SMM 10
Surveys of Modern Mathematics

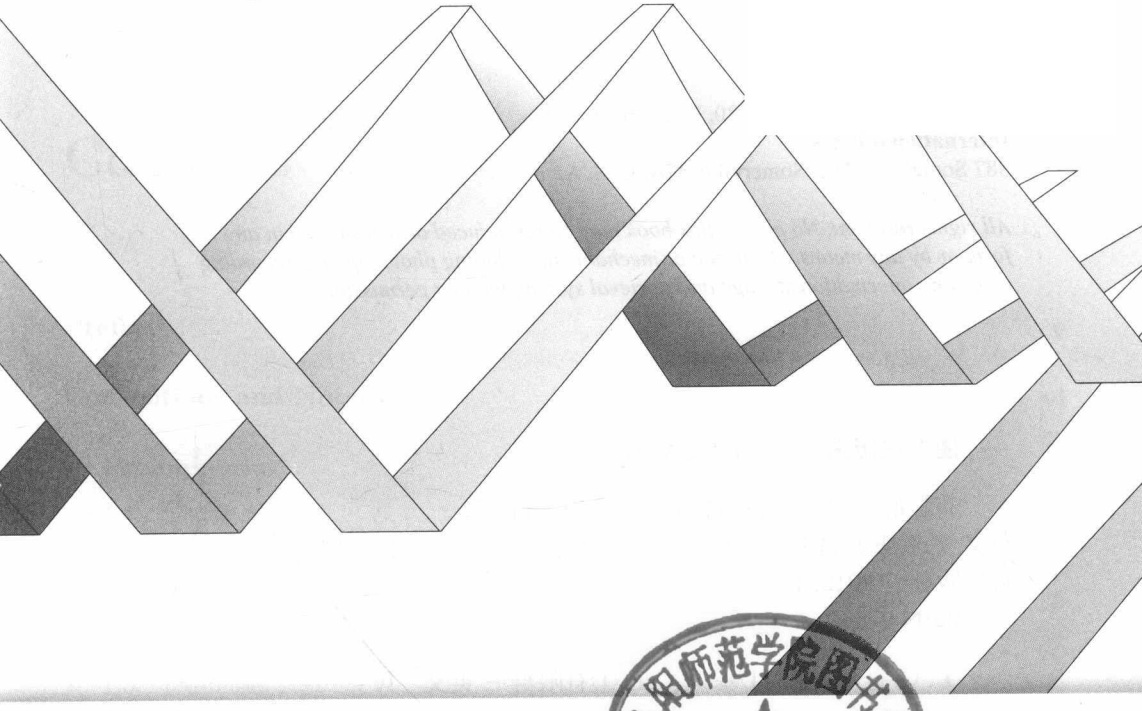
Finite Groups: An Introduction

有限群导引

Jean-Pierre Serre

Higher Education Press

SMM 10
Surveys of Modern Mathematics



Finite Groups: An Introduction
有限群导引

YOUXIANQUN DAOYIN

Jean-Pierre Serre
Translated with the help of Garving K. Luli, Pin Yu

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

International Press

Author
Jean-Pierre Serre
Collège de France

图书在版编目（CIP）数据

有限群导引 = Finite Groups: An Introduction : 英文 /（法）塞尔（Serre, J. P.）著. -- 北京 : 高等教育出版社，2016.4
ISBN 978-7-04-044641-8

Ⅰ. ①有… Ⅱ. ①塞… Ⅲ. ①有限群－英文 Ⅳ. ① O152.1

中国版本图书馆 CIP 数据核字（2016）第 044662 号

策划编辑 王丽萍　责任编辑 王丽萍　封面设计 李小璐　责任印制 毛斯璐

出版发行	高等教育出版社	网　址	http://www.hep.edu.cn
社　址	北京市西城区德外大街4号		http://www.hep.com.cn
邮政编码	100120	网上订购	http://www.hepmall.com.cn
印　刷	北京中科印刷有限公司		http://www.hepmall.com
开　本	787mm×1092mm 1/16		http://www.hepmall.cn
印　张	12.25		
字　数	230 千字	版　次	2016 年 4 月第 1 版
购书热线	010-58581118	印　次	2016 年 4 月第 1 次印刷
咨询电话	400-810-0598	定　价	59.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换
版权所有 侵权必究
物 料 号 44641-00

Surveys of Modern Mathematics

Surveys of Modern Mathematics

Mathematics has developed to a very high level and is still developing rapidly. An important feature of the modern mathematics is strong interaction between different areas of mathematics. It is both fruitful and beautiful. For further development in mathematics, it is crucial to educate students and younger generations of mathematicians about important theories and recent developments in mathematics. For this purpose, accessible books that instruct and inform the reader are crucial. This new book series "Surveys of Modern Mathematics" (SMM) is especially created with this purpose in mind. Books in SMM will consist of either lecture notes of introductory courses, collections of survey papers, expository monographs on well-known or developing topics.

With joint publication by Higher Education Press (HEP) inside China and International Press (IP) in the West with affordable prices, it is expected that books in this series will broadly reach out to the reader, in particular students, around the world, and hence contribute to mathematics and the world mathematics community.

Series Editors

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, I added two chapters on finite subgroups of GL_n, and on "small groups", and I also added about 160 exercises.

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

Jean-Pierre Serre, Paris, Spring 2016

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 either $A.B$ or 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 $\geqslant 0$, then:

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

$\mathrm{GL}_n(A) = \mathrm{M}_n(A)^\times$ = group of invertible $n \times n$ 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 $\mathrm{PSL}_n(k)$.

Contents

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 that 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

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

Inner automorphisms and conjugacy classes. Let $g \in G$. The map $\mathrm{int}_g : x \mapsto gxg^{-1}$ is an automorphism of G, which is called the **inner automorphism** defined by g. The map $g \mapsto \mathrm{int}_g$ is a homomorphism of G into the automorphism group $\mathrm{Aut}(G)$ of G. It defines an action of G on itself; the orbits of that action are the **conjugacy classes** of G. 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:

Proposition 1.1. *Let G be a finite group and let X be a finite G-set. For every $g \in G$, let $X^g \subset X$ be the set of elements x of X which are fixed under the action of g, and let $\chi_X(g) = |X^g|$. Then :*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} \chi_X(g). \tag{1.3}$$

[In other words, the number of orbits is the average of the number of fixed points of the elements of the group.]

Proof. By splitting X into orbits, we may assume that G acts transitively, hence that $X = G/H$, where H is a subgroup of G. If $(g, x) \in G \times X$, define $f(g, x)$ to be equal to 1 if $gx = x$, and to 0 if $gx \neq x$. Let us compute in two different ways the sum $S = \sum_{(g,x) \in G \times X} f(g, x)$:

i) For $x \in X$, the sum $\sum_{g \in G} f(g, x)$ is the number of elements of G which fix x, i.e., $|H|$. Hence $S = |X|\,|H| = |G|$.

ii) For $g \in G$, the sum $\sum_{x \in X} f(g, x)$ is the number of elements of X fixed by g, i.e., $\chi_X(g)$. Hence $S = \sum_{g \in G} \chi_X(g)$.

By comparing the two formulas, we obtain $|G| = \sum_{g \in G} \chi_X(g)$, which is equivalent to (1.3) since $|X/G| = 1$.

1.2 Normal subgroups, automorphisms, characteristic subgroups, simple groups

Recall that a subgroup H of G is **normal** if, for all $x \in G$ and all $h \in H$, we have $xhx^{-1} \in H$. This means that H is stable under the inner automorphisms of G. The quotient G/H has a unique group structure such that $G \to G/H$ is a homomorphism, and we have the exact sequence:

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1\,.$$

Note. A sequence of group homomorphisms $\cdots \to G_i \to G_{i+1} \to \cdots$ is said to be **exact** if, for every i, the kernel of $G_i \to G_{i+1}$ is equal to the image of $G_{i-1} \to G_i$.

Example. The inner automorphisms $\{\mathrm{int}_g\}_{g \in G}$ make up a normal subgroup $\mathrm{Int}(G)$ of the group $\mathrm{Aut}(G)$ of all the automorphisms of G. The quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Int}(G)$ is the **outer automorphism group** of G. We thus have exact sequences :

$$1 \to Z(G) \to G \to \mathrm{Int}(G) \to 1 \quad \text{and} \quad 1 \to \mathrm{Int}(G) \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1,$$

where $Z(G) = C_G(G)$ is the **center** of G.

If H is a normal subgroup of a group G, the action of G on H by inner automorphisms defines a homomorphism $G \to \mathrm{Aut}(H)$; this homomorphism maps H onto $\mathrm{Int}(H)$, hence defines a map: $G/H \to \mathrm{Out}(H)$.

Proposition 1.2. *Let M and N be two normal subgroups of G such that $M \cap N = 1$. Then M and N commute elementwise, i.e., $xy = yx$ for every $x \in M$ and $y \in N$.*

Indeed, the element $x\,yx^{-1}y^{-1} = xyx^{-1}\,y^{-1}$ belongs to both M and N, hence is equal to 1.

Definition 1.6. *A subgroup H of G is **characteristic** if it is stable under every automorphism of G.*

Such a subgroup is normal in G. More generally, if $H \subset N \subset G$, with H is characteristic in N, and N normal in G, then H is normal in G.

Examples. The **center** $Z(G) = C_G(G)$ of G is a characteristic subgroup. The **derived group** of G is characteristic, and so are the subgroups D^nG, C^iG and $\Phi(G)$ defined in chap.3.

Definition 1.7. *A group G is **simple** if the number of its normal subgroups is 2. Equivalently, $G \neq 1$, and the only normal subgroups of G are 1 and G.*

Examples.

1. The abelian simple groups are the cyclic groups of prime order, i.e., the groups $\mathbf{Z}/p\mathbf{Z}$ for some prime p.
2. The alternating subgroup $\mathcal{A}_n$ is simple abelian if $n = 3$, and simple nonabelian if $n \geqslant 5$, cf. exerc.19, or Huppert [25], p.156, Satz 2.4, or Lang [29], chap.I, th. 5.5.
3. If K is a field, the group $\mathbf{PSL}_n(K)$ is simple for $n \geqslant 2$, except when $n = 2$ and $|K| = 2$ or 3, cf. chap.3, exerc.7, or Huppert [25], p.182, Satz 6.13, or Lang [29], chap.XIII, §8 and §9.
4. A nonabelian simple group of order < 200 has order either 60 or 168; it is isomorphic to either $\mathcal{A}_5$ or $\mathrm{SL}_3(\mathbf{F}_2)$, cf. §7.7.

For more information on the structure of the finite simple groups, including the *sporadic* ones, see Gorenstein [21], Gorenstein-Lyons-Solomon [22] and Wilson [39]. The reader will find in these books a precise statement of the *Classification of Finite Simple Groups* (CFSG), and of its many remarkable consequences (see especially [21], §1.7). Whether this statement is presently a theorem is not clear. The only detailed proof is that of the series [22], and it is not complete yet.

In this book, when we quote a result which depends on CFSG, we state this dependence explicitly.

1.3 Filtrations and Jordan-Hölder theorem

Definition 1.8. *A **filtration** of a group G is a sequence of subgroups $(G_i)_{0\leqslant i\leqslant n}$ such that*

$$G_0 = G \supset G_1 \supset \cdots \supset G_i \supset \cdots \supset G_n = 1, \tag{1.4}$$

with G_{i+1} normal in G_i, for $i = 1, \ldots, n-1$. Given a filtration $(G_i)_{0\leqslant i\leqslant n}$, the successive quotients $G_i/G_{i+1}, 0 \leqslant i < n$, are denoted by $\mathrm{gr}_i(G)$. The sequence of the $\mathrm{gr}_i(G)$ is denoted by $\mathrm{gr}(G)$.

Remark. There are several variants of the above definition: one may use infinite filtrations, or filtrations beginning with G_1 intead of G_0, or filtrations not ending with 1, etc.

Definition 1.9. *A filtration $(G_i)_{0\leqslant i\leqslant n}$ of G is called a **Jordan-Hölder filtration** (or a **Jordan-Hölder series** or a **composition series**) if $\mathrm{gr}_i(G) = G_i/G_{i+1}$ is simple for every i such that $0 \leqslant i < n$. The number n is called the **length** of the filtration.*

Proposition 1.3. *Every finite group has a Jordan-Hölder filtration.*

Proof. If $G = 1$, take the trivial Jordan-Hölder filtration with $n = 0$ in (1.4); if G is simple, take $n = 1$ in (1.4). Suppose that G is neither 1 nor simple. Use induction on the order of G. Let N be a normal subgroup of G, distinct from G, and of maximal order. Then G/N is simple. Since $|N| < |G|$, we apply the induction hypothesis to N and we obtain a Jordan-Hölder filtration (N_i) for N. Then $(G, N_0, N_1, \ldots)$ is a Jordan-Hölder filtration for G.

Remark. An infinite group may not have a Jordan-Hölder filtration; example: $\mathbf{Z}$.

Theorem 1.4 (Jordan-Hölder). *Let $(G_i)_{0\leqslant i\leqslant n}$ be a Jordan-Hölder filtration of a group G. Then the $\mathrm{gr}_i(G)$ (the successive factor groups) do not depend on the choice of the filtration, up to permutation of the indices. In particular, the length of the filtration is independent of the filtration.*

[The length of the filtration is called the *length of* G, and is denoted by $\ell(G)$; when G has no Jordan-Hölder filtration, we write $\ell(G) = \infty$.]

Proof.

Let S be a simple group, and let $n(G, (G_i), S)$ be the number of j such that G_j/G_{j+1} is isomorphic to S. What we have to prove is that $n(G, (G_i), S)$ does not depend on the chosen filtration (G_i).

Note first that, if H is a subgroup of G, a filtration (G_i) of G induces a filtration (H_i) of H by putting $H_i = G_i \cap H$.

Similarly, if N is a normal subgroup of G, we obtain a filtration of G/N by putting $(G/N)_i = G_i/(G_i \cap N) = G_iN/N$. The exact sequence $1 \to N \to G \to G/N \to 1$ gives an exact sequence

$$1 \to N_i/N_{i+1} \to G_i/G_{i+1} \to (G/N)_i/(G/N)_{i+1} \to 1,$$