Grundlehren der mathematischen Wissenschaften 364
A Series of Comprehensive Studies in Mathematics

Bertram Huppert

Finite Groups I

Springer

Grundlehren der mathematischen Wissenschaften

A Series of Comprehensive Studies in Mathematics

Volume 364

Grundlehren der mathematischen Wissenschaften (subtitled Comprehensive Studies in Mathematics), Springer's first series in higher mathematics, was founded by Richard Courant in 1920. It was conceived as a series of modern textbooks. A number of significant changes appear after World War II. Outwardly, the change was in language: whereas most of the first 100 volumes were published in German, the following volumes are almost all in English. A more important change concerns the contents of the books. The original objective of the Grundlehren had been to lead readers to the principal results and to recent research questions in a single relatively elementary and accessible book. Good examples are van der Waerden's 2-volume Introduction to Algebra or the two famous volumes of Courant and Hilbert on Methods of Mathematical Physics.

Today, it is seldom possible to start at the basics and, in one volume or even two, reach the frontiers of current research. Thus many later volumes are both more specialized and more advanced. Nevertheless, most volumes of the series are meant to be textbooks of a kind, with occasional reference works or pure research monographs. Each book should lead up to current research, without over-emphasizing the author's own interests. Proofs of the major statements should be enunciated, however the presentation should remain expository. Examples of books that fit this description are Maclane's Homology, Siegel & Moser on Celestial Mechanics, Gilbarg & Trudinger on Elliptic PDE of Second Order, Dafermos's Hyperbolic Conservation Laws in Continuum Physics ... Longevity is an important criterion: a GL volume should continue to have an impact over many years. Topics should be of current mathematical relevance, and not too narrow.

The tastes of the editors play a pivotal role in the selection of topics.

Authors are encouraged to follow their individual style, but keep the interests of the reader in mind when presenting their subject. The inclusion of exercises and historical background is encouraged.

The GL series does not strive for systematic coverage of all of mathematics. There are both overlaps between books and gaps. However, a systematic effort is made to cover important areas of current interest in a GL volume when they become ripe for GL-type treatment.

As far as the development of mathematics permits, the direction of GL remains true to the original spirit of Courant. Many of the oldest volumes are popular to this day and some have not been superseded. One should perhaps never advertise a contemporary book as a classic but many recent volumes and many forthcoming volumes will surely earn this attribute through their use by generations of mathematicians.

Bertram Huppert

Finite Groups I

Translated by Christopher A. Schroeder

Springer

Bertram Huppert†

ISSN 0072-7830 ISSN 2196-9701 (electronic)
Grundlehren der mathematischen Wissenschaften
ISBN 978-3-031-87528-1 ISBN 978-3-031-87529-8 (eBook)
https://doi.org/10.1007/978-3-031-87529-8

Mathematics Subject Classification (2020): 20-01, 20-02

Translation from the German language edition: "Endliche Gruppen I" by Bertram Huppert, © Springer-Verlag Berlin Heidelberg 1967. Published by Springer Berlin Heidelberg. All Rights Reserved.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

In honor of Bertram Huppert (*1927–2023*).

Since its publication in 1967, Bertram Huppert's *Endliche Gruppen I* has remained a vital mathematical resource because it is clear, precise and complete. With this in mind, I have aspired to an especially faithful translation. The theorem numbers remain the same, so the German original and this translation can be referenced interchangeably. The only significant change I have made is to update the following notation:

Object	German original	English translation
Group	$\mathfrak{G}$	G
Order of group	g	n or $\lvert G\rvert$
Index of subgroup	$\lvert G : H\rvert$	$[G : H]$
Identity subgroup	$\mathfrak{E}$	1
Group element	G	g
Group identity	E	1
Order of group element	$O(G)$	$\lvert g\rvert$
Ring	$\mathfrak{R}$	R

Open problems that have been resolved by more recent work are updated in the footnotes. Corrections from the errata are incorporated and are also noted in the text. The remaining errors are my own.

I would like to thank Thomas Keller for supervising the translation, Rémi Lodh for his editorial assistance and Gunter Malle for his heroic proofreading of the entire manuscript. I also thank Tim Burness, Bettina Eick, Bob Guralnick, Evgeny Khukhro, Klaus Lux, Gunter Malle, Alexander Moretó, Chris Parker and Gunnar Traustason for their help updating the text. Above all, I am grateful for Professor Huppert's permission to undertake the translation. With his passing, I deeply appreciate this connection to his life and work, and I would be thrilled if this translation enables more readers to spend time in his company.

New York, 10.22.2024 *Christopher A. Schroeder*

Preface

(Jan van Eyck, on several paintings after 1433)

When I began the preliminary work for this book in 1958, it still seemed possible to give a somewhat complete presentation of the structure of finite groups in a single volume. The tempestuous development of the theory since then, of which the bibliography gives an impression, has made this objective impossible. In addition to the foundational material, the present volume contains the theory of nilpotent, p-nilpotent and solvable groups, as well as ordinary representation theory. As recent developments have not focused on these areas at the time of writing, a somewhat complete overview of the state of these topics can be given here. (The theory of formations and Fitting classes, which arose in the few years before publication of this book, could only be discussed in part.) The second and third volumes are planned to contain the theory of subnormal subgroups, a more refined theory of p-length, multiply-transitive permutation groups and several newer applications of character theory. Due to the wealth of results in these areas, it is not possible for us to aspire to a complete treatment.

Several topics were excluded from this volume:

1. A unified treatment of the now well-known series of finite simple groups that follow from the methods of Chevalley would have required considerable prior knowledge of Lie algebras. I restricted myself in Chapter II to the projective and symplectic groups. The simple groups of Mathieu and Suzuki will be discussed in Volume 3.

2. The theory of p-groups of exponent p and the connection between nilpotent groups and Lie rings were not touched upon. This theory and its methods have few connections to current questions regarding the structure of finite groups, and their applications lie largely in the theory of infinite groups.

3. The cohomology theory of finite groups has thus far found its most important application in class field theory and not in the structure theory of finite groups. Therefore, I have developed only as much cohomology theory (dispensing with the functorial description of cohomology groups) that is required to handle the topics covered in this book (extension theory, automorphisms of p-groups, Schur multipliers) in §16 of Chapter I.

Although this book requires no previous exposure to groups, it is intended for readers with a basic knowledge of algebra. Chapter I develops the fundamental principles and elementary tools of group theory in full, although concisely and without motivation. Tools from ring theory, such as the theory of principal ideal domains (Chapter I, §13) and semisimple algebras (Chapter V, §2–§4), are developed in full. In contrast, I occasionally used simple observations about $\mathfrak{p}$-adic fields and algebraic number fields without proof.

I did not attempt to provide exercises consistently throughout the book. In Chapter I, numerous observations and proof variants are offered in the exercises, whereas later chapters are nearly devoid of problems. The results of exercises are rarely referenced in the main text.

Numerous people supported me in the writing of this book. R. Baer, N. Itô, O. H. Kegel and J. Rose read different versions of several chapters closely. N. Blackburn and H. Lüneberg read the complete manuscript. I was able to thoroughly discuss almost every chapter in the manuscript or in the galley proof with W. Gaschütz, F. Gross and J. Neubüser. This led to numerous improvements, including correcting errors and improving clarity. I thank N. Blackburn, R. Carter, E. Dade, W. Gaschütz, P. Hall, P. Roquette, D. Taunt, J. G. Thompson and H. Wielandt for unpublished results, proofs or examples. A. Brandis, K. Doerk, W. Gaschütz, K. D. Graf, F. Gross, B. Klaiber, J. Neubüser and A. Schlette helped with the lengthy corrections. I deeply thank all of the above for their assistance. In addition, I have to thank the following institutions for the opportunity to work on this book and for fruitful discussions with colleagues: the British Council for a stay in Manchester 1958/59; the University of Illinois in Urbana for a guest professor position 1963/64; the California Institute of Technology in Pasadena for a guest professor position in Fall 1964. Finally, I thank the publisher for generously accepting the many changes that I requested during proofreading and for the excellent quality of the production of this book.

My very special thanks go to my teacher Helmut Wielandt. His lectures, which introduced me to the theory of finite groups, were often the starting point for writing sections and sometimes entire chapters of this book. They have frequently influenced the content and style of my presentation.

Mainz, 9.15.1967 *Bertram Huppert*

Contents

Chapter I
Foundations

We begin Chapter I by developing in a concise but complete fashion the basic concepts of group theory (§1–§4). These sections contain numerous elementary theorems and lemmas that will be used repeatedly later on; this applies in particular to the product formula in Lemma 2.12 a), the Dedekind identity in Lemma 2.12 c), Lemma 2.13 and Theorems 4.5, 4.8 and 4.9. The representations of a group as a permutation group (§6) yield the fundamental Sylow theorems (§7) as an important consequence. Several elementary criteria for solvability will be deduced from Sylow's theorems in §8.

The remaining sections of Chapter I are dedicated in large part to various constructions in finite group theory: direct products (§9 and §12), extension theory (§14) and wreath products (§15). We describe two constructions that are derived from the direct product, namely the direct product with identified central subgroups (also known as the central product) in Theorem 9.10 and the direct product with identified factor groups (also known as the subdirect product) in Theorem 9.11. We return multiple times to the important question of when a given group can be built from simpler groups by one of these constructions. In this way, we obtain in §13 the fundamental theorem of finitely generated abelian groups as a special case of the theory of modules over principal ideal domains. The Zassenhaus theorem (§18), which provides sufficient conditions for an extension to be a semidirect product, is of fundamental importance for the entire theory of finite groups. In §16, we treat the theory of group cohomology only to the extent needed for a further study of p-group automorphisms (Chapter III, §19) and Schur multipliers (Chapter V, §23).

In several places, it was ideal or even necessary to remove our restriction to finite groups. The theory of direct products, composition series and the direct decomposition of groups with operators and of modules (§9–§13) is developed so that many of the theorems about modules required in representation theory (Chapter V) can be deduced as special cases. Finally, it was unavoidable to discuss free groups in order to develop the description of groups by generators and relations in §19.

We recommend that the inexperienced reader restrict themselves to §1–§9 and §18 on a first reading; a proof of Theorem 17.5 without the use of cohomology theory is sketched in Exercise 70.

B. Huppert, *Finite Groups I*, Grundlehren der mathematischen Wissenschaften 364,
https://doi.org/10.1007/978-3-031-87529-8_1

1 The group axioms

Group Axioms 1.1. *A nonempty set G is called a group if the following conditions are satisfied:*

a) *To every ordered pair (a, b) of elements $a, b \in G$ there is assigned a unique element $c \in G$. We write $c = ab$ and call c the product of a and b.*

b) *The associative property $(ab)c = a(bc)$ holds for all $a, b, c \in G$.*

c) *There exists an element $e \in G$ with the property that $ea = a$ for all $a \in G$. We call e an identity element of G. (We will show that there is only one such element, and we will then denote it by* 1.)

d) *For every element $a \in G$, there exists an element $b \in G$ such that $ba = e$.*

We first derive a few simple corollaries from the axioms.

Corollary 1.2. *The formation of products in a group is independent of the parentheses; more exactly:*

For arbitrary elements $a_1, a_2, \ldots$ of G we define the subsets $\mathscr{P}_k(a_1, \ldots, a_k)$ of G recursively by

$$\mathscr{P}_1(a_1) = \{a_1\}, \quad \mathscr{P}_2(a_1, a_2) = \{a_1 a_2\}$$

and

$$\mathscr{P}_k(a_1, \ldots, a_k) = \{xy \mid x \in \mathscr{P}_m(a_1, \ldots, a_m), y \in \mathscr{P}_n(a_{m+1}, \ldots, a_{m+n}), k = m + n\}.$$

(The elements of $\mathscr{P}_k(a_1, \ldots, a_k)$ are therefore the products $a_1 \cdots a_k$ with all possible meaningful parentheses.) We claim that the subset $\mathscr{P}_k(a_1, \ldots, a_k)$ contains exactly one element for every k. We denote this element by $a_1 \cdots a_k$.

Proof. We prove by induction on k that every $\mathscr{P}_k(a_1, \ldots, a_k)$ contains exactly one element. For $k = 1, 2$ this is clear from the definition. Let $k \geq 3$, and let $g = xy \in \mathscr{P}_k(a_1, \ldots, a_k)$ with $x \in \mathscr{P}_m(a_1, \ldots, a_m)$ and $y \in \mathscr{P}_n(a_{m+1}, \ldots, a_k)$. By our induction hypothesis, $x = a_1 z$ with $z = a_2 \cdots a_m$; if $m = 1$, $z = e$ is omitted. Using Group Axiom 1.1 b), we have

$$g = xy = (a_1 z)y = a_1(zy).$$

It then follows by induction that $zy \in \mathscr{P}_{k-1}(a_2, \ldots, a_k) = \{a_2 \cdots a_k\}$, and we are done. □

Corollary 1.3.

a) *If e is an identity element of the group G, then $ae = a$ for all $a \in G$.*

b) *If $ba = e$, then $ab = e$.*

c) *If $ax = ay$ or $xa = ya$, then $x = y$.*

Proof. a) By the Group Axiom 1.1 d), there exist elements $x, y \in G$ such that $xa = e$ and $yx = e$. It follows that

$$ye = y(xa) = (yx)a = ea = a.$$

Since $ee = e$, we obtain

$$a = ye = y(ee) = (ye)e = ae,$$

as claimed.

b) By the Group Axiom 1.1 d), there exists some $x \in G$ such that $xb = e$. Using Corollary 1.2, we have

$$\begin{aligned} e = xb = xeb = x(ba)b \\ = (xb)(ab) = e(ab) = ab. \end{aligned}$$

c) Let $ba = e$. Then we also have $ab = e$ and

$$x = ex = (ba)x = b(ax) = b(ay) = (ba)y = ey = y,$$

and similarly

$$x = xe = x(ab) = (xa)b = (ya)b = y(ab) = ye = y. \qquad \square$$

Corollary 1.4. *Let G be a group. For each pair of elements $a, b \in G$, there exists a unique element $x \in G$ such that $ax = b$. Likewise, there exists a unique element $y \in G$ such that $ya = b$.*

Proof. Let c be an element such that $ca = e$, which exists by the Group Axiom 1.1 d). By Corollary 1.3 b), we also have $ac = e$. Then $x = cb$ is an element with the desired property, for we have

$$ax = a(cb) = (ac)b = eb = b.$$

If x_1 and x_2 are elements satisfying $ax_1 = ax_2 = b$, then it follows immediately from Corollary 1.3 c) that $x_1 = x_2$. $\square$

It follows directly from Corollary 1.4 that G possesses a unique identity element, which we denote by 1 in the rest of the text. Furthermore, we have the following:

Corollary 1.5.

a) *For each $a \in G$, there is a unique element $x \in G$ such that $xa = 1$. Then $ax = 1$, as well. We call x the inverse of a and write $x = a^{-1}$.*

b) *We have $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a$.*

Proof. Part a) is a consequence of Corollary 1.4 and Corollary 1.3 b). Then part b) follows by Corollary 1.2 and the uniqueness of inverse elements since

$$(b^{-1}a^{-1})(ab) = (b^{-1}(a^{-1}a))b = b^{-1}b = 1, \quad aa^{-1} = 1. \qquad \square$$

Definition 1.6. We define the powers of the group element $g \in G$ recursively by $g^0 = 1$ and $g^{i+1} = g^i g$; for $i < 0$ we define $g^i = (g^{-i})^{-1}$. It is easy to see that $g^{i+j} = g^i g^j$ for all integers i and j.

Definition 1.7. We denote the cardinality of a set M by $|M|$. If G is a group, we refer to $|G|$ as the order of G. We say that G is a finite group if $|G|$ is finite.

Oftentimes, we are not interested in the nature of the specific elements of a group, but rather only in the algebraic relationships between elements. In order to allow for this, we introduce the following equivalence relation:

Definition 1.8. Two groups G_1 and G_2 are said to be isomorphic if there is a bijective map π from G_1 to G_2 such that

$$(gh)^\pi = g^\pi h^\pi$$

for all $g, h \in G_1$. In this case, we write $G_1 \cong G_2$. Isomorphism is clearly an equivalence relation. We understand group properties to be the properties satisfied by G and every group isomorphic to G.

We note the following:

Corollary 1.9. *If π is an isomorphism from G_1 to G_2 and 1_i is the identity element of G_i, then $1_1^\pi = 1_2$. Furthermore, we have $(g^{-1})^\pi = (g^\pi)^{-1}$ for all $g \in G_1$.*

Proof. The claim $1_1^\pi = 1_2$ follows from the fact that, for all $g \in G_1$,

$$1_1^\pi g^\pi = (1_1 g)^\pi = g^\pi$$

together with the uniqueness guaranteed by Corollary 1.4. It follows from

$$(g^{-1})^\pi g^\pi = (g^{-1} g)^\pi = 1_1^\pi = 1_2$$

that $(g^{-1})^\pi = (g^\pi)^{-1}$. □

Definition 1.10. A group G is called abelian (or commutative) if for all $a, b \in G$ we have $ab = ba$. In this case, every product $a_1 \cdots a_n$ with $a_i \in G$ is independent of the ordering of the a_i.

2 Subgroups

Definition 2.1. A subset U of the group G is called a subgroup of G whenever U is a group with respect to the product defined on G. This means:

If $u_1, u_2 \in U$, then $u_1 u_2 \in U$; if $u \in U$, then $u^{-1} \in U$; the identity element 1 of G lies in U. (Of course, 1 is then the identity element of U.)

We write $U \leq G$ whenever U is a subgroup of G; if U is a proper subgroup of G, then we write $U < G$. Every group contains the subgroup $\{1\}$ consisting solely of the identity element. In an abuse of notation, we will denote this group by 1. We occasionally refer to the groups 1 and G as the trivial subgroups of G.

The following is often useful:

Lemma 2.2. *If U is a finite subset of the group G and $u_1u_2 \in U$ for all $u_1, u_2 \in U$, then U is a subgroup of G.*

Proof. Let u_0 be an arbitrary element of U. The products uu_0 with $u \in U$ are distinct by Corollary 1.3 c), so they yield exactly $|U|$ elements of U. Hence, $U = \{uu_0 \mid u \in U\}$. In particular, there is a $u_1 \in U$ such that $u_1u_0 = u_0 = 1u_0$. Then $u_1 = 1$ by Corollary 1.3 c). Furthermore, there exists some $u_2 \in U$ such that $u_2u_0 = 1$, and therefore $u_2 = (u_0)^{-1}$ lies in U as well. □

Theorem 2.3. *If U_i is a subgroup of G for every i in an index set I, then the intersection $\bigcap_{i \in I} U_i$ is a subgroup of G.*

Proof. If a and b lie in all subgroups U_i, then a^{-1} and ab lie in all U_i, and so also in $\bigcap_{i \in I} U_i$. Clearly, 1 also lies in the intersection. □

Definition 2.4. Let M be a subset of the group G. We denote by $\langle M \rangle$ the intersection of all subgroups of G that contain M and refer to it as the subgroup of G generated by M. It is clear that $\langle M \rangle$ is the smallest subgroup of G that contains the set M. If we define $M^{-1} = \{m^{-1} \mid m \in M\}$, then we have

$$\langle M \rangle = \{1, x_1 \cdots x_s \mid x_i \in M \cup M^{-1},\ s = 1, 2, \dots\}.$$

If $M = \{a, b, \dots\}$, we also write $\langle M \rangle = \langle a, b, \dots \rangle$. If $G = \langle M \rangle$, then we say that M is a generating set for G. A group generated by one element is called cyclic. Defining $a^0 = 1$, the group $\langle a \rangle$ then consists exactly of the elements a^i with $i = 0, \pm 1, \pm 2, \dots$, which are not necessarily all distinct.

Theorem 2.5. *Let U be a subgroup of G. The sets*

$$gU = \{gu \mid u \in U\} \quad (\textit{with } g \in G)$$

are called the left cosets of U in G. For all $g, h \in G$, we have either $gU \cap hU = \emptyset$ or $gU = hU$. The group G is the disjoint union of the distinct left cosets gU. If a set R contains exactly one element of every left coset of U, then we say R is a set of left coset representatives (or a left transversal) for U in G. We refer to the partition

$$G = \bigcup_{r \in R} rU$$

as the decomposition of G into left cosets of U. All cosets of U have the same cardinality $|U|$. We refer to the cardinality $|R|$ of R as the index of U in G and denote it by $[G : U]$. (Analogous statements hold for the right cosets Ug.)

Proof. We define an equivalence relation on the elements of G by $x \sim y$ if $x^{-1}y \in U$. This is actually an equivalence relation:

The relation is reflexive since $x^{-1}x = 1 \in U$ implies $x \sim x$. If $x \sim y$, then $x^{-1}y \in U$. It follows that $(x^{-1}y)^{-1} = y^{-1}x \in U$ and so $y \sim x$, which means the relation is symmetric. Finally, if $x \sim y$ and $y \sim z$, then $x^{-1}y \in U$ and $y^{-1}z \in U$, and we deduce that $x^{-1}z = (x^{-1}y)(y^{-1}z) \in U$. So $x \sim z$ and the relation is transitive.

It is well known that we can now write G as the disjoint union of the equivalence classes of our relation. The class containing $g \in G$ is clearly the left coset gU. The other claims are now clear. □

Theorem 2.6.

a) *Let U be a subgroup of G. If $G = \bigcup_{r \in R} Ur$ is the decomposition of G into right cosets of U, then $G = \bigcup_{r \in R} r^{-1}U$ is the decomposition of G into left cosets of U.*
(*In particular, we need not distinguish between a left and right index of U in G.*)

b) *If $G = \bigcup_{r \in R} Ur$ is the decomposition of G into right cosets of the subgroup U and $U = \bigcup_{s \in S} Vs$ is the decomposition of U into right cosets of V, then $G = \bigcup_{s \in S, r \in R} Vsr$ is the decomposition of G into rights cosets of V. In particular, we have $[G : V] = [G : U][U : V]$.*

Proof. a) The map α defined by $g^\alpha = g^{-1}$ is a bijective map from G to itself, and $(Ur)^\alpha = r^{-1}U$.

b) If $Vs_1r_1 = Vs_2r_2$, then by multiplying on the left by U we have $Ur_1 = Ur_2$. So $r_1 = r_2$, and then $s_1 = s_2$. It is trivial that $G = \bigcup_{s \in S, r \in R} Vsr$. □

The following theorem of Lagrange is fundamental to the theory of finite groups. It brings an arithmetical element into the theory.

Main Theorem 2.7 (Lagrange). *Let G be a finite group and U a subgroup of G. Then $|G| = |U|[G : U]$. In particular, the order and index of a subgroup of a finite group are divisors of the group order.*

Proof. This is the special case $V = 1$ of Theorem 2.6 b). □

Definition 2.8. Let g be an element of the group G. The smallest natural number n such that $g^n = 1$ is called the order $|g|$ of g; if there is no such natural number, we write $|g| = \infty$. The least common multiple of the orders $|g|$ of the elements $g \in G$, if it exists, is called the exponent $\exp G$ of G.

Theorem 2.9. *Let G be a group. Suppose $g \in G$ has finite order $|g| = n < \infty$.*

a) *If $g^m = 1$, then $n \mid m$.*

b) *We have $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ and $|\langle g \rangle| = |g| = n$. In particular, if G is a finite group, then $|g|$ is a divisor of $|G|$.*

c) *We have $|g^k| = n/(n, k)$ for every integer k.*

Proof. a) Let $m = nr + s$ with $0 \le s < n$. Then

$$1 = g^m = g^{nr+s} = (g^n)^r g^s = g^s.$$

The minimality of $n = |g|$ then forces $s = 0$, so that $n \mid m$.

b) Let $i+j = nr+s$ with $0 \le s < n$. Then $g^{i+j} = g^s$. The finite set $\{g^s \mid 0 \le s < n\}$ is then a group by Lemma 2.2, so it is exactly $\langle g \rangle$. Assume that $g^i = g^j$ with $0 \le i \le j < n$. Then $g^{j-i} = 1$. It follows from a) that $n \mid j - i$, so $i = j$. Hence, the g^i with $0 \le i \le n - 1$ are pairwise distinct. Since $g^{nk+r} = g^r$, we have

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}.$$

It follows from Theorem 2.7 that $|g| = |\langle g \rangle|$ is a divisor of $|G|$.

c) Since $n \mid k\frac{n}{(n,k)}$, we have that

$$g^{k\frac{n}{(n,k)}} = 1.$$

Then a) implies that $|g^k|$ divides $\frac{n}{(n,k)}$. Conversely, it follows from $g^{kt} = 1$ and a) that $n \mid kt$, so $\frac{n}{(n,k)} \mid t$. Therefore, $|g^k| = \frac{n}{(n,k)}$. □

Theorem 2.10. *Every group of prime order is cyclic.*

Proof. Let $|G| = p$ be a prime number, and let $g \in G$ be distinct from the identity. We set $U = \langle g \rangle$. Then $|U|$ is a divisor of $|G| = p$ by Theorem 2.7. Since $1 < |U|$ it follows that $|U| = |G|$, so $U = G$ and G is cyclic. □

Theorem 2.10 is the first in a long series of theorems that deduce statements about G from the prime factorization of $|G|$.

Definition 2.11. Let A and B be subsets of the group G. We define

$$AB = \{ab \mid a \in A,\ b \in B\}.$$

We emphasize that AB is not necessarily a subgroup of G, even if A and B are subgroups of G! (See §5, Exercise 18.)

The following is often useful:

Lemma 2.12. *Let A and B be subgroups of G.*

a) *Let $A = \bigcup_{r \in R} r(A \cap B)$ be the decomposition of A into cosets of $A \cap B$. Then $AB = \bigcup_{r \in R} rB$ is a disjoint union. In particular, if A and B are finite, then*

$$|AB| = \frac{|A||B|}{|A \cap B|}.$$

b) *AB is a subgroup of G if and only if $AB = BA$.*

c) *(Dedekind identity) If $A \le C \le G$ and $C \subseteq AB$, then $C = AB \cap C = A(B \cap C)$.*

Proof. a) Clearly, $AB = \bigcup_{r \in R} rB$. We show that the union is disjoint. Assume that $rB \cap r'B \neq \emptyset$. Then there exist elements $b, b' \in B$ with $rb = r'b'$. Since $R \subseteq A$, it follows that

$$(r')^{-1}r = b'b^{-1} \in A \cap B,$$

so $r = r'$.

b) First assume that AB is a subgroup of G. Then

$$\begin{aligned} AB &= \{ab \mid a \in A,\ b \in B\} = \{(ab)^{-1} \mid a \in A,\ b \in B\} \\ &= \{b^{-1}a^{-1} \mid b \in B, a \in A\} = BA. \end{aligned}$$

Conversely, if $AB = BA$ then every product ba with $a \in A$ and $b \in B$ can be written as $ba = a'b'$ with $a' \in A$ and $b' \in B$.

For elements $a_i \in A$ and $b_i \in B$ $(i = 1, 2)$, it follows that

$$(a_1b_1)(a_2b_2) = (a_1a_2')(b_1'b_2) \in AB$$

and

$$(ab)^{-1} = b^{-1}a^{-1} = (a^{-1})'(b^{-1})' \in AB.$$

So AB is a subgroup of G.

c) Let $c \in C$. Since $C \subseteq AB$, $c = ab$ for some $a \in A$, $b \in B$. Since $A \leq C$, $b = a^{-1}c \in B \cap C$, so $C \subseteq A(B \cap C)$. The reverse inclusion $A(B \cap C) \subseteq C$ is trivial as the group C contains A and $B \cap C$, so C contains their product. □

Lemma 2.13. *Let A and B be subgroups of G with finite index. Then:*

a) $[G : A \cap B] \leq [G : A][G : B]$.

b) *If $[G : A]$ and $[G : B]$ are coprime, then $[G : A \cap B] = [G : A][G : B]$. If in addition G is finite, then $G = AB$.*

Proof. a) Let d be the number of left cosets of B in G that lie in AB. By Lemma 2.12 a), we have $[A : A \cap B] = d \leq [G : B]$. Then by Theorem 2.6 b),

$$[G : A \cap B] = [G : A][A : A \cap B] \leq [G : A][G : B].$$

b) Since $[G : A]$ divides $[G : A \cap B]$, $[G : B]$ divides $[G : A \cap B]$ and $([G : A], [G : B]) = 1$, we have that $[G : A][G : B]$ is a divisor of $[G : A \cap B]$. It therefore follows from a) that $[G : A \cap B] = [G : A][G : B]$. If G is finite, then Lemma 2.12 a) implies that

$$|AB| = \frac{|A||B|}{|A \cap B|} = |G|,$$

and therefore $G = AB$. □

Lemma 2.14. *For all $a, g \in G$, we define $g^a = a^{-1}ga$. We call the map $g \mapsto g^a$ conjugation by a. The following identities hold:*
(1) $g^{ab} = (g^a)^b$
(2) $(gh)^a = g^a h^a$.
(3) $(g^a)^{-1} = (g^{-1})^a$.
We define g^{a+b} to be $g^{a+b} = g^a g^b$. However, it is important to note that $g^{a+b} \neq g^{b+a}$ in general since the elements g^a and g^b do not necessarily commute. In any case, it is always true that:
(4) $g^{ab+ac} = (g^a)^{b+c}$ *and*
(5) $g^{ba+ca} = (g^{b+c})^a$.

Proof. Identity (1) follows from

$$g^{ab} = (ab)^{-1}g(ab) = b^{-1}(a^{-1}ga)b = (g^a)^b$$

and (2) from

$$(gh)^a = a^{-1}gha = (a^{-1}ga)(a^{-1}ha) = g^a h^a.$$

The equality

$$(g^a)^{-1} = (a^{-1}ga)^{-1} = a^{-1}g^{-1}a = (g^{-1})^a$$

gives us (3). The equalities

$$g^{ab+ac} = g^{ab}g^{ac} = (g^a)^b(g^a)^c = (g^a)^{b+c}$$

and

$$g^{ba+ca} = g^{ba}g^{ca} = (g^b g^c)^a = (g^{b+c})^a$$

give (4) and (5). □

Definition 2.15. If M is a nonempty subset of G and $g \in G$, then we define

$$M^g = \{m^g \mid m \in M\}.$$

We refer to the sets M^g as the conjugates of M in G.

If U is a subgroup of G, then U^g is a subgroup of G isomorphic to U: The group properties of U^g follow from Lemma 2.14 (2) and (3). The map π from U onto U^g defined by $u^\pi = u^g$, which is inverted by the map α defined by $(u^g)^\alpha = (u^g)^{g^{-1}} = u$, is an isomorphism from U to U^g by Lemma 2.14 (2).

A special case of Definition 2.15 is particularly important:

Theorem 2.16. *Let $M = \{m\}$ be a set containing a single element. Then we call the set consisting of the elements that are G-conjugate to m, namely $\{m^g \mid g \in G\}$, the conjugacy class of m in G. The conjugacy classes are the equivalence classes of the following equivalence relation:*

We say $x \sim y$ if there exists some $g \in G$ such that $x^g = y$. If G is finite, then the partition of G into its conjugacy classes gives rise to a disjoint union

$$G = \bigcup_{i=1}^{h} K_i$$

and the equation

$$|G| = \sum_{i=1}^{h} |K_i| \quad (\textit{the so-called class equation}),$$

where the K_i are the distinct conjugacy classes of G. We refer to the number h of conjugacy classes as the class number of G.

Proof. We only need to show that the given relation is an equivalence relation. It follows from $x^1 = x$ that $x \sim x$. If $x \sim y$, then $x^g = y$ for some $g \in G$, and so $y^{g^{-1}} = x$ implies $y \sim x$; so the relation is symmetric. Finally, if $x \sim y$ and $y \sim z$, then

$$x^a = y \quad \text{and} \quad y^b = z$$

for suitable $a, b \in G$. Then by Lemma 2.14 (1), we have

$$x^{ab} = (x^a)^b = y^b = z,$$

so $x \sim z$. □

Definition 2.17.

a) Let M be a subset of G. Then $\mathbf{N}_G(M) = \{g \in G \mid M^g = M\}$ is called the normalizer of M in G. Clearly, $\mathbf{N}_G(M)$ is a subgroup of G. If U is a subgroup of G, then $U \leq \mathbf{N}_G(U)$. Note that $\mathbf{N}_G(M^x) = \mathbf{N}_G(M)^x$ for all $x \in G$.

b) The set $\mathbf{C}_G(M) = \{g \in G \mid gm = mg \text{ for all } m \in M\}$ is called the centralizer of M in G. Clearly, $\mathbf{C}_G(M)$ is a subgroup of G and $\mathbf{C}_G(M) \leq \mathbf{N}_G(M)$. If U is an abelian subgroup of G, then $U \leq \mathbf{C}_G(U)$.

c) We define $\mathbf{C}_G(G) = \mathbf{Z}(G)$ and call this the center of G. The center $\mathbf{Z}(G)$ of G consists of the elements of G that commute with all the elements of G.

Theorem 2.18. *The index $[G : \mathbf{N}_G(M)]$ is the number of distinct conjugates of the set M in G.*

Proof. If $x = ny$ with $n \in \mathbf{N}_G(M)$, then

$$M^x = M^{ny} = M^y.$$

Conversely, if $M^x = M^y$, then $M^{xy^{-1}} = M$. So $xy^{-1} \in \mathbf{N}_G(M)$ and then $\mathbf{N}_G(M)x = \mathbf{N}_G(M)y$. We conclude that a right coset of $\mathbf{N}_G(M)$ gives rise to exactly one conjugate of M, and distinct cosets give rise to distinct conjugates. □

Theorem 2.19. *Let U and V be subgroups of G. The double cosets of G with respect to U and V are the sets*

$$UgV = \{ugv \mid u \in U,\ v \in V\} \quad (\textit{with } g \in G).$$

If $UgV \cap UhV \neq \emptyset$, then $UgV = UhV$. So the double cosets give rise to a partition of G. If G is finite, then

$$G = \bigcup_{i=1}^{n} Ug_iV \quad (\textit{disjoint})$$

and

$$|G| = \sum_{i=1}^{n} \frac{|U||V|}{|U^{g_i} \cap V|}.$$

Proof. Assume that $u_1gv_1 = u_2hv_2$ with $u_i \in U$ and $v_i \in V$ $(i = 1, 2)$. Then it follows that

$$g = u_1^{-1}u_2hv_2v_1^{-1}$$

and therefore

$$UgV = U(u_1^{-1}u_2hv_2v_1^{-1})V = UhV.$$

So the given union is certainly disjoint. Since $|UgV| = |g^{-1}UgV|$ and $|U^g| = |U|$, the claim regarding the orders follows from Lemma 2.12 a) because

$$|UgV| = |U^gV| = \frac{|U^g||V|}{|U^g \cap V|} = \frac{|U||V|}{|U^g \cap V|}. \qquad \square$$

Theorem 2.20. *Let $G = \langle g \rangle$ be a cyclic group of order n. For every divisor d of n, there exists exactly one subgroup of G of order d; namely, $\langle g^k \rangle$ with $k = \frac{n}{d}$.*

Proof. By Theorem 2.9 c), we have $|\langle g^k \rangle| = \frac{n}{k} = d$. So $U = \langle g^k \rangle$ is indeed a subgroup of G of order d.

Let $V < G$ and $|V| = d$. Let t be the greatest common divisor of all a_i with $0 \leq a_i < n$ and $g^{a_i} \in V$. It is well known that there exist integers b_i $(i = 1, \ldots, m)$ such that $t = \sum_{i=1}^{m} a_ib_i$. It follows that

$$g^t = \prod_{i=1}^{m} g^{a_ib_i} \in V.$$

If $g^a \in V$, then $t \mid a$ and therefore $g^a \in \langle g^t \rangle$. We conclude that $V = \langle g^t \rangle$. It follows from Theorem 2.9 c) that $d = |V| = \frac{n}{(n,t)}$. Let $t = (n, t)s$. Then $t = \frac{ns}{d} = ks$ and $V = \langle g^t \rangle \leq \langle g^k \rangle = U$. So $U = V$, and U is the unique subgroup of G of order d. $\square$

Exercises

1) If $g^2 = 1$ for all group elements $g \in G$, then G is abelian.
2) (Itô, Szép [286]) Let $H < G$, and let $H_1, \ldots, H_n$ be the distinct conjugates of H in G, written in some arbitrary but fixed order. Show that

$$\langle H_1, \ldots, H_n \rangle = \{h_1 h_2 \cdots h_n \mid h_i \in H_i\}.$$

(Hint: To every decomposition $x = h_{i_1} \cdots h_{i_s}$ with $h_{i_j} \in H_{i_j}$, assign the s-tuple $m(x) = (i_1, \ldots, i_s)$. Order the $m(x)$ according to their length s and those of equal length lexicographically. Suppose there is an x that cannot be written in the desired form $h_1 \cdots h_n$ and consider a decomposition of x with $m(x)$ minimal.)
3) Let A and B be subgroups of G. Then $A \cup B$ is a subgroup of G if and only if $A \leq B$ or $B \leq A$.
4) If U is a proper subgroup of the finite group G, then the union $\bigcup_{g \in G} U^g$ of all conjugates of U in G is always a proper subset of G.
5) Let U and V be subgroups of G, and suppose $Ug = Vh$ for elements $g, h \in G$. Then $U = V$.
6) Let $a, b \in G$ with $(|a|, |b|) = 1$ and $ab = ba$. Then $|ab| = |a||b|$, and the group $\langle a, b \rangle$ is cyclic and generated by ab.

3 Normal subgroups, factor groups and homomorphisms

Definition 3.1. A subgroup N of G is called a normal subgroup of G (sometimes also called an invariant subgroup) if $N^g \leq N$ for all $g \in G$. In this case, we write $N \trianglelefteq G$, or $N \lhd G$ if N is distinct from G. Every group G contains the trivial normal subgroups G and 1. If the only normal subgroups of G are 1 and G, then G is said to be simple. Clearly, every group of prime order is simple.

Theorem 3.2. *Let N be a subgroup of G. The following are equivalent:*
a) $N \trianglelefteq G$.
b) $N^g = N$ *for all* $g \in G$.
c) $gN = Ng$ *for all* $g \in G$.
d) *Every left coset of N is a right coset of N.*

Proof. a) $\Rightarrow$ b): We have for all $g \in G$ that $N^g \leq N$ and $N^{g^{-1}} \leq N$. Consequently,

$$N = (N^{g^{-1}})^g \leq N^g.$$

So $N^g = N$.

b) $\Rightarrow$ c): We have

$$gN = g(N^g) = g(g^{-1}Ng) = Ng.$$

c) $\Rightarrow$ d): This is trivial.
d) $\Rightarrow$ a): For all $g \in G$, there exists by assumption some $g^* \in G$ such that

$$gN = Ng^*.$$

So we have $1 \in gNg^{-1} = Ng^*g^{-1}$. It follows that

$$N \leq Ng^*g^{-1} = gNg^{-1},$$

and thus $N \trianglelefteq G$. □

Remark 3.3. If N is a subgroup of G with $[G : N] = 2$, then $N \lhd G$.

Proof. For every $g \in G - N$, we have

$$G = N \cup gN = N \cup Ng.$$

Therefore, $gN = G - N = Ng$ and then $N \lhd G$ by Theorem 3.2. □

Theorem 3.4. *A subgroup N of G is normal in G if and only if the assignment*

$$(gN)(hN) = ghN$$

on the set of left cosets of N in G defines a multiplication. With this multiplication, the cosets form a group.

Proof. a) Assume that the above definition of the product of two cosets of N is well defined; that is, it does not depend on g and h, but rather only on the cosets gN and hN. For $g' = gn$ with $n \in N$, we must then have

$$ghN = g'hN = gnhN.$$

This forces $h^{-1}nh \in N$ for all $n \in N$ and $h \in G$. We therefore have $N^h \leq N$ for all $h \in G$. So N is a normal subgroup of G.

b) Let N be a normal subgroup of G and $n_i \in N$ $(i = 1, 2)$. Since

$$gn_1hn_2 = ghn_1^h n_2 \in ghN,$$

the multiplication defined on cosets of N by $(gN)(hN) = ghN$ is well defined. It is certainly associative since the multiplication of group elements is associative. Then we have $(gN)N = gN$ and $(g^{-1}N)(gN) = N$. Therefore, N is the identity element of the group constructed from cosets and $g^{-1}N$ is the inverse of gN. □

(If $N \trianglelefteq G$, then one can also understand the equality $(gN)(hN) = ghN$ in the sense of Definition 2.11 as

$$(gN)(hN) = \{xy \mid x \in gN,\ y \in hN\}$$

since $gn_1hn_2 = ghn_1^h n_2 \in ghN$ for $n_i \in N$.)

Definition 3.5. If N is a normal subgroup of G, then the group constructed from the cosets of N with respect to the multiplication

$$(gN)(hN) = ghN$$

is called the factor group (or quotient group) of G by N, written G/N. Clearly, $|G/N| = [G : N]$.

Definition 3.6.

a) A map π from the group G to the group H is called a homomorphism from G to H if for all $g, g' \in G$ we have

$$(gg')^\pi = g^\pi (g')^\pi.$$

We define

$$G^\pi = \{g^\pi \mid g \in G\}$$

and call G^π the image of G under π.

b) A homomorphism π from G to H is called an epimorphism if π is a map from G onto H; that is, if $H = G^\pi$.

c) A homomorphism π from G to H is called a monomorphism if π is a bijection from G to G^π.

d) A homomorphism from G to G is called an endomorphism of G.

Remark 3.7. Let π be a homomorphism from G to H.

a) If 1 is the identity element of G, then 1^π is the identity element of H.

b) For all $g \in G$, $(g^{-1})^\pi = (g^\pi)^{-1}$.

c) $G^\pi = \{g^\pi \mid g \in G\}$ is a subgroup of H.

d) If M is a generating set for G, then the homomorphism π is uniquely determined by the values of m^π for all $m \in M$.

Proof. The claims a) and b) follow immediately from

$$g^\pi = (1g)^\pi = 1^\pi g^\pi$$

and

$$1^\pi = (g^{-1}g)^\pi = (g^{-1})^\pi g^\pi.$$

Since $g^\pi g'^\pi = (gg')^\pi$ and $(g^\pi)^{-1} = (g^{-1})^\pi$, it follows that $G^\pi \leq H$. If $g = m_1^{a_1} \cdots m_s^{a_s}$ with $m_i \in M$ and $a_i = \pm 1$, then $g^\pi = (m_1^\pi)^{a_1} \cdots (m_s^\pi)^{a_s}$. □

In what follows, we will denote the identity element of any group by 1.

Homomorphism Theorem 3.8.

a) *If K is a normal subgroup of G, then the map α defined by $g^\alpha = gK$ is an epimorphism from G onto G/K. We call α the natural homomorphism from G onto G/K.*

b) *Let π be a homomorphism from G to H. Let*

$$K = \{g \in G \mid g^\pi = 1\}.$$

We call K the kernel $\ker \pi$ *of π. Then K is a normal subgroup of G, and there is a monomorphism φ from G/K to H with $\alpha\varphi = \pi$. In particular, we have*

$$G/K \cong G^\pi.$$

Proof. a) Since

$$(gg')^\alpha = (gg')K = (gK)(g'K) = g^\alpha g'^\alpha,$$

the map α is an epimorphism from G onto G/K.

b) If $k \in K$, then it follows from $k^\pi = 1$ that

$$(g^{-1}kg)^\pi = (g^\pi)^{-1}k^\pi g^\pi = 1,$$

so k^g is also in K. Hence, $K^g \subseteq K$. If $k, k' \in K$, then

$$(kk')^\pi = k^\pi k'^\pi = 1$$

and

$$(k^{-1})^\pi = (k^\pi)^{-1} = 1.$$

So $kk' \in K$ and $k^{-1} \in K$, which means K is a subgroup of G. Hence, K is a normal subgroup of G.

Consider the map φ from G/K to H defined by $(gK)^\varphi = g^\pi$. If $gK = g'K$, then $g = g'k$ for some $k \in K$ and therefore

$$g^\pi = g'^\pi k^\pi = g'^\pi.$$

So φ is well defined. Since

$$((gK)(g'K))^\varphi = (gg'K)^\varphi = (gg')^\pi = g^\pi g'^\pi = (gK)^\varphi (g'K)^\varphi,$$

we see that φ is a homomorphism from G/K to H. If $(gK)^\varphi = (g'K)^\varphi$, then $g^\pi = g'^\pi$ and thus $gg'^{-1} \in K$. So $gK = g'K$. Hence, φ is a monomorphism from G/K to H.

For all $g \in G$, we have

$$g^\pi = (gK)^\varphi = g^{\alpha\varphi}.$$

Since φ is both a monomorphism and an epimorphism from $G/K = G^\alpha$ to G^π, we have

$$G^\pi \cong G^\alpha = G/K. \qquad \square$$

Theorem 3.9. *If M_i is a normal subgroup of G for all $i \in I$, then the intersection $\bigcap_{i\in I} M_i$ and the subgroup $\langle M_i \mid i \in I\rangle$ generated by the M_i are normal subgroups of G.*

Proof. We have

$$\left(\bigcap_{i\in I} M_i\right)^g = \bigcap_{i\in I} M_i^g = \bigcap_{i\in I} M_i$$

and

$$\langle M_i \mid i \in I\rangle^g = \langle M_i^g \mid i \in I\rangle = \langle M_i \mid i \in I\rangle. \qquad \square$$

Theorem 3.10. *Let N be a normal subgroup of G.*

a) *The map α defined by $U^\alpha = U/N$ is a bijective correspondence between the subgroups U of G with $N \le U \le G$ and the subgroups of $\overline{G} = G/N$. This map respects intersection and generating sets.*

b) *For $N \le U \le G$, we have $[G : U] = [G/N : U/N]$.*

c) *If $N \le M \trianglelefteq G$, then we have $M/N \trianglelefteq G/N$ and*

$$G/N \Big/ M/N \cong G/M.$$

Proof. a) One sees immediately that it follows from $N \trianglelefteq G$ and $N \le U \le G$ that $N \trianglelefteq U$. Let α be the map from the collection of subgroups U with $N \le U \le G$ to subgroups of G/N defined by

$$U^\alpha = U/N = \{uN \mid u \in U\}.$$

We define a map ϵ in the opposite direction in the following way:

If $\overline{U} \le \overline{G} = G/N$, then define

$$\overline{U}^\epsilon = \{g \mid gN \in \overline{U}\}.$$

Clearly, $N \le \overline{U}^\epsilon \le G$. We have

$$\overline{U}^{\epsilon\alpha} = \{gN \mid g \in \overline{U}^\epsilon\} = \{gN \mid gN \in \overline{U}\} = \overline{U}.$$

Furthermore, we have

$$U^{\alpha\epsilon} = (U/N)^\epsilon = \{g \mid gN = uN \in U/N \text{ for some } u \in U\}.$$

If $gN = uN$, then $g = un$ for some $n \in N \le U$, and so $g \in U$. This shows that $U^{\alpha\epsilon} = U$.

The map α is therefore one-to-one since it is inverted by ϵ. Furthermore, α is a map onto all subgroups of $\overline{G}$ since $\overline{U}^{\epsilon\alpha} = \overline{U}$. Finally, for all $N \le U$ and $N \le V$ we have

$$U^\alpha \cap V^\alpha = \{xN \mid x \in U \cap V\} = (U \cap V)/N = (U \cap V)^\alpha$$

and

$$\begin{aligned}\langle U, V\rangle^\alpha = \langle U, V\rangle/N &= \left\{\Big(\prod_i x_i\Big)N \;\Big|\; x_i \in U \cup V\right\} \\ &= \left\{\prod_i (x_i N) \;\Big|\; x_i N \in U/N \cup V/N\right\} \\ &= \langle U/N, V/N\rangle = \langle U^\alpha, V^\alpha\rangle.\end{aligned}$$

b) It follows from the coset decomposition $G = \bigcup_{i\in I} g_i U$ that

$$G/N = \bigcup_{i\in I} (g_i N)(U/N).$$

We show that this is a disjoint union:

Suppose that

$$xN \in (g_i N)(U/N) \cap (g_j N)(U/N).$$

Then we have

$$xN = g_i u_1 N = g_i N u_1 = g_j u_2 N$$

for some $u_k \in U$, therefore

$$g_j^{-1} g_i \in u_2 N u_1^{-1} \subseteq U,$$

and then $i = j$. It follows that

$$[G/N : U/N] = |I| = [G : U].$$

c) Finally, let $N \leq M \trianglelefteq G$. We define the map φ from G/N onto G/M by $(gN)^\varphi = gM$. Then φ is well defined: If $g_1 N = g_2 N$, then $g_2^{-1} g_1 \in N \leq M$ and so $g_1 M = g_2 M$. Since

$$(g_1 N g_2 N)^\varphi = (g_1 g_2 N)^\varphi = g_1 g_2 M = g_1 M g_2 M = (g_1 N)^\varphi (g_2 N)^\varphi,$$

the map φ is a homomorphism from G/N onto G/M. The kernel of φ consists of the cosets gN with $g \in M$, so M/N is the kernel of φ. By the Homomorphism Theorem 3.8, it follows that $M/N \trianglelefteq G/N$ and

$$G/M \cong G/N \Big/ M/N. \qquad \square$$

Lemma 3.11. *If N is a normal subgroup of G and U is a subgroup of G, then the subgroup $\langle N, U\rangle$ is equal to the product UN defined in Definition 2.11. In particular, $NU = UN$.*

Proof. It is enough to show that UN is a subgroup of G. We proceed as follows: For $u_i \in U$ and $n_i \in N$ $(i = 1, 2)$, we have

$$u_1 n_1 u_2 n_2 = u_1 u_2 n_1^{u_2} n_2,$$

and this lies again in UN since $N \trianglelefteq G$ implies $n_1^{u_2} \in N$. Furthermore, we have that

$$(u_1 n_1)^{-1} = n_1^{-1} u_1^{-1} = u_1^{-1}(u_1 n_1^{-1} u_1^{-1})$$

lies in UN. □

Theorem 3.12. *If N is a normal subgroup of G and U is a subgroup of G, then $N \cap U \trianglelefteq U$ and*

$$UN/N \cong U/(U \cap N).$$

Proof. If $u \in U \cap N$ and $u' \in U$, it follows that $u^{u'} \in U \cap N$. Thus, $U \cap N$ is a normal subgroup of U.

Let α be the map from UN/N to $U/(U \cap N)$ defined by $(uN)^\alpha = u(U \cap N)$. Then α is well defined:

If $u_1 N = u_2 N$, then $u_2^{-1} u_1 \in U \cap N$ and so $u_1(U \cap N) = u_2(U \cap N)$.

Clearly, α is an epimorphism from UN/N to $U/(U \cap N)$. The kernel of α consists of the cosets uN with $u(U \cap N) = U \cap N$, and this is equivalent to $uN = N$. □

Theorem 3.13. *If M and N are normal subgroups of G with $M \cap N = 1$, then $mn = nm$ for all $m \in M$ and $n \in N$. In this case, we say that M and N commute.*

Proof. The element $n^{-1}m^{-1}nm = n^{-1}n^m$ lies in N. Since

$$n^{-1}m^{-1}nm = (m^{-1})^n m$$

also lies in M, it follows that $n^{-1}m^{-1}nm = 1$, which was our claim. □

Definition 3.14. If M is a subset of G, we define

$$M^G = \langle m^g \mid m \in M,\ g \in G\rangle.$$

Note that M^G is clearly the smallest normal subgroup of G containing M.

Exercises

7) Let π be a homomorphism from G to H. For all $g \in G$, $|g^\pi|$ divides $|g|$.
8) Let $N \lhd G$ and $g \in G$ with $(|g|, |G/N|) = 1$. Then $g \in N$.

4 Automorphisms

Definition 4.1. An isomorphism from G to itself is called an automorphism of G. The automorphisms of G form a group $\mathbf{Aut}(G)$ with respect to the following product:

For $\alpha, \beta \in \mathbf{Aut}(G)$, define the map $\alpha\beta$ by $g^{\alpha\beta} = (g^\alpha)^\beta$ for all $g \in G$.

The group $\mathbf{Aut}(G)$ is called the automorphism group of G. If G is finite, then clearly so is $\mathbf{Aut}(G)$.

Theorem 4.2. *Every map α of the form $x^\alpha = x^g$ for some $g \in G$ is an automorphism of G, a so-called inner automorphism. The inner automorphisms form a normal subgroup $\mathbf{Inn}(G)$ of $\mathbf{Aut}(G)$. The group $\mathbf{Inn}(G)$ is called the inner automorphism group of G. It is isomorphic to the quotient $G/\mathbf{Z}(G)$ of G by its center $\mathbf{Z}(G)$.*

Proof. That every α of the given form is an automorphism of G follows immediately from

$$(xy)^\alpha = (xy)^g = x^g y^g = x^\alpha y^\alpha$$

and the bijectivity of α.

Let α and β be inner automorphisms of G with $x^\alpha = x^g$ and $x^\beta = x^h$. Then

$$x^{\alpha\beta} = (x^\alpha)^\beta = (x^g)^h = x^{gh}.$$

Thus, $\alpha\beta$ is the inner automorphism of G induced by gh. Furthermore, one sees easily that α^{-1} is the inner automorphism induced by g^{-1}.

Let φ be an arbitrary automorphism of G and α the inner automorphism defined by $x^\alpha = x^g$. Then we have

$$x^{\varphi^{-1}\alpha\varphi} = (g^{-1}x^{\varphi^{-1}}g)^\varphi = (g^\varphi)^{-1}xg^\varphi.$$

Therefore, $\varphi^{-1}\alpha\varphi$ is the inner automorphism induced by g^φ and the inner automorphisms form a normal subgroup $\mathbf{Inn}(G)$ of $\mathbf{Aut}(G)$.

The mapping of $g \in G$ to the inner automorphism α defined by $x^\alpha = x^g$ is clearly an epimorphism from G to $\mathbf{Inn}(G)$, and the kernel is the center $\mathbf{Z}(G)$ of G. The claim that $\mathbf{Inn}(G) \cong G/\mathbf{Z}(G)$ then follows from the Homomorphism Theorem 3.8. □

Theorem 4.3. *Let M and N be normal subgroups of G with $M \leq N$. Let A be a subgroup of the automorphism group $\mathbf{Aut}(G)$ of G. Suppose that for every $\alpha \in A$, we have $M^\alpha = M$ and $N^\alpha = N$. Then the map $\overline{\alpha}$ defined by*

$$(nM)^{\overline{\alpha}} = n^\alpha M \quad (\text{for } n \in N)$$

is an automorphism of N/M. The map $\alpha \mapsto \overline{\alpha}$ is a homomorphism that takes A to the automorphism group $\mathbf{Aut}(N/M)$ of N/M. The kernel of this homomorphism consists of the automorphisms $\alpha \in A$ of the form $n^\alpha = n\,m(n)$, where $m(n) \in M$ for all $n \in N$. The $m(n)$ satisfy the functional equation