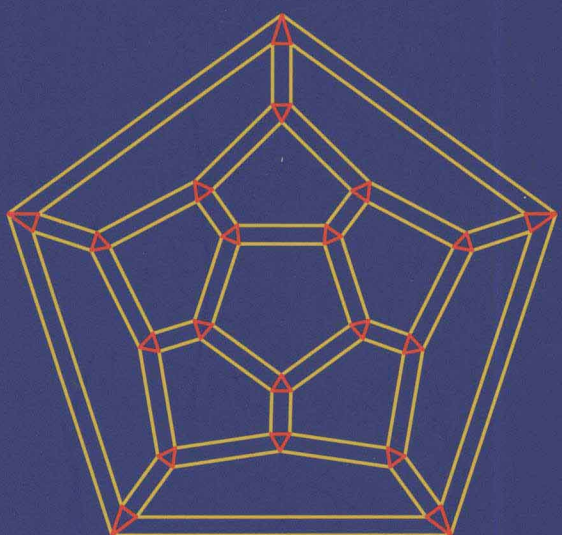
EMS Textbooks in Mathematics

Oleg Bogopolski

Introduction to Group Theory



European Mathematical Society

Oleg Bogopolski

Introduction to Group Theory

European Mathematical Society

Author:

Oleg Bogopolski
Technische Universität Dortmund
Fakultät Mathematik
Lehrstuhl VI (Algebra)
Vogelpothsweg 87
44221 Dortmund
Germany

and

Sobolev Institute of Mathematics
Siberian Branch of the Russian Academy of Sciences
4 Acad. Koptyug avenue
630090 Novosibirsk
Russia

E-mail: Oleg_Bogopolski@yahoo.com

Originally published by Institute of Computer Science, Moscow-Izhevsk
2002, under the title **Введение в теорию групп**, ISBN 5-93972-165-6

2000 Mathematical Subject Classification (primary; secondary): 20-01; 20D08, 20E05, 20E06, 20E08, 20F28

Key words: Simple groups, sporadic groups, Steiner systems, codes, free products with amalgamation, HNN extensions, actions on trees, free groups and their automorphisms, train tracks

The Swiss National Library lists this publication in The Swiss Book, the Swiss national bibliography, and the detailed bibliographic data are available on the Internet at http://www.helveticat.ch.

ISBN 978-3-03719-041-8

Contact address:

European Mathematical Society Publishing House
Seminar for Applied Mathematics
ETH-Zentrum FLI C4
CH-8092 Zürich
Switzerland

Phone: +41 (0)44 632 34 36
Email: info@ems-ph.org
Homepage: www.ems-ph.org

Typeset using the author's TEX files: I. Zimmermann, Freiburg
Printed on acid-free paper produced from chlorine-free pulp. TCF ∞
Printed in Germany

9 8 7 6 5 4 3 2 1

EMS Textbooks in Mathematics

EMS Textbooks in Mathematics is a book series aimed at students or professional mathematicians seeking an introduction into a particular field. The individual volumes are intended to provide not only relevant techniques, results and their applications, but afford insight into the motivations and ideas behind the theory. Suitably designed exercises help to master the subject and prepare the reader for the study of more advanced and specialized literature.

Jørn Justesen and Tom Høholdt, *A Course In Error-Correcting Codes*
Markus Stroppel, *Locally Compact Groups*
Peter Kunkel and Volker Mehrmann, *Differential-Algebraic Equations*
Dorothee D. Haroske and Hans Triebel, *Distributions, Sobolev Spaces, Elliptic Equations*
Thomas Timmermann, *An Invitation to Quantum Groups and Duality*
Marek Jarnicki and Peter Pflug, *First Steps in Several Complex Variables: Reinhardt Domains*

Preface

This English edition differs from the Russian original by the addition of a new chapter. In this new Chapter 3 we give an account of the theory of train tracks for automorphisms of free groups, which was developed in the seminal paper of M. Bestvina and M. Handel [9]. Our exposition is more algebraic than in this paper, but it is less technical than the account in the book [29] of W. Dicks and E. Ventura. In Section 10 of Chapter 3 we consider two examples in detail. We have added an appendix containing the famous Perron–Frobenius Theorem on nonnegative matrices, which is used in this chapter. Also we have added solutions to selected exercises.

The reader is assumed to have the knowledge of algebra expected after the first semester of university (permutations, fields, matrices, vector spaces; see [23], [39] or [55].

My sincere thanks go to Derek Robinson for invaluable help with the translation of this book and for useful comments that helped to improve the exposition. I also like to thank Hans Schneider and Enric Ventura for their suggestions on the improvement of the appendix and Chapter 3. Last but not least, I thank my wife Marie-Theres for her constant support.

Dortmund, January 2008 O. Bogopolski

Preface to the Russian Edition

This book is an extended version of a course given by me at Novosibirsk University from 1996 to 2001. The purpose of the book is to present the fundamentals of group theory and to describe some nontrivial constructions and techniques, which will be useful to specialists. The fundamentals are given in Sections 1–9 of Chapter 1; also one can read Chapters 1 and 2 independently.

In Chapter 1 we quickly introduce beginners to the classification of finite simple groups. It is shown that such complicated combinatorial objects as the Mathieu group M_{22} and the Higman–Sims group HS have a natural geometric description. In Section 17 we describe the relationship between Mathieu groups and Steiner systems with coding theory.

In Chapter 2 we describe the Bass–Serre theory of groups acting on trees. This theory gives a clear and natural explanation of many results about free groups and free constructions. We also explain the theory of coverings: the attentive reader will see a bridge from one theory to the other. I hope that numerous examples, exercises and figures will help to give a deeper understanding of the subject.

The reader is assumed to have the knowledge of algebra expected after the first semester of university (permutations, fields, matrices, vector spaces; see [39]). In addition, the fundamentals of group theory (especially abelian, nilpotent and solvable groups) can be read in the excellent book of M. I. Kargapolov and Ju. I. Merzljakov [38].

I thank many colleagues whose comments helped to improve the content and exposition of the material presented in this book. In particular I thank V. G. Bardakov, A. V. Vasiljev, E. P. Vdovin, A. V. Zavarnitzin, V. D. Mazurov, D. O. Revin, O. S. Tishkin and V. A. Churkin.

I thank M.-T. Bochnig for the help in designing this book.

Novosibirsk, May 11, 2002 O. Bogopolski

A tree in the neighborhood of Sprockhövel (Germany)

Contents

Chapter 1
Introduction to finite group theory

1 Main definitions

A *binary operation* $\cdot$ on a set G assigns to any two elements a, b of G an element of G denoted by $a \cdot b$. A binary operation can be denoted not only by $\cdot$ but by any other symbol, for example by $+$. Usually one writes ab instead of $a \cdot b$.

A set G with a binary operation is called a *group* if the following holds:

1) the operation is *associative*, i.e., $(ab)c = a(bc)$ for all a, b, c in G;
2) in G there is an element e – called the *identity element* – such that $ae = ea = a$ for all a in G;
3) for each a in G there is in G an element b – called *the inverse* of a – such that $ab = ba = e$.

The identity element can be denoted by 1 if the operation is denoted by $\cdot$, and it can be denoted by 0 if the operation is denoted by $+$.

1.1 Exercise. 1) The identity element of any group G is unique. Each element a in G has a unique inverse (denoted by a^{-1}).

2) For any element a in G, the mapping $\varphi_a : G \to G$ given by the rule $\varphi_a(g) = ag$ $(g \in G)$ is a bijection.

A group is called *trivial* if it only contains the identity element.

A group G is called *abelian* or *commutative* if $ab = ba$ for any a, b in G. The set $\mathbb{Z}$ of integers with the usual addition is an abelian group. Examples 1.3 show that there exist nonabelian groups.

Two groups G and G_1 are called *isomorphic* (one writes $G \cong G_1$) if there exists an *isomorphism* $\varphi : G \to G_1$, i.e., a bijection φ from G onto G_1 such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all a, b in G.

Thanks to the associative law for groups, the product $a_1 a_2 \ldots a_n$ of n elements of a group does not depend on the bracketing. The product of n elements all equal to a is denoted by a^n. We define $a^0 = e$ and $a^m = (a^{-1})^{-m}$ for negative integers m.

If $a^n = e$ for some $n > 0$, then the smallest n with this property is called the *order of the element* a and is denoted by $|a|$. If $a^n \neq e$ for every $n > 0$, we say that a has *infinite order* and write $|a| = \infty$. The cardinality $|G|$ of a group G is called the *order* of G. If this cardinality is finite, then we say that the group is *finite*, and in the contrary case *infinite*. A finite group G is called a *p-group* if $|G| = p^k$ for a prime number p and an integer $k \geqslant 1$.

1.2 Exercise. 1) If $a^n = e$, then $|a|$ divides n.

2) If a and b commute, that is $ab = ba$, and their orders are relatively prime, then $|ab| = |a| \cdot |b|$.

A nonempty subset H of a group G is called a *subgroup* of G if for any a, b from H the elements ab and a^{-1} also lie in H. In that case we write $H \leqslant G$. A subgroup H of a group G is itself a group under the restriction of the operation of the group G. If $H \leqslant G$ and $H \neq G$, then H is called a *proper* subgroup of G; in symbols $H < G$.

Following the terminology of the textbooks [39], [55], we use the following rule for composition of two mappings: $(fg)(x) = f(g(x))$. Thus we multiply permutations from the right to the left.

1.3 Examples. 1) An *isometry* of the Euclidean plane is any mapping of the plane onto itself, preserving the distances between any two points.

Let F be a figure in the Euclidean plane. The set of all isometries of the plane, sending F onto itself, is a group under the composition of isometries. This group is called the *symmetry group* of F.

Let P_n be a regular n-gon. The symmetry group of P_n has exactly $2n$ elements: n clockwise rotations through the angles $\frac{2\pi k}{n}$ $(k = 0, 1, \ldots, n-1)$ about the center of P_n and n reflections across the lines, passing through its center and one of its vertices, or through its center and the middle point of one of its sides. All rotations in the symmetry group of P_n form a subgroup, which is called the *rotation group* of P_n.

2) The set of all permutations of the set $\{1, 2, \ldots, n\}$ is a group under the usual multiplication of the permutations. This group is called the *symmetric group of degree n* and is denoted by S_n. All even permutations in S_n form a subgroup which is denoted by A_n and is called the *alternating group of degree n*. The order of the group S_n is $n!$ and the order of the group A_n is $n!/2$ for $n \geqslant 2$.

3) The set $\mathrm{GL}_n(K)$ of all invertible matrices of size $n \times n$ over a field K is a group under the usual matrix multiplication. It is called the *general linear group* of degree n over the field K. Its subgroup $\mathrm{SL}_n(K)$ consisting of all matrices with determinant 1 is called the *special linear group* of degree n over K. The group $\mathrm{SL}_n(K)$ contains a subgroup $\mathrm{UT}_n(K)$ consisting of those matrices with all entries below the main diagonal zero, and with the entries on the main diagonal equal to the identity. This subgroup is called the *unitriangular group* of degree n over K.

It is known (see [39] or [55] for example) that a finite field is defined up to an isomorphism by the number of its elements, and this number must be a power of a prime number. Therefore if a field K contains exactly q elements, we will write $\mathrm{GL}_n(q)$ instead of $\mathrm{GL}_n(K)$, and similarly for the other matrix groups.

1.4 Exercise. The symmetry group of a regular triangle is isomorphic to the group S_3.

For any nonempty subset M of a group G the set

$$\{a_1^{\epsilon_1} \dots a_m^{\epsilon_m} \mid a_i \in M,\ \epsilon_i = \pm 1,\ m = 1, 2, \dots\}$$

forms a subgroup of G. This subgroup is called the subgroup *generated* by the set M and is denoted by $\langle M \rangle$. It is easily seen that $\langle M \rangle$ is the smallest subgroup of G containing the set M.

For ease of notations we write $\langle a, b, \dots, c \rangle$ instead of $\langle \{a, b, \dots, c\} \rangle$ and we say that this subgroup is *generated* by the elements $a, b, \dots, c$. Some other simplifications of notations are also allowed. For example, if A and B are two subsets of a group G and c is an element of G, then we write $\langle A, B, c \rangle$ instead of $\langle A \cup B \cup \{c\} \rangle$.

A group is called *finitely generated* if it can be generated by a finite number of elements.

A group G is called *cyclic* if in G there exists an element a with $G = \langle a \rangle$. In this case $G = \{a^n \mid n \in \mathbb{Z}\}$. Notice: it may happen that a^n coincides with a^m for some $n \neq m$. In that case G is finite. An example of an infinite cyclic group is the group $\mathbb{Z}$ of all integers under the usual addition (as a one can take 1 or -1).

Let $n \geqslant 1$ be a natural number. To each integer i there corresponds the remainder on division of i by n, i.e., an integer $\bar{i}$ such that $0 \leqslant \bar{i} \leqslant n - 1$ and $n \mid (i - \bar{i})$. It is easy to verify that the set $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ with the operation $\oplus$, defined by the rule $i \oplus j = \overline{i + j}$, is a cyclic group generated by 0 if $n = 1$ and by 1 if $n > 1$.

1.5 Exercise. The rotation group of a regular n-gon is isomorphic to the group $\mathbb{Z}_n$.

1.6 Theorem. *Any infinite cyclic group is isomorphic to the group $\mathbb{Z}$, and any finite cyclic group of order n is isomorphic to the group $\mathbb{Z}_n$.*

Proof. Let $\langle a \rangle$ be an infinite cyclic group. Define a mapping $\varphi\colon \mathbb{Z} \to \langle a \rangle$ by the rule $\varphi(i) = a^i$. Clearly, $\varphi(i + j) = \varphi(i)\varphi(j)$ and φ is onto. Moreover, φ is injective: if we had $a^i = a^j$ for some $i < j$, then $a^{j-i} = e$ and the group $\langle a \rangle$ would contain only the elements $e, a, \dots, a^{j-i-1}$, which is impossible. Therefore φ is an isomorphism.

If $\langle a \rangle$ is a cyclic group of order n, then the mapping $\varphi\colon \mathbb{Z}_n \to \langle a \rangle$, given by the same rule $\varphi(i) = a^i$, is an isomorphism. □

An arbitrary infinite cyclic group will be denoted by Z and an arbitrary finite cyclic group of order n will be denoted by Z_n.

1.7 Theorem. *Any subgroup of a cyclic group is cyclic.*

Proof. Let $\langle a \rangle$ be a cyclic group. Clearly, the trivial subgroup is cyclic. Let H be a nontrivial subgroup of $\langle a \rangle$ and let m be the smallest positive integer such that $a^m \in H$. Clearly $\langle a^m \rangle \leqslant H$. We will prove that $\langle a^m \rangle = H$. An arbitrary element of H has the form a^k. Dividing k by m, we get $k = mq + r$, $0 \leqslant r < m$. Then $a^r = a^k (a^m)^{-q} \in H$. By the minimality of m it follows that $r = 0$. Hence $a^k = (a^m)^q \in \langle a^m \rangle$. □

1.8 Exercise. 1) The order of any subgroup of Z_n is a divisor of n. Moreover, for any divisor d of n there exists a unique subgroup of Z_n of order d.

2) The number of solutions of the equation $x^k = 1$ in the group Z_n is equal to $\gcd(n, k)$, the greatest common divisor of n and k.

The *center* of a group G is the subset

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

Clearly $Z(G)$ is a subgroup of G and G is abelian if and only if $Z(G) = G$.

The *commutator* of two elements a and b is the element $aba^{-1}b^{-1}$. We denote it by $[a, b]$. The *commutator subgroup* or *derived subgroup* of a group G is the subgroup $G' = \langle [a, b] \mid a, b \in G \rangle$.

We say that an element a of a group G is *conjugate* to an element b by an element g if $a = gbg^{-1}$. Similarly, we say that a subgroup A of a group G is conjugate to a subgroup B by an element g if $A = \{gbg^{-1} \mid b \in B\}$. This set will be denoted by gBg^{-1}. It is easy to verify that the orders of conjugate elements (subgroups) are the same.

The *conjugacy class* of an element b of a group G is the set of all elements in G which are conjugate to b. The group G is divided into disjoint conjugacy classes, one of them being $\{e\}$.

An *automorphism* of a group G is an isomorphism of G onto itself. The set of all automorphisms of G with functional composition is a group, denoted by $\mathrm{Aut}(G)$.

1.9 Exercise. 1) Prove that $\mathrm{Aut}(\mathbb{Z}) \cong Z_2$.

2) Find the center, the commutator subgroup and the conjugacy classes of the permutation group S_3.

3) Prove that $S_n = \langle (12), (13), \ldots, (1n) \rangle$.

4) Prove that the group $\mathbb{Q}$ of rational numbers under addition is not finitely generated.

2 Lagrange's theorem. Normal subgroups and factor groups

Let H be a subgroup of a group G. The sets $gH = \{gh \mid h \in H\}$, where $g \in G$, are called *left cosets* of the subgroup H in the group G. *Right cosets* Hg are defined similarly. It is easy to verify that

$$g_1 H = g_2 H \quad \text{if and only if} \quad g_1^{-1} g_2 \in H.$$

2.1 Example. The set of all left cosets of the subgroup $\{e, (12)\}$ in the group S_3 consists of

$$\{e, (12)\}, \quad \{(13), (123)\}, \quad \{(23), (132)\}.$$

The set of all right cosets of the subgroup $\{e, (12)\}$ in the group S_3 consists of

$$\{e, (12)\}, \quad \{(13), (132)\}, \quad \{(23), (123)\}.$$

The correspondence $xH \leftrightarrow Hx^{-1}$ is one-to-one, and therefore the cardinality of the set of left cosets of H coincides with the cardinality of the set of right cosets of H. This cardinality is called the *index* of the subgroup H in the group G and is denoted by $|G : H|$.

2.2 Theorem (Lagrange). *If H is a subgroup of a finite group G, then*

$$|G| = |H| \cdot |G : H|.$$

Proof. Since $g \in gH$, the group G is the union of the left cosets of H in G. Any two different cosets have empty intersection: if $g_1H \cap g_2H \neq \varnothing$, then $g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$ and so $g_1H = g_2h_2h_1^{-1}H = g_2H$. It remains to notice that these left cosets have the same cardinality: a bijection $H \to gH$ is given by the rule $h \mapsto gh$, $h \in H$. □

2.3 Corollary. 1) *The order of an element of a finite group divides the order of this group.*

2) *Any group of prime order p is isomorphic to the group Z_p.*

Proof. If g is an element of a finite group G, then $|g| = |\langle g \rangle|$ and $|\langle g \rangle|$ divides $|G|$. In particular, if $|G| = p$ is a prime number and $g \neq e$, then $|\langle g \rangle| = |G|$, hence $G = \langle g \rangle \cong Z_p$. □

The product of two subsets A and B of a group G is defined as $AB = \{ab \mid a \in A, b \in B\}$. Let $H \leqslant G$ and $g \in G$. Then the product $\{g\}H$ coincides with the left coset gH. Moreover, we have $HH = H$.

We say that a subgroup H of G is *normal* in G and write $H \trianglelefteqslant G$ if $gH = Hg$ for every $g \in G$. Let $H \trianglelefteqslant G$. Then the product of any two cosets of H in G is again a coset of H in G:

$$g_1H \cdot g_2H = g_1(Hg_2)H = g_1(g_2H)H = g_1g_2H.$$

The set of all cosets of H in G with this product forms a group. Its identity element is the coset H, the inverse of the coset xH is the coset $x^{-1}H$. This group is called the *quotient group* or the *factor group* of the group G by the normal subgroup H and is denoted by G/H. By Lagrange's theorem, if G is finite then $|G| = |H| \cdot |G/H|$.

2.4 Example. The subgroup $K = \{e, (12)(34), (13)(24), (14)(23)\}$ of S_4 is normal and

$$S_4/K = \{K, (12)K, (13)K, (23)K, (123)K, (132)K\} \cong S_3.$$

2.5 Exercise. 1) Prove that $Z(G) \trianglelefteqslant G$, $G' \trianglelefteqslant G$ and G/G' is an abelian group.

2) If $H_1 \leqslant H \leqslant G$, then $|G : H_1| = |G : H| \cdot |H : H_1|$.

3) If H is a subgroup of index 2 in a group G, then $H \trianglelefteq G$.

4) The product of any two subsets H_1, H_2 of a group G need not be a subgroup, even if both H_1 and H_2 are subgroups. If both H_1 and H_2 are subgroups and one of them is normal in G, then H_1H_2 is a subgroup in G. If both subgroups H_1 and H_2 are normal in G, then the subgroup H_1H_2 is also normal in G.

5) If A, B are finite subgroups of a group G, then

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

3 Homomorphism theorems

A mapping φ from a group G to a group G_1 is called a *homomorphism*, if $\varphi(ab) = \varphi(a)\varphi(b)$ for every $a, b \in G$. The *kernel* of the homomorphism φ is the set $\ker\varphi = \{g \in G \mid \varphi(g) = e\}$. The *image* of the homomorphism φ is the set $\operatorname{im}\varphi = \{\varphi(g) \mid g \in G\}$.

3.1 Exercise. Let $\varphi\colon G \to G_1$ be a homomorphism. Then the following assertions are valid.

1) $\varphi(e) = e$, $\varphi(g^{-1}) = (\varphi(g))^{-1}$ for $g \in G$.
2) If $g \in G$ is an element of a finite order, then $|\varphi(g)|$ divides $|g|$.
3) $\ker\varphi \trianglelefteq G$, $\operatorname{im}\varphi \leqslant G_1$.
4) For any two nonempty subsets A, B of a group G holds[1]

$$\varphi(A) = \varphi(B) \iff A \cdot \ker\varphi = B \cdot \ker\varphi.$$

3.2 Example. 1) Let K^* be a *multiplicative group* of a field K, i.e., the group of all its nonzero elements under multiplication. The mapping $\varphi\colon \mathrm{GL}_n(K) \to K^*$, assigning to a matrix its determinant, is a homomorphism with kernel $\mathrm{SL}_n(K)$.

2) Let $H \trianglelefteq G$. The mapping $\varphi\colon G \to G/H$ given by the rule $\varphi(g) = gH$ is a homomorphism with kernel H.

Given a subgroup H of a group G, we denote by $L(G, H)$ the set of all subgroups of G containing H. In particular $L(G, \{1\})$ is the set of all subgroups of the group G.

3.3 Theorem. *Let $\varphi\colon G \to G_1$ be a homomorphism onto a group G_1. Then*

1) *the mapping $\psi\colon L(G, \ker\varphi) \to L(G_1, \{1\})$, sending a subgroup from the first set into its image under φ is a bijection;*
2) *this bijection preserves indexes:*

$$\textit{if } \ker\varphi \leqslant H_1 \leqslant H_2, \textit{ then } |H_2 : H_1| = |\varphi(H_2) : \varphi(H_1)|;$$

[1] We use the notation $\varphi(A) = \{\varphi(a) \mid a \in A\}$.

3) *this bijection preserves the normality:*

$$\text{if } \ker\varphi \leqslant H_1 \leqslant H_2, \text{ then } H_1 \lhd H_2 \iff \varphi(H_1) \lhd \varphi(H_2).$$

Proof. 1) The mapping ψ is onto, since the full preimage of the subgroup of the group G_1 is a subgroup of G containing $\ker\varphi$. The mapping is one-to-one: this follows from Exercise 3.1.4 and the fact that $H \cdot \ker\varphi = H$ for any subgroup H of the group G containing $\ker\varphi$.

2) The mapping from the set of the left cosets of H_1 in H_2 to the set of the left cosets of $\varphi(H_1)$ in $\varphi(H_2)$, given by the rule $xH_1 \mapsto \varphi(x)\varphi(H_1)$, is onto. The mapping is one-to-one since $\varphi(xH_1) = \varphi(yH_1)$ implies $xH_1 \cdot \ker\varphi = yH_1 \cdot \ker\varphi$, that is $xH_1 = yH_1$.

3) We have $H_1 \cdot \ker\varphi = H_1$ and $x \cdot \ker\varphi = \ker\varphi \cdot x$ for $x \in G$. Therefore the condition $xH_1 = H_1x$ is equivalent to $xH_1 \cdot \ker\varphi = H_1x \cdot \ker\varphi$, which is equivalent to $\varphi(x)\varphi(H_1) = \varphi(H_1)\varphi(x)$ because of Exercise 3.1.4. □

3.4 Theorem. *If $\varphi\colon G \to G_1$ is a homomorphism, then $G/\ker\varphi \cong \operatorname{im}\varphi$.*

Hint. The isomorphism is given by the rule $g\ker\varphi \mapsto \varphi(g)$, $g \in G$.

3.5 Theorem. *Let $A \leqslant B \leqslant G$, $A \lhd G$, $B \lhd G$. Then $B/A \lhd G/A$ and $(G/A)/(B/A) \cong G/B$.*

Hint. Apply Theorem 3.4 to the homomorphism $\varphi\colon G/A \to G/B$ given by the rule $gA \mapsto gB$.

3.6 Theorem. *Let $H \lhd G$, $B \leqslant G$. Then $BH/H \cong B/B \cap H$.*

Hint. The homomorphism $\varphi\colon BH \to B/B\cap H$ given by the rule $bh \mapsto b(B\cap H)$, $b \in B$, $h \in H$, has the kernel H.

Finally we explain some terminology. A homomorphism $\varphi\colon G \to G_1$ is called an *epimorphism* if its image is equal to G_1. A homomorphism is called a *monomorphism* (or *an embedding*) if its kernel is trivial. The group G is *embeddable* into the group G_1 if there exists an embedding of G into G_1. Obviously, an isomorphism is an epimorphism and a monomorphism simultaneously.

4 Cayley's theorem

For any set M we denote by $S(M)$ the group of all bijections of M onto itself, i.e., permutations of M. If the cardinality m of M is finite, then we can identify the group $S(M)$ with the group S_m.

4.1 Theorem (Cayley). *Let H be a subgroup of a group G and let M be the set of all left cosets of H in G. Define the mapping $\varphi\colon G \to S(M)$ by the rule: for any $g \in G$ the permutation $\varphi(g)$ sends a coset xH to the coset gxH.*

Then φ is a homomorphism (not necessarily onto) with kernel

$$\ker\varphi = \bigcap_{x\in G} xHx^{-1}.$$

Proof. Clearly $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ since $g_1g_2(xH) = g_1(g_2xH)$ for any $x \in G$. Moreover,

$$g \in \ker\varphi \iff (xH = gxH \text{ for all } xH) \iff (g \in xHx^{-1} \text{ for all } x). \quad \square$$

If $H = \{1\}$, the homomorphism φ from Cayley's theorem is called the (*left*) *regular representation* of the group G.

4.2 Corollary. 1) *The regular representation of a group G is an embedding of the group G into the group $S(G)$. The image of any nontrivial element of G under this embedding is a permutation, which sends each element of G to a different element of G.*

Any finite group G can be embedded into the group S_m where $m = |G|$.

2) *Any finite group G can be embedded into the group $\mathrm{GL}_m(F)$, where F is any field and $m = |G|$.*

Proof. The first claim follows from Cayley's theorem, the second from the first, using the embedding of S_m into $\mathrm{GL}_m(F)$ given by the rule $\sigma \mapsto A_\sigma$, where $(A_\sigma)_{ij} = 1$ if $\sigma(j) = i$ and $(A_\sigma)_{ij} = 0$ otherwise. $\square$

4.3 Exercise. Any group of order 4 is isomorphic to the group Z_4 or to the group $K = \{e, (12)(34), (13)(24), (14)(23)\}$.

Solution. Let G be a group of order 4. We identify G with its image under the regular representation into S_4. Then any nontrivial element of the group G is either a cycle of length 4, or the product of two disjoint transpositions (otherwise a fixed element would appear). If G contains a cycle of length 4, then $G \cong Z_4$ and otherwise $G \cong K$.

4.4 Corollary (Poincaré). *Every subgroup H of finite index m in a group G contains a subgroup N which is normal in G and has finite index k such that $m \mid k$ and $k \mid (m!)$.*

Proof. We set $N = \ker\varphi$, where φ is the homomorphism from Cayley's theorem. Let $k = |G : N|$. By Theorem 3.4, $k = |\mathrm{im}\,\varphi|$. Since $\mathrm{im}\,\varphi$ is a subgroup of the group S_m, we obtain $k \mid (m!)$. The claim that $m \mid k$ follows from $\ker\varphi \leqslant H \leqslant G$ with the help of Exercise 2.5.2. $\square$