Finite Groups: An Introduction

Jean-Pierre Serre

Collège de France, Paris

With assistance in translation provided by:
Garving K. Luli (University of California at Davis)
Pin Yu (Tsinghua University, Beijing)
# Contents

Preface vii

Conventions and Notation viii

## 1 Preliminaries

1.1 Group actions ........................................... 1
1.2 Normal subgroups, automorphisms, characteristic subgroups, simple groups 3
1.3 Filtrations and Jordan-Hölder Theorem .............................. 5
1.4 Subgroups of products: Goursat’s lemma and Ribet’s lemma ........ 7
1.5 Exercises ............................................. 9

## 2 Sylow Theorems

2.1 Definitions ........................................... 15
2.2 Existence of $p$-Sylow subgroups .................................. 16
2.3 Properties of the $p$-Sylow subgroups ..................................... 17
2.4 Fusion in the normalizer of a $p$-Sylow subgroup .................. 19
2.5 Local conjugacy and Alperin’s Theorem .............................. 20
2.6 Other Sylow-like theories ...................................... 23
2.7 Exercises ............................................. 24

## 3 Solvable groups and nilpotent groups

3.1 Commutators and abelianization ........................................ 29
3.2 Solvable groups ........................................... 30
3.3 Descending central series and nilpotent groups ..................... 33
3.4 Nilpotent groups and Lie algebras ................................... 35
3.5 Kolchin’s Theorem ......................................... 36
3.6 Finite nilpotent groups ....................................... 37
3.7 Applications of 2-groups to field theory .................................................. 39
3.8 Abelian groups ............................................................................. 41
3.9 The Frattini subgroup ..................................................................... 42
3.10 Characterizations using subgroups generated by two elements. ........ 44
3.11 Exercises ...................................................................................... 46

4 Group extensions ...................................................................................... 51
4.1 Cohomology groups ........................................................................ 51
4.2 A vanishing criterion for the cohomology of finite groups ............... 54
4.3 Extensions, sections and semidirect products .................................... 55
4.4 Extensions with abelian kernel .......................................................... 55
4.5 Extensions with arbitrary kernel ....................................................... 58
4.6 Extensions of groups of relatively prime orders ............................... 61
4.7 Liftings of homomorphisms ............................................................... 63
4.8 Application to p-adic liftings ............................................................. 63
4.9 Exercises ......................................................................................... 65

5 Hall subgroups ............................................................................................ 70
5.1 π-subgroups ....................................................................................... 70
5.2 Preliminaries: permutable subgroups ............................................... 71
5.3 Permutable families of Sylow subgroups .......................................... 73
5.4 Proof of Theorem 5.1 ....................................................................... 73
5.5 Sylow-like properties of the π-subgroups .......................................... 74
5.6 A solvability criterion ..................................................................... 74
5.7 Proof of theorem 5.3 ....................................................................... 75
5.8 Exercises ......................................................................................... 75

6 Frobenius groups ....................................................................................... 77
6.1 Union of conjugates of a subgroup .................................................. 77
6.2 An improvement of Jordan’s Theorem ............................................ 78
6.3 Frobenius groups: definition ............................................................. 79
6.4 Frobenius kernels ............................................................................. 81
6.5 Frobenius complements .................................................................... 83
6.6 Exercises ......................................................................................... 85
7 Transfer 88
7.1 Definition of Ver: \( G^{ab} \rightarrow H^{ab} \) .......................... 88
7.2 Computation of the transfer ................................. 89
7.3 A two-century-old example of transfer: Gauss lemma .................. 91
7.4 An application of transfer to infinite groups .................... 92
7.5 Transfer applied to Sylow subgroups ............................ 92
7.6 Application: groups of odd order < 200 ........................ 94
7.7 Application: simple groups of order \( \leq 200 \) .................. 94
7.8 The use of transfer outside group theory ........................ 97
7.9 Exercises .................................... 99

8 Characters 103
8.1 Linear representations and characters .......................... 103
8.2 Characters, hermitian forms and irreducible representations .......... 105
8.3 Schur’s lemma ................................... 108
8.4 Orthogonality relations .................................. 109
8.5 Structure of the group algebra and of its center ................. 111
8.6 Integrality properties .................................. 114
8.7 Galois properties of characters .............................. 116
8.8 The ring \( R(G) \) .................................. 118
8.9 Realizing representations over a subfield of \( \mathbb{C} \), for instance the field \( \mathbb{R} \) . 120
8.10 Application of character theory: proof of Frobenius’s Theorem 6.7 ... 124
8.11 Application of character theory: proof of Burnside’s Theorem 5.4 ... 126
8.12 The character table of \( A_5 \) .......................... 127
8.13 Exercises .................................... 131

9 Finite subgroups of \( \text{GL}_n \) 142
9.1 Minkowski’s theorem on the finite subgroups of \( \text{GL}_n(\mathbb{Q}) \) ....... 142
9.2 Jordan’s theorem on the finite subgroups of \( \text{GL}_n(\mathbb{C}) \) .......... 146
9.3 Exercises .................................... 152
Contents

10 Small Groups

10.1 Small groups and their isomorphisms ............................................. 154
10.2 Embeddings of $A_4$, $S_4$ and $A_5$ in $PGL_2(F_q)$ .......................... 158
10.3 Exercises .................................................................................. 161

Bibliography .................................................................................... 164

Index ............................................................................................... 170

Index of names ................................................................................ 176
Preface

This book is based on a course given at École Normale Supérieure de Jeunes Filles, Paris, in 1978-1979. Its aim is to give an introduction to the main elementary theorems of finite group theory.

Handwritten notes were taken by Martine Buhler and Catherine Goldstein (Montrouge, 1979); they were later type-set by Nicolas Billerey, Olivier Dodane and Emmanuel Rey (Strasbourg-Paris, 2004), and made freely available through arXiv:math/0503154. In 2013, they were translated into English by Garving K. Luli and Pin Yu. In 2014-2015, I revised and expanded them (by a factor 2) for the present publication: I gave many references to old and recent results (even controversial ones), I added two chapters (on finite subgroups of $\text{GL}_n$, and on “small” groups) and also about 150 exercises in order to complement the main text.

I thank heartily all the people mentioned above, without whom this book would not have been published.

Conventions and Notation

The symbols $\mathbb{Z}, \mathbb{Q}, \mathbb{F}_p, \mathbb{F}_q, \mathbb{R}, \mathbb{C}$ have their usual meaning.

Set theory
If $X \supset Y$, the complement of $Y$ in $X$ is written $X - Y$.
The number of elements of a finite set $X$ is denoted by $|X|$.

Rings
Rings have a unit element, written 1.
If $A$ is a ring, $A^\times$ is the group of invertible elements of $A$.
The word field means commutative field.

Group theory
We use standard notation such as $(G : H)$, $G/H$, $H\backslash G$ when $H$ is a subgroup of a group $G$.
A group $G$ is abelian (= commutative) if $xy = yx$ for every $x, y \in G$.
If $A$ is a subset of $G$, the centralizer of $A$ in $G$ is written $C_G(A)$; it is the set of all $g \in G$ such that $ga = ag$ for every $a \in A$. The normalizer of $A$ is written $N_G(A)$; it is the set of all $g \in G$ such that $gAg^{-1} = A$.
If $A, B$ are subsets of $G$, the set of all products $ab$ with $a \in A$ and $b \in B$ is written $AB$; the subgroup of $G$ generated by $A$ and $B$ is written $\langle A, B \rangle$.
The formula $G = 1$ means that $|G| = 1$; when $G$ is abelian, and written additively, we write $G = 0$ instead.

Symmetric groups
The symmetric and alternating groups of permutations of $\{1, \ldots, n\}$ are written $\mathcal{S}_n$ and $\mathcal{A}_n$. The group of permutations of a set $X$ is written $\mathcal{S}_X$.

Linear groups
If $A$ is a commutative ring, and $n$ is an integer $\geq 0$, then:
$M_n(A) = A$-algebra of $n \times n$ matrices with coefficients in $A$,
$GL_n(A) = M_n(A)^\times = $ invertible $n \times n$ matrices with coefficients in $A$,
$SL_n(A) = \ker(\det: GL_n(A) \to A^\times)$.

We use $\text{End}(V)$, $\text{GL}(V)$ and $\text{SL}(V)$ for the similar notions relative to a vector space of finite dimension.

Let $k$ be a field. If $n \geq 1$, there is a natural isomorphism of $k^\times$ onto the center of $\text{GL}_n(k)$; the quotient $\text{GL}_n(k)/k^\times$ is the $n$-th projective linear group $\text{PGL}_n(k)$.

The image of $\text{SL}_n(k)$ into $\text{PGL}_n(k)$ is denoted by $\text{PSL}_n(k)$. 
Chapter 1

Preliminaries

Let $G$ be a group (finite or infinite). Let us recall a few standard definitions and results relative to $G$.

1.1 Group actions

Definition 1.1. A (left) group action of $G$ on a set $X$ is a map

$$G \times X \to X$$

$$(g, x) \mapsto gx$$

that satisfies the following conditions:

1. $g(g'x) = (gg')x$ for all $x \in X$ and all $g, g' \in G$.
2. $1x = x$ for all $x \in X$, where $1$ is the identity element of $G$.

Note. Right group actions $G \times X \to X$ are defined in a similar way, and denoted by $(x, g) \mapsto xg$. We shall rarely use them. Note that every right action can be replaced by a left one via the recipe: $gx = xg^{-1}$.

Remark. Equivalently, a group action of $G$ on $X$ can be defined as a group homomorphism $\tau$ from $G$ to the symmetric group $S_X$ of $X$, namely $\tau(g)(x) = gx$ for all $g \in G$ and $x \in X$.

Definition 1.2. A set $X$, together with an action of $G$ on it, is called a $G$-set. If $X$ and $Y$ are $G$-sets, a map $f : X \to Y$ is called a $G$-map if $f(gx) = gf(x)$ for every $g \in G$.

If $X$ is a $G$-set, the action of $G$ partitions $X$ into orbits: two elements $x$ and $y$ in $X$ are in the same orbit if and only if there exists $g \in G$ such that $x = gy$. The quotient of $X$ by $G$ is the set of orbits and is written $X/G$ (or sometimes $G \setminus X$).

Definition 1.3. The group $G$ acts transitively on $X$ if $X/G$ consists of only one element.
1.1. Group actions

In particular, the group $G$ acts transitively on each orbit.

**Definition 1.4.** For $x \in X$, the stabilizer of $x$ in $G$, denoted by $G_x$, is the subgroup of elements $g \in G$ that fix $x$ (i.e., such that $gx = x$).

**Definition 1.5.** The action of $G$ on $X$ is said to be faithful if $G \rightarrow S_X$ is injective, i.e., if $\bigcap_{x \in X} G_x = 1$. It is said to be free if $G_x = 1$ for every $x \in X$. If $G$ acts freely and transitively, $X$ is called a $G$-torsor.

**Remark.** If $G$ acts transitively on $X$ and if $x \in X$, we have a bijection from $G/G_x$ to $X$ given by $gG_x \mapsto gx$, where $G/G_x$ is the set of left cosets of $G_x$ in $G$. If $x' \in X$, there exists $g \in G$ such that $x' = gx$. Thus, $G_{x'} = gG_x g^{-1}$. In other words, changing $x$ amounts to replacing its stabilizer by a conjugate. Conversely, if $H$ is a subgroup of $G$, then $G$ acts transitively on $G/H$ and $H$ fixes the class of $1$. Therefore, giving a set $X$ on which $G$ acts transitively amounts to giving a subgroup of $G$, up to conjugation.

**Example.** Let $K$ be a field, and let $G$ be the group of automorphisms of the set $K$ defined by:

$$G = \{ x \mapsto ax + b, \ a \in K^\times, \ b \in K \}.$$

Then $G$ acts transitively on $K$. If $x_0 \in K$, the stabilizer of $x_0$ is the group of homotheties centered at $x_0$, namely $x \mapsto x_0 + a(x - x_0), \ a \in K^\times$; it is isomorphic to $K^\times$.

**Application.** Suppose $G$ is finite and let $|G|$ denote its order. If $X$ is a finite $G$-set, we have $X = \bigcup_{x \in X} Gx_i$, where the $Gx_i$ are the pairwise disjoint orbits under the action of $G$ and $x_i$ is a representative element from each orbit. We have $|Gx_i| = |G| \cdot |G_{x_i}|^{-1}$. Hence

$$|X| = \sum_{i \in I} (G : G_{x_i}) = |G| \sum_{i \in I} \frac{1}{|G_{x_i}|}. \quad (1.1)$$

A special case. Let $G$ act on itself by inner automorphisms: This gives a map

$$G \rightarrow S_G,$$

$$x \mapsto \text{int}_x,$$

where $\text{int}_x(y) = xyx^{-1} = y$. The orbits are the conjugacy classes. The stabilizer of an element $x$ of $G$ is the set of elements of $G$ that commute with $x$, i.e., the centralizer of $x$; we denote it by $C_G(x)$. We have

$$1 = \sum_{i=1}^{h} \frac{1}{|C_G(x_i)|}, \quad (1.2)$$

where $h$ is the number of conjugacy classes, and the $x_i$ are representatives of these classes. In this equation the largest value of $|C_G(x_i)|$ is $|G|$; this fact can be used to obtain an upper bound for $|G|$ when $h$ is known, cf. exerc.7.

**Counting orbits.**

The following result is usually called **Burnside’s lemma**, even though it had already been published before Burnside by Cauchy and later by Frobenius: