylow 5-subgroup, and let Q b e a Sylow 7-subgroup. Now $P \cap Q = \{e\}$ since e is the only element whose order divides $|P| = 5$ and $|Q| = 7$. Since either P or Q is normal, it follows PQ is a subgroup of G of order 35, as desired.

Application 8

Let G be a finite group and let N be a normal subgroup of G. Show that

$$n_p(G/N) \leq n_p(G)$$

Proof

We show, for any $P \in Syl_p(G)$, that PN/N is a Sylow p-subgroup of G/N, and that every Sylow p-subgroup of G/N arises in this way.

Let $P \in Syl_p(G)$. The subgroup PN/N is a p-subgroup, since $PN/N \cong P/(P \cap N)$. Now we have the inclusions

$$N \subseteq PN \subseteq G,\ P \subseteq PN \subseteq G$$

and the first of these show that $[G/N : PN/N] = [G : PN]$ and the second shows that $[G : PN] \neq 0 \bmod p$; therefore PN/N is a Sylow p-subgroup of G/N.

Next we show that every Sylow p-subgroup of G/N has the form PN/N for some Sylow p-subgroup P of G. Let $Q \in Syl_p(G/N)$ and write $Q = H/N$ for some subgroup $H < G$ containing N. Then

$$[G : H] = [G/N : Q] \neq 0 \bmod p$$

Choose $P \in Syl_p(H)$ so that $P \in Syl_p(G)$, which follows from the above congruence and $[G : P] = [G : H][H : P]$. Then PN/N is a subgroup of Q; but we have just shown that it is also a Sylow p-subgroup of G/N, so $Q = PN/N$ as desired.

Application 9

Let G be a finite group and $H < G$. Show that $n_p(H) \leq n_p(G)$.

Proof

If Q, Q' are distinct Sylow p-subgroups of H, and they lie in a common Sylow p-subgroup P of G, then $\langle Q, Q' \rangle$ is a p-subgroup of H. But Q, Q' are distinct, so $\langle Q, Q' \rangle$ strictly contains Q (and Q'), whose order then exceeds that of Q (and Q'). In other words, any Sylow p-subgroup of G contains at most one Sylow p-subgroup of H, so the inequality follows.

Application 10

Let G be a finite group and H < G. For any $P \in Syl_p(G)$ there is a $g \in G$ such that $gPg^{-1} \cap H \in Syl_p(H)$.

Proof

Note that $P \cap H$ is p-subgroup of H, so there is a Sylow p-subgroup Q of H containing $P \cap H$. As Q is also a p-subgroup of G, it is contained in a Sylow p-subgroup of G, we have that $Q < gPg^{-1}$ for some g. Therefore

$$Q < gPg^{-1} \cap H$$

This intersection is a p-subgroup of H, so by maximality, it must be equal to Q.

Here is another proof: note that for any g, the subgroup $gPg^{-1} \cap H$ is a p-subgroup of G. To show that it is indeed a Sylow p-subgroup of H, it is enough to show that its index in H is not divisible by p. To do this, consider the action of H by left multiplication on G/P, the set of left cosets of P in G. Since $[G:P]$ is not divisible by p, there is some left coset gP who se H-orbit has size not divisible by p. But the s ize of this orbit is the index of the sta bilizer of gP in H:

$$Stab(gP) = \{h \in H : h(gP) = gP\} = \{h \in H : g^{-1}hg \in P\} =$$
$$= \{h \in H : h \in gPg^{-1}\} = gPg^{-1} \cap H$$

Application 11

S_5 contains no subgroup of order 30 or 40.

Proof

Let H be a subgroup of order 30, and consider the action of S_5 on the set of the left cosets of H; this gives rise to a permutation representation $\rho : S_5 \to S_4$ whose kernel is contained in H, i.e. $Ker\rho < H$. In particular, ρ is nontrivial, and since 120 does not divide 24, ρ cannot be injective. So either $Ker\rho = H$ in which case H is normal in S_5, or H contains a nontrivial normal subgroup, a contradiction, since the only proper nontrivial normal subgroup of S_5 is A_5.

Adapt this argument when K is a subgroup of order 40.

Application 12

No group of order 144 is simple.

Proof

Suppose G is a simple group of order 144. We have either $n_3 = 4$ or 16; if

$n_3 = 4$, then the normalizer of any Sylow 3-subgroup P has index 4 in G, so G contains a nontrivial normal subgroup contained in $N_G(P)$, and G cannot be simple, so we must have $n_3 = 16$.

If all the Sylow 3-subgroups have trivial intersection, then there are $8 \cdot 16 = 128$ elements of order a divisor of 9, so there are 16 remaining elements in G, and these elements constitute the unique Sylow 2-subgroup, which is normal in G.

If two (distinct) Sylow 3-subgroups P, Q intersect nontrivially, then $|P \cap G| = 3$. Consider the normalizer of $T := P \cap Q$; it contains both P and Q as normal subgroups, so PQ is a (normal) subgroup of $N_G(T)$ of order $|PQ| = |P| \cdot |Q| / |T|$. So $|N_G(T)|$ is at least 36, since it is a divisor of $|G|$, so the index of $N_G(T)$ in G is at most 4, in which case G must contain a nontrivial proper normal subgroup.

Application 13

There is no simple group of order 528.

Proof

If G is a simple group of order 528, we must have $n_{11} = 12$. Let P be a Sylow 11-subgroup, whose normalizer $N_G(P)$ has index 12 in G; by the embedding theorem, G is isomorphic to a subgroup of A_{12}.

Now P is cyclic of order 11, and $|N_G(P)/C_G(P)|$ divides $|Aut(P)| = 10$; and since $|N| = 44$ this forces $|C| = 22$ or 44. In either case, C contains an element x of order 2, and it commutes with a generator y of P, which has order 11, thus xy is an element of order 22. But A_{12} contains no element of order 22.

Application 14

Group of order 240 is simple.

Proof

Let G be a simple group of order 240. Notice that G cannot have

subgroups of index < 6; otherwise, G can be embedded in S_n for $n < 6$. If $n_5 = 6$, then G can be embedded in S_6 (to see this, let G act on the left cosets of the normalizer of any Sylow 5-subgroup). However, 240 does not divide $|A_6| = 360$, so $|A_6 \cap G| = 120$ (since any subgroup of S_n is either contained in A_n or else it has the same number of even and odd permutations), and A_6 has a subgroup of index 3. But A_6 is simple and cannot have a subgroup of any index n, whenever $|A_6|$ does not divide $n!$. Therefore, $n_5 = 16$. If $Q \in Syl_5(G)$, then $N := N_G(Q)$ has index 16, so $|N| = 15$. Up to isomorphism there is a unique cyclic group of order 15 and thus $N = Z(N)$. Since $Q < N = Z(N)$, then Q is an abelian Sylow subgroup of G which is contained in the centre of its normalizer. According to Burnside's Normal Complement Theorem, Q has a normal complement K, i.e. K is normal in G and $QK = G$. Hence, G cannot be simple.

Application 15

A group of order 255 is cyclic.

Proof

Let G be a group of order 255; then G has a unique Sylow 17-subgroup. Let Q be a Sylow 5-subgroup, and consider the subgroup PQ, of order $|PQ| = 85$. Now, PQ is normal in G since it has index 3, and 3 is the smallest prime dividing $|G|$. Also, PQ is cyclic, since it contains a unique Sylow 5- and 17-subgroup, and so $|Aut(PQ)| = \varphi(85)=64$. Next, consider the action of a Sylow 3-subgroup S on PQ by conjugation; this induces a homomorphism $\pi : S \to Aut(PQ)$, which then must be trivial. Since $S \cap PQ = \{1\}$, and $G = S(PQ)$ we have an isomorphism $G = S(PQ) \cong S \times PQ \cong Z/3 \times Z/85 \cong Z/255$, as desired.

3.3 Alternative applications

Consider, for a moment, a Rubik's cube. If we label each face of the cube Front, Back, Up, Down, Left and Right, and then let F, B, U, D, L and R denote the quarter-turn clockwise rotation of each respective face as we look directly at it, then the group $R = \langle F, B, U, D, L, R \rangle$ is the group of possible configurations of the smaller cubes which compose the Rubik's cube. We will call these smaller cubes "cubies." There are three different kinds of cubies: face cubies, which are in the center of each face of the Rubik's cube, and do not move relative to each other, corner cubies, which have three faces exposed and lie at the corners of the cube, and edge cubies, which have two faces exposed and lie between two corner cubies. There are 12 corner cubies, and each has 3 orientations; likewise there are 8 edge cubies, each with 2 orientations. It follows that the number of configurations of a Rubik's cube should be $12!8!2^{12}3^8$, but this is not the case. Instead, because certain parities must be maintained among cubies, only $1/12$ of the above configurations result in a solvable Rubik's cube. Thus there are $12!8!2^{10}3^7 = 43252003274489856000 = 2^{27}3^{14}5^3 7^2 11$ configurations possible, which is also the order of R.

According to Sylow's theorem, since the order of R is divisible by 11, and no higher power of 11, there exists at least one Sylow 11-subgroup of R. There are in fact many more Sylow 11-subgroups of R, but by Sylow's theorem we know that the number of them must be of the form $n_{11} = 1 + 11k, k \in Z^+$ such that n_{11} divides $2^{27}3^{14}5^3 7^2$. We can demonstrate that this must be the case simply by looking at a Rubik's cube itself. Imagine a Rubik's cube configuration where 11 of the twelve edge cubies have been cycled amongst each other, leaving the remaining cubies where they started. If we cycle the cubies in the same way 10 more times, the cube will return to its original configuration. An example of one such cycle is ruFBufDBUDbuRRdLLuLLdLLuRR, where lowercase letters denote

counter-clockwise rotations of their respective faces. The group generated by the above element has eleven elements, and is thus a Sylow 11-subgroup of R.

References

1. Israel Kleiner "A history of abstract algebra", Springer, 2007, 17-35

2. Morris Kline "Mathematical thought from ancient to modern times, Volume 3", Oxford University Press US, 1990, 1136-1158

3. G. A. Miller "A proof of Sylow's theorem"

4. M. Suzuki: Group Theory I, Springer-Verlag (Berlin, 1982) [English translation of Gunron, Iwanami Shoten (Tokyo, 1977)].

5. V. Pannone: A rounded proof of Sylow's Theorem, seminar notes typewritten by P. Santaniello (2000).

6. R. Gow, Sylow's proof of Sylow's theorem, Irish Math. Soc. Bull. (1994), 55–63.

7. W. C. Waterhouse, The early proofs of Sylow's theorem, Arch. Hist. Exact Sci. 21 (1979/80), 279–290.

8. J. Castillo, "The Smarandache Semigroup", International Conference on 9. Combinatorial Methods in Mathematics, II Meeting of the project "Algebra, Geometria e Combinatoria", Faculdade de Ciencias da Universidade do Porto, Portugal, 9-11 July 1998.

10. R. Padilla, "Smarandache Algebraic Structures", Smarandache Notions Journal, USA, Vol.9, No. 1-2, 36-38, (1998).

11. R. Padilla. "Smarandache Algebraic Structures", Bulletin of Pure and Applied Sciences, Delhi, Vol. 17 E, No. 1, 119-121, (1998);

12. F. Smarandache, "Special Algebraic Structures", in Collected Papers, Vol. III, Abaddaba, Oradea, 78-81, (2000).

13. Arithmetic and normal structure of finite groups by Helmut Wielandt and Bertram Huppert, Proc. Sympos. Pure Math.,
Vol. VI, Page 17–38 (Year 1962), MR 0147530

14. A brief history of the classification of the finite simple groups by Ronald M. Solomon, Bulletin of the American Mathematical Society, ISSN 10889485

(electronic), ISSN 02730979 (print), Volume 38, Page 315–352 (Year 2001): An expository paper by Ronald Mark Solomon describing the 110-year history of the classification of finite simple groups.

15. Finite Groups by Daniel Gorenstein, American Mathematical Society, ISBN–10 0821843427, ISBN–13 9780821843420

16. Solvability of groups of odd order by Walter Feit and John G. Thompson, Pacific Journal of Mathematics, Volume 13, Page 775–1029 (Year 1963), MR 0166261

17. Finite simple groups, edited by Graham Higman and Martin B. Powell, Academic Press, ISBN–10 0125638507, ISBN–13, 9780125638500

18. Introduction to fusion systems by Markus Linckelmann, URL http://web.mat.bham.ac.uk/C.W.Parker/Fusion/
fusion-intro.pdf