Group Theory

J.S. Milne

e	r	r^2	f	rf	fr
r	r^2	e	rf	fr	f
r^2	e	r	fr	f	rf
f	fr	rf	e	r^2	r
rf	f	fr	r	e	r^2
fr	rf	f	r^2	r	e

$$S_3$$

$$\begin{aligned} r &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ f &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \end{aligned}$$

Version 4.00
June 23, 2021

The first version of these notes was written for a first-year graduate algebra course. As in most such courses, the notes concentrated on abstract groups and, in particular, on finite groups. However, it is not as abstract groups that most mathematicians encounter groups, but rather as algebraic groups, topological groups, or Lie groups, and it is not just the groups themselves that are of interest, but also their linear representations. It is my intention (one day) to expand the notes to take account of this, and to produce a volume that, while still modest in size (c200 pages), will provide a more comprehensive introduction to group theory for beginning graduate students in mathematics, physics, and related fields.

BibTeX information

```
@misc{milneGT,
  author={Milne, James S.},
  title={Group Theory (v4.00)},
  year={2021},
  note={Available at www.jmilne.org/math/},
  pages={139}
}
```

Please send comments and corrections to me at jmilne at umich dot edu.
v2.01 (August 21, 1996). First version on the web; 57 pages.
v2.11 (August 29, 2003). Revised and expanded; numbering; unchanged; 85 pages.
v3.00 (September 1, 2007). Revised and expanded; 121 pages.
v3.16 (July 16, 2020). Revised and expanded; 137 pages.
v4.00 (June 23, 2021). Made document (including source code) available under Creative Commons licence.

The multiplication table of S_3 on the front page was produced by Group Explorer.

Version 4.0 is published under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International licence (CC BY-NC-SA 4.0).

Licence information: https://creativecommons.org/licenses/by-nc-sa/4.0

Copyright ©1996–2021 J.S. Milne.

Contents

Contents 3

1 Basic Definitions and Results **7**
Definitions and examples . . . 7
Multiplication tables . . . 11
Subgroups . . . 12
Groups of small order . . . 15
Homomorphisms . . . 16
Cosets . . . 17
Normal subgroups . . . 18
Kernels and quotients . . . 20
Theorems concerning homomorphisms . . . 21
Direct products . . . 23
Commutative groups . . . 25
The order of ab . . . 28
Exercises . . . 29

2 Free Groups and Presentations; Coxeter Groups **31**
Free monoids . . . 31
Free groups . . . 32
Generators and relations . . . 35
Finitely presented groups . . . 37
Coxeter groups . . . 38
Exercises . . . 41

3 Automorphisms and Extensions **43**
Automorphisms of groups . . . 43
Characteristic subgroups . . . 45
Semidirect products . . . 46
Extensions of groups . . . 50
The Hölder program. . . . 52
Exercises . . . 54

4 Groups Acting on Sets **57**
Definition and examples . . . 57
Permutation groups . . . 64
The Todd-Coxeter algorithm. . . . 70
Primitive actions. . . . 71
Exercises . . . 73

5 The Sylow Theorems; Applications **75**

The Sylow theorems . . . 75
Alternative approach to the Sylow theorems . . . 79
Examples . . . 80
Exercises . . . 83

6 Subnormal Series; Solvable and Nilpotent Groups 85
Subnormal Series. . . . 85
Solvable groups . . . 88
Nilpotent groups . . . 91
Groups with operators . . . 94
Krull-Schmidt theorem . . . 96
Exercises . . . 97

7 Representations of Finite Groups 99
Matrix representations . . . 99
Roots of 1 in fields . . . 100
Linear representations . . . 100
Maschke's theorem . . . 101
The group algebra; semisimplicity . . . 103
Semisimple modules . . . 104
Simple F-algebras and their modules . . . 106
Semisimple F-algebras and their modules . . . 110
The representations of G . . . 112
The characters of G . . . 113
The character table of a group . . . 116
Examples . . . 116
Exercises . . . 116

A Additional Exercises 119

B Solutions to the Exercises 123

C Two-Hour Examination 131

Bibliography 133

Index 135

Notation.

We use the standard (Bourbaki) notation: $\mathbb{N} = \{0, 1, 2, \ldots\}$; $\mathbb{Z}$ is the ring of integers; $\mathbb{Q}$ is the field of rational numbers; $\mathbb{R}$ is the field of real numbers; $\mathbb{C}$ is the field of complex numbers; $\mathbb{F}_q$ is a finite field with q elements, where q is a power of a prime number. In particular, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p a prime number.

For integers m and n, $m|n$ means that m divides n, i.e., $n \in m\mathbb{Z}$. Throughout the notes, p is a prime number, i.e., $p = 2, 3, 5, 7, 11, \ldots, 1000000007, \ldots$.

Given an equivalence relation, $[*]$ denotes the equivalence class containing $*$. The empty set is denoted by $\emptyset$. The cardinality of a set S is denoted by $|S|$ (so $|S|$ is the number of elements in S when S is finite). Let I and A be sets; a family of elements of A indexed by I, denoted $(a_i)_{i \in I}$, is a function $i \mapsto a_i : I \to A$.[1]

Rings are required to have an identity element 1, and homomorphisms of rings are required to take 1 to 1. An element a of a ring is a unit if it has an inverse (element b such that $ab = 1 = ba$). The identity element of a ring is required to act as 1 on a module over the ring.

$X \subset Y$	X is a subset of Y (not necessarily proper);
$X \overset{\text{def}}{=} Y$	X is defined to be Y, or equals Y by definition;
$X \approx Y$	X is isomorphic to Y;
$X \simeq Y$	X and Y are canonically isomorphic (or there is a given or unique isomorphism);

Prerequisites

An undergraduate “abstract algebra” course.

Computer algebra programs

GAP is an open source computer algebra program, emphasizing computational group theory. To get started with GAP, I recommend going to Alexander Hulpke’s page here, where you will find versions of GAP for both Windows and Macs and a guide “Abstract Algebra in GAP”. The Sage page here provides a front end for GAP and other programs. I also recommend N. Carter’s “Group Explorer” here for exploring the structure of groups of small order. Earlier versions of these notes (v3.02) described how to use Maple for computations in group theory.

Acknowledgements

I thank the following for providing corrections and comments for earlier versions of these notes: V.V. Acharya; Yunghyun Ahn; Max Black; Tony Bruguier; Vigen Chaltikyan; Dustin Clausen; Benoît Claudon; Keith Conrad; Demetres Christofides; Adam Glesser; Darij Grinberg; Sylvan Jacques; Martin Klazar; Thomas Lamm; Mark Meckes; Max Menzies; Victor Petrov; Flavio Poletti; Diego Silvera; Efthymios Sofos; Dave Simpson; David Speyer; Kenneth Tam; Robert Thompson; Bhupendra Nath Tiwari; Leandro Vendramin; Michiel Vermeulen.

Also, I have benefited from the posts to mathoverflow by Richard Borcherds, Robin Chapman, Steve Dalton, Leonid Positselski, Noah Snyder, Richard Stanley, Qiaochu Yuan, and others.

A reference **monnnn** means question nnnn on mathoverflow.net and **sxnnnn** similarly refers to math.stackexchange.com.

[1] A family should be distinguished from a set. For example, if f is the function $\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ sending an integer to its equivalence class, then $\{f(i) \mid i \in \mathbb{Z}\}$ is a set with three elements whereas $(f(i))_{i \in \mathbb{Z}}$ is family with an infinite index set.

The theory of groups of finite order may be said to date from the time of Cauchy. To him are due the first attempts at classification with a view to forming a theory from a number of isolated facts. Galois introduced into the theory the exceedingly important idea of a [normal] sub-group, and the corresponding division of groups into simple and composite. Moreover, by shewing that to every equation of finite degree there corresponds a group of finite order on which all the properties of the equation depend, Galois indicated how far reaching the applications of the theory might be, and thereby contributed greatly, if indirectly, to its subsequent developement.

Many additions were made, mainly by French mathematicians, during the middle part of the [nineteenth] century. The first connected exposition of the theory was given in the third edition of M. Serret's "*Cours d'Algèbre Supérieure,*" which was published in 1866. This was followed in 1870 by M. Jordan's "*Traité des substitutions et des équations algébriques.*" The greater part of M. Jordan's treatise is devoted to a developement of the ideas of Galois and to their application to the theory of equations.

No considerable progress in the theory, as apart from its applications, was made till the appearance in 1872 of Herr Sylow's memoir "*Théorèmes sur les groupes de substitutions*" in the fifth volume of the *Mathematische Annalen.* Since the date of this memoir, but more especially in recent years, the theory has advanced continuously.

W. Burnside, Theory of Groups of Finite Order, 1897.

Galois introduced the concept of a normal subgroup in 1832, and Camille Jordan in the preface to his *Traité…* in 1870 flagged Galois' distinction between groupes simples and groupes composées as the most important dichotomy in the theory of permutation groups. Moreover, in the *Traité*, Jordan began building a database of finite simple groups — the alternating groups of degree at least 5 and most of the classical projective linear groups over fields of prime cardinality. Finally, in 1872, Ludwig Sylow published his famous theorems on subgroups of prime power order.

R. Solomon, Bull. Amer. Math. Soc., 2001.

Why are the finite simple groups classifiable?

It is unlikely that there is any easy reason why a classification is possible, unless someone comes up with a completely new way to classify groups. One problem, at least with the current methods of classification via centralizers of involutions, is that every simple group has to be tested to see if it leads to new simple groups containing it in the centralizer of an involution. For example, when the baby monster was discovered, it had a double cover, which was a potential centralizer of an involution in a larger simple group, which turned out to be the monster. The monster happens to have no double cover so the process stopped there, but without checking every finite simple group there seems no obvious reason why one cannot have an infinite chain of larger and larger sporadic groups, each of which has a double cover that is a centralizer of an involution in the next one. Because of this problem (among others), it was unclear until quite late in the classification whether there would be a finite or infinite number of sporadic groups.

Richard Borcherds, mo38161.

CHAPTER **1**

Basic Definitions and Results

> *The axioms for a group are short and natural.... Yet somehow hidden behind these axioms is the monster simple group, a huge and extraordinary mathematical object, which appears to rely on numerous bizarre coincidences to exist. The axioms for groups give no obvious hint that anything like this exists.*
>
> Richard Borcherds, in *Mathematicians: An Outer View....*

> *The one thing I would really like to know before I die is why the monster group exists.*
>
> John Conway, in a 2014 interview on Numberphile.

Group theory is the study of symmetries.

Definitions and examples

DEFINITION 1.1 A ***group*** is a set G together with a binary operation

$$(a,b) \mapsto a * b \colon G \times G \to G$$

satisfying the following conditions:

G1: (associativity) for all $a,b,c \in G$,

$$(a*b)*c = a*(b*c);$$

G2: (existence of a neutral element) there exists an element $e \in G$ such that

$$a*e = a = e*a \tag{1}$$

for all $a \in G$;

G3: (existence of inverses) for each $a \in G$, there exists an $a' \in G$ such that

$$a*a' = e = a'*a.$$

We usually abbreviate $(G,*)$ to G. Also, we usually write ab for $a*b$ and 1 for e; alternatively, we write $a+b$ for $a*b$ and 0 for e. In the first case, the group is said to be ***multiplicative***, and in the second, it is said to be ***additive***.

1.2 In the following, $a, b, \ldots$ are elements of a group G.

(a) An element e satisfying (1) is called a ***neutral element***. If e' is a second such element, then $e' = e * e' = e$. In fact, e is the unique element of G satisfying $x * x = x$ (apply G3).

(b) If $b * a = e$ and $a * c = e$, then

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

Hence the element a' in (G3) is uniquely determined by a. We call it the ***inverse*** of a, and denote it a^{-1} (or the ***negative*** of a, and denote it $-a$).

(c) Note that (G1) shows that the product of any ordered triple a_1, a_2, a_3 of elements of G is unambiguously defined: whether we form $a_1 a_2$ first and then $(a_1 a_2)a_3$, or $a_2 a_3$ first and then $a_1(a_2 a_3)$, the result is the same. In fact, (G1) implies that the product of any ordered n-tuple a_1, a_2,..., a_n of elements of G is unambiguously defined. We prove this by induction on n. In one multiplication, we might end up with

$$(a_1 \cdots a_i)(a_{i+1} \cdots a_n) \tag{2}$$

as the final product, whereas in another we might end up with

$$(a_1 \cdots a_j)(a_{j+1} \cdots a_n). \tag{3}$$

Note that the expression within each pair of parentheses is well defined because of the induction hypotheses. Thus, if $i = j$, (2) equals (3). If $i \neq j$, we may suppose $i < j$. Then

$$\begin{aligned}(a_1 \cdots a_i)(a_{i+1} \cdots a_n) &= (a_1 \cdots a_i)\left((a_{i+1} \cdots a_j)(a_{j+1} \cdots a_n)\right)\\ (a_1 \cdots a_j)(a_{j+1} \cdots a_n) &= \left((a_1 \cdots a_i)(a_{i+1} \cdots a_j)\right)(a_{j+1} \cdots a_n)\end{aligned}$$

and the expressions on the right are equal because of (G1).

(d) The inverse of $a_1 a_2 \cdots a_n$ is $a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$, i.e., the inverse of a product is the product of the inverses in the reverse order.

(e) (G3) implies that the cancellation laws hold in groups,

$$ab = ac \implies b = c, \qquad ba = ca \implies b = c$$

(multiply on left or right by a^{-1}). Conversely, if G is *finite*, then the cancellation laws imply (G3): the map $x \mapsto ax \colon G \to G$ is injective, and hence (by counting) bijective; in particular, e is in the image, and so a has a right inverse; similarly, it has a left inverse, and the argument in (b) above shows that the two inverses are equal.

Two groups $(G, *)$ and $(G', *')$ are ***isomorphic*** if there exists a one-to-one correspondence $a \leftrightarrow a'$, $G \leftrightarrow G'$, such that $(a * b)' = a' *' b'$ for all $a, b \in G$.

The ***order*** $|G|$ of a group G is its cardinality. A finite group whose order is a power of a prime p is called a ***p-group***.

For an element a of a group G, define

$$a^n = \begin{cases} aa \cdots a & n > 0 \quad (n \text{ copies of } a)\\ e & n = 0\\ a^{-1}a^{-1} \cdots a^{-1} & n < 0 \quad (|n| \text{ copies of } a^{-1})\end{cases}$$

The usual rules hold:

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}, \quad \text{all } m,n \in \mathbb{Z}. \tag{4}$$

It follows from (4) that the set

$$\{n \in \mathbb{Z} \mid a^n = e\}$$

is an ideal in $\mathbb{Z}$, and so equals $m\mathbb{Z}$ for some integer $m \geq 0$. When $m = 0$, $a^n \neq e$ unless $n = 0$, and a is said to have ***infinite order***. When $m \neq 0$, it is the smallest integer $m > 0$ such that $a^m = e$, and a is said to have ***finite order*** m. In this case, $a^{-1} = a^{m-1}$, and

$$a^n = e \iff m|n.$$

EXAMPLES

1.3 Let C_∞ be the group $(\mathbb{Z}, +)$, and, for an integer $m \geq 1$, let C_m be the group $(\mathbb{Z}/m\mathbb{Z}, +)$.

1.4 ***Permutation groups.*** Let S be a set and let $\mathrm{Sym}(S)$ be the set of bijections $\alpha\colon S \to S$. We define the product of two elements of $\mathrm{Sym}(S)$ to be their composite:

$$\alpha\beta = \alpha \circ \beta.$$

In other words, $(\alpha\beta)(s) = \alpha(\beta(s))$ for all $s \in S$. For any $\alpha, \beta, \gamma \in \mathrm{Sym}(S)$ and $s \in S$,

$$((\alpha \circ \beta) \circ \gamma)(s) = (\alpha \circ \beta)(\gamma(s)) = \alpha(\beta(\gamma(s))) = (\alpha \circ (\beta \circ \gamma))(s), \tag{5}$$

and so associativity holds. The identity map $s \mapsto s$ is an identity element for $\mathrm{Sym}(S)$, and inverses exist because we required the elements of $\mathrm{Sym}(S)$ to be bijections. Therefore $\mathrm{Sym}(S)$ is a group, called the ***group of symmetries*** of S. For example, the ***permutation group on*** n ***letters*** S_n is defined to be the group of symmetries of the set $\{1, ..., n\}$ — it has order $n!$.

1.5 When G and H are groups, we can construct a new group $G \times H$, called the ***(direct) product*** of G and H. As a set, it is the cartesian product of G and H, and multiplication is defined by

$$(g,h)(g',h') = (gg',hh').$$

1.6 A group G is ***commutative*** (or ***abelian***)[1] if

$$ab = ba, \quad \text{all } a,b \in G.$$

In a commutative group, the product of any finite (not necessarily ordered) family S of elements is well defined, for example, the empty product is e. Usually, we write commutative groups additively. With this notation, Equation (4) becomes:

$$ma + na = (m+n)a, \quad m(na) = mna.$$

When G is commutative,

$$m(a+b) = ma + mb \text{ for } m \in \mathbb{Z} \text{ and } a,b \in G,$$

[1] "Abelian group" is more common than "commutative group", but I prefer to use descriptive names.

and so the map

$$(m,a) \mapsto ma\colon \mathbb{Z} \times G \to G$$

makes G into a $\mathbb{Z}$-module. In a commutative group G, the elements of finite order form a subgroup G_{tors} of G, called the ***torsion subgroup***.

1.7 Let F be a field. The $n \times n$ matrices with coefficients in F and nonzero determinant form a group $\mathrm{GL}_n(F)$ called the ***general linear group of degree*** n. For a finite-dimensional F-vector space V, the F-linear automorphisms of V form a group $\mathrm{GL}(V)$ called the ***general linear group of*** V. Note that if V has dimension n, then the choice of a basis determines an isomorphism $\mathrm{GL}(V) \to \mathrm{GL}_n(F)$ sending an automorphism to its matrix with respect to the basis.

1.8 Let V be a finite-dimensional vector space over a field F. A bilinear form on V is a mapping $\phi\colon V \times V \to F$ that is linear in each variable. An ***automorphism*** of such a ϕ is an isomorphism $\alpha\colon V \to V$ such that

$$\phi(\alpha v, \alpha w) = \phi(v,w) \text{ for all } v,w \in V. \tag{6}$$

The automorphisms of ϕ form a group $\mathrm{Aut}(\phi)$. Let $\{e_1,\ldots,e_n\}$ be a basis for V, and let

$$P = (\phi(e_i,e_j))_{1 \le i,j \le n}$$

be the matrix of ϕ. The choice of the basis identifies $\mathrm{Aut}(\phi)$ with the group of invertible matrices A such that[2]

$$A^{\mathrm{T}} \cdot P \cdot A = P. \tag{7}$$

When ϕ is symmetric, i.e.,

$$\phi(v,w) = \phi(w,v) \text{ all } v,w \in V,$$

and nondegenerate, $\mathrm{Aut}(\phi)$ is called the ***orthogonal group*** of ϕ.

When ϕ is skew-symmetric, i.e.,

$$\phi(v,w) = -\phi(w,v) \text{ all } v,w \in V,$$

and nondegenerate, $\mathrm{Aut}(\phi)$ is called the ***symplectic group*** of ϕ. In this case, there exists a basis for V for which the matrix of ϕ is

$$J_{2m} = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}, \quad 2m = n,$$

[2] When we use the basis to identify V with F^n, the pairing ϕ becomes

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \mapsto (a_1,\ldots,a_n) \cdot P \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

If A is the matrix of α with respect to the basis, then α corresponds to the map $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto A \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$.Therefore, (6) becomes the statement that

$$(a_1,\ldots,a_n) \cdot A^{\mathrm{T}} \cdot P \cdot A \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = (a_1,\ldots,a_n) \cdot P \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \text{ for all } \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in F^n.$$

On examining this statement on the standard basis vectors for F^n, we see that it is equivalent to (7).

and the group of invertible matrices A such that

$$A^{\mathrm{T}} J_{2m} A = J_{2m}$$

is called the symplectic group Sp_{2m}.

REMARK 1.9 A set S together with a binary operation $(a,b) \mapsto a \cdot b \colon S \times S \to S$ is called a ***magma***. When the binary operation is associative, $(S,\cdot)$ is called a ***semigroup***. The product

$$\prod A \overset{\text{def}}{=} a_1 \cdots a_n$$

of any sequence $A = (a_i)_{1 \le i \le n}$ of elements in a semigroup S is well-defined (see 1.2(c)), and for any pair A and B of such sequences,

$$\left(\prod A\right)\left(\prod B\right) = \prod (A \sqcup B). \tag{8}$$

Let $\emptyset$ be the empty sequence, i.e., the sequence of elements in S indexed by the empty set. What should $\prod \emptyset$ be? Clearly, we should have

$$\left(\prod \emptyset\right)\left(\prod A\right) = \prod (\emptyset \sqcup A) = \prod A = \prod (A \sqcup \emptyset) = \left(\prod A\right)\left(\prod \emptyset\right).$$

In other words, $\prod \emptyset$ should be a neutral element. A semigroup with a neutral element is called a ***monoid***. In a monoid, the product of any finite (possibly empty) sequence of elements is well-defined, and (8) holds.

ASIDE 1.10 (a) The group conditions (G2,G3) can be replaced by the following weaker conditions (existence of a left neutral element and left inverses): (G2′) there exists an e such that $e * a = a$ for
each for (G3′)a; all
and (G3), let $a \in G$, and apply (G3′) to find a' and a'' such that $a' * a = e$ and $a'' * a' = e$. Then

$$a * a' = e * (a * a') = (a'' * a') * (a * a') = a'' * \big((a' * a) * a'\big) = a'' * a' = e,$$

whence (G3), and

$$a = e * a = (a * a') * a = a * (a' * a) = a * e,$$

whence (G2).

(b) A group can be defined to be a set G with a binary operation $*$ satisfying the following conditions: (g1) $*$ is associative; (g2) G is nonempty; (g3) for each $a \in G$, there exists an $a' \in G$ such that $a' * a$ is neutral. As there is at most one neutral element in a set with an associative binary operation, these conditions obviously imply those in (a). They are minimal in the sense that there exist sets with a binary operation satisfying any two of them but not the third. For example, $(\mathbb{N},+)$ satisfies (g1) and (g2) but not (g3); the empty set satisfies (g1) and (g3) but not (g2); the set of integers with $m * n = m - n$ satisfies (g2) and (g3) but not (g1).

Multiplication tables

A binary operation on a finite set can be described by its multiplication table:

	e	a	b	c	$\ldots$
e	ee	ea	eb	ec	$\ldots$
a	ae	a^2	ab	ac	$\ldots$
b	be	ba	b^2	bc	$\ldots$
c	ce	ca	cb	c^2	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

The element e is an identity element if and only if the first row and column of the table simply repeat the elements. Inverses exist if and only if each element occurs exactly once in each row and in each column (see 1.2e). If there are n elements, then verifying the associativity law requires checking n^3 equalities.

For the multiplication table of S_3, see the front page. Note that each colour occurs exactly once in each row and and each column.

This suggests an algorithm for finding all groups of a given finite order n, namely, list all possible multiplication tables and check the axioms. Except for very small n, this is not practical! The table has n^2 positions, and if we allow each position to hold any of the n elements, then that gives a total of n^{n^2} possible tables very few of which define groups. For example, there are $8^{64} = 6277\,101\,735\,386\,680\,763\,835\,789\,423\,207\,666\,416\,102\,355\,444\,464\,034\,512\,896$ binary operations on a set with 8 elements, but only five isomorphism classes of groups of order 8 (see 4.21).

Subgroups

PROPOSITION 1.11 *Let S be a nonempty subset of a group G. If*

S1: $a,b \in S \implies ab \in S$, *and*
S2: $a \in S \implies a^{-1} \in S$,

then the binary operation on G makes S into a group.

PROOF. (S1) implies that the binary operation on G defines a binary operation $S \times S \to S$ on S, which is automatically associative. By assumption S contains at least one element a, its inverse a^{-1}, and the product $e = aa^{-1}$. Finally (S2) shows that the inverses of elements in S lie in S. □

A nonempty subset S satisfying (S1) and (S2) is called a ***subgroup*** of G. When S is finite, condition (S1) implies (S2): let $a \in S$; then $\{a, a^2, \ldots\} \subset S$, and so a has finite order, say $a^n = e$; now $a^{-1} = a^{n-1} \in S$. The example $(\mathbb{N}, +) \subset (\mathbb{Z}, +)$ shows that (S1) does not imply (S2) when S is infinite.

EXAMPLE 1.12 The ***centre*** of a group G is the subset

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

It is a subgroup of G.

PROPOSITION 1.13 *An intersection of subgroups of G is a subgroup of G.*

PROOF. It is nonempty because it contains e, and (S1) and (S2) obviously hold. □

REMARK 1.14 It is generally true that an intersection of subobjects of an algebraic object is a subobject. For example, an intersection of subrings of a ring is a subring, an intersection of submodules of a module is a submodule, and so on.

PROPOSITION 1.15 *For any subset X of a group G, there is a smallest subgroup of G containing X. It consists of all finite products of elements of X and their inverses (repetitions allowed).*

PROOF. The intersection S of all subgroups of G containing X is again a subgroup containing X, and it is evidently the smallest such group. Clearly S contains with X, all finite products of elements of X and their inverses. But the set of such products satisfies (S1) and (S2) and hence is a subgroup containing X. It therefore equals S. □

The subgroup S given by the proposition is denoted $\langle X\rangle$, and is called the ***subgroup generated by*** X. For example, $\langle\emptyset\rangle = \{e\}$. If every element of X has finite order, for example, if G is finite, then the set of all finite products of elements of X is already a group and so equals $\langle X\rangle$.

We say that X ***generates*** G if $G = \langle X\rangle$, i.e., if every element of G can be written as a finite product of elements from X and their inverses. Note that the order of an element a of a group is the order of the subgroup $\langle a\rangle$ it generates.

EXAMPLES

1.16 ***The cyclic groups.*** A group is said to be ***cyclic*** if it is generated by a single element, i.e., if $G = \langle r\rangle$ for some $r \in G$. If r has finite order n, then

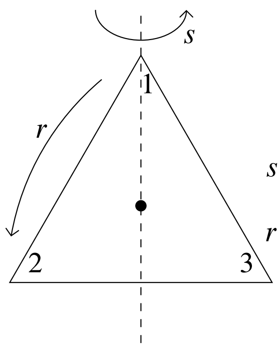
$$G = \{e, r, r^2, ..., r^{n-1}\} \approx C_n, \quad r^i \leftrightarrow i \mod n,$$

and G can be thought of as the group of rotational symmetries about the centre of a regular polygon with n-sides. If r has infinite order, then

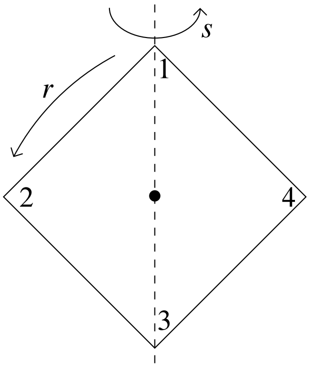
$$G = \{\ldots, r^{-i}, \ldots, r^{-1}, e, r, \ldots, r^i, \ldots\} \approx C_\infty, \quad r^i \leftrightarrow i.$$

Thus, up to isomorphism, there is exactly one cyclic group of order n for each $n \le \infty$. In future, we shall loosely use C_n to denote any cyclic group of order n (not necessarily $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}$).

1.17 ***The dihedral groups*** D_n.[3] For $n \ge 3$, D_n is the group of symmetries of a regular polygon with n-sides.[4] Number the vertices $1, \ldots, n$ in the counterclockwise direction. Let r be the rotation through $2\pi/n$ about the centre of polygon (so $i \mapsto i+1 \mod n$), and let s be the reflection in the line (= rotation about the line) through the vertex 1 and the centre of the polygon (so $i \mapsto n+2-i \mod n$). For example, the pictures



$$s = \begin{cases} 1 \leftrightarrow 1 \\ 2 \leftrightarrow 3 \end{cases}$$
$$r = 1 \to 2 \to 3 \to 1$$



$$s = \begin{cases} 1 \leftrightarrow 1 \\ 2 \leftrightarrow 4 \\ 3 \leftrightarrow 3 \end{cases}$$
$$r = 1 \to 2 \to 3 \to 4 \to 1$$

[3] This group is denoted D_{2n} or D_n depending on whether the author is viewing it abstractly or concretely as the symmetries of an n-polygon (or perhaps on whether the author is a group theorist or not; see mo48434).

[4] More formally, D_n can be defined to be the subgroup of S_n generated by $r{:}i \mapsto i+1 \pmod n$ and $s{:}i \mapsto n+2-i \pmod n$. Then all the statements concerning D_n can proved without appealing to geometry.

illustrate the groups D_3 and D_4. In the general case

$$r^n = e; \quad s^2 = e; \quad srs = r^{-1} \quad (\text{so } sr = r^{n-1}s).$$

These equalites imply that

$$D_n = \{e, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\},$$

and it is clear from the geometry that the elements of the set are distinct, and so $|D_n| = 2n$.

Let t be the reflection in the line through the midpoint of the side joining the vertices 1 and 2 and the centre of the polygon (so $i \mapsto n+3-i \mod n$). Then $r = ts$, because

$$i \overset{s}{\mapsto} n+2-i \overset{t}{\mapsto} n+3-(n+2-i) = i+1 \mod n.$$

Hence $D_n = \langle s, t \rangle$ and

$$s^2 = e, \quad t^2 = e, \quad (ts)^n = e = (st)^n.$$

We define D_1 to be $C_2 = \{1, r\}$ and D_2 to be $C_2 \times C_2 = \{1, r, s, rs\}$. The group D_2 is also called the ***Klein Vierergruppe*** or, more simply, the ***4-group*** and denoted V or V_4. Note that D_3 is the full group of permutations of $\{1,2,3\}$. It is the smallest noncommutative group.

By adding a tick at each vertex of a regular polygon, we can reduce its symmetry group from D_n to C_n. By adding a line from the centre of the polygon to the vertex 1, we reduce its symmetry group to $\langle s \rangle$. Physicist like to say that we have “broken the symmetry”.

1.18 ***The quaternion group*** Q: Let $a = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then

$$a^4 = e, \quad a^2 = b^2, \quad bab^{-1} = a^3 \ (\text{so } ba = a^3 b).$$

The subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by a and b is

$$Q = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

The group Q can also be described as the subset $\{\pm 1, \pm i, \pm j, \pm k\}$ of the quaternion algebra $\mathbb{H}$. Recall that

$$\mathbb{H} = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

with the multiplication determined by

$$i^2 = -1 = j^2, \quad ij = k = -ji.$$

The map $i \mapsto a$, $j \mapsto b$ extends uniquely to a homomorphism $\mathbb{H} \to M_2(\mathbb{C})$ of $\mathbb{R}$-algebras, which maps the group $\langle i, j \rangle$ isomorphically onto $\langle a, b \rangle$.

1.19 Recall that S_n is the permutation group on $\{1, 2, ..., n\}$. A ***transposition*** is a permutation that interchanges two elements and leaves all other elements unchanged. It is not difficult to see that S_n is generated by transpositions (see (4.26) below for a more precise statement).

Groups of small order

> *[For] $n = 6$, there are three* (sic) *groups, a group C_6, and two groups $C_2 \times C_3$ and S_3.*
> Cayley, American J. Math. 1 (1878), p. 51.

For each prime p, there is only one group of order p, namely C_p (see 1.28 below). In the following table, $c + n = t$ means that there are c commutative groups and n noncommutative groups (up to isomorphism, of course).

$\lvert G\rvert$	$c+n=t$	Groups	Ref.
4	$2+0=2$	C_4, $C_2 \times C_2$	4.18
6	$1+1=2$	C_6; S_3	4.23
8	$3+2=5$	C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$; Q, D_4	4.21
9	$2+0=2$	C_9, $C_3 \times C_3$	4.18
10	$1+1=2$	C_{10}; D_5	5.14
12	$2+3=5$	C_{12}, $C_2 \times C_6$; $C_2 \times S_3$, A_4, $C_4 \rtimes C_3$	5.16
14	$1+1=2$	C_{14}; D_7	5.14
15	$1+0=1$	C_{15}	5.14
16	$5+9=14$	See Wild 2005	
18	$2+3=5$	C_{18}, $C_3 \times C_6$; D_9, $S_3 \times C_3$, $(C_3 \times C_3) \rtimes C_2$	
20	$2+3=5$	$C_{20}, C_2 \times C_{10}$; $D_{10}, C_5 \rtimes C_4, \langle a,b \mid a^5 = b^2 = c^2 = abc\rangle$	
21	$1+1=2$	C_{21}; $\langle a,b \mid a^3 = b^7 = 1, ba = ab^2\rangle$	
22	$1+1=2$	C_{22}; D_{11}	5.14
24	$3+12=15$	`groupprops.subwiki.org/wiki/Groups_of_order_24`	

Here $\langle a,b \mid a^5 = b^2 = c^2 = abc\rangle$ is the group with generators a and b and relations $a^5 = b^2 = c^2 = abc$ (see Chapter 2). It is the dicyclic group.

Roughly speaking, the more high powers of primes divide n, the more groups of order n there should be. In fact, if $f(n)$ is the number of isomorphism classes of groups of order n, then

$$f(n) \le n^{(\frac{2}{27}+o(1))e(n)^2},$$

where $e(n)$ is the largest exponent of a prime dividing n and $o(1) \to 0$ as $e(n) \to \infty$ (see Pyber 1993).

By 2001, a complete irredundant list of groups of order ≤ 2000 had been found — up to isomorphism, there are exactly 49,910,529,484 (Besche et al. 2001).[5]

[5] In fact Besche et al. did not construct the groups of order 1024 individually, but it is known that there are 49487365422 groups of that order. The remaining 423164062 groups of order up to 2000 (of which 408641062 have order 1536) are available as libraries in GAP and Magma. I would guess that 2048 is the smallest number such that the exact number of groups of that order is unknown (Derek Holt, mo46855; Nov 21, 2010).

Homomorphisms

DEFINITION 1.20 A ***homomorphism*** from a group G to a second G' is a map $\alpha\colon G \to G'$ such that $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in G$. An ***isomorphism*** is a bijective homomorphism.

For example, the determinant map $\det\colon \mathrm{GL}_n(F) \to F^{\times}$ is a homomorphism.

1.21 Let α be a homomorphism. For any elements $a_1, \ldots, a_m$ of G,

$$\begin{aligned}\alpha(a_1 \cdots a_m) &= \alpha(a_1(a_2 \cdots a_m))\\ &= \alpha(a_1)\alpha(a_2 \cdots a_m)\\ &\cdots\\ &= \alpha(a_1)\cdots\alpha(a_m),\end{aligned}$$

and so homomorphisms preserve all products. In particular, for $m \geq 1$,

$$\alpha(a^m) = \alpha(a)^m. \tag{9}$$

Moreover $\alpha(e) = \alpha(ee) = \alpha(e)\alpha(e)$, and so $\alpha(e) = e$ (apply 1.2a). Also

$$aa^{-1} = e = a^{-1}a \implies \alpha(a)\alpha(a^{-1}) = e = \alpha(a^{-1})\alpha(a),$$

and so $\alpha(a^{-1}) = \alpha(a)^{-1}$. It follows that (9) holds for all $m \in \mathbb{Z}$, and so a homomorphism of commutative groups is also a homomorphism of $\mathbb{Z}$-modules.

As we noted above, each row of the multiplication table of a group is a permutation of the elements of the group. As Cayley pointed out, this allows one to realize the group as a group of permutations.

THEOREM 1.22 (CAYLEY) *There is a canonical injective homomorphism*

$$\alpha\colon G \to \mathrm{Sym}(G).$$

PROOF. For $a \in G$, define $a_L\colon G \to G$ to be the map $x \mapsto ax$ (left multiplication by a). For $x \in G$,

$$(a_L \circ b_L)(x) = a_L(b_L(x)) = a_L(bx) = abx = (ab)_L(x),$$

and so $(ab)_L = a_L \circ b_L$. As $e_L = \mathrm{id}$, this implies that

$$a_L \circ (a^{-1})_L = \mathrm{id} = (a^{-1})_L \circ a_L,$$

and so a_L is a bijection, i.e., $a_L \in \mathrm{Sym}(G)$. Hence $a \mapsto a_L$ is a homomorphism $G \to \mathrm{Sym}(G)$, and it is injective because of the cancellation law. □

COROLLARY 1.23 *A finite group of order n can be realized as a subgroup of S_n.*

PROOF. List the elements of the group as $a_1, \ldots, a_n$. □

Unfortunately, unless n is small, S_n is too large to be manageable. We shall see later (4.22) that G can often be embedded in a permutation group of much smaller order than $n!$.

Cosets

For a subset S of a group G and an element a of G, we let

$$aS = \{as \mid s \in S\}$$
$$Sa = \{sa \mid s \in S\}.$$

Because of the associativity law, $a(bS) = (ab)S$, and so we can denote this set unambiguously by abS.

When H is a subgroup of G, the sets of the form aH are called the ***left cosets*** of H in G, and the sets of the form Ha are called the ***right cosets*** of H in G. Because $e \in H$, $aH = H$ if and only if $a \in H$.

EXAMPLE 1.24 Let $G = (\mathbb{R}^2, +)$, and let H be a subspace of dimension 1 (line through the origin). Then the cosets (left or right) of H are the lines $a + H$ parallel to H.

PROPOSITION 1.25 *Let H be a subgroup of a group G.*

(a) An element a of G lies in a left coset C of H if and only if $C = aH$.

(b) Two left cosets are either disjoint or equal.

(c) $aH = bH$ if and only if $a^{-1}b \in H$.

(d) Any two left cosets have the same number of elements (possibly infinite).

PROOF. (a) Certainly $a \in aH$. Conversely, if a lies in the left coset bH, then $a = bh$ for some h, and so

$$aH = bhH = bH.$$

(b) If C and C' are not disjoint, then they have a common element a, and $C = aH$ and $C' = aH$ by (a).

(c) If $a^{-1}b \in H$, then $H = a^{-1}bH$, and so $aH = aa^{-1}bH = bH$. Conversely, if $aH = bH$, then $H = a^{-1}bH$, and so $a^{-1}b \in H$.

(d) The map $(ba^{-1})_L \colon ah \mapsto bh$ is a bijection $aH \to bH$. □

The ***index*** $(G : H)$ of H in G is defined to be the number of left cosets of H in G.[6] For example, $(G : 1)$ is the order of G.

As the left cosets of H in G cover G, (1.25b) shows that they form a partition G. In other words, the condition "a and b lie in the same left coset" is an equivalence relation on G.

THEOREM 1.26 (LAGRANGE) *If G is finite, then*

$$(G : 1) = (G : H)(H : 1).$$

In particular, the order of every subgroup of a finite group divides the order of the group.

PROOF. The left cosets of H in G form a partition of G, there are $(G : H)$ of them, and each left coset has $(H : 1)$ elements. □

COROLLARY 1.27 *The order of each element of a finite group divides the order of the group.*

[6] More formally, $(G : H)$ is the cardinality of the set $\{aH \mid a \in G\}$.

PROOF. Apply Lagrange's theorem to $H = \langle g \rangle$, recalling that $(H:1) = \mathrm{order}(g)$. □

EXAMPLE 1.28 If G has order p, a prime, then every element of G has order 1 or p. But only e has order 1, and so G is generated by any element $a \neq e$. In particular, G is cyclic and so $G \approx C_p$. This shows, for example, that, up to isomorphism, there is only one group of order $1{,}000{,}000{,}007$ (because this number is prime). In fact there are only two groups of order $1{,}000{,}000{,}014{,}000{,}000{,}049$ (see 4.18).

1.29 For a subset S of G, let $S^{-1} = \{g^{-1} \mid g \in S\}$. Then $(aH)^{-1}$ is the right coset Ha^{-1}, and $(Ha)^{-1} = a^{-1}H$. Therefore $S \mapsto S^{-1}$ defines a one-to-one correspondence between the set of left cosets and the set of right cosets under which $aH \leftrightarrow Ha^{-1}$. Hence $(G:H)$ is also the number of right cosets of H in G. But, in general, a left coset will *not* be a right coset (see 1.34 below).

1.30 Lagrange's theorem has a partial converse: if a *prime* p divides $m = (G:1)$, then G has an *element* of order p (Cauchy's theorem 4.13); if a *prime power* p^n divides m, then G has a *subgroup* of order p^n (Sylow's theorem 5.2). However, note that the 4-group $C_2 \times C_2$ has order 4, but has no element of order 4, and A_4 has order 12, but has no subgroup of order 6 (see Exercise 4-15).

More generally, we have the following result.

PROPOSITION 1.31 *For any subgroups $H \supset K$ of G,*

$$(G:K) = (G:H)(H:K)$$

(meaning either both are infinite or both are finite and equal).

PROOF. Write $G = \bigsqcup_{i \in I} g_i H$ (disjoint union), and $H = \bigsqcup_{j \in J} h_j K$ (disjoint union). On multiplying the second equality by g_i, we find that $g_i H = \bigsqcup_{j \in J} g_i h_j K$ (disjoint union), and so $G = \bigsqcup_{i,j \in I \times J} g_i h_j K$ (disjoint union). This shows that

$$(G:K) = |I||J| = (G:H)(H:K).$$ □

Normal subgroups

When S and T are two subsets of a group G, we let

$$ST = \{st \mid s \in S, t \in T\}.$$

Because of the associativity law, $R(ST) = (RS)T$, and so we can denote this set unambiguously as RST.

A subgroup N of G is ***normal***, denoted $N \triangleleft G$, if $gNg^{-1} = N$ for all $g \in G$.

REMARK 1.32 To show that N is normal, it suffices to check that $gNg^{-1} \subset N$ for all g, because multiplying this inclusion on the left and right with g^{-1} and g respectively gives the inclusion $N \subset g^{-1}Ng$, and rewriting this with g^{-1} for g gives that $N \subset gNg^{-1}$ for all g. However, the next example shows that there can exist a subgroup N of a group G and an element g of G such that $gNg^{-1} \subset N$ but $gNg^{-1} \neq N$.

EXAMPLE 1.33 Let $G = \mathrm{GL}_2(\mathbb{Q})$, and let $H = \left\{\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right) \,\middle|\, n \in \mathbb{Z}\right\}$. Then H is a subgroup of G; in fact $H \simeq \mathbb{Z}$. Let $g = \left(\begin{smallmatrix}5 & 0\\ 0 & 1\end{smallmatrix}\right)$. Then

$$g\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}g^{-1} = \begin{pmatrix}5 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\begin{pmatrix}5^{-1} & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 5n\\ 0 & 1\end{pmatrix}.$$

Hence $gHg^{-1} \subsetneqq H$ (and $g^{-1}Hg \not\subset H$).

PROPOSITION 1.34 *A subgroup N of G is normal if and only if every left coset of N in G is also a right coset, in which case, $gN = Ng$ for all $g \in G$.*

PROOF. Clearly,

$$gNg^{-1} = N \iff gN = Ng.$$

Thus, if N is normal, then every left coset is a right coset (in fact, $gN = Ng$). Conversely, if the left coset gN is also a right coset, then it must be the right coset Ng by (1.25a). Hence $gN = Ng$, and so $gNg^{-1} = N$. □

1.35 The proposition says that, in order for N to be normal, we must have that for all $g \in G$ and $n \in N$, there exists an $n' \in N$ such that $gn = n'g$ (equivalently, for all $g \in G$ and $n \in N$, there exists an n' such that $ng = gn'$). In other words, to say that N is normal amounts to saying that an element of G can be moved past an element of N at the cost of replacing the element of N by another element of N.

EXAMPLE 1.36 (a) Every subgroup of index two is normal. Indeed, let $g \in G \smallsetminus H$. Then $G = H \sqcup gH$ (disjoint union). Hence gH is the complement of H in G. Similarly, Hg is the complement of H in G, and so $gH = Hg$.

(b) Consider the dihedral group

$$D_n = \{e, r, \ldots, r^{n-1}, s, \ldots, r^{n-1}s\}.$$

Then $C_n = \{e, r, \ldots, r^{n-1}\}$ has index 2, and hence is normal. For $n \geq 3$ the subgroup $\{e, s\}$ is not normal because $r^{-1}sr = r^{n-2}s \notin \{e, s\}$.

(c) Every subgroup of a commutative group is normal (obviously), but the converse is false: the quaternion group Q is not commutative, but every subgroup is normal (see Exercise 1-1).

A group G is said to be ***simple*** if it has no normal subgroups other than G and $\{e\}$. Such a group can still have lots of nonnormal subgroups — in fact, the Sylow theorems (Chapter 5) imply that every finite group has nontrivial subgroups unless it is cyclic of prime order.

PROPOSITION 1.37 *If H and N are subgroups of G and N is normal, then HN is a subgroup of G. If H is also normal, then HN is a normal subgroup of G.*

PROOF. The set HN is nonempty, and

$$(h_1n_1)(h_2n_2) \overset{1.35}{=} h_1h_2n_1'n_2 \in HN,$$

and so it is closed under multiplication. Since

$$(hn)^{-1} = n^{-1}h^{-1} \overset{1.35}{=} h^{-1}n' \in HN$$

it is also closed under the formation of inverses, and so HN is a subgroup. If both H and N are normal, then

$$gHNg^{-1} = gHg^{-1} \cdot gNg^{-1} = HN$$

for all $g \in G$. □

An intersection of normal subgroups of a group is again a normal subgroup (cf. 1.14). Therefore, we can define the ***normal subgroup generated by a subset*** X of a group G to be the intersection of the normal subgroups containing X. Its description in terms of X is a little complicated. We say that a subset X of a group G is ***normal*** (or ***closed under conjugation***) if $gXg^{-1} \subset X$ for all $g \in G$.

LEMMA 1.38 *If X is normal, then the subgroup $\langle X \rangle$ generated by it is normal.*

PROOF. The map "conjugation by g", $a \mapsto gag^{-1}$, is a homomorphism $G \to G$. If $a \in \langle X \rangle$, say, $a = x_1 \cdots x_m$ with each x_i or its inverse in X, then

$$gag^{-1} = (gx_1g^{-1}) \cdots (gx_mg^{-1}).$$

As X is closed under conjugation, each gx_ig^{-1} or its inverse lies in X, and so $g\langle X \rangle g^{-1} \subset \langle X \rangle$. □

LEMMA 1.39 *For any subset X of G, the subset $\bigcup_{g \in G} gXg^{-1}$ is normal, and it is the smallest normal set containing X.*

PROOF. Obvious. □

On combining these lemmas, we obtain the following proposition.

PROPOSITION 1.40 *The normal subgroup generated by a subset X of G is $\langle \bigcup_{g \in G} gXg^{-1} \rangle$.*

Kernels and quotients

The ***kernel*** of a homomorphism $\alpha: G \to G'$ is

$$\text{Ker}(\alpha) = \{g \in G \mid \alpha(g) = e\}.$$

If α is injective, then $\text{Ker}(\alpha) = \{e\}$. Conversely, if $\text{Ker}(\alpha) = \{e\}$, then α is injective, because

$$\alpha(g) = \alpha(g') \implies \alpha(g^{-1}g') = e \implies g^{-1}g' = e \implies g = g'.$$

PROPOSITION 1.41 *The kernel of a homomorphism is a normal subgroup.*

PROOF. It is obviously a subgroup, and if $a \in \text{Ker}(\alpha)$, so that $\alpha(a) = e$, and $g \in G$, then

$$\alpha(gag^{-1}) = \alpha(g)\alpha(a)\alpha(g)^{-1} = \alpha(g)\alpha(g)^{-1} = e.$$

Hence $gag^{-1} \in \text{Ker}(\alpha)$. □

For example, the kernel of the homomorphism $\det: \text{GL}_n(F) \to F^\times$ is the group of $n \times n$ matrices with determinant 1 — this group $\text{SL}_n(F)$ is called the ***special linear group of degree*** n.

PROPOSITION 1.42 *Every normal subgroup occurs as the kernel of a homomorphism. More precisely, if N is a normal subgroup of G, then there is a unique group structure on the set G/N of cosets of N in G for which the natural map $a \mapsto [a]\colon G \to G/N$ is a homomorphism.*

PROOF. Write the cosets as left cosets, and define $(aN)(bN) = (ab)N$. We have to check (a) that this is well-defined, and (b) that it gives a group structure on the set of cosets. It will then be obvious that the map $g \mapsto gN$ is a homomorphism with kernel N.

(a). Let $aN = a'N$ and $bN = b'N$; we have to show that $abN = a'b'N$. But

$$abN = a(bN) = a(b'N) \overset{1.34}{=} aNb' = a'Nb' \overset{1.34}{=} a'b'N.$$

(b). The product is certainly associative, the coset N is an identity element, and $a^{-1}N$ is an inverse for aN. □

The group G/N is called the[7] ***quotient*** of G by N.

Propositions 1.41 and 1.42 show that the normal subgroups are exactly the kernels of homomorphisms.

PROPOSITION 1.43 *The map $a \mapsto aN\colon G \to G/N$ has the following universal property: for any homomorphism $\alpha\colon G \to G'$ of groups such that $\alpha(N) = \{e\}$, there exists a unique homomorphism $G/N \to G'$ making the diagram at right commute:*

$$\begin{tikzcd} G \arrow[r, "a\mapsto aN"] \arrow[dr, "\alpha"'] & G/N \arrow[d, dashed] \\ & G'. \end{tikzcd}$$

PROOF. Note that for $n \in N$, $\alpha(gn) = \alpha(g)\alpha(n) = \alpha(g)$, and so α is constant on each left coset gN of N in G. It therefore defines a map

$$\bar{\alpha}\colon G/N \to G', \quad \bar{\alpha}(gN) = \alpha(g),$$

and $\bar{\alpha}$ is a homomorphism because

$$\bar{\alpha}((gN)\cdot(g'N)) = \bar{\alpha}(gg'N) = \alpha(gg') = \alpha(g)\alpha(g') = \bar{\alpha}(gN)\bar{\alpha}(g'N).$$

The uniqueness of $\bar{\alpha}$ follows from the surjectivity of $G \to G/N$. □

EXAMPLE 1.44 (a) Consider the subgroup $m\mathbb{Z}$ of $\mathbb{Z}$. The quotient group $\mathbb{Z}/m\mathbb{Z}$ is a cyclic group of order m.

(b) Let L be a line through the origin in $\mathbb{R}^2$. Then $\mathbb{R}^2/L$ is isomorphic to $\mathbb{R}$ (because it is a one-dimensional vector space over $\mathbb{R}$).

(c) For $n \geq 2$, the quotient $D_n/\langle r\rangle = \{\bar{e}, \bar{s}\}$ (cyclic group of order 2).

Theorems concerning homomorphisms

The theorems in this subsection are sometimes called the isomorphism theorems (first, second, ..., or first, third, ..., or ...).

[7] Some authors say “factor” instead of “quotient”, but this can be confused with “direct factor”.

FACTORIZATION OF HOMOMORPHISMS

Recall that the image of a map $\alpha\colon S \to T$ is $\alpha(S) = \{\alpha(s) \mid s \in S\}$.

THEOREM 1.45 (HOMOMORPHISM THEOREM) *For any homomorphism $\alpha\colon G \to G'$ of groups, the kernel N of α is a normal subgroup of G, the image I of α is a subgroup of G', and α factors in a natural way into the composite of a surjection, an isomorphism, and an injection:*

$$\begin{tikzcd}
G \arrow[r, "\alpha"] \arrow[d, "g\mapsto gN"', "\text{surjective}"] & G' \\
G/N \arrow[r, "gN\mapsto\alpha(g)", "\text{isomorphism}"'] & I. \arrow[u, "\text{injective}"']
\end{tikzcd}$$

PROOF. We have already seen (1.41) that the kernel is a normal subgroup of G. If $b = \alpha(a)$ and $b' = \alpha(a')$, then $bb' = \alpha(aa')$ and $b^{-1} = \alpha(a^{-1})$, and so $I \overset{\text{def}}{=} \alpha(G)$ is a subgroup of G'. The universal property of quotients (1.43) shows that the map $x \mapsto \alpha(x)\colon G \to I$ defines a homomorphism $\bar{\alpha}\colon G/N \to I$ with $\bar{\alpha}(gN) = \alpha(g)$. The homomorphism $\bar{\alpha}$ is certainly surjective, and if $\bar{\alpha}(gN) = e$, then $g \in \operatorname{Ker}(\alpha) = N$, and so $\bar{\alpha}$ has trivial kernel. This implies that it is injective (p. 20). □

THE ISOMORPHISM THEOREM

THEOREM 1.46 (ISOMORPHISM THEOREM) *Let H be a subgroup of G and N a normal subgroup of G. Then HN is a subgroup of G, $H \cap N$ is a normal subgroup of H, and the map*

$$h(H \cap N) \mapsto hN\colon H/H \cap N \to HN/N$$

is an isomorphism.

PROOF. We have already seen (1.37) that HN is a subgroup. Consider the map

$$H \to G/N, \quad h \mapsto hN.$$

This is a homomorphism, and its kernel is $H \cap N$, which is therefore normal in H. According to Theorem 1.45, the map induces an isomorphism $H/H \cap N \to I$, where I is its image. But I is the set of cosets of the form hN with $h \in H$, i.e., $I = HN/N$. □

It is not necessary to assume that N be normal in G as long as $hNh^{-1} = N$ for all $h \in H$ (i.e., H is contained in the normalizer of N — see later). Then $H \cap N$ is still normal in H, but it need not be a normal subgroup of G.

THE CORRESPONDENCE THEOREM

The next theorem shows that if $\bar{G}$ is a quotient group of G, then the lattice of subgroups in $\bar{G}$ captures the structure of the lattice of subgroups of G lying over the kernel of $G \to \bar{G}$.

THEOREM 1.47 (CORRESPONDENCE THEOREM) *Let $\alpha\colon G \twoheadrightarrow \bar{G}$ be a surjective homomorphism, and let $N = \operatorname{Ker}(\alpha)$. Then there is a one-to-one correspondence*

$$\{\text{subgroups of } G \text{ containing } N\} \overset{1:1}{\leftrightarrow} \{\text{subgroups of } \bar{G}\}$$

under which a subgroup H of G containing N corresponds to $\bar{H} = \alpha(H)$ and a subgroup $\bar{H}$ of $\bar{G}$ corresponds to $H = \alpha^{-1}(\bar{H})$. Moreover, if $H \leftrightarrow \bar{H}$ and $H' \leftrightarrow \bar{H}'$, then

(a) $\bar{H} \subset \bar{H}' \iff H \subset H'$, *in which case* $(\bar{H}' : \bar{H}) = (H' : H)$;
(b) $\bar{H}$ *is normal in* $\bar{G}$ *if and only if* H *is normal in* G, *in which case,* α *induces an isomorphism*

$$G/H \xrightarrow{\simeq} \bar{G}/\bar{H}.$$

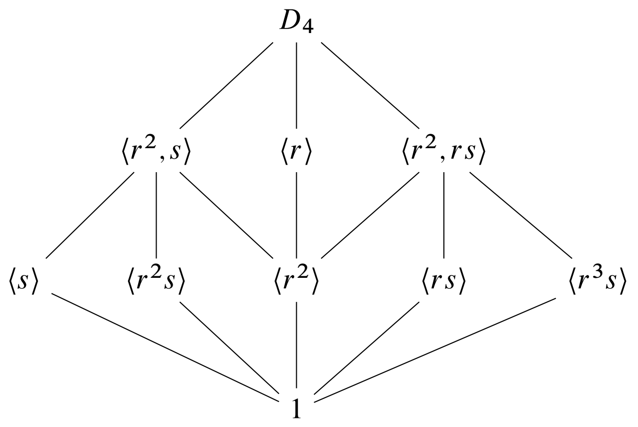
PROOF. If $\bar{H}$ is a subgroup of $\bar{G}$, then $\alpha^{-1}(\bar{H})$ is easily seen to be a subgroup of G containing N, and if H is a subgroup of G, then $\alpha(H)$ is a subgroup of $\bar{G}$ (see 1.45). Clearly, $\alpha^{-1}\alpha(H) = HN$, which equals H if and only if $H \supset N$, and $\alpha\alpha^{-1}(\bar{H}) = \bar{H}$. Therefore, the two operations give the required bijection. The remaining statements are easily verified. For example, a decomposition $H' = \bigsqcup_{i\in I} a_i H$ of H' into a disjoint union of left cosets of H gives a similar decomposition $\bar{H}' = \bigsqcup_{i\in I} \alpha(a_i)\bar{H}$ of $\bar{H}'$. □

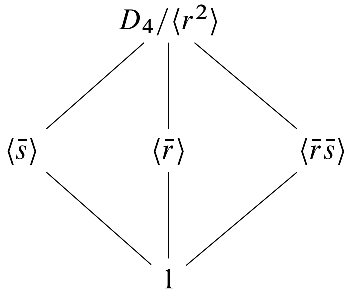
COROLLARY 1.48 *Let* N *be a normal subgroup of* G; *then there is a one-to-one correspondence between the set of subgroups of* G *containing* N *and the set of subgroups of* G/N, $H \leftrightarrow H/N$. *Moreover* H *is normal in* G *if and only if* H/N *is normal in* G/N, *in which case the homomorphism* $g \mapsto gN : G \to G/N$ *induces an isomorphism*

$$G/H \xrightarrow{\simeq} (G/N)/(H/N).$$

PROOF. This is the special case of the theorem in which α is $g \mapsto gN : G \to G/N$. □

EXAMPLE 1.49 Let $G = D_4$ and let N be its subgroup $\langle r^2\rangle$. Recall (1.17) that $srs^{-1} = r^3$, and so $sr^2s^{-1} = \left(r^3\right)^2 = r^2$. Therefore N is normal. The groups G and G/N have the following lattices of subgroups:





Direct products

Let G be a group, and let $H_1,\ldots,H_k$ be subgroups of G. We say that G is a ***direct product*** of the subgroups H_i if the map

$$(h_1,h_2,\ldots,h_k) \mapsto h_1h_2\cdots h_k : H_1 \times H_2 \times \cdots \times H_k \to G$$

is an isomorphism of groups. This means that each element g of G can be written uniquely in the form $g = h_1h_2\cdots h_k$, $h_i \in H_i$, and that if $g = h_1h_2\cdots h_k$ and $g' = h_1'h_2'\cdots h_k'$, then

$$gg' = (h_1h_1')(h_2h_2')\cdots(h_kh_k').$$

The following propositions give criteria for a group to be a direct product of subgroups.

PROPOSITION 1.50 *A group G is a direct product of subgroups H_1, H_2 if and only if*

(a) $G = H_1H_2$,
(b) $H_1 \cap H_2 = \{e\}$, *and*
(c) *every element of H_1 commutes with every element of H_2.*

PROOF. If G is the direct product of H_1 and H_2, then certainly (a) and (c) hold, and (b) holds because, for any $g \in H_1 \cap H_2$, the element (g, g^{-1}) maps to e under $(h_1, h_2) \mapsto h_1h_2$ and so equals (e, e).

Conversely, (c) implies that $(h_1, h_2) \mapsto h_1h_2$ is a homomorphism, and (b) implies that it is injective:

$$h_1h_2 = e \implies h_1 = h_2^{-1} \in H_1 \cap H_2 = \{e\}.$$

Finally, (a) implies that it is surjective. □

PROPOSITION 1.51 *A group G is a direct product of subgroups H_1, H_2 if and only if*

(a) $G = H_1H_2$,
(b) $H_1 \cap H_2 = \{e\}$, *and*
(c) *H_1 and H_2 are both normal in G.*

PROOF. Certainly, these conditions are implied by those in the previous proposition, and so it remains to show that they imply that each element h_1 of H_1 commutes with each element h_2 of H_2. Two elements h_1, h_2 of a group commute if and only if their commutator

$$[h_1, h_2] \overset{\text{def}}{=} (h_1h_2)(h_2h_1)^{-1}$$

is e. But

$$(h_1h_2)(h_2h_1)^{-1} = h_1h_2h_1^{-1}h_2^{-1} = \begin{cases} (h_1h_2h_1^{-1}) \cdot h_2^{-1} \\ h_1 \cdot \left(h_2h_1^{-1}h_2^{-1}\right) \end{cases},$$

which is in H_2 because H_2 is normal, and is in H_1 because H_1 is normal. Therefore (b) implies $[h_1, h_2] = e$. □

PROPOSITION 1.52 *A group G is a direct product of subgroups $H_1, H_2, \ldots, H_k$ if and only if*

(a) $G = H_1H_2 \cdots H_k$,
(b) *for each j, $H_j \cap (H_1 \cdots H_{j-1}H_{j+1} \cdots H_k) = \{e\}$, and*
(c) *each of $H_1, H_2, \ldots, H_k$ is normal in G,*

PROOF. The necessity of the conditions being obvious, we shall prove only the sufficiency. For $k = 2$, we have just done this, and so we argue by induction on k. An induction argument using (1.37) shows that $H_1 \cdots H_{k-1}$ is a normal subgroup of G. The conditions (a,b,c) hold for the subgroups $H_1, \ldots, H_{k-1}$ of $H_1 \cdots H_{k-1}$, and so the induction hypothesis shows that

$$(h_1, h_2, \ldots, h_{k-1}) \mapsto h_1h_2 \cdots h_{k-1} \colon H_1 \times H_2 \times \cdots \times H_{k-1} \to H_1H_2 \cdots H_{k-1}$$

is an isomorphism. The pair $H_1 \cdots H_{k-1}$, H_k satisfies the hypotheses of (1.51), and so

$$(h, h_k) \mapsto hh_k \colon (H_1 \cdots H_{k-1}) \times H_k \to G$$

is also an isomorphism. The composite of these isomorphisms

$$H_1 \times \cdots \times H_{k-1} \times H_k \xrightarrow{(h_1, \ldots, h_k) \mapsto (h_1 \cdots h_{k-1}, h_k)} H_1 \cdots H_{k-1} \times H_k \xrightarrow{(h, h_k) \mapsto hh_k} G$$

sends $(h_1, h_2, \ldots, h_k)$ to $h_1h_2 \cdots h_k$. □

Commutative groups

The classification of finitely generated commutative groups is most naturally studied as part of the theory of modules over a principal ideal domain, but, for the sake of completeness, I include an elementary exposition here.

Let M be a commutative group, written additively. The subgroup $\langle x_1,\ldots,x_k\rangle$ of M generated by the elements $x_1,\ldots,x_k$ consists of the sums $\sum m_i x_i$, $m_i \in \mathbb{Z}$. A subset $\{x_1,\ldots,x_k\}$ of M is a ***basis*** for M if it generates M and

$$m_1x_1+\cdots+m_kx_k=0, \quad m_i\in\mathbb{Z} \implies m_ix_i=0 \text{ for every } i;$$

then

$$M=\langle x_1\rangle\oplus\cdots\oplus\langle x_k\rangle.$$

LEMMA 1.53 *Let $x_1,\ldots,x_k$ generate M. For any $c_1,\ldots,c_k\in\mathbb{N}$ with $\gcd(c_1,\ldots,c_k)=1$, there exist generators $y_1,\ldots,y_k$ for M such that $y_1=c_1x_1+\cdots+c_kx_k$.*

PROOF. We argue by induction on $s=c_1+\cdots+c_k$. The lemma certainly holds if $s=1$, and so we assume $s>1$. Then, at least two c_i are nonzero, say, $c_1\geq c_2>0$. Now

- ◇ $\{x_1,x_2+x_1,x_3,\ldots,x_k\}$ generates M,
- ◇ $\gcd(c_1-c_2,c_2,c_3,\ldots,c_k)=1$, and
- ◇ $(c_1-c_2)+c_2+\cdots+c_k<s$,

and so, by induction, there exist generators $y_1,\ldots,y_k$ for M such that

$$\begin{aligned} y_1 &= (c_1-c_2)x_1+c_2(x_1+x_2)+c_3x_3+\cdots+c_kx_k \\ &= c_1x_1+\cdots+c_kx_k. \end{aligned}$$

□

THEOREM 1.54 *Every finitely generated commutative group M has a basis; hence it is a finite direct sum of cyclic groups.*

PROOF. [8]We argue by induction on the number of generators of M. If M can be generated by one element, the statement is trivial, and so we may assume that it requires at least $k>1$ generators. Among the generating sets $\{x_1,\ldots,x_k\}$ for M with k elements there is one for which the order of x_1 is the smallest possible. We shall show that M is then the direct sum of $\langle x_1\rangle$ and $\langle x_2,\ldots,x_k\rangle$. This will complete the proof, because the induction hypothesis provides us with a basis for the second group, which together with x_1 forms a basis for M.

If M is not the direct sum of $\langle x_1\rangle$ and $\langle x_2,\ldots,x_k\rangle$, then there exists a relation

$$m_1x_1+m_2x_2+\cdots+m_kx_k=0 \tag{10}$$

with $m_1x_1\neq 0$. After possibly changing the sign of some of the x_i, we may suppose that $m_1,\ldots,m_k\in\mathbb{N}$ and $m_1<\text{order}(x_1)$. Let $d=\gcd(m_1,\ldots,m_k)>0$, and let $c_i=m_i/d$. According to the lemma, there exists a generating set $y_1,\ldots,y_k$ such that $y_1=c_1x_1+\cdots+c_kx_k$. But

$$dy_1=m_1x_1+m_2x_2+\cdots+m_kx_k=0$$

and $d\leq m_1<\text{order}(x_1)$, and so this contradicts the choice of $\{x_1,\ldots,x_k\}$. □

[8] John Stillwell tells me that, for finite commutative groups, this is similar to the first proof of the theorem, given by Kronecker in 1870.

COROLLARY 1.55 *A finite commutative group is cyclic if, for each $n > 0$, it contains at most n elements of order dividing n.*

PROOF. After the Theorem 1.54, we may suppose that $G = C_{n_1} \times \cdots \times C_{n_r}$ with $n_i \in \mathbb{N}$. If n divides n_i and n_j with $i \neq j$, then G has more than n elements of order dividing n. Therefore, the hypothesis implies that the n_i are relatively prime. Let a_i generate the ith factor. Then $(a_1,\ldots,a_r)$ has order $n_1 \cdots n_r$, and so generates G. □

EXAMPLE 1.56 Let F be a field. The elements of order dividing n in $F^\times$ are the roots of the polynomial $X^n - 1$. Because unique factorization holds in $F[X]$, there are at most n of these, and so the corollary shows that every finite subgroup of $F^\times$ is cyclic.

THEOREM 1.57 *A nonzero finitely generated commutative group M can be expressed*

$$M \approx C_{n_1} \times \cdots \times C_{n_s} \times C_\infty^r \tag{11}$$

for certain integers $n_1,\ldots,n_s \geq 2$ and $r \geq 0$. Moreover,

(a) *r is uniquely determined by M;*
(b) *the n_i can be chosen so that $n_1 \geq 2$ and $n_1|n_2,\ldots,n_{s-1}|n_s$, and then they are uniquely determined by M;*
(c) *the n_i can be chosen to be powers of prime numbers, and then they are uniquely determined by M.*

The number r is called the ***rank*** of M. By r being uniquely determined by M, we mean that in any two decompositions of M of the form (11), the number of copies of C_∞ will be the same (and similarly for the n_i in (b) and (c)). The integers $n_1,\ldots,n_s$ in (b) are called the ***invariant factors*** of M. Statement (c) says that M can be expressed

$$M \approx C_{p_1^{e_1}} \times \cdots \times C_{p_t^{e_t}} \times C_\infty^r, \quad e_i \geq 1, \tag{12}$$

for certain prime powers $p_i^{e_i}$ (repetitions of primes allowed), and that the integers $p_1^{e_1},\ldots,p_t^{e_t}$ are uniquely determined by M; they are called the ***elementary divisors*** of M.

PROOF. The first assertion is a restatement of Theorem 1.54.

(a) For a prime p not dividing any of the n_i,

$$M/pM \approx (C_\infty/pC_\infty)^r \approx (\mathbb{Z}/p\mathbb{Z})^r,$$

and so r is the dimension of M/pM as an $\mathbb{F}_p$-vector space.

(b,c) If $\gcd(m,n) = 1$, then $C_m \times C_n$ contains an element of order mn, and so

$$C_m \times C_n \approx C_{mn}. \tag{13}$$

Use (13) to decompose the C_{n_i} into products of cyclic groups of prime power order. Once this has been achieved, (13) can be used to combine factors to achieve a decomposition as in (b); for example, $C_{n_s} = \prod C_{p_i^{e_i}}$, where the product is over the distinct primes among the p_i and e_i is the highest exponent for the prime p_i.

In proving the uniqueness statements in (b) and (c), we can replace M with its torsion subgroup (and so assume $r = 0$). A prime p will occur as one of the primes p_i in (12) if and only M has an element of order p, in which case p will occur exact a times, where p^a

is the number of elements of order dividing p. Similarly, p^2 will divide some $p_i^{e_i}$ in (12) if and only if M has an element of order p^2, in which case it will divide exactly b of the $p_i^{e_i}$, where $p^{a-b}p^{2b}$ is the number of elements in M of order dividing p^2. Continuing in this fashion, we find that the elementary divisors of M can be read off from knowing the numbers of elements of M of each prime power order.

The uniqueness of the invariant factors can be derived from that of the elementary divisors, or it can be proved directly: n_s is the smallest integer > 0 such that $n_s M = 0$; n_{s-1} is the smallest integer > 0 such that $n_{s-1}M$ is cyclic; n_{s-2} is the smallest integer such that n_{s-2} can be expressed as a product of two cyclic groups, and so on. □

SUMMARY 1.58 Each finite commutative group is isomorphic to exactly one of the groups

$$C_{n_1} \times \cdots \times C_{n_r}, \quad n_1|n_2, \ldots, n_{r-1}|n_r.$$

The order of this group is $n_1 \cdots n_r$. For example, each commutative group of order 90 is isomorphic to exactly one of C_{90} or $C_3 \times C_{30}$ — to see this, note that the largest invariant factor must be a factor of 90 divisible by all the prime factors of 90.

THE LINEAR CHARACTERS OF A COMMUTATIVE GROUP

Let $\mu(\mathbb{C}) = \{z \in \mathbb{C} \mid |z| = 1\}$. This is an infinite group. For any integer n, the set $\mu_n(\mathbb{C})$ of elements of order dividing n is cyclic of order n; in fact,

$$\mu_n(\mathbb{C}) = \{e^{2\pi i m/n} \mid 0 \leq m \leq n-1\} = \{1, \zeta, \ldots, \zeta^{n-1},\}$$

where $\zeta = e^{2\pi i/n}$ is a primitive nth root of 1.

A ***linear character*** (or just ***character***) of a group G is a homomorphism $G \to \mu(\mathbb{C})$. The homomorphism $a \mapsto 1$ is called the ***trivial*** (or ***principal***) ***character.***

EXAMPLE 1.59 The Legendre symbol modulo p of an integer a not divisible by p is

$$\left(\frac{a}{p}\right) \overset{\text{def}}{=} \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{Z}/p\mathbb{Z} \\ -1 & \text{otherwise.} \end{cases}$$

Clearly, this depends only on a modulo p, and if neither a nor b is divisible by p, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ (because $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic). Therefore $[a] \mapsto \left(\frac{a}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\} = \mu_2(\mathbb{C})$ is a character of $(\mathbb{Z}/p\mathbb{Z})^\times$, sometimes called the quadratic character.

The set of characters of a group G becomes a group $G^\vee$ under the addition,

$$(\chi + \chi')(g) = \chi(g)\chi'(g),$$

called the ***dual group*** of G. For example, the dual group $\mathbb{Z}^\vee$ of $\mathbb{Z}$ is isomorphic to $\mu(\mathbb{C})$ by the map $\chi \mapsto \chi(1)$.

THEOREM 1.60 *Let G be a finite commutative group.*

(a) *The dual of $G^\vee$ is isomorphic to G.*
(b) *The map $G \to G^{\vee\vee}$ sending an element a of G to the character $\chi \mapsto \chi(a)$ of $G^\vee$ is an isomorphism.*

In other words, $G \approx G^\vee$ and $G \simeq G^{\vee\vee}$.

PROOF. The statements are obvious for cyclic groups, and $(G \times H)^\vee \simeq G^\vee \times H^\vee$. □

ASIDE 1.61 The statement that the natural map $G \to G^{\vee\vee}$ is an isomorphism is a special case of the Pontryagin theorem. For infinite groups, it is necessary to consider groups together with a topology. For example, as we observed above, $\mathbb{Z}^\vee \simeq \mu(\mathbb{C})$. Each $m \in \mathbb{Z}$ does define a character $\zeta \mapsto \zeta^m : \mu(\mathbb{C}) \to \mu(\mathbb{C})$, but there are many homomorphisms $\mu(\mathbb{C}) \to \mu(\mathbb{C})$ not of this form, and so the dual of $\mu(\mathbb{C})$ is larger than $\mathbb{Z}$. However, *these are the only continuous homomorphisms.* In general, let G be a commutative group endowed with a locally compact topology[9] for which the group operations are continuous; then the group $G^\vee$ of *continuous characters* $G \to \mu(\mathbb{C})$ has a natural topology for which it is locally compact, and the Pontryagin duality theorem says that the natural map $G \to G^{\vee\vee}$ is an isomorphism.

THEOREM 1.62 (ORTHOGONALITY RELATIONS) *Let G be a finite commutative group. For any characters χ and ψ of G,*

$$\sum\nolimits_{a \in G} \chi(a)\psi(a^{-1}) = \begin{cases} |G| & \text{if } \chi = \psi \\ 0 & \text{otherwise.} \end{cases}$$

In particular,

$$\sum\nolimits_{a \in G} \chi(a) = \begin{cases} |G| & \text{if } \chi \text{ is trivial} \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. If $\chi = \psi$, then $\chi(a)\psi(a^{-1}) = 1$, and so the sum is $|G|$. Otherwise there exists a $b \in G$ such that $\chi(b) \neq \psi(b)$. As a runs over G, so also does ab, and so

$$\sum\nolimits_{a \in G} \chi(a)\psi(a^{-1}) = \sum\nolimits_{a \in G} \chi(ab)\psi((ab)^{-1}) = \chi(b)\psi(b)^{-1} \sum\nolimits_{a \in G} \chi(a)\psi(a^{-1}).$$

Because $\chi(b)\psi(b)^{-1} \neq 1$, this implies that $\sum_{a \in G} \chi(a)\psi(a^{-1}) = 0$. □

COROLLARY 1.63 *For any $a \in G$,*

$$\sum\nolimits_{\chi \in G^\vee} \chi(a) = \begin{cases} |G| & \text{if } a = e \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. Apply the theorem to $G^\vee$, noting that $(G^\vee)^\vee \simeq G$. □

The order of *ab*

Let a and b be elements of a group G. If a has order m and b has order n, what can we say about the order of ab? The next theorem shows that we can say nothing at all.

THEOREM 1.64 *For any integers $m, n, r > 1$, there exists a finite group G with elements a and b such that a has order m, b has order n, and ab has order r.*

PROOF. We shall show that, for a suitable prime power q, there exist elements a and b of $\mathrm{SL}_2(\mathbb{F}_q)$ such that a, b, and ab have orders $2m$, $2n$, and $2r$ respectively. As $-I$ is the unique element of order 2 in $\mathrm{SL}_2(\mathbb{F}_q)$, the images of a, b, ab in $\mathrm{SL}_2(\mathbb{F}_q)/\{\pm I\}$ will then have orders m, n, and r as required.

[9] Following Bourbaki, I require locally compact spaces to be Hausdorff.

Let p be a prime number not dividing $2mnr$. Then p is a unit in the finite ring $\mathbb{Z}/2mnr\mathbb{Z}$, and so some power of it, q say, is 1 in the ring. This means that $2mnr$ divides $q-1$. As the group $\mathbb{F}_q^\times$ has order $q-1$ and is cyclic (see 1.56), there exist elements u, v, and w of $\mathbb{F}_q^\times$ having orders $2m$, $2n$, and $2r$ respectively. Let

$$a=\begin{pmatrix} u & 1 \\ 0 & u^{-1}\end{pmatrix} \text{ and } b=\begin{pmatrix} v & 0 \\ t & v^{-1}\end{pmatrix} \qquad \text{(elements of } \mathrm{SL}_2(\mathbb{F}_q)),$$

where t has been chosen so that

$$uv+t+u^{-1}v^{-1}=w+w^{-1}.$$

The characteristic polynomial of a is $(X-u)(X-u^{-1})$, and so a is similar to $\mathrm{diag}(u,u^{-1})$. Therefore a has order $2m$. Similarly b has order $2n$. The matrix

$$ab=\begin{pmatrix} uv+t & v^{-1} \\ u^{-1}t & u^{-1}v^{-1}\end{pmatrix},$$

has characteristic polynomial

$$X^2-(uv+t+u^{-1}v^{-1})X+1=(X-w)(X-w^{-1}),$$

and so ab is similar to $\mathrm{diag}(w,w^{-1})$. Therefore ab has order $2r$.[10] □

Exercises

1-1 Show that the quaternion group has only one element of order 2, and that it commutes with all elements of Q. Deduce that Q is not isomorphic to D_4, and that every subgroup of Q is normal.[11]

1-2 Consider the elements

$$a=\begin{pmatrix} 0 & -1 \\ 1 & 0\end{pmatrix} \quad b=\begin{pmatrix} 0 & 1 \\ -1 & -1\end{pmatrix}$$

in $\mathrm{GL}_2(\mathbb{Z})$. Show that $a^4=1$ and $b^3=1$, but that ab has infinite order, and hence that the group $\langle a,b\rangle$ is infinite.

1-3 Show that every finite group of even order contains an element of order 2.

1-4 Let $n=n_1+\cdots+n_r$ be a partition of the positive integer n. Use Lagrange's theorem to show that $n!$ is divisible by $\prod_{i=1}^r n_i!$.

1-5 Let N be a normal subgroup of G of index n. Show that if $g\in G$, then $g^n\in N$. Give an example to show that this may be false when the subgroup is not normal.

[10] I don't know who found this beautiful proof. Apparently the original proof of G.A. Miller is very complicated; see mo24913.

[11] This property of Q is unusual. In fact, the only noncommutative groups in which every subgroup is normal are the groups of the form $Q\times A\times B$ with Q the quaternion group, A a commutative group whose elements have finite odd order, and B a commutative group whose elements have order 2 (or 1). See Hall 1959, 12.5.4.

1-6 A group G is said to have ***finite exponent*** if there exists an $m > 0$ such that $a^m = e$ for every a in G; the smallest such m is then called the ***exponent*** of G.

(a) Show that every group of exponent 2 is commutative.
(b) Show that, for an odd prime p, the group of matrices

$$\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a,b,c \in \mathbb{F}_p \right\}$$

has exponent p, but is not commutative.

1-7 Two subgroups H and H' of a group G are said to be ***commensurable*** if $H \cap H'$ is of finite index in both H and H'. Show that commensurability is an equivalence relation on the subgroups of G.

1-8 Show that a nonempty finite set with an associative binary operation satisfying the cancellation laws is a group.

1-9 Let G be a set with an associative binary operation. Show that if left multiplication $x \mapsto ax$ by every element a is bijective and right multiplication by some element is injective, then G is a group. Give an example to show that the second condition is needed.

1-10 Show that a commutative monoid M is a submonoid of a commutative group if and only if cancellation holds in M:

$$mn = m'n \implies m = m'.$$

Hint: The group is constructed from M as $\mathbb{Q}$ is constructed from $\mathbb{Z}$.

CHAPTER 2

Free Groups and Presentations; Coxeter Groups

It is frequently useful to describe a group by giving a set of generators for the group and a set of relations for the generators from which every other relation in the group can be deduced. For example, D_n can be described as the group with generators r, s and relations

$$r^n = e, \quad s^2 = e, \quad srsr = e.$$

In this chapter, we make precise what this means. First we need to define the free group on a set X of generators — this is a group generated by X and with no relations except for those implied by the group axioms. Because inverses cause problems, we first do this for monoids. Recall that a monoid is a set S with an associative binary operation having an identity element e. A homomorphism $\alpha\colon S \to S'$ of monoids is a map such that $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in S$ and $\alpha(e) = e$ — unlike the case of groups, the second condition is not automatic. A homomorphism of monoids preserves all finite products.

Free monoids

Let $X = \{a, b, c, \ldots\}$ be a (possibly infinite) set of symbols. A ***word*** is a finite sequence of symbols from X in which repetition is allowed. For example,

$$aa, \quad aabac, \quad b$$

are distinct words. Two words can be multiplied by juxtaposition, for example,

$$aaaa * aabac = aaaaaabac.$$

This defines on the set of all words an associative binary operation. The empty sequence is allowed, and we denote it by 1. (In the unfortunate case that the symbol 1 is already an element of X, we denote it by a different symbol.) Then 1 serves as an identity element. Write SX for the set of words together with this binary operation. Then SX is a monoid, called the ***free monoid*** on X.

When we identify an element a of X with the word a, X becomes a subset of SX and generates it (i.e., no proper submonoid of SX contains X). Moreover, the map $X \to SX$ has the following universal property: for any map of sets $\alpha\colon X \to S$ from X to a monoid S, there exists a unique homomorphism $SX \to S$ making the diagram at right commute:

$$\begin{tikzcd}
X \arrow[r, "a \mapsto a"] \arrow[dr, "\alpha"'] & SX \arrow[d, dashed] \\
 & S.
\end{tikzcd}$$

Free groups

We want to construct a group FX containing X and having the same universal property as SX with "monoid" replaced by "group". Define X' to be the set consisting of the symbols in X and also one additional symbol, denoted a^{-1}, for each $a \in X$; thus

$$X' = \{a, a^{-1}, b, b^{-1}, \ldots\}.$$

Let W' be the set of words using symbols from X'. This becomes a monoid under juxtaposition, but it is not a group because a^{-1} is not yet the inverse of a, and we can't cancel out the obvious terms in words of the following form:

$$\cdots aa^{-1} \cdots \text{ or } \cdots a^{-1}a \cdots$$

A word is said to be ***reduced*** if it contains no pairs of the form aa^{-1} or $a^{-1}a$. Starting with a word w, we can perform a finite sequence of cancellations to arrive at a reduced word (possibly empty), which will be called the ***reduced form*** w_0 of w. There may be many different ways of performing the cancellations, for example,

$$ca\underline{bb^{-1}}a^{-1}c^{-1}ca \to c\underline{aa^{-1}}c^{-1}ca \to \underline{cc^{-1}}ca \to ca,$$

$$cabb^{-1}a^{-1}\underline{c^{-1}c}a \to cabb^{-1}\underline{a^{-1}a} \to ca\underline{bb^{-1}} \to ca.$$

We have underlined the pair we are cancelling. Note that the middle a^{-1} is cancelled with different a's, and that different terms survive in the two cases (the ca at the right in the first cancellation, and the ca at left in the second). Nevertheless we ended up with the same answer, and the next result says that this always happens.

PROPOSITION 2.1 *There is only one reduced form of a word.*

PROOF. We use induction on the length of the word w. If w is reduced, there is nothing to prove. Otherwise a pair of the form $a_0a_0^{-1}$ or $a_0^{-1}a_0$ occurs — assume the first, since the argument is the same in both cases.

Observe that any two reduced forms of w obtained by a sequence of cancellations in which $a_0a_0^{-1}$ is cancelled first are equal, because the induction hypothesis can be applied to the (shorter) word obtained by cancelling $a_0a_0^{-1}$.

Next observe that any two reduced forms of w obtained by a sequence of cancellations in which $a_0a_0^{-1}$ is cancelled at some point are equal, because the result of such a sequence of cancellations will not be affected if $a_0a_0^{-1}$ is cancelled first.

Finally, consider a reduced form w_0 obtained by a sequence in which no cancellation cancels $a_0a_0^{-1}$ directly. Since $a_0a_0^{-1}$ does not remain in w_0, at least one of a_0 or a_0^{-1} must be cancelled at some point. If the pair itself is not cancelled, then the first cancellation involving the pair must look like

$$\cdots \cancel{a}_0^{-1}\,\underline{\cancel{a}_0 a_0^{-1}} \cdots \text{ or } \cdots \underline{a_0\,\cancel{a}_0^{-1}}\,\cancel{a}_0 \cdots,$$

where our original pair is underlined. But the word obtained after this cancellation is the same as if our original pair were cancelled, and so we may cancel the original pair instead. Thus we are back in the case just proved. □

We say two words w, w' are ***equivalent***, denoted $w \sim w'$, if they have the same reduced form. This is an equivalence relation (obviously).

PROPOSITION 2.2 *Products of equivalent words are equivalent, i.e.,*

$$w \sim w', \quad v \sim v' \implies wv \sim w'v'.$$

PROOF. Let w_0 and v_0 be the reduced forms of w and of v. To obtain the reduced form of wv, we can first cancel as much as possible in w and v separately, to obtain w_0v_0 and then continue cancelling. Thus the reduced form of wv is the reduced form of w_0v_0. A similar statement holds for $w'v'$, but (by assumption) the reduced forms of w and v equal the reduced forms of w' and v', and so we obtain the same result in the two cases. □

Let FX be the set of equivalence classes of words. Proposition 2.2 shows that the binary operation on W' defines a binary operation on FX, which obviously makes it into a monoid. It also has inverses, because

$$(ab\cdots gh)\left(h^{-1}g^{-1}\cdots b^{-1}a^{-1}\right) \sim 1.$$

Thus FX is a group, called the ***free group*** on X. To summarize: the elements of FX are represented by words in X'; two words represent the same element of FX if and only if they have the same reduced forms; multiplication is defined by juxtaposition; the empty word represents 1; inverses are obtained in the obvious way. Alternatively, each element of FX is represented by a unique reduced word; multiplication is defined by juxtaposition and passage to the reduced form.

When we identify $a \in X$ with the equivalence class of the (reduced) word a, then X becomes identified with a subset of FX — clearly it generates FX. The next proposition is a precise statement of the fact that there are no relations among the elements of X when regarded as elements of FX except those imposed by the group axioms.

PROPOSITION 2.3 *For any map of sets $\alpha\colon X \to G$ from X to a group G, there exists a unique homomorphism $FX \to G$ making the following diagram commute:*

$$\begin{tikzcd}
X \arrow[r, "a \mapsto a"] \arrow[dr, "\alpha"'] & FX \arrow[d, dashed] \\
 & G.
\end{tikzcd}$$

PROOF. Consider a map $\alpha\colon X \to G$. We extend it to a map of sets $X' \to G$ by setting $\alpha(a^{-1}) = \alpha(a)^{-1}$. Because G is, in particular, a monoid, α extends to a homomorphism of monoids $SX' \to G$. This map will send equivalent words to the same element of G, and so will factor through $FX = SX'/{\sim}$. The resulting map $FX \to G$ is a group homomorphism. It is unique because we know it on a set of generators for FX. □

REMARK 2.4 The universal property of the map $\iota: X \to FX$, $x \mapsto x$, characterizes it: if $\iota': X \to F'$ is a second map with the same universal property, then there is a unique isomorphism $\alpha: FX \to F'$ such that $\alpha \circ \iota = \iota'$,

$$\begin{tikzcd}
 & FX \arrow[dd, dashed, "\alpha"] \\
X \arrow[ur, "\iota"] \arrow[dr, "\iota'"'] & \\
 & F'.
\end{tikzcd}$$

We recall the proof: by the universality of ι, there exists a unique homomorphism $\alpha: FX \to F'$ such that $\alpha \circ \iota = \iota'$; by the universality of ι', there exists a unique homomorphism $\beta: F' \to FX$ such that $\beta \circ \iota' = \iota$; now $(\beta \circ \alpha) \circ \iota = \iota$, but by the universality of ι, id_{FX} is the unique homomorphism $FX \to FX$ such that $\mathrm{id}_{FX} \circ \iota = \iota$, and so $\beta \circ \alpha = \mathrm{id}_{FX}$; similarly, $\alpha \circ \beta = \mathrm{id}_{F'}$, and so α and β are inverse isomorphisms.

COROLLARY 2.5 *Every group is a quotient of a free group.*

PROOF. Choose a set X of generators for G (e.g., $X = G$), and let F be the free group generated by X. According to (2.3), the map $a \mapsto a$: $X \to G$ extends to a homomorphism $F \to G$, and the image, being a subgroup containing X, must equal G. □

The free group on the set $X = \{a\}$ is simply the infinite cyclic group C_∞ generated by a, but the free group on a set consisting of two elements is already very complicated.

I now discuss, without proof, some important results on free groups.

THEOREM 2.6 (NIELSEN-SCHREIER) [1] *Subgroups of free groups are free.*

The best proof uses topology, and in particular covering spaces—see Serre 1980 or Rotman 1995, Theorem 11.44.

Two free groups FX and FY are isomorphic if and only if X and Y have the same cardinality. Thus we can define the ***rank*** of a free group G to be the cardinality of any free generating set (subset X of G for which the homomorphism $FX \to G$ given by (2.3) is an isomorphism). Let H be a finitely generated subgroup of a free group G. Then there is an algorithm for constructing from any finite set of generators for H a free finite set of generators. If G has finite rank n and $(G : H) = i < \infty$, then H is free of rank

$$ni - i + 1.$$

In particular, H may have rank greater than that of F (or even infinite rank[2]). For proofs, see Rotman 1995, Chapter 11, and Hall 1959, Chapter 7.

[1] Nielsen (1921) proved this for finitely generated subgroups, and in fact gave an algorithm for deciding whether a word lies in the subgroup; Schreier (1927) proved the general case.

[2] For example, the commutator subgroup of the free group on two generators has infinite rank.

Generators and relations

Consider a set X and a set R of words made up of symbols in X'. Each element of R represents an element of the free group FX, and the quotient G of FX by the normal subgroup generated by these elements (1.40) is said to have X as ***generators*** and R as ***relations*** (or as a ***set of defining relations***). One also says that (X, R) is a ***presentation*** for G, and denotes G by $\langle X \mid R\rangle$.

EXAMPLE 2.7 (a) The dihedral group D_n has generators r, s and defining relations

$$r^n, s^2, srsr.$$

(See 2.9 below for a proof.)

(b) The ***generalized quaternion group*** Q_n, $n \geq 3$, has generators a, b and relations[3]

$$a^{2^{n-1}} = 1, a^{2^{n-2}} = b^2, bab^{-1} = a^{-1}.$$

For $n = 3$ this is the group Q of (1.18). In general, it has order 2^n (for more on it, see Exercise 2-5).

(c) Two elements a and b in a group commute if and only if their ***commutator*** $[a, b] \overset{\text{def}}{=} aba^{-1}b^{-1}$ is 1. The ***free abelian group*** on generators $a_1, \ldots, a_n$ has generators $a_1, a_2, \ldots, a_n$ and relations

$$[a_i, a_j], \qquad i \neq j.$$

(d) Let $G = \langle s, t \mid s^3t, t^3, s^4\rangle$. Then $G = \{1\}$ because

$$\begin{aligned} s &= ss^3t = s^4t = t \\ 1 &= s^3tt^{-3} = s^3ss^{-3} = s. \end{aligned}$$

For the remaining examples, see Massey 1967, which contains a good account of the interplay between group theory and topology. For example, for many types of topological spaces, there is an algorithm for obtaining a presentation for the fundamental group.

(e) The fundamental group of the open disk with one point removed is the free group on σ, where σ is any loop around the point (ibid. II 5.1).

(f) The fundamental group of the sphere with r points removed has generators $\sigma_1, ..., \sigma_r$ (σ_i is a loop around the ith point) and a single relation

$$\sigma_1 \cdots \sigma_r = 1.$$

(g) The fundamental group of a compact Riemann surface of genus g has $2g$ generators $u_1, v_1, ..., u_g, v_g$ and a single relation

$$u_1v_1u_1^{-1}v_1^{-1} \cdots u_gv_gu_g^{-1}v_g^{-1} = 1$$

(ibid. IV Exercise 5.7).

[3] Strictly speaking, I should say the relations $a^{2^{n-1}}$, $a^{2^{n-2}}b^{-2}$, $bab^{-1}a$.

PROPOSITION 2.8 *Let G be the group defined by the presentation (X,R). For any group H and map of sets $\alpha\colon X \to H$ sending each element of R to 1 (in the obvious sense[4]), there exists a unique homomorphism $G \to H$ making the following diagram commute:*

$$\begin{tikzcd}
X \arrow[r, "a \mapsto a"] \arrow[dr, "\alpha"'] & G \arrow[d, dashed] \\
& H.
\end{tikzcd}$$

PROOF. From the universal property of free groups (2.3), we know that α extends to a homomorphism $FX \to H$, which we again denote α. Let ιR be the image of R in FX. By assumption $\iota R \subset \mathrm{Ker}(\alpha)$, and therefore the normal subgroup N generated by ιR is contained in $\mathrm{Ker}(\alpha)$. By the universal property of quotients (see 1.43), α factors through $FX/N = G$. This proves the existence, and the uniqueness follows from the fact that we know the map on a set of generators for X. □

EXAMPLE 2.9 Let $G = \langle a,b \mid a^n, b^2, baba\rangle$. We prove that G is isomorphic to the dihedral group D_n (see 1.17). Because the elements $r,s \in D_n$ satisfy these relations, the map

$$\{a,b\} \to D_n, \quad a \mapsto r, \quad b \mapsto s$$

extends uniquely to a homomorphism $G \to D_n$. This homomorphism is surjective because r and s generate D_n. The equalities

$$a^n = 1, \quad b^2 = 1, \quad ba = a^{n-1}b$$

imply that each element of G is represented by one of the following elements,

$$1, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b,$$

and so $|G| \le 2n = |D_n|$. Therefore the homomorphism is bijective (and these symbols represent distinct elements of G).

Similarly,

$$\langle a,b \mid a^2, b^2, (ab)^n\rangle \simeq D_n$$

by $a \mapsto s$, $b \mapsto t$.

EXAMPLE 2.10 (a) Let $G = \langle x,y \mid x^m, y^n\rangle$, where $m,n > 1$. Then x has order m, y has order n, and xy has infinite order in G. To see this, recall that for any integers $m,n,r > 1$, there exists a group H with elements a and b such that a, b, and ab have orders m, n, and r respectively (Theorem 1.64). According to (2.8), there exists a homomorphism $\alpha\colon G \to H$ such that $\alpha(x) = a$ and $\alpha(y) = b$. The order of x certainly divides m, and the fact that $\alpha(x)$ has order m shows that x has order exactly m. Similarly, y has order n. As $\alpha(xy) = ab$, the element xy must have order at least r. As this is true for all $r > 1$, the element xy has infinite order.

(b) Let $G = \langle x,y \mid x^m, y^n, (xy)^r\rangle$. where $m,n,r > 1$. There exists a homomorphism from G to the group in (1.64) sending x and y to a and b, which shows that x, y, and xy

[4] Each element of R represents an element of FX, and the condition requires that the unique extension of α to FX sends each of these elements to 1.

have orders m, n, and r in G. The group G may be finite or infinite, depending on the triple (m,n,r). These groups occur naturally as subgroups of index 2 in certain symmetry groups — see the Wikipedia: Triangle group.

(c) Let $G = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$, and let S and T be the elements of G represented by the matrices $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Then S and ST generate G, and $S^2 = 1 = (ST)^3$ (see Theorem 2.12 of my course notes on modular forms). It is known that this is a full set of relations for S and ST in G, and so every group generated by an element of order 2 and an element of order 3 is a quotient of G. Most finite simple groups of Lie type, and all but three of the sporadic simple groups, fall into this class.

Finitely presented groups

A group is said to be ***finitely presented*** if it admits a presentation (X, R) with both X and R finite.

EXAMPLE 2.11 Consider a finite group G. Let $X = G$, and let R be the set of words

$$\{abc^{-1} \mid ab = c \text{ in } G\}.$$

I claim that (X, R) is a presentation of G, and so G is finitely presented. Let $G' = \langle X \mid R\rangle$. The extension of $a \mapsto a\colon X \to G$ to FX sends each element of R to 1, and therefore defines a homomorphism $G' \to G$, which is obviously surjective. But every element of G' is represented by an element of X, and so $|G'| \le |G|$. Therefore the homomorphism is bijective.

Although it is easy to define a group by a finite presentation, calculating the properties of the group can be very difficult — note that we are defining the group, which may be quite small, as the quotient of a huge free group by a huge subgroup. I list some negative results.

THE WORD PROBLEM

Let G be the group defined by a finite presentation (X, R). The word problem for G asks whether there exists an algorithm (decision procedure) for deciding whether a word on X' represents 1 in G. The answer is negative: Novikov and Boone showed that there exist finitely presented groups G for which no such algorithm exists. Of course, there do exist other groups for which there is an algorithm.

The same ideas lead to the following result: there does not exist an algorithm that will determine for an arbitrary finite presentation whether or not the corresponding group is trivial, finite, abelian, solvable, nilpotent, simple, torsion, torsion-free, free, or has a solvable word problem.

See Rotman 1995, Chapter 12, for proofs of these statements.

THE BURNSIDE PROBLEM

Recall that a group is said to have exponent e if $g^e = 1$ for all $g \in G$ and e is the smallest natural number with this property. It is easy to write down examples of infinite groups generated by a finite number of elements of finite order (see Exercise 1-2 or Example 2.10), but does there exist such a group with finite exponent? (Burnside problem). In 1968, Adjan and Novikov showed the answer is yes: there do exist infinite finitely generated groups of finite exponent.

THE RESTRICTED BURNSIDE PROBLEM

The ***Burnside group*** of exponent e on r generators $B(r,e)$ is the quotient of the free group on r generators by the subgroup generated by all eth powers. The Burnside problem asked whether $B(r,e)$ is finite, and it is known to be infinite except some small values of r and e. The restricted Burnside problem asks whether $B(r,e)$ has only finitely many finite quotients; equivalently, it asks whether there is one finite quotient of $B(r,e)$ having all other finite quotients as quotients. The classification of the finite simple groups (see p. 52) showed that in order prove that $B(r,e)$ always has only finitely many finite quotients, it suffices to prove it for e equal to a prime power. This was shown by Efim Zelmanov in 1989 after earlier work of Kostrikin. See Feit 1995.

TODD-COXETER ALGORITHM

There are some quite innocuous looking finite presentations that are known to define quite small groups, but for which this is very difficult to prove. The standard approach to these questions is to use the Todd-Coxeter algorithm (see Chapter 4 below).

We shall develop various methods for recognizing groups from their presentations (see also the exercises).

Coxeter groups

A ***Coxeter system*** is a pair (G,S) consisting of a group G and a set of generators S for G subject only to relations of the form $(st)^{m(s,t)} = 1$, where

$$\begin{cases} m(s,s) & = & 1 \text{ all } s, \\ m(s,t) & \geq & 2 \\ m(s,t) & = & m(t,s). \end{cases} \tag{14}$$

When no relation occurs between s and t, we set $m(s,t) = \infty$. Thus a Coxeter system is defined by a set S and a mapping

$$m\colon S \times S \to \mathbb{N} \cup \{\infty\}$$

satisfying (14), and the group $G = \langle S \mid R \rangle$, where

$$R = \{(st)^{m(s,t)} \mid m(s,t) \neq \infty\}.$$

The ***Coxeter groups*** are those that arise as part of a Coxeter system. The cardinality of S is called the ***rank*** of the Coxeter system.

EXAMPLES

2.12 Up to isomorphism, the only Coxeter system of rank 1 is $(C_2, \{s\})$.

2.13 The Coxeter systems of rank 2 are indexed by $m(s,t) \geq 2$.

(a) If $m(s,t)$ is an integer n, then the Coxeter system is $(G, \{s,t\})$, where

$$G = \langle s,t \mid s^2, t^2, (st)^n \rangle.$$

According to (2.9), $G \simeq D_n$. In particular, $s \neq t$ and st has order n.

(b) If $m(s,t) = \infty$, then the Coxeter system is $(G,\{s,t\})$, where $G = \langle s,t \mid s^2,t^2\rangle$. According to (2.10a), s and t each have order 2, and st has infinite order.

2.14 Let $V = \mathbb{R}^n$ endowed with the standard positive definite symmetric bilinear form

$$((x_i),(y_i)) = \sum\nolimits_{i=1}^{n} x_i y_i.$$

A ***reflection*** is a linear map $s\colon V \to V$ sending some nonzero vector α to $-\alpha$ and fixing the points of the hyperplane H_α orthogonal to α. We write s_α for the reflection defined by α; it is given by the formula

$$s_\alpha v = v - \frac{2(v,\alpha)}{(\alpha,\alpha)}\alpha,$$

because this is correct for $v = \alpha$ and for $v \in H_\alpha$, and hence (by linearity) for all v in $V = \langle\alpha\rangle \oplus H_\alpha$. A ***finite reflection group*** is a finite group generated by reflections. For such a group G, it is possible to choose a set S of generating reflections for which (G,S) is a Coxeter system (Humphreys 1990, 1.9). Thus, the finite reflection groups are all Coxeter groups (in fact, they are precisely the finite Coxeter groups, ibid., 6.4).

EXAMPLE 2.15 (a) Let S_n act on $\mathbb{R}^n$ by permuting the coordinates,

$$\sigma(a_1,\ldots,a_n) = (a_{\sigma(1)},\ldots,a_{\sigma(n)}).$$

The transposition (ij), interchanging i and j, sends the vector

$$\alpha = (0,\ldots,0,\overset{i}{1},0,\ldots,0,\overset{j}{-1},0,\ldots)$$

to its negative and leaves the points of the hyperplane

$$H_\alpha = (a_1,\ldots,\overset{i}{a_i},\ldots,\overset{j}{a_i},\ldots,a_n)$$

fixed. Therefore, (ij) is a reflection. As S_n is generated by transpositions, this shows that it is a finite reflection group (hence also a Coxeter group).

(b) Consider the dihedral group D_n of symmetries of a regular polygon with n-sides, $n \geq 3$. The composite of two reflections relative to a pair of adjacent diagonals (meeting at an angle π/n) is a rotation through $2\pi/n$. Therefore, D_n is generated by reflections.

THE STRUCTURE OF COXETER GROUPS

THEOREM 2.16 *Let (G,S) be the Coxeter system defined by a map $m\colon S \times S \to \mathbb{N} \cup \{\infty\}$ satisfying (14).*

(a) *The natural map $S \to G$ is injective.*
(b) *Each $s \in S$ has order 2 in G.*
(c) *For each $s \neq t$ in S, st has order $m(s,t)$ in G.*

The proof will occupy the rest of this section. Note that the order of s is 1 or 2, and the order of st divides $m(s,t)$, and so the theorem says that the elements of S remain distinct in G and that each s and each st has the largest possible order.

Let ε be the map $S \to \{\pm 1\}$ such that $\varepsilon(s) = -1$ for all s. This sends st to 1 for all $s,t \in S$, and so it extends to a homomorphism of groups $G \to \{\pm 1\}$ (by 2.8). Every s maps to -1, and so has order 2.

This proves (b), and to prove the remaining statements we shall consider an $\mathbb{R}$-vector space V with basis a family $(e_s)_{s\in S}$ indexed by S. We define on V a "geometry" for which there exist distinct "reflections" σ_s, $s \in S$, such that $\sigma_s\sigma_t$ has order $m(s,t)$. According to Proposition 2.8, the map $s \mapsto \sigma_s$ extends to a homomorphism of groups $G \to \mathrm{GL}(V)$. As the σ_s are distinct, the s must be distinct in G, and as $\sigma_s\sigma_t$ has order $m(s,t)$, the element st of G must also have order $m(s,t)$.

Define a symmetric bilinear form B on V by the rule

$$B(e_s,e_t) = \begin{cases} -\cos(\pi/m(s,t)) & \text{if } m(s,t) \neq \infty \\ -1 & \text{otherwise.} \end{cases}$$

As $B(e_s,e_s) = 1 \neq 0$, the orthogonal complement of e_s with respect to B is a hyperplane H_s not containing e_s, and so $V = \langle e_s \rangle \oplus H_s$. This allows us to define a "reflection" by the rule

$$\sigma_s v = v - 2B(v,e_s)e_s, \quad v \in V.$$

Clearly σ_s is a linear map sending e_s to its negative and fixing the elements of H_s, and so $\sigma_s^2 = 1$ in $\mathrm{GL}(V)$. Moreover, σ_s preserves the form B, i.e., $B(\sigma_s v, \sigma_s w) = B(v,w)$.

The σ_s are clearly distinct, and so it remains to show that $\sigma_s\sigma_t$ has order $m(s,t)$. For $s,t \in S$, let $V_{s,t}$ denote the 2-dimensional vector space $\mathbb{R}e_s \oplus \mathbb{R}e_t$. Clearly σ_s and σ_t both map $V_{s,t}$ into itself.

LEMMA 2.17 *The restriction of B to $V_{s,t}$ is positive definite if $m(s,t) \neq \infty$, and positive semidefinite otherwise .*

PROOF. Let $v = ae_s + be_t \in V_{s,t}$. If $m(s,t) \neq \infty$, then

$$\begin{aligned} B(v,v) &= a^2 - 2ab\cos(\pi/m) + b^2 \\ &= (a - b\cos(\pi/m))^2 + b^2\sin^2(\pi/m) \\ &> 0 \end{aligned}$$

because $\sin(\pi/m) \neq 0$. If $m(s,t) = \infty$, then

$$B(v,v) = a^2 - 2ab + b^2 = (a-b)^2 \geq 0$$

(and $B(v,v) = 0$ if $v = e_s + e_t$). □

LEMMA 2.18 *The restriction of $\sigma_s\sigma_t$ to $V_{s,t}$ has order $m(s,t)$.*

PROOF. Let $m = m(s,t)$. When $m \neq \infty$, the form $B|V_{s,t}$ is positve definite, and so $(V_{s,t}, B|V_{s,t})$ is a euclidean plane. Moreover, σ_s and σ_t are the reflections in $V_{s,t}$ in the sense of (2.14) defined by the vectors e_s and e_t. As $B(e_s,e_t) = -\cos(\pi/m) = \cos(\pi - \pi/m)$, the angle between the lines fixed by e_s and e_t is π/m. From (2.15b), we see that σ_s and σ_t generate a dihedral group D_m and that $\sigma_s\sigma_t$ has order m.

When $m = \infty$, then, relative to the basis $\{e_s, e_t\}$,

$$\sigma_s = \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \sigma_t = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}.$$

Now $\sigma_s\sigma_t = \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}$, and so

$$\sigma_s\sigma_t \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \sigma_s\sigma_t \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 2\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Therefore,

$$(\sigma_s\sigma_t)^m \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 2m\begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

which shows that $\sigma_s\sigma_t$ has infinite order. □

This completes the proof of Theorem 2.16.

REMARK 2.19 The homomorphism $G \to \mathrm{GL}(V)$ in the proof of Theorem 2.16 is injective (Humphreys 1990, 5.4), and so it realizes G as a group of automorphisms of a "geometry".

Exercises

2-1 Let $D_n = \langle a, b | a^n, b^2, abab \rangle$ be the nth dihedral group. If n is odd, prove that $D_{2n} \approx \langle a^n \rangle \times \langle a^2, b \rangle$, and hence that $D_{2n} \approx C_2 \times D_n$.

2-2 Prove that the group with generators $a_1, \ldots, a_n$ and relations $[a_i, a_j] = 1$, $i \neq j$, is the free *abelian* group on $a_1, \ldots, a_n$. [Hint: Use universal properties.]

2-3 Let a and b be elements of an arbitrary free group F. Prove:

(a) If $a^n = b^n$ with $n > 1$, then $a = b$.
(b) If $a^m b^n = b^n a^m$ with $mn \neq 0$, then $ab = ba$.
(c) If the equation $x^n = a$ has a solution x for every n, then $a = 1$.

2-4 Let F_n denote the free group on n generators. Prove:

(a) If $n < m$, then F_n is isomorphic to both a subgroup and a quotient group of F_m.
(b) Prove that $F_1 \times F_1$ is not a free group.
(c) Prove that the centre $Z(F_n) = 1$ provided $n > 1$.

2-5 Prove that Q_n (see 2.7b) has a unique subgroup of order 2, which is $Z(Q_n)$. Prove that $Q_n/Z(Q_n)$ is isomorphic to $D_{2^{n-2}}$.

2-6 (a) Prove that $\langle a, b \mid a^2, b^2, (ab)^n \rangle \simeq D_n$ (cf. 2.9).
(b) Prove that $G = \langle a, b \mid a^2, abab \rangle$ is an infinite group. (This is usually known as the infinite dihedral group.)

2-7 Let $G = \langle a, b, c \mid a^3, b^3, c^4, acac^{-1}, aba^{-1}bc^{-1}b^{-1} \rangle$. Prove that G is the trivial group $\{1\}$. [Hint: Expand $(aba^{-1})^3 = (bcb^{-1})^3$.]

2-8 Let F be the free group on the set $\{x, y\}$ and let $G = C_2$, with generator $a \neq 1$. Let α be the homomorphism $F \to G$ such that $\alpha(x) = a = \alpha(y)$. Find a minimal generating set for the kernel of α. Is the kernel a free group?

2-9 Let $G = \langle s, t \mid t^{-1}s^3t = s^5 \rangle$. Prove that the element

$$g = s^{-1}t^{-1}s^{-1}tst^{-1}st$$

is in the kernel of every map from G to a finite group.

> Coxeter came to Cambridge and gave a lecture [in which he stated a] problem for which he gave proofs for selected examples, and he asked for a unified proof. I left the lecture room thinking. As I was walking through Cambridge, suddenly the idea hit me, but it hit me while I was in the middle of the road. When the idea hit me I stopped and a large truck ran into me.... So I pretended that Coxeter had calculated the difficulty of this problem so precisely that he knew that I would get the solution just in the middle of the road.... Ever since, I've called that theorem "the murder weapon". One consequence of it is that in a group if $a^2 = b^3 = c^5 = (abc)^{-1}$, then $c^{610} = 1$.
>
> John Conway, Math. Intelligencer 23 (2001), no. 2, pp. 8–9.

CHAPTER 3

Automorphisms and Extensions

Automorphisms of groups

An ***automorphism*** of a group G is an isomorphism of the group with itself. The set $\mathrm{Aut}(G)$ of automorphisms of G becomes a group under composition: the composite of two automorphisms is again an automorphism; composition of maps is always associative (see (5), p. 9); the identity map $g \mapsto g$ is an identity element; an automorphism is a bijection, and therefore has an inverse, which is again an automorphism.

For $g \in G$, the map i_g "conjugation by g",

$$x \mapsto gxg^{-1} : G \to G$$

is an automorphism of G. An automorphism of this form is called an ***inner automorphism***, and the remaining automorphisms are said to be ***outer***.

Note that

$$(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1}, \text{ i.e., } i_{gh}(x) = (i_g \circ i_h)(x),$$

and so the map $g \mapsto i_g : G \to \mathrm{Aut}(G)$ is a homomorphism. Its image is denoted by $\mathrm{Inn}(G)$. Its kernel is the centre of G,

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

and so we obtain from (1.45) an isomorphism

$$G/Z(G) \to \mathrm{Inn}(G).$$

In fact, $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$: for $g \in G$ and $\alpha \in \mathrm{Aut}(G)$, we have

$$\alpha \circ i_g \circ \alpha^{-1} = i_{\alpha(g)}.$$

EXAMPLE 3.1 (a) Let $G = \mathbb{F}_p^n$. The automorphisms of G as a commutative group are just the automorphisms of G as a vector space over $\mathbb{F}_p$; thus $\mathrm{Aut}(G) = \mathrm{GL}_n(\mathbb{F}_p)$. Because G is commutative, all nontrivial automorphisms of G are outer.

(b) As a particular case of (a), we see that

$$\mathrm{Aut}(C_2 \times C_2) = \mathrm{GL}_2(\mathbb{F}_2).$$

(c) As the centre of the quaternion group Q is $\langle a^2\rangle$,

$$\mathrm{Inn}(Q) \simeq Q/\langle a^2\rangle \approx C_2 \times C_2.$$

In fact, $\mathrm{Aut}(Q) \approx S_4$. See Exercise 3-4.

ASIDE 3.2 Let α be an automorphism of a group H. If α is inner, then it extends to every group G containing H as a subgroup. The converse is also true (Schupp 1987).

COMPLETE GROUPS

DEFINITION 3.3 A group G is ***complete*** if the map $g \mapsto i_g\colon G \to \mathrm{Aut}(G)$ is an isomorphism.

Thus, a group G is complete if and only if (a) the centre $Z(G)$ of G is trivial, and (b) every automorphism of G is inner.

EXAMPLE 3.4 (a) The group S_n is complete for $n \neq 2,6$, but S_2 fails (a) and S_6 fails (b) (because $\mathrm{Aut}(S_6)/\mathrm{Inn}(S_6) \simeq C_2$). See Rotman 1995, Theorems 7.5, 7.10.

(b) If G is a simple noncommutative group, then $\mathrm{Aut}(G)$ is complete. See Rotman 1995, Theorem 7.14.

According to Exercise 3-3, $\mathrm{GL}_2(\mathbb{F}_2) \approx S_3$, and so the nonisomorphic groups $C_2 \times C_2$ and S_3 have isomorphic automorphism groups.

AUTOMORPHISMS OF CYCLIC GROUPS

Let G be a cyclic group of order n, say, $G = \langle a\rangle$. Let m be an integer ≥ 1. The smallest multiple of m divisible by n is $m \cdot \frac{n}{\gcd(m,n)}$. Therefore, a^m has order $\frac{n}{\gcd(m,n)}$, and so the generators of G are exactly the elements a^m with $\gcd(m,n) = 1$. An automorphism α of G must send a to another generator of G, and so $\alpha(a) = a^m$ for some m relatively prime to n. The map $\alpha \mapsto m$ defines an isomorphism

$$\mathrm{Aut}(C_n) \to (\mathbb{Z}/n\mathbb{Z})^\times,$$

where

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\text{units in the ring } \mathbb{Z}/n\mathbb{Z}\} = \{m + n\mathbb{Z} \mid \gcd(m,n) = 1\}.$$

This isomorphism is independent of the choice of a generator a for G: if $\alpha(a) = a^m$, then for any other element $b = a^i$ of G,

$$\alpha(b) = \alpha(a^i) = \alpha(a)^i = a^{mi} = (a^i)^m = (b)^m.$$

It remains to determine $(\mathbb{Z}/n\mathbb{Z})^\times$. If $n = p_1^{r_1} \cdots p_s^{r_s}$ is the factorization of n into a product of powers of distinct primes, then

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z}, \quad m \bmod n \leftrightarrow (m \bmod p^{r_1}, \ldots)$$

by the Chinese remainder theorem. This is an isomorphism of rings, and so

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})^\times.$$

It remains to consider the case $n = p^r$, p prime.

Suppose first that p is odd. Then $\{0, 1, \ldots, p^r - 1\}$ is a complete set of representatives for $\mathbb{Z}/p^r\mathbb{Z}$, and one pth of its elements are divisible by p. Hence $(\mathbb{Z}/p^r\mathbb{Z})^\times$ has order $p^r - \frac{p^r}{p} = p^{r-1}(p-1)$. The homomorphism

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

is surjective with kernel of order p^{r-1}, and we know that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. Let $a \in (\mathbb{Z}/p^r\mathbb{Z})^\times$ map to a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $a^{p^r(p-1)} = 1$ and a^{p^r} again maps to a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Therefore $(\mathbb{Z}/p^r\mathbb{Z})^\times$ contains an element $\zeta \overset{\text{def}}{=} a^{p^r}$ of order $p-1$. Using the binomial theorem, one finds that $1+p$ has order p^{r-1} in $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Therefore $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic with generator $\zeta \cdot (1+p)$ (cf. (13), p. 26), and every element can be written uniquely in the form

$$\zeta^i \cdot (1+p)^j, \quad 0 \le i < p-1, \quad 0 \le j < p^{r-1}.$$

On the other hand,

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} = \langle \bar{3}, \bar{5} \rangle \approx C_2 \times C_2$$

is not cyclic.

SUMMARY 3.5 (a) For a cyclic group of G of order n, $\mathrm{Aut}(G) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. The automorphism of G corresponding to $[m] \in (\mathbb{Z}/n\mathbb{Z})^\times$ is $a \mapsto a^m$.

(b) If $n = p_1^{r_1} \cdots p_s^{r_s}$ with the p_i distinct primes, then

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})^\times, \quad m \bmod n \leftrightarrow (m \bmod p^{r_1}, \ldots).$$

(c) For a prime p,

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \approx \begin{cases} C_{(p-1)p^{r-1}} & p \text{ odd,} \\ C_2 & p^r = 2^2 \\ C_2 \times C_{2^{r-2}} & p = 2, r > 2. \end{cases}$$

Characteristic subgroups

DEFINITION 3.6 A ***characteristic subgroup*** of a group G is a subgroup H such that $\alpha(H) = H$ for all automorphisms α of G.

The same argument as in (1.32) shows that it suffices to check that $\alpha(H) \subset H$ for all $\alpha \in \mathrm{Aut}(G)$. Thus, a subgroup H of G is normal if it is stable under *all inner* automorphisms of G, and it is characteristic if it stable under *all* automorphisms. In particular, a characteristic subgroup is normal.

REMARK 3.7 (a) Consider a group G and a normal subgroup N. An inner automorphism of G restricts to an automorphism of N, which may be outer (for an example, see 3.16 below). Thus a normal subgroup of N need not be a normal subgroup of G. However, a characteristic subgroup of N will be a normal subgroup of G. Also a characteristic subgroup of a characteristic subgroup is a characteristic subgroup.

(b) The centre $Z(G)$ of G is a characteristic subgroup, because

$$zg = gz \text{ all } g \in G \implies \alpha(z)\alpha(g) = \alpha(g)\alpha(z) \text{ all } g \in G,$$

and as g runs over G, $\alpha(g)$ also runs over G. Expect subgroups with a general group-theoretic definition to be characteristic.

(c) If H is the only subgroup of G of order m, then it must be characteristic, because $\alpha(H)$ is again a subgroup of G of order m.

(d) Every subgroup of a commutative group is normal but not necessarily characteristic. For example, every subspace of dimension 1 in $\mathbb{F}_p^2$ is subgroup of $\mathbb{F}_p^2$, but it is not characteristic because it is not stable under $\mathrm{Aut}(\mathbb{F}_p^2) = \mathrm{GL}_2(\mathbb{F}_p)$.

Semidirect products

Let N be a normal subgroup of G. Each element g of G defines an automorphism of N, $n \mapsto gng^{-1}$, and this defines a homomorphism

$$\theta\colon G \to \mathrm{Aut}(N), \quad g \mapsto i_g|N.$$

If there exists a subgroup Q of G such that $G \to G/N$ maps Q isomorphically onto G/N, then I claim that we can reconstruct G from N, Q, and the restriction of θ to Q. Indeed, an element g of G can be written uniquely in the form

$$g = nq, \quad n \in N, \quad q \in Q;$$

— q must be the unique element of Q mapping to $gN \in G/N$, and n must be gq^{-1}. Thus, we have a one-to-one correspondence of *sets*

$$G \overset{\text{1-1}}{\longleftrightarrow} N \times Q.$$

If $g = nq$ and $g' = n'q'$, then

$$gg' = (nq)\left(n'q'\right) = n(qn'q^{-1})qq' = n \cdot \theta(q)(n') \cdot qq'.$$

DEFINITION 3.8 A group G is a ***semidirect product*** of its subgroups N and Q if N is normal and the homomorphism $G \to G/N$ induces an isomorphism $Q \to G/N$.

Equivalently, G is a semidirect product of subgroup N and Q if

$$N \triangleleft G; \qquad NQ = G; \qquad N \cap Q = \{1\}. \tag{15}$$

Note that Q need *not* be a normal subgroup of G. When G is the semidirect product of subgroups N and Q, we write $G = N \rtimes Q$ (or $N \rtimes_\theta Q$, where $\theta\colon Q \to \mathrm{Aut}(N)$ gives the action of Q on N by inner automorphisms).

EXAMPLE 3.9 (a) In D_n, $n \geq 2$, let $C_n = \langle r \rangle$ and $C_2 = \langle s \rangle$; then

$$D_n = \langle r \rangle \rtimes_\theta \langle s \rangle = C_n \rtimes_\theta C_2,$$

where $\theta(s)(r^i) = r^{-i}$ (see 1.17).

(b) The alternating subgroup A_n is a normal subgroup of S_n (because it has index 2), and $C_2 = \langle (12) \rangle$ maps isomorphically onto S_n/A_n. Therefore $S_n = A_n \rtimes C_2$.

(c) The quaternion group can not be written as a semidirect product in any nontrivial fashion (see Exercise 3-1).

(d) A cyclic group of order p^2, p prime, is not a semidirect product (because it has only one subgroup of order p).

(e) Let $G = \mathrm{GL}_n(F)$. Let B be the subgroup of upper triangular matrices in G, T the subgroup of diagonal matrices in G, and U the subgroup of upper triangular matrices with all their diagonal coefficients equal to 1. Thus, when $n = 2$,

$$B = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}, \quad T = \left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\}, \quad U = \left\{\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\right\}.$$

Then, U is a normal subgroup of B, $UT = B$, and $U \cap T = \{1\}$. Therefore,

$$B = U \rtimes T.$$

Note that, when $n \geq 2$, the action of T on U is not trivial, for example,

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{pmatrix} = \begin{pmatrix} 1 & ac/b \\ 0 & 1 \end{pmatrix},$$

and so B is not the direct product of T and U.

We have seen that, from a semidirect product $G = N \rtimes Q$, we obtain a triple

$$(N, Q, \theta\colon Q \to \mathrm{Aut}(N)),$$

and that the triple determines G. We now prove that every triple (N, Q, θ) consisting of two groups N and Q and a homomorphism $\theta\colon Q \to \mathrm{Aut}(N)$ arises from a semidirect product. As a set, let $G = N \times Q$, and define

$$(n, q)(n', q') = (n \cdot \theta(q)(n'), qq').$$

PROPOSITION 3.10 *The composition law above makes G into a group, in fact, the semidirect product of N and Q.*

PROOF. Write ${}^q n$ for $\theta(q)(n)$, so that the composition law becomes

$$(n, q)(n', q') = (n \cdot {}^q n', qq').$$

Then

$$((n,q),(n',q'))(n'',q'') = (n \cdot {}^q n' \cdot {}^{qq'} n'', qq'q'') = (n,q)((n',q')(n'',q''))$$

and so the associative law holds. Because $\theta(1) = 1$ and $\theta(q)(1) = 1$,

$$(1,1)(n,q) = (n,q) = (n,q)(1,1),$$

and so $(1,1)$ is an identity element. Next

$$(n,q)({}^{q^{-1}} n^{-1}, q^{-1}) = (1,1) = ({}^{q^{-1}} n^{-1}, q^{-1})(n,q),$$

and so $({}^{q^{-1}} n^{-1}, q^{-1})$ is an inverse for (n,q). Thus G is a group, and it is obvious that $N \lhd G$, $NQ = G$, and $N \cap Q = \{1\}$, and so $G = N \rtimes Q$. Moreover, when N and Q are regarded as subgroups of G, the action of Q on N is that given by θ. □

EXAMPLES

3.11 **A group of order** 12. Let θ be the (unique) nontrivial homomorphism

$$C_4 \to \mathrm{Aut}(C_3) \simeq C_2,$$

namely, that sending a generator of C_4 to the map $a \mapsto a^2$. Then $G \overset{\text{def}}{=} C_3 \rtimes_\theta C_4$ is a noncommutative group of order 12, not isomorphic to A_4. If we denote the generators of C_3 and C_4 by a and b, then a and b generate G, and have the defining relations

$$a^3 = 1, \quad b^4 = 1, \quad bab^{-1} = a^2.$$

3.12 **Direct products.** The bijection of sets

$$(n,q) \mapsto (n,q) \colon N \times Q \to N \rtimes_\theta Q$$

is an isomorphism of groups if and only if θ is the trivial homomorphism $Q \to \mathrm{Aut}(N)$, i.e., $\theta(q)(n) = n$ for all $q \in Q$, $n \in N$.

3.13 **Groups of order** 6. Both S_3 and C_6 are semidirect products of C_3 by C_2, but they correspond to distinct homomorphisms $C_2 \to C_2 \simeq \mathrm{Aut}(C_3)$.

3.14 **Groups of order** p^3 **(element of order** p^2**).** Let $N = \langle a \rangle$ be cyclic of order p^2, and let $Q = \langle b \rangle$ be cyclic of order p, where p is an odd prime. Then $\mathrm{Aut}\, N \approx C_{p-1} \times C_p$ (see 3.5), and C_p is generated by $\alpha \colon a \mapsto a^{1+p}$ (note that $\alpha^2(a) = a^{1+2p}, \ldots$). Define $Q \to \mathrm{Aut}\, N$ by $b \mapsto \alpha$. The group $G \overset{\text{def}}{=} N \rtimes_\theta Q$ has generators a, b and defining relations

$$a^{p^2} = 1, \quad b^p = 1, \quad bab^{-1} = a^{1+p}.$$

It is a noncommutative group of order p^3, and possesses an element of order p^2.

3.15 **Groups of order** p^3 **(no element of order** p^2**).** Let $N = \langle a, b \rangle$ be the product of two cyclic groups $\langle a \rangle$ and $\langle b \rangle$ of order p, and let $Q = \langle c \rangle$ be a cyclic group of order p. Define $\theta \colon Q \to \mathrm{Aut}(N)$ to be the homomorphism such that

$$\theta(c^i)(a) = ab^i, \quad \theta(c^i)(b) = b.$$

(If we regard N as the additive group $N = \mathbb{F}_p^2$ with a and b the standard basis elements, then $\theta(c^i)$ is the automorphism of N defined by the matrix $\begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix}$.) The group $G \overset{\text{def}}{=} N \rtimes_\theta Q$ is a group of order p^3, with generators a, b, c and defining relations

$$a^p = b^p = c^p = 1, \quad ab = cac^{-1}, \quad [b,a] = 1 = [b,c].$$

Because $b \neq 1$, the middle equality shows that the group is not commutative. When p is odd, all elements except 1 have order p. When $p = 2$, $G \approx D_4$, which does have an element of order 2^2. Note that this shows that a group can have quite different representations as a semidirect product:

$$D_4 \overset{(3.9\text{a})}{\approx} C_4 \rtimes C_2 \approx (C_2 \times C_2) \rtimes C_2.$$

For an odd prime p, a noncommutative group of order p^3 is isomorphic to the group in (3.14) if it has an element of order p^2 and to the group in (3.15) if it doesn't (see Exercise 4-4). In particular, up to isomorphism, there are exactly two noncommutative groups of order p^3.

3.16 **Making outer automorphisms inner.** Let α be an automorphism, possibly outer, of a group N. We can realize N as a normal subgroup of a group G in such a way that α becomes the restriction to N of an inner automorphism of G. To see this, let $\theta: C_\infty \to \mathrm{Aut}(N)$ be the homomorphism sending a generator a of C_∞ to $\alpha \in \mathrm{Aut}(N)$, and let $G = N \rtimes_\theta C_\infty$. The element $g = (1, a)$ of G has the property that $g(n,1)g^{-1} = (\alpha(n), 1)$ for all $n \in N$.

Criteria for semidirect products to be isomorphic

It will be useful to have criteria for when two triples (N, Q, θ) and (N, Q, θ') determine isomorphic groups.

LEMMA 3.17 *If there exists an $\alpha \in \mathrm{Aut}(N)$ such that*

$$\theta'(q) = \alpha \circ \theta(q) \circ \alpha^{-1}, \quad \textit{all } q \in Q,$$

then the map

$$(n,q) \mapsto (\alpha(n), q) \colon N \rtimes_\theta Q \to N \rtimes_{\theta'} Q$$

is an isomorphism.

PROOF. For $(n,q) \in N \rtimes_\theta Q$, let $\gamma(n,q) = (\alpha(n), q)$. Then

$$\begin{aligned}
\gamma(n,q)\cdot\gamma(n',q') &= (\alpha(n),q)\cdot(\alpha(n'),q') \\
&= (\alpha(n)\cdot\theta'(q)(\alpha(n')), qq') \\
&= (\alpha(n)\cdot(\alpha\circ\theta(q)\circ\alpha^{-1})(\alpha(n')), qq') \\
&= (\alpha(n)\cdot\alpha(\theta(q)(n')), qq'),
\end{aligned}$$

and

$$\begin{aligned}
\gamma((n,q)\cdot(n',q')) &= \gamma(n\cdot\theta(q)(n'), qq') \\
&= (\alpha(n)\cdot\alpha\left(\theta(q)(n')\right), qq').
\end{aligned}$$

Therefore γ is a homomorphism. The map

$$(n,q) \mapsto (\alpha^{-1}(n), q) \colon N \rtimes_{\theta'} Q \to N \rtimes_\theta Q$$

is also a homomorphism, and it is inverse to γ, and so both are isomorphisms. □

LEMMA 3.18 *If $\theta = \theta' \circ \alpha$ with $\alpha \in \mathrm{Aut}(Q)$, then the map*

$$(n,q) \mapsto (n, \alpha(q)) \colon N \rtimes_\theta Q \approx N \rtimes_{\theta'} Q$$

is an isomorphism.

PROOF. Routine verification. □

LEMMA 3.19 *If Q is finite and cyclic and the subgroup $\theta(Q)$ of* $\mathrm{Aut}(N)$ *is conjugate to $\theta'(Q)$, then*

$$N \rtimes_{\theta} Q \approx N \rtimes_{\theta'} Q.$$

PROOF. Let a generate Q. By assumption, there exists an $a' \in Q$ and an $\alpha \in \mathrm{Aut}(N)$ such that

$$\theta'(a') = \alpha \cdot \theta(a) \cdot \alpha^{-1}.$$

The element $\theta'(a')$ generates $\theta'(Q)$, and so we can choose a' to generate Q, say $a' = a^i$ with i relatively prime to the order of Q. Now the map $(n,q) \mapsto (\alpha(n), q^i)$ is an isomorphism $N \rtimes_{\theta} Q \to N \rtimes_{\theta'} Q$. □

SUMMARY 3.20 Let G be a group with subgroups H_1 and H_2 such that $G = H_1 H_2$ and $H_1 \cap H_2 = \{e\}$, so that each element g of G can be written uniquely as $g = h_1 h_2$ with $h_1 \in H_1$ and $h_2 \in H_2$.

(a) If H_1 and H_2 are both normal, then G is the direct product of H_1 and H_2, $G = H_1 \times H_2$ (1.51).
(b) If H_1 is normal in G, then G is the semidirect product of H_1 and H_2, $G = H_1 \rtimes H_2$ ((15), p. 46).
(c) If neither H_1 nor H_2 is normal, then G is the Zappa-Szép (or knit) product of H_1 and H_2 (see Wikipedia: Zappa-Szep product).

NOTES If Q is infinite, the proof Lemma 3.19 fails (it may not be possible to choose a' to generate Q). The following counterexample was provided by Thomas Lamm.

Let $N = C_{25}$ with generator a, $Q = C_{\infty}$ with generator b. Then $\mathrm{Aut}(N)$ is cyclic of order 20. Let $\theta\colon Q \to \mathrm{Aut}(N)$ be such that $\theta(b)$ takes a to a^6, which is an automorphism of order 5. Then $\theta(Q)$ is the cyclic subgroup of $\mathrm{Aut}(N)$ generated by $\theta(b)$ consisting of the automorphisms of order dividing 5. Let $\theta'\colon Q \to \mathrm{Aut}(N)$ be such that $\theta'(b)$ takes a to a^{11}, which is also of order 5. Then $\theta'(Q) = \theta(Q)$, so the conditions of the Lemma are satisfied.

The semidirect product defined by (N, Q, θ) is isomorphic to $G = \langle a, b | a^{25} = 1, ba = a^6 b\rangle$, while the one corresponding to θ' is isomorphic to $G' = \langle c, d | c^{25} = 1, dc = c^{11} d\rangle$. If $G = G'$, we can express c, d in terms of a, b, and vice versa. Now a and c generate the torsion subgroups (equal to N) of G and G', so $c = a^i$ for some i prime to 5. Similarly, b, d generate the quotients (equal to Q) of G and G' by their torsion subgroups, so $d = a^j b$ for some j (or $d = a^j b^{-1}$ and the proof is similar). But then $a^{11i} = c^{11} = dcd^{-1} = a^j b a^i b^{-1} a^{-j} = a^j (bab^{-1})^i a^{-j} = a^{6i}$. So $a^{5i} = 1$, and 5 divides i, a contradiction.

Extensions of groups

A sequence of groups and homomorphisms

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1 \tag{16}$$

is ***exact*** if ι is injective, π is surjective, and $\mathrm{Ker}(\pi) = \mathrm{Im}(\iota)$. Thus $\iota(N)$ is a normal subgroup of G (isomorphic by ι to N) and $G/\iota(N) \xrightarrow{\simeq} Q$. We often identify N with the subgroup $\iota(N)$ of G and Q with the quotient G/N.

An exact sequence (16) is also called an ***extension of Q by N***.[1] An extension is ***central*** if $\iota(N) \subset Z(G)$. For example, a semidirect product $N \rtimes_{\theta} Q$ gives rise to an extension of Q by N,

$$1 \to N \to N \rtimes_{\theta} Q \to Q \to 1,$$

[1] This is Bourbaki's terminology (Algèbre, I §6); some authors call (16) an extension of N by Q.

which is central if and only if θ is the trivial homomorphism and N is commutative.

Two extensions of Q by N are said to be ***isomorphic*** if there exists a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, equal] & G \arrow[r] \arrow[d, "\approx"] & Q \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & N \arrow[r] & G' \arrow[r] & Q \arrow[r] & 1.
\end{tikzcd}$$

An extension of Q by N,

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1,$$

is said to be ***split*** if it is isomorphic to the extension defined by a semidirect product $N \rtimes_\theta Q$. Equivalent conditions:

(a) there exists a subgroup $Q' \subset G$ such that π induces an isomorphism $Q' \to Q$; or
(b) there exists a homomorphism $s\colon Q \to G$ such that $\pi \circ s = \mathrm{id}$.

In general, an extension will not split. For example,

$$1 \to C_p \to C_{p^2} \to C_p \to 1$$

doesn't split. If Q is the quaternion group and N is its centre, then

$$1 \to N \to Q \to Q/N \to 1 \tag{17}$$

doesn't split (if it did, Q would be commutative because N and Q/N are commutative and θ is trivial).

THEOREM 3.21 (SCHUR-ZASSENHAUS) *An extension of finite groups of relatively prime order is split.*

PROOF. Rotman 1995, 7.41. □

PROPOSITION 3.22 *An extension (16) splits if N is complete. In fact, G is then the direct product of N with the centralizer of N in G,*

$$C_G(N) \overset{\text{def}}{=} \{g \in G \mid gn = ng \text{ all } n \in N\}.$$

PROOF. Let $H = C_G(N)$. We shall check that N and H satisfy the conditions of Proposition 1.51.

Observe first that, for any $g \in G$, $n \mapsto gng^{-1}\colon N \to N$ is an automorphism of N, and (because N is complete), it must be the inner automorphism defined by an element γ of N; thus

$$gng^{-1} = \gamma n \gamma^{-1} \quad \text{all } n \in N.$$

This equation shows that $\gamma^{-1}g \in H$, and hence $g = \gamma(\gamma^{-1}g) \in NH$. Since g was arbitrary, we have shown that $G = NH$.

Next note that every element of $N \cap H$ is in the centre of N, which (because N is complete) is trivial; hence $N \cap H = 1$.

Finally, for any element $g = nh \in G$,

$$gHg^{-1} = n(hHh^{-1})n^{-1} = nHn^{-1} = H$$

(recall that every element of N commutes with every element of H). Therefore H is normal in G. □

An extension

$$1 \to N \to G \to Q \to 1$$

gives rise to a homomorphism $\theta'\colon G \to \mathrm{Aut}(N)$, namely,

$$\theta'(g)(n) = gng^{-1}.$$

Let $\tilde{q} \in G$ map to q in Q; then the image of $\theta'(\tilde{q})$ in $\mathrm{Aut}(N)/\mathrm{Inn}(N)$ depends only on q; therefore we get a homomorphism

$$\theta : Q \to \mathrm{Out}(N) \overset{\text{def}}{=} \mathrm{Aut}(N)/\mathrm{Inn}(N).$$

This map θ depends only on the isomorphism class of the extension, and we write $\mathrm{Ext}^1(Q,N)_\theta$ for the set of isomorphism classes of extensions with a given θ. These sets have been extensively studied.

When Q and N are commutative, there is a commutative group structure on the set $\mathrm{Ext}^1(Q,N)_\theta$. Moreover, endomorphisms of Q and N act as endomorphisms on $\mathrm{Ext}^1(Q,N)_\theta$. In particular, multiplication by m on Q or N induces multiplication by m on $\mathrm{Ext}^1(Q,N)_\theta$. Thus, if Q and N are killed by m and n respectively, then $\mathrm{Ext}^1(Q,N)_\theta$ is killed by m and by n, and hence by $\gcd(m,n)$. This proves the Schur-Zassenhaus theorem in this case.

The Hölder program.

> It would be of the greatest interest if it were possible to give an overview of the entire collection of finite simple groups.
>
> Otto Hölder, Math. Ann., 1892

Recall that a group G is simple if it contains no normal subgroup except 1 and G. In other words, a group is simple if it can't be realized as an extension of smaller groups. Every finite group can be obtained by taking repeated extensions of simple groups. Thus the simple finite groups can be regarded as the basic building blocks for all finite groups.

The problem of classifying all simple groups falls into two parts:

A. Classify all finite simple groups;
B. Classify all extensions of finite groups.

A. THE CLASSIFICATION OF FINITE SIMPLE GROUPS

There is a complete list of finite simple groups. They are[2]

(a) the cyclic groups of prime order,
(b) the alternating groups A_n for $n \geq 5$ (see the next chapter),
(c) certain infinite families of matrix groups (said to be of Lie type), and
(d) the 26 "sporadic groups".

[2] It has been shown that every group on the list can be generated by two elements, and so this is true for all finite simple groups. If a proof of this could be found that doesn't use the classification, then the proof of the classification would be greatly simplified (mo59213).

By far the largest class is (c), but the 26 sporadic groups are of more interest than their small number might suggest. Some have even speculated that the largest of them, the Fischer-Griess monster, is built into the fabric of the universe.

As an example of a matrix group, consider

$$\mathrm{SL}_m(\mathbb{F}_q) \overset{\text{def}}{=} \{m \times m \text{ matrices } A \text{ with entries in } \mathbb{F}_q \text{ such that } \det A = 1\}.$$

Here $q = p^n$, p prime, and $\mathbb{F}_q$ is "the" field with q elements. This group is not simple if $q \neq 2$, because the scalar matrices $\mathrm{diag}(\zeta, \ldots, \zeta)$, $\zeta^m = 1$, are in the centre for any m dividing $q-1$, but these are the only matrices in the centre, and the groups

$$\mathrm{PSL}_n(\mathbb{F}_q) \overset{\text{def}}{=} \mathrm{SL}_n(\mathbb{F}_q)/\{\text{centre}\}$$

are simple when $m \geq 3$ (Rotman 1995, 8.23) and when $m = 2$ and $q > 3$ (ibid. 8.13). Other finite simple groups can be obtained from the groups in (1.8). The smallest noncommutative group is A_5, and the second smallest is $\mathrm{PSL}_3(\mathbb{F}_2)$, which has order 168 (see Exercise 4-8).

B The classification of all extensions of finite groups

Much is known about the extensions of finite groups, for example, about the extensions of one simple group by another. However, as Solomon writes (2001, p. 347):

> ... the classification of all finite groups is completely infeasible. Nevertheless experience shows that most of the finite groups which occur in "nature" ... are "close" either to simple groups or to groups such as dihedral groups, Heisenberg groups, etc., which arise naturally in the study of simple groups.

As we noted earlier, by the year 2001, a complete irredundant list of finite groups was available only for those up to an order of about 2000, and the number of groups on the list is overwhelming.

Notes The dream of classifying the finite simple groups goes back at least to Hölder 1892. However a clear strategy for accomplishing this did not begin to emerge until the 1950s, when work of Brauer and others suggested that the key was to study the centralizers of elements of order 2 (the involution centralizers). For example, Brauer and Fowler (1955) showed that, for any finite group H, the determination of the finite simple groups with an involution centralizer isomorphic to H is a finite problem. Later work showed that the problem is even tractable, and so the strategy became: (a) list the groups H that are candidates for being an involution centralizer in some finite simple group, and (b) for each H in (a) list the finite simple groups for which H occurs as an involution centralizer. Of course, this approach applies only to the finite simple groups containing an element of order 2, but an old conjecture said that, except for the cyclic groups of prime order, every finite simple group has even order and hence contains an element of order 2 by Cauchy's theorem (4.13). With the proof of this conjecture by Feit and Thompson (1963), the effort to complete the classification of the finite simple groups began in earnest. A complete classification was announced in 1982, but there remained sceptics, because the proof depended on thousands of pages of rarely read journal articles, and, in fact, in reworking the proof, gaps were discovered. However, these have been closed, and with the publication of Aschbacher and Smith 2004 it has become generally accepted that the proof of the classification is indeed complete.

For a popular account of the history of the classification, see the book Ronan 2006, and for a more technical account, see the expository article Solomon 2001.

Exercises

3-1 Let G be the quaternion group (1.18). Prove that G can't be written as a semidirect product in any nontrivial fashion.

3-2 Let G be a group of order mn, where m and n have no common factor. If G contains exactly one subgroup M of order m and exactly one subgroup N of order n, prove that G is the direct product of M and N.

3-3 Prove that $\mathrm{GL}_2(\mathbb{F}_2) \approx S_3$.

3-4 Let G be the quaternion group (1.18). Prove that $\mathrm{Aut}(G) \approx S_4$.

3-5 Let G be the set of all matrices in $\mathrm{GL}_3(\mathbb{R})$ of the form $\left(\begin{smallmatrix} a & 0 & b \\ 0 & a & c \\ 0 & 0 & d \end{smallmatrix}\right)$, $ad \neq 0$. Check that G is a subgroup of $\mathrm{GL}_3(\mathbb{R})$, and prove that it is a semidirect product of $\mathbb{R}^2$ (additive group) by $\mathbb{R}^\times \times \mathbb{R}^\times$. Is it a direct product of these two groups?

3-6 Find the automorphism groups of C_∞ and S_3.

3-7 Let $G = N \rtimes Q$, where N and Q are finite groups, and let $g = nq$ be an element of G with $n \in N$ and $q \in Q$. Denote the order of an element x by $o(x)$.

(a) Show that $o(g) = k \cdot o(q)$ for some divisor k of $|N|$.

(b) When Q acts trivially on N, show that $o(g) = \mathrm{lcm}(o(n), o(q))$.

(c) Let $G = S_5 = A_5 \rtimes Q$ with $Q = \langle(1,2)\rangle$. Let $n = (1,4,3,2,5)$ and let $q = (1,2)$. Show that $o(g) = 6$, $o(n) = 5$, and $o(q) = 2$.

(d) Suppose that $G = (C_p)^p \rtimes Q$, where Q is cyclic of order p and that, for some generator q of Q,

$$q(a_1,\ldots,a_n)q^{-1} = (a_n, a_1, \ldots, a_{n-1}).$$

Show inductively that, for $i \leq p$,

$$((1,0,\ldots,0),q)^i = ((1,\ldots,1,0,\ldots,0), q^i)$$

(i copies of 1). Deduce that $((1,0,\ldots,0),q)$ has order p^2 (hence $o(g) = o(n) \cdot o(q)$ in this case).

(e) Suppose that $G = N \rtimes Q$, where N is commutative, Q is cyclic of order 2, and the generator q of Q acts on N by sending each element to its inverse. Show that $(n,1)$ has order 2 no matter what n is (in particular, $o(g)$ is independent of $o(n)$).

3-8 Let G be the semidirect $G = N \rtimes Q$ of its subgroups N and Q, and let

$$C_N(Q) = \{n \in N \mid nq = qn \text{ for all } q \in Q\}$$

(centralizer of Q in N). Show that

$$Z(G) = \{n \cdot q \mid n \in C_N(Q),\, q \in Z(Q),\, nn'n^{-1} = q^{-1}n'q \text{ for all } n' \in N\}.$$

Let θ be the homomorphism $Q \to \mathrm{Aut}(N)$ giving the action of Q on N (by conjugation). Show that if N is commutative, then

$$Z(G) = \{n \cdot q \mid n \in C_N(Q),\, q \in Z(Q) \cap \mathrm{Ker}(\theta)\},$$

and if N and Q are commutative, then

$$Z(G) = \{n \cdot q \mid n \in C_N(Q),\, q \in \mathrm{Ker}(\theta)\}.$$

3-9 A homomorphism $a\colon G \to H$ of groups is ***normal*** if $a(G)$ is a normal subgroup of H. The cokernel of a normal homomorphism a is defined to be $H/a(G)$. Show that, if in the following commutative diagram, the blue sequences are exact and the homomorphisms a, b, c are normal, then the red sequence exists and is exact:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}\, f \arrow[r] & \mathrm{Ker}\, a \arrow[r] \arrow[d] & \mathrm{Ker}\, b \arrow[r] \arrow[d] & \mathrm{Ker}\, c \arrow[d] \arrow[dddll, bend left, "d"'] & \\
 & & A \arrow[r, "f"] \arrow[d, "a"] & B \arrow[r, "g"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\
 & 0 \arrow[r] & A' \arrow[r, "f'"'] \arrow[d] & B' \arrow[r, "g'"'] \arrow[d] & C' \arrow[d] & \\
 & & \mathrm{Coker}\, a \arrow[r] & \mathrm{Coker}\, b \arrow[r] & \mathrm{Coker}\, c &
\end{tikzcd}$$

3-10 Let N and H be subgroups of G, and assume that H normalizes N, i.e., $hNh^{-1} \subset N$ for all $h \in H$. Let θ denote the action of H on N, $\theta(h)(n) = hnh^{-1}$. Show that

$$(n, h) \mapsto nh\colon N \rtimes_\theta H \to G$$

is a homomorphism with image NH.

3-11 Let N and Q be subgroups of a group G. Show that G is the semidirect product of N and Q if and only if there exists a homomorphism $G \to Q$ whose restriction to Q is the identity map and whose kernel is N.

CHAPTER **4**

Groups Acting on Sets

Definition and examples

DEFINITION 4.1 Let X be a set and let G be a group. A ***left action*** of G on X is a mapping $(g,x) \mapsto gx: G \times X \to X$ such that

(a) $1x = x$, for all $x \in X$;
(b) $(g_1 g_2)x = g_1(g_2 x)$, all $g_1, g_2 \in G$, $x \in X$.

A set together with a (left) action of G is called a (left) ***G-set***. An action is ***trivial*** if $gx = x$ for all $g \in G$.

The conditions imply that, for each $g \in G$, left translation by g,

$$g_L: X \to X, \quad x \mapsto gx,$$

has $(g^{-1})_L$ as an inverse, and therefore g_L is a bijection, i.e., $g_L \in \mathrm{Sym}(X)$. Axiom (b) now says that

$$g \mapsto g_L: G \to \mathrm{Sym}(X) \tag{18}$$

is a homomorphism. Thus, from a left action of G on X, we obtain a homomorphism $G \to \mathrm{Sym}(X)$; conversely, every such homomorphism defines an action of G on X. The action is said to be ***faithful*** (or ***effective***) if the homomorphism (18) is injective, i.e., if

$$gx = x \text{ for all } x \in X \implies g = 1.$$

EXAMPLE 4.2 (a) Every subgroup of the symmetric group S_n acts faithfully on $\{1, 2, ..., n\}$.

(b) Every subgroup H of a group G acts faithfully on G by left translation,

$$H \times G \to G, \quad (h,x) \mapsto hx.$$

(c) Let H be a subgroup of G. The group G acts on the set of left cosets of H,

$$G \times G/H \to G/H, \quad (g,C) \mapsto gC.$$

The action is faithful if, for example, $H \neq G$ and G is simple.

(d) Every group G acts on itself by conjugation,

$$G \times G \to G, \quad (g,x) \mapsto {}^g x \overset{\text{def}}{=} gxg^{-1}.$$

For any normal subgroup N, G acts on N and G/N by conjugation.

(e) For any group G, $\mathrm{Aut}(G)$ acts on G.

(f) The ***group of rigid motions*** of $\mathbb{R}^n$ is the group of bijections $\mathbb{R}^n \to \mathbb{R}^n$ preserving lengths. It acts on $\mathbb{R}^n$ on the left.

A ***right action*** $X \times G \to G$ is defined similarly. To turn a right action into a left action, set $g * x = xg^{-1}$. For example, there is a natural right action of G on the set of right cosets of a subgroup H in G, namely, $(C,g) \mapsto Cg$, which can be turned into a left action $(g,C) \mapsto Cg^{-1}$.

A ***map of G-sets*** (alternatively, a ***G-map*** or a ***G-equivariant map***) is a map $\varphi\colon X \to Y$ such that

$$\varphi(gx) = g\varphi(x), \quad \text{all } g \in G, \quad x \in X.$$

An ***isomorphism*** of G-sets is a bijective G-map; its inverse is then also a G-map.

ORBITS

Let G act on X. A subset $S \subset X$ is said to be ***stable*** under the action of G if

$$g \in G, \quad x \in S \implies gx \in S.$$

The action of G on X then induces an action of G on S.

Write $x \sim_G y$ if $y = gx$, some $g \in G$. This relation is reflexive because $x = 1x$, symmetric because

$$y = gx \implies x = g^{-1}y$$

(multiply by g^{-1} on the left and use the axioms), and transitive because

$$y = gx, \quad z = g'y \implies z = g'(gx) = (g'g)x.$$

It is therefore an equivalence relation. The equivalence classes are called ***G-orbits***. Thus the G-orbits partition X. Write $G\backslash X$ for the set of orbits.

By definition, the G-orbit containing x_0 is

$$Gx_0 = \{gx_0 \mid g \in G\}.$$

It is the smallest G-stable subset of X containing x_0.

EXAMPLE 4.3 (a) Suppose G acts on X, and let $\alpha \in G$ be an element of order n. Then the orbits of $\langle\alpha\rangle$ are the sets of the form

$$\{x_0, \alpha x_0, \ldots, \alpha^{n-1}x_0\}.$$

(These elements need not be distinct, and so the set may contain fewer than n elements.)

(b) The orbits for a subgroup H of G acting on G by left multiplication are the right cosets of H in G. We write $H\backslash G$ for the set of right cosets. Similarly, the orbits for H acting by right multiplication are the left cosets, and we write G/H for the set of left cosets. Note that the group law on G will *not* induce a group law on G/H unless H is normal.

(c) For a group G acting on itself by conjugation, the orbits are called ***conjugacy classes:*** for $x \in G$, the conjugacy class of x is the set

$$\{gxg^{-1} \mid g \in G\}$$

of conjugates of x. The conjugacy class of x_0 always contains x_0, and it consists only of x_0 if and only if x_0 is in the centre of G. In linear algebra the conjugacy classes in $G = \mathrm{GL}_n(k)$ are called similarity classes, and the theory of rational canonical forms provides a set of representatives for the conjugacy classes: two matrices are similar (conjugate) if and only if they have the same rational canonical form.

Note that a subset of X is stable if and only if it is a union of orbits. For example, a subgroup H of G is normal if and only if it is a union of conjugacy classes.

The action of G on X is said to be ***transitive***, and G is said to act ***transitively*** on X, if there is only one orbit, i.e., for any two elements x and y of X, there exists a $g \in G$ such that $gx = y$. The set X is then called a ***homogeneous*** G-set. For example, S_n acts transitively on $\{1,2,...,n\}$. For any subgroup H of a group G, G acts transitively on G/H, but the action of G on itself is never transitive if $G \neq 1$ because $\{1\}$ is always a conjugacy class.

The action of G on X is ***doubly transitive*** if for any two pairs (x_1,x_2), (y_1,y_2) of elements of X with $x_1 \neq x_2$ and $y_1 \neq y_2$, there exists a (single) $g \in G$ such that $gx_1 = y_1$ and $gx_2 = y_2$. Define k***-fold transitivity*** for $k \geq 3$ similarly.

STABILIZERS

Let G act on X. The ***stabilizer*** (or ***isotropy group***) of an element $x \in X$ is

$$\mathrm{Stab}(x) = \{g \in G \mid gx = x\}.$$

It is a subgroup, but it need not be a normal subgroup (see the next lemma). The action is ***free*** if $\mathrm{Stab}(x) = \{e\}$ for all x.

LEMMA 4.4 *For any $g \in G$ and $x \in X$,*

$$\mathrm{Stab}(gx) = g \cdot \mathrm{Stab}(x) \cdot g^{-1}.$$

PROOF. Certainly, if $g'x = x$, then

$$(gg'g^{-1})gx = gg'x = gx = y,$$

and so $g \cdot \mathrm{Stab}(x) \cdot g^{-1} \subset \mathrm{Stab}(gx)$. Conversely, if $g'(gx) = gx$, then

$$(g^{-1}g'g)x = g^{-1}g'(gx) = g^{-1}y = x,$$

and so $g^{-1}g'g \in \mathrm{Stab}(x)$, i.e., $g' \in g \cdot \mathrm{Stab}(x) \cdot g^{-1}$. □

Clearly

$$\bigcap_{x \in X} \mathrm{Stab}(x) = \mathrm{Ker}(G \to \mathrm{Sym}(X)),$$

which is a normal subgroup of G. The action is faithful if and only if $\bigcap \mathrm{Stab}(x) = \{1\}$.

EXAMPLE 4.5 (a) Let G act on itself by conjugation. Then

$$\mathrm{Stab}(x) = \{g \in G \mid gx = xg\}.$$

This group is called the ***centralizer*** $C_G(x)$ of x in G. It consists of all elements of G that commute with, i.e., centralize, x. The intersection

$$\bigcap_{x \in G} C_G(x) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$$

is the centre of G.

(b) Let G act on G/H by left multiplication. Then $\mathrm{Stab}(H) = H$, and the stabilizer of gH is gHg^{-1}.

(c) Let G be the group of rigid motions of $\mathbb{R}^n$ (4.2f). The stabilizer of the origin is the orthogonal group O_n for the standard positive definite form on $\mathbb{R}^n$ (Artin 1991, Chap. 4, 5.16). Let $T \simeq (\mathbb{R}^n, +)$ be the subgroup of G of translations of $\mathbb{R}^n$, i.e., maps of the form $v \mapsto v + v_0$ some $v_0 \in \mathbb{R}^n$. Then T is a normal subgroup of G and $G \simeq T \rtimes O$ (cf. Artin 1991, Chap. 5, §2).

For a subset S of X, we define the ***stabilizer*** of S to be

$$\mathrm{Stab}(S) = \{g \in G \mid gS = S\}.$$

Then $\mathrm{Stab}(S)$ is a subgroup of G, and the same argument as in the proof of (4.4) shows that

$$\mathrm{Stab}(gS) = g \cdot \mathrm{Stab}(S) \cdot g^{-1}.$$

EXAMPLE 4.6 Let G act on G by conjugation, and let H be a subgroup of G. The stabilizer of H is called the ***normalizer*** $N_G(H)$ of H in G:

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Clearly $N_G(H)$ is the largest subgroup of G containing H as a normal subgroup.

It is possible for $gS \subset S$ but $g \notin \mathrm{Stab}(S)$ (see 1.33).

TRANSITIVE ACTIONS

PROPOSITION 4.7 *If G acts transitively on X, then for any $x_0 \in X$, the map*

$$g\,\mathrm{Stab}(x_0) \mapsto gx_0 \colon G/\mathrm{Stab}(x_0) \to X$$

is an isomorphism of G-sets.

PROOF. It is well-defined because, if $h \in \mathrm{Stab}(x_0)$, then $ghx_0 = gx_0$. It is injective because

$$gx_0 = g'x_0 \implies g^{-1}g'x_0 = x_0 \implies g, g' \text{ lie in the same left coset of } \mathrm{Stab}(x_0).$$

It is surjective because G acts transitively. Finally, it is obviously G-equivariant. □

Thus every homogeneous G-set X is isomorphic to G/H for some subgroup H of G, but such a realization of X is *not canonical*: it depends on the choice of $x_0 \in X$. To say this another way, the G-set G/H has a preferred point, namely, the coset H; to give a homogeneous G-set X *together with a preferred point* is essentially the same as to give a subgroup of G.

COROLLARY 4.8 *Let G act on X, and let $O = Gx_0$ be the orbit containing x_0. Then the cardinality of O is*

$$|O| = (G : \mathrm{Stab}(x_0)). \tag{19}$$

For example, the number of conjugates gHg^{-1} of a subgroup H of G is $(G : N_G(H))$.

PROOF. The action of G on O is transitive, and so $g \mapsto gx_0$ defines a bijection $G/\operatorname{Stab}(x_0) \to Gx_0$. □

The equation (19) is frequently useful for computing $|O|$.

PROPOSITION 4.9 *Let $x_0 \in X$. If G acts transitively on X, then*

$$\operatorname{Ker}(G \to \operatorname{Sym}(X))$$

is the largest normal subgroup contained in $\operatorname{Stab}(x_0)$.

PROOF. When

$$\operatorname{Ker}(G \to \operatorname{Sym}(X)) = \bigcap_{x \in X} \operatorname{Stab}(x) = \bigcap_{g \in G} \operatorname{Stab}(gx_0) \overset{(4.4)}{=} \bigcap g \cdot \operatorname{Stab}(x_0) \cdot g^{-1}.$$

Hence, the proposition is a consequence of the following lemma. □

LEMMA 4.10 *For any subgroup H of a group G, $\bigcap_{g \in G} gHg^{-1}$ is the largest normal subgroup contained in H.*

PROOF. Note that $N_0 \overset{\text{def}}{=} \bigcap_{g \in G} gHg^{-1}$, being an intersection of subgroups, is itself a subgroup. It is normal because

$$g_1 N_0 g_1^{-1} = \bigcap_{g \in G} (g_1 g) N_0 (g_1 g)^{-1} = N_0$$

— for the second equality, we used that, as g runs over the elements of G, so also does $g_1 g$. Thus N_0 is a normal subgroup of G contained in $eHe^{-1} = H$. If N is a second such group, then

$$N = gNg^{-1} \subset gHg^{-1}$$

for all $g \in G$, and so

$$N \subset \bigcap_{g \in G} gHg^{-1} = N_0.$$

□

THE CLASS EQUATION

When X is finite, it is a disjoint union of a finite number of orbits:

$$X = \bigcup_{i=1}^{m} O_i \qquad \text{(disjoint union).}$$

Hence:

PROPOSITION 4.11 *The number of elements in X is*

$$|X| = \sum_{i=1}^{m} |O_i| = \sum_{i=1}^{m} (G : \operatorname{Stab}(x_i)), \quad x_i \text{ in } O_i. \tag{20}$$

When G acts on itself by conjugation, this formula becomes:

PROPOSITION 4.12 (CLASS EQUATION)

$$|G| = \sum (G : C_G(x)) \tag{21}$$

(x runs over a set of representatives for the conjugacy classes), or

$$|G| = |Z(G)| + \sum (G : C_G(y)) \tag{22}$$

(y runs over set of representatives for the conjugacy classes containing more than one element).

THEOREM 4.13 (CAUCHY) *If the prime p divides $|G|$, then G contains an element of order p.*

PROOF. We use induction on $|G|$. If for some y not in the centre of G, p does not divide $(G : C_G(y))$, then p divides the order of $C_G(y)$ and we can apply induction to find an element of order p in $C_G(y)$. Thus we may suppose that p divides all of the terms $(G : C_G(y))$ in the class equation (second form), and so also divides $Z(G)$. But $Z(G)$ is commutative, and it follows from the structure theorem[1] of such groups that $Z(G)$ will contain an element of order p. □

COROLLARY 4.14 *A finite group G is a p-group if and only if every element has order a power of p.*

PROOF. If $|G|$ is a power of p, then Lagrange's theorem (1.26) shows that the order of every element is a power of p. The converse follows from Cauchy's theorem. □

COROLLARY 4.15 *Every group of order $2p$, p an odd prime, is cyclic or dihedral.*

PROOF. From Cauchy's theorem, we know that such a G contains elements s and r of orders 2 and p respectively. Let $H = \langle r \rangle$. Then H is of index 2, and so is normal. Obviously $s \notin H$, and so $G = H \cup Hs$:

$$G = \{1, r, \ldots, r^{p-1}, s, rs, \ldots, r^{p-1}s\}.$$

As H is normal, $srs^{-1} = r^i$, some i. Because $s^2 = 1$, $r = s^2rs^{-2} = s(srs^{-1})s^{-1} = r^{i^2}$, and so $i^2 \equiv 1 \bmod p$. Because $\mathbb{Z}/p\mathbb{Z}$ is a field, its only elements with square 1 are ± 1, and so $i \equiv 1$ or $-1 \bmod p$. In the first case, the group is commutative (any group generated by a set of commuting elements is obviously commutative); in the second $srs^{-1} = r^{-1}$ and we have the dihedral group (2.9). □

[1] Here is a direct proof that the theorem holds for an abelian group Z. We use induction on the order of Z. It suffices to show that Z contains an element whose order is divisible by p, because then some power of the element will have order exactly p. Let $g \neq 1$ be an element of Z. If p doesn't divide the order of g, then it divides the order of $Z/\langle g \rangle$, in which case there exists (by induction) an element of G whose order in $Z/\langle g \rangle$ is divisible by p. But the order of such an element must itself be divisible by p.

p-GROUPS

THEOREM 4.16 *Every nontrivial finite p-group has nontrivial centre.*

PROOF. By assumption, $(G:1)$ is a power of p, and so $(G:C_G(y))$ is power of p $(\neq p^0)$ for all y not in the centre of G. As p divides every term in the class equation (22) except (perhaps) $|Z(G)|$, it must divide $|Z(G)|$ also. □

COROLLARY 4.17 *A group of order p^n has normal subgroups of order p^m for all $m \leq n$.*

PROOF. We use induction on n. The centre of G contains an element g of order p, and so $N = \langle g \rangle$ is a normal subgroup of G of order p. Now the induction hypothesis allows us to assume the result for G/N, and the correspondence theorem (1.47) then gives it to us for G. □

PROPOSITION 4.18 *Every group of order p^2 is commutative, and hence is isomorphic to $C_p \times C_p$ or C_{p^2}.*

PROOF. We know that the centre Z is nontrivial, and that G/Z therefore has order 1 or p. In either case it is cyclic, and the next result implies that G is commutative. □

LEMMA 4.19 *Suppose G contains a subgroup H in its centre (hence H is normal) such that G/H is cyclic. Then G is commutative.*

PROOF. Let a be an element of G whose image in G/H generates it. Then every element of G can be written $g = a^i h$ with $h \in H$, $i \in \mathbb{Z}$. Now

$$\begin{aligned} a^i h \cdot a^{i'} h' &= a^i a^{i'} h h' \qquad \text{because } H \subset Z(G) \\ &= a^{i'} a^i h' h \\ &= a^{i'} h' \cdot a^i h. \end{aligned}$$

□

REMARK 4.20 The above proof shows that if $H \subset Z(G)$ and G contains a set of representatives for G/H whose elements commute, then G is commutative.

For p odd, it is now not difficult to show that any noncommutative group of order p^3 is isomorphic to exactly one of the groups constructed in (3.14, 3.15) (Exercise 4-4). Thus, up to isomorphism, there are exactly two noncommutative groups of order p^3.

EXAMPLE 4.21 Let G be a noncommutative group of order 8. Then G must contain an element a of order 4 (see Exercise 1-6). If G contains an element b of order 2 not in $\langle a \rangle$, then $G \simeq \langle a \rangle \rtimes_\theta \langle b \rangle$, where θ is the unique isomorphism $\mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/4\mathbb{Z})^\times$, and so $G \approx D_4$. If not, any element b of G not in $\langle a \rangle$ must have order 4, and $a^2 = b^2$. Now bab^{-1} is an element of order 4 in $\langle a \rangle$. It can't equal a, because otherwise G would be commutative, and so $bab^{-1} = a^3$. Therefore G is the quaternion group (1.18, 2.7b).

NOTES As every finite p-group is obtained by successive extensions from the cyclic group of order p, one might think that there is little to say about such groups. Nothing could be further from the truth — the literature on them is vast. To quote P. Hall, "There is no apparent limit to the complication of a prime-power group. As we pass from the groups of order p^3 to those of order p^4, then to those of order p^5, and so on, at each stage new structural phenomena make their appearance." For example, there are five groups of order p^3 and fifteen of order p^4 (fourteen if $p = 2$), but for p^5 and larger orders p^n, the number of groups of that order tends to infinity with p. See MR3793194.

ACTION ON THE LEFT COSETS

The action of G on the set of left cosets G/H of H in G is a very useful tool in the study of groups. We illustrate this with some examples.

Let $X = G/H$. Recall that, for any $g \in G$,

$$\operatorname{Stab}(gH) = g\operatorname{Stab}(H)g^{-1} = gHg^{-1}$$

and the kernel of

$$G \to \operatorname{Sym}(X)$$

is the largest normal subgroup $\bigcap_{g\in G} gHg^{-1}$ of G contained in H.

REMARK 4.22 (a) Let H be a subgroup of G not containing a normal subgroup of G other than 1. Then $G \to \operatorname{Sym}(G/H)$ is injective, and we have realized G as a subgroup of a symmetric group of order much smaller than $(G:1)!$. For example, if G is simple, then the Sylow theorems (see Chapter 5) show that G has many proper subgroups $H \neq 1$ (unless G is cyclic), but (by definition) it has no such normal subgroup.

(b) If $(G:1)$ does not divide $(G:H)!$, then

$$G \to \operatorname{Sym}(G/H)$$

can't be injective (Lagrange's theorem, 1.26), and we can conclude that H contains a normal subgroup $\neq 1$ of G. For example, if G has order 99, then it will have a subgroup N of order 11 (Cauchy's theorem, 4.13), and the subgroup must be normal. In fact, G is the product $G = N \times Q$ of N with a group Q of order 9.

EXAMPLE 4.23 Corollary 4.15 shows that every group G of order 6 is either cyclic or dihedral. Here we present a slightly different argument. According to Cauchy's theorem (4.13), G must contain an element r of order 3 and an element s of order 2. Moreover $N \overset{\text{def}}{=} \langle r\rangle$ must be normal because 6 doesn't divide 2! (or simply because it has index 2). Let $H = \langle s\rangle$. Either (a) H is normal in G, or (b) H is not normal in G. In the first case, $rsr^{-1} = s$, i.e., $rs = sr$, and so $G \simeq \langle r\rangle \times \langle s\rangle \approx C_2 \times C_3$. In the second case, $G \to \operatorname{Sym}(G/H)$ is injective, hence surjective, and so $G \approx S_3 \approx D_3$.

Permutation groups

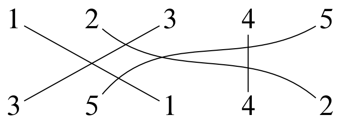
Consider $\operatorname{Sym}(X)$, where X has n elements. Since (up to isomorphism) a symmetry group $\operatorname{Sym}(X)$ depends only on the number of elements in X, we may take $X = \{1, 2, \ldots, n\}$, and so work with S_n. The symbol $\left(\begin{smallmatrix}1&2&3&4&5&6&7\\2&5&7&4&3&1&6\end{smallmatrix}\right)$ denotes the permutation sending $1 \mapsto 2$, $2 \mapsto 5$, $3 \mapsto 7$, and so on.

Consider a permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

The ordered pairs (i, j) with $i < j$ and $\sigma(i) > \sigma(j)$ are called the ***inversions*** of σ, and σ is said to be ***even*** or ***odd*** according as the number its inversions is even or odd. The ***signature***, $\operatorname{sign}(\sigma)$, of σ is $+1$ or -1 according as σ is even or odd. For example, $\operatorname{sign}(\sigma) = -1$ if σ is a transposition.

REMARK 4.24 To compute the signature of σ, connect (by a line) each element i in the top row to the element i in the bottom row, and count the number of times that the lines cross: σ is even or odd according as this number is even or odd. For example,



is even (6 intersections). This works, because there is one crossing for each inversion.

For a permutation σ, consider the products

$$\begin{aligned} V = \prod_{1\le i<j\le n}(j-i) = {} & (2-1)(3-1)\cdots(n-1) \\ & \qquad\quad (3-2)\cdots(n-2) \\ & \qquad\qquad\qquad \cdots \\ & \qquad\qquad\quad (n-(n-1)) \\ \sigma V = \prod_{1\le i<j\le n}(\sigma(j)-\sigma(i)) = {} & (\sigma(2)-\sigma(1))(\sigma(3)-\sigma(1))\cdots(\sigma(n)-\sigma(1)) \\ & \qquad\qquad (\sigma(3)-\sigma(2))\cdots(\sigma(n)-\sigma(2)) \\ & \qquad\qquad\qquad\qquad \cdots \\ & \qquad\qquad\qquad (\sigma(n)-\sigma(n-1)). \end{aligned}$$

Both products run over the 2-element subsets $\{i,j\}$ of $\{1,2,\dots,n\}$, and the terms corresponding to a subset are the same except that each inversion introduces a negative sign. Therefore,

$$\sigma V = \operatorname{sign}(\sigma)V.$$

Now let P be the additive group of maps $\mathbb{Z}^n \to \mathbb{Z}$. For $f \in P$ and $\sigma \in S_n$, let σf denote the element of P defined by

$$(\sigma f)(z_1,\dots,z_n) = f(z_{\sigma(1)},\dots,z_{\sigma(n)}).$$

For $z \in \mathbb{Z}^n$ and $\sigma \in S_n$, let z^σ denote the element of $\mathbb{Z}^n$ such that $(z^\sigma)_i = z_{\sigma(i)}$. Then $(z^\sigma)^\tau = z^{\sigma\tau}$. By definition, $(\sigma f)(z) = f(z^\sigma)$, and so $((\sigma\tau)f)(z) = f(z^{\sigma\tau}) = f((z^\sigma)^\tau) = (\tau f)(z^\sigma) = (\sigma(\tau f))(z)$, i.e.,

$$\sigma(\tau f) = (\sigma\tau)f. \tag{23}$$

Let p be the element of P defined by

$$p(z_1,\dots,z_n) = \prod_{1\le i<j\le n}(z_j - z_i).$$

The same argument as above shows that

$$\sigma p = \operatorname{sign}(\sigma)p.$$

On putting $f = p$ in (23), one finds that

$$\operatorname{sign}(\sigma)\operatorname{sign}(\tau) = \operatorname{sign}(\sigma\tau).$$

Therefore, "sign" is a homomorphism $S_n \to \{\pm 1\}$. When $n \ge 2$, it is surjective, and so its kernel is a normal subgroup of S_n of order $\frac{n!}{2}$, called the ***alternating group*** A_n.

REMARK 4.25 We have shown that there exists a homomorphism sign: $S_n \to \{\pm 1\}$ such that $\text{sign}(\sigma) = -1$ for every transposition σ. The transpositions generate S_n, and so sign is uniquely determined by this property. Now let $G = \text{Sym}(X)$, where X is a set with n elements. The choice of an ordering of X determines an isomorphism of G with S_n sending transpositions to transpositions. Therefore G also admits a unique isomorphism $\varepsilon\colon G \to \{\pm 1\}$ such that $\varepsilon(\sigma) = -1$ for every transposition σ. Once we have chosen an ordering of X, we can speak of the inversions of an element σ of G, and define a sign homomorphism $G \to \{\pm 1\}$ as before. This must agree with ε, and so $\varepsilon(\sigma)$ equals $+1$ or -1 according as σ has an even or an odd number of inversions. As ε is independent of the choice of the ordering, we see that the parity of the number of inversions of σ is independent of the choice of the ordering on X. Can you prove this directly?

A ***cycle*** is a permutation of the following form

$$i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_r \mapsto i_1, \quad \text{remaining } i\text{'s fixed.}$$

The i_j are required to be distinct. We denote this cycle by $(i_1 i_2 ... i_r)$, and call r its ***length*** — note that r is also its order as an element of S_n. A cycle of length 2 is a transposition. A cycle (i) of length 1 is the identity map. The ***support of the cycle*** $(i_1 \ldots i_r)$ is the set $\{i_1, \ldots, i_r\}$, and cycles are said to be ***disjoint*** if their supports are disjoint. Note that disjoint cycles commute. If

$$\sigma = (i_1 ... i_r)(j_1 ... j_s) \cdots (l_1 ... l_u) \qquad \text{(disjoint cycles)},$$

then

$$\sigma^m = (i_1 ... i_r)^m (j_1 ... j_s)^m \cdots (l_1 ... l_u)^m \qquad \text{(disjoint cycles)},$$

and it follows that σ has order $\text{lcm}(r, s, ..., u)$.

PROPOSITION 4.26 *Every permutation can be written (in essentially one way) as a product of disjoint cycles.*

PROOF. Let $\sigma \in S_n$, and let $O \subset \{1, 2, \ldots, n\}$ be an orbit for $\langle\sigma\rangle$. If $|O| = r$, then for any $i \in O$,

$$O = \{i, \sigma(i), \ldots, \sigma^{r-1}(i)\}.$$

Therefore σ and the cycle $(i\,\sigma(i)\,\ldots\,\sigma^{r-1}(i))$ have the same action on any element of O. Let

$$\{1, 2, \ldots, n\} = \bigcup_{j=1}^{m} O_j$$

be the decomposition of $\{1, \ldots, n\}$ into a disjoint union of orbits for $\langle\sigma\rangle$, and let γ_j be the cycle associated (as above) with O_j. Then

$$\sigma = \gamma_1 \cdots \gamma_m$$

is a decomposition of σ into a product of disjoint cycles. For the uniqueness, note that a decomposition $\sigma = \gamma_1 \cdots \gamma_m$ into a product of disjoint cycles must correspond to a decomposition of $\{1, ..., n\}$ into orbits (ignoring cycles of length 1 and orbits with only one element). We can drop cycles of length one, change the order of the cycles, and change how we write each cycle (by choosing different initial elements), but that's all because the orbits are intrinsically attached to σ. □

For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 4 & 2 & 1 & 3 & 6 & 8 \end{pmatrix} = (15)(27634)(8). \tag{24}$$

It has order $\operatorname{lcm}(2,5) = 10$.

COROLLARY 4.27 *Each permutation σ can be written as a product of transpositions; the number of transpositions in such a product is even or odd according as σ is even or odd.*

PROOF. The cycle

$$(i_1 i_2 ... i_r) = (i_1 i_2) \cdots (i_{r-2} i_{r-1})(i_{r-1} i_r),$$

and so the first statement follows from the proposition. Because sign is a homomorphism, and the signature of a transposition is -1, $\operatorname{sign}(\sigma) = (-1)^{\#\text{transpositions}}$. □

Note that the formula in the proof shows that the signature of a cycle of length r is $(-1)^{r-1}$, that is, an r-cycle is even or odd according as r is odd or even.

It is possible to define a permutation to be even or odd according as it is a product of an even or odd number of transpositions, but then one has to go through an argument as above to show that this is a well-defined notion.

The corollary says that S_n is generated by transpositions. For A_n there is the following result.

COROLLARY 4.28 *The alternating group A_n is generated by cycles of length three.*

PROOF. Any $\sigma \in A_n$ is the product (possibly empty) of an even number of transpositions, $\sigma = t_1 t_1' \cdots t_m t_m'$, but the product of two transpositions can always be written as a product of 3-cycles:

$$(ij)(kl) = \begin{cases} (ij)(jl) = (ijl) & \text{case } j = k, \\ (ij)(jk)(jk)(kl) = (ijk)(jkl) & \text{case } i,j,k,l \text{ distinct,} \\ 1 & \text{case } (ij) = (kl). \end{cases}$$

□

Recall that two elements a and b of a group G are said to be conjugate $a \sim b$ if there exists an element $g \in G$ such that $b = gag^{-1}$, and that conjugacy is an equivalence relation. For a group G, it is useful to determine the conjugacy classes in G.

EXAMPLE 4.29 In S_n, the conjugate of a cycle is given by:

$$g(i_1 \ldots i_k)g^{-1} = (g(i_1) \ldots g(i_k)).$$

Hence $g(i_1 \ldots i_r) \cdots (l_1 \ldots l_u) g^{-1} = (g(i_1) \ldots g(i_r)) \cdots (g(l_1) ... g(l_u))$ (even if the cycles are not disjoint, because conjugation is a homomorphism). In other words, to obtain $g\sigma g^{-1}$, replace each element in each cycle of σ by its image under g.

We shall now determine the conjugacy classes in S_n. By a ***partition*** of n, we mean a sequence of integers $n_1, \ldots, n_k$ such that

$$1 \le n_1 \le n_2 \le \cdots \le n_k \le n \text{ and}$$
$$n_1 + n_2 + \cdots + n_k = n.$$

For example, there are exactly 5 partitions of 4, namely,

$$4=1+1+1+1, \quad 4=1+1+2, \quad 4=1+3, \quad 4=2+2, \quad 4=4,$$

and $1,121,505$ partitions of 61. Note that a partition

$$\{1,2,...,n\}=O_1\cup...\cup O_k \qquad \text{(disjoint union)}$$

of $\{1,2,\ldots,n\}$ determines a partition of n,

$$n=n_1+n_2+...+n_k, \quad n_i=|O_i|,$$

provided the numbering has been chosen so that $|O_i|\leq|O_{i+1}|$. Since the orbits of an element σ of S_n form a partition of $\{1,\ldots,n\}$, we can attach to each such σ a partition of n. For example, the partition of 8 attached to (15)(27634)(8) is $1,2,5$ and the partition attached to n attached to

$$\sigma=(i_1\ldots i_{n_1})\cdots(l_1\ldots l_{n_k}), \quad \text{(disjoint cycles)} \quad 1<n_i\leq n_{i+1},$$

is $1,1,\ldots,1,n_1,\ldots,n_k \qquad (n-\sum n_i$ ones).

PROPOSITION 4.30 *Two elements σ and τ of S_n are conjugate if and only if they define the same partitions of n.*

PROOF. $\Longrightarrow$: We saw in (4.29) that conjugating an element preserves the type of its disjoint cycle decomposition.

$\Longleftarrow$: Since σ and τ define the same partitions of n, their decompositions into products of disjoint cycles have the same type:

$$\sigma=(i_1\ldots i_r)(j_1\ldots j_s)\ldots(l_1\ldots l_u),$$
$$\tau=(i'_1\ldots i'_r)(j'_1\ldots j'_s)\ldots(l'_1\ldots l'_u).$$

If we define g to be

$$\begin{pmatrix} i_1 & \cdots & i_r & j_1 & \cdots & j_s & \cdots & l_1 & \cdots & l_u \\ i'_1 & \cdots & i'_r & j'_1 & \cdots & j'_s & \cdots & l'_1 & \cdots & l'_u \end{pmatrix},$$

then

$$g\sigma g^{-1}=\tau.$$

□

EXAMPLE 4.31 $(ijk)=(\begin{smallmatrix}1234\ldots\\ ijk4\ldots\end{smallmatrix})(123)(\begin{smallmatrix}1234\ldots\\ ijk4\ldots\end{smallmatrix})^{-1}$.

REMARK 4.32 For $1<k\leq n$, there are $\frac{n(n-1)\cdots(n-k+1)}{k}$ distinct k-cycles in S_n. The $\frac{1}{k}$ is needed so that we don't count

$$(i_1i_2\ldots i_k)=(i_ki_1\ldots i_{k-1})=\ldots$$

k times. Similarly, it is possible to compute the number of elements in any conjugacy class in S_n, but a little care is needed when the partition of n has several terms equal. For example, the number of permutations in S_4 of type $(ab)(cd)$ is

$$\frac{1}{2}\left(\frac{4\times 3}{2}\times\frac{2\times 1}{2}\right)=3.$$

The $\frac{1}{2}$ is needed so that we don't count $(ab)(cd) = (cd)(ab)$ twice. For S_4 we have the following table:

Partition	Element	No. in Conj. Class	Parity
$1+1+1+1$	1	1	even
$1+1+2$	(ab)	6	odd
$1+3$	(abc)	8	even
$2+2$	$(ab)(cd)$	3	even
4	$(abcd)$	6	odd

Note that A_4 contains exactly 3 elements of order 2, namely those of type $2+2$, and that together with 1 they form a subgroup V. This group is a union of conjugacy classes, and is therefore a normal subgroup of S_4.

THEOREM 4.33 (GALOIS) *The group A_n is simple if $n \geq 5$*

REMARK 4.34 For $n = 2$, A_n is trivial, and for $n = 3$, A_n is cyclic of order 3, and hence simple; for $n = 4$ it is nonabelian and nonsimple — it contains the normal, even characteristic, subgroup V (see 4.32).

LEMMA 4.35 *Let N be a normal subgroup of A_n $(n \geq 5)$; if N contains a cycle of length three, then it contains all cycles of length three, and so equals A_n (by 4.28).*

PROOF. Let γ be the cycle of length three in N, and let σ be a second cycle of length three in A_n. We know from (4.30) that $\sigma = g\gamma g^{-1}$ for some $g \in S_n$. If $g \in A_n$, then this shows that σ is also in N. If not, because $n \geq 5$, there exists a transposition $t \in S_n$ disjoint from σ. Then $tg \in A_n$ and

$$\sigma = t\sigma t^{-1} = tg\gamma g^{-1}t^{-1},$$

and so again $\sigma \in N$. □

The next lemma completes the proof of the Theorem.

LEMMA 4.36 *Every normal subgroup N of A_n, $n \geq 5$, $N \neq 1$, contains a cycle of length 3.*

PROOF. Let $\sigma \in N$, $\sigma \neq 1$. If σ is not a 3-cycle, we shall construct another element $\sigma' \in N$, $\sigma' \neq 1$, which fixes more elements of $\{1, 2, \ldots, n\}$ than does σ. If σ' is not a 3-cycle, then we can apply the same construction. After a finite number of steps, we arrive at a 3-cycle.

Suppose σ is not a 3-cycle. When we express it as a product of disjoint cycles, either it contains a cycle of length ≥ 3 or else it is a product of transpositions, say

(i) $\sigma = (i_1 i_2 i_3 \ldots) \cdots$ or
(ii) $\sigma = (i_1 i_2)(i_3 i_4) \cdots$.

In the first case, σ moves two numbers, say i_4, i_5, other than i_1, i_2, i_3, because $\sigma \neq (i_1 i_2 i_3)$, $(i_1 \ldots i_4)$. Let $\gamma = (i_3 i_4 i_5)$. Then $\sigma_1 \overset{\text{def}}{=} \gamma\sigma\gamma^{-1} = (i_1 i_2 i_4 \ldots) \cdots \in N$, and is distinct from σ (because it acts differently on i_2). Thus $\sigma' \overset{\text{def}}{=} \sigma_1\sigma^{-1} \neq 1$, but $\sigma' = \gamma\sigma\gamma^{-1}\sigma^{-1}$ fixes i_2 and all elements other than $i_1, \ldots, i_5$ fixed by σ — it therefore fixes more elements than σ.

In the second case, form γ, σ_1, σ' as in the first case with i_4 as in (ii) and i_5 any element distinct from i_1, i_2, i_3, i_4. Then $\sigma_1 = (i_1 i_2)(i_4 i_5) \cdots$ is distinct from σ because it acts differently on i_4. Thus $\sigma' = \sigma_1\sigma^{-1} \neq 1$, but σ' fixes i_1 and i_2, and all elements $\neq i_1, \ldots, i_5$ not fixed by σ — it therefore fixes at least one more element than σ. □

COROLLARY 4.37 *For $n \geq 5$, the only normal subgroups of S_n are 1, A_n, and S_n.*

PROOF. If N is normal in S_n, then $N \cap A_n$ is normal in A_n. Therefore either $N \cap A_n = A_n$ or $N \cap A_n = \{1\}$. In the first case, $N \supset A_n$, which has index 2 in S_n, and so $N = A_n$ or S_n. In the second case, the map $x \mapsto xA_n : N \to S_n/A_n$ is injective, and so N has order 1 or 2, but it can't have order 2 because no conjugacy class in S_n (other than $\{1\}$) consists of a single element. □

ASIDE 4.38 There exists a description of the conjugacy classes in A_n, from which it is possible to deduce its simplicity for $n \geq 5$ (see Exercise 4-12).

ASIDE 4.39 A group G is said to be solvable if there exist subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_{i-1} \supset G_i \supset \cdots \supset G_r = \{1\}$$

such that each G_i is normal in G_{i-1} and each quotient G_{i-1}/G_i is commutative. Thus A_n (also S_n) is not solvable if $n \geq 5$. Let $f(X) \in \mathbb{Q}[X]$ be of degree n.

In Galois theory, one attaches to f a subgroup G_f of the group of permutations of the roots of f, and shows that the roots of f can be obtained from the coefficients of f by the algebraic operations of addition, subtraction, multiplication, division, and the extraction of mth roots if and only if G_f is solvable (Galois's theorem). For every n, there exist lots of polynomials f of degree n with $G_f \approx S_n$, and hence (when $n \geq 5$) lots of polynomials not solvable in radicals.

The Todd-Coxeter algorithm.

Let G be a group described by a finite presentation, and let H be a subgroup described by a generating set. Then the Todd-Coxeter algorithm[2] is a strategy for writing down the set of left cosets of H in G together with the action of G on the set. I illustrate it with an example (from Artin 1991, 6.9, which provides more details, but note that he composes permutations in the reverse direction from us).

Let $G = \langle a, b, c \mid a^3, b^2, c^2, cba \rangle$ and let H be the subgroup generated by c (strictly speaking, H is the subgroup generated by the element of G represented by the reduced word c). The operation of G on the set of cosets is described by the action of the generators, which must satisfy the following rules:

(i) Each generator (a, b, c in our example) acts as a permutation.
(ii) The relations (a^3, b^2, c^2, cba in our example) act trivially.
(iii) The generators of H (c in our example) fix the coset $1H$.
(iv) The operation on the cosets is transitive.

The strategy is to introduce cosets, denoted $1, 2, \ldots$ with $1 = 1H$, as necessary.

Rule (iii) tells us simply that $c1 = 1$. We now apply the first two rules. Since we don't know what $a1$ is, let's denote it 2: $a1 = 2$. Similarly, let $a2 = 3$. Now $a3 = a^3 1$, which according to (ii) must be 1. Thus, we have introduced three (potential) cosets 1, 2, 3, permuted by a as follows:

$$1 \overset{a}{\mapsto} 2 \overset{a}{\mapsto} 3 \overset{a}{\mapsto} 1.$$

[2] To solve a problem, an algorithm must always terminate in a finite time with the correct answer to the problem. The Todd-Coxeter algorithm does not solve the problem of determining whether a finite presentation defines a finite group (in fact, there is no such algorithm). It does, however, solve the problem of determining the order of a finite group from a finite presentation of the group (use the algorithm with H the trivial subgroup 1.)

What is $b1$? We don't know, and so it is prudent to introduce another coset $4 = b1$. Now $b4 = 1$ because $b^2 = 1$, and so we have

$$1 \overset{b}{\mapsto} 4 \overset{b}{\mapsto} 1.$$

We still have the relation cba. We know $a1 = 2$, but we don't know what $b2$ is, and so we set $b2 = 5$:

$$1 \overset{a}{\mapsto} 2 \overset{b}{\mapsto} 5.$$

By (iii) $c1 = 1$, and by (ii) applied to cba we have $c5 = 1$. Therefore, according to (i) we must have $5 = 1$; we drop 5, and so now $b2 = 1$. Since $b4 = 1$ we must have $4 = 2$, and so we can drop 4 also. What we know can be summarized by the table:

	a	a	a	b	b	c	c	a	b	c
1	2	3	**1**	2	**1**	1	**1**	2	1	**1**
2	3	1	**2**	1	**2**		**2**	3		**2**
3	1	2	**3**		**3**		**3**	1	2	**3**

The bottom right corner, which is forced by (ii), tells us that $c2 = 3$. Hence also $c3 = 2$, and this then determines the rest of the table:

	a	a	a	b	b	c	c	a	b	c
1	2	3	**1**	2	**1**	1	**1**	2	1	**1**
2	3	1	**2**	1	**2**	3	**2**	3	3	**2**
3	1	2	**3**	3	**3**	2	**3**	1	2	**3**

We find that we have three cosets on which a, b, c act as

$$a = (123) \quad b = (12) \quad c = (23).$$

More precisely, we have written down a map $G \to S_3$ that is consistent with the above rules. A theorem (Artin 1991, 9.10) now says that this does in fact describe the action of G on G/H. Since the three elements (123), (12), and (23) generate S_3, this shows that the action of G on G/H induces an isomorphism $G \to S_3$, and that H is a subgroup of order 2.

In Artin 1991, 6.9, it is explained how to make this procedure into an algorithm which, when it succeeds in producing a consistent table, will in fact produce the correct table.

This algorithm is implemented in GAP.

Primitive actions.

Let G be a group acting on a set X, and let π be a partition of X. We say that π is ***stabilized*** by G if

$$A \in \pi \implies gA \in \pi.$$

It suffices to check the condition for a set of generators for G.

EXAMPLE 4.40 (a) The subgroup $G = \langle(1234)\rangle$ of S_4 stabilizes the partition $\{\{1,3\},\{2,4\}\}$ of $\{1,2,3,4\}$.

(b) Identify $X = \{1,2,3,4\}$ with the set of vertices of the square on which D_4 acts in the usual way, namely, with $r = (1234)$, $s = (2,4)$. Then D_4 stabilizes the partition $\{\{1,3\},\{2,4\}\}$ (opposite vertices stay opposite).

(c) Let X be the set of partitions of $\{1,2,3,4\}$ into two sets, each with two elements. Then S_4 acts on X, and $\mathrm{Ker}(S_4 \to \mathrm{Sym}(X))$ is the subgroup V defined in (4.32).

The group G always stabilizes the trivial partitions of X, namely, the set of all one-element subsets of X, and $\{X\}$. When it stabilizes only those partitions, we say that the action is ***primitive***; otherwise it is ***imprimitive***. A subgroup of $\mathrm{Sym}(X)$ (e.g., of S_n) is said to be ***primitive*** if it acts primitively on X. Obviously, S_n itself is primitive, but Example 4.40b shows that D_4, regarded as a subgroup of S_4 in the obvious way, is not primitive.

EXAMPLE 4.41 A doubly transitive action is primitive: if it stabilized

$$\{\{x, x', \ldots\}, \{y, \ldots\} \ldots\},$$

then there would be no element sending (x, x') to (x, y).

REMARK 4.42 The G-orbits form a partition of X that is stabilized by G. If the action is primitive, then the partition into orbits must be one of the trivial ones. Hence

$$\text{action primitive} \implies \text{action transitive or trivial.}$$

For the remainder of this section, G is a finite group acting transitively on a set X with at least two elements.

PROPOSITION 4.43 *The group G acts imprimitively if and only if there is a proper subset A of X with at least 2 elements such that,*

$$\text{for each } g \in G, \text{ either } gA = A \text{ or } gA \cap A = \emptyset. \tag{25}$$

PROOF. $\Longrightarrow$: The partition π stabilized by G contains such an A.

$\Longleftarrow$: From such an A, we can form a partition $\{A, g_1A, g_2A, \ldots\}$ of X, which is stabilized by G. □

A subset A of X satisfying (25) is called ***block***.

PROPOSITION 4.44 *Let A be a block in X with $|A| \geq 2$ and $A \neq X$. For any $x \in A$,*

$$\mathrm{Stab}(x) \subsetneqq \mathrm{Stab}(A) \subsetneqq G.$$

PROOF. We have $\mathrm{Stab}(A) \supset \mathrm{Stab}(x)$ because

$$gx = x \implies gA \cap A \neq \emptyset \implies gA = A.$$

Let $y \in A$, $y \neq x$. Because G acts transitively on X, there is a $g \in G$ such that $gx = y$. Then $g \in \mathrm{Stab}(A)$, but $g \notin \mathrm{Stab}(x)$.

Let $y \notin A$. There is a $g \in G$ such that $gx = y$, and then $g \notin \mathrm{Stab}(A)$. □

THEOREM 4.45 *The group G acts primitively on X if and only if, for one (hence all) x in X, $\mathrm{Stab}(x)$ is a maximal subgroup of G.*

PROOF. If G does not act primitively on X, then (see 4.43) there is a block $A \subsetneqq X$ with at least two elements, and so (4.44) shows that $\mathrm{Stab}(x)$ will not be maximal for any $x \in A$.

Conversely, suppose that there exists an x in X and a subgroup H such that

$$\mathrm{Stab}(x) \subsetneqq H \subsetneqq G.$$

Then I claim that $A = Hx$ is a block $\neq X$ with at least two elements.

Because $H \neq \mathrm{Stab}(x)$, $Hx \neq \{x\}$, and so $\{x\} \subsetneqq A \subsetneqq X$.

If $g \in H$, then $gA = A$. If $g \notin H$, then gA is disjoint from A: for suppose $ghx = h'x$ some $h' \in H$; then $h'^{-1}gh \in \mathrm{Stab}(x) \subset H$, say $h'^{-1}gh = h''$, and $g = h'h''h^{-1} \in H$. □

Exercises

4-1 Let H_1 and H_2 be subgroups of a group G. Show that the maps of G-sets $G/H_1 \to G/H_2$ are in natural one-to-one correspondence with the elements gH_2 of G/H_2 such that $H_1 \subset gH_2g^{-1}$.

4-2 (a) Show that a finite group G can't be equal to the union of the conjugates of a proper subgroup H.

(b) Show that (a) holds for an infinite group G provided that $(G{:}H)$ is finite.

(c) Give an example to show that (a) fails in general for infinite groups.

(d) Give an example of a proper subset S of a finite group G such that $G = \bigcup_{g \in G} gSg^{-1}$.

4-3 Show that any set of representatives for the conjugacy classes in a finite group generates the group.

4-4 Prove that any noncommutative group of order p^3, p an odd prime, is isomorphic to one of the two groups constructed in (3.14, 3.15).

4-5 Let p be the smallest prime dividing $(G : 1)$ (assumed finite). Show that any subgroup of G of index p is normal.

4-6 Show that a group of order $2m$, m odd, contains a subgroup of index 2. (Hint: Use Cayley's theorem 1.22)

4-7 For $n \geq 5$, show that the k-cycles in S_n generate S_n or A_n according as k is even or odd.

4-8 Let $G = \mathrm{GL}_3(\mathbb{F}_2)$.

(a) Show that $(G : 1) = 168$.

(b) Let X be the set of lines through the origin in $\mathbb{F}_2^3$; show that X has 7 elements, and that there is a natural injective homomorphism $G \hookrightarrow \mathrm{Sym}(X) = S_7$.

(c) Use Jordan canonical forms to show that G has six conjugacy classes, with 1, 21, 42, 56, 24, and 24 elements respectively. [Note that if M is a free $\mathbb{F}_2[\alpha]$-module of rank one, then $\mathrm{End}_{\mathbb{F}_2[\alpha]}(M) = \mathbb{F}_2[\alpha]$.]

(d) Deduce that G is simple.

4-9 Let G be a group. If $\mathrm{Aut}(G)$ is cyclic, prove that G is commutative; if further, G is finite, prove that G is cyclic.

4-10 Show that S_n is generated by $(1\,2), (1\,3), \ldots, (1\,n)$; also by $(1\,2), (2\,3), \ldots, (n-1\,n)$.

4-11 Let K be a conjugacy class of a finite group G contained in a normal subgroup H of G. Prove that K is a union of k conjugacy classes of equal size in H, where $k = (G : H \cdot C_G(x))$ for any $x \in K$.

4-12 (a) Let $\sigma \in A_n$. From Exercise 4-11 we know that the conjugacy class of σ in S_n either remains a single conjugacy class in A_n or breaks up as a union of two classes of equal size. Show that the second case occurs $\iff$ σ does not commute with an odd permutation $\iff$ the partition of n defined by σ consists of distinct odd integers.
(b) For each conjugacy class K in A_7, give a member of K, and determine $|K|$.

4-13 Let G be the group with generators a, b and relations $a^4 = 1 = b^2$, $aba = bab$.

(a) Use the Todd-Coxeter algorithm (with $H = 1$) to find the image of G under the homomorphism $G \to S_n$, $n = (G:1)$, given by Cayley's Theorem 1.11. [No need to include every step; just an outline will do.]
(b) Use Sage/GAP to check your answer.

4-14 Show that if the action of G on X is primitive and effective, then the action of any normal subgroup $H \neq 1$ of G is transitive.

4-15 (a) Check that A_4 has 8 elements of order 3, and 3 elements of order 2. Hence it has no element of order 6.
(b) Prove that A_4 has no subgroup of order 6 (cf. 1.30). (Use 4.23.)
(c) Prove that A_4 is the only subgroup of S_4 of order 12.

4-16 Let G be a group with a subgroup of index r. Prove:

(a) If G is simple, then $(G:1)$ divides $r!$.
(b) If $r = 2, 3,$ or 4, then G can't be simple (except for te trivial cases C_2, C_3).
(c) There exists a nonabelian simple group with a subgroup of index 5.

4-17 Prove that S_n is isomorphic to a subgroup of A_{n+2}.

4-18 Let H and K be subgroups of a group G. A ***double coset*** of H and K in G is a set of the form
$$HaK = \{hak \mid h \in H, k \in K\}$$
for some $a \in G$.

(a) Show that the double cosets of H and K in G partition G.
(b) Let $H \cap aKa^{-1}$ act on $H \times K$ by $b(h,k) = (hb, a^{-1}b^{-1}ak)$. Show that the orbits for this action are exactly the fibres of the map $(h,k) \mapsto hak\colon H \times K \to HaK$.
(c) (Double coset counting formula). Use (b) to show that
$$|HaK| = \frac{|H||K|}{|H \cap aKa^{-1}|}.$$

4-19 The normal subgroups N of a group G are those with the following property: for every set X on which G acts transitively, N fixes one x in X if and only if N fixes every x in X.

4-20 (This exercise assumes a knowledge of categories.) Let G be a group, and let F be the functor sending a G-set to its underlying set. We can regard G as a G-set, and so an automorphism a of F defines an automorphism a_G of G (as a set). Show that the map $a \mapsto a_G(1)\colon \mathrm{Aut}(F) \to G$ is an isomorphism of groups (cf. sx66588).

CHAPTER 5

The Sylow Theorems; Applications

> *As an undergraduate, I learned the Sylow theorems in my algebra classes but could never retain either the statement or proof of these theorems in memory except for short periods of time… I think the problem was that I was exposed to these theorems long before I had internalised the concept of a group action. But once one has the mindset to approach a mathematical object through the various natural group actions on that object, and then look at the various dynamical features of that action (orbits, stabilisers, quotients, etc.) then the Sylow theorems (and Cauchy's theorem, Lagrange's theorem, etc.) all boil down to observing an action on some natural space (e.g. the conjugacy action on the group, or on tuples of elements on that group) and counting orbits and stabilisers.*
>
> Terry Tao mo130883.

In this chapter, all groups are finite.

Let G be a group and let p be a prime dividing $(G\colon 1)$. A subgroup of G is called a ***Sylow*** ***p-subgroup of*** G if its order is the highest power of p dividing $(G:1)$. In other words, H is a Sylow p-subgroup of G if it is a p-group and its index in G is prime to p.

The Sylow theorems state that there exist Sylow p-subgroups for all primes p dividing $(G\colon 1)$, that the Sylow p-subgroups for a fixed p are conjugate, and that every p-subgroup of G is contained in such a subgroup; moreover, the theorems restrict the possible number of Sylow p-subgroups in G.

The Sylow theorems

In the proofs, we frequently use that if O is an orbit for a group H acting on a set X, and $x_0 \in O$, then the map $H \to X$, $h \mapsto hx_0$ induces a bijection

$$H/\operatorname{Stab}(x_0) \to O;$$

see (4.7). Therefore

$$(H : \operatorname{Stab}(x_0)) = |O|.$$

In particular, when H is a p-group, $|O|$ is a power of p, and so either O consists of a single element, or $|O|$ is divisible by p. Since X is a disjoint union of the orbits, we can conclude:

LEMMA 5.1 *Let H be a p-group acting on a finite set X, and let X^H be the set of points fixed by H; then*

$$|X| \equiv |X^H| \quad (mod\ p).$$

When the lemma is applied to a p-group H acting on itself by conjugation, we find that

$$(Z(H):1) \equiv (H:1) \mod p$$

and so $p|(Z(H)\colon 1)$ (cf. the proof of 4.16).

THEOREM 5.2 (SYLOW I) *Let G be a finite group, and let p be prime. If $p^r|(G:1)$, then G has a subgroup of order p^r.*

PROOF. According to (4.17), it suffices to prove this with p^r the highest power of p dividing $(G:1)$, and so from now on we assume that $(G:1) = p^r m$ with m not divisible by p. Let

$$X = \{\text{sub}\mathit{sets} \text{ of } G \text{ with } p^r \text{ elements}\},$$

with the action of G defined by

$$G \times X \to X, \quad (g, A) \mapsto gA \overset{\text{def}}{=} \{ga \mid a \in A\}.$$

Let $A \in X$, and let

$$H = \mathrm{Stab}(A) \overset{\text{def}}{=} \{g \in G \mid gA = A\}.$$

For any $a_0 \in A$, $h \mapsto ha_0\colon H \to A$ is injective (cancellation law), and so $(H:1) \leq |A| = p^r$. In the equation

$$(G:1) = (G:H)(H:1)$$

we know that $(G:1) = p^r m$, $(H:1) \leq p^r$, and that $(G:H)$ is the number of elements in the orbit of A. If we can find an A such that p doesn't divide the number of elements in its orbit, then we can conclude that (for such an A), $H = \mathrm{Stab}\, A$ has order p^r.

The number of elements in X is

$$|X| = \binom{p^r m}{p^r} = \frac{(p^r m)(p^r m - 1)\cdots(p^r m - i)\cdots(p^r m - p^r + 1)}{p^r(p^r - 1)\cdots(p^r - i)\cdots(p^r - p^r + 1)}.$$

Note that, because $i < p^r$, the power of p dividing $p^r m - i$ is the power of p dividing i. The same is true for $p^r - i$. Therefore the corresponding terms on top and bottom are divisible by the same powers of p, and so p does not divide $|X|$. Because the orbits form a partition of X,

$$|X| = \sum |O_i|, \quad O_i \text{ the distinct orbits},$$

and so at least one of the $|O_i|$ is not divisible by p. □

EXAMPLE 5.3 Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field with p elements, and let $G = \mathrm{GL}_n(\mathbb{F}_p)$. The $n \times n$ matrices in G are precisely those whose columns form a basis for $\mathbb{F}_p^n$. Thus, the first column can be any nonzero vector in $\mathbb{F}_p^n$, of which there are $p^n - 1$; the second column can be any vector not in the span of the first column, of which there are $p^n - p$; and so on. Therefore, the order of G is

$$(p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1}),$$

and so the power of p dividing $(G:1)$ is $p^{1+2+\cdots+(n-1)}$. Consider the upper triangular matrices with 1's down the diagonal:

$$\begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

They form a subgroup U of order $p^{n-1}p^{n-2}\cdots p$, which is therefore a Sylow p-subgroup G.

REMARK 5.4 The theorem gives another proof of Cauchy's theorem (4.13). If a prime p divides $(G{:}1)$, then G will have a subgroup H of order p, and any $g \in H$, $g \neq 1$, is an element of G of order p.

REMARK 5.5 The proof of Theorem 5.2 can be modified to show directly that for each power p^r of p dividing $(G:1)$ there is a subgroup H of G of order p^r. One again writes $(G:1) = p^r m$ and considers the set X of all subsets of order p^r. In this case, the highest power p^{r_0} of p dividing $|X|$ is the highest power of p dividing m, and it follows that there is an orbit in X whose order is not divisible by p^{r_0+1}. For an A in such an orbit, the same counting argument shows that Stab(A) has p^r elements. We recommend that the reader write out the details.

THEOREM 5.6 (SYLOW II) *Let G be a finite group, and let $|G| = p^r m$ with m not divisible by p.*

(a) Any two Sylow p-subgroups are conjugate.
(b) Let s_p be the number of Sylow p-subgroups in G; then $s_p \equiv 1 \bmod p$ and $s_p | m$.
(c) Every p-subgroup of G is contained in a Sylow p-subgroup.

Let H be a subgroup of G. Recall (4.6, 4.8) that the normalizer of H in G is

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\},$$

and that the number of conjugates of H in G is $(G : N_G(H))$.

LEMMA 5.7 *Let P be a Sylow p-subgroup of G, and let H be a p-subgroup. If H normalizes P, i.e., if $H \subset N_G(P)$, then $H \subset P$. In particular, no Sylow p-subgroup of G other than P normalizes P.*

PROOF. Because H and P are subgroups of $N_G(P)$ with P normal in $N_G(P)$, HP is a subgroup, and $H/H \cap P \simeq HP/P$ (apply 1.46). Therefore $(HP : P)$ is a power of p (here is where we use that H is a p-group), but

$$(HP:1) = (HP:P)(P:1),$$

and $(P:1)$ is the largest power of p dividing $(G:1)$, hence also the largest power of p dividing $(HP:1)$. Thus $(HP:P) = p^0 = 1$, and $H \subset P$. □

PROOF (OF SYLOW II) (a) Let X be the set of Sylow p-subgroups in G, and let G act on X by conjugation,

$$(g,P)\mapsto gPg^{-1}\colon G\times X\to X.$$

Let O be one of the G-orbits: we have to show O is all of X.

Let $P\in O$, and let P act on O through the action of G. This single G-orbit may break up into several P-orbits, one of which will be $\{P\}$. In fact this is the only one-point orbit because

$$\{Q\}\text{ is a }P\text{-orbit}\iff P\text{ normalizes }Q,$$

which we know (5.7) happens only for $Q=P$. Hence the number of elements in every P-orbit other than $\{P\}$ is divisible by p, and we have that $|O|\equiv 1\bmod p$.

Suppose there exists a $P\notin O$. We again let P act on O, but this time the argument shows that there are no one-point orbits, and so the number of elements in every P-orbit is divisible by p. This implies that $\#O$ is divisible by p, which contradicts what we proved in the last paragraph. There can be no such P, and so O is all of X.

(b) Since s_p is now the number of elements in O, we have also shown that $s_p\equiv 1$ (mod p).

Let P be a Sylow p-subgroup of G. According to (a), s_p is the number of conjugates of P, which equals

$$(G:N_G(P))=\frac{(G:1)}{(N_G(P):1)}=\frac{(G:1)}{(N_G(P):P)\cdot(P:1)}=\frac{m}{(N_G(P):P)}.$$

This is a factor of m.

(c) Let H be a p-subgroup of G, and let H act on the set X of Sylow p-subgroups by conjugation. Because $|X|=s_p$ is not divisible by p, X^H must be nonempty (Lemma 5.1), i.e., at least one H-orbit consists of a single Sylow p-subgroup. But then H normalizes P and Lemma 5.7 implies that $H\subset P$. □

COROLLARY 5.8 *A Sylow p-subgroup is normal if and only if it is the only Sylow p-subgroup.*

PROOF. Let P be a Sylow p-subgroup of G. If P is normal, then (a) of Sylow II implies that it is the only Sylow p-subgroup. The converse statement follows from (3.7c) (which shows, in fact, that P is even characteristic). □

COROLLARY 5.9 *Suppose that a group G has only one Sylow p-subgroup for each prime p dividing its order. Then G is a direct product of its Sylow p-subgroups.*

PROOF. Let $P_1,\ldots,P_k$ be Sylow subgroups of G, and let $|P_i|=p_i^{r_i}$; the p_i are distinct primes. Because each P_i is normal in G, the product $P_1\cdots P_k$ is a normal subgroup of G. We shall prove by induction on k that it has order $p_1^{r_1}\cdots p_k^{r_k}$. If $k=1$, there is nothing to prove, and so we may suppose that $k\geq 2$ and that $P_1\cdots P_{k-1}$ has order $p_1^{r_1}\cdots p_{k-1}^{r_{k-1}}$. Then $P_1\cdots P_{k-1}\cap P_k=1$; therefore (1.51) shows that $(P_1\cdots P_{k-1})P_k$ is the direct product of $P_1\cdots P_{k-1}$ and P_k, and so has order $p_1^{r_1}\cdots p_k^{r_k}$. Now (1.52) applied to the full set of Sylow subgroups of G shows that G is their direct product. □

EXAMPLE 5.10 Let $G = \mathrm{GL}(V)$, where V is a vector space of dimension n over $\mathbb{F}_p$. There is a geometric description of the Sylow subgroups of G. A ***maximal flag*** F in V is a sequence of subspaces

$$V = V_n \supset V_{n-1} \supset \cdots \supset V_i \supset \cdots \supset V_1 \supset \{0\}$$

with $\dim V_i = i$. Given such a flag F, let $U(F)$ be the set of linear maps $\alpha: V \to V$ such that

(a) $\alpha(V_i) \subset V_i$ for all i, and
(b) the endomorphism of V_i / V_{i-1} induced by α is the identity map.

I claim that $U(F)$ is a Sylow p-subgroup of G. Indeed, we can construct a basis $\{e_1, \ldots, e_n\}$ for V such $\{e_1\}$ is basis for V_1, $\{e_1, e_2\}$ is a basis for V_2, and so on. Relative to this basis, the matrices of the elements of $U(F)$ are exactly the elements of the group U of (5.3).

Let $g \in \mathrm{GL}_n(\mathbb{F})$. Then $gF \overset{\mathrm{def}}{=} \{gV_n, gV_{n-1}, \ldots\}$ is again a maximal flag, and $U(gF) = g \cdot U(F) \cdot g^{-1}$. From (a) of Sylow II, we see that the Sylow p-subgroups of G are precisely the groups of the form $U(F)$ for some maximal flag F.

EXAMPLE 5.11 The group S_4 has order $24 = 2^3 \cdot 3$. When we visualize it through its action on a tetrahedron, the Sylow 3-subgroups are the stabilizers of faces. They are conjugate because S_4 obviously acts transitively on the faces. The Sylow 2-subgroups are the stabilizers of pairs of opposite edges. For pictures, see the blog of Daniel Litt, Jan 1, 2021.

Some books use different numberings for Sylow's theorems. I have essentially followed the original (Sylow 1872).

Alternative approach to the Sylow theorems

We briefly forget that we have proved the Sylow theorems.

THEOREM 5.12 *Let G be a group, and let P be a Sylow p-subgroup of G. For any subgroup H of G, there exists an $a \in G$ such that $H \cap aPa^{-1}$ is a Sylow p-subgroup of H.*

PROOF. Recall (Exercise 4-18) that G is a disjoint union of the double cosets for H and P, and so

$$|G| = \sum\nolimits_a |HaP| = \sum\nolimits_a \frac{|H||P|}{|H \cap aPa^{-1}|},$$

where the sum is over a set of representatives for the double cosets. On dividing by $|P|$ we find that

$$\frac{|G|}{|P|} = \sum\nolimits_a \frac{|H|}{|H \cap aPa^{-1}|},$$

and so there exists an a such that $(H : H \cap aPa^{-1})$ is not divisible by p. For such an a, $H \cap aPa^{-1}$ is a Sylow p-subgroup of H. □

PROOF (OF SYLOW I) According to Cayley's theorem (1.22), G embeds into S_n, and S_n embeds into $\mathrm{GL}_n(\mathbb{F}_p)$ (see 7.1b below). As $\mathrm{GL}_n(\mathbb{F}_p)$ has a Sylow p-subgroup (see 5.3), so also does G. □

PROOF (OF SYLOW II(a,c)) Let P be a Sylow p-subgroup of G, and let P' be a p-subgroup of G. Then P' is the unique Sylow p-subgroup of P', and so the theorem with $H = P'$ shows that $aPa^{-1} \supset P'$ for some a. This implies (a) and (c) of Sylow II. □

Examples

We apply what we have learnt to obtain information about groups of various orders.

5.13 (GROUPS OF ORDER 99) Let G have order 99. The Sylow theorems imply that G has at least one subgroup H of order 11, and in fact $s_{11} \,\big|\, \frac{99}{11}$ and $s_{11} \equiv 1 \mod 11$. It follows that $s_{11} = 1$, and H is normal. Similarly, $s_9|11$ and $s_9 \equiv 1 \mod 3$, and so the Sylow 3-subgroup is also normal. Hence G is isomorphic to the direct product of its Sylow subgroups (5.9), which are both commutative (4.18), and so G commutative.

Here is an alternative proof. Verify as before that the Sylow 11-subgroup N of G is normal. The Sylow 3-subgroup Q maps bijectively onto G/N, and so $G = N \rtimes Q$. It remains to determine the action by conjugation of Q on N. But $\mathrm{Aut}(N)$ is cyclic of order 10 (see 3.5), and so there is only the trivial homomorphism $Q \to \mathrm{Aut}(N)$. It follows that G is the direct product of N and Q.

5.14 (GROUPS OF ORDER pq, p,q PRIMES, $p < q$) Let G be such a group, and let P and Q be Sylow p and q subgroups. Then $(G:Q) = p$, which is the smallest prime dividing $(G:1)$, and so (see Exercise 4-5) Q is normal. Because P maps bijectively onto G/Q, we have that

$$G = Q \rtimes P,$$

and it remains to determine the action of P on Q by conjugation.

The group $\mathrm{Aut}(Q)$ is cyclic of order $q-1$ (see 3.5), and so, unless $p|q-1$, $G = Q \times P$.

If $p|q-1$, then $\mathrm{Aut}(Q)$ (being cyclic) has a unique subgroup P' of order p. In fact P' consists of the maps

$$x \mapsto x^i, \quad \{i \in \mathbb{Z}/q\mathbb{Z} \mid i^p = 1\}.$$

Let a and b be generators for P and Q respectively, and suppose that the action of a on Q by conjugation is $x \mapsto x^{i_0}$, $i_0 \neq 1$ (in $\mathbb{Z}/q\mathbb{Z}$). Then G has generators a,b and relations

$$a^p, \quad b^q, \quad aba^{-1} = b^{i_0}.$$

Choosing a different i_0 amounts to choosing a different generator a for P, and so gives an isomorphic group G.

In summary: if $p \nmid q-1$, then the only group of order pq is the cyclic group C_{pq}; if $p|q-1$, then there is also a nonabelian group given by the above generators and relations.

5.15 (GROUPS OF ORDER 30) Let G be a group of order 30. Then

$$s_3 = 1,4,7,10,\ldots \text{ and divides } 10;$$
$$s_5 = 1,6,11,\ldots \text{ and divides } 6.$$

Hence $s_3 = 1$ or 10, and $s_5 = 1$ or 6. In fact, at least one is 1, for otherwise there would be 20 elements of order 3 and 24 elements of order 5, which is impossible. Therefore, a Sylow 3-subgroup P or a Sylow 5-subgroup Q is normal, and so $H = PQ$ is a subgroup of G. Because 3 doesn't divide $5-1=4$, (5.14) shows that H is commutative, $H \approx C_3 \times C_5$. Hence

$$G = (C_3 \times C_5) \rtimes_\theta C_2,$$

and it remains to determine the possible homomorphisms $\theta\colon C_2 \to \mathrm{Aut}(C_3 \times C_5)$. But such a homomorphism θ is determined by the image of the nonidentity element of C_2, which must be an element of order 2. Let a, b, c generate C_3, C_5, C_2. Then

$$\mathrm{Aut}(C_3 \times C_5) = \mathrm{Aut}(C_3) \times \mathrm{Aut}(C_5),$$

and the only elements of $\mathrm{Aut}\, C_3$ and $\mathrm{Aut}\, C_5$ of order 2 are $a \mapsto a^{-1}$ and $b \mapsto b^{-1}$. Thus there are exactly 4 homomorphisms θ, and $\theta(c)$ is one of the following elements:

$$\begin{cases} a \mapsto a \\ b \mapsto b \end{cases} \quad \begin{cases} a \mapsto a \\ b \mapsto b^{-1} \end{cases} \quad \begin{cases} a \mapsto a^{-1} \\ b \mapsto b \end{cases} \quad \begin{cases} a \mapsto a^{-1} \\ b \mapsto b^{-1} \end{cases}.$$

The groups corresponding to these homomorphisms have centres of order 30, 3 (generated by a), 5 (generated by b), and 1 respectively, and hence are nonisomorphic. We have shown that (up to isomorphism) there are exactly 4 groups of order 30. For example, the third on our list has generators a, b, c and relations

$$a^3, \quad b^5, \quad c^2, \quad ab = ba, \quad cac^{-1} = a^{-1}, \quad cbc^{-1} = b.$$

5.16 (Groups of order 12) Let G be a group of order 12, and let P be its Sylow 3-subgroup. If P is not normal, then P doesn't contain a nontrivial normal subgroup of G, and so the map (4.2, action on the left cosets)

$$\varphi : G \to \mathrm{Sym}(G/P) \approx S_4$$

is injective, and its image is a subgroup of S_4 of order 12. From Sylow II we see that G has exactly 4 Sylow 3-subgroups, and hence it has exactly 8 elements of order 3. But all elements of S_4 of order 3 are in A_4 (see the table in 4.32), and so $\varphi(G)$ intersects A_4 in a subgroup with at least 8 elements. By Lagrange's theorem $\varphi(G) = A_4$, and so $G \approx A_4$.

Now assume that P is normal. Then $G = P \rtimes Q$, where Q is the Sylow 4-subgroup. If Q is cyclic of order 4, then there is a unique nontrivial map $Q (= C_4) \to \mathrm{Aut}(P) (= C_2)$, and hence we obtain a single noncommutative group $C_3 \rtimes C_4$. If $Q = C_2 \times C_2$, there are exactly 3 nontrivial homomorphism $\theta\colon Q \to \mathrm{Aut}(P)$, but the three groups resulting are all isomorphic to $S_3 \times C_2$ with $C_2 = \mathrm{Ker}\,\theta$. (The homomorphisms differ by an automorphism of Q, and so we can also apply Lemma 3.18.)

In total, there are 3 noncommutative groups of order 12 and 2 commutative groups.

5.17 (Groups of order p^3) Let G be a group of order p^3, with p an odd prime, and assume G is not commutative. We know from (4.17) that G has a normal subgroup N of order p^2.

If every element of G has order p (except 1), then $N \approx C_p \times C_p$ and there is a subgroup Q of G of order p such that $Q \cap N = \{1\}$. Hence

$$G = N \rtimes_\theta Q$$

for some homomorphism $\theta\colon Q \to N$. The order of $\mathrm{Aut}(N) \approx \mathrm{GL}_2(\mathbb{F}_p)$ is $(p^2 - 1)(p^2 - p)$ (see 5.3), and so its Sylow p-subgroups have order p. By the Sylow theorems, they are conjugate, and so Lemma 3.19 shows that there is exactly one nonabelian group in this case.

Suppose G has elements of order p^2, and let N be the subgroup generated by such an element a. Because $(G : N) = p$ is the smallest (in fact only) prime dividing $(G : 1)$, N is normal in G (Exercise 4-5). We next show that G contains an element of order p not in N.

We know $Z(G) \neq 1$, and, because G isn't commutative, that $G/Z(G)$ is not cyclic (4.19). Therefore $(Z(G):1) = p$ and $G/Z(G) \approx C_p \times C_p$. In particular, we see that for all $x \in G$, $x^p \in Z(G)$. Because $G/Z(G)$ is commutative, the commutator of any pair of elements of G lies in $Z(G)$, and an easy induction argument shows that

$$(xy)^n = x^n y^n [y,x]^{\frac{n(n-1)}{2}}, \quad n \geq 1.$$

Therefore $(xy)^p = x^p y^p$, and so $x \mapsto x^p \colon G \to G$ is a homomorphism. Its image is contained in $Z(G)$, and so its kernel has order at least p^2. Since N contains only $p-1$ elements of order p, we see that there exists an element b of order p outside N. Hence $G = \langle a \rangle \rtimes \langle b \rangle \approx C_{p^2} \rtimes C_p$, and it remains to observe (3.19) that the nontrivial homomorphisms $C_p \to \mathrm{Aut}(C_{p^2}) \approx C_p \times C_{p-1}$ give isomorphic groups.

Thus, up to isomorphism, the only noncommutative groups of order p^3 are those constructed in (3.14, 3.15).

5.18 (GROUPS OF ORDER $2p^n$, $4p^n$, AND $8p^n$, p ODD) Let G be a group of order $2^m p^n$, $1 \leq m \leq 3$, p an odd prime, $1 \leq n$. We shall show that G is not simple. Let P be a Sylow p-subgroup and let $N = N_G(P)$, so that $s_p = (G:N)$.

From Sylow II, we know that $s_p | 2^m$, $s_p = 1, p+1, 2p+1, \ldots$. If $s_p = 1$, P is normal. If not, there are two cases to consider:

(i) $s_p = 4$ and $p = 3$, or
(ii) $s_p = 8$ and $p = 7$.

In the first case, the action by conjugation of G on the set of Sylow 3-subgroups[1] defines a homomorphism $G \to S_4$, which, if G is simple, must be injective. Therefore $(G:1)|4!$, and so $n = 1$; we have $(G:1) = 2^m 3$. Now the Sylow 2-subgroup has index 3, and so we have a homomorphism $G \to S_3$. Its kernel is a nontrivial normal subgroup of G.

In the second case, the same argument shows that $(G:1)|8!$, and so $n = 1$ again. Thus $(G:1) = 56$ and $s_7 = 8$. Therefore G has 48 elements of order 7, and so there can be only one Sylow 2-subgroup, which must therefore be normal.

Note that groups of order pq^r, p, q primes, $p < q$ are not simple, because Exercise 4-5 shows that the Sylow q-subgroup is normal. An examination of cases now reveals that A_5 is the smallest noncyclic simple group.

5.19 (GROUPS OF ORDER 60) Let G be a simple group of order 60. We shall show that G is isomorphic to A_5. Let P be a Sylow 2-subgroup and $N = N_G(P)$, so that $s_2 = (G:N)$. According to the Sylow theorems, $s_2 = 1, 3, 5$, or 15.

(a) The case $s_2 = 1$ is impossible, because P would be normal (see 5.8).

(b) The case $s_2 = 3$ is impossible, because the kernel of $G \to \mathrm{Sym}(G/N)$ would be a nontrivial normal subgroup of G.

(c) In the case $s_2 = 5$, we get an inclusion $G \hookrightarrow \mathrm{Sym}(G/N) = S_5$, which realizes G as a subgroup of index 2 in S_5, but we saw in (4.37) that, for $n \geq 5$, A_n is the only subgroup of index 2 in S_n.

(d) In the case $s_2 = 15$, a counting argument (using that $s_5 = 6$) shows that there exist two Sylow 2-subgroups P and Q intersecting in a group of order 2. The normalizer N

[1] Equivalently, the usual map $G \to \mathrm{Sym}(G/N)$.

of $P \cap Q$ contains P and Q, and so it has index 1, 3, or 5 in G. The first two cases are impossible for the same reasons as in (a) and (b). If $(G\colon N) = 5$, the argument in (c) gives an isomorphism $G \approx A_5$; but this is impossible because $s_2(A_5) = 5$.

Exercises

5-1 Show that a finite group (*not* necessarily commutative) is cyclic if, for each $n > 0$, it contains at most n elements of order dividing n.

CHAPTER **6**

Subnormal Series; Solvable and Nilpotent Groups

Subnormal Series.

Let G be a group. A chain of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_i \supset G_{i+1} \supset \cdots \supset G_n = \{1\}.$$

is called a ***subnormal series*** if G_i is normal in G_{i-1} for every i, and it is called a ***normal series*** if G_i is normal in G for every i.[1] The series is said to be ***without repetitions*** if all the inclusions $G_{i-1} \supset G_i$ are proper (i.e., $G_{i-1} \neq G_i$). Then n is called the ***length*** of the series. The quotient groups G_{i-1}/G_i are called the ***quotient*** (or ***factor) groups*** of the series.

A subnormal series is said to be a ***composition series*** if it has no proper refinement that is also a subnormal series. In other words, it is a composition series if G_i is maximal among the proper normal subgroups G_{i-1} for each i. Thus a subnormal series is a composition series if and only if each quotient group is simple and nontrivial. Obviously, every finite group has a composition series (usually many): choose G_1 to be a maximal proper normal subgroup of G; then choose G_2 to be a maximal proper normal subgroup of G_1, etc.. An infinite group may or may not have a finite composition series.

Note that from a subnormal series

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd G_n = \{1\}$$

we obtain a sequence of exact sequences

$$\begin{gathered} 1 \to G_{n-1} \to G_{n-2} \to G_{n-2}/G_{n-1} \to 1 \\ \cdots \\ 1 \to G_{i+1} \to G_i \to G_i/G_{i+1} \to 1 \\ \cdots \\ 1 \to G_1 \to G_0 \to G_0/G_1 \to 1. \end{gathered}$$

Thus G is built up out of the quotients $G_0/G_1, G_1/G_2, \ldots, G_{n-1}$ by forming successive extensions. In particular, since every finite group has a composition series, it can be regarded

[1] Some authors write "normal series" where we write "subnormal series" and "invariant series" where we write "normal series".

as being built up out of simple groups. The Jordan–Hölder theorem, which is the main topic of this section, says that these simple groups are independent of the composition series (up to order and isomorphism).

Note that if G has a subnormal series $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$, then

$$(G:1) = \prod_{1 \le i \le n} (G_{i-1} : G_i) = \prod_{1 \le i \le n} (G_{i-1}/G_i : 1).$$

EXAMPLE 6.1 (a) The symmetric group S_3 has a composition series

$$S_3 \rhd A_3 \rhd 1$$

with quotients C_2, C_3.

(b) The symmetric group S_4 has a composition series

$$S_4 \rhd A_4 \rhd V \rhd \langle (13)(24) \rangle \rhd 1,$$

where $V \approx C_2 \times C_2$ consists of all elements of order 2 in A_4 (see 4.32). The quotients are C_2, C_3, C_2, C_2.

(c) Any maximal flag in $\mathbb{F}_p^n$, p a prime, is a composition series. Its length is n, and its quotients are $C_p, C_p, \ldots, C_p$.

(d) Consider the cyclic group $C_m = \langle a \rangle$. For any factorization $m = p_1 \cdots p_r$ of m into a product of primes (not necessarily distinct), there is a composition series

$$\begin{array}{ccccccc} C_m & \rhd & C_{\frac{m}{p_1}} & \rhd & C_{\frac{m}{p_1 p_2}} & \rhd & \cdots \\ \| & & \| & & \| & & \\ \langle a \rangle & & \langle a^{p_1} \rangle & & \langle a^{p_1 p_2} \rangle & & \end{array}$$

The length is r, and the quotients are $C_{p_1}, C_{p_2}, \ldots, C_{p_r}$.

(e) Suppose G is a direct product of simple groups, $G = H_1 \times \cdots \times H_r$. Then G has a composition series

$$G \rhd H_2 \times \cdots \times H_r \rhd H_3 \times \cdots \times H_r \rhd \cdots$$

of length r and with quotients $H_1, H_2, \ldots, H_r$. Note that for any permutation σ of $\{1, 2, \ldots r\}$, there is another composition series with quotients $H_{\sigma(1)}, H_{\sigma(2)}, \ldots, H_{\sigma(r)}$.

(f) We saw in (4.37) that for $n \ge 5$, the only normal subgroups of S_n are S_n, A_n, $\{1\}$, and in (4.33) that A_n is simple. Hence $S_n \rhd A_n \rhd \{1\}$ is the *only* composition series for S_n.

THEOREM 6.2 (JORDAN–HÖLDER) [2]*Let G be a finite group. If*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_s = \{1\}$$
$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_t = \{1\}$$

are two composition series for G, then $s = t$ and there is a permutation σ of $\{1, 2, \ldots, s\}$ such that $G_i/G_{i+1} \approx H_{\sigma(i)}/H_{\sigma(i)+1}$.

[2] Jordan showed that corresponding quotients had the same order, and Hölder that they were isomorphic.

PROOF. We use induction on the order of G.

Case I: $H_1 = G_1$. In this case, we have two composition series for G_1, to which we can apply the induction hypothesis.

Case II: $H_1 \neq G_1$. Because G_1 and H_1 are both normal in G, the product G_1H_1 is a normal subgroup of G. It properly contains both G_1 and H_1, which are maximal normal subgroups of G, and so $G_1H_1 = G$. Therefore

$$G/G_1 = G_1H_1/G_1 \simeq H_1/G_1 \cap H_1 \qquad \text{(see 1.46).}$$

Similarly $G/H_1 \simeq G_1/G_1 \cap H_1$. Let $K_2 = G_1 \cap H_1$; then K_2 is a maximal normal subgroup in both G_1 and H_1, and

$$G/G_1 \simeq H_1/K_2, \quad G/H_1 \simeq G_1/K_2. \tag{26}$$

Choose a composition series

$$K_2 \rhd K_3 \rhd \cdots \rhd K_u.$$

We have the picture:

$$\begin{tikzcd}
 & G_1 \arrow[r, phantom, "\rhd"] \arrow[dr, dash, "||" marking] & G_2 \arrow[r, phantom, "\rhd"] & \cdots \arrow[r, phantom, "\rhd"] & G_s \\
G \arrow[ur, dash, "|" marking] \arrow[dr, dash, "||" marking] & & K_2 \arrow[r, phantom, "\rhd"] & \cdots \arrow[r, phantom, "\rhd"] & K_u \\
 & H_1 \arrow[r, phantom, "\rhd"] \arrow[ur, dash, "|" marking] & H_2 \arrow[r, phantom, "\rhd"] & \cdots \arrow[r, phantom, "\rhd"] & H_t.
\end{tikzcd}$$

On applying the induction hypothesis to G_1 and H_1 and their composition series in the diagram, we find that

$$\begin{aligned}
\text{Quotients}(G \rhd G_1 \rhd G_2 \rhd \cdots) &= \{G/G_1, G_1/G_2, G_2/G_3, \ldots\} && \text{(definition)}\\
&\sim \{G/G_1, G_1/K_2, K_2/K_3, \ldots\} && \text{(induction)}\\
&\sim \{H_1/K_2, G/H_1, K_2/K_3, \ldots\} && \text{(apply (26))}\\
&\sim \{G/H_1, H_1/K_2, K_2/K_3, \ldots\} && \text{(reorder)}\\
&\sim \{G/H_1, H_1/H_2, H_2/H_3, \ldots\} && \text{(induction)}\\
&= \text{Quotients}(G \rhd H_1 \rhd H_2 \rhd \cdots) && \text{(definition).} \qquad \square
\end{aligned}$$

Note that the theorem applied to a cyclic group C_m implies that the factorization of an integer into a product of primes is unique.

REMARK 6.3 (a) There are infinite groups having finite composition series (there are even infinite simple groups). For such a group, let $d(G)$ be the minimum length of a composition series. Then the Jordan–Hölder theorem extends to show that all composition series have length $d(G)$ and have isomorphic quotient groups. The same proof works except that you have to use induction on $d(G)$ instead of $|G|$ and verify that a normal subgroup of a group with a finite composition series also has a finite composition series (Exercise 6-1).

(b) Analogues of the Jordan–Hölder theorem hold in many situations, but not in all situations. Consider, for example, the category of finitely generated projective modules over a Dedekind domain R. Every such module is isomorphic to a finite direct sum $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ of nonzero ideals in R, and two modules $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ and $\mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$ are isomorphic if and only if $r = s$ and $\mathfrak{a}_1 \cdots \mathfrak{a}_r$ equals $\mathfrak{b}_1 \cdots \mathfrak{b}_s$ in the ideal class group of R. If $\mathfrak{a}$ is a nonprincipal ideal in R and $\mathfrak{b}$ is such that $\mathfrak{a}\mathfrak{b}$ is principal, then $\mathfrak{a} \oplus \mathfrak{b} \approx R^2$, and so R^2 has composition series with distinct quotients $\{\mathfrak{a}, \mathfrak{b}\}$ and $\{R, R\}$.

The quotients of a composition series are sometimes called ***composition factors.***

Solvable groups

A subnormal series whose quotient groups are all commutative is called a ***solvable series***. A group is ***solvable*** (or ***soluble***) if it has a solvable series. Alternatively, we can say that a group is solvable if it can be obtained by forming successive extensions of commutative groups. Since a commutative group is simple if and only if it is cyclic of prime order, we see that G is solvable if and only if for one (hence every) composition series the quotients are all cyclic groups of prime order.

Every commutative group is solvable, as is every dihedral group. The results in Chapter 5 show that every group of order < 60 is solvable. By contrast, a noncommutative simple group, e.g., A_n for $n \geq 5$, will not be solvable.

THEOREM 6.4 (FEIT-THOMPSON) *Every finite group of odd order is solvable.*[3]

PROOF. The proof occupies an entire issue of the Pacific Journal of Mathematics (Feit and Thompson 1963). □

In other words, every finite group is either solvable or contains an element of order 2. For the role this theorem played in the classification of the finite simple groups, see p. 53. For a more recent look at the Feit-Thompson theorem, see Glauberman 1999.

EXAMPLE 6.5 Consider the subgroups $B = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\}$ and $U = \left\{\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\right\}$ of $\mathrm{GL}_2(F)$, some field F. Then U is a normal subgroup of B, and $B/U \simeq F^\times \times F^\times$, $U \simeq (F, +)$. Hence B is solvable.

PROPOSITION 6.6 *(a) Every subgroup and every quotient group of a solvable group is solvable.*

(b) An extension of solvable groups is solvable.

PROOF. (a) Let $G \triangleright G_1 \triangleright \cdots \triangleright G_n$ be a solvable series for G, and let H be a subgroup of G. The homomorphism

$$x \mapsto xG_{i+1} : H \cap G_i \to G_i/G_{i+1}$$

[3] Burnside (1897, p. 379) wrote:

> No simple group of odd order is at present known to exist. An investigation as to the existence or non-existence of such groups would undoubtedly lead, whatever the conclusion might be, to results of importance; it may be recommended to the reader as well worth his attention. Also, there is no known simple group whose order contains fewer than three different primes....

Significant progress in the first problem was not made until Suzuki, M., *The nonexistence of a certain type of simple group of finite order*, 1957. However, the second problem was solved by Burnside himself, who proved using characters that any group whose order contains fewer than three different primes is solvable (see Alperin and Bell 1995, p. 182).

has kernel $(H \cap G_i) \cap G_{i+1} = H \cap G_{i+1}$. Therefore, $H \cap G_{i+1}$ is a normal subgroup of $H \cap G_i$ and the quotient $H \cap G_i / H \cap G_{i+1}$ injects into G_i / G_{i+1}, which is commutative. We have shown that

$$H \triangleright H \cap G_1 \triangleright \cdots \triangleright H \cap G_n$$

is a solvable series for H.

Let $\bar{G}$ be a quotient group of G, and let $\bar{G}_i$ be the image of G_i in $\bar{G}$. Then

$$\bar{G} \triangleright \bar{G}_1 \triangleright \cdots \triangleright \bar{G}_n = \{1\}$$

is a solvable series for $\bar{G}$.

(b) Let N be a normal subgroup of G, and let $\bar{G} = G/N$. We have to show that if N and $\bar{G}$ are solvable, then so also is G. Let

$$\bar{G} \triangleright \bar{G}_1 \triangleright \cdots \triangleright \bar{G}_n = \{1\}$$

$$N \triangleright N_1 \triangleright \cdots \triangleright N_m = \{1\}$$

be solvable series for $\bar{G}$ and N, and let G_i be the inverse image of $\bar{G}_i$ in G. Then $G_i / G_{i+1} \simeq \bar{G}_i / \bar{G}_{i+1}$ (see 1.48), and so

$$G \triangleright G_1 \triangleright \cdots \triangleright G_n (= N) \triangleright N_1 \triangleright \cdots \triangleright N_m$$

is a solvable series for G. □

COROLLARY 6.7 *A finite p-group is solvable.*

PROOF. We use induction on the order the group G. According to (4.16), the centre $Z(G)$ of G is nontrivial, and so the induction hypothesis implies that $G/Z(G)$ is solvable. Because $Z(G)$ is commutative, (b) of the proposition shows that G is solvable. □

Let G be a group. Recall that the commutator of $x, y \in G$ is

$$[x, y] = xyx^{-1}y^{-1} = xy(yx)^{-1}$$

Thus

$$[x, y] = 1 \iff xy = yx,$$

and G is commutative if and only if every commutator equals 1.

EXAMPLE 6.8 For any finite-dimensional vector space V over a field k and any maximal flag $F = \{V_n, V_{n-1}, \ldots\}$ in V, the group

$$B(F) = \{\alpha \in \mathrm{Aut}(V) \mid \alpha(V_j) \subset V_j \text{ all } j\}$$

is solvable. Indeed, let $U(F)$ be the group defined in Example 5.10. Then $B(F)/U(F)$ is commutative, and, when $k = \mathbb{F}_p$, $U(F)$ is a p-group. This proves that $B(F)$ is solvable when $k = \mathbb{F}_p$, and in the general case one defines subgroups $B_0 \supset B_1 \supset \cdots$ of $B(F)$ with

$$B_i = \{\alpha \in B(F) \mid \alpha \text{ induces the identity map on } V_j / V_{j-i} \text{ all } i\},$$

and notes that the commutator of two elements of B_i lies in B_{i+1}.

For any homomorphism $\varphi: G \to H$

$$\varphi([x,y]) = \varphi(xyx^{-1}y^{-1}) = [\varphi(x), \varphi(y)],$$

i.e., φ maps the commutator of x, y to the commutator of $\varphi(x), \varphi(y)$. In particular, we see that if H is commutative, then φ maps all commutators in G to 1.

The group $G' = G^{(1)}$ generated by the commutators in G is called the ***commutator*** or ***first derived subgroup*** of G.

PROPOSITION 6.9 *The commutator subgroup G' is a characteristic subgroup of G; it is the smallest normal subgroup of G such that G/G' is commutative.*

PROOF. An automorphism α of G maps the generating set for G' into G', and hence maps G' into G'. Since this is true for all automorphisms of G, G' is characteristic.

Write $g \mapsto \bar{g}$ for the homomorphism $g \mapsto gG': G \to G/G'$. Then $[\bar{g}, \bar{h}] = \overline{[g,h]}$, which is 1 because $[g,h] \in G'$. Hence $[\bar{g}, \bar{h}] = 1$ for all $\bar{g}$, $\bar{h} \in G/G'$, which shows that G/G' is commutative.

Let N be a second normal subgroup of G such that G/N is commutative. Then $[g,h] \mapsto 1$ in G/N, and so $[g,h] \in N$. Since these elements generate G', $N \supset G'$. □

For $n \geq 5$, A_n is the smallest normal subgroup of S_n giving a commutative quotient. Hence $(S_n)' = A_n$.

The ***second derived subgroup*** of G is $(G')'$; the ***third*** is $G^{(3)} = (G'')'$; and so on. Since a characteristic subgroup of a characteristic subgroup is characteristic (3.7a), each derived group $G^{(n)}$ is a characteristic subgroup of G. Hence we obtain a normal series

$$G \supset G^{(1)} \supset G^{(2)} \supset \cdots,$$

which is called the ***derived series*** of G. For example, when $n \geq 5$, the derived series of S_n is

$$S_n \supset A_n \supset A_n \supset A_n \supset \cdots.$$

PROPOSITION 6.10 *A group G is solvable if and only if its kth derived subgroup $G^{(k)} = 1$ for some k.*

PROOF. If $G^{(k)} = 1$, then the derived series is a solvable series for G. Conversely, let

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_s = 1$$

be a solvable series for G. Because G/G_1 is commutative, $G_1 \supset G'$. Now $G'G_2$ is a subgroup of G_1, and from

$$G'/G' \cap G_2 \xrightarrow{\simeq} G'G_2/G_2 \subset G_1/G_2$$

we see that

$$G_1/G_2 \text{ commutative} \implies G'/G' \cap G_2 \text{ commutative} \implies G'' \subset G' \cap G_2 \subset G_2.$$

Continuing in the fashion, we find that $G^{(i)} \subset G_i$ for all i, and hence $G^{(s)} = 1$. □

Thus, a solvable group G has a *canonical* solvable series, namely the derived series, in which all the groups are normal in G. The proof of the proposition shows that the derived series is the shortest solvable series for G. Its length is called the ***solvable length*** of G.

ASIDE 6.11 Not every element of the commutator subgroup of a group is itself a commutator, but the smallest groups where this occurs have order 96. This was shown by a computer search through the libraries of small groups. In 1951 Ore proved that every element of A_n is a commutator when $n \geq 5$ and conjectured that the same is true of all finite simple groups. This was proved in 2008. For a discussion of this question, see mo44269.

Nilpotent groups

Let G be a group. Recall that we write $Z(G)$ for the centre of G. Let $Z^2(G) \subset G$ be the subgroup of G corresponding to $Z(G/Z(G)) \subset G/Z(G)$. Thus

$$g \in Z^2(G) \iff [g,x] \in Z(G) \text{ for all } x \in G.$$

Continuing in this fashion, we get a sequence of subgroups (***ascending central series***)

$$\{1\} \subset Z(G) \subset Z^2(G) \subset \cdots,$$

where

$$g \in Z^i(G) \iff [g,x] \in Z^{i-1}(G) \text{ for all } x \in G.$$

If $Z^m(G) = G$ for some m, then G is said to be ***nilpotent***, and the smallest such m is called the ***(nilpotency) class*** of G. For example, all finite p-groups are nilpotent (apply 4.16).

Only the group $\{1\}$ has class 0, and the groups of class 1 are exactly the commutative groups. A group G is of class 2 if and only if $G/Z(G)$ is commutative — such a group is said to be ***metabelian***.

EXAMPLE 6.12 (a) A nilpotent group is obviously solvable, but the converse is false. For example, for a field F, let

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a,b,c \in F, \quad ac \neq 0 \right\}.$$

Then $Z(B) = \{aI \mid a \neq 0\}$, and the centre of $B/Z(B)$ is trivial. Therefore $B/Z(B)$ is not nilpotent, but we saw in (6.5) that it is solvable.

(b) The group $G = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}$ is metabelian: its centre is $\left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$, and $G/Z(G)$ is commutative.

(c) Any nonabelian group G of order p^3 is metabelian. In fact, $G' = Z(G)$ has order p (see 5.17), and G/G' is commutative (4.18). In particular, the quaternion and dihedral groups of order 8, Q and D_4, are metabelian. The dihedral group D_{2^n} is nilpotent of class n — this can be proved by induction, using that $Z(D_{2^n})$ has order 2, and $D_{2^n}/Z(D_{2^n}) \approx D_{2^{n-1}}$. If n is not a power of 2, then D_n is not nilpotent (use Theorem 6.18 below).

PROPOSITION 6.13 *(a) A subgroup of a nilpotent group is nilpotent.*

(b) A quotient of a nilpotent group is nilpotent.

PROOF. (a) Let H be a subgroup of a nilpotent group G. Clearly, $Z(H) \supset Z(G) \cap H$. Assume (inductively) that $Z^i(H) \supset Z^i(G) \cap H$; then $Z^{i+1}(H) \supset Z^{i+1}(G) \cap H$, because (for $h \in H$)

$$h \in Z^{i+1}(G) \implies [h,x] \in Z^i(G) \text{ all } x \in G \implies [h,x] \in Z^i(H) \text{ all } x \in H.$$

(b) Straightforward. □

REMARK 6.14 It should be noted that if H is a subgroup of G, then $Z(H)$ may be bigger than $Z(G)$. For example, the centre of

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| ab \neq 0 \right\} \subset \mathrm{GL}_2(F).$$

is H itself, but the centre of $\mathrm{GL}_2(F)$ consists only of the scalar matrices.

PROPOSITION 6.15 *A group G is nilpotent of class $\leq m$ if and only if*

$$[\ldots[[g_1,g_2],g_3],\ldots,,g_{m+1}]=1$$

for all $g_1,...,g_{m+1}\in G$.

PROOF. Recall, $g\in Z^i(G) \iff [g,x]\in Z^{i-1}(G)$ for all $x\in G$.

Assume G is nilpotent of class $\leq m$; then

$$\begin{aligned} G=Z^m(G) &\implies [g_1,g_2]\in Z^{m-1}(G) \text{ all } g_1,g_2\in G\\ &\implies [[g_1,g_2],g_3]\in Z^{m-2}(G) \text{ all } g_1,g_2,g_3\in G\\ &\cdots\cdots\\ &\implies [\cdots[[g_1,g_2],g_3],...,g_m]\in Z(G) \text{ all } g_1,\ldots,g_m\in G\\ &\implies [\cdots[[g_1,g_2],g_3],\ldots,g_{m+1}]=1 \text{ all } g_1,\ldots,g_m\in G. \end{aligned}$$

For the converse, let $g_1\in G$. Then

$$\begin{aligned} &[[...[[g_1,g_2],g_3],...,g_m],g_{m+1}]=1 \text{ for all } g_1,g_2,...,g_{m+1}\in G\\ &\implies [...[[g_1,g_2],g_3],...,g_m]\in Z(G), \text{ for all } g_1,...,g_m\in G\\ &\implies [...[[g_1,g_2],g_3],...,g_{m-1}]\in Z^2(G), \text{ for all } g_1,...,g_{m-1}\in G\\ &\cdots\cdots\\ &\implies g_1\in Z^m(G) \text{ all } g_1\in G. \end{aligned}$$

□

An extension of nilpotent groups need not be nilpotent, i.e.,

$$N \text{ and } G/N \text{ nilpotent } \not\Rightarrow G \text{ nilpotent.} \tag{27}$$

For example, the subgroup U of the group B in Examples 6.5 and 6.12 is commutative and B/U is commutative, but B is not nilpotent.

However, the implication (27) holds when N is contained in the centre of G. In fact, we have the following more precise result.

COROLLARY 6.16 *For any subgroup N of the centre of G,*

$$G/N \text{ nilpotent of class } m \implies G \text{ nilpotent of class } \leq m+1.$$

PROOF. Write π for the map $G\to G/N$. Then

$$\pi([...[[g_1,g_2],g_3],...,g_m],g_{m+1}])=[...[[\pi g_1,\pi g_2],\pi g_3],...,\pi g_m],\pi g_{m+1}]=1$$

all $g_1,...,g_{m+1}\in G$. Hence $[...[[g_1,g_2],g_3],...,g_m],g_{m+1}]\in N\subset Z(G)$, and so

$$[...[[g_1,g_2],g_3],...,g_{m+1}],g_{m+2}]=1 \text{ all } g_1,...,g_{m+2}\in G.$$

□

COROLLARY 6.17 *A finite p-group is nilpotent.*

PROOF. We use induction on the order of G. Because $Z(G)\neq 1$, $G/Z(G)$ nilpotent, which implies that G is nilpotent. □

Recall that an extension

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1$$

is central if $\iota(N) \subset Z(G)$. Then:

> the nilpotent groups are those that can be obtained from commutative groups by successive central extensions.

Contrast:

> the solvable groups are those that can be obtained from commutative groups by successive extensions (not necessarily central).

THEOREM 6.18 *A finite group is nilpotent if and only if it is equal to a direct product of its Sylow subgroups.*

PROOF. A direct product of nilpotent groups is obviously nilpotent, and so the "if" direction follows from the preceding corollary. For the converse, let G be a finite nilpotent group. According to (5.9) it suffices to prove that all Sylow subgroups are normal. Let P be such a subgroup of G, and let $N = N_G(P)$. The first lemma below shows that $N_G(N) = N$, and the second then implies that $N = G$, i.e., that P is normal in G. □

LEMMA 6.19 *Let P be a Sylow p-subgroup of a finite group G. For any subgroup H of G containing $N_G(P)$, we have $N_G(H) = H$.*

PROOF. Let $g \in N_G(H)$, so that $gHg^{-1} = H$. Then $H \supset gPg^{-1} = P'$, which is a Sylow p-subgroup of H. By Sylow II, $hP'h^{-1} = P$ for some $h \in H$, and so $hgPg^{-1}h^{-1} \subset P$. Hence $hg \in N_G(P) \subset H$, and so $g \in H$. □

LEMMA 6.20 *Let H be proper subgroup of a finite nilpotent group G; then $H \neq N_G(H)$.*

PROOF. The statement is obviously true for commutative groups, and so we can assume G to be noncommutative. We use induction on the order of G. Because G is nilpotent, $Z(G) \neq 1$. Certainly the elements of $Z(G)$ normalize H, and so if $Z(G) \not\subseteq H$, we have $H \subsetneqq Z(G) \cdot H \subset N_G(H)$. Thus we may suppose $Z(G) \subset H$. Then the normalizer of H in G corresponds under (1.47) to the normalizer of $H/Z(G)$ in $G/Z(G)$, and we can apply the induction hypothesis. □

REMARK 6.21 For a finite abelian group G we recover the fact that G is a direct product of its p-primary subgroups.

PROPOSITION 6.22 (FRATTINI'S ARGUMENT) *Let H be a normal subgroup of a finite group G, and let P be a Sylow p-subgroup of H. Then $G = H \cdot N_G(P)$.*

PROOF. Let $g \in G$. Then $gPg^{-1} \subset gHg^{-1} = H$, and both gPg^{-1} and P are Sylow p-subgroups of H. According to Sylow II, there is an $h \in H$ such that $gPg^{-1} = hPh^{-1}$, and it follows that $h^{-1}g \in N_G(P)$ and so $g \in H \cdot N_G(P)$. □

THEOREM 6.23 *A finite group is nilpotent if and only if every maximal proper subgroup is normal.*

PROOF. We saw in Lemma 6.20 that for any proper subgroup H of a nilpotent group G, $H \subsetneqq N_G(H)$. Hence,

$$H \text{ maximal} \implies N_G(H) = G,$$

i.e., H is normal in G.

Conversely, suppose every maximal proper subgroup of G is normal. We shall check the condition of Theorem 6.18. Thus, let P be a Sylow p-subgroup of G. If P is not normal in G, then there exists a maximal proper subgroup H of G containing $N_G(P)$. Being maximal, H is normal, and so Frattini's argument shows that $G = H \cdot N_G(P) = H$ — contradiction.□

ASIDE 6.24 Consider a nilpotent group G of class 2:

$$1 \to A \to G \to B \to 1, \quad A, B \text{ commutative}, \quad A \subset Z(G).$$

Taking commutators induces a map $\bigwedge^2 B \to A$ (and every such map occurs for some extension). The image of this map is the commutator subgroup and the image of the pure tensors $b \wedge b'$ is the set of actual commutators. This can be used to give examples of groups whose commutator subgroup doesn't consist entirely of commutators (Torsten Ekedahl, mo44269).

Groups with operators

Recall that the set $\mathrm{Aut}(G)$ of automorphisms of a group G is again a group. Let A be a group. A pair (G, φ) consisting of a group G together with a homomorphism $\varphi\colon A \to \mathrm{Aut}(G)$ is called an ***A*-group**, or G is said to have A as a ***group of operators***.

Let G be an A-group, and write ${}^{\alpha}x$ for $\varphi(\alpha)x$. Then

(a) ${}^{(\alpha\beta)}x = {}^{\alpha}({}^{\beta}x)$ (φ is a homomorphism);
(b) ${}^{\alpha}(xy) = {}^{\alpha}x \cdot {}^{\alpha}y$ ($\varphi(\alpha)$ is a homomorphism);
(c) ${}^{1}x = x$ (φ is a homomorphism).

Conversely, a map $(\alpha, x) \mapsto {}^{\alpha}x : A \times G \to G$ satisfying (a), (b), (c) arises from a homomorphism $A \to \mathrm{Aut}(G)$. Conditions (a) and (c) show that $x \mapsto {}^{\alpha}x$ is inverse to $x \mapsto {}^{(\alpha^{-1})}x$, and so $x \mapsto {}^{\alpha}x$ is a bijection $G \to G$. Condition (b) then shows that it is an automorphism of G. Finally, (a) shows that the map $\varphi(\alpha) = (x \mapsto {}^{\alpha}x)$ is a homomorphism $A \to \mathrm{Aut}(G)$.

Let G be a group with operators A. A subgroup H of G is ***admissible*** or ***A*-invariant** if

$$x \in H \implies {}^{\alpha}x \in H, \text{ all } \alpha \in A.$$

An intersection of admissible groups is admissible. If H is admissible, so also are its normalizer $N_G(H)$ and centralizer $C_G(H)$.

An ***A*-homomorphism** (or ***admissible homomorphism***) of A-groups is a homomorphism $\gamma\colon G \to G'$ such that $\gamma({}^{\alpha}g) = {}^{\alpha}\gamma(g)$ for all $\alpha \in A$, $g \in G$.

EXAMPLE 6.25 (a) A group G can be regarded as a group with $\{1\}$ as group of operators. In this case all subgroups and homomorphisms are admissible, and so the theory of groups with operators includes the theory of groups without operators.

(b) Consider G acting on itself by conjugation, i.e., consider G together with the homomorphism

$$g \mapsto i_g\colon G \to \mathrm{Aut}(G).$$

In this case, the admissible subgroups are the normal subgroups.

(c) Consider G with $A = \mathrm{Aut}(G)$ as group of operators. In this case, the admissible subgroups are the characteristic subgroups.

Almost everything we have proved for groups also holds for groups with operators. In particular, the Theorems 1.45, 1.46, and 1.47 hold for groups with operators. In each case, the proof is the same as before except that admissibility must be checked.

THEOREM 6.26 *For any admissible homomorphism $\gamma\colon G \to G'$ of A-groups, $N \overset{\text{def}}{=} \operatorname{Ker}(\gamma)$ is an admissible normal subgroup of G, $\gamma(G)$ is an admissible subgroup of G', and γ factors in a natural way into the composite of an admissible surjection, an admissible isomorphism, and an admissible injection:*

$$G \twoheadrightarrow G/N \xrightarrow{\simeq} \gamma(G) \hookrightarrow G'.$$

THEOREM 6.27 *Let G be a group with operators A, and let H and N be admissible subgroups with N normal. Then $H \cap N$ is a normal admissible subgroup of H, HN is an admissible subgroup of G, and $h(H \cap N) \mapsto hH$ is an admissible isomorphism $H/H \cap N \to HN/N$.*

THEOREM 6.28 *Let $\varphi\colon G \to \bar{G}$ be a surjective admissible homomorphism of A-groups. Under the one-to-one correspondence $H \leftrightarrow \bar{H}$ between the set of subgroups of G containing $\operatorname{Ker}(\varphi)$ and the set of subgroups of $\bar{G}$ (see 1.47), admissible subgroups correspond to admissible subgroups.*

Let $\varphi\colon A \to \operatorname{Aut}(G)$ be a group with A operating. An ***admissible subnormal series*** is a chain of admissible subgroups of G

$$G \supset G_1 \supset G_2 \supset \cdots \supset G_r$$

with each G_i normal in G_{i-1}. Define similarly an admissible composition series. The quotients of an admissible subnormal series are A-groups, and the quotients of an admissible composition series are simple A-groups, i.e., they have no normal admissible subgroups apart from the obvious two.

The Jordan–Hölder theorem continues to hold for A-groups. In this case the isomorphisms between the corresponding quotients of two composition series are admissible. The proof is the same as that of the original theorem, because it uses only the isomorphism theorems, which we have noted also hold for A-groups.

EXAMPLE 6.29 (a) Consider G with G acting by conjugation. In this case an admissible subnormal series is a sequence of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_s = \{1\},$$

with each G_i normal in G, i.e., a normal series. The action of G on G_i by conjugation passes to the quotient, to give an action of G on G_i/G_{i+1}. The quotients of two admissible composition series are isomorphic as G-groups.

(b) Consider G with $A = \operatorname{Aut}(G)$ as operator group. In this case, an admissible subnormal series is a sequence

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_s = \{1\}$$

with each G_i a characteristic subgroup of G, and the quotients of two admissible composition series are isomorphic as $\operatorname{Aut}(G)$-groups.

Krull-Schmidt theorem

A group G is ***indecomposable*** if $G \neq 1$ and G is not isomorphic to a direct product of two nontrivial groups, i.e., if

$$G \approx H \times H' \implies H = 1 \text{ or } H' = 1.$$

EXAMPLE 6.30 (a) A simple group is indecomposable, but an indecomposable group need not be simple: it may have a normal subgroup. For example, S_3 is indecomposable but has C_3 as a normal subgroup.

(b) A finite commutative group is indecomposable if and only if it is cyclic of prime-power order.

Of course, this is obvious from the classification, but it is not difficult to prove it directly. Let G be cyclic of order p^n, and suppose that $G \approx H \times H'$. Then H and H' must be p-groups, and they can't both be killed by p^m, $m < n$. It follows that one must be cyclic of order p^n, and that the other is trivial. Conversely, suppose that G is commutative and indecomposable. Since every finite commutative group is (obviously) a direct product of p-groups with p running over the primes, G is a p-group. If g is an element of G of highest order, one shows that $\langle g \rangle$ is a direct factor of G, $G \approx \langle g \rangle \times H$, which is a contradiction.

(c) Every finite group can be written as a direct product of indecomposable groups (obviously).

THEOREM 6.31 (KRULL-SCHMIDT) [4] *Suppose that G is a direct product of indecomposable subgroups $G_1, \ldots, G_s$ and of indecomposable subgroups $H_1, \ldots, H_t$:*

$$G \simeq G_1 \times \cdots \times G_s, \quad G \simeq H_1 \times \cdots \times H_t.$$

Then $s = t$, and there is a re-indexing such that $G_i \approx H_i$. Moreover, given r, we can arrange the numbering so that

$$G = G_1 \times \cdots \times G_r \times H_{r+1} \times \cdots \times H_t.$$

PROOF. See Rotman 1995, 6.36. □

EXAMPLE 6.32 Let $G = \mathbb{F}_p \times \mathbb{F}_p$, and think of it as a two-dimensional vector space over $\mathbb{F}_p$. Let

$$G_1 = \langle (1,0) \rangle, \quad G_2 = \langle (0,1) \rangle; \quad H_1 = \langle (1,1) \rangle, \quad H_2 = \langle (1,-1) \rangle.$$

Then $G = G_1 \times G_2$, $G = H_1 \times H_2$, $G = G_1 \times H_2$.

REMARK 6.33 (a) The Krull-Schmidt theorem holds also for an infinite group provided it satisfies both chain conditions on subgroups, i.e., ascending and descending sequences of subgroups of G become stationary.

(b) The Krull-Schmidt theorem also holds for groups with operators. For example, let $\mathrm{Aut}(G)$ operate on G; then the subgroups in the statement of the theorem will all be characteristic.

(c) When applied to a finite abelian group, the theorem shows that the groups C_{m_i} in a decomposition $G = C_{m_1} \times \ldots \times C_{m_r}$ with each m_i a prime power are uniquely determined up to isomorphism (and ordering).

[4] Strictly, this should be called the Wedderburn-Remak-Schmidt-Krull-Ore theorem — see the Wikipedia: Krull-Schmidt theorem.

Exercises

6-1 Let G be a group (not necessarily finite) with a finite composition series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1,$$

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

$$N = N \cap G_0 \supset N \cap G_1 \supset \cdots \supset N \cap G_n = 1$$

becomes a composition series for N once the repetitions have been omitted.

6-2 If G_1 and G_2 are groups such that $G_1' \approx G_2'$ and $G_1/G_1' \approx G_2/G_2'$, are G_1 and G_2 necessarily isomorphic? (Here $'$ denotes the commutator subgroup.)

CHAPTER **7**

Representations of Finite Groups

Throughout this chapter, G is a finite group and F is a field. All vector spaces are finite-dimensional.

An F-algebra is a ring A containing F in its centre and finite dimensional as an F-vector space. We *do not* assume A to be commutative; for example, A could be the matrix algebra $M_n(F)$. Let $\{e_1,\ldots,e_n\}$ be a basis for A as an F-vector space; then $e_i e_j = \sum_k a_{ij}^k e_k$for some $a_{ij}^k \in F$, called the *structure constants* of A relative to the basis; once a basis has been chosen, the algebra A is uniquely determined by its structure constants.

All A-modules are finite-dimensional when regarded as F-vector spaces. For an A-module V, mV denotes the direct sum of m copies of V.

The ***opposite*** A^{opp} of an F-algebra A is the same F-algebra as A but with the multiplication reversed, i.e., $A^{\mathrm{opp}} = (A,+,\cdot')$ with $a\cdot' b = ba$. In other words, there is a one-to-one correspondence $a \leftrightarrow a'\colon A \leftrightarrow A^{\mathrm{opp}}$ which is an isomorphism of F-vector spaces and has the property that $a'b' = (ba)'$.

An A-module M is ***simple*** if it is nonzero and contains no submodules except 0 and M, and it is ***semisimple*** if it is isomorphic to a direct sum of simple modules.

Matrix representations

A ***matrix representation of degree*** n of G over F is a homomorphism $G \to \mathrm{GL}_n(F)$. The representation is said to be ***faithful*** if the homomorphism is injective. Thus a faithful representation identifies G with group of $n \times n$ matrices.

EXAMPLE 7.1 (a) There is a representation $Q \to \mathrm{GL}_2(\mathbb{C})$ of the quaternion group $Q = \langle a,b\rangle$ sending a to $\begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$ and b to $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. In fact, that is how we originally defined Q in 1.18.

(b) Let $G = S_n$. For each $\sigma \in S_n$, let $I(\sigma)$ be the matrix obtained from the identity matrix by using σ to permute the rows. Then, for any $n \times n$ matrix A, $I(\sigma)A$ is obtained from A by using σ to permute the rows. In particular, $I(\sigma)I(\sigma') = I(\sigma\sigma')$, and so $\sigma \mapsto I(\sigma)$ is a representation of S_n. Clearly, it is faithful. As every finite group embeds into S_n for some n (Cayley's theorem, see 1.22), this shows that every finite group has a faithful matrix representation.

(c) Let $G = C_n = \langle\sigma\rangle$. If F contains an nth root of 1, say ζ, then there is representation $\sigma^i \mapsto \zeta^i\colon C_n \to \mathrm{GL}_1(F) = F^\times$. The representation is faithful if and only if ζ has order exactly n. If $n = p$ is prime and F has characteristic p, then $X^p - 1 = (X-1)^p$, and so 1 is the only pth root of 1 in F. In this case, the representation is trivial, but there is a faithful representation

$$\sigma^i \mapsto \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} : C_p \to \mathrm{GL}_2(F).$$

ASIDE 7.2 Recall that the Burnside problem asks whether every finitely generated group with finite exponent is finite (see p. 37). Burnside proved that the problem has a *positive* answer for subgroups of $\mathrm{GL}_n(\mathbb{C})$. Therefore, no infinite finitely generated group with finite exponent has a faithful representation over $\mathbb{C}$.

Roots of 1 in fields

As the last example indicates, the representations of a group over a field F depend on the roots of 1 in the field. The nth roots of 1 in a field F form a subgroup $\mu_n(F)$ of $F^\times$, which is cyclic (see 1.56).

If the characteristic of F divides n, then $|\mu_n(F)| < n$. Otherwise, $X^n - 1$ has distinct roots (a multiple root would have to be a root of its derivative nX^{n-1}), and we can always arrange that $|\mu_n(F)| = n$ by extending F, for example, by replacing a subfield F of $\mathbb{C}$ with $F[\zeta]$, where $\zeta = e^{2\pi i/n}$, or by replacing F with $F[X]/(g(X))$, where $g(X)$ is an irreducible factor of $X^n - 1$ not dividing $X^m - 1$ for any proper divisor m of n.

An element of order n in $F^\times$ is called a ***primitive*** nth root of 1. To say that F contains a primitive nth root ζ of 1 means that $\mu_n(F)$ is a cyclic group of order n and that ζ generates it (and it implies that either F has characteristic 0 or it has characteristic a prime not dividing n).

Linear representations

Recall (4.1) that we have defined the notion of a group G acting a set. When the set is an F-vector space V, we say that the action is ***linear*** if the map

$$g_V : V \to V,\ x \mapsto gx,$$

is linear for each $g \in G$. Then g_V has inverse the linear map $(g^{-1})_V$, and $g \mapsto g_V : G \to \mathrm{GL}(V)$ is a homomorphism. Thus, from a linear action of G on V, we obtain a homomorphism of groups $G \to \mathrm{GL}(V)$; conversely, every such homomorphism defines a linear action of G on V. We call a homomorphism $G \to \mathrm{GL}(V)$ a ***linear representation*** of G on V. Note that a linear representation of G on F^n is just a matrix representation of degree n.

EXAMPLE 7.3 (a) Let $G = C_n = \langle\sigma\rangle$, and assume that F contains a primitive nth root ζ of 1. Let $G \to \mathrm{GL}(V)$ be a linear representation of G. Then $(\sigma_V)^n = (\sigma^n)_V = 1$, and so the minimal polynomial of σ_V divides $X^n - 1$. As $X^n - 1$ has n distinct roots $\zeta^0, \ldots, \zeta^{n-1}$ in F, the vector space V decomposes into a direct sum of eigenspaces

$$V = \bigoplus\nolimits_{0 \le i \le n-1} V_i, \quad V_i \overset{\text{def}}{=} \{v \in V \mid \sigma v = \zeta^i v\}.$$

Conversely, every such direct sum decomposition of V arises from a representation of G.

(b) Let G be a commutative group of exponent n, and assume that F contains a primitive nth root of 1. Let

$$G^{\vee} = \mathrm{Hom}(G, F^{\times}) = \mathrm{Hom}(G, \mu_n(F))$$

To give a representation of G on a vector space V is the same as to give a direct sum decomposition

$$V = \bigoplus\nolimits_{\chi \in G^{\vee}} V_{\chi}, \quad V_{\chi} \overset{\text{def}}{=} \{v \in V \mid \sigma v = \chi(\sigma)v\}.$$

When G is cyclic, this is a restatement of (a), and the general case follows easily (decompose V with respect to the action of one cyclic factor of G; then decompose each summand with respect to the action of a second cyclic factor of G; and so on).

Maschke's theorem

Let $G \to \mathrm{GL}(V)$ be a linear representation of G on an F-vector space V. A subspace W of V is said to be ***G*-invariant** if $gW \subset W$ for all $g \in G$. An F-linear map $\alpha: V \to V'$ of vector spaces on which G acts linearly is said to be ***G*-invariant** if

$$\alpha(gv) = g(\alpha v) \text{ for all } g \in G, v \in V.$$

Finally, a bilinear form $\phi: V \times V \to F$ is said to be ***G*-invariant** if

$$\phi(gv, gv') = \phi(v, v') \text{ for all } g \in G,\ v, v' \in V.$$

THEOREM 7.4 (MASCHKE) *Let $G \to \mathrm{GL}(V)$ be a linear representation of G. If the characteristic of F does not divide $|G|$, then every G-invariant subspace W of V has a G-invariant complement, i.e., there exists a G-invariant subspace W' such that $V = W \oplus W'$.*

Note that the theorem always applies when F has characteristic zero.

The condition on the characteristic is certainly necessary: let $G = \langle\sigma\rangle$ be the cyclic group of order p, where p is the characteristic of F, and let σ acts on $V = F^2$ as the matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ (see 7.1c); the subspace $\left(\begin{smallmatrix}*\\ 0\end{smallmatrix}\right)$ is G-invariant, and its complementary subspaces are those of the form $F\left(\begin{smallmatrix}a\\ b\end{smallmatrix}\right)$, $b \neq 0$; none of them is G-invariant. In fact, in every representation of C_p on a nonzero vector space over a field of characteristic p, there is a nonzero fixed vector.

Because of the importance of the ideas involved, we present two proofs of Maschke's theorem.

PROOF OF MASCHKE'S THEOREM (CASE $F = \mathbb{R}$ OR $\mathbb{C}$)

LEMMA 7.5 *Let ϕ be a symmetric bilinear form on V, and let W be a subspace of V. If ϕ and W are G-invariant, then so also is $W^{\perp} \overset{\text{def}}{=} \{v \in V \mid \phi(w, v) = 0$ for all $w \in W\}$.*

PROOF. Let $v \in W^{\perp}$ and let $g \in G$. For any $w \in W$, $\phi(w, gv) = \phi(g^{-1}w, v)$ because ϕ is G-invariant, and $\phi(g^{-1}w, v) = 0$ because W is G-invariant. This shows that $gv \in W^{\perp}$. □

Recall from linear algebra that if ϕ is positive definite, then $V = W \oplus W^{\perp}$. Therefore, in order to prove Maschke's theorem, it suffices to show that there exists a G-invariant positive definite symmetric bilinear from $\phi: V \times V \to F$.

LEMMA 7.6 *For any symmetric bilinear form ϕ on V,*

$$\bar{\phi}(v,w) \overset{\text{def}}{=} \sum_{g \in G} \phi(gv, gw)$$

is a G-invariant symmetric bilinear form on V.

PROOF. The form $\bar{\phi}$ is obviously bilinear and symmetric, and for $g_0 \in G$,

$$\bar{\phi}(g_0 v, g_0 w) \overset{\text{def}}{=} \sum_{g \in G} \phi(g g_0 v, g g_0 w),$$

which equals $\sum_g \phi(gv, gw)$ because, as g runs over G, so also does gg_0. □

Unfortunately, we can't conclude that $\bar{\phi}$ is nondegenerate when ϕ is (otherwise we could prove that *all* $F[G]$-modules are semisimple, with no restriction on F or G).

LEMMA 7.7 *Let $F = \mathbb{R}$. If ϕ is a positive definite symmetric bilinear form on V, then so also is $\bar{\phi}$.*

PROOF. If ϕ is positive definite, then for every nonzero v in V,

$$\bar{\phi}(v,v) = \sum_{g \in G} \phi(gv, gv) > 0.$$

□

This completes the proof of Maschke's theorem when $F = \mathbb{R}$, because there certainly exist positive definite symmetric bilinear forms ϕ on V. A similar argument using hermitian forms applies when $F = \mathbb{C}$ (or, indeed, when F is any subfield of $\mathbb{C}$).

ASIDE 7.8 A representation of a group G on a real vector space V is ***unitary*** if there exists a G-invariant positive definite symmetric bilinear form on V. Lemma 7.5 shows that every unitary representation is semisimple (see 7.13 below), and Lemma 7.7 shows that every real representation of a finite group is unitary.

PROOF OF MASCHKE'S THEOREM (GENERAL CASE)

An endomorphism π of an F-vector space V is called a ***projector*** if $\pi^2 = \pi$. The minimal polynomial of a projector π divides $X^2 - X = X(X-1)$, and so V decomposes into a direct sum of eigenspaces,

$$V = V_0(\pi) \oplus V_1(\pi), \text{ where } \begin{cases} V_0(\pi) = \{v \in V \mid \pi v = 0\} = \mathrm{Ker}(\pi) \\ V_1(\pi) = \{v \in V \mid \pi v = v\} = \mathrm{Im}(\pi). \end{cases}$$

Conversely, a decomposition $V = V_0 \oplus V_1$ arises from a projector $(v_0, v_1) \mapsto (0, v_1)$.

Now suppose that G acts linearly on V. If a projector π is G-invariant, then $V_1(\pi)$ and $V_0(\pi)$ are obviously G-invariant. Thus, to prove the theorem it suffices to show that W is the image of a G–invariant projector π.

We begin by choosing an F-linear projector π with image W, which certainly exists, and we modify it to obtain a G-invariant projector $\bar{\pi}$ with the same image. For $v \in V$, let

$$\bar{\pi}(v) = \frac{1}{|G|} \sum_{g \in G} g\left(\pi(g^{-1}v)\right).$$

This makes sense because $|G|\cdot 1\in F^{\times}$, and it defines an F-linear map $\bar{\pi}\colon V\to V$. Let $w\in W$; then $g^{-1}w\in W$, and so

$$\bar{\pi}(w)=\frac{1}{|G|}\sum_{g\in G}g(g^{-1}w)=\frac{1}{|G|}\sum_{g\in G}w=w. \tag{28}$$

The image of $\bar{\pi}$ is contained in W, because $\operatorname{Im}(\pi)\subset W$ and W is G-invariant, and so

$$\bar{\pi}^{2}(v)\overset{\text{def}}{=}\bar{\pi}(\bar{\pi}(v))\overset{(28)}{=}\bar{\pi}(v)$$

for any $v\in V$. Thus, $\bar{\pi}$ is a projector, and (28) shows that $\operatorname{Im}(\bar{\pi})\supset W$, and hence $\operatorname{Im}(\bar{\pi})=W$. It remains to show that $\bar{\pi}$ is G-invariant. For $g_0\in V$

$$\bar{\pi}(g_0v)=\frac{1}{|G|}\sum_{g\in G}g\left(\pi(g^{-1}g_0v)\right)=g_0\frac{1}{|G|}\sum_{g\in G}(g_0^{-1}g)\left(\pi(g^{-1}g_0v)\right),$$

which equals $g_0\bar{\pi}(v)$ because, as g runs over G, so also does $g_0^{-1}g$.

The group algebra; semisimplicity

The ***group algebra*** $F[G]$ of G is defined to be the F-vector space with basis the elements of G endowed with the multiplication extending that on G. Thus, an element of $F[G]$ is a sum

$$\sum c_g g,\quad c_g\in F,\quad g\in G,$$

two elements of $F[G]$ are equal,

$$\sum\nolimits_g c_g g=\sum\nolimits_g c'_g g,$$

if and only if $c_g=c'_g$ for all g, and

$$\left(\sum\nolimits_g c_g g\right)\left(\sum\nolimits_g c'_g g\right)=\sum\nolimits_g c''_g g,$$

with $c''_g=\sum_{g_1g_2=g}c_{g_1}c'_{g_2}$. A linear action

$$g,v\mapsto gv\colon G\times V\to V$$

of G on an F-vector space extends uniquely to an action of $F[G]$ on V,

$$\sum\nolimits_g c_g g,v\mapsto\sum\nolimits_g c_g gv\colon F[G]\times V\to V,$$

and makes V into an $F[G]$-module. The submodules for this action are exactly the G-invariant subspaces.

Let $G\to\mathrm{GL}(V)$ be a linear representation of G. When V is simple (resp. semisimple) as an $F[G]$-module, the representation is usually said to be ***irreducible*** (resp. ***completely reducible***). However, I prefer to call them ***simple*** (resp. ***semisimple***) representations.

PROPOSITION 7.9 *If the characteristic of F does not divide $|G|$, then every $F[G]$-module is a direct sum of simple submodules.*

PROOF. Let V be a $F[G]$-module. If V is simple, then there is nothing to prove. Otherwise, it contains a nonzero proper submodule W. According to Maschke's theorem, $V = W \oplus W'$ with W' an $F[G]$-submodule. If W and W' are simple, then the proof is complete; otherwise, we can continue the argument, which terminates in a finite number of steps because V has finite dimension as an F-vector space. □

As we have observed, the linear representations of G can be regarded as $F[G]$-modules. Thus, to understand the linear representations of G, we need to understand the $F[G]$-modules, and for this we need to understand the structure of the F-algebra $F[G]$. In the next three sections we study F-algebras and their modules. In particular, we prove the famous Wedderburn theorems concerning F-algebras whose modules are all semisimple.

Semisimple modules

In this section, A is an F-algebra.

THEOREM 7.10 *Every A-module V admits a filtration*

$$V = V_0 \supset V_1 \supset \cdots \supset V_s = \{0\}$$

such that the quotients V_i/V_{i+1} are simple A-modules. If

$$V = W_0 \supset W_1 \supset \cdots \supset W_t = \{0\}$$

is a second such filtration, then $s = t$ and there is a permutation σ of $\{1,\ldots,s\}$ such that $V_i/V_{i+1} \approx W_{\sigma(i)}/W_{\sigma(i)+1}$ for all i.

PROOF. This is a variant of the Jordan–Hölder theorem (6.2), which can be proved by the same argument. □

COROLLARY 7.11 *Suppose*

$$V \approx V_1 \oplus \cdots \oplus V_s \approx W_1 \oplus \cdots \oplus W_t$$

with all the A-modules V_i and W_j simple. Then $s = t$ and there is a permutation σ of $\{1,\ldots,s\}$ such that $V_i \approx W_{\sigma(i)}$.

PROOF. Each decomposition defines a filtration, to which the proposition can be applied.□

PROPOSITION 7.12 *Let V be an A-module. If V is a sum of simple submodules, say $V = \sum_{i \in I} S_i$ (the sum need not be direct), then for any submodule W of V, there is a subset J of I such that*

$$V = W \oplus \bigoplus_{i \in J} S_i.$$

PROOF. Let J be maximal among the subsets of I such the sum $S_J \overset{\text{def}}{=} \sum_{j \in J} S_j$ is direct and $W \cap S_J = 0$. I claim that $W + S_J = V$ (hence V is the direct sum of W and the S_j with $j \in J$). For this, it suffices to show that each S_i is contained in $W + S_J$. Because S_i is simple, $S_i \cap (W + S_J)$ equals S_i or 0. In the first case, $S_i \subset W + S_J$, and in the second $S_J \cap S_i = 0$ and $W \cap (S_J + S_i) = 0$, contradicting the definition of I. □

COROLLARY 7.13 *The following conditions on an A-module V are equivalent:*

(a) *V is semisimple;*
(b) *V is a sum of simple submodules;*
(c) *every submodule of V has a complement.*

PROOF. The proposition shows that (b) implies (c), and the argument in the proof of (7.9) shows that (c) implies (a). It is obvious that (a) implies (b). □

COROLLARY 7.14 *Sums, submodules, and quotient modules of semisimple modules are semisimple.*

PROOF. Each is a sum of simple modules. □

Every semisimple A-module V can be written as a direct sum

$$V \simeq m_1 S_1 \oplus \cdots \oplus m_r S_r \tag{29}$$

with each S_i simple and no two are isomorphic. An A-module is said to be ***isotypic*** (of type the isomorphism class of S) if it isomorphic to a direct sum of copies of a simple module S. The decomposition (29) shows that every semisimple module V is a direct sum of isotypic modules of distinct types, called the ***isotypic components*** of V. The isotypic component of V corresponding to a simple module S is the sum of all simple submodules of V isomorphic to S. From this description, we see that a homomorphism $V \to V'$ of semisimple A-modules maps each isotypic component of V into the isotypic component of V' of the same type.

PROPOSITION 7.15 *Let V be a semisimple A-module. A submodule of V is stable under all endomorphisms of V if and only if it is a sum of isotypic components of V.*

PROOF. The sufficiency follows from the above statement. For the necessity, let W be a submodule of V stable under all endomorphisms of V, and let S be a simple submodule of W. If S' is a submodule of V isomorphic to S, then the endomorphism

$$V \xrightarrow{\text{project}} S \xrightarrow{\approx} S' \hookrightarrow V$$

of V maps W into W, and so $S' \subset W$. Therefore W contains the isotypic component of V containing S. □

7.16 Let A be an F-algebra, and let ${}_AA$ denote A regarded as a left A-module. Right multiplication $x \mapsto xa$ on ${}_AA$ by an element a of A is an A-linear endomorphism of ${}_AA$. Moreover, every A-linear map $\varphi\colon {}_AA \to {}_AA$ is of this form with $a = \varphi(1)$. Thus, $\mathrm{End}_A({}_AA) \simeq A$ as F-vector spaces. Let φ_a be the map $x \mapsto xa$. Then

$$(\varphi_a \circ \varphi_{a'})(1) \overset{\text{def}}{=} \varphi_a(\varphi_{a'}(1)) = \varphi_a(a') = a'a = \varphi_{a'a}(1),$$

and so

$$\mathrm{End}_A({}_AA) \simeq A^{\mathrm{opp}} \quad \text{(as } F\text{-algebras).}$$

More generally, $\mathrm{End}_A(V) \simeq A^{\mathrm{opp}}$ for any A-module V that is free of rank 1, and

$$\mathrm{End}_A(V) \simeq M_n(A^{\mathrm{opp}})$$

for any free A-module V of rank n (cf. 7.34 below).

An F-algebra A is said to be ***semisimple*** if every A-module is semisimple. Since every A-module is a quotient of a direct sum of copies of ${}_AA$, for this it suffices to check that the A-module ${}_AA$ is semisimple.

PROPOSITION 7.17 *Let A be a semisimple F-algebra. The isotypic components of the A-module ${}_AA$ are the minimal two-sided ideals of A. Every two-sided ideal of A is a direct sum of minimal two-sided ideals.*

PROOF. The two-sided ideals of A are the submodules of ${}_AA$ stable under right multiplication by the elements of A, i.e., by the endomorphisms of ${}_AA$ (7.16), and so they are the sums of isotypic components of ${}_AA$ (7.15). In particular, the minimal two-sided ideals are exactly the isotypic components of ${}_AA$. The second statement is obvious from the above discussion. □

Simple F-algebras and their modules

An F-algebra A is said to be ***simple*** if it contains no two-sided ideals except 0 and A. We shall make frequent use of the following observation:

> The kernel of a homomorphism $f\colon A \to B$ of F-algebras is an ideal in A not containing 1; therefore, if A is simple, then f is injective.

EXAMPLE 7.18 An F-algebra is said to be a ***division algebra*** if every nonzero element a has an inverse, i.e., there exists a b such that $ab = 1 = ba$. Thus a division algebra satisfies all the axioms to be a field except commutativity (and for this reason is sometimes called a ***skew field***). Clearly, a division algebra has no nonzero proper ideals, left, right, or two-sided, and so is simple.

Much of linear algebra does not require that the field be commutative. For example, the usual arguments show that a finitely generated module V over a division algebra D has a basis, and that all bases have the same number n of elements — n is called the ***dimension*** of V. In particular, all finitely generated D-modules are free.

EXAMPLE 7.19 Let D be a division algebra over F, and consider the matrix algebra $M_n(D)$. Let e_{ij} be the matrix with 1 in the (i,j)th position and zeros elsewhere.

(a) Let I be a two-sided ideal in $M_n(D)$, and suppose that I contains a nonzero matrix $M = (m_{ij})$ with, say, $m_{i_0 j_0} \neq 0$. As

$$e_{ii_0} \cdot M \cdot e_{j_0 j} = m_{i_0 j_0} e_{ij}$$

and $e_{ii_0} \cdot M \cdot e_{j_0 j} \in I$, we see that I contains all the matrices e_{ij} and so equals $M_n(D)$. We have shown that $M_n(D)$ is simple.

(b) For $M, N \in M_n(D)$, the jth column of $M \cdot N$ is $M \cdot N_j$, where N_j is the jth column of N. Therefore, for a given matrix N,

$$\begin{cases} N_j = 0 & \Rightarrow \quad (M \cdot N)_j = 0 \\ N_j \neq 0 & \Rightarrow \quad (M \cdot N)_j \text{ can be arbitrary.} \end{cases} \tag{30}$$

For $1 \leq i \leq n$, let $L(i)$ be the set of matrices whose jth columns are zero for $j \neq i$ and whose ith column is arbitrary. For example, when $n = 4$,

$$L(3) = \left\{ \begin{pmatrix} 0 & 0 & * & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & * & 0 \end{pmatrix} \right\} \subset M_4(D).$$

It follows from (30) that $L(i)$ is a minimal left ideal in $M_n(D)$. Note that $M_n(D)$ is a direct sum

$$M_n(D) = L(1) \oplus \cdots \oplus L(n)$$

of minimal left ideals.

EXAMPLE 7.20 For $a, b \in F^\times$, let $H(a,b)$ be the F-algebra with basis $\{1, i, j, k\}$ (as an F-vector space) and with the multiplication determined by

$$i^2 = a, \quad j^2 = b, \quad ij = k = -ji$$

(so $ik = iij = aj$ etc.). Then $H(a,b)$ is an F-algebra, called a ***quaternion algebra*** over F. For example, if $F = \mathbb{R}$, then $H(-1,-1)$ is the usual quaternion algebra. One can show that $H(a,b)$ is either a division algebra or it is isomorphic to $M_2(F)$. In particular, it is simple.

CENTRALIZERS

Let A be an F-subalgebra of an F-algebra B. The ***centralizer of A in B*** is

$$C_B(A) = \{b \in B \mid ba = ab \text{ for all } a \in A\}.$$

It is again an F-subalgebra of B.

EXAMPLE 7.21 In the following examples, the centralizers are taken in $M_n(F)$.

(a) Let A be the set of scalar matrices in $M_n(F)$, i.e., $A = F \cdot I_n$. Clearly, $C(A) = M_n(F)$.

(b) Let $A = M_n(F)$. Then $C(A)$ is the centre of $M_n(F)$, which we now compute. Let e_{ij} be the matrix with 1 in the (i,j)th position and zeros elsewhere, so that

$$e_{ij}e_{lm} = \begin{cases} e_{im} & \text{if } j = l \\ 0 & \text{if } j \neq l. \end{cases}$$

Let $\alpha = (a_{ij}) \in M_n(F)$. Then $\alpha = \sum_{i,j} a_{ij}e_{ij}$, and so $\alpha e_{lm} = \sum_i a_{il}e_{im}$ and $e_{lm}\alpha = \sum_j a_{mj}e_{lj}$. If α is in the centre of $M_n(F)$, then $\alpha e_{lm} = e_{lm}\alpha$, and so $a_{il} = 0$ for $i \neq l$, $a_{mj} = 0$ for $j \neq m$, and $a_{ll} = a_{mm}$. It follows that the centre of $M_n(F)$ is set of scalar matrices $F \cdot I_n$. Thus $C(A) = F \cdot I_n$.

(c) Let A be the set of diagonal matrices in $M_n(F)$. In this case, $C(A) = A$.

Notice that in all three cases, $C(C(A)) = A$.

THEOREM 7.22 (DOUBLE CENTRALIZER THEOREM) *Let A be an F-algebra, and let V be a faithful semisimple A-module. Then $C(C(A)) = A$ (centralizers taken in* $\mathrm{End}_F(V)$*).*

PROOF. Let $D = C(A)$ and let $B = C(D)$. Clearly $A \subset B$, and the reverse inclusion follows from the next lemma when we take $v_1, \ldots, v_n$ to generate V as a F-vector space. □

LEMMA 7.23 *For any $v_1, \ldots, v_n \in V$ and $b \in B$, there exists an $a \in A$ such that*

$$av_1 = bv_1, \quad av_2 = bv_2, \quad \ldots, \quad av_n = bv_n.$$

PROOF. We first prove this for $n = 1$. Note that Av_1 is an A-submodule of V, and so (see 7.13) there exists an A-submodule W of V such that $V = Av_1 \oplus W$. Let $\pi: V \to V$ be the map $(av_1, w) \mapsto (av_1, 0)$ (projection onto Av_1). It is A-linear, hence lies in D, and has the property that $\pi(v) = v$ if and only if $v \in Av_1$. Now

$$\pi(bv_1) = b(\pi v_1) = bv_1,$$

and so $bv_1 \in Av_1$, as required.

We now prove the general case. Let W be the direct sum of n copies of V with A acting diagonally, i.e.,

$$a(v_1, \ldots, v_n) = (av_1, \ldots, av_n), \quad a \in A, \quad v_i \in V.$$

Then W is again a semisimple A-module (7.14). The centralizer of A in $\mathrm{End}_F(W)$ consists of the matrices $(\gamma_{ij})_{1 \le i,j \le n}$, $\gamma_{ij} \in \mathrm{End}_F(V)$, such that $(\gamma_{ij} a) = (a\gamma_{ij})$ for all $a \in A$, i.e., such that $\gamma_{ij} \in D$ (cf. 7.34). In other words, the centralizer of A in $\mathrm{End}_F(W)$ is $M_n(D)$. An argument as in Example 7.21(b), using the matrices $e_{ij}(\delta)$ with δ in the ijth position and zeros elsewhere, shows that the centralizer of $M_n(D)$ in $\mathrm{End}_F(W)$ consists of the diagonal matrices

$$\begin{pmatrix} \beta & 0 & \cdots & 0 \\ 0 & \beta & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \beta \end{pmatrix}$$

with $\beta \in B$. We now apply the case $n = 1$ of the lemma to A, W, b, and the vector $(v_1, \ldots, v_n)$ to complete the proof. □

LEMMA 7.24 (SCHUR'S LEMMA) *For every F-algebra A and simple A-module S, $\mathrm{End}_A(S)$ is a division algebra.*

PROOF. Let γ be an A-linear map $S \to S$. Then $\mathrm{Ker}(\gamma)$ is an A-submodule of S, and so it is either S or 0. In the first case, γ is zero, and in the second it is an isomorphism, which means that it has an inverse that is also A-linear. □

THEOREM 7.25 *Every simple F-algebra is isomorphic to $M_n(D)$ for some n and some division F-algebra D.*

PROOF. Choose a simple A-module S, for example, any minimal left ideal of A. Then A acts faithfully on S, because the kernel of $A \to \mathrm{End}_F(S)$ is a two-sided ideal of A not containing 1, and hence is 0.

Let D be the centralizer of A in the F-algebra $\mathrm{End}_F(S)$ of F-linear maps $S \to S$. According to the double centralizer theorem (7.22), the centralizer of D in $\mathrm{End}_F(S)$ is A, i.e., $A = \mathrm{End}_D(S)$. Schur's lemma (7.24) implies that D is a division algebra. Therefore S is a free D-module (7.18), say, $S \approx D^n$, and so $\mathrm{End}_D(S) \approx M_n(D^{\mathrm{opp}})$ (see 7.16). □

Modules over simple F-algebras

Let A be an F-algebra. The submodules of ${}_AA$ are the left ideals in A, and the simple submodules of ${}_AA$ are the minimal left ideals.

Proposition 7.26 *Every simple F-algebra A is semisimple.*

Proof. It suffices to show that the A-module ${}_AA$ is semisimple. After Theorem 7.25, we may assume that $A = M_n(D)$ for some division algebra D. We saw in 7.19 that the sets $L(i)$ are minimal left ideals in $M_n(D)$, and that $M_n(D) = L(1) \oplus \cdots \oplus L(n)$ as an $M_n(D)$-module. This shows that ${}_AA$ is semisimple. □

Theorem 7.27 *Let A be a semisimple F-algebra. The following conditions on A are equivalent:*

(a) *A is simple;*
(b) *the A-module ${}_AA$ is isotypic;*
(c) *any two simple A-modules are isomorphic.*

Proof. The equivalence of (a) and (b) follows from Proposition 7.17, and (c) obviously implies (b). Finally (b) implies (c) because, if ${}_AA$ is isotypic, so also is a direct sum of copies of ${}_AA$, and every A-module is a quotient of such a direct sum. □

Corollary 7.28 *Let A be a simple F-algebra. Any two minimal left ideals of A are isomorphic as left A-modules, and A is a direct sum of its minimal left ideals.*

Proof. Minimal left ideals are simple A-modules, and so the first statement follows from (c) of the theorem. The second statement was proved in the proof of 7.26. □

Corollary 7.29 *Let A be a simple F-algebra, and let S be a simple A-module. Every A-module is isomorphic to a direct sum of copies of S. Any two A-modules having the same dimension over F are isomorphic.*

Proof. As A is semisimple, the first assertion follows from (c) of the theorem, and the second assertion follows from the first. □

Corollary 7.30 *The integer n in Theorem 7.25 is uniquely determined by A, and D is uniquely determined up to isomorphism.*

Proof. If $A \approx M_n(D)$, then $D^{\text{opp}} \approx \text{End}_A(S)$ for any simple A-module S, and n is the dimension of S as a D-vector space. Since any two simple A-modules are isomorphic (7.27), this implies the statement. □

Classification of the division algebras over F

After Theorem 7.25, to classify the simple algebras over F, it remains to classify the division algebras over F.

Proposition 7.31 *The only division algebra over an algebraically closed field F is F itself.*

Proof. Let D be division algebra over F. For any element α of D, the F-subalgebra $F[\alpha]$ of D generated by α is a field because it is an integral domain of finite degree over F. As F is algebraically closed, $\alpha \in F$. □

7.32 The classification of the isomorphism classes of division algebras over a field F is one the most difficult and interesting problems in algebra and number theory. It is well beyond the scope of these notes.

For $F = \mathbb{R}$, the only division algebra $\neq \mathbb{R}$ is the usual quaternion algebra (7.20). All finite division algebras are commutative (theorem of Wedderburn).

A division algebra over F is said to be ***central*** if its centre is F. Brauer showed that the set of isomorphism classes of central division algebras over a field F can be made into a group, now called the ***Brauer group*** of F. The tensor product $D \otimes_F D'$ of two central simple algebras over F is again a central simple algebra over F, and hence is isomorphic to $M_r(D'')$ for some central simple algebra D''. Define

$$[D][D'] = [D''].$$

This product is associative because of the associativity of tensor products, the isomorphism class of F is an identity element, and $[D^{\mathrm{opp}}]$ is an inverse for $[D]$. The above remarks show that the Brauer group is zero if F is algebraically closed or finite, and of order 2 if $F = \mathbb{R}$. The Brauer groups of $\mathbb{Q}$ and its finite extensions were computed by Albert, Brauer, Hasse, and Noether in the 1930s as part of class field theory (see CFT).

Semisimple F-algebras and their modules

Recall that an F-algebra A is said to be semisimple if every A-module is semisimple. Simple F-algebras are semisimple (7.26), and Maschke's theorem shows that the group algebra $F[G]$ is semisimple when the order of G is not divisible by the characteristic of F (see 7.9).

EXAMPLE 7.33 Let A be a finite product of simple F-algebras. Every minimal left ideal of a simple factor of A is a simple A-submodule of ${}_AA$. Therefore, ${}_AA$ is a sum of simple A-modules, and so is semisimple. Since every A-module is a quotient of a direct sum of copies of ${}_AA$, this shows that A is semisimple.

Before stating the main result of this section, we recall some elementary module theory.

7.34 Let A be an F-algebra, and consider modules

$$\begin{aligned} M &= M_1 \oplus \cdots \oplus M_n \\ N &= N_1 \oplus \cdots \oplus N_m. \end{aligned}$$

Let α be an A-linear map $M \to N$. For $x_j \in M_j$, let

$$\alpha(0,\ldots,0,x_j,0,\ldots,0) = (y_1,\ldots,y_m).$$

Then $x_j \mapsto y_i$ is an A-linear map $M_j \to N_i$, which we denote α_{ij}. Thus, α defines an $m \times n$ matrix whose ijth coefficient is an A-linear map $M_j \to N_i$. Conversely, every such matrix (α_{ij}) defines an A-linear map $M \to N$, namely,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1j} & \cdots & \alpha_{1n} \\ \vdots & & \vdots & & \vdots \\ \alpha_{i1} & \cdots & \alpha_{ij} & \cdots & \alpha_{jn} \\ \vdots & & \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mj} & \cdots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} \overset{\mathrm{def}}{=} \begin{pmatrix} \alpha_{11}(x_1) + \cdots + \alpha_{1n}(x_n) \\ \vdots \\ \alpha_{i1}(x_1) + \cdots + \alpha_{in}(x_n) \\ \vdots \\ \alpha_{m1}(x_1) + \cdots + \alpha_{mn}(x_n) \end{pmatrix}.$$

Thus, we see

$$\mathrm{Hom}_A(M,N) \simeq \left(\mathrm{Hom}_A(M_j,N_i)\right)_{1\le j\le n,\, 1\le i\le m} \tag{31}$$

(isomorphism of F-vector spaces). When $M = N$, this becomes an isomorphism of F-algebras. For example, if M is a direct sum of m copies of M_0, then

$$\mathrm{End}_A(M) \simeq M_m(\mathrm{End}_A(M_0)) \tag{32}$$

($m \times m$ matrices with coefficients in the ring $\mathrm{End}_A(M_0)$).

THEOREM 7.35 *Let V be a finite-dimensional F-vector space and A an F-subalgebra of* $\mathrm{End}_F(V)$*. If V is semisimple as an A-module, then the centralizer of A in* $\mathrm{End}_F(V)$ *is a product of simple F-algebras (hence it is a semisimple F-algebra).*

PROOF. By assumption, we can write $V \approx \bigoplus_i r_i S_i$, where the S_i are simple A-modules, no two of which are isomorphic. The centralizer of A in $\mathrm{End}_F(V)$ is $\mathrm{End}_A(V)$, and $\mathrm{End}_A(V) \approx \mathrm{End}_A(\bigoplus_i r_i S_i)$. Because $\mathrm{Hom}_A(S_j,S_i) = 0$ for $i \neq j$,

$$\begin{aligned}\mathrm{End}_A(\textstyle\bigoplus r_i S_i) &\simeq \textstyle\prod_i \mathrm{End}_A(r_i S_i) \quad \text{by (31)}\\ &\simeq \textstyle\prod_i M_{r_i}(D_i) \quad \text{by (32)}\end{aligned}$$

where $D_i = \mathrm{End}_A(S_i)$. According to Schur's lemma (7.24), D_i is a division algebra, and therefore $M_{r_i}(D_i)$ is a simple F-algebra (7.19). □

THEOREM 7.36 *Every semisimple F-algebra is isomorphic to a product of simple F-algebras.*

PROOF. Choose an A-module V on which A acts faithfully, for example, $V = {}_AA$. Then A is equal to its double centralizer $C(C(A))$ in $\mathrm{End}_F(V)$ (see 7.22). According to Theorem 7.35, $C(A)$ is semisimple, and so $C(C(A))$ is a product of simple algebras. □

Modules over a semisimple F-algebra

Let $A = B \times C$ be a product of F-algebras. A B-module M becomes an A-module with the action $(b,c)m = bm$.

THEOREM 7.37 *Let A be a semisimple F-algebra, say, $A = A_1 \times \cdots \times A_t$ with the A_i simple. For each A_i, let S_i be a simple A_i-module (cf. 7.29).*

(a) *Each S_i is a simple A-module, and every simple A-module is isomorphic to exactly one of the S_i.*

(b) *Every A-module is isomorphic to $\bigoplus r_i S_i$ for some $r_i \in \mathbb{N}$, and two modules $\bigoplus r_i S_i$ and $\bigoplus r_i' S_i$ are isomorphic if and only if $r_i = r_i'$ for all i.*

PROOF. (a) It is obvious that each S_i is simple when regarded as an A-module, and that no two of them are isomorphic. It follows from 7.28 that ${}_AA \approx \bigoplus r_i S_i$ for some $r_i \in \mathbb{N}$. Let S be a simple A-module, and let x be a nonzero element of S. Then the map $a \mapsto ax: {}_AA \to S$ is surjective, and so its restriction to some S_i in ${}_AA$ is nonzero, and hence an isomorphism.

(b) The first part follows from (a) and the definition of a semisimple ring, and the second part follows from 7.11. □

The representations of G

PROPOSITION 7.38 *The dimension of the centre of $F[G]$ as an F-vector space is the number of conjugacy classes in G.*

PROOF. Let $C_1,\ldots,C_t$ be the conjugacy classes in G, and, for each i, let c_i be the element $\sum_{a\in C_i} a$ in $F[G]$. We shall prove the stronger statement,

$$\text{centre of } F[G] = Fc_1 \oplus \cdots \oplus Fc_t \tag{33}$$

As $c_1,\ldots,c_t$ are obviously linearly independent, it suffices to show that they span the centre.

For any $g\in G$ and $\sum_{a\in G} m_a a \in F[G]$,

$$g\left(\sum\nolimits_{a\in G} m_a a\right) g^{-1} = \sum\nolimits_{a\in G} m_a gag^{-1}.$$

The coefficient of a in the right hand sum is $m_{g^{-1}ag}$, and so

$$g\left(\sum\nolimits_{a\in G} m_a a\right) g^{-1} = \sum\nolimits_{a\in G} m_{g^{-1}ag} a.$$

This shows that $\sum_{a\in G} m_a a$ lies in the centre of $F[G]$ if and only if the function $a\mapsto m_a$ is constant on conjugacy classes, i.e., if and only if $\sum_{a\in G} m_a a \in \sum_i Fc_i$. □

REMARK 7.39 An element $\sum_{a\in G} m_a a$ of $F[G]$ can be regarded as a map $a\mapsto m_a\colon G\to F$. In this way, $F[G]\simeq \mathrm{Map}(G,F)$. The action of G on $F[G]$ corresponds to the action $(gf)(a) = f(g^{-1}a)$ of $g\in G$ on $f\colon G\to F$. In the above proof, we showed that the elements of the centre of $F[G]$ correspond exactly to the functions $f\colon G\to F$ that are constant on each conjugacy class. Such functions are called ***class functions***.

In the remainder of this chapter, we assume that F is an algebraically closed field of characteristic zero (e.g., $\mathbb{C}$)

PROPOSITION 7.40 *The group algebra $F[G]$ is isomorphic to a product of matrix algebras over F.*

PROOF. Recall that, when F has characteristic zero, Maschke's theorem (7.9) implies that $F[G]$ is semisimple, and so is a product of simple algebras (7.36). Each of these is a matrix algebra over a division algebra (7.25), but the only division algebra over an algebraically closed field is the field itself (7.31). □

The representation $G\to \mathrm{GL}({}_{F[G]}F[G])$ is called the ***regular representation***.

THEOREM 7.41 *(a) The number of isomorphism classes of simple $F[G]$-modules is equal to the number of conjugacy classes in G.*

(b) The multiplicity of any simple representation S in the regular representation is equal to its degree $\dim_F S$.

(c) Let $S_1,\ldots,S_t$ be a set of representatives for the isomorphism classes of simple $F[G]$-modules, and let $f_i = \dim_F S_i$. Then

$$\sum_{1\le i\le t} f_i^2 = |G|.$$

PROOF. (a) Under our hypothesis, $F[G] \approx M_{f_1}(F) \times \cdots \times M_{f_t}(F)$ for some integers $f_1, \ldots, f_t$. According to Theorem 7.37, the number of isomorphism classes of simple $F[G]$-modules is the number of factors t. The centre of a product of F-algebras is the product of their centres, and so the centre of $F[G]$ is isomorphic to tF. Therefore t is the dimension of the centre of F, which we know equals the number of conjugacy classes of G.

(b) With the notation of 7.19, $M_f(F) \simeq L(1) \oplus \cdots \oplus L(f)$.

(c) The equality is simply the statement

$$\sum_{1 \leq i \leq t} \dim_F M_{f_i}(F) = \dim_F F[G].$$

□

The characters of G

Recall that the trace $\mathrm{Tr}_V(\alpha)$ of an endomorphism $\alpha\colon V \to V$ of a vector space V is $\sum a_{ii}$, where (a_{ij}) is the matrix of α with respect to some basis for V. It is independent of the choice of the basis (conjugate matrices have the same trace).

From each representation of $g \mapsto g_V\colon G \to \mathrm{GL}(V)$, we obtain a function χ_V on G,

$$\chi_V(g) = \mathrm{Tr}_V(g_V),$$

called the ***character*** of ρ. Note that χ_V depends only on the isomorphism class of the $F[G]$-module V, and that χ_V is a class function. The character χ is said to be ***simple*** (or ***irreducible***) if it is defined by a simple $F[G]$-module. The ***principal character*** χ_1 is that defined by the trivial representation of G (so $\chi_1(g) = 1$ for all $g \in G$), and the ***regular character*** χ_{reg} is that defined by the regular representation. On computing $\chi_{\mathrm{reg}}(g)$ by using the elements of G as a basis for $F[G]$, one see that $\chi_{\mathrm{reg}}(g)$ is the number of elements a of G such that $ga = a$, and so

$$\chi_{\mathrm{reg}}(g) = \begin{cases} |G| & \text{if } g = e \\ 0 & \text{otherwise.} \end{cases}$$

When V has dimension 1, the character χ_V of ρ is said to be ***linear***. In this case, $\mathrm{GL}(V) \simeq F^\times$, and so $\chi_V(g) = \rho(g)$. Therefore, χ_V is a homomorphism $G \to F^\times$, and so this definition of "linear character" essentially agrees with the earlier one.

LEMMA 7.42 *For all $F[G]$-modules V and V',*

$$\chi_{V \oplus V'} = \chi_V + \chi_{V'}.$$

PROOF. Compute the matrix of $g_{V \oplus V'}$ with respect to a basis of $V \oplus V'$ that is the union of a basis for V with a basis for V'. □

Let $S_1, \ldots, S_t$ be a set of representatives for the isomorphism classes of simple $F[G]$-modules with S_1 chosen to be the trivial representation, and let $\chi_1, \ldots, \chi_t$ be the corresponding characters.

PROPOSITION 7.43 *The functions $\chi_1, \ldots, \chi_t$ are linearly independent over F, i.e., if $c_1, \ldots, c_t \in F$ are such that $\sum_i c_i \chi_i(g) = 0$ for all $g \in G$, then the c_i are all zero.*

PROOF. Write $F[G] \approx M_{f_1}(F) \times \cdots \times M_{f_t}(F)$, and let $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$. Then e_j acts as 1 on S_j and as 0 on S_i for $i \neq j$, and so

$$\chi_i(e_j) = \begin{cases} f_j = \dim_F S_j & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases} \tag{34}$$

Therefore,

$$\sum\nolimits_i c_i \chi_i(e_j) = c_j f_j,$$

from which the claim follows. □

PROPOSITION 7.44 *Two $F[G]$-modules are isomorphic if and only if their characters are equal.*

PROOF. We have already observed that the character of a representation depends only on its isomorphism class. Conversely, if $V = \bigoplus_{1 \leq i \leq t} c_i S_i$, $c_i \in \mathbb{N}$, then its character is $\chi_V = \sum_{1 \leq i \leq t} c_i \chi_i$, and (34) shows that $c_i = \chi_V(e_i)/f_i$. Therefore χ_V determines the multiplicity with which each S_i occurs in V, and hence it determines the isomorphism class of V. □

ASIDE 7.45 The proposition is false if F is allowed to have characteristic $p \neq 0$. For example, the representation $\sigma^i \mapsto \left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right) : C_p \to \mathrm{GL}_2(F)$ of (7.1c) is not trivial, but it has the same character as the trivial representation. The proposition is false even when the characteristic of F doesn't divide the order of the group, because, for any representation $G \to \mathrm{GL}(V)$, the character of the representation of G on pV is identically zero. However, a theorem of Brauer and Nesbitt says that if F has characteristic zero, A is an F-algebra, and ρ_1 and ρ_2 are semisimple representations of A such that $\rho_1(a)$ and $\rho_2(a)$ have the same characteristic polynomials for all $a \in A$, then the representations are isomorphic.

Any function $G \to F$ that can be expressed as a $\mathbb{Z}$-linear combination of characters is called a ***virtual character***.[1]

PROPOSITION 7.46 *The simple characters of G form a $\mathbb{Z}$-basis for the virtual characters of G.*

PROOF. Let $\chi_1, \ldots, \chi_t$ be the simple characters of G. Then the characters of G are exactly the class functions that can be expressed in the form $\sum m_i \chi_i$, $m_i \in \mathbb{N}$, and so the virtual characters are exactly the class functions that can be expressed $\sum m_i \chi_i$, $m_i \in \mathbb{Z}$. Therefore the simple characters certainly generate the $\mathbb{Z}$-module of virtual characters, and Proposition 7.43 shows that they are linearly independent over $\mathbb{Z}$ (even over F). □

PROPOSITION 7.47 *The simple characters of G form an F-basis for the class functions on G.*

PROOF. The class functions are the functions from the set of conjugacy classes in G to F. As this set has t elements, they form an F-vector space of dimension t. As the simple characters are a set of t linearly independent elements of this vector space, they must form a basis. □

[1] Some authors call it a generalized character, but this is to be avoided: there is more than one way to generalize the notion of a character.

We now assume that F is a subfield of $\mathbb{C}$ stable under complex conjugation $c \mapsto \bar{c}$.

For class functions f_1 and f_2 on G, define

$$(f_1|f_2) = \frac{1}{|G|}\sum_{a\in G} f_1(a)\overline{f_2(a)}.$$

LEMMA 7.48 *The pairing $(\,|\,)$ is an inner product on the F-space of class functions on G.*

PROOF. We have to check:

- ◇ $(f_1+f_2|f) = (f_1|f)+(f_2|f)$ for all class functions f_1, f_2, f;
- ◇ $(cf_1|f_2) = c(f_1, f_2)$ for $c \in F$ and class functions f_1, f_2;
- ◇ $(f_2|f_1) = \overline{(f_1|f_2)}$ for all class functions f_1, f_2;
- ◇ $(f|f) > 0$ for all nonzero class functions f.

All of these are obvious from the definition. □

For an $F[G]$-module V, we let V^G denote the submodule of elements fixed by G,

$$V^G = \{v \in V \mid gv = v \text{ for all } g \in G\}.$$

LEMMA 7.49 *Let π be the element $\frac{1}{|G|}\sum_{a\in G} a$ of $F[G]$. For any $F[G]$-module V, π_V is a projector with image V^G.*

PROOF. For any $g \in G$,

$$g\pi = \frac{1}{|G|}\sum_{a\in G} ga = \frac{1}{|G|}\sum_{a\in G} a = \pi, \tag{35}$$

from which it follows that $\pi\pi = \pi$ (in the F-algebra $F[G]$). Therefore, for any $F[G]$-module V, $\pi_V^2 = \pi_V$ and so π_V is a projector. If v is in its image, say $v = \pi v_0$, then

$$gv = g\pi v_0 \overset{(35)}{=} \pi v_0 = v$$

and so v lies in V^G. Conversely, if $v \in V^G$, then obviously $\pi v = \frac{1}{|G|}\sum_{a\in G} av = v$, and so v is in the image of π. □

PROPOSITION 7.50 *For any $F[G]$-module V,*

$$\dim_F V^G = \frac{1}{|G|}\sum_{a\in G}\chi_V(a).$$

PROOF. Let π be as in Lemma 7.49. Because π_V is a projector, V is the direct sum of its 0-eigenspace and its 1-eigenspace, and we showed that the latter is V^G. Therefore, $\mathrm{Tr}_V(\pi_V) = \dim_F V^G$. On the other hand, because the trace is a linear function,

$$\mathrm{Tr}_V(\pi_V) = \frac{1}{|G|}\sum_{a\in G}\mathrm{Tr}_V(a_V) = \frac{1}{|G|}\sum_{a\in G}\chi_V(a).$$

□

THEOREM 7.51 *For any $F[G]$-modules V and W,*

$$\dim_F \mathrm{Hom}_{F[G]}(V,W) = (\chi_V|\chi_W).$$

PROOF. The group G acts on the space $\mathrm{Hom}_F(V,W)$ of F-linear maps $V \to W$ by the rule,

$$(g\varphi)(v) = g(\varphi(g^{-1}v)), \quad g \in G, \quad \varphi \in \mathrm{Hom}_F(V,W), \quad v \in V,$$

and $\mathrm{Hom}_F(V,W)^G = \mathrm{Hom}_{F[G]}(V,W)$. □

COROLLARY 7.52 *If χ and χ' are simple characters, then*

$$(\chi|\chi') = \begin{cases} 1 & \text{if } \chi = \chi' \\ 0 & \text{otherwise.} \end{cases}$$

Therefore the simple characters form an orthonormal basis for the space of class functions on G.

The character table of a group

To be written.

Examples

To be written.

Exercises

7-1 Let C be an $n \times r$ matrix with coefficients in a field F. Show that

$$\{M \in M_n(F) \mid MC = 0\}$$

is a left ideal in $M_n(F)$, and that every left ideal is of this form for some C.

7-2 This exercise shows how to recover a finite group G from its category of representations over a field k. Let S be a finite set, and let A be the set of maps $S \to k$.

(a) Show that A becomes a commutative ring with the product

$$(f_1 f_2)(g) = f_1(g) f_2(g), \quad f_1, f_2 \in A, \quad g \in S.$$

Moreover, when we identify $c \in k$ with the constant function, A becomes a k-algebra.

(b) Show that

$$A \simeq \prod\nolimits_{s \in S} k_s \qquad \text{(product of copies of } k \text{ indexed by the elements of } S\text{)},$$

and that the k_s are exactly the minimal k-subalgebras of A. Deduce that $\mathrm{End}_{k\text{-alg}}(A) \simeq \mathrm{Sym}(S)$.

(c) Let $(f_1, f_2) \in A \times A$ act on $S \times S$ by $(f_1, f_2)(s_1, s_2) = f_1(s_1) f_2(s_2)$; show that this defines a bijection $A \otimes A \simeq \mathrm{Map}(S \times S, k)$. Now take $S = G$.

(d) Show that the map $r_A\colon G \to \mathrm{End}_{k\text{-linear}}(A)$,

$$(r_A(g)f)(g') = f(gg'), \quad f \in A, \quad g, g' \in G$$

is a representation of G (this is the regular representation).

(e) Define $\Delta: A \to A \otimes A$ by $\Delta(f)(g_1, g_2) = f(g_1 g_2)$. Show that, for any homomorphism $\alpha: A \to A$ of k-algebras such $(1 \otimes \alpha) \circ \Delta = \Delta \circ \alpha$, there exists a unique element $g \in G$ such that $\alpha(f) = gf$ for all $f \in A$. [Hint: Deduce from (b) that there exists a bijection $\phi: G \to G$ such that $(\alpha f)(g) = f(\phi g)$ for all $g \in G$. From the hypothesis on α, deduce that $\phi(g_1 g_2) = g_1 \cdot \phi(g_2)$ for all $g_1, g_2 \in G(R)$. Hence $\phi(g) = g \cdot \phi(e)$ for all $g \in G$. Deduce that $\alpha(f) = \phi(e) f$ for all $f \in A$.]

(f) Show that the following maps are G-equivariant

$$\begin{array}{ll} e{:}k \to A & \text{(trivial representation on } k\text{; } r_A \text{ on } A\text{)} \\ m{:}A \otimes A \to A & (r_A \otimes r_A \text{ on } A \otimes A\text{; } r_A \text{ on } A) \\ \Delta{:}A \to A \otimes A & (r_A \text{ on } A\text{; } 1 \otimes r_A \text{ on } A \otimes A). \end{array}$$

(g) Suppose that we are given, for each finite-dimensional representation (V, r_V), a k-linear map λ_V. If the family (λ_V) satisfies the conditions

i) for all representations V, W, $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$;

ii) for k with its trivial representation, $\lambda_k = \mathrm{id}_k$;

iii) for all G-equivariant maps $\alpha: V \to W$, $\lambda_W \circ \alpha = \alpha \circ \lambda_V$;

then there exists a unique $g \in G(R)$ such that $\lambda_V = r_V(g)$ for all V. [Hint: show that λ_A satisfies the conditions of (d).]

NOTES For a historical account of the representation theory of finite groups, emphasizing the work of “the four principal contributors to the theory in its formative stages: Ferdinand Georg Frobenius, William Burnside, Issai Schur, and Richard Brauer”, see Curtis 1999.

> At a time when many physicists were considering giving up on even the possibility of developing an understanding of particle physics using the techniques that had worked so well with QED, Gell-Mann, in 1961, discovered the importance of group theory, which gave him a mathematical tool to classify the plethora of new elementary particles according to their symmetry properties.... In Gell-Mann’s scheme ..., the different particles fell into sets of representations whose properties ... could be graphed so that they formed the vertices of a polyhedron, and all of the particles in each polyhedron could then be transformed into each other by symmetries, which could effectively rotate the polyhedron in different directions.
>
> Lawrence Krauss, *Quantum Man*, p. 288

Appendix A

Additional Exercises

34. Prove that a finite group G having just one maximal subgroup must be a cyclic p-group, p prime.

35. Let a and b be two elements of S_{76}. If a and b both have order 146 and $ab = ba$, what are the possible orders of the product ab?

37. Suppose that the group G is generated by a set X.

(a) Show that if $gxg^{-1} \in X$ for all $x \in X$, $g \in G$, then the commutator subgroup of G is generated by the set of all elements $xyx^{-1}y^{-1}$ for $x, y \in X$.
(b) Show that if $x^2 = 1$ for all $x \in X$, then the subgroup H of G generated by the set of all elements xy for $x, y \in X$ has index 1 or 2.

38. Suppose $p \geq 3$ and $2p-1$ are both prime numbers (e.g., $p = 3, 7, 19, 31, \ldots$). Prove, or disprove by example, that every group of order $p(2p-1)$ is commutative.

39. Let H be a subgroup of a group G. Prove or disprove the following:

(a) If G is finite and P is a Sylow p-subgroup, then $H \cap P$ is a Sylow p-subgroup of H.
(b) If G is finite, P is a Sylow p-subgroup, and $H \supset N_G(P)$, then $N_G(H) = H$.
(c) If g is an element of G such that $gHg^{-1} \subset H$, then $g \in N_G(H)$.

40. Prove that there is no simple group of order 616.

41. Let n and k be integers $1 \leq k \leq n$. Let H be the subgroup of S_n generated by the cycle $(a_1 \ldots a_k)$. Find the order of the centralizer of H in S_n. Then find the order of the normalizer of H in S_n. [The ***centralizer*** of H is the set of $g \in G$ such $ghg^{-1} = h$ for all $h \in H$. It is again a subgroup of G.]

42. Prove or disprove the following statement: if H is a subgroup of an infinite group G, then for all $x \in G$, $xHx^{-1} \subset H \implies x^{-1}Hx \subset H$.

43. Let H be a finite normal subgroup of a group G, and let g be an element of G. Suppose that g has order n and that the only element of H that commutes with g is 1. Show that:

(a) the mapping $h \mapsto g^{-1}h^{-1}gh$ is a bijection from H to H;
(b) the coset gH consists of elements of G of order n.

44. Show that if a permutation in a subgroup G of S_n maps x to y, then the normalizers of the stabilizers $\mathrm{Stab}(x)$ and $\mathrm{Stab}(y)$ of x and y have the same order.

45. Prove that if all Sylow subgroups of a finite group G are normal and abelian, then the group is abelian.

46. A group is generated by two elements a and b satisfying the relations: $a^3 = b^2$, $a^m = 1$, $b^n = 1$, where m and n are positive integers. For what values of m and n can G be infinite.

47. Show that the group G generated by elements x and y with defining relations $x^2 = y^3 = (xy)^4 = 1$ is a finite solvable group, and find the order of G and its successive derived subgroups G', G'', G'''.

48. A group G is generated by a normal set X of elements of order 2. Show that the commutator subgroup G' of G is generated by all squares of products xy of pairs of elements of X.

49. Determine the normalizer N in $\mathrm{GL}_n(F)$ of the subgroup H of diagonal matrices, and prove that N/H is isomorphic to the symmetric group S_n.

50. Let G be a group with generators x and y and defining relations x^2, y^5, $(xy)^4$. What is the index in G of the commutator group G' of G.

51. Let G be a finite group, and H the subgroup generated by the elements of odd order. Show that H is normal, and that the order of G/H is a power of 2.

52. Let G be a finite group, and P a Sylow p-subgroup. Show that if H is a subgroup of G such that $N_G(P) \subset H \subset G$, then

(a) the normalizer of H in G is H;
(b) $(G : H) \equiv 1 \pmod{p}$.

53. Let G be a group of order $33 \cdot 25$. Show that G is solvable. (Hint: A first step is to find a normal subgroup of order 11 using the Sylow theorems.)

54. Suppose that α is an endomorphism of the group G that maps G onto G and commutes with all inner automorphisms of G. Show that if G is its own commutator subgroup, then $\alpha x = x$ for all x in G.

55. Let G be a finite group with generators s and t each of order 2. Let $n = (G : 1)/2$.

(a) Show that G has a cyclic subgroup of order n. Now assume n odd.
(b) Describe all conjugacy classes of G.
(c) Describe all subgroups of G of the form $C(x) = \{y \in G | xy = yx\}$, $x \in G$.
(d) Describe all cyclic subgroups of G.
(e) Describe all subgroups of G in terms of (b) and (d).
(f) Verify that any two p-subgroups of G are conjugate (p prime).

56. Let G act transitively on a set X. Let N be a normal subgroup of G, and let Y be the set of orbits of N in X. Prove that:

(a) There is a natural action of G on Y which is transitive and shows that every orbit of N on X has the same cardinality.
(b) Show by example that if N is not normal then its orbits need not have the same cardinality.

57. Prove that every maximal subgroup of a finite p-group is normal of prime index (p is prime).

58. A group G is *metacyclic* if it has a cyclic normal subgroup N with cyclic quotient G/N. Prove that subgroups and quotient groups of metacyclic groups are metacyclic. Prove or disprove that direct products of metacyclic groups are metacylic.

59. Let G be a group acting doubly transitively on X, and let $x \in X$. Prove that:

(a) The stabilizer G_x of x is a maximal subgroup of G.
(b) If N is a normal subgroup of G, then either N is contained in G_x or it acts transitively on X.

60. Let x, y be elements of a group G such that $xyx^{-1} = y^5$, x has order 3, and $y \neq 1$ has odd order. Find (with proof) the order of y.

61. Let H be a maximal subgroup of G, and let A be a normal subgroup of H and such that the conjugates of A in G generate it.

(a) Prove that if N is a normal subgroup of G, then either $N \subset H$ or $G = NA$.
(b) Let M be the intersection of the conjugates of H in G. Prove that if G is equal to its commutator subgroup and A is abelian, then G/M is a simple group.

62. (a) Prove that the centre of a nonabelian group of order p^3, p prime, has order p.
(b) Exhibit a nonabelian group of order 16 whose centre is not cyclic.

63. Show that the group with generators α and β and defining relations

$$\alpha^2 = \beta^2 = (\alpha\beta)^3 = 1$$

is isomorphic with the symmetric group S_3 of degree 3 by giving, with proof, an explicit isomorphism.

64. Prove or give a counter-example:

(a) Every group of order 30 has a normal subgroup of order 15.
(b) Every group of order 30 is nilpotent.

65. Let $t \in \mathbb{Z}$, and let G be the group with generators x, y and relations $xyx^{-1} = y^t$, $x^3 = 1$.

(a) Find necessary and sufficient conditions on t for G to be finite.
(b) In case G is finite, determine its order.

66. Let G be a group of order pq, $p \neq q$ primes.

(a) Prove G is solvable.
(b) Prove that G is nilpotent $\iff$ G is abelian $\iff$ G is cyclic.
(c) Is G always nilpotent? (Prove or find a counterexample.)

67. Let X be a set with p^n elements, p prime, and let G be a finite group acting transitively on X. Prove that every Sylow p-subgroup of G acts transitively on X.

68. Let $G = \langle a,b,c \mid bc = cb, a^4 = b^2 = c^2 = 1, aca^{-1} = c, aba^{-1} = bc\rangle$. Determine the order of G and find the derived series of G.

69. Let N be a nontrivial normal subgroup of a nilpotent group G. Prove that $N \cap Z(G) \neq 1$.

70. Do not assume Sylow's theorems in this problem.

(a) Let H be a subgroup of a finite group G, and P a Sylow p-subgroup of G. Prove that there exists an $x \in G$ such that $xPx^{-1} \cap H$ is a Sylow p-subgroup of H.

(b) Prove that the group of $n \times n$ matrices $\begin{pmatrix} 1 & * & \dots \\ 0 & 1 & \cdots \\ & \cdots & \\ 0 & & 1 \end{pmatrix}$ is a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$.

(c) Indicate how (a) and (b) can be used to prove that any finite group has a Sylow p-subgroup.

71. Suppose H is a normal subgroup of a finite group G such that G/H is cyclic of order n, where n is relatively prime to $(G:1)$. Prove that G is equal to the semidirect product $H \rtimes S$ with S a cyclic subgroup of G of order n.

72. Let H be a minimal normal subgroup of a finite solvable group G. Prove that H is isomorphic to a direct sum of cyclic groups of order p for some prime p.

73. (a) Prove that subgroups A and B of a group G are of finite index in G if and only if $A \cap B$ is of finite index in G.
(b) An element x of a group G is said to be an *FC-element* if its centralizer $C_G(x)$ has finite index in G. Prove that the set of all FC elements in G is a normal.

74. Let G be a group of order p^2q^2 for primes $p > q$. Prove that G has a normal subgroup of order p^n for some $n \geq 1$.

75. (a) Let K be a finite nilpotent group, and let L be a subgroup of K such that $L \cdot \delta K = K$, where δK is the derived subgroup. Prove that $L = K$. [You may assume that a finite group is nilpotent if and only if every maximal subgroup is normal.]
(b) Let G be a finite group. If G has a subgroup H such that both $G/\delta H$ and H are nilpotent, prove that G is nilpotent.

76. Let G be a finite noncyclic p-group. Prove that the following are equivalent:

(a) $(G : Z(G)) \leq p^2$.
(b) Every maximal subgroup of G is abelian.
(c) There exist at least two maximal subgroups that are abelian.

77. Prove that every group G of order 56 can be written (nontrivially) as a semidirect product. Find (with proofs) two non-isomorphic non-abelian groups of order 56.

78. Let G be a finite group and $\varphi : G \to G$ a homomorphism.

(a) Prove that there is an integer $n \geq 0$ such that $\varphi^n(G) = \varphi^m(G)$ for all integers $m \geq n$. Let $\alpha = \varphi^n$.
(b) Prove that G is the semi-direct product of the subgroups $\mathrm{Ker}\,\alpha$ and $\mathrm{Im}\,\alpha$.
(c) Prove that $\mathrm{Im}\,\alpha$ is normal in G or give a counterexample.

79. Let S be a set of representatives for the conjugacy classes in a finite group G and let H be a subgroup of G. Show that $S \subset H \implies H = G$.

80. Let G be a finite group.

(a) Prove that there is a unique normal subgroup K of G such that (i) G/K is solvable and (ii) if N is a normal subgroup and G/N is solvable, then $N \supset K$.
(b) Show that K is characteristic.
(c) Prove that $K = [K, K]$ and that $K = 1$ or K is nonsolvable.

APPENDIX **B**

Solutions to the Exercises

These solutions fall somewhere between hints and complete solutions. Students were expected to write out complete solutions.

1-1 By inspection, the only element of order 2 is $c = a^2 = b^2$. Since gcg^{-1} also has order 2, it must equal c, i.e., $gcg^{-1} = c$ for all $g \in Q$. Thus c commutes with all elements of Q, and $\{1, c\}$ is a normal subgroup of Q. The remaining subgroups have orders 1, 4, or 8, and are automatically normal (see 1.36a).

1-2 The product $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

1-3 Consider the subsets $\{g, g^{-1}\}$ of G. Each set has exactly 2 elements unless g has order 1 or 2, in which case it has 1 element. Since G is a disjoint union of these sets, there must be a (nonzero) even number of sets with 1 element, and hence at least one element of order 2.

1-4 The symmetric group S_n contains a subgroup that is a direct product of subgroups S_{n_1}, $\ldots$, S_{n_r}.

1-5 Because the group G/N has order n, $(gN)^n = 1$ for every $g \in G$ (see 1.27). But $(gN)^n = g^n N$, and so $g^n \in N$. For the second statement, consider the subgroup $\{1, s\}$ of D_3. It has index 3 in D_3, but the element t has order 2, and so $t^3 = t \notin \{1, s\}$.

The symmetric group S_n contains a subgroup that is a direct product of subgroups S_{n_1}, $\ldots$, S_{n_r}.

1-5 Because the group G/N has order n, $(gN)^n = 1$ for every $g \in G$ (see 1.27). But $(gN)^n = g^n N$, and so $g^n \in N$. For the second statement, consider the subgroup $\{1, s\}$ of D_3. It has index 3 in D_3, but the element t has order 2, and so $t^3 = t \notin \{1, s\}$.

1-6 (a) Let $a, b \in G$. We are given that $a^2 = b^2 = (ab)^2 = e$. In particular, $abab = e$. On multiplying this on right by ba, we find that $ab = ba$. (b) Show by induction that

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb + \frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}.$$

1-7 Commensurability is obviously reflexive and symmetric, and so it suffices to prove transitivity. We shall use that if a subgroup H of a group G has finite index in G, then $H \cap G'$

has finite index in G' for any subgroup G' of G (because the natural map $G'/H \cap G' \to G/H$ is injective). Using this, it follows that if H_1 and H_3 are both commensurable with H_2, then $H_1 \cap H_2 \cap H_3$ is of finite index in $H_1 \cap H_2$ and in $H_2 \cap H_3$ (and therefore also in H_1 and H_3). As $H_1 \cap H_3 \supset H_1 \cap H_2 \cap H_3$, it also has finite index in each of H_1 and H_3.

1-8 By assumption, the set G is nonempty, so let $a \in G$. Because G satisfies the cancellation law, the map $x \mapsto ax\colon G \to G$ is a permutation of G, and some power of this permutation is the identity permutation. Therefore, for some $n \geq 1$, $a^n x = x$ for all $x \in G$, and so a^n is a left neutral element. By counting, one sees that every element has a left inverse, and so we can apply (1.10a).

1-9 Let b be such that the right multiplication $x \mapsto xb$ is injective. Let $a_0 \in G$; there is a unique $e \in G$ such that $a_0 e = a_0$. Then $a_0 eb = a_0 b$, which implies that $eb = b$. Then $aeb = ab$ for all $a \in A$, which implies that $ae = a$. Therefore e is a right neutral element. For each $a \in G$, there is a unique a' such that $aa' = e$. Therefore G also has right inverses, and so it is a group (1.10a).

Let G be a set, and consider the binary operation $a, b \mapsto b$ on G. This is associative, and all left multiplications are bijective (in fact, the identity map), but G is not a group if it has at least two elements.

2-1 The key point is that $\langle a \rangle = \langle a^2 \rangle \times \langle a^n \rangle$. Apply (1.50) to see that D_{2n} breaks up as a product.

2-2 Note first that any group generated by a commuting set of elements must be commutative, and so the group G in the problem is commutative. According to (2.8), any map $\{a_1, \ldots, a_n\} \to A$ with A commutative extends uniquely to homomorphism $G \to A$, and so G has the universal property that characterizes the free abelian group on the generators a_i.

2-3 (a) If $a \neq b$, then the word $a \cdots ab^{-1} \cdots b^{-1}$ is reduced and $\neq 1$. Therefore, if $a^n b^{-n} = 1$, then $a = b$. (b) is similar. (c) The reduced form of x^n, $x \neq 1$, has length at least n.

2-4 (a) Universality. (b) $C_\infty \times C_\infty$ is commutative, and the only commutative free groups are 1 and C_∞. (c) Suppose a is a nonempty reduced word in $x_1, \ldots, x_n$, say $a = x_i \cdots$ (or $x_i^{-1} \cdots$). For $j \neq i$, the reduced form of $[x_j, a] \overset{\text{def}}{=} x_j a x_j^{-1} a^{-1}$ can't be empty, and so a and x_j don't commute.

2-5 The unique element of order 2 is b^2. Since gb^2g^{-1} also has order 2 for any $g \in Q_n$, we see that $gb^2g^{-1} = b^2$, and so b^2 lies in the centre. [Check that it is the full centre.] The quotient group $Q_n/\langle b^2 \rangle$ has generators a and b, and relations $a^{2^{n-2}} = 1$, $b^2 = 1$, $bab^{-1} = a^{-1}$, which is a presentation for $D_{2^{n-2}}$ (see 2.9).

2-6 (a) A comparison of the presentation $D_n = \langle r, s \mid r^n, s^2, srsr = 1 \rangle$ with that for G suggests putting $r = ab$ and $s = a$. Check (using 2.8) that there are homomorphisms:

$$D_n \to G, \quad r \mapsto ab, \quad s \mapsto a, \qquad G \to D_n, \quad a \mapsto s, \quad b \mapsto s^{-1}r.$$

The composites $D_n \to G \to D_n$ and $G \to D_n \to G$ are the both the identity map on generating elements, and therefore (2.8 again) are identity maps. (b) Omit.

2-7 The hint gives $ab^3a^{-1} = bc^3b^{-1}$. But $b^3 = 1$. So $c^3 = 1$. Since $c^4 = 1$, this forces $c = 1$. From $acac^{-1} = 1$ this gives $a^2 = 1$. But $a^3 = 1$. So $a = 1$. The final relation then gives $b = 1$.

2-8 The elements x^2, xy, y^2 lie in the kernel, and it is easy to see that $\langle x,y|x^2,xy,y^2\rangle$ has order (at most) 2, and so they must generate the kernel (at least as a normal group — the problem is unclear). One can prove directly that these elements are free, or else apply the Nielsen-Schreier theorem (2.6). Note that the formula on p. 34 (correctly) predicts that the kernel is free of rank $2 \cdot 2 - 2 + 1 = 3$

2-9 We have to show that if s and t are elements of a finite group satisfying $t^{-1}s^3t = s^5$, then the given element g is equal to 1. Because the group is finite, $s^n = 1$ for some n. If $3|n$, the proof is easy, and so we suppose that $\gcd(3,n) = 1$. But then

$$3r + nr' = 1, \text{ some } r, r' \in \mathbb{Z},$$

and so $s^{3r} = s$. Hence

$$t^{-1}st = t^{-1}s^{3r}t = (t^{-1}s^3t)^r = s^{5r}.$$

Now,

$$g = s^{-1}(t^{-1}s^{-1}t)s(t^{-1}st) = s^{-1}s^{-5r}ss^{5r} = 1,$$

as required. [In such a question, look for a pattern. Note that g has two conjugates in it, as does the relation for G, and so it is natural to try to relate them.]

3-1 Let N be the unique subgroup of order 2 in G. Then G/N has order 4, but there is no subgroup $Q \subset G$ of order 4 with $Q \cap N = 1$ (because every group of order 4 contains a group of order 2), and so $G \neq N \rtimes Q$ for any Q. A similar argument applies to subgroups N of order 4.

3-2 For any $g \in G$, gMg^{-1} is a subgroup of order m, and therefore equals M. Thus M (similarly N) is normal in G, and MN is a subgroup of G. The order of any element of $M \cap N$ divides $\gcd(m,n) = 1$, and so equals 1. Now (1.51) shows that $M \times N \approx MN$, which therefore has order mn, and so equals G.

3-3 Show that $\mathrm{GL}_2(\mathbb{F}_2)$ permutes the 3 nonzero vectors in $\mathbb{F}_2 \times \mathbb{F}_2$ (2-dimensional vector space over $\mathbb{F}_2$).

3-4 I thank readers for their help with these solutions. We write the quaternion group as

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}.$$

Note the Q has one element of order 2, namely, -1, and six elements of order 4, namely, $\pm i$, $\pm j$, $\pm k$. (A) The automorphism group of Q must permute the elements of order 4. Write the six elements of order 4 on the six faces of a cube with i opposite $-i$, etc. Each rotation of the cube induces an automorphism of Q, and $\mathrm{Aut}(Q)$ is the symmetry group of the cube, S_4. (B) Every automorphism of Q permutes the circularly ordered sets $\{i,j,k\}$, $\{-i,-k,-j\}$, $\{-i,-j,k\}$, ... There are 8 of these which can be divided into two sets of 4, each of which is permuted transitively by $\mathrm{Aut}(Q)$. (C). The action of $\mathrm{Aut}(Q)$ on the set $\{\langle i\rangle, \langle j\rangle, \langle k\rangle\}$ of subgroups of order 3 defines a homomorphism $\varphi\colon \mathrm{Aut}\, Q \to S_3$. The automorphisms $i \leftrightarrow j$ and $j \leftrightarrow k$ of Q map onto generators of S_3, and so they generate a subgroup of $\operatorname{Aut} Q$ mapped isomorphically onto S_3 by φ. Automorphisms of Q in the kernel of φ map i to $\pm i$ and j to $\pm j$. This gives us four possibilities, and in fact there is a subgroup of $\operatorname{Aut} Q$ isomorphic to V_4 in the kernel of φ. Now $\operatorname{Aut}(Q) \approx V_4 \rtimes S_3 \approx S_4$ (see sx195932).

3-5 The pair

$$N = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right\} \text{ and } Q = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & d \end{pmatrix} \right\}$$

satisfies the conditions (i), (ii), (iii) of (3.8). For example, for (i) (Maple says that)

$$\begin{pmatrix} a & 0 & b \\ 0 & a & c \\ 0 & 0 & d \end{pmatrix} \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 & b \\ 0 & a & c \\ 0 & 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & -\frac{b}{d} + \frac{1}{d}(b+ab) \\ 0 & 1 & -\frac{c}{d} + \frac{1}{d}(c+ac) \\ 0 & 0 & 1 \end{pmatrix}$$

It is not a direct product of the two groups because it is not commutative.

3-6 Let g generate C_∞. Then the only other generator is g^{-1}, and the only nontrivial automorphism is $g \mapsto g^{-1}$. Hence $\operatorname{Aut}(C_\infty) = \{\pm 1\}$. The homomorphism $S_3 \to \operatorname{Aut}(S_3)$ is injective because $Z(S_3) = 1$, but S_3 has exactly 3 elements a_1, a_2, a_3 of order 2 and 2 elements b, b^2 of order 3. The elements a_1, b generate S_3, and there are only 6 possibilities for $\alpha(a_1)$, $\alpha(b)$, and so $S_3 \to \operatorname{Aut}(S_3)$ is also onto.

3-7 (a) The element $g^{o(q)} \in N$, and so has order dividing $|N|$. (c) The element $g = (1,4,3)(2,5)$, and so this is obvious. (d) By the first part, $((1,0,\ldots,0),q)^p = ((1,\ldots,1),1)$, and $(1,\ldots,1)$ has order p in $(C_p)^p$. (e) We have $(n,q)(n,q) = (nn^{-1}, qq) = (1,1)$.

3-8 Let $n \cdot q \in Z(G)$. Then

$$\left.\begin{array}{rcl} (n\cdot q)(1\cdot q') & = & n \cdot qq' \\ (1\cdot q')(n\cdot q) & = & q'nq'^{-1} \cdot q'q \end{array} \quad \text{all } q' \in Q \right\} \implies \begin{array}{c} n \in C_N(Q) \\ q \in Z(Q) \end{array}$$

and

$$\left.\begin{array}{rcl} (n\cdot q)(n'\cdot 1) & = & nqn'q^{-1} \cdot q \\ (n'\cdot 1)(n\cdot q) & = & n'n \cdot q \end{array} \quad n' \in N \quad \right\} \implies n^{-1}n'n = qn'q^{-1}.$$

The converse and the remaining statements are easy.

4-1 Let $\varphi: G/H_1 \to G/H_2$ be a G-map, and let $\varphi(H_1) = gH_2$. For $a \in G$, $\varphi(aH_1) = a\varphi(H_1) = agH_2$. When $a \in H_1$, $\varphi(aH_1) = gH_2$, and so $agH_2 = gH_2$; hence $g^{-1}ag \in H_2$, and so $a \in gH_2g^{-1}$. We have shown $H_1 \subset gH_2g^{-1}$. Conversely, if g satisfies this condition, the $aH_1 \mapsto agH_2$ is a well-defined map of G-sets.

4-2 (a) Let H be a proper subgroup of G, and let $N = N_G(H)$. The number of conjugates of H is $(G:N) \leq (G:H)$ (see 4.8). Since each conjugate of H has $(H:1)$ elements and the conjugates overlap (at least) in $\{1\}$, we see that

$$\left| \bigcup gHg^{-1} \right| < (G:H)(H:1) = (G:1).$$

(b) Use that the action of G on the left cosets of H defines a homomorphism $\varphi\colon G \to S_n$, and look at the finite group $G/\operatorname{Ker}(\varphi)$.

(c) Let $G = \mathrm{GL}_n(k)$ with k an algebraically closed field. Every element of G is conjugate to an upper triangular matrix (its Jordan form). Therefore G is equal to the union of the conjugates of the subgroup of upper triangular matrices.

(d) Choose S to be a set of representatives for the conjugacy classes.

4-3 Let H be a subgroup of a finite group G, and assume that H contains at least one element from each conjugacy class of G. Then G is the union of the conjugates of H, and so we can apply Exercise 4-2. (According to Serre 2003, this result goes back to Jordan in the 1870s.)

4-4 According to 4.17, 4.18, there is a normal subgroup N of order p^2, which is commutative. Now show that G has an element c of order p not in N, and deduce that $G = N \rtimes \langle c \rangle$, etc..

4-5 Let H be a subgroup of index p, and let N be the kernel of $G \to \operatorname{Sym}(G/H)$ — it is the largest normal subgroup of G contained in H (see 4.22). If $N \neq H$, then $(H:N)$ is divisible by a prime $q \geq p$, and $(G:N)$ is divisible by pq. But pq doesn't divide $p!$ — contradiction.

4-6 Embed G into S_{2m}, and let $N = A_{2m} \cap G$. Then $G/N \hookrightarrow S_{2m}/A_{2m} = C_2$, and so $(G:N) \leq 2$. Let a be an element of order 2 in G, and let $b_1, \ldots, b_m$ be a set of right coset representatives for $\langle a \rangle$ in G, so that $G = \{b_1, ab_1, \ldots, b_m, ab_m\}$. The image of a in S_{2m} is the product of the m transpositions $(b_1, ab_1), \ldots, (b_m, ab_m)$, and since m is odd, this implies that $a \notin N$.

4-7 The set X of k-cycles in S_n is normal, and so the group it generates is normal (1.38). But, when $n \geq 5$, the only nontrivial normal subgroups of S_n are A_n and S_n itself. If k is odd, then X is contained in A_n, and if k is even, then it isn't.

4-8 (a) The number of possible first rows is $2^3 - 1$; of second rows $2^3 - 2$; of third rows $2^3 - 2^2$; whence $(G:1) = 7 \times 6 \times 4 = 168$. (b) Let $V = \mathbb{F}_2^3$. Then $|V| = 2^3 = 8$. Each line through the origin contains exactly one point $\neq$ origin, and so $|X| = 7$. (c) We make a list of possible characteristic and minimal polynomials:

	Characteristic poly.	Min'l poly.	Size	Order of element in class
1	X^3+X^2+X+1	$X+1$	1	1
2	X^3+X^2+X+1	$(X+1)^2$	21	2
3	X^3+X^2+X+1	$(X+1)^3$	42	4
4	$X^3+1=(X+1)(X^2+X+1)$	Same	56	3
5	X^3+X+1 (irreducible)	Same	24	7
6	X^3+X^2+1 (irreducible)	Same	24	7

Here size denotes the number of elements in the conjugacy class. *Case 5:* Let α be an endomorphism with characteristic polynomial X^3+X+1. Check from its minimal polynomial that $\alpha^7 = 1$, and so α has order 7. Note that V is a free $\mathbb{F}_2[\alpha]$-module of rank one, and so the centralizer of α in G is $\mathbb{F}_2[\alpha] \cap G = \langle \alpha \rangle$. Thus $|C_G(\alpha)| = 7$, and the number of elements in the conjugacy class of α is $168/7 = 24$. *Case 6:* Exactly the same as Case 5. *Case 4:* Here $V = V_1 \oplus V_2$ as an $\mathbb{F}_2[\alpha]$-module, and

$$\operatorname{End}_{\mathbb{F}_2[\alpha]}(V) = \operatorname{End}_{\mathbb{F}_2[\alpha]}(V_1) \oplus \operatorname{End}_{\mathbb{F}_2[\alpha]}(V_2).$$

Deduce that $|C_G(\alpha)| = 3$, and so the number of conjugates of α is $\frac{168}{3} = 56$. *Case 3:* Here $C_G(\alpha) = \mathbb{F}_2[\alpha] \cap G = \langle\alpha\rangle$, which has order 4. *Case 1:* Here α is the identity element. *Case 2:* Here $V = V_1 \oplus V_2$ as an $\mathbb{F}_2[\alpha]$-module, where α acts as 1 on V_1 and has minimal polynomial $X^2 + 1$ on V_2. Either analyse, or simply note that this conjugacy class contains all the remaining elements. (d) Since $168 = 2^3 \times 3 \times 7$, a proper nontrivial subgroup H of G will have order

$$2, 4, 8, 3, 6, 12, 24, 7, 14, 28, 56, 21, 24, \text{ or } 84.$$

If H is normal, it will be a disjoint union of $\{1\}$ and some other conjugacy classes, and so $(N : 1) = 1 + \sum c_i$ with c_i equal to 21, 24, 42, or 56, but this doesn't happen.

4-9 Since $G/Z(G) \hookrightarrow \text{Aut}(G)$, we see that $G/Z(G)$ is cyclic, and so by (4.19) that G is commutative. If G is finite and not cyclic, it has a factor $C_{p^r} \times C_{p^s}$ etc..

4-10 Clearly $(ij) = (1j)(1i)(1j)$. Hence any subgroup containing $(12), (13), \ldots$ contains all transpositions, and we know S_n is generated by transpositions.

4-11 Note that $C_G(x) \cap H = C_H(x)$, and so $H/C_H(x) \approx H \cdot C_G(x)/C_G(x))$. Prove each class has the same number c of elements. Then

$$|K| = (G : C_G(x)) = (G : H \cdot C_G(x))(H \cdot C_G(x) : C_G(x)) = kc.$$

4-12 (a) The first equivalence follows from the preceding problem. For the second, note that σ commutes with all cycles in its decomposition, and so they must be even (i.e., have odd length); if two cycles have the same odd length k, one can find a product of k transpositions which interchanges them, and commutes with σ; conversely, show that if the partition of n defined by σ consists of distinct integers, then σ commutes only with the group generated by the cycles in its cycle decomposition. (b) List of conjugacy classes in S_7, their size, parity, and (when the parity is even) whether it splits in A_7.

	Cycle	Size	Parity	Splits in A_7?	$C_7(\sigma)$ contains
1	(1)	1	E	N	
2	(12)	21	O		
3	(123)	70	E	N	(67)
4	(1234)	210	O		
5	(12345)	504	E	N	(67)
6	(123456)	840	O		
7	(1234567)	720	E	Y	720 doesn't divide 2520
8	(12)(34)	105	E	N	(67)
9	(12)(345)	420	O		
10	(12)(3456)	630	E	N	(12)
11	(12)(3456)	504	O		
12	(123)(456)	280	E	N	(14)(25)(36)
13	(123)(4567)	420	O		
14	(12)(34)(56)	105	O		
15	(12)(34)(567)	210	E	N	(12)

4-13 According to GAP, $n = 6$, $a \mapsto (13)(26)(45)$, $b \mapsto (12)(34)(56)$.

4-14 Since $\mathrm{Stab}(gx_0) = g\,\mathrm{Stab}(x_0)g^{-1}$, if $H \subset \mathrm{Stab}(x_0)$ then $H \subset \mathrm{Stab}(x)$ for all x, and so $H = 1$, contrary to hypothesis. Now $\mathrm{Stab}(x_0)$ is maximal, and so $H \cdot \mathrm{Stab}(x_0) = G$, which shows that H acts transitively.

5-1 Let p be a prime dividing $|G|$ and let P be a Sylow p-subgroup, of order p^m say. The elements of P all have order dividing p^m, and P (even G) has at most p^{m-1} elements of order dividing p^{m-1}; therefore P must have an element of order p^m, and so it is cyclic. Each Sylow p-subgroup has exactly p^m elements of order dividing p^m, and so there can be only one. Now (5.9) shows that G is a product of its Sylow subgroups.

6-2 No, D_4 and the quaternion group have isomorphic commutator subgroups and quotient groups but are not isomorphic. Similarly, S_n and $A_n \times C_2$ are not isomorphic when $n \geq 5$.

APPENDIX **C**

Two-Hour Examination

1. Which of the following statements are true (give *brief* justifications for each of (a), (b), (c), (d); give a correct set of implications for (e)).

(a) If a and b are elements of a group, then $a^2 = 1, \quad b^3 = 1 \implies (ab)^6 = 1$.

(b) The following two elements are conjugate in S_7:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}.$$

(c) If G and H are finite groups and $G \times A_{594} \approx H \times A_{594}$, then $G \approx H$.

(d) The only subgroup of A_5 containing (123) is A_5 itself.

(e) Nilpotent $\implies$ cyclic $\implies$ commutative $\implies$ solvable (for a finite group).

2. How many Sylow 11-subgroups can a group of order $110 = 2 \cdot 5 \cdot 11$ have? Classify the groups of order 110 containing a subgroup of order 10. Must every group of order 110 contain a subgroup of order 10?

3. Let G be a finite nilpotent group. Show that if every commutative quotient of G is cyclic, then G itself is cyclic. Is the statement true for nonnilpotent groups?

4. (a) Let G be a subgroup of $\mathrm{Sym}(X)$, where X is a set with n elements. If G is commutative and acts transitively on X, show that each element $g \neq 1$ of G moves every element of X. Deduce that $(G:1) \leq n$.
(b) For each $m \geq 1$, find a commutative subgroup of S_{3m} of order 3^m.
(c) Show that a commutative subgroup of S_n has order $\leq 3^{\frac{n}{3}}$.

5. Let H be a normal subgroup of a group G, and let P be a subgroup of H. Assume that every automorphism of H is inner. Prove that $G = H \cdot N_G(P)$.

6. (a) Describe the group with generators x and y and defining relation $yxy^{-1} = x^{-1}$.
(b) Describe the group with generators x and y and defining relations $yxy^{-1} = x^{-1}$, $xyx^{-1} = y^{-1}$.

You may use results proved in class or in the notes, but you should indicate clearly what you are using.

SOLUTIONS

1. (a) False: in $\langle a,b|a^2,b^3\rangle$, ab has infinite order.

(b) True, the cycle decompositions are (1357)(246), (123)(4567).

(c) True, use the Krull-Schmidt theorem.

(d) False, the group it generates is proper.

(e) Cyclic $\implies$ commutative $\implies$ nilpotent $\implies$ solvable.

2. The number of Sylow 11-subgroups $s_{11} = 1, 12, \ldots$ and divides 10. Hence there is only one Sylow 11-subgroup P. Have

$$G = P \rtimes_\theta H, \quad P = C_{11}, \quad H = C_{10} \text{ or } D_5.$$

Now have to look at the maps $\theta : H \to \mathrm{Aut}(C_{11}) = C_{10}$. Yes, by the Schur-Zassenhaus lemma.

3. Suppose G has class > 1. Then G has quotient H of class 2. Consider

$$1 \to Z(H) \to H \to H/Z(H) \to 1.$$

Then H is commutative by (4.17), which is a contradiction. Therefore G is commutative, and hence cyclic.

Alternatively, by induction, which shows that $G/Z(G)$ is cyclic.

No! In fact, it's not even true for solvable groups (e.g., S_3).

4. (a) If $gx = x$, then $ghx = hgx = hx$. Hence g fixes every element of X, and so $g = 1$. Fix an $x \in X$; then $g \mapsto gx : G \to X$ is injective. [Note that Cayley's theorem gives an embedding $G \hookrightarrow S_n$, $n = (G : 1)$.]

(b) Partition the set into subsets of order 3, and let $G = G_1 \times \cdots \times G_m$.

(c) Let $O_1, \ldots, O_r$ be the orbits of G, and let G_i be the image of G in $\mathrm{Sym}(O_i)$. Then $G \hookrightarrow G_1 \times \cdots \times G_r$, and so (by induction),

$$(G : 1) \le (G_1 : 1) \cdots (G_r : 1) \le 3^{\frac{n_1}{3}} \cdots 3^{\frac{n_r}{3}} = 3^{\frac{n}{3}}.$$

5. Let $g \in G$, and let $h \in H$ be such that conjugation by h on H agrees with conjugation by g. Then $gPg^{-1} = hPh^{-1}$, and so $h^{-1}g \in N_G(P)$.

6. (a) It's the group .

$$G = \langle x \rangle \rtimes \langle y \rangle = C_\infty \rtimes_\theta C_\infty$$

with $\theta\colon C_\infty \to \mathrm{Aut}(C_\infty) = \pm 1$. Alternatively, the elements can be written uniquely in the form $x^i y^j$, $i, j \in \mathbb{Z}$, and $yx = x^{-1}y$.

(b) It's the quaternion group. From the two relations get

$$yx = x^{-1}y, \quad yx = xy^{-1}$$

and so $x^2 = y^2$. The second relation implies

$$xy^2x^{-1} = y^{-2}, = y^2,$$

and so $y^4 = 1$.

Alternatively, the Todd-Coxeter algorithm shows that it is the subgroup of S_8 generated by (1287)(3465) and (1584)(2673).

Bibliography

ALPERIN, J. L. AND BELL, R. B. 1995. Groups and representations, volume 162 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

ARTIN, M. 1991. Algebra. Prentice Hall Inc., Englewood Cliffs, NJ.

ASCHBACHER, M. AND SMITH, S. D. 2004. The classification of quasithin groups. I, II, volume 111, 112 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI. Structure of strongly quasithin K-groups.

BESCHE, H. U., EICK, B., AND O'BRIEN, E. A. 2001. The groups of order at most 2000. *Electron. Res. Announc. Amer. Math. Soc.* 7:1–4 (electronic).

BRAUER, R. AND FOWLER, K. A. 1955. On groups of even order. *Ann. of Math. (2)* 62:565–583.

BURNSIDE, W. 1897. Theory of groups of finite order. Cambridge: at the University Press, Cambridge.

CURTIS, C. W. 1999. Pioneers of representation theory: Frobenius, Burnside, Schur, and Brauer, volume 15 of *History of Mathematics*. American Mathematical Society, Providence, RI.

FEIT, W. 1995. On the work of Efim Zelmanov. *In* Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994), pp. 17–24, Basel. Birkhäuser.

FEIT, W. AND THOMPSON, J. G. 1963. Solvability of groups of odd order. *Pacific J. Math.* 13:775–1029.

GLAUBERMAN, G. 1999. A new look at the Feit-Thompson odd order theorem. *Mat. Contemp.* 16:73–92. 15th School of Algebra (Portuguese) (Canela, 1998). Available at www.mat.unb.br/~matcont/16_5.ps.

HALL, JR., M. 1959. The theory of groups. The Macmillan Co., New York, N.Y.

HUMPHREYS, J. E. 1990. Reflection groups and Coxeter groups, volume 29 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge.

MASSEY, W. S. 1967. Algebraic topology: An introduction. Harcourt, Brace & World, Inc., New York.

PYBER, L. 1993. Enumerating finite groups of given order. *Ann. of Math. (2)* 137:203–220.

RONAN, M. 2006. Symmetry and the monster. One of the greatest quests of mathematics. Oxford University Press, Oxford.

ROTMAN, J. J. 1995. An introduction to the theory of groups, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition.

SCHUPP, P. E. 1987. A characterization of inner automorphisms. *Proc. Amer. Math. Soc.* 101:226–228.

SERRE, J.-P. 1980. Trees. Springer-Verlag, Berlin. Translated from the French by John Stillwell.

SERRE, J.-P. 2003. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)* 40:429–440.

SOLOMON, R. 2001. A brief history of the classification of the finite simple groups. *Bull. Amer. Math. Soc. (N.S.)* 38:315–352.

SYLOW, M. L. 1872. Théorèmes sur les groupes de substitutions. *Math. Ann.* 5:584–594.

WILD, M. 2005. The groups of order sixteen made easy. *Amer. Math. Monthly* 112:20–31.

Index

action
  doubly transitive, 59
  effective, 57
  faithful, 57
  free, 59
  imprimitive, 72
  k-fold transitive, 59
  left, 57
  linear, 100
  primitive, 72
  right, 58
  transitive, 59
  trivial, 57
algebra
  division, 106
  group, 103
  quaternion, 107
  semisimple, 106
  simple, 106
algorithm
  Todd-Coxeter, 38, 70
A_n, 65
automorphism
  inner, 43
  of a bilinear form, 10
  of a group, 43
  outer, 43

basis
  for a commutative group, 25
block, 72

centralizer
  of element, 59
  of subgroup, 119
centralizer, of a subalgebra, 107
centre
  of a group, 12
class
  nilpotency, 91
class equation
  class, 62
C_m, 9
commutator, 24, 35
composition factors, 88
conjugacy class, 58
coset
  left, 17
  right, 17
Coxeter system, 38
cycle, 66

dimension, 106
disjoint cycles, 66
D_n, 13

element
  neutral, 8
elementary divisors, 26
equivariant map, 58
exact sequence, 50
exponent
  of a group, 30, 37
extension
  central, 50
  isomorphic, 51
  split, 51
extension, of groups, 50

faithful representation, 99
flag
  full, 79
Frattini's argument, 93

G-map, 58
G-set, 57
generates, 13
generators
  of a group, 35
$\mathrm{GL}_n(F)$, 10
group, 7
  4-, 14
  A-, 94
  abelian, 9
  additive, 7
  alternating, 65
  Burnside, 38

commutative, 9
complete, 44
Coxeter, 38
cyclic, 13
dihedral, 13
factor, 21
finite reflection, 39
finitely presented, 37
free, 33
free abelian, 35
general linear, 10
indecomposable, 96
isotropy, 59
metabelian, 91
metacyclic, 121
multiplicative, 7
nilpotent, 91
of rigid motions, 58
of symmetries, 9
orthogonal, 10
p, 8
permutation, 9
primitive, 72
quaternion, 14
generalized, 35
quotient, 21
reflection, 39
simple, 19
soluble, 88
solvable, 70, 88
special linear, 20
symplectic, 10
Vierergruppe, 14
with operators, 94

groups
of order 12, 81
of order $2^m p^n$, $m \leq 3.$, 82
of order $2p$, 62
of order 30, 80
of order 60, 82
of order 99, 80
of order p, 18
of order p^2, 63
of order p^3, 81
of order pq, 80
of small order, 15

homogeneous, 59
homomorphism
admissible, 94
normal, 55
of groups, 16

index of a subgroup, 17

invariant factors, 26
inverse, 8
inversion, of a permutation, 64
isomorphism
of G-sets, 58
of groups, 8, 16
isotypic, 105

kernel, 20
Klein Vierergruppe, 14

length
of a subnormal series, 85
solvable, 90
length of a cycle, 66

map, of G-sets, 58
module
semisimple, 99
simple, 99
monoid
free, 31

negative, 8
normalizer
of a subgroup, 60

opposite algebra, 99
orbit, 58
order
of a group, 8
of an element, 9

partition
of a natural number, 67
stabilized, 71
permutation
even, 64
odd, 64
presentation
of a group, 35
problem
Burnside, 37
restricted Burnside, 38
word, 37
product
direct, 9, 23
knit, 50
semidirect, 46
Zappa-Szép, 50
projector, 102

quotients, of a normal series
of a normal series, 85

rank

of a commutative group, 26
of a Coxeter system, 38
of a free group, 34
reduced form
of a word, 32
reflection, 39
relations, 35
defining, 35
representation
completely reducible, 103
irreducible, 103
linear, 100
matrix, 99
semisimple, 103
simple, 103

series
admissible subnormal, 95
ascending central, 91
composition, 85
derived, 90
normal, 85
solvable, 88
subnormal, 85
without repetitions, 85
signature, 64
skew field, 106
S_n, 9, 14
stabilizer
of a subset, 60
of an element, 59
stable subset
stable, 58
subgroup, 12
A-invariant, 94
admissible, 94
characteristic, 45
commutator, 90
first derived, 90
generated by a set, 13
normal, 18
normal generated by a set, 20
second derived, 90
Sylow p-, 75
torsion, 10
subset
normal, 20
support
of a cycle, 66

table
multiplication, 11
theorem
Cauchy, 62
Cayley, 16
centre of a p-group, 63
commutative groups have bases, 25
correspondence, 22
double centralizer, 107
factorization of homomorphisms, 22
Feit-Thompson, 88
Galois, 69
isomorphism, 22
Jordan–Hölder, 86
Krull-Schmidt, 96
Lagrange, 17
Maschke, 101
Nielsen-Schreier, 34
nilpotency condition, 93
primitivity condition, 72
Schur-Zassenhaus, 51
structure of commutative groups, 26
structure of Coxeter groups, 39
Sylow I, 76
Sylow II, 77
Sylow subgroups of subgroups, 79
transposition, 14

V_4, 14

word, 31
reduced, 32
words
equivalent, 33