Graduate Texts in Mathematics

Groups and Representations

群及其表示

J.L.Alperin

Rowen B.Bell

Springer-Verlag
世界图书出版公司

J.L. Alperin
with Rowen B. Bell

Groups and Representations

Springer-Verlag
世界图书出版公司
北京·广州·上海·西安

J.L. Alperin
Rowen B. Bell
Department of Mathematics
University of Chicago
Chicago, IL 60637-1514

Mathematics Subject Classifications (1991): 20-01

Library of Congress Cataloging-in-Publication Data
Alperin, J.L.
Groups and representations / J.L. Alperin with Rowen B. Bell.
p. cm. – (Graduate texts in mathematics ; 162)
Includes bibliographical references (p. –) and index.
ISBN 0-387-94525-3 (alk. paper). – ISBN 0-387-94526-1 (pbk.: alk. paper)
1. Representations of groups. I. Bell, Rowen B. II. Title.
III. Series.
QA176.A46 1995
512'.2–dc20 95-17160

Printed on acid-free paper.

ISBN 0-387-94525-3 Springer-Verlag New York Berlin Heidelberg (Hardcover)
ISBN 0-387-94526-1 Springer-Verlag New York Berlin Heidelberg (Softcover)

Preface

This book is based on a first-year graduate course given regularly by the first author at the University of Chicago, most recently in the autumn quarters of 1991, 1992, and 1993. The lectures given in this course were expanded and prepared for publication by the second author.

The aim of this book is to provide a concise yet thorough treatment of some topics from group theory and representation theory with which every mathematician should be well acquainted. Of course, the topics covered naturally reflect the viewpoints and interests of the authors; for instance, we make no mention of free groups, and the emphasis throughout is admittedly on finite groups. Our hope is that this book will enable graduate students from every mathematical field, as well as bright undergraduates with an interest in algebra, to solidify their knowledge of group theory.

As the course on which this book is based is required for all incoming mathematics graduate students at Chicago, we make very modest assumptions about the algebraic background of the reader. A nodding familiarity with groups, rings, and fields, along with some exposure to elementary number theory and a solid knowledge of linear algebra (including, at times, familiarity with canonical forms of matrices), should be sufficient preparation.

We now give a brief summary of the book's contents. The first four chapters are devoted to group theory. Chapter 1 contains a review (largely without proofs) of the basics of group theory, along with material on automorphism groups, semidirect products, and group actions. These latter concepts are among our primary tools in the book and are often not covered adequately during one's first exposure to group theory. Chapter 2 discusses the structure of the general linear groups and culminates with a proof of the simplicity of the projective special linear groups. An understanding of this material is an essential (but often overlooked) component of any substantive study of group theory; for, as the first author once wrote:

> The typical example of a finite group is $\mathrm{GL}(n, q)$, the general linear group of n dimensions over the field with q elements. The student who is introduced to the subject with other examples is being completely misled. [3, p. 121]

Chapter 3 concentrates on the examination of finite groups through their p-subgroups, beginning with Sylow's theorem and moving on to such results as the Schur-Zassenhaus theorem. Chapter 4 starts with the Jordan-Hölder theorem and continues with a discussion of solvable and nilpotent groups. The final two chapters focus on finite-dimensional algebras and the representation theory of finite groups. Chapter 5 is centered around Maschke's theorem and Wedderburn's structure theorems for semisimple algebras. Chapter 6 develops the ordinary character theory of finite groups, including induced characters, while the Appendix treats some additional topics in character theory that require a somewhat greater algebraic background than does the core of the book.

We have included close to 200 exercises, and they form an integral part of the book. We have divided these problems into "exercises" and "further exercises;" the latter category is generally reserved for exercises that introduce and develop theoretical concepts not included in the text. The level of the problems varies from routine to difficult, and there are a few that we do not expect any student to be able to handle. We give no indication of the degree of difficulty of each exercise, for in mathematical research one does not know in advance what amount of work will be required to complete any step! In an effort to keep our exposition self-contained, we have strived to keep references in the text to the exercises at a minimum.

The sections of this book are numbered continuously, so that Section 4 is actually the first section of Chapter 2, and so forth. A citation of the form "Proposition Y" refers to the result of that name in the current section, while a citation of the form "Proposition X.Y" refers to Proposition Y of Section X.

We would like to extend our thanks to: Michael Maltenfort and Colin Rust, for their thought-provoking proofreading and their many constructive suggestions during the preparation of this book; the students in the first author's 1993 course, for their input on an earlier draft of this book which was used as that course's text; Efim Zelmanov and the students in his 1994 Chicago course, for the same reason; and the University of Chicago mathematics department, for continuing to provide summer support for graduate students, as without such support this book would not have been written in its present form. We invite you to send notice of errors, typographical or otherwise, to the second author at `bell@math.uchicago.edu`.

In remembrance of a life characterized by integrity, devotion to family, and service to community, the second author would like to dedicate this book to David Wellman (1953–1995).

Contents

1
Rudiments of Group Theory

In this introductory chapter, we review the elementary notions of group theory and develop many of the tools that we will use in the remaining chapters. Section 1 consists primarily of those facts with which we assume the reader is familiar from some prior study of group theory; consequently, most proofs in this section have been omitted. In Section 2 we introduce some important concepts, such as automorphism groups and semidirect products, which are not necessarily covered in a first course on group theory. Section 3 treats the theory of group actions; here we present both elementary applications and results of a more technical nature which will be needed in later chapters.

1. Review

Recall that a *group* consists of a non-empty set G and a binary operation on G, usually written as multiplication, satisfying the following conditions:

- The binary operation is associative: $(xy)z = x(yz)$ for any $x, y, z \in G$.
- There is a unique element $1 \in G$, called the *identity element* of G, such that $x1 = x$ and $1x = x$ for any $x \in G$.

- For every $x \in G$ there is a unique element $x^{-1} \in G$, called the *inverse* of x, with the property that $xx^{-1} = 1$ and $x^{-1}x = 1$.

Associativity allows us to consider unambiguously the product of any finite number of elements of a group. The order of the elements in such a product is critically important, for if x and y are elements of a group G, then it is not necessarily true that $xy = yx$. If this happens, then we say that x and y *commute*. More generally, we define the *commutator* of x and y to be the element $[x, y] = xyx^{-1}y^{-1}$, so that x and y commute iff $[x, y] = 1$. (Many authors define $[x, y] = x^{-1}y^{-1}xy$.) We say that G is *abelian* if all pairs of elements of G commute, in which case the order of elements in a product is irrelevant; otherwise, we say that G is *non-abelian*. The group operation of an abelian group may be written additively, meaning that the product of elements x and y is written as $x+y$ instead of xy, the inverse of x is denoted by $-x$, and the identity element is denoted by 0.

If x is an element of a group G, then for $n \in \mathbb{N}$ we use x^n (resp., x^{-n}) to mean the product $x \cdots x$ (resp., $x^{-1} \cdots x^{-1}$) involving n terms. We also define $x^0 = 1$. (In an abelian group that is written additively, we write nx instead of x^n for $n \in \mathbb{Z}$.) It is easily seen that the usual rules for exponentiation hold. We say that x is of *finite order* if there is some $n \in \mathbb{N}$ such that $x^n = 1$. If x is of finite order, then we define the *order* of x to be the least positive integer n such that $x^n = 1$. Clearly, x is of order n iff $1, x, x^2, \ldots, x^{n-1}$ are distinct elements of G and $x^n = 1$.

A group G is said to be *finite* if it has a finite number of elements, and *infinite* otherwise. We define the *order* of a finite group G, denoted $|G|$, to be the number of elements of G; we may also use $|S|$ for the cardinality of any finite set S. Every element of a finite group is of finite order, and there are infinite groups with this property; these groups are said to be *periodic*. However, there are infinite groups in which the identity element is the only element of finite order; such groups are said to be *torsion-free*.

A subset H of a group G is said to be a *subgroup* of G if it forms a group under the restriction to H of the binary operation on G. Equivalently, $H \subseteq G$ is a subgroup iff the following conditions hold:

- The identity element 1 of G lies in H.
- If $x, y \in H$, then their product xy in G lies in H.
- If $x \in H$, then its inverse x^{-1} in G lies in H.

Clearly G is a subgroup of itself. The set $\{1\}$ is also a subgroup of G; it is called the *trivial subgroup*, and for the sake of simplicity we denote it by 1. Every subgroup of a finite group is finite; however, an infinite group always has both finite and infinite subgroups, namely its trivial subgroup and itself, respectively. Similarly, every subgroup of an abelian group is abelian, but a non-abelian group always has both abelian and non-abelian subgroups. If H is a subgroup of G, then we write $H \leqslant G$; if H is properly contained in G, then we call H a *proper subgroup* of G, and we may write $H < G$. (This notational distinction is common, but not universal.) If $K \leqslant H$ and $H \leqslant G$, then evidently $K \leqslant G$.

PROPOSITION 1. If H and K are subgroups of a group G, then so is their intersection $H \cap K$. More generally, the intersection of any collection of subgroups of a group is also a subgroup of that group. ■

The following theorem gives important information about the nature of subgroups of a finite group.

LAGRANGE'S THEOREM. Let G be a finite group, and let $H \leqslant G$. Then $|H|$ divides $|G|$. ■

If X is a subset of a group G, then we define $<X>$ to be the intersection of all subgroups of G which contain X. By Proposition 1, $<X>$ is a subgroup of G, which we call the *subgroup of G generated by X*. We see that $<X>$ is the smallest subgroup of G which contains X, in the sense that it is contained in any such subgroup; hence if $X \leqslant G$, then $<X> = X$. If $X = \{x\}$, then we write $<x>$ in lieu of $<X>$; similarly, if $X = \{x_1, \ldots, x_n\}$, then we write $<x_1, \ldots, x_n>$ for $<X>$.

PROPOSITION 2. Let X be a subset of a group G. Then $<X>$ consists of the identity and all products of the form $x_1^{\epsilon_1} \cdots x_r^{\epsilon_r}$ where $r \in \mathbb{N}$, $x_i \in X$, and $\epsilon_i = \pm 1$ for all i. ■

A group G is said to be *cyclic* if $G = <g>$ for some $g \in G$; the element g is called a *generator* of G. For example, if G is a group of order n having an element g of order n, then $G = <g>$ since $g, \ldots, g^{n-1}, g^n = 1$ are n distinct elements of G. By Proposition 2 we have $<g> = \{g^n \mid n \in \mathbb{Z}\}$, and consequently we see via the exponentiation relations that cyclic groups are abelian; nonetheless,

we will generally write cyclic groups multiplicatively instead of additively. If g is of order n, then $<g> = \{1, g, \ldots, g^{n-1}\}$, and hence $|<g>| = n$. If g is not of finite order, then $<g>$ is a torsion-free infinite abelian group. Any two finite cyclic groups of the same order are "equivalent" in a sense that will be made precise later in this section, and any two infinite cyclic groups are equivalent in the same sense. The canonical infinite cyclic group is $\mathbf{Z}$, the set of integers under addition, while the canonical cyclic group of order n is $\mathbf{Z}/n\mathbf{Z}$, the set of residue classes of the integers under addition modulo n.

Suppose that G is a finite group and $g \in G$ is of order n. Then $<g>$ is a subgroup of G of order n, so by Lagrange's theorem we see that n divides $|G|$. Thus, the order of an element of a finite group must divide the order of that group. Consequently, if $|G|$ is equal to some prime p, then the order of each element of G must be a non-trivial divisor of p, from which it follows that G is cyclic with every non-identity element of G being a generator.

If X and Y are subsets of a group G, then we define the *product* of X and Y in G to be $XY = \{xy \mid x \in X, y \in Y\} \subseteq G$. We can extend this definition to any finite number of subsets of G. We also define the *inverse* of $X \subseteq G$ by $X^{-1} = \{x^{-1} \mid x \in X\} \subseteq G$. If H is a non-empty subset of G, then $H \leqslant G$ iff $HH = H$ and $H^{-1} = H$.

PROPOSITION 3. Let H and K be subgroups of a group G. Then HK is a subgroup of G iff $HK = KH$. ■

Observe that if H and K are subgroups of G, then their product HK contains both H and K; if in addition $K \leqslant H$, then $HK = H$. (These properties do not hold if H and K are arbitrary subsets of G.) If G is abelian, then $HK = KH$ for any subgroups H and K of G, and hence the product of any two subgroups of an abelian group is a subgroup.

We can now describe the subgroup structure of finite cyclic groups.

THEOREM 4. Let $G = <g>$ be a cyclic group of order n. Then:

(i) For each divisor d of n, there is exactly one subgroup of G of order d, namely $<g^{\frac{n}{d}}>$.

(ii) If d and e are divisors of n, then the intersection of the subgroups of orders d and e is the subgroup of order $\gcd(d, e)$.

(iii) If d and e are divisors of n, then the product of the subgroups of orders d and e is the subgroup of order $\operatorname{lcm}(d, e)$. ■

If $H \leqslant G$ and $x \in G$, then we write xH instead of $\{x\}H$; the set xH is called a *left coset* of H in G. Similarly, we write Hx instead of $H\{x\}$, and we call Hx a *right coset* of H in G. In this book we shall use left cosets, and consequently from now on the word "coset" should be read as "left coset." Our use of left cosets instead of right cosets is essentially arbitrary, as any statement that we make about left cosets has a valid counterpart involving right cosets. Indeed, many group theory texts use right cosets where we use left cosets. There is a bijective correspondence between left and right cosets of H in G, sending a left coset xH to its inverse $(xH)^{-1} = Hx^{-1}$.

Let H be a subgroup of G. Any two cosets of H in G are either equal or disjoint, with cosets xH and yH being equal iff $y^{-1}x \in H$. Consequently, an element $x \in G$ lies in exactly one coset of H, namely xH. For any $x \in G$, there is a bijective correspondence between H and xH; one such correspondence sends $h \in H$ to xh. We define the *index* of H in G, denoted $|G : H|$, to be the number of cosets of H in G. (If there is an infinite number of cosets of H in G, then we could define $|G : H|$ to be the appropriate cardinal number without changing the truth of any statements made below, as long as we redefine $|G|$ as being the cardinal number $|G : 1|$.) The cosets of H in G partition G into $|G : H|$ disjoint sets of cardinality $|H|$, and hence we have $|G| = |G : H||H|$. (This observation proves Lagrange's theorem; however, it is possible to prove Lagrange's theorem without reference to cosets by means of a simple counting argument.) In particular, all subgroups of a finite group are of finite index, while subgroups of an infinite group may be of finite or infinite index. We denote the set of cosets (or the *coset space*) of H in G by G/H.

We can now give a complete description of the subgroups of infinite cyclic groups. We invite the reader to restate Theorem 4 in such a way so as to make the parallelism between Theorems 4 and 5 more explicit.

THEOREM 5. Let $G = \langle g \rangle$ be an infinite cyclic group. Then:

(i) For each $d \in \mathbb{N}$, there is exactly one subgroup of G of index d, namely $\langle g^d \rangle$. Furthermore, every non-trivial subgroup of G is of finite index.

(ii) Let $d, e \in \mathbb{N}$. Then the intersection of the subgroups of indices d and e is the subgroup of index $\operatorname{lcm}(d, e)$.

(iii) Let $d, e \in \mathbb{N}$. Then the product of the subgroups of indices d and e is the subgroup of index $\gcd(d, e)$. ■

The following result generalizes Lagrange's theorem and shall be referred to as "factorization of indices."

THEOREM 6. If $K \leqslant H \leqslant G$, then $|G : K| = |G : H||H : K|$. ■

Let H be a subgroup of a group G, and let $\mathcal{I}$ be an indexing set that is in bijective correspondence with the coset space of H in G. A subset $T = \{t_i \mid i \in \mathcal{I}\}$ of G is said to be a (*left*) *transversal* for H (or a set of (*left*) *coset representatives* of H in G) if the sets t_iH are precisely the cosets of H in G, with no coset omitted or duplicated.

Let N be a subgroup of a group G. We say that N is a *normal subgroup* of G (or that N is *normal* in G) if $xN = Nx$ for all $x \in G$, or equivalently if $xNx^{-1} \subseteq N$ for all $x \in G$. If G is abelian, then every subgroup of G is normal. The subgroups 1 and G are always normal in G; if these are the only normal subgroups of G, then we say that G is *simple*. For example, a cyclic group of prime order is simple. (A group having only one element is by convention not considered to be simple.) If N is normal in G, then we write $N \trianglelefteq G$; if N is both proper and normal in G, then we may write $N \triangleleft G$. (Once again, many authors do not make this distinction and instead use $N \triangleleft G$ to mean simply that N is normal in G.) If $H \trianglelefteq G$ and $K \trianglelefteq H$, then it is not necessarily true that $K \trianglelefteq G$; we will provide a counterexample momentarily. However, it is clearly true that if $K \trianglelefteq G$ and $K \leqslant H \leqslant G$, then $K \trianglelefteq H$.

PROPOSITION 7. Let H and K be subgroups of a group G. If $K \trianglelefteq G$, then $HK \leqslant G$ and $H \cap K \trianglelefteq H$; if also $H \trianglelefteq G$, then $HK \trianglelefteq G$ and $H \cap K \trianglelefteq G$. ■

PROPOSITION 8. Any subgroup of index 2 is normal.

PROOF. Let $H \leqslant G$, and suppose that $|G : H| = 2$. Then there are two left cosets of H in G; one is H, and thus the other must be $G - H$. Similarly, H and $G - H$ are the two right cosets of H in G. It now follows that $x \in H$ iff $xH = H = Hx$, and $x \notin H$ iff $xH = G - H = Hx$; hence $H \trianglelefteq G$. ■

Normal subgroups are important because they allow us to create new groups from old, in the following way:

THEOREM 9. If $N \trianglelefteq G$, then the coset space G/N forms a group under the binary operation defined by $(xN)(yN) = (xy)N$. ■

If $N \trianglelefteq G$, then we call G/N with the above binary operation the *quotient group* of G by N. The identity element of G/N is N, and the inverse of $xN \in G/N$ is $x^{-1}N$. If G is abelian, then G/N is also abelian.

Let x and g be elements of a group G. The *conjugate* of x by g is defined to be the element gxg^{-1} of G. (Some authors define the conjugate of x by g to be $g^{-1}xg$. The notations ${}^{g}x$ and x^{g} are sometimes used for gxg^{-1} and $g^{-1}xg$, respectively.) Two elements x and y of G are said to be *conjugate* if there exists some $g \in G$ such that $y = gxg^{-1}$. No two distinct elements of an abelian group can be conjugate. A subgroup N of G is normal iff every conjugate of an element of N by an element of G lies in N.

Let X be a set. A *permutation* of X is a bijective set map from X to X. The set of permutations of X, denoted Σ_X, forms a group under composition of mappings. If $X = \{1, \ldots, n\}$ for some $n \in \mathbb{N}$, then this group is called the *symmetric group of degree* n and is denoted Σ_n. (Many authors denote this group by S_n or $\mathfrak{S}_n$.) The group Σ_n is finite and of order $n! = n(n-1)\cdots 2 \cdot 1$.

An element ρ of Σ_n is called a *cycle of length* r (or an *r-cycle*) if there are distinct integers $1 \leq a_1, \ldots, a_r \leq n$ such that $\rho(a_i) = (a_{i+1})$ for all $1 \leq i < r$, $\rho(a_r) = a_1$, and $\rho(b) = b$ for any $1 \leq b \leq n$ which is not equal to some a_i. If the cycle ρ is as defined above, then we write $\rho = (a_1 \ \cdots \ a_r)$. Of course, this can be done in r different ways; for example, (1 2 4), (2 4 1), and (4 1 2) denote the same 3-cycle in Σ_4. The cycle ρ as defined above is said to *move* each a_i and *fix* every other number. Two cycles are said to be *disjoint* if there is no number that is moved by both cycles. The product of two cycles $(a_1 \ \cdots \ a_r)$ and $(b_1 \ \cdots \ b_s)$ is written $(a_1 \ \cdots \ a_r)(b_1 \ \cdots \ b_s)$; if $a_i = b_j$, then this product moves b_{j-1} to a_{i+1}. (We read from "right to left" in this manner because we think of the cycles as being functions on $\{1, \ldots, n\}$, and so the product of two cycles corresponds to a composition of functions, which we choose to perform from right to left in the usual fashion. In many group theory texts, composition is performed from left to right.)

Every element of Σ_n can be written as a product of disjoint cycles; such an expression is called a *disjoint cycle decomposition* of the permutation. Any two disjoint cycle decompositions of a given permutation must necessarily include the same cycles, but possibly

in some different order. Therefore we can associate, in a well-defined way, a collection of positive integers whose sum is n to each element ρ of Σ_n; this partition of n consists of the lengths of the cycles that appear in a disjoint cycle decomposition of ρ and is called the *cycle structure* of ρ. For example, the cycle structure of an r-cycle in Σ_n is the partition $(r, 1, \ldots, 1)$ having $n - r$ ones; the cycle structure of $(1\ 2\ 4)(3\ 5)$ in Σ_6 is the partition $(3, 2, 1)$. We generally omit 1-cycles when writing a permutation as a product of disjoint cycles. As usual, we will use 1 to denote the identity element of Σ_n, whose disjoint cycle decomposition consists solely of 1-cycles.

PROPOSITION 10. Let $n \in \mathbb{N}$. Then two elements of Σ_n are conjugate iff they have the same cycle structure. ■

For a proof, see [24, pp. 46–7].

A *transposition* in Σ_n is a 2-cycle. Every element of Σ_n can be written as a (not necessarily disjoint) product of transpositions in many different ways. However, it can be shown that any two expressions of a given permutation as a product of transpositions use the same number, modulo 2, of transpositions. (See [24, pp. 8–9].) Hence we can say that a permutation is *even* (resp., *odd*) if it can be written as a product of an even (resp., odd) number of transpositions, for a permutation is either even or odd, but never both. For example, since an r-cycle can be written as a product of $r - 1$ transpositions, we see that a cycle is an even permutation iff its length is odd. The subset of Σ_n consisting of all even permutations is a subgroup of index 2, and hence is normal in Σ_n by Proposition 8; it is called the *alternating group of degree n* and is denoted A_n.

Consider $H = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subseteq A_4$. One can show that $H \trianglelefteq A_4$. (In fact, H is normal in Σ_4. This group H is historically called the *Klein four-group*.) Let $K = \{1, (1\ 2)(3\ 4)\}$. Then K is a subgroup of H with $|H : K| = |H|/|K| = 4/2 = 2$, and hence $K \trianglelefteq H$ by Proposition 8. However, by conjugating $(1\ 2)(3\ 4)$ by the even permutation $(1\ 2\ 3)$, we see that K is not normal in A_4. This provides the counterexample referred to on page 6.

Let G and H be groups. A *homomorphism* is a map $\varphi\colon G \to H$ with the property that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$; that is, a homomorphism is a map between groups which preserves the respective group structures. If φ is a homomorphism, then $\varphi(1) = 1$,

and $\varphi(x^{-1}) = \varphi(x)^{-1}$ for any element x. The *trivial homomorphism* from G to H is the map sending every element of G to the identity element of H. If a homomorphism φ is injective, then we call φ a *monomorphism*, and if φ is surjective, we call φ an *epimorphism*; we say that φ is an *isomorphism* if φ is bijective. (Recall that a set map $f: X \to Y$ is called injective if $f(x) = f(x')$ forces $x = x'$, surjective if for any $y \in Y$ we have $f(x) = y$ for some $x \in X$, and bijective if it is both injective and surjective.) If φ is an isomorphism, then so is $\varphi^{-1}: H \to G$. A homomorphism $\varphi: G \to G$ is called an *endomorphism* of G; a bijective endomorphism is called an *automorphism*.

If G and H are groups and there is an isomorphism $\varphi: G \to H$, then we say that G and H are *isomorphic*, or that G is isomorphic with H, and we write $G \cong H$. The notion of isomorphism is an equivalence relation on groups; that is, it is reflexive ($G \cong G$), symmetric ($G \cong H$ implies $H \cong G$), and transitive ($G \cong H$ and $H \cong K$ together imply $G \cong K$). Therefore, we can speak of the "isomorphism class" to which a given group belongs. Isomorphic groups are to be thought of as being virtually identical, in the sense that any statement made about a group is true (after making appropriate identifications) for any other group with which it is isomorphic. If we say that a group having certain properties is "unique," then we often mean that it is "unique up to isomorphism," by which we mean that any two groups having the specified properties are isomorphic.

We now consider some standard examples.

- Let $G = \langle g \rangle$ and $H = \langle h \rangle$ be two cyclic groups of order n. We define a map $\varphi: G \to H$ by setting $\varphi(g^a) = h^a$ for every $0 \leq a < n$. This map φ is an isomorphism. Consequently, any two finite cyclic groups of the same order are isomorphic. In particular, any cyclic group of order n is isomorphic with $\mathbb{Z}/n\mathbb{Z}$, and there is a unique group of order p for each prime p. We will use $\mathbf{Z_n}$ to denote a cyclic group of order n, written multiplicatively. We can similarly show that any two infinite cyclic groups are isomorphic; we will use $\mathbf{Z}$ to denote an infinite cyclic group, written multiplicatively.
- Let G be a group, let $H \leqslant G$, and let $g \in G$. The *conjugate* of H by g is the set $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ consisting of all conjugates of elements of H by g. It is easily verified that $gHg^{-1} \leqslant G$. We say that $K \leqslant G$ is a *conjugate* of H