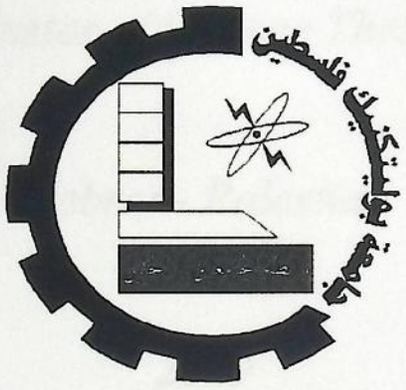
Palestine Polytechnic University

Deanship of Graduate Studies and Scientific Research

Master Program of Mathematics



Solvable and Nilpotent Groups

By

Abeer Roshdi Qunaibi

Master of Science Thesis

Hebron- Palestine

2009

Solvable and Nilpotent Groups

By

Abeer Roshdi Qunaibi

Master of Science Thesis

Hebron- Palestine

2009

Supervisor: Dr.Nureddin Rabie

A thesis submitted to the Department of Mathmatics at Palestine Polytechnic University as a partial fulfillment of the requirements for the degree of master of science.

The program of graduated studies / Department of Mathmatics

Deanship of the Graduate Studies

Solvable and Nilpotent Groups

By

Student Name: Abeer Roshdi Qunaibi

Supervisor : Dr.Nureddin Rabie

Master thesis submitted and accepted, Date: ----------.

The name and signatures of the examining committee members are as follows:

1. Dr. Nureddin Rabie.	*Head of committee Signature* ----------
2. Dr. Amjad Barham .	*Internal Examiner Signature* ----------
3. Dr. Ali Altawaiha.	*External Examiner Signature* ----------

Palestine Polytechnic University

2009

Declaration

I certify that this thesis, submitted for the degree of master, is the result of my own research except where otherwise acknowledged, and that this thesis (or any part of the same) has not been submitted for a higher degree to any other university or institution.

Signed:.....
Abeer Roshdi Qunaibi
Date:.....

Dedication

To my family.

To my mother and sisters.

To my husband "Ashraf".

To my kids Salsabeel, Batool, Hammam Habeballah & Abdullah.

To my father's and to my mother's- in -law souls.

Acknowledgment

I gratefully extend my thanks to those people who helped in completing this work , specially and personally to my supervisor , Dr. Nureddin Rabie for his help and advice throughout the period of study . And I would like to thank Dr. Ali Abd Al-Mohsen Altawaiha from Hebron University for his help. Also, I would like to thank all doctors in my faculty who helped me in completing this research.

Abstract

This thesis introduces the concepts of solvable and nilpotent groups and presents important definitions like supersolvable groups, polycyclic groups, Carter subgroups, metabelian groups ,hypercentral groups, HM-groups, and Chernicov groups. This thesis includes applications in Galois theory, and the solvability by radicals. Also, this research presents examples, propositions, and applications related to solvable and nilpotent groups.*

Finally, this thesis presents three applications of solvable and nilpotent groups, it discusses the solvability of Carter subgroups in the groups in which every element is conjugate to its inverse, proofs of interesting properties of metabelian groups, and this thesis study groups with many hypercentral subgroups.

Contents

Introduction

Algebra comes from Arabic word (al-jabr, الجبر); it means a branch of mathematics concerning the study of structure, relation, and quantity. Together with geometry, analysis, and number theory, algebra is one of the main branches of mathematics. In addition to working directly with numbers, algebra covers working with symbols, variables, and set elements. Addition and multiplication are viewed as general operations, and their precise definitions lead to structures such as groups, rings and fields.

This thesis consists of four chapters:

In **chapter 1** we present a short summary of notions and notations for groups that are used in this research. A discussion of mathematical definitions is also included.

In **chapter 2** we present a history of solvable groups which was introduced by Galois. We include important definitions, propositions, properties, and examples that help every one in studying the concept of solvable groups. Also, we present important definitions like (supersolvable & polycyclic groups) that are related to solvability of groups.

In **chapter 3** we define nilpotent groups. In addition, this chapter includes great theorems and their proofs about nilpotent groups, finally we study a great relation between solvable and nilpotent groups.

In **chapter 4** we study very important theorems and their proofs from different papers for solvable and nilpotent groups .The first one is about the solvability of Carter subgroups in the groups in which every element is conjugate to its inverse, the second is about interesting properties of metabelian groups, and the third is about groups with many hypercentral subgroups.

Chapter (1)

In the beginning, before Galois, a group meant a collection of permutations, and group multiplication was the composition of permutations. The abstract notion of group, as a set in its own right, did not exist .Galois first identified the abstract notion of groups. Although Galois did not clarify his abstractions, subsequent work by others led to notions (such as, solvable group, normal subgroups) that would have been difficult to develop by viewing a group as a collection of permutations.

The term group dates back to the early nineteenth century. It comes from the earlier phrase group of transformations which was how groups were perceived.

This abstraction of the group concept proved to be very helpful when there was a general switch from permutation representations to linear representations (where a linear representation of G is any homomorphisim from G into GL (V)).

1.1Groups

Definition 1.1.1 (Group)

A group is a nonempty set G with a binary operation * (termed the multiplication or product) such that the following hold:

- For any a, b, c in G, $a * (b * c) = (a * b) * c$. This property is termed associativity.
- There exists an element e in G such that $a * e = e * a = a$ for all a in G. Such an e is termed an identity element for G.
- For any a in G, there is an element b such that $a * b = b * a = e$. Such a (b) is termed an inverse of a and is denoted as a^{-1}.

From the above definition, we can prove that there is only one identity element, and that the inverse is unique.

Example1.1.2

Number systems provide several examples of groups. (Z, +),(Q, +), (R,+), and (C, +) all are groups. But (N, +) is not a group, and Z, Q ,R, C are not groups under multiplication,

since their element 0 has no inverse. However, nonzero rational numbers, nonzero real numbers, nonzero complex numbers, all constitute groups under multiplication; so do positive rational numbers, positive real numbers, and complex numbers with absolute value 1. The set of all $n \times n$ matrices (with entries in R, or in any given field) is a group under addition, but not under multiplication; however, invertible $n \times n$ matrices constitute a group under multiplication. So do, more generally, invertible linear transformations of a vector space into itself.

Now let us give a precise definition of the term abelian group that comes from Niels Henrick Abel, a mathematician who worked with groups even before the formal theory [an axiomatic system] was laid down, in order to prove unsolvability of the quintic [a polynomial of degree 5].

Definition 1.1.3 (Abelian group)

An Abelian group is a group where any two elements commute. In other words, a group G is said to be Abelian if for any elements a and b in G, $ab = ba$ (here ab denotes the product of a and b in G). Also we can easily show that the following are true.

- A group is abelian if its center is the whole group.

An element of a group is termed central if it commutes with every element of the group.

Definition 1.1.4 (cyclic group)

A group G is cyclic if G can be generated by a single element, i.e., there is some element $g \in G$ such that

$$G = \{ g^n \mid n \text{ is an integer}\}$$

(where as usual the operation is multiplication).

In additive notation G is cyclic if $G = \{ng \mid n \text{ is an integer}\}$

In both cases we shall write $G = \langle g \rangle$, and say G generated by g.

A cyclic group may have more than one generator. Also by the laws for exponents cyclic groups are abelian group.

Proposition 1.1.5

Every group of prime order is cyclic.

Definition 1.1.6 (Subgroup)

Given a group G under a binary operation *, we say that some subset A of G is a subgroup of G if A also forms a group under the operation *. This is usually represented notationally by $A \leq G$, read as (A is a subgroup of G).

Also, the intersection of subgroups A and B is again a subgroup .But the union of subgroups A and B is a subgroup if and only if either A or B contains the other.

Definition 1.1.7 (proper Subgroup)

A proper subgroup of a group G is a subgroup A which is a proper subset of G (i.e. $A \neq G$). The trivial subgroup of any group is the subgroup {e} consisting of just the identity element. If A is a subgroup of G, then G is sometimes called an overgroup of A.

Example 1.1.8

(Z, +) is a subgroup of (Q, +) ; (Q, +) is a subgroup of (R, +) ; (R, +) is a subgroup of (C, +). On the other hand, (N, +) is not a subgroup of (Z, +) (even though N is closed under addition).

Definition 1.1.9 (normal subgroup)

A subgroup N of a group G is called a normal subgroup if for each element, n in N and each g in G, the element gng^{-1} is still in N. We write

$$N \lhd G \Leftrightarrow \forall n \in N, \forall g \in G, gng^{-1} \in N$$

Definition 1.1.10 (quotient group)

Let N be a normal subgroup of a group G. We define the set G/N to be the set of all left cosets of N in G, i.e., G/N = {aN: a in G}. The group operation on G/N is the product of cosets where, for each aN and bN in G/N, the product of aN and bN is

$$(aN)(bN) = (ab)N.$$

The normality of N is used in this equation. Because of the normality of N, each left coset is itself a right coset, and so G/N could be defined as the set of right cosets of N in G.

Note: Index of N in G denoted by

$$[G:N] = |G/N| = \frac{|G|}{|N|} \text{ If G is finite.}$$

Definition 1.1.11 (simple group)

A simple group is a group which is not the trivial group and whose only normal subgroups are the trivial group and the group itself.

Example 1.1.12

The cyclic group G = **Z**/3**Z** of congruence classes modulo 3 is simple. If H is a subgroup of this group, its order (the number of elements) must be a divisor of the order of G which is 3. Since 3 is prime, its only divisors are 1 and 3, so either H is *G*, or H is the trivial group. On the other hand, the group G = **Z**/12**Z** is not simple. Because the set H of congruence classes of 0, 4, and 8 modulo 12 is a subgroup of order 3, and it is a normal subgroup since any subgroup of an abelian group is normal. Similarly, the additive group **Z** of integers is not simple; the set of even integers is a non-trivial proper normal subgroup.

Definition 1.1.13 (The commutator of two elements)

The commutator of two elements, x and y, of a group G , is the element

$$[x, y] = xy\,x^{-1}y^{-1}.$$

Definition 1.1.14 (commutator subgroup)

The commutator subgroup or derived subgroup of a group is the subgroup generated by all its commutators, or elements of the form $[x , y] = x\,y\,x^{-1}y^{-1}$.

Now in abstract algebra , the commutator subgroup is important because it is the smallest normal subgroup such that the quotient group of the original group by this subgroup is abelian .Also a group G is an abelian group if and only if the derived group is trivial: $[G,G] = \{e\}$. Note that one must consider the subgroup generated by the set of commutators because in general the set of commutators is not closed under the group operation. Commutators are used to define nilpotent and solvable groups. The commutator subgroup $[G,G]$ (also called the derived subgroup), is denoted by G' or $G^{(1)}$.

Example1.1.15

- The commutator subgroup of the Alternating group A_4 is the Klien four group (which is isomorphic to the direct product $\mathbb{Z}_2 \times \mathbb{Z}_2$).
- The commutator subgroup of the symmetric group S_n is the alternating group A_n.

Definition 1.1.16(commutator series)

The commutator series is the smallest descending sequence of subgroups of a group G with abelian factors.

$$G = G^0 \supseteq G' \supseteq G'' \supseteq \dots$$

For example: $S_3 \supseteq A_3 \supseteq \{e\}$ is a commutator series of a group G.

Definition 1.1.17 (Homomorphisms)

Homomorphisms of groups are mappings that preserve products. They allow different groups to relate to each other. A homomorphism of a group A into a group B (written multiplicatively) is a mapping ϕ of A into B such that:

$$\phi\ (x\ y) = \phi\ (x)\ \phi\ (y)$$

for all x, $y \in A$. If A is written additively, then $\phi\ (x\ y)$ becomes $\phi\ (x + y)$; if B is written additively, then $\phi\ (x)\ \phi\ (y)$ becomes $\phi\ (x) + \phi\ (y)$.

Example 1.1.18

Given an element a of a group G, the power map $n \to a^n$ is a homomorphism of Z into G. The natural alogarithm function is a homomorphism of the multiplicative group of all positive reals into (R, +). If H is a subgroup of a group G, then the inclusion mapping $\iota : H \to G$, defined by $\iota\ (x) = x$ for all $x \in H$, is the inclusion homomorphism of H into G.

Definition 1.1.19 (Isomorphism):

Given two groups (G, *) and (H ,$\odot$), a group isomorphism from (G, *) to (H ,$\odot$) is a bijective group homomorphisim from G to H.

This means that a group isomorphism is a bijective function $f : G \to H$ such that for all u and v in G we have:

$$f(u * v) = f(u) \odot f(v).$$

The two groups (G, *) and (H , $\odot$) are isomorphic if an isomorphism exists between them.

In such a case we write: $G \cong H$

Example 1.1.20

The group of all real numbers with addition, (R ,+), is isomorphic to the group of all positive real numbers with multiplication (R^+, •):

$$(R,+) \cong (R^+,\bullet)$$

By $f(x) = e^x$.

Definition 1.1.21 (Automorphism)

An isomorphism from a group (*G*,*) to itself is called an automorphism of this group. Thus it is a bijection $f : G \to G$ such that:

$$f(u) * f(v) = f(u * v).$$

An automorphism always maps the identity to itself. The composition of two automorphisms is again an automorphism, and with this operation the set of all automorphisms of a group G, denoted by Aut(G), forms itself a group, the automorphism group of G.

Definition 1.1.22 (characteristic subgroup)

A characteristic subgroup of a group G is a subgroup H that is invariant under each automorphism φ of G. That is,

$$\varphi(H) = H$$

for every automorphism φ of G (where φ(H) denotes the image of H under φ).
The statement "H is a characteristic subgroup of G" is written

$$H \, char \, G$$

Notes:

1-Every subgroup of a cyclic group is characteristic subgroup.

2-Every characteristic subgroup of G is also a normal subgroup of G.

Since if G is a group, and g is a fixed element of G, then the conjugation map:

$x \mapsto gxg^{-1}$

is an automorphism of G (known as an inner automorphism). A subgroup of G that is invariant under all inner automorphisms is called normal. Since a characteristic subgroup is invariant under all automorphisms, every characteristic subgroup is normal.

Example 1.1.23

1- Every group is char as a subgroup of itself.

2- {e}char G. Since $\varphi(\{e\}) = \{e\}$.

Definition 1.1.24 (Fully characteristic subgroup)

A subgroup H of a group G is termed fully invariant or fully characteristic, if for any homomorphisim φ of G we have:

$$\varphi(H) \leq H$$

Every group G has itself and the trivial subgroup as two of its fully characteristic subgroups. Also, the commutator subgroup of a group is always a fully characteristic subgroup.

Definition 1.1.25 (normal series)

A normal series of a group G is a finite sequence $(G_0,\ldots,G_m)$ of normal subgroups of G such that

$$\{e\} = G_0 \lhd G_1 \lhd \ \ldots \lhd G_m = G$$

For example: $\{e\} \leq 8Z \leq 4Z \leq Z$ is a normal series of Z under addition.

Definition 1.1.26 (subnormal series)

A subnormal series is a subgroup series where each member of the series is normal in the next one containing it.

We have two kinds of subnormal series:

(1) A descending series:

$$G = A_0 \geq A_1 \geq \ldots \geq A_r$$

of subgroups of a group G is termed a subnormal series if A_{i+1} is a normal subgroup of A_i for $0 \leq i \leq r-1$

(2) An ascending series:

$$A_0 \leq A_1 \leq \ldots \leq A_r = G$$

of subgroups of a group G is termed a subnormal series if each A_i is a normal subgroup of A_{i+1}.

Every group G has a trivial normal series $\{e\} \lhd G$, where {e} is the trivial subgroup of G. While S_n has a nontrivial normal series $\{e\} \lhd A_n \lhd S_n$.

Note that the subnormal series must have its largest member equal to the whole group. Also for abelian groups the notations of subnormal and normal series concide, since every subgroup is normal. A normal series is always subnormal, but the converse need not be true. For example :

$\{\rho_0\} \leq \{\rho_0, \mu_1\} \leq \{\rho_0, \rho_2, \mu_1, \mu_2\} \leq D_4$ is a subnormal series of D_4 (the group of symmetries of the square). But $\{\rho_0\} \leq \{\rho_0, \mu_1\} \leq \{\rho_0, \rho_2, \mu_1, \mu_2\} \leq D_4$ is not normal in D_4 since $\{\rho_0, \mu_1\}$ is not normal in D_4.

Definition 1.1.27 (composition series)

A composition series of a group G is a subnormal series ,

$$\{e\} = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$$

Such that each factor H_{i+1}/H_i is simple, for all i, such that $0 \le i \le n-1$.

For example: $\{e\} \lhd A_n \lhd S_n$ for $n \ge 5$ is a composition series of S_n, since $A_n/\{e\}$ is isomorophic to A_n, which is simple for $n \ge 5$, and S_n/A_n is isomorophic to Z_2, which is simple.

Definition 1.1.28 (derived series)

The derived series of a group G is a sequence of subgroups such that:

$$G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \ldots$$

Where

$$G^{(0)} = G$$

$$G^{(n)} = \left[G^{(n-1)}, G^{(n-1)}\right], n \in N$$

The groups $G^{(2)}, G^{(3)}, \ldots$ are called the second derived subgroup, third derived subgroup, and so on.

For a finite group, the derived series terminates in a perfect group [a group G is perfect if G = G'], which may or may not be trivial. [19]

Definition 1.1.29 (characteristic series)

A subgroup series of a group is termed a characteristic series if all members of the series are characteristic subgroups of the whole group.

For example: $\{e\} \lhd 2Z \lhd Z$ is a characteristic series, since 2Z char Z.

Definition 1.1.30 (fully characteristic series)

A subgroup series of a group is termed a fully characteristic series if all members of the series are fully characteristic subgroups of the whole group.

Definition 1.1.31(center of a group)

The center of a group G is $Z(G) = \{ g \in G, \ gxg^{-1} = x \text{ for all } x \in G \}$.

Equivalently, $Z(G) = \{ g \in G, gx = xg \text{ for all } x \in G\}$.

Note: If G is abelian, then $Z(G) = G$.

For example, $Z(S_3) = \{\rho_0\}$, $Z(D_4) = \{\rho_0, \rho_2\}$, and $Z(Z_5) = Z_5$.

Proposition 1.1.32

Z(G) and all its subgroups are normal subgroups of G.

Definition 1.1.33 (The centralizer in G)

The centralizer in G of an element x of a group G is $C_G(x) = \{ g \in G, \ gxg^{-1} = x \}$.

Equivalently, $C_G(x) = \{ g \in G, \ gx = xg \}$.

Definition 1.1.34 (The normalizer of subgroup S in G)

The normalizer of subgroup S in a group G is defined as $N_G(S) = \{x \in G: xS = Sx\}$.

Note: $N_G(S)$ can easily be seen to be a subgroup of G.

A subgroup H of a group G is called a **self-normalizing subgroup** of G if $N_G(H) = H$.

Definition 1.1.35 (Central normal series).

A normal series $\{e\} = C_0 \lhd C_1 \lhd \ \ldots \lhd C_m = G$ is central, when $C_i \lhd G$ and $C_{i+1}/C_i \subseteq Z(G/C_i)$, for all $0 \leq i < m$.

Central normal series are also called just central series. A central normal series has abelian factors, but a normal series with abelian factors need not be central.

Definition 1.1.36 (finite p- group)

A finite group is a p-group, where p is a prime number, if and only if its order (the number of its elements) is a power of p.

Also, given a prime number p, a p-group (also p-primary group) is a group such that for each element g of the group there exists a nonnegative integer n such that g to the power p^n is equal to the identity element.

Definition 1.1.37 (sylow p- subgroup)

A Sylow p-subgroup (sometimes p-Sylow subgroup) of a group G is a maximal p-subgroup of G, i.e., a subgroup which is a p-group, and which is not a proper subgroup of any other p-subgroup of G. The set of all Sylow p-subgroups for a given prime p is sometimes written $\mathrm{Syl}_p(G)$.

The following theorems were first proposed and proven by Ludwig Sylow in 1872.

Theorem 1.1.38 (Sylow's first theorem)

For any prime factor p with multiplicity n of the order of a finite group G, there exists a Sylow p-subgroup of G, of order p^n.

The following weaker version of theorem 1.1.38 was first proved by Cauchy.

Corollary: Given a finite group G and a prime number p dividing the order of G, then there exists an element of order p in G.

Theorem 1.1.39 (Sylow's second theorem)

Given a finite group G and a prime number p, all Sylow p-subgroups of G are conjugate (and therefore isomorphic) to each other, i.e. if H and K are Sylow p-subgroups of G, then there exists an element g in G with $g^{-1}Hg = K$.

Theorem 1.1.40 (Sylow's third theorem)

Let p be a prime factor with multiplicity n of the order of a finite group G, so that the order of G can be written as $p^n \cdot m$, where $n > 0$ and p does not divide m. Let n_p be the number of Sylow p-subgroups of G. Then the following hold:

- n_p divides m, which is the index of the Sylow p-subgroup in G.
- $n_p \equiv 1 \bmod p$.
- $n_p = [G : N_G(P)]$, where P is any Sylow p-subgroup of G and $N_G(P)$ denotes the normalizer of P in G.

Definition 1.1.41 (Direct Products)

The direct product of two groups G_1 and G_2 is their Cartesian product $G_1 \times G_2$, also denoted by :

$G_1 \oplus G_2$, together with the componentwise operation : in the multiplicative notation,

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2).$$

1.2 Galois Group

First of all we have to define some notions and notations that are helpful in this section.

Definition 1.2.1 (field)

A field is a set together with two operations, usually called addition and multiplication, and denoted by + and ·, respectively, such that the following axioms hold:

Closure of F under addition and multiplication.

For all a, b in F, both $a + b$ and $a \cdot b$ are in F.

Associativity of addition and multiplication.

For all a, b, and c in F, the following equalities hold: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Commutativity of addition and multiplication:

For all a and b in F, the following equalities hold: $a + b = b + a$ and $a \cdot b = b \cdot a$.

Additive and multiplicative identity :

There exists an element of F, called the additive identity element, denoted by 0, such that for all a in F, $a + 0 = a$. Likewise, there is an element, called the multiplicative identity element, denoted by 1, such that for all a in F, $a \cdot 1 = a$. For technical reasons, the additive identity and the multiplicative identity are required to be distinct.

Additive and multiplicative inverses:

For every a in F, there exists an element $-a$ in F, such that $a + (-a) = 0$. Similarly, for any a in F other than 0, there exists an element a^{-1} in F, such that $a \cdot a^{-1} = 1$. (The elements $a + (-b)$ and $a \cdot b^{-1}$ are also denoted $a - b$ and a / b, respectively.)

Distributivity of multiplication over addition:

For all a , b and c in F, the following equality holds: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Definition 1.2.2 (extension field)

A field E is said to be an extension field (or field extension, or extension) of a field F, (written as E/F and read E over F), if F is a subfield of E.

For example, the complex numbers are an extension field of the real numbers, and the real numbers are an extension field of the rational numbers.

Definition 1.2.3 (Algebric field)

A field extension L/K is called algebraic if every element of L is algebraic over K, i.e. if every element of L is a root of some non-zero polynomial with coefficients in K.

Field extensions which are not algebraic, i.e. which contain transcendental elements, are called transcendental.

For example $\sqrt{2}$ is algebraic over $\mathbf{Q}$, since it is the root of the polynomial $g(x) = x^2 - 2$ whose coefficients are rational. Also π is transcendental over $\mathbf{Q}$ but algebraic over the field of real numbers $\mathbf{R}$: it is the root of $g(x) = x - \pi$, whose coefficients (1 and $-\pi$) are both real, but not of any polynomial with only rational coefficients.

Also, the field extension $\mathbf{R}/\mathbf{Q}$, that is the field of real numbers as an extension of the field of rational numbers, is transcendental, while the field extensions $\mathbf{C}/\mathbf{R}$ and $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ are algebraic, where $\mathbf{C}$ is the field of complex numbers and

$$\mathbf{Q}(\sqrt{2}) = \{q + t\sqrt{2} : q, t \in \mathbf{Q}\}.$$

Definition 1.2.4 (Splitting field)

The extension field E of a field F is called a splitting field for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in $E[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of E containing F.

For example, the field extension $\mathbf{Q}(\sqrt{3}i)/\mathbf{Q}$ is the splitting field for x^2+3 since it is the smallest field containing its roots, $\sqrt{3}i$ and $-\sqrt{3}i$. Note that it is also the splitting field for x^3+1. Where $\mathbf{Q}(\sqrt{3}i) = \{a+b\sqrt{3}i, a,b \in \mathbf{Q}\}$

Definition 1.2.5(Normal field)

An algebraic field extension E/F is said to be normal if E is the splitting field of a family of polynomials in F [X].

For example, $\mathbf{Q}(\sqrt{2})$ is a normal extension of $\mathbf{Q}$, since it is the splitting field of x^2-2. On the other hand, $\mathbf{Q}(\sqrt[3]{2})$ is not a normal extension of $\mathbf{Q}$ since the polynomial x^3-2 has one root in it (namely, $\sqrt[3]{2}$), but not all of them (it does not have the non-real cubic roots of 2).

Definition 1.2.6(separable field)

An algebraic field extension L/K is separable if it can be generated by adjoining to K a set each of whose elements is a root of a separable polynomial over K. (where a polynomial f(x) is seperable over K if and only if all its roots are distinct, for example the polynomial x^2-2 is seperable over $\mathbf{Q}$).

The condition of separability is central in Galois theory. A perfect field is one for which all algebraic extensions are separable. There exists a simple criterion for perfectness: a field F is perfect if F has characteristic 0, so inparticular the fields $\mathbf{R}$, $\mathbf{Q}$ and $\mathbf{C}$ are perfect.

In particular, all fields of characteristic 0 and all finite fields are perfect [13]. This means that the separability condition can be assumed in many contexts.

Now, we exhibit an example of a field that is not a perfect field.

Let $F = F_p(t)$, where F_p is the field with p elements and t transcendental over F_p. The splitting field E of the irreducible polynomial $[f(x) = x^p - t]$ is not separable over F. Indeed, if β is an element of E such that $\beta^p = t$, we have:

$$x^p - t = x^p - \beta^p = (x - \beta)^p$$

this shows that f has one root of multiplicity p.

Definition 1.2.7(Galois extension)

An algebraic field extension E/F is Galois if it is normal and separable.

Equivalently, the extension E/F is Galois if and only if it is algebraic, and the field fixed by the automorphism group Aut (E/F) is precisely the base field F.

Definition 1.2.8 (Galois Group)

Suppose that E is an extension of the field F. Consider the set of all automorphisms of E/F (that is isomorphisms α from E to itself such that $\alpha(x) = x$ for every x in F). This set of automorphisms with the operation of function composition forms a group, sometimes denoted by Aut(E/F).

If E/F is a Galois extension, then Aut(E/F) is called the Galois group of (the extension) E over F, and is usually denoted by Gal(E/F).

Example 1.2.9

Gal(F/F) is the trivial group that has a single element, namely the identity automorphism, since the identity automorophisim is the only automorphisim that fix F.

Example 1.2.10

Gal($\mathbf{Q}(\sqrt{2})/\mathbf{Q}$) has two elements, the identity automorphism and the automorphism which exchanges $\sqrt{2}$ and $-\sqrt{2}$.

Galois theory 1.2.11 [11, 13]

In mathematics, more specifically in abstract algebra, Galois theory, named after Évariste Galois, provides a connection between field theory and group theory. Using Galois theory, certain problems in field theory can be reduced to group theory, which is in some sense simpler and better understood.

Originally Galois used permutation groups to describe how the various roots of a given polynomial equation are related to each other. The modern approach to Galois theory, developed by Richard Dedekind, Leopold Kronecker and Emil Artin, among others, involves studying automorphisms of field extensions. The birth of Galois theory was originally motivated by the following question, whose answer is known as the Abel-Ruffini theorem.

> "Why is there no formula for the roots of a fifth (or higher) degree polynomial equation in terms of the coefficients of the polynomial, using only the usual

Definition 1.2.8 (Galois Group)

Suppose that E is an extension of the field F. Consider the set of all automorphisms of E/F (that is isomorphisms α from E to itself such that $\alpha(x) = x$ for every x in F). This set of automorphisms with the operation of function composition forms a group, sometimes denoted by Aut(E/F).

If E/F is a Galois extension, then Aut(E/F) is called the Galois group of (the extension) E over F, and is usually denoted by Gal(E/F).

Example 1.2.9

Gal(F/F) is the trivial group that has a single element, namely the identity automorphism, since the identity automorophisim is the only automorphisim that fix F.

Example 1.2.10

Gal($\mathbf{Q}(\sqrt{2})/\mathbf{Q}$) has two elements, the identity automorphism and the automorphism which exchanges $\sqrt{2}$ and $-\sqrt{2}$.

Galois theory 1.2.11 [11, 13]

In mathematics, more specifically in abstract algebra, Galois theory, named after Évariste Galois, provides a connection between field theory and group theory. Using Galois theory, certain problems in field theory can be reduced to group theory, which is in some sense simpler and better understood.

Originally Galois used permutation groups to describe how the various roots of a given polynomial equation are related to each other. The modern approach to Galois theory, developed by Richard Dedekind, Leopold Kronecker and Emil Artin, among others, involves studying automorphisms of field extensions. The birth of Galois theory was originally motivated by the following question, whose answer is known as the Abel-Ruffini theorem.

> "Why is there no formula for the roots of a fifth (or higher) degree polynomial equation in terms of the coefficients of the polynomial, using only the usual

algebraic operations (addition, subtraction, multiplication, division) and application of radicals (square roots, cube roots, etc)?" [41]

Galois theory not only provides a beautiful answer to this question, it also explains in details why it is possible to solve equations of degree four or lower in the above manner, and why their solutions take the form that they do. Further, it gives a conceptually clear, and often practical, means of telling when some particular equation of higher degree can be solved in that manner.

While Ruffini and Abel established that the general quintic could not be solved, some particular quintics can be solved, such as $(x - 1)^5$, and the precise criterion by which a given quintic or higher polynomial could be determined to be solvable or not was given by Évariste Galois, who showed that whether a polynomial was solvable or not was equivalent to whether or not the permutation group of its roots – in modern terms, its Galois group – had a certain structure – in modern terms, whether or not it was a solvable group. This group was always solvable for polynomials of degree four or less, but not always so for polynomials of degree five and greater, which explains why there is no general solution in higher degree.[40]

algebraic operations (addition, subtraction, multiplication, division) and application of radicals (square roots, cube roots, etc)?" [41]

Galois theory not only provides a beautiful answer to this question, it also explains in details why it is possible to solve equations of degree four or lower in the above manner, and why their solutions take the form that they do. Further, it gives a conceptually clear, and often practical, means of telling when some particular equation of higher degree can be solved in that manner.

While Ruffini and Abel established that the general quintic could not be solved, some particular quintics can be solved, such as $(x - 1)^5$, and the precise criterion by which a given quintic or higher polynomial could be determined to be solvable or not was given by Évariste Galois, who showed that whether a polynomial was solvable or not was equivalent to whether or not the permutation group of its roots – in modern terms, its Galois group – had a certain structure – in modern terms, whether or not it was a solvable group. This group was always solvable for polynomials of degree four or less, but not always so for polynomials of degree five and greater, which explains why there is no general solution in higher degree.[40]

Chapter Two

Solvable Groups

Introduction

This term of solvable group was introduced by Galois. The notion of solvable group arose from the attempt to characterize the Galois groups of those field extensions which could be solved by radicals (which essentially means there is an algebric formula for the roots). [see page 35].

Also, in the history of mathematics, the origins of group theory lie in the search for a proof of the general unsolvability of quintic and higher equations, finally realized by Galois theory. The concept of solvable (or soluble) groups arose to describe a property shared by the automorphism groups of those polynomials whose roots can be expressed using only radicals (square roots, cube roots, etc., and their sums and products).

2.1 solvable groups

A solvable group is a group with a normal series whose factors are abelian. So, solvable groups are a large class of groups with remarkable properties.

Definition 2.1.1 (solvable group)

A group G is called solvable if it has a normal series whose factor groups are all abelian, that is, if there are subgroups

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_k = G$$

Such that G_j is normal in G, and G_j / G_{j-1} is an abelian group, for $j = 1, 2, \ldots, k$ .And {e} is the trivial subgroup. [10]

Proposition 2.1.2

G' is a normal subgroup of G; in fact, G' is the smallest normal subgroup of G such that G/ G' is abelian.

Proof:

The inverse of a commutator $xyx^{-1}y^{-1}$ is a commutator, and a conjugate of a commutator is again a commutator:

$$a\ xyx^{-1}y^{-1}\ a^{-1} = axa^{-1}\ aya^{-1}\ (axa^{-1})^{-1}\ (aya^{-1})^{-1}.$$

Hence every $x \in G'$ is a product of commutators $x = c_1 c_2 \ldots c_n$, and then

$$axa^{-1} = ac_1\ a^{-1}\ ac_2\ a^{-1} \ldots a\ c_n\ a^{-1} \in G' \text{ for all } a \in G.$$

Thus $G' \triangleleft G$.

Next, $xyx^{-1}\ y^{-1} \in G'$ for all $x, y \in G$; hence $G'xy = G'yx$ and G/G' is abelian.

Conversely, if $N \triangleleft G$ and G/N is abelian, then $Nxy = Nyx$ and $xyx^{-1}y^{-1} \in N$ for all $x, y \in G$, and $G' \subseteq N$.

Definition 2.1.3. (Commutator series)

The commutator series of a group G is the sequence

$$G \rhd G' \rhd G'' \rhd \ldots \rhd G^{(k)} \rhd G^{(k+1)} \rhd \ldots$$

The group $G^{(k)}$ is the kth derived group of G; it is normal in $G^{(k-1)}$ by proposition 2.1.2. The commutator series is not a normal series, but it becomes one if some $G^{(r)} = \{e\}$ and the tail $G^{(r+1)} \rhd \ldots$ is chopped off. [23]

Definition 2.1.4 (solvable length)

Given a solvable group G, we define its solvable length or derived length as follows: it is the length of the derived series of the group G.

Note here that by length of the series, we mean the number of successive inclusions, so the length is one less than the actual number of subgroups in the derived series. The least n such that $G^{(n)} = \{e\}$ is called the derived length of the solvable group G.

For finite groups, an equivalent definition to solvable group is that a solvable group is a group with a composition series whose factors are all cyclic groups of prime order. This equivalent because a finite abelian group has finite composition length and every finite simple abelian group is cyclic of prime order. The **Jordan-Hölder theorem** states that if one composition series has this property, then all composition series will have this

property as well. For the Galois group of a polynomial, these cyclic groups correspond to *n*th roots (radicals) over some field. "The equivalence does not necessarily hold for infinite groups: for example, since every nontrivial subgroup of the group **Z** of integers under addition is isomorphic to **Z** itself, it has no composition series, but the normal series {0,**Z**}, with its only factor group isomorphic to **Z**, proves that it is in fact solvable".[32]

Solvable groups are often useful for reducing a conjecture about a complicated group into a conjecture about a series of groups with simple structure: abelian groups (and in the finite case, cyclic groups of prime order).

Definition 2.1.5(metabelian group)

A metabelian group is a group whose commutator subgroup is abelian.

Equivalently, a group G is metabelian if and only if there is an abelian normal subgroup K such that the quotient group G/K is abelian. So, all abelian groups are metabelian.

Solvable groups are sometimes called metabelian. In fact, metabelian groups are precisely the solvable groups of derived length at most 2 . But solvable groups need not be abelian . [28]

Properties of metabelian group :

1- Any subgroup of a metabelian group is metabelian. This follows from the general fact that the derived series of the subgroup is contained in the derived series of the whole group.

2- Any quotient group of a metabelian group is metabelian. This follows from the fact that the derived series of the quotient is the quotient of the derived series of the original group.

3- A direct product of metabelian groups is metabelian. This follows from the fact that the derived series of the direct product is the direct product of the respective derived series.

Abelian groups are solvable; on the other hand, nonabelian simple groups aren't solvable, since the single factor in their one normal series is not abelian; thus, A_n (if $n \geq 5$) and the simple groups are not solvable. The first major step of the Classification theorem, **"the Feit and Thompson theorem [1963], states that all nonabelian finite simple groups have even orders; equivalently, every group of odd order is solvable".** [12]

Proposition 2.1.6.

A group G is solvable if and only if $G^{(r)} = \{e\}$ for some $r \geq 0$.

Proof:

If $G^{(r)} = \{e\}$, then $\{e\} = G^{(r)} \lhd G^{(r-1)} \lhd \ldots \lhd G' \lhd G$ is a normal series whose factors are abelian, by proposition 2.1.2.

Conversely, assume that G has a normal series $\{e\} = A_0 \lhd A_1 \lhd \ldots \lhd A_m = G$ whose factors A_i / A_{i-1} are all abelian.

Then G/A_{m-1} is abelian; by proposition 2.1.2, $G' \subseteq A_{m-1}$.

In general, A_{m-k} / A_{m-k-1} is abelian, so $G^{(k)} \subseteq A_{m-k}$ implies $G^{(k+1)} \subseteq A'_{m-k} \subseteq A_{m-k-1}$ by proposition 2.1.2.

Induction then yields $G^{(k)} \subseteq A_{m-k}$ for all $k \leq m$, in particular $G^{(m)} = \{e\}$.

Proposition 2.1.6 is often used as a definition of solvable groups.

Proposition 2.1.7. [10]

Let $\varphi : G \to H$ be a surjective homomorphisim .Then $\varphi(G^{(n)}) = H^{(n)}$ for every $n \geq 0$.

Proof:

We have $\varphi([x, y]) = [\varphi(x), \varphi(y)]$, and since $\varphi(G) = H$, we see that φ maps the set of commutators in G onto those in H.

It follows that $\varphi(G') = H'$, and repeated application of this argument yields that $\varphi(G^{(n)}) = H^{(n)}$, as required.

Proposition 2.1.8.

If G is solvable, and there is a homomorphism from G onto H, then H is solvable

Proof:

Assume that G is solvable, and there is a homomorphisim φ from G onto H.

Then, $\varphi(G^{(n)}) = H^{(n)}$ [by Proposition 2.1.7.].

Also, $H^{(n)} = \{e\}$ [since G is solvable and φ is a homomorphisim map]

Therefore, H is solvable. [by Proposition 2.1.6.]

Proposition 2.1.9.

Every subgroup of a solvable group is solvable.

Proof:

Let A be a subgroup of G .Then $A \subseteq G$ implies that $A' \subseteq G'$ and in general $A^{(k)} \subseteq G^{(k)}$

Now if G is solvable, then for some n we have $A^{(n)} \subseteq G^{(n)} = \{e\}$ and so A is solvable.

Proposition 2.1.10.

Every quotient group of a solvable group is solvable.

Proof:

Let N $\lhd$ G, then by using the canonical homomorphisim $\varphi : G \to G/N$ we have, $(G/N)^{(k)} = \varphi(G^{(k)})$, and so if $G^{(r)} = \{e\}$, we have $(G/N)^{(r)} = \{e\}$.

Proposition 2.1.11. [10]

If $N \lhd G$ and G/N are solvable, then G is solvable.

Proof:

To see this let $\bar{G}$ =G/N, and let $\{e\} = N_0 \lhd N_1 \lhd \ldots \lhd N_n = N$ be a chain of subgroups of N such that N_{i+1}/N_i is abelian for all $0 \le i < n$.

And let $\overline{\{e\}} = \bar{G} \lhd \overline{G_1} \lhd \ldots \lhd \overline{G_m} = \bar{G}$ be a chain of subgroups of $\bar{G}$ such that $\overline{G_{i+1}}/\overline{G_i}$ is abelian for all $0 \le i < m$.

Then there are subgroups G_i of G with N $\le G_i$ such that $G_i/N = \overline{G_i}$ and $G_i \lhd G_{i+1}$, $0 \le i < m$ (by lattice isomorphism theorem [10]).

Now by the third isomorphism theorem

$$\overline{G_{i+1}}/\overline{G_i} = (G_{i+1}/N)/(G_i/N) \cong G_{i+1}/G_i .$$

Thus

$\{e\} = N_0 \lhd N_1 \lhd \ldots \lhd N_n = N = G_0 \lhd G_1 \lhd \ldots \lhd G_m = G$ is a chain of subgroups of G all of whose successive quotient groups are abelian . Therefore G is solvable.

Proposition 2.1.12

Every finite p-group is solvable.

Proof.

That a group G of order p^k is solvable is proved by induction on k.

1st Step. For $k = 1$ our group is a cyclic group of prime order thus it is solvable by definition of solvable group.

2nd step. Let the statement hold for all $n \leq k$.

3d Step. We will prove that it holds for $k = n + 1$. Now since G is a p-group $Z(G) \neq \{e\}$. Also $Z(G)$ is a normal subgroup of G and $Z(G)$ is abelian. Thus $Z(G)$ is solvable. Now $G/Z(G)$ is again a p-group or trivial.

If it is trivial then $G = Z(G)$ thus G is abelian hence it is solvable.

If it is not trivial then $|G/Z(G)| \leq p^k$,so by the inductive step it is solvable.

Therefore by theorem 2.1.11 G is also solvable and we are done.

Proposition 2.1.13 [17]

Every group of order $p^n q$ (where p and q are primes) is solvable.

Proof:

We may assume that $p \neq q$. The proof is by induction on n.

Let S be a Sylow p-subgroup of G. If $S \lhd G$, then G/S is cyclic, since $|G/S| = q$ is prime, S is solvable by proposition 2.1.12 and G is solvable by proposition 2.1.11.

Now assume that S is not normal. Then $S \subseteq N_G(S) \subsetneq G$; since $[G : S] = q$ is prime ,this implies $N_G(S) = S$, and S has $[G : N_G(S)] = q$ conjugates. Thus there are q Sylow p-subgroups.

If the q Sylow p-subgroups of G are pairwise disjoint ($S \cap T = \{e\}$ when $S \neq T$), then G has $q (p^n - 1)$ elements whose order is a positive power of p , leaving at most q elements whose order is a power of q .

Therefore G has only one Sylow q -subgroup Q, and $Q \lhd G$. Then Q is cyclic, G/Q is solvable by proposition 2.1.12 and G is solvable by proposition 2.1.11.

In particular, proposition 2.1.13 holds when n= 1.

Now assume that the q Sylow p-subgroups of G are not pairwise disjoint.

Then there are Sylow p-subgroups S and T such that $S \cap T \neq \{e\}$, and one can choose S and T so that $M = S \cap T$ has the greatest possible number of elements.

By Lemma 2.1.14 below $H = N_G(M)$ has more than one Sylow p-subgroup; M is the intersection of all the Sylow p-subgroups of H; and every Sylow p-subgroup of H is contained in a unique Sylow p-subgroup of G. Now, the number of Sylow p-subgroups of H divides p^nq but is not divisible by p; hence H has q Sylow p-subgroups.

Since G also has q Sylow p-subgroups, M is contained in every Sylow p-subgroup of G.

Therefore M is the intersection of all the Sylow p-subgroups of G. Since the latter are all conjugate, this implies that $M \lhd G$.

Now, $|M| = p^k$, where $1 \leq k < n$.

Hence G/M is solvable, by the induction hypothesis; *M* is solvable by proposition 2.1.12; and *G* is solvable, by proposition 2.1.11.

Lemma 2.1.14.

Let M be the intersection of two distinct Sylow p - subgroups of a group G. If M has the greatest possible number of elements, then $H = N_G(M)$ has more than one sylow p-subgroup; M is the intersection of all the Sylow p-subgroups of H ; and every sylow p-subgroup of H is contained in a unique Sylow p-subgroup of G.

Proof:

We have $M \lhd S$ for some Sylow p-subgroup S of G.

Now $M \not\subset N_S(M) = H \cap S$. As, $N_S(M) \subseteq S$ is a p -subgroup of H and is contained in a Sylow p-subgroup P of H , which is in turn contained in a Sylow p-subgroup T of G, then $M \not\subset N_S(M) \subseteq S \cap T$ and $S = T$ by the choice of M.

Hence $P \subseteq H \cap S = N_S(M)$ and $N_S(M) = P$ is a Sylow p-subgroup of H.

Since $M \lhd N_G(M) = H$, M is contained in every conjugate of P and is contained in every Sylow p-subgroup of H.

We also have $M = S \cap T$ for some Sylow p-subgroups $S \neq T$ of G.

Then $M \subseteq N_S(M) \cap N_T(M) \subseteq S \cap T$ and $M = N_S(M) \cap N_T(M)$.

Then $N_S(M) \neq N_T(M)$, since $M \not\subset N_S(M), N_T(M)$.

By the above, applied to S and to T, M is the intersection of two distinct Sylow p-subgroups of H.

Therefore H has more than one Sylow p-subgroup, and M is the intersection of all the Sylow p-subgroups of H.

Finally, let P be any Sylow p-subgroup of H .(Since in a finite group, every p-subgroup is contained in a Sylow p-subgroup) then, P is contained in a Sylow p-subgroup S of G, but P is not contained in two distinct Sylow p-subgroups S and T of G. Otherwise, $M \not\subset P \subseteq S \cap T$ contradicts the choice of M.

The Hall Theorems... [17]

The three theorems below, due to Hall [1928], are stronger versions of the Sylow theorems that hold in solvable groups. First we prove a lemma.

Lemma 2.1.15

Every nontrivial finite solvable group contains a nontrivial abelian normal p-subgroup for some prime p.

Proof:

Let G be a finite solvable group.

There is a smallest integer $r > 0$ such that $G^{(r)} = \{e\}$.

Then $A = G^{(r-1)}$ is a nontrivial abelian normal subgroup of G.

Some prime p divides $|A| > 1$, let N be the set of all elements of A whose order is a power of p. Then $N \neq \{e\}$, $N \leq A$, and N is a p-group.

If $x \in N$ and $g \in G$, then $gxg^{-1} \in A$ and the order of gxg^{-1} is a power of p, so that $gxg^{-1} \in N$; thus $N \lhd G$.

The proof of the first theorem also uses **Schur's theorem** which states that" If m and n are relatively prime, then a group of order mn that contains an abelian normal subgroup of order n also contains a subgroup of order m". [17, page 102]

Theorem 2.1.16.

Let m and n be relatively prime. Every solvable group of order mn contains a subgroup of order m.

Proof:

Let G be solvable of order mn. If m is a power of a prime, then theorem 2.1.16 follows from the first Sylow theorem.

Otherwise, we proceed by induction on |G|.

By lemma 2.1.15, G contains a nontrivial abelian normal subgroup N of order $p^k > 1$ for some prime p.

Now, p^k divides |G| = mn; since m and n are relatively prime, either p^k divides m, or p^k divides n.

If p^k divides m, then $|G/N| = (m/p^k)\, n$, where m/p^k and n are relatively prime and $|G/N| < |G|$.

By the induction hypothesis, G/N has a subgroup H/N of order m/p^k, where $N \subseteq H \leq G$; then |H| = m.

If p^k divides n, then $|G/N| = (n/p^k)m$, where n/p^k and m are relatively prime and $|G / N| < |G|$. By the induction hypothesis, G/N has a subgroup H/N of order m, where $N \subseteq H \leq G$.

Then $|H| = m\, p^k$.

Now, $N \lhd H$, N is abelian, and N has order p^k, which is relatively prime to m; by Schur's theorem , H has a subgroup of order m, and then so does G.

The subgroups of G of order m are the Hall subgroups of G. [Hall subgroup of G is subgroup with order and index are relatively prime].

Lemma 2.1.17

Let m and n be relatively prime and let G be a group of order mn with an abelian normal subgroup of order n. Then all subgroups of G of order m are conjugate.

Proof:

Let $|G| = mn$ and let $N \lhd G$, with $|N| = n$ and N abelian.

Let A and B be subgroups of G of order m. Since m and n are relatively prime we have

$$A \cap N = B \cap N = \{e\};$$

Hence

$$AN = BN = G.$$

Therefore

Every coset of N intersects A in exactly one element, and similarly for B. The element of $Nx \cap B$ can then be written as:

$$u_x x \text{ for some unique } u_x \in N.$$

Then

$$u_a(au_b a^{-1})ab = (u_a a)(u_b b) \in B \text{ , for all a, b} \in A$$

And

$$u_{ab} = u_a a u_b a^{-1}$$

Let,

$$v = \prod_{b \in A} u_b \in N .$$

Since N is abelian,

$$v = \prod_{b \in A} u_{ab} = \prod_{b \in A} (u_a a u_b a^{-1}) = u_a^m ava^{-1}.$$

For all $a \in A$.

We also have $u_a^n = 1$, since $|N| = n$.

Now, $qm + r n = 1$ for some $q, r \in Z$, since m and n are relatively prime; hence

$$u_a = u_a^{qm+rn} = u_a^{qm}$$

$$\omega = v^q = u_a^{mq} (ava^{-1})^q = u_a a\omega a^{-1},$$

and

$$u_a a = \omega a \omega^{-1}$$, for all a ∈ A.

Therefore

$$B = \omega A \omega^{-1}$$ is a conjugate of A.

Theorem 2.1.18

In a solvable group of order mn, where m and n are relatively prime, all subgroups of order m are conjugates.

Proof:

Let G be solvable of order mn.

If m is a power of a prime, then 2.1.18 follows from the third Sylow theorem. Otherwise, we proceed by induction on $|G|$. By 2.1.15, G contains an abelian normal subgroup N of order $p^k > 1$ for some prime p, and p^k divides m or n.

Let $A, B \leq G$ have order m.

Assume that p^k divides m. Then $|NA| = |A|\,(|N| / |A \cap N|) = mp^h$ for some $h \leq k$.

Now, $mp^h = |NA|$ divides $mn = |G|$; since p^h and n are relatively prime this implies $p^h = 1$. Hence

$$|NA| = |A| \text{ and } N \subseteq A. \text{ Similarly, } N \subseteq B.$$

By the induction hypothesis, A/N and B/N are conjugate in G/N:

$$B/N = (Nx)(A/N)(Nx)^{-1} \text{ for some } x \in G.$$

Then,

$$B = \bigcup_{b \in B} Nb = \bigcup_{a \in A} (Nx)(Na)(Nx)^{-1}$$
$$= \bigcup_{a \in A} Nxax^{-1} = N(xAx^{-1}) = xAx^{-1}$$

Since $N = xNx^{-1} \subseteq xAx^{-1}$. Thus A and B are conjugate in G.

Now assume that p^k divides n. Then $A \cap N = B \cap N = \{e\}$; hence $|NA| = |NB| = p^k m$, and the subgroups $NA/N \cong A/(A \cap N)$ and $NB/N \cong B/(B \cap N)$ of G/N have order m.

By the induction hypothesis, NA/N and NB/N are conjugate in G/N.

As above, it follows that NA and NB are conjugate in G:

$$NB = xNAx^{-1} \text{ for some } x \in G.$$

Then B and $x\,Ax^{-1}$ are subgroups of NB of order m. Hence B and xAx^{-1} are conjugate in NB: this follows from the induction hypothesis if $p^k < n$, from Lemma 2.1.17 if $p^k = n$. Therefore A and B are conjugate in G.

Theorem 2.1.19. [19]

In a solvable group of order mn, where m and n are relatively prime, every subgroup whose order divides m is contained in a subgroup of order m.

Proof:

Let G be solvable of order mn. If m is a power of a prime, then theorem 2.1.19 follows from Proposition. "In a finite group, every p-subgroup is contained in a Sylow p-subgroup".

Otherwise, we proceed by induction on $|G|$.

By 2.1.15, G contains an abelian normal subgroup N of order $p^k > 1$ for some prime p , and p^k divides m or n.

Let H be a subgroup of G whose order ℓ divides m.

Assume that p^k divides m. Then $|NH/N| = |H|/|H \cap N|$ divides m, is relatively prime to n , and divides $|G/N| = (m/p^k)\,n$.

By the induction hypothesis, H/N is contained in a subgroup K/N of G/N of order m/p^k, where $N \subseteq K \leq G$; then H is contained in the subgroup K of G of order m.

Assume that p^k divides n. Then $H \cap N = \{e\}$ and $|NH| = p^k\,\ell$.

Hence $|NH/N| = \ell$ divides m, is relatively prime to n, and divides $|G/N| = (n/p^k)m$.

By the induction hypothesis, NH/N is contained in a subgroup K/N of G/N of order m, where

$N \subseteq K \leq G$; then $|K| = p^k m$ and $H \subseteq NH \subseteq K$.

If $p^k < n$, then $|K| < |G|$ and H is contained in a subgroup of K of order m, by the induction hypothesis.

Now assume that $p^k = n$. Let A be a subgroup of G of order m.

Then $A \cap N = \{e\}$, $|NA| = |N|\,|A| = |G|$, and $NA = G$. Hence $|A \cap NH| = |A|\,|NH| / |ANH|$ $= mp^k \ell / mn = \ell$. Thus H and $K = A \cap NH$ are subgroups of NH of order ℓ.
By 2.1.18, H and K are conjugate in NH : $H = xKx^{-1}$ for some $x \in NH$.
Then H is contained in the subgroup xAx^{-1} of G, which has order m.

2.2 Supersolvable groups

A group is said to be supersolvable if it has a normal series (where in all the members are normal in the whole group) of finite length, starting from the trivial group and ending at the whole group, such that all the successive quotients are cyclic. Supersolvablility is stronger than the notion of solvability.

Definition 2.2.1 (supersolvable)

A group G is said to be supersolvable if there exists a normal series:

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \ldots \leq H_n = G$$

where each $H_i \lhd G$ and further, each H_{i+1} / H_i is cyclic. By contrast, for a solvable group the definition requires each quotient to be abelian. [42]

Properties of supersolvable groups 2.2.2

1-Any subgroup of a supersolvable group is supersolvable.
The normal series for the subgroup can be obtained simply by intersecting the normal series of the group, with the subgroup.

2-Any quotient group of a supersolvable group is supersolvable.

The normal series for the quotient is obtained by taking the image of the normal series for the original group under the quotient map.

3-Any direct product of finitely many supersolvable groups is supersolvable.

Proof:

Suppose G and K are supersolvable groups and let $\{e\}=G_0 \leq G_1 \leq \ldots \leq G_n = G$ be asupersolvable series of G, also let $\{e\}=K_0 \leq K_1 \leq \ldots \leq K_m = K$ be a supersolvable series of K.

We note that for all $1 \leq i \leq n$, since $G_i \lhd G$

$$G_i \times \{e\} = G_i \times K_0 \lhd G \times K$$

Similarly, for all $1 \leq j \leq m$

$$G \times K_j \lhd G \times K$$

Furthermore,

$$(G_i \times \{e\})/(G_{i-1} \times \{e\}) \cong G_i / G_{i-1} \times \{e\}/\{e\} \cong G_i / G_{i-1}$$

For $1 \leq i \leq n$

And

$$(G \times K_j)/(G \times K_{j-1}) \cong G / G \times K_j / K_{j-1} \cong K_j / K_{j-1}$$

For $1 \leq j \leq m$,we see that

$$\{e\} = G_0 \times \{e\} \leq G_1 \times \{e\} \leq \ldots \leq G_n \times \{e\} = G \times K_o \leq G \times K_1 \leq \ldots \leq G \times K_m = G \times K$$

Is a supersolvable series of $G \times K$.

4-A finite group is supersolvable if and only if every maximal chain of subgroups has the same length. This is important to those interested in the lattice of subgroups of a group, and is sometimes called the Jordan-Dedekind condition.

Examples: 2.2.3

Z_3 , $Z_4 \times Z_4$ and Z_4 are supersolvable groups .While A_4 is not supersolvable.

2.3 Polycyclic groups

Polycyclic group is a solvable group that satisfies the maximal condition on subgroups (that is, every subgroup is finitely generated).A group is said to be polycyclic if it has a subnormal series (where in each member is normal in its successor) of finite length, starting from the trivial group and ending at the whole group, such that all the successive quotients are cyclic.

Definition 2.3.1 (polycyclic)

A group G with symbols is said to be polycyclic if there exists a series of subgroups:

$$\{e\} = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \ldots \triangleleft H_n = G$$

where each H_{i+1} / H_i is cyclic. [42]

Polycyclic groups are finitely presented, and this makes them very interesting from acomputational point of view. Examples of polycyclic groups include finitely generated abelian groups, and finite solvable groups. Supersolvable groups are always polycyclic, and hence solvable.

In another direction, a polycyclic group must have a normal series with each quotient cyclic, but there is no requirement that each H_i be normal in G. As every finite solvable group is polycyclic, this can be seen as one of the key differences between the definitions. For a concrete example, the alternating group on four points, A_4, is solvable but not supersolvable.

Example 2.3.2.

Klien four group is an example of noncyclic supersolvable group, so it is polycyclic.

2.4 Solvability by Radicals

When we say that a polynomial equation is solvable by radicals, we mean that the solutions can be obtained from the coefficients in a finite sequence of steps, each of which may involve addition, subtraction, multiplication, division, or taking *n*th roots. Only the extraction of an *n*th root leads to a larger field, and so our formal definition is phrased in terms of subfields and adjunction of roots of $x^n - a$ for suitable elements a.

Definition 2.4.1. (radical extension)

An extension field F of a field K is called a radical extension of K if there exist elements $u_1, u_2, \ldots, u_m$ in F and positive integers $n_1, n_2, \ldots, n_m$ such that

(i) $F = K(u_1, u_2, \ldots, u_m)$, and

(ii) $u_1^{n_1}$ is in K and $u_i^{n_i}$ is in $K(u_1, \ldots, u_{i-1})$ for $i = 2, \ldots, m$.

For a polynomial f(x) in K[x], the polynomial equation $f(x) = 0$ is said to be solvable by radicals if there exists a radical extension F of K that contains all roots of f(x). [13]

To study solvability by radicals of a polynomial equation $f(x) = 0$, we let K be the field generated by the coefficients of f(x). We let F be an extension field of K that is generated by the roots of f(x) over K. This is called the splitting field for f(x) over K, and is unique up to isomorphism.

Theorem 2.4.2. [41]

Let p(x) be a polynomial over a field K of characteristic zero. The equation $p(x) = 0$ is solvable by radicals if and only if the Galois group of p(x) over K is solvable.

Theorem 2.4.3. [9]

Let F be the splitting field of $x^n - 1$ over a field K of characteristic zero. Then Gal(F/K) is an abelian group.

Theorem 2.4.4. [10]

There exists a polynomial of degree 5 with rational coefficients that is not solvable by radicals.

Theorem 2.4.5.[45]

Let K be a field of characteristic zero that contains all nth roots of unity, let a be an element of K, and let F be the splitting field of x^n-a over K. Then Gal(F/K) is a cyclic group whose order is a divisor of n.

Theorem 2.4.6. [45]

For every positive integer n, the Galois group of the *n*th cyclotomic polynomial $\Phi_n(x)$ [13]over **Q** is isomorphic to $\mathbf{Z}_n^{\times}$. (Where $Z_n^{\times}$ is the set of units of Z_n)

Theorem 2.4.7. [45]

Let K be a field, let p(x) be a polynomial in K[x], and let F be a splitting field for p(x) over K. If p(x) has no repeated roots, then $|Gal(F/K)| = [F:K]$

Eisenstein's criterion 2.4.8 [10]

Eisenstein's criterion gives sufficient conditions for a polynomial to be irreducible over the rational numbers.

Suppose we have the following polynomial with integer coefficients.

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

If there exists a prime number p such that the following three conditionals all apply:

- p divides each a_i for $i \neq n$,
- p does *not* divide a_n, and
- p^2 does *not* divide a_0,

then $f(x)$ is irreducible over the rationals. Thus there cannot be any rational roots.

Example2.4.9

Consider $g(x) = 3x^4 + 15x^2 + 10$.

Using $p = 5$, as 5 does divide 15, the coefficient of x^2, and 10, the constant term. Also, 5 does not divide 3, the leading coefficient. Finally, $25 = 5^2$ does not divide 10. So, we conclude that $g(x)$ is irreducible over $\mathbf{Q}$.

In some cases the prime to choose can be unclear, but can be revealed by a change of variable $y = x + a$, which is often referred to as a shift.

For example consider $h(x) = x^2 + x + 2$. This looks difficult as no prime will divide 1, the coefficient of x. But if we shift $h(x)$ to $h(x + 3) = x^2 + 7x + 14$ we see instantly that the prime 7 divides the coefficient of x and the constant term and that 49 cannot divide 14. So by shifting the polynomial we have made it satisfy Eisenstein's criterion. [10]

Examples 2.4.10.

1. Find the Galois group of x^9-1 over $\mathbf{Q}$.

Solution:

We can construct the splitting field F of x^9-1 over $\mathbf{Q}$ by adjoining a primitive 9th root of unity to $\mathbf{Q}$. We have the factorization

$$x^9-1 = (x^3-1)(x^6+x^3+1)$$
$$= (x-1)(x^2+x+1)(x^6+x^3+1).$$

Substituting x+1 in the last factor yields

$$(x+1)^6+(x+1)^3+1 = x^6+6x^5+15x^4+21x^3+18x^2+9x+3.$$

This polynomial satisfies Eisenstein's criterion for the prime 3, which implies that the factor x^6+x^3+1 is irreducible over $\mathbf{Q}$. The roots of this factor are the primitive 9th roots of unity, so it follows that $[F:\mathbf{Q}] = 6$. The proof of Theorem 2.4.3 shows that Gal (F/$\mathbf{Q}$) is isomorphic to a subgroup of $\mathbf{Z}_9^{\times}$. Since $\mathbf{Z}_9^{\times}$ is abelian of order 6, it is isomorphic to $\mathbf{Z}_6$. It follows that Gal (F/$\mathbf{Q}$) $\cong \mathbf{Z}_6$.

Comment: Theorem 2.4.6 shows that the Galois group of x^n-1 over $\mathbf{Q}$ is isomorphic to $Z_n^{\times}$ and so the Galois group is cyclic.

2. Show that $x^4-x^3+x^2-x+1$ is irreducible over $\mathbf{Q}$, and use it to find the Galois group of $x^{10}-1$ over $\mathbf{Q}$.

Solution: We can construct the splitting field F of $x^{10}-1$ over $\mathbf{Q}$ by adjoining a primitive 10th root of unity to $\mathbf{Q}$. We have the factorization

$$x^{10}-1 = (x^5-1)(x^5+1)$$
$$= (x-1)(x^4+x^3+x^2+x+1)\,(x+1)(x^4-x^3+x^2-x+1).$$

Substituting x-1 in the last factor yields

$$(x-1)^4-(x-1)^3+(x-1)^2-(x-1)+1$$
$$= (x^4-4x^3+6x^2-4x+1) - (x^3-3x^2+3x-1) + (x^2-2x+1) - (x-1) + 1$$
$$= x^4-5x^3+10x^2-10x+5.$$

This polynomial satisfies Eisenstein's criterion for the prime 5, which implies that the factor

$x^4-x^3+x^2-x+1$ is irreducible over $\mathbf{Q}$.

So it follows that $[F:\mathbf{Q}] = 4$. The proof of theorem 2.4.3 and theorem 2.4.6 show that Gal $(F/\mathbf{Q}) \cong Z_{10}^{\times}$ and so the Galois group is cyclic of order 4.

3. Show that $p(x) = x^5-4x+2$ is irreducible over $\mathbf{Q}$, and find the number of real roots.

Solution: The polynomial p(x) is irreducible over $\mathbf{Q}$ since it satisfies Eisenstein's criterion for p = 2. Since p(-2) = -22, p(-1) = 5, p(0) = 2, p(1) = -1, and p(2) = 26, we see that p(x) has a real root between -2 and -1, another between 0 and 1, and a third between 1 and 2. The derivative $p'(x) = 5x^4- 4$ has two real roots, so p(x) has one relative maximum and one relative minimum, and thus it must have exactly three real roots. Also it has precisely two non- real roots in $\mathbf{C}$ .So, the Galois group of $p(x) = x^5-4x+2$ over $\mathbf{Q}$ is S_5 ,and so it is not solvable .(Since if f (x) is irreducible over $\mathbf{Q}$ and of degree prime p with precisely two nonreal roots in C then the Galois group of f is S_p [10]).

2.5 Burnside's theorem

Burnside's theorem has long been one of the best-known applications of representation theory to the theory of finite groups, though a proof avoiding the use of group characters was published by D. Goldschmidt around 1970. The theorem was proved by William Burnside in the early years of the 20th century.

Lemma 2.5.1 [10]

If $|\kappa|$ is a power of prime for some nonidentity conjugcy class κ of G, then G is not a non-abelian simple group.

Theorem 2.5.2:(Burnside's theorem) [10]

If G is a finite group of order $p^a q^b$, where p and q are prime numbers, and a and b are non-negative integers, then G is solvable.

Proof:

Let G be a group of order $p^a q^b$ for some primes p and q .

Now if p = q or either exponent is 0 then G is solvable .

Thus we may assume this is not the case .Proceeding by induction let G be a counter example of minimal order.

If G has a proper, nontrivial normal subgroup N, then by induction both N and G/N are solvable, hence so is G.

Thus we may assume G is non-abelian simple group.

Let $P \in syl_p(G)$.

Then $\exists\ g \in Z(P)$ with $g \neq e$. Now since $P \leq C_G(g)$, the order of the conjugacy class of g (which equals $|G : C_G(g)|$ is prime to p. i.e. is a power of q. This violates lemma 2.5.1 and so completes the proof of Burnsides theorem.

Chapter Three

3.1 Nilpotent groups

Nilpotent groups are a class of solvable groups with even more striking properties. In group theory, a nilpotent group is a group having a special property that makes it"almost" abelian, through repeated application of the commutator operation, [x,y] = $xyx^{-1}y^{-1}$.

This idea is motivated by the fact that nilpotent groups are solvable, and for finite nilpotent groups, two elements having relatively prime orders must commute.

It is also true that finite nilpotent groups are supersolvable. Nilpotent groups arise in Galois theory, as well as in the classification of groups.

Definition 3.1.1 (Nilpotent groups).

A group G is called nilpotent if there exists a finite collection of normal subgroups $G_0,G_1,\ldots,G_k$, with

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_k = G$$

such that, $G_{j+1} / G_j \subseteq$ $Z(G/G_j)$ for $j = 1,2,\ldots,k-1$.

That means a group is nilpotent when it has a central normal series.

"In particular, abelian groups are nilpotent, and nilpotent groups are solvable .The converses are not true; we shall see that D_4 is nilpotent but not abelian, and that $D3$ and $D5$ are solvable but not nilpotent". [17]

Nilpotent groups have two explicit central normal series:

1- The descending (lower)central series
2- The ascending(upper) central series

Definition 3.1.2

The descending (lower)central series of a group G is the sequence

$$G \rhd G^1 \rhd \ldots \rhd G^k \rhd G^{k+1} \rhd \ldots$$

in which $G^0 = G$, and G^{k+1} is the subgroup generated by all commutators $xyx^{-1}\,y^{-1}$ with

Chapter Three

3.1 Nilpotent groups

Nilpotent groups are a class of solvable groups with even more striking properties. In group theory, a nilpotent group is a group having a special property that makes it"almost" abelian, through repeated application of the commutator operation, [x,y] = $xyx^{-1}y^{-1}$.

This idea is motivated by the fact that nilpotent groups are solvable, and for finite nilpotent groups, two elements having relatively prime orders must commute.

It is also true that finite nilpotent groups are supersolvable. Nilpotent groups arise in Galois theory, as well as in the classification of groups.

Definition 3.1.1 (Nilpotent groups).

A group G is called nilpotent if there exists a finite collection of normal subgroups $G_0,G_1,\ldots,G_k$, with

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_k = G$$

such that, $G_{j+1} / G_j \subseteq$ Z(G/Gj) for $j = 1,2,...,k-1$.

That means a group is nilpotent when it has a central normal series.

"In particular, abelian groups are nilpotent, and nilpotent groups are solvable .The converses are not true; we shall see that D_4 is nilpotent but not abelian, and that $D3$ and $D5$ are solvable but not nilpotent". [17]

Nilpotent groups have two explicit central normal series:

1- The descending (lower)central series

2- The ascending(upper) central series

Definition 3.1.2

The descending (lower)central series of a group G is the sequence

$$G \rhd G^1 \rhd \ldots \rhd G^k \rhd G^{k+1} \rhd \cdots$$

in which G^0 = G, and G^{k+1} is the subgroup generated by all commutators $xyx^{-1}y^{-1}$ with

$x \in G$ and $y \in G^k$.

In particular, $G^1 = G'$. The descending central series yields a central normal series if some $G^r = \{e\}$ and subsequent terms are removed.

Proposition 3.1.3

$G^k \lhd G$ and $G^k/G^{k+1} \subseteq Z(G/G^{k+1})$, for all k.

Proof:

The proof is by induction on k.

First, $G^0 = G \lhd G$, and $G^0/G^1 = G/G' \subseteq Z(G/G^1)$ since G/G' is abelian by proposition 2.1.2. Now assume that $G^k \lhd G$. As in the proof of proposition 2.1.2. , the inverse of the commutator $xyx^{-1}y^{-1}$ of x and y is the commutator of y and x, and a conjugate

$a\,xyx^{-1}y^{-1}a^{-1} = axa^{-1}aya^{-1}(axa^{-1})^{-1}(aya^{-1})^{-1}$

of $xyx^{-1}y^{-1}$ is the commutator of a conjugate of x and a conjugate of y.

Hence every $g \in G^{k+1}$ is a product $g = c_1, \ldots, c_n$ of commutators $xyx^{-1}y^{-1}$ of $x \in G$ and $y \in G^k$, and commutators $xyx^{-1}y^{-1}$ of $x \in G^k$ and $y \in G$; then

$$aga^{-1} = ac_1a^{-1} \ldots ac_na^{-1}$$

is a product of similar commutators.

Thus $G^{k+1} \lhd G$. For all $x \in G$ and $y \in G^k$, $xyx^{-1}y^{-1} \in G^{k+1}$; hence $G^{k+1}xy = G^{k+1}yx$ and $G^{k+1}y \in Z(G/G^{k+1})$. Thus $G^k/G^{k+1} \subseteq Z(G/G^{k+1})$.

The other series ascends by way of centers and is constructed as follows:

Proposition 3.1.4.

Every group G has unique normal subgroups $Z_k(G)$ such that $Z_0(G) = \{e\}$ and $Z_{k+1}(G)/Z_k(G) = Z(G/Z_k(G))$ for all $k \geq 0$.

Proof.

First, $Z_0(G) = \{e\}$ is normal in G. If $Z_k \lhd G$, then $Z(G/Z_k(G))$ is a normal subgroup of $G/Z_k(G)$. Now since $Z_k \lhd G$, then (every subgroup of G/Z_k is the quotient H/Z_k of a unique subgroup H of G that contains Z_k). So there is a unique normal subgroup $H = Z_{k+1}(G) \supseteq Z_k(G)$ of G such that $Z(G/Z_k(G)) = Z_{k+1}(G)/Z_k(G)$.

In particular, $Z_1(G) = Z(G)$ is the center of G.

Definition 3.1.5.

The ascending(upper) central series of a group G is the sequence

$$\{e\} = Z_0(G) \lhd Z_1(G) \lhd \ldots \lhd Z_k(G) \lhd Z_{k+1}(G) \lhd \ldots$$

constructed in Proposition 3.1.4

The ascending central series yields a central normal series if some $Z_r(G) = G$ and subsequent terms are removed. [17]

A group is said to be nilpotent if it satisfies the following equivalent conditions:

- Its upper central series stabilizes after a finite length at the whole group.

Clearly, the upper central series, when finite, is itself a central series, so its length puts an upper bound on the minimum possible length of a central series. But the fact that the upper central series is the fastest ascending central series, also shows that every central series has length at least as much as the upper central series. Thus, the length of the upper central series is the minimum possible length of a central series.

- Its lower central series stabilizes after a finite length at the trivial subgroup.

Clearly, the lower central series, when finite, is itself a central series, so its length puts an upper bound on the minimum possible length of a central series. But the fact that the lower central series is the fastest descending central series, also shows that every central series has length at least as much as the lower central series. Thus, the length of the lower central series is the minimum possible length of a central series.

For a nilpotent group, the lower central series and upper central series are closely related.

The length after which the upper central series stabilizes equals the length after which the lower central series stabilizes, and this length is termed the nilpotence class of the group. For any c greater than or equal to the nilpotence class, the group is said to be of class c. Equivalently, the nilpotency class of G equals the length of the lower central series or upper central series (the minimum n such that the nth term is the trivial subgroup, respectively the whole group).

So, The nilpotence class of a nilpotent group is the length of its lower central series, i.e., for a group G, it is the smallest c such that G^{c+1} is trivial, and The nilpotence class of a nilpotent group is the length of its upper central series, i.e., for a group G, it is the smallest c such that $Z_c(G) = G$.

If a group has nilpotency class at most m, then it is sometimes called a **nil-m** group. For example, Z_4 is a nil-1 group, and Q_8 is a nil-2 group.

The trivial group is the unique group of nilpotency class 0, and groups of nilpotency class 1 are exactly non-trivial abelian groups.

Examples 3.1.6

These are some important examples of nilpotent groups:

- The dihedral group of order 8 (D4) is the smallest nilpotent group which is not abelian.
- The quaternion group (Q_8) is also the smallest nilpotent group which is not abelian.

Proposition 3.1.7

A group G is nilpotent if and only if $G^r = \{e\}$ for some $r \geq 0$, if and only if $Z_r(G) = G$ for some $r \geq 0$.

Proof:

If $G^r = \{e\}$ for some $r \geq 0$, or if $Z_r(G) = G$ for some $r \geq 0$, then the descending central series, or the ascending central series, yields a central normal series, and G is nilpotent.

Conversely, assume that G has a central normal series $\{e\} = C_0 \lhd C_1 \lhd \ldots \lhd C_m = G$. We prove by induction on k that $G^k \subseteq C_{m-k}$ and $C_k \subseteq Z_k(G)$ for all $0 \leq k \leq m$; hence $G^m = \{e\}$ and $Z_m(G) = G$. (Thus, the ascending and descending central series are in this sense the "fastest" central series.)

We have $G^{m-m} = G = C_m$. Assume that $G^{m-j} \subseteq C_j$, where $j > 0$. Let $x \in G$ and $y \in G^{m-j} \subseteq C_j$. Since $C_{j-1}\, y \in C_j / C_{j-1} \subseteq Z(G/Cj-1)$, we have $C_{j-1}xy = C_{j-1}yx$ and $xyx^{-1}y^{-1} \in C_{j-1}$. Thus C_{j-1} contains every generator of G^{m-j+1}; hence $G^{m-j+1} \subseteq C_{j-1}$.

We also have $Z_0(G) = \{e\} = C_0$. Assume that $C_k \subseteq Z_k = Z_k(G)$, where $k < m$. Then $G/Z_k \cong (G/C_k)/(Z_k/C_k)$ and there is a surjective homomorphism $\pi: G/C_k \to G/Z_k$ with kernel Z_k/C_k, namely $\pi : C_k x \to Z_k x$.

Since π is surjective, π sends the center of G/C_k into the center of G/Z_k:
$\pi(C_{k+1}/C_k) \subseteq \pi Z(G/C_k) \subseteq Z(G/Z_k) = Z_{k+1}/Z_k$;
hence $Z_k x \in Z_{k+1}/Z_k$ for all $x \in C_{k+1}$, and $C_{k+1} \in Z_{k+1}$.

In fact, we have shown that $G^r = \{e\}$ if and only if $Z_r(G) = G$; the least such r is the nilpotency index of G.

3.2 Properties of nilpotent groups

1. Any subgroup of a nilpotent group is nilpotent. In fact, any subgroup of a group of nilpotence class *r* has nilpotence class *r*.

   Let G be a nilpotent group of nilpotence class r . $H \leq G$ then $H^{(r)} \leq G^{(r)}$ but $G^{(r)}=\{e\}$ .So $H^{(r)} = \{e\}$,hence H is nilpotent of nilpotence class r.

2. Any quotient of a nilpotent group is nilpotent. In fact, any quotient of a group of nilpotence class *r* has nilpotence class *r*.

   Suppose that G is nilpotent group of nilpotence class r ,and N a normal subgroup of G .Then by using canonical homomorphism $\varphi : G \to G/N$ we have, $(G/N)^{(r)} = \varphi(G^{(r)}) = \varphi(\{e\}) = \{e\}$.Then the result holds.

3. Any direct product of groups of nilpotent groups is nilpotent. In fact, if both of them are of nilpotence class *r* (we can *r* as the higher of their nilpotence classes) then their product is also of nilpotence class *r*.

   This follows from the fact that the central series of the direct product is the direct product of the respective central series.

Remark:

Nilpotence is closed under taking joins of finitely many normal subgroups. In other words, if a group is generated by finitely many nilpotent normal subgroups, it is also nilpotent.

Proposition 3.2.1

If $N \subseteq Z(G)$ and G/N is nilpotent, then G is nilpotent.

Proposition 3.2.2

Every finite p-group is nilpotent.

Proof.

That a group G of order p^n is nilpotent is proved by induction on n.

If $n \leq 2$, then G is abelian, hence nilpotent, (since every group of order p^2, where p is prime, is abelian).

If $n > 2$, then G has a nontrivial center, (since every nontrivial p-group has a nontrivial center). Then $G/Z(G)$ is nilpotent, by the induction hypothesis, and G is nilpotent, by proposition 3.2.1 (3).

Theorem 3.2.3.

A finite group is nilpotent if and only if all its Sylow subgroups are normal, if and only if it is isomorphic to a direct product of p-groups (for various primes p).

Proof:

The ascending central series of any group G has the following property:
if $Z_k \subseteq H \leq G$, then $Z_{k+1} \subseteq N_G(H)$. Indeed, let $x \in Z_{k+1}$ and $y \in H$. Since $Z_k x \in Z_{k+1}/Z_k \subseteq Z(G/Z_k)$ we have $Z_k xy = Z_k yx$, so that $xyx^{-1} y^{-1} \in Z_k$ and $xyx^{-1} = (xyx^{-1} y^{-1}) y \in H$. Thus $x \in N_G(H)$.

Now let G be a finite group. Let S be a Sylow p-subgroup of G. (since in a finite group, a subgroup that contains the normalizer of a Sylow p-subgroup is its own normalizer).
$N_G(S)$ is its own normalizer. Hence $Z_0 = \{e\} \subseteq N_G(S)$, and $Z_k \subseteq N_G(S)$ implies $Z_{k+1} \subseteq N_G(N_G(S)) = N_G(S)$ by the above, so that $Z_k \subseteq N_G(S)$ for all k. If G is nilpotent, then $N_G(S) = G$, by Proposition 3.1.7., and $S \lhd G$.

Next, assume that every Sylow subgroup of G is normal. Let $p_1, p_2, \ldots, p_m$ be the prime divisors of $|G|$. Then G has one Sylow p_i-subgroup S_i for every

p_i. We have $|G| = |S_1|\,|S_2| \dots |S_m|$; hence $G = S_1\, S_2 \dots S_m$. Moreover, $(S_1 \dots S_i) \cap S_{i+1} = \{e\}$ for all $i < m$, since $|S_{i+1}|$ and $|S_1 \dots S_i|$ are relatively prime. Hence $G \cong S_1 \times S_2 \times \dots \times S_m$, by (Proposition. A group G is isomorphic to the direct product $G_1 \times G_2 \times \dots \times G_n$ of groups $G_1, G_2, \dots, G_n$ if and only if it contains normal subgroups $A_i \cong G_i$ such that $A_1\, A_2 \dots A_n = G$ and $(A_1\, A_2 \dots A_i) \cap A_{i+1} = \{e\}$ for all $i < n$. Then every element g of G can be written uniquely in the form $g = a_1\, a_2 \dots a_n$ with $a_i \in A_i$; $a_i \in A_i$ and $a_j \in A_j$ commute whenever $i \neq j$; and the mapping $(a_1, a_2, \dots, a_n) \rightarrow a_1\, a_2 \dots a_n$ is an isomorphism of $A_1 \times A_2 \times \dots \times A_n$ onto G).

Finally, if G is isomorphic to a direct product of p-groups, then G is nilpotent, by Proposition 3.2.2 and Property 3 page 44.

In particular, D_4 and Q_8 are nilpotent, by Proposition 3.2.2, but the solvable groups D_3 and D_5 are not nilpotent, by theorem 3.2.3. If G is a nilpotent finite group, we will easily deduce from theorem 3.2.3 that every divisor of |G| is the order of a subgroup of G. This property does not extend to solvable groups; for instance, the solvable group A_4 of order 12 does not have a subgroup of order 6.

Theorem 3.2.4:

Any abelian group is a nilpotent group. In fact, abelian groups are the nilpotent groups of nilpotence class 1.

Proof:

Suppose that G is an abelian group .Now G is abelian if and only if Z(G)=G, and so, the first member $Z_1(G)$ of the upper central series is the center of G, which is the whole of G. Thus the upper central series terminates in 1 step, and G is nilpotent of nilpotence class 1.

Remark: we can prove theorem 3 .2.4 easily by using the lower central series of G.

Theorem 3.2.5:

Not every nilpotent group is abelian.

Proof:

For a small non-abelian example, consider the quaternion group Q_8, which is a smallest non-abelian p- group. It has center $\{1, -1\}$ of order 2, and its upper central series is $\{1\}$, $\{1,-1\}$, Q8; so it is nilpotent of class 2.

Proposition 3.2.6.

Let G be nilpotent with derived length d and nilpotent class c .Then

$$d < 1+\log_2(c+1)$$

Proof:

We have $G' = G^2$ and since if $G = G^1 \supseteq G^2 \supseteq \ldots$ be lower central series of an arbitrary group G .Then $\left[G^i, G^j\right] \subseteq G^{i+j}$ for all i,j ≥ 1

We get $G'' = \left[G^2, G^2\right] \subseteq G^4$

$$G''' = [G'', G''] \subseteq [G^4, G^4] \subseteq G^8$$

Continuing we see that $G^{(k)} \subseteq G^{2k}$

Now $\{e\} < G^{d-1} \subseteq G^{2^{d-1}}$ and yet $G^{c+1} = \{e\}$.This gives $c+1 > 2^{d-1}$, and so $d < 1+\log_2(c+1)$.

3.3 Relation between Solvable groups and Nilpotent groups

Lemma 3.3.1: [10]

For any group, the i^{th} member of the derived series is contained in the i^{th} member of the lower central series.

Proof:

We prove this lemma inductively.

For $i = 1$: Both $G^{(1)}$ and G_1 are the same.

Thus $G^{(1)} \leq G_1$

Suppose $G^{(m)} \leq G_m$. Then we have:

$G_{m+1} = [G,G_m]$ and $G^{(m+1)} = [G^{(m)},G^{(m)}]$

Now, $G^{(m)} \leq G$ and $G^{(m)} \leq G_m$ (using the induction assumption). Thus, every commutator between $G^{(m)}$ and $G^{(m)}$ is also a commutator between G and G_m. Thus, we have a generating set for $[G^{(m)},G^{(m)}]$ which is a subset of a generating set for $[G,G_m]$.

From this, it follows that $[G^{(m)},G^{(m)}]$ is a subgroup of $[G,G_m]$. Thus:

$$G^{(m+1)} \leq G_{m+1}.$$

Theorem 3.3.2

Any nilpotent group is a solvable group.

Proof:

We now use the fact that for any group G, $G^{(i)} \leq Gi$ [by lemma3.3.1].

Suppose G is a nilpotent group. Let c be the nilpotence class of G, so the length of the lower central series of G is c or the smallest c such that G_c is the trivial group. Then, by the lemma 3.3.1: $G^{(c)} \leq G_c = \{e\}$

and hence $G^{(c)}$ is trivial. This means that G is solvable.

Remark:

Not every solvable group is nilpotent.

Since the smallest solvable non-nilpotent group is the symmetric group on three letters. This is centerless, so it cannot be nilpotent. On the other hand, it is clearly solvable, because its commutator subgroup is the alternating group on three letters, which is abelian.

Chapter Four

Applications

4.1 Carter subgroup of solvable group in ©

Let © denotes the class of finite groups in which every element is conjugate to its inverse [see definition 4.1.1]. Here we investigate solvable groups in ©.
In particular we show that if G ∈ © and G is solvable then the Carter subgroup of G is a Sylow 2-subgroup. [9]

Definition 4.1.1 (conjugate elements) [10]

Suppose G is a group. Two elements a and b of G are called conjugate if there exists an element g in G with

$$gag^{-1} = b.$$

It can be readily shown that conjugacy is an equivalence relation [reflexive, symmetric and transitive], and therefore partitions G into equivalence classes. (This means that every element of the group belongs to precisely one conjugacy class, and the classes Cl(a) and Cl(b) are equal if and only if a and b are conjugate, and disjoint otherwise.) .The equivalence class (conjugacy class) that contains the element a in G is:

$$\mathrm{Cl}(a) = \{gag^{-1} : g \in G\}.$$

The class number of G is the number of distinct (nonequivalent) conjugacy classes.

For example: The symmetric group S_3 has three conjugacy classes:

- The class of the identity element.
- The class of transpositions.
- The class of 3-cycles

Definition 4.1.2(self-normalizing subgroup)

A subgroup H of a group G is called a self-normalizing subgroup of G if $N_G(H) = H$.

Definition 4.1.3 (Carter subgroup)

Carter subgroup of a finite group G is a subgroup H that is a nilpotent group, and self-normalizing.

For example: the sylow 2- subgroups in S_3 are the Carter subgroups

Definition 4.1.4(central element)

An element of a group is termed central if it commutes with every element of the group or if its centralizer is the whole group

Lemma 4.1.5

Let C be a Carter subgroup of the solvable group G and let A and B be subsets of C, both normal in C. If $A \neq B$ then A and B are not conjugate in G.

Theorem 4.1.6

If G is a solvable group in © then a Carter subgroup of G is a Sylow 2-subgroup of G.

Proof:

Let C be a Carter subgroup of G. If C has a nonidentity element of odd order then C has a nonidentity central element g of odd order, since C is nilpotent. Then with $A = \{g\}$ and $B = \{g^{-1}\}$ the hypotheses of Lemma 4.1.5 are satisfied and, since $A \neq B$, g and g^{-1} are not conjugate in G, contradicting our supposition that $G \in ©$. Hence C is a 2-group. As C is self-normalizing in G, C must be a Sylow 2-subgroup of G.

Corollary 4.1.7.

If T is a Sylow 2-subgroup of a solvable group $G \in ©$. then $N_G(T) = T$.

Proof:

By Theorem 4.1.6 T is a Carter subgroup of G. and by def 4.1.3 it is clear that T is self-normalizing.

4.2 Metabelian Groups

Metabelian groups can be thought of as groups that are "close" to being abelian, in the sense that every abelian group is metabelian, but not every metabelian group is abelian.This closeness is reflected in the particular structure of their commutator subgroups. As we have developed techniques for examining commutator subgroups, we are now able to apply the techniques to examine this particular class of groups. Because, as we will see later, metabelian groups are very simple instances of solvable groups, it is worthwhile for us to examine metabelian groups before we move on to studying solvable groups in general. The goal of this section is to prove several interesting properties of metabelian groups.[46]

Definition 4.2.1

A group G is metabelian if there exists a normal subgroup A of G such that both A and G/A are abelian.

Proposition 4.2.2.

Every abelian group is metabelian.

Proof:

Let G be an abelian group. Then all subgroups of G are normal, and $G' = \{e\}$. So all of G's quotient groups are abelian [since if G is a group and N is normal subgroup of G with $G' \subseteq N$ then G/N is abelian], and thus G is metabelian.

We may now prove the following three theorems.

Theorem 4.2.3

G is metabelian if and only if $G'' = \{e\}$ (G'' is the commutator subgroup of G').

Proof:

We first prove the only if direction. Let G be a metabelian group; we will show that $G'' = \{e\}$. Because G is metabelian, it has a normal abelian subgroup N, and G/N is abelian.

Thus, $G' \subseteq N$. Since N is abelian, $G' = \{e\}$, and so $G'' = \{e\}$.

We now prove the if direction. Let $G'' = \{e\}$. We will show that G is metabelian. We will do this by first establishing the existence of a normal abelian subgroup of G and then by showing that G's quotient with that group is abelian. Note that if G is abelian, then G is metabelian by proposition 4.2.2. So, we have only to consider the case where G is not abelian, and hence $G' \neq \{e\}$. Thus, assume that G is not abelian.

We will now show the existence of a normal abelian subgroup of G. Consider the commutation of two elements x, y $\in G'$. We know that $xyx^{-1}y^{-1} = e$ since $G'' = \{e\}$ and so we have that xy = yx. Thus, arbitrary elements x, y $\in G'$ commute, so $G' \neq \{e\}$.is an abelian subgroup of G. We must now show that G' is normal in G to establish the existence of a normal abelian subgroup of G. Let g $\in$ G and h $\in G'$.

To show normality:

we must show that $ghg^{-1} \in G'$. We know that $ghg^{-1}h^{-1} \in G'$ because $ghg^{-1}h^{-1}$ is the commutation of g, h $\in G'$. Because G' is a group containing h and $ghg^{-1}h^{-1}$, multiplying $ghg^{-1}h^{-1}$ by h yields another element in G'.

Thus, $ghg^{-1}h^{-1}h = ghg^{-1} \in G'$, and so G' is normal in G. Thus, G' is a normal abelian subgroup of G.

We have established the existence of a normal abelian subgroup of G, namely G', so all that remains is to show that G/G' is abelian. Because $G' \lhd$ G and $G' \subseteq G'$, we have that G/G' is abelian. Thus, G has an abelian normal subgroup, G', and G/G' is abelian, so G is metabelian.

Theorem 4.2.4

If H is a subgroup of a metabelian group G, then H is metabelian.

Proof:

Let H be a subgroup of the metabelian group G. Since G is metabelian, by theorem 4.2.3, $G'' = \{e\}$.

Consider H'. As H is a subgroup of G, it must be the case that H' is a subgroup of G' To see this, let x be a generator of H', so that $x = aba^{-1}b^{-1} \in H'$ for some a, b $\in H$. Since $H \subseteq$ G, a, b $\in$ G and hence $aba^{-1}b^{-1} = x \in G'$. Therefore, H' is a subgroup of G'.

Thus, it must also be the case that H'' is a subgroup of G''. Since $G'' = \{e\}$, it follows that $H'' = \{e\}$. Thus, by theorem 4.2.3, H is metabelian.

Theorem 4.2.5

If G is metabelian and $\varphi: G \to K$ is a group homomorphism, then $\varphi(G)$ is metabelian.

Proof:

Let G be metabelian and φ be as above. We will show that $\varphi(G)'' = \{e\}$, so that $\varphi(G)$ is metabelian by theorem 4.2.4.

To that end, we will show that commutation is respected by group homomorphisms in general. In other words, we will show that the image of a commutator subgroup is the commutator subgroup of the image. Let A and B be groups, and let X be a subgroup of A; let $\psi: A \to B$ be a group homomorphism. We will show that $\psi(X)' = \psi(X')$ by showing that:

$$\psi(X)' \subseteq \psi(X') \text{ and } \psi(X') \subseteq \psi(X)'.$$

Note that the notation $\psi(X)'$ denotes the commutator subgroup of ψ (X). Let $\alpha \in \psi(X)'$ be a generator of $\psi(X)'$.

Then

$$\alpha = \psi(a)\,\psi(b)\,\psi(a)^{-1}\,\psi(b)^{-1}$$

for some a, b $\in$ X. Because ψ is a group homomorphism, we may simply the expression to get $\alpha = \psi(aba^{-1}b^{-1}) \in \psi(X')$, as $aba^{-1}b^{-1} \in X'$.

Thus,

$$\psi(X)' \subseteq \psi(X').$$

Now, let $\beta \in \psi(X')$ be a generator of $\psi(X')$.

Then $\beta = \psi(aba^{-1}b^{-1})$ for some a, b $\in$ X. As ψ is a group homomorphism, we may expand this expression to get

$$\beta = \psi(a)\,\psi(b)\,\psi(a)^{-1}\,\psi(b)^{-1} \in \psi(X)',$$

as β is the commutation of two elements ψ (a), ψ (b) $\in$ ψ (X).

Thus,

$$\psi(X') \subseteq \psi(X)'.$$

Therefore,

$$\psi(X)' = \psi(X').$$

For our particular case, this means that for a subgroup H of G, that $\varphi(H)' = \varphi(H')$

Thus, have that

$$\varphi(G)'' = \varphi(G')' = \varphi(G'')$$

.

Since G is metabelian, $G'' = \{e\}$, and as group homomorphisms always map identity to identity, we have that .

$$\varphi(G)'' = \varphi(G'') = \varphi(e) = e$$

Thus, by theorem 4.2.4, $\varphi(G)$ is metabelian.

We can now see that metabelian groups really are simple instances of solvable groups.

A metabelian group is a solvable group which has the sequence of subgroups

$$\{e\} = G_0 \subseteq G' \subseteq G_2 = G$$

4.3 Groups with many hypercentral subgroups

We obtain a characterization of solvable groups with the minimal condition [see definition 4.3.5] on non-hypercentral (respectively non-nilpotent) subgroups.

Definition 4.3.1(Maximal subgroup)

A subgroup H of G is maximal if there is no proper subgroup K contains H strictly .

For example: A_4 is maximal subgroup of S_4.

Definition 4.3.2(Minimal non-abelian group)

A minimal non-abelian group G is a non-abelian group in which every proper subgroup is abelian .

For example: S_3 is minimal non-abelian group.

Definition 4.3.3(Minimal non-nilpotent)

A group G is minimal non-nilpotent if each of its maximal subgroup S is nilpotent but G itself is not. [39]

For example : S_3 is minimal non-nilpotent group

Definition 4.3.4(Maximal condition)

A group G is said to satisfy the maximal condition if every strictly ascending chain of subgroups

$$G_1 \subset G_2 \subset G_3 \subset \ldots$$

is finite.

Definition 4.3.5 (Hypercentral Groups)

A group G is said to be hypercentral if the last term of its upper central series is a group G itself. [40]

For example: Q_8 is hypercentral group.

Definition 4.3.6 (minimal condition Min-ZA)

A group G satisfies the minimal condition on a non-hypercentral subgroups Min-ZA (respectively, the minimal condition on non- nilpotent subgroups Min-N) if for any properly descending chain $G_1 \geq G_2 \geq \ldots \geq G_n \geq \ldots$ of subgroups G_n in G there exists a number m ∈ N such that G_n is hypercentral (respectively, nilpotent) for each $n \geq m$.[41]

Definition 4.3.7(Quasicyclic group)

The p-quasicyclic group (or Prufer p-group) is the p-primary component of Q/Z ,that is , the unique maximal p-subgroup of Q/Z.

The p-quasicyclic group will be denoted by $Z(p^{\infty})$

Definition 4.3.8 (Cernicov group)

A Cerinkov group (or Cherincov group) is a group G that has a normal subgroup N such that G/N is finite and N is a direct product of finitely many quasicyclic groups.

Cherincov groups are named after Sergei Cherincov, who proved that every solvable group that satisfies the minimal condition is a Chernicov group. Also, afinite extension of an abelian group with minimum condition is called Chernicov group.

Definition 4.3.9 (Non - χ-group)

Let χ be a class of groups .A group which does not belong to χ but all of whose proper quotients belong to χ is called just Non-χ-group.

Also, a group which does not belong to χ but all of whose proper subgroups belong to χ is called minimal-Non-χ - subgroup.[43]

Definition 4.3.10(HM*- group)

A group G is HM*- group if its commutator subgroup G' is hypercentral and the quotient group G/G' is a divisible Cernikov p-group. [43]

Definition 4.3.11 (subnormal subgroup)

A subgroup H of a group G is subnormal if there is a finite chain of subgroups of the group G each one normal in the next beginning at H and ending at G .

In notation, H is k-subnormal in G if there are subgroups

$$H = H_0, H_1, H_2, \ldots H_k = G$$

of G such that $H_i \lhd H_{i+1}$ for each i.

Definition 4.3.12 (Conjugate Closure): [37]

The conjugate closure (or normal closure) of a subset S of a group G is the subgroup of G generated by S^G, i.e. the closure of S^G under the group operation, where S^G is the conjugate of the elements of S:

$$S^G = \{g^{-1}sg: g \in G \text{ and } s \in S\}$$

The conjugate closure of any subset S of a group G is always a normal subgroup of G; in fact it is the smallest normal subgroup of G which contains S.

For example: the conjugate closure of the empty set is the trivial group.

Also, any normal subgroup is equal to its normal closure.

Definition 4.3.13(Heineken – Mohamed group)

Heineken – Mohamed group is a non-nilpotent p- group (p a prime)in which every subgroup is both subnormal and nilpotent .

Heineken and Mohamed construct a metabelian group G with the property that every proper subgroup of G is nilpotent and subnormal in G but G itself has trivial center. [42]

Also, any Heineken – Mohamed type group is a minimal non-nilpotent group and satisfies Min-N and Min-ZA.Therefore S_3 is Heineken – Mohamed type group.

Definition 4.3.14(Normalizer condition)

A group G is said to satisfy the normalizer condition (NC) if every proper subgroup of G is properly containd in its normalizer in G.

That is, if and only if $H < N_G(H)$ for all $H < G$.

A group that satisfies the normalizer condition is sometimes called an N-group. [42]

For example: Every nilpotent group is an N-group.

Definition 4.3.15 (Locally Nilpotent Group)

A locally nilpotent group is a group G in which every finitely generated subgroup is nilpotent. [40]

For example: All nilpotent groups is locally nilpotent.

Lemma 4.3.16 : [43]

Let G be a locally nilpotent group. If G satisfies Min-N (respectively,Min-ZA), then G satisfies the normalizer condition and every minimal non-nilpotent (respectively, non-hypercentral) subgroup of G is subnormal.

Proof:

Let H be a proper subgroup of G. If H is either a non-nilpotent (respectively, non-hypercentral) or maximal nilpotent (respectively, hypercentral) subgroup of G, then the set $\{S : H < S \leq G\}$ has a minimal element, say M. Since H is a maximal subgroup of M, we conclude that H is normal in M. Moreover, every nilpotent (respectively, hypercentral) subgroup of G satisfies the normalizer condition and so G has also this property.

Let H be a minimal non-nilpotent (respectively, non-hypercentral) subgroup of G. Then the quotient group G/G′ is quasicyclic (respectively, quasicyclic or trivial).
If the derived subgroup H′ is not normal in G, then $N_G(H')$ is a proper subgroup of $N_G(N_G(H'))$. Since any radicable abelian ascendant subgroup is subnormal, the subgroup H/H′ is subnormal in M/H′. As a consequence, H is subnormal in M. The quotient group

M/H' has a finite series whose quotients satisfy the minimal condition on subgroups and so it is a Cernikov group.

Let $t \in N_G(M) \setminus M$. Then $(H')^t$ is normal in M and therefore M/ $(H' \cap (H')^t$ is Cernikov. Hence $H' = H' \cap (H')^t$. Now it is not difficult to prove that $H' = (H')^t$, a contrary with the choice of t . Thus a subgroup H' is normal in G. Since H/H' is ascendant in G/H', we conclude by the same argument as above that H/H' is subnormal in $G/H'$and consequently H is subnormal in G.

Corollary 4.3.17.

Let G be a non-nilpotent (respectively, non-hypercentral) locally nilpotent group satisfying Max-N (respectively, Max-ZA). If all proper normal subgroups of G are nilpotent (respectively, hypercentral), then G is minimal non-nilpotent (respectively, non-hypercentral) group.

Proof.

Let H be a proper subgroup of G and H be a minimal non-nilpotent (respectively, non-hypercentral) group. By Lemma 4.3.16 H is subnormal in G. Then the normal closure H^G of H in G is a proper normal subgroup of G and, moreover, HG is non-nilpotent (respectively, non-hypercentral), a contradiction. Hence G is a minimal non-nilpotent (respectively, non-hypercentral) group.

Theorem 4.3.18 [43]

Let G be a solvable group. Then G satisfies the minimal condition on non-hypercentral (respectively, non-nilpotent) subgroups if and only if one of the following holds:

(1) G is a hypercentral (respectively, nilpotent) group;

(2) G is a Cernikov group;

(3) G = P ×Q is a group direct product of a hypercentral (respectively, nilpotent) Cernicov p'- group Q and a non-hypercentral (respictivily, non-nilpotent) p-group P which contains a normal HM*-subgroup H of finite index (respictively , HM*- subgroup H of finite index with the nilpotent commutator subgroup H') with the normalizer condition .

Proof:

Let G be a solvable group satisfying Min-N (respectively, Min-ZA). We assume that G is neither nilpotent (respectively, hypercentral) nor a Cernikov group.
Then G contains a subnormal non-nilpotent (respectively, non-hypercentral) sub-group H in which any normal subgroup is nilpotent (respectively, hypercentral).
Furthermore, if $H = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ is a finite subnormal series connecting H to G, then every quotient G_{i+1}/G_i satisfies the minimal condition on subgroups and so it is Cernikov.

If the subgroup H is not locally nilpotent, then it contains a finitely generated non-nilpotent subgroup F. Then $H = H' F$ and the quotient H/H' is cyclic of prime power order, because in other case H is nilpotent (respectively, hypercentral) as product of two nilpotent (respectively, hypercentral) normal subgroups.
So the intersection $H' \cap F$ is a nilpotent subgroup.
Now it is easy to see that F is finite. Since the set of all subgroups containing F satisfies the minimal condition, G is a Cernikov group. This is a contradiction.
Hence H is a locally nilpotent group and therefore by Corollary 4.3.17 H is a minimal non-nilpotent (respectively, non-hypercentral) p-group for some prime p.
As a consequence, G is a locally finite group. By the above argument G is a locally nilpotent group.
To complete the proof it is enough to suppose that G is a p-group and to prove that in this case it contains an HM*-subgroup of finite index satisfying the normalizer condition. This is obvious if $n = 0$ because $G = H$ is a minimal non-nilpotent (respectively, non-hypercentral) group and so G/G' is quasicyclic.
By induction on n, we may suppose that G_{n-1} contains an HM*-group T of finite index. Since G_{n-1} is normal in G, without loss of generality we can assume that T is normal in G. Then the quotient group G/T is Cernikov. If D is a preimage of the finite residual D/T of G/T, then D is an HM*-subgroup of finite index in G.

In view of Lemma 4.3.16 D satisfies the normalizer condition. The proof is complete.

Corollary 4.3.18

Let G be a non-hypercentral (respectively, non-nilpotent) group. Then G satisfies Min-ZA (respectively, Min-N) if and only if G satisfies the normalizer condition (respectively, G satisfies the normalizer condition and G′ is nilpotent).

References

1. Artin.E, **Galois Theory.** Notre Dame: University of Notre Dame Press, 1944.
2. Artin. M, **Algebra.** Englewood Cliffes, N.J: Printice-Hall, 1991.
3. Beidleman. J. C and Spencer A. E, **"The normal index of maximal subgroups in finite groups"**. Illinois J. Math, 16 (1972), 95-101.
4. Berkovich.Y, **"Groups of prime power order"**. Berlin, New york (2) (2008), 516-518.
5. Bewersdorff. J,**Galois Theory for Beginners.** A Historical Perspective. American Mathematical Society. 2006.
6. Bhattacharya. P. and Mukherjee. N, **"A family of maximal subgroups containing the Sylow subgroups and some solvability conditions"**. Archiv Math., 45 (1985), 390-397.
7. Bludov.V, **" locally nilpotent groups with the minimal condition in centralizers"**. Algebra and Logic, Vol 37.No.3, 1998.
8. Burnside.W, **Theory of Groups of Finite Order.** Second eddition.New York: Dover, 1955.
9. Berggren J. L, **" Solvable and supersolvable groups in which every element is conjugate to its inverse"**. Pacific J. Math. Volume 37, Number 1 (1971), 21-27.
10. Dummit. D. S and Foote R. M, **Abstract Algebra** .John Wiley and Sons, 2004.
11. Edgar.D, **Algebraic Equations: An Introduction to the Theories of Lagrange and Galois.** Columbia University Press, 1930.
12. Feit .W and Thompson .J.G,**"Solvability of groups of odd order "**.Pacific J .math.13(1963),775-1029.
13. Fraleigh.J.B, **A First Course in Abstract Algebra (6th Edition).**New York: Wesley ,1967.
14. Garling D.J.H, **A Course in Galois Theory.** Cambridge University Press, (1986)
15. Gorenstein. D.L and Solomon. R .**Mathematical Surveys and Monographs.** United States: American Mathematical Society, 2005.
16. Gruenberg K. W. **"The Engel elements of a soluble group"**, Illinois J. Math. Volume 3, Issue 2 (1959), 151-168.
17. Grillet .P. A. **Graduate Texts in Mathmatics (second edition).** New York: Springer, 2007.

18. Hamblin J. E. **On Solvable Groups Satisfying the Two-Prime Hypothesis.** Ph. D. Thesis, University of Wisconsin, Madison, 2002.

19. Hall. M. **The Theory of Groups.** The Macmillan Company, NewYork, 1960.

20. Hall and G.Higman. **"The p-length of a p-solvable group and reduction theorems for Burnsides problem".** Proc.London Math .Soc, 7(1956), 1-41.

21. Harold M. E .**Galois Theory.** Springer-Verlag. 1984.

22. Haward. S. **"Hypercentral Groups with all subgroups subnormal".** Bulletin of the London mathematical society 1983 15(3):229-234.

23. Herstein I. N.**Topics in Algebra** .New York: Blaisdell, 1964.

24. Hungerford T.W. **Algebra** .New York: Springer, 1974.

25. Holt, D. G and Plesken. W. **Perfect Groups.** Oxford, England: Clarendon Press, 1989.

26. Isaacs .I.M. **Algebra(A Graduate Course).** 1993

27. Isaacs. I. M. **"The P-parts of character degrees in P-solvable groups".** Pacific J. Math. 36 (1971), 677-691.

28. Kurosh .A.G.**The Theory of Groups (English Translation).** New York : Chelsea ,1955.

29. Lang.S.**Algebraic Number Theory.** Berlin, New York: Springer-Verlag,1994.

30. Lang .S ,**Algebra.:** Addison-Wesely, 1993.

31. Lewis. M. L, **"Derived lengths of solvable groups satisfying the one-prime hypothesis III".** Comm. Algebra 29 (2001), 5755-5765.

32. Malcev, A. I, **"Generalized nilpotent algebras and their associated groups".** Mat. Sbornik N.S. **25** (67) (1949): 347–366

33. Manz. O. and Wolf. T. R, **"Representations of Solvable Groups".** Cambridge University Press, Cambridge, 1993. MR 95c:20013

34. Nathan . J , **Basic Algebra I (2nd ed).** W.H. Freeman and Company. 1985.

35. Postnikov. M. M, **Foundations of Galois Theory.** Dover Publications.2004.

36. Rose. J.S, **A Course in Group Theory.** New York: Dover, 1994.

37. Robinson Derek J. S, **A Course in the Theory of Groups** .New york:Springer,1965.

38. *Roseblade . J. E, "**Group rings of polycyclic groups**". J. Pure and Applied Algebra 3 (1973), 307-328.*

39. *Robinson.D.J, **An Introduction to Abstract Algebra** .Berlin: Gmbh &Co.KG, 2003.*

40. *Scott. W.R, **Group Theory**. Dover, 1987.*

41. *Stewart. I, **Galois Theory**. Chapman and Hall. 1989.*

42. *Schenkman, Eugene, **Group Theory**. Krieger, 1975.*

43. *Skaskiv.L.V and Artemovych.O.D, **"Groups with many hypercentral subgroups"**. A Republich Moldova.Matematica, Number2 (57), 2008, pages 106-109.*

44. *Tignol. J.P, **Galois Theory of Algebraic Equations**. World Scientific, 2001.*

45. *William D.Blair and John A.Beachy ,**Abstract Algebra**.Waveland Press,1996*

46. *Wisnesky. R. J, Solvable groups (subsection Metabelian Groups),2005*