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)

International Press
www.intlpress.com

Finite Groups: An Introduction
by Jean-Pierre Serre (Collège de France, Paris)

ISBN 978-1-57146-327-2

Library of Congress Cataloging-in-Publication Data

Names: Serre, Jean-Pierre, 1926-
Title: 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).
Description: Somerville, Massachusetts : International Press, [2016] | Includes bibliographical references and index.
Identifiers: LCCN 2016043217| ISBN 9781571463272 (hardcover, revised : alk. paper) | ISBN 9781571463203 (prelim. pbk.)
Subjects: LCSH: Finite groups--Textbooks. | Group theory--Textbooks.
Classification: LCC QA177 .S4695 2016 | DDC 512/.23--dc23
LC record available at https://lccn.loc.gov/2016043217

Printed in the United States of America.

20 19 18 17 16 1 2 3 4 5 6 7 8 9

Front and back cover illustrations by Xixi Huang.

Contents

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 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.

Jean-Pierre Serre, Paris, Winter 2015

Conventions and Notation

The symbols $\mathbf{Z}, \mathbf{Q}, \mathbf{F}_p, \mathbf{F}_q, \mathbf{R}, \mathbf{C}$ 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 $\{1, \dots, n\}$ 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 $\geqslant 0$, then:

$$\mathrm{M}_n(A) = A\text{-algebra of } n \times n \text{ matrices with coefficients in } A,$$

$$\mathrm{GL}_n(A) = \mathrm{M}_n(A)^\times = \text{invertible } n \times n \text{ matrices with coefficients in } A,$$

$$\mathrm{SL}_n(A) = \mathrm{Ker}(\det : \mathrm{GL}_n(A) \to A^\times).$$

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

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

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

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*

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto gx \end{aligned}$$

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 τ from G to the symmetric group $\mathcal{S}_X$ 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 $G\backslash X$).

Definition 1.3. *The group G acts transitively on X if X/G consists of only one element.*

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*** *is $G \to \mathcal{S}_X$ 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 $gG_x \longmapsto gx$, 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, $G_{x'} = gG_xg^{-1}$. 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 :

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

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 $X = \bigcup_{i\in I} Gx_i$, 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 $|Gx_i| = |G|.\,|G_{x_i}|^{-1}$. Hence

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

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

$$\begin{aligned} G &\longrightarrow \mathcal{S}_G\,, \\ x &\longmapsto \mathrm{int}_x\,, \end{aligned}$$

where $\mathrm{int}_x(y) = xyx^{-1} = {}^xy$. 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

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

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: