Groups

Table of Contents

1. Definitions, examples, and basic properties 2
   1.1. Semigroups, monoids, and groups 2
   1.2. Examples of groups 2
   1.3. The very elementary properties and the order of elements of a group 4
   1.4. Isomorphisms of groups 4
   1.5. Subgroups 4
   1.6. Generating sets and relations 5
   1.7. Cyclic groups and their subgroups 5
   1.8. Direct products of groups 5
   1.9. Finite groups of matrices 6
   1.10. The lattice of subgroups of a group 6
   1.11. Commuting elements, conjugate elements, the center, and the centralizers of elements 6
   1.12. The symmetric group $S_n$ 7

2. Factorization and homomorphisms 7
   2.1. Cosets and counting principles 7
   2.2. Normal subgroups and factorization 8
   2.3. Conjugation, normalizers and centralizers 9
   2.4. Simple groups and composition series 10
   2.5. Conjugacy classes in $S_n$ and simplicity of $A_n$ for $n \geq 5$ 10
   2.6. Homomorphisms of groups 11
   2.7. The isomorphism theorems 11
   2.8. Reduction of a homomorphism to a quotient group 12

3. Actions of groups on sets and on themselves 13
   3.1. Group actions 13
   3.2. The left regular action 13
   3.3. The action of a group on itself by conjugations 14

4. Direct product of groups 14
   4.1. Direct products of two groups 14
   4.2. A relative direct product 15
   4.3. Direct product of several groups 15
   4.4. Direct product of infinitely many groups 16

5. The Chinese remainder theorem and a complete classification of finite abelian groups 16
   5.1. The Chinese remainder theorem 16
   5.2. The classification of finite abelian groups 16
   5.3. The groups $\mathbb{Z}_n^\ast$. 18

6. Groups of automorphisms and semidirect products of groups 19
   6.1. Groups of automorphisms 19
   6.2. Characteristic subgroups 19
   6.3. Semidirect product of groups 20

7. Sylow theorems and groups of small orders 22
   7.1. $p$-groups 22
   7.2. Sylow’s theorems 22
   7.3. Groups of small orders 24
   7.4. Some simple methods of proving that a finite group is not simple 26

8. Commutator calculus, solvable and nilpotent groups 26
   8.1. Commutators and the derived subgroup 26
   8.2. Derived series and solvable groups 27
   8.3. Central series and nilpotent groups 27

9. Some facts about free groups 28
1. Definitions, examples, and basic properties

1.1. Semigroups, monoids, and groups

1.1.1. Let \( S \) be a set. A binary operation \( * : S \times S \rightarrow S \). The result of the application of the operation to elements \( a, b \in S \) is usually denoted by \( a * b \) (instead of \( *(a, b) \)).

Examples. Examples of binary operations are addition (on \( \mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C} \), etc.), subtraction (on \( \mathbb{Z}, \mathbb{R}, \mathbb{C} \), etc.), multiplication (on \( \mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C} \), etc.), division (on \( \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^* = \mathbb{R} \setminus \{0\}, \mathbb{C}^* = \mathbb{C} \setminus \{0\} \), etc.); addition and multiplication of matrices; union and intersection (on the power set \( \mathcal{P}(X) \) of a set \( X \)); composition (on the set of self-mappings of a set \( X \)); concatenation (on the set of words in an alphabet \( A \)).

1.1.2. A binary operation \( * \) on a set \( S \) is said to be associative if \( (a * b) * c = a * (b * c) \) for all \( a, b, c \in S \). A binary operation \( * \) on a set \( S \) is said to be commutative if \( a * b = b * a \) for all \( a, b \in S \).

Examples. Addition and multiplication of numbers are associative and commutative, subtraction and division are neither. Composition of mappings and concatenation of words are associative but not commutative.

A set with an associative binary operation is called a semigroup. If this operation is commutative, then the semigroup is said to be commutative.

1.1.3. An element \( e \) of a semigroup \((S, \ast)\) is said to be left-neutral, or a left identity, if \( e * a = a \) for all \( a \in S \); right-neutral, or a right identity, if \( a * e = a \) for all \( a \in S \); and neutral, or an identity, if both \( e * a = a * e = a \) for all \( a \in S \).

Lemma. If a semigroup has both a left- and a right-neutral elements, then they are unique and equal. In particular, if a semigroup has a neutral element, it is unique.

A semigroup with a neutral element is called a monoid.

1.1.4. Let \((S, \ast)\) be a monoid, with a neutral element \( e \). Let \( a \in S \); an element \( b \in S \) is called a left inverse of \( a \) if \( b * a = e \); a right inverse of \( a \) if \( a * b = e \); and an inverse of \( a \) if both \( b * a = a * b = e \).

Lemma. If an element \( a \) of a monoid has both a left and a right inverse, then these inverses are unique and equal. In particular, if a has an inverse, it is unique.

1.1.5. A group is a monoid in which every element has an inverse. (That is, a group is a set with an associative binary operation, a neutral element, and in which every element has an inverse.)

The operation in a group is usually called multiplication, and its result is called the product; the multiplication is denoted by “\( \, \cdot \, \) or just skipped (we write \( ab \) instead of \( a \cdot b \)). The neutral element is denoted by 1 or by \( 1_G \) and is called the identity. The inverse of \( a \in G \) is denoted by \( a^{-1} \). Because of the associativity of the multiplication, in products of several elements of the group the parentheses can be dropped. (For example, \((a_1a_2a_3)a_4 = a_1((a_2a_3)a_4) = a_1(a_2(a_3a_4))\) is written as \( a_1a_2a_3a_4 \).)

1.1.6. A commutative group is also called abelian. If a group is abelian, additive notation are sometimes used for it: the operation is called addition and is denoted by “\( + \)”, its result is called the sum, the neutral element is denoted by 0 and is called zero, the inverse of an element \( a \) is denoted by \( -a \).

1.1.7. Lemma. For any monoid \( S \), the set \( S^* \) of invertible elements of \( S \) is a group.

1.1.8. The number of elements in a group \( G \) is called the order of \( G \) and is denoted by \(|G|\).

1.2. Examples of groups

1.2.1. Numbers

(i) \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \) under addition and \( \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^* \) under multiplication are abelian groups.

(ii) The set \( \mathbb{Z}_n = \{0, 1, \ldots, n-1\} \) of residues modulo \( n \in \mathbb{N} \), with the operation of addition modulo \( n \), is a group of order \( n \).

(iii) \( \mathbb{Z}_n \) is a monoid under multiplication modulo \( n \); the set \( \{k \in \mathbb{Z}_n : \text{gcd}(k, n) = 1\} \) of its invertible elements is a group, denoted by \( \mathbb{Z}_n^* \). The order of \( \mathbb{Z}_n^* \) is \( \varphi(n) \), Euler’s totient function.

1.2.2. Vectors and matrices

(i) Any vector space, over any field, is an abelian group under addition.
(ii) The set $\text{Mat}_{n,m}(F)$ of $n \times m$-matrices, over a field $F$, is, actually, an $nm$-dimensional vector space. Under multiplication, the set $\text{Mat}_{n,n}(F)$ of $n \times n$ matrices is a monoid; the set $\text{Mat}^*_{n,n}(F)$ of invertible $n \times n$-matrices is a (nonabelian) group.

1.2.3. Mappings

(i) Given a set $X$, let $F(X)$ be the set of mappings $X \rightarrow X$. The operation of composition turns $F(X)$ into a noncommutative monoid. (The operation of composition can be defined in two ways: $(f \circ g)(x) = f(g(x))$, or $(f \circ g)(x) = g(f(x))$; they define two different monoid structures on $F(X)$. We will assume the first definition.) The invertible elements of $F(X)$, that is, self-bijections of $X$, form a group, called the group of permutations of $X$ and denoted by $S_X$. The group of permutations of the $n$-element set $\{1, \ldots, n\}$ is called the $n$-th symmetric group and is denoted by $S_n$.

(ii) If $X$ is a set with “a structure” (metric, topology, operation(s), etc.), then the set of mappings $f \in S_X$ such that both $f$ and $f^{-1}$ preserve this structure is a group. Such are the group of self-homeomorphisms of a topological space, the group of invertible isometries of a metric space, the group $\text{GL}(n)$ of invertible linear transformations of a vector space $V$, the group of Möbius (linear fractional) transformations of the Riemann sphere or of the unit disc.

(iii) If $R$ is a subset of a metric space $X$, then the group of isometries of $X$ preserving $R$ is called the symmetry group of $R$. In the case $R$ is a regular $n$-gon in the plane (with $n \geq 3$), the symmetry group of $R$ is called the $n$-th dihedral group and is denoted by $D_{2n}$. $D_{2n}$ is a subgroup of $S_n$, with $|D_{2n}| = 2n$, – it contains $n$ rotations (including the trivial one) and $n$ reflections.

1.2.4. Set-theoretical groups

Let $X$ be a set; under the operation $\triangle$ of symmetric difference, $A \triangle B = (A \setminus B) \cup (B \setminus A)$, the power set $\mathcal{P}(X)$ is a group. In this group, $\emptyset$ is the identity, and $A^2 = 1(= \emptyset)$, so $A^{-1} = A$, for all $A \in \mathcal{P}(X)$. (A group $G$ with the property $a^2 = 1$ for all $a \in G$ is called Boolean.)

1.2.5. Groups, appearing in topology

(i) A knot is a simple loop in $\mathbb{R}^3$ (that is, a continuous injective mapping $C \rightarrow \mathbb{R}^3$, where $C$ is a circle) up to homotopy: two loops are assumed to represent the same knot if one can be continuously transformed into the other without self-intersections. The operation on knots is concatenation; under this operation, the set of knots is a commutative monoid, with the neutral element being “the trivial” knot (a circle). However, it can be shown that no nontrivial knot has an inverse in this monoid.

(ii) A braid of $n$ strands, or an $n$-braid, is a collection of continuous mappings $f_1, \ldots, f_n: [0, 1] \rightarrow \mathbb{R}^2$ such that $f_i(0) = i$ for all $i = 1, \ldots, n$, $\{f_1(1), \ldots, f_n(1)\} = \{1, \ldots, n\}$, and $f_i(t) \neq f_j(t)$ for all $t \in [0, 1]$ and all $i \neq j$. The operation on $n$-braids is concatenation; under this operation the $n$-braids form a group, denoted by $B_n$.

(iii) Let $X$ be a (path-connected) topological (or metric) space. Choose a point $x_0 \in X$, and consider the set of loops (continuous mappings $\gamma: [0, 1] \rightarrow X$ with $\gamma(0) = \gamma(1) = x_0$, up to homotopy (up to continuous deformation) in $X$. Under the operation of concatenation, the (classes of equivalence of) these loops form a group, called the fundamental group of $X$ and denoted by $\pi_1(X)$.

1.2.6. Groups of words

(i) Given an alphabet (that is, just a set) $A$, the finite words in alphabet $A$ with the operation of concatenation form a noncommutative monoid (with the empty word being the neutral element), called the free monoid over $A$.

(ii) Given an alphabet $A$, let $A^{-1} = \{a^{-1}, a \in A\}$. Consider the free monoid over the alphabet $A \cup A^{-1}$, and in the elements of this monoid allow cancellations: any occurrences of subwords of the form $aa^{-1}$ or $a^{-1}a$, where $a \in A$, can be deleted. (For example, the word $a_1a_3a_1^{-1}a_1a_3^{-1}a_1$ is assumed to be equal to the word $a_1a_2a_1$.) We will get a group, called the free group over $A$, denoted by $F_A$. The inverse of an element $w = a_1a_2 \cdots a_k$ of this group, where $a_i \in A \cup A^{-1}$, is $w^{-1} = a_k^{-1} \cdots a_2^{-1}a_1^{-1}$ (where we assume $(a^{-1})^{-1} = a$).

(iii) In a free group $F_A$, allow replacement of certain subwords by some other words; we will then get a group with relations. (For example, given the relation $a_1a_2a_1^{-1}a_2a_3 = a_2a_3$, we have $a_1a_2 = a_1a_2a_1^{-1}a_1 = a_2a_3a_1$.)

By introducing the relations $ab = ba$ for all $a, b \in A$ in $F_A$ we will get a (free) abelian group over $A$.

1.2.7. Groups, defined by a multiplication table
Given a set $G$, a group structure on $G$ can be introduced by a multiplication table, explicitly defining the binary operation: for $a, b \in G$, at the $(a, b)$-position (the intersection of the $a$-th row and the $b$-th column) of this table the element $ab$ of $G$ appears. (One only has to check that the operation defined by this table is associative (which is hard), that a neutral element exists in $G$ (easy), and that every element of $G$ has an inverse (easy).) For example, the quaternion group $Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$ is defined by the following multiplication table:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>i</th>
<th>j</th>
<th>k</th>
<th>-1</th>
<th>-i</th>
<th>-j</th>
<th>-k</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>i</td>
<td>j</td>
<td>k</td>
<td>-1</td>
<td>-i</td>
<td>-j</td>
<td>-k</td>
</tr>
<tr>
<td>i</td>
<td>i</td>
<td>-1</td>
<td>k</td>
<td>-j</td>
<td>-i</td>
<td>1</td>
<td>k</td>
<td>j</td>
</tr>
<tr>
<td>j</td>
<td>j</td>
<td>-k</td>
<td>-1</td>
<td>i</td>
<td>-j</td>
<td>1</td>
<td>-k</td>
<td>i</td>
</tr>
<tr>
<td>k</td>
<td>k</td>
<td>j</td>
<td>i</td>
<td>-1</td>
<td>k</td>
<td>j</td>
<td>i</td>
<td>-1</td>
</tr>
<tr>
<td>-1</td>
<td>-1</td>
<td>-i</td>
<td>-j</td>
<td>-k</td>
<td>1</td>
<td>i</td>
<td>j</td>
<td>k</td>
</tr>
<tr>
<td>-i</td>
<td>-i</td>
<td>1</td>
<td>-k</td>
<td>j</td>
<td>i</td>
<td>-1</td>
<td>k</td>
<td>j</td>
</tr>
<tr>
<td>-j</td>
<td>-j</td>
<td>k</td>
<td>1</td>
<td>i</td>
<td>-j</td>
<td>-k</td>
<td>1</td>
<td>-j</td>
</tr>
<tr>
<td>-k</td>
<td>-k</td>
<td>-j</td>
<td>i</td>
<td>1</td>
<td>k</td>
<td>-j</td>
<td>i</td>
<td>1</td>
</tr>
</tbody>
</table>

### 1.3. The very elementary properties and the order of elements of a group

#### 1.3.1. The cancellation property. If $G$ is a group, then for any $a, b_1, b_2 \in G$, if $ab_1 = ab_2$, then $b_1 = b_2$, and if $b_1a = b_2a$, then $b_1 = b_2$.

#### 1.3.2. Properties of inverses. Let $G$ be a group. For any $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$, and for any $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in G$, $(a_1 \cdot \cdots \cdot a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

#### 1.3.3. Let $G$ be a group and let $a \in G$. For any $n \in \mathbb{N}$, we define $a^n = \underbrace{a \cdot a \cdots a}_{n\text{ times}}, a^0 = 1_a, a^{-n} = (a^n)^{-1} = (a^{-1})^n$.

Then for any $n, m \in \mathbb{Z}$, $a^{n+m} = a^n a^m$ and $(a^n)^m = a^{nm}$.

#### 1.3.4. Let $G$ be a group and let $a \in G$. The minimal positive integer $n$ for which $a^n = 1$ is called the order of $a$ and is denoted by $|a|$; if such $n$ does not exist, $a$ is said to have infinite order, $|a| = \infty$. If $|a| = \infty$, then in the two-sided sequence $\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots$ of powers of $a$ all elements are distinct; if $|a| = n$, then this sequence is periodic with period $n$: $\ldots, 1, a, a^2, \ldots, a^{n-1}, 1, a, a^2, \ldots, a^{n-1}, \ldots$.

### 1.4. Isomorphisms of groups

#### 1.4.1. Two groups (more generally, two sets with binary operations) $G_1$ and $G_2$ are said to be isomorphic if there is a bijection $\varphi: G_1 \rightarrow G_2$ such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G_1$; such a bijection $\varphi$ is called an isomorphism.

#### 1.4.2. Example. The group $\text{Mat}^*_{n \times n}(F)$ of invertible $n \times n$-matrices over a field $F$ under multiplication is isomorphic to the group $\text{GL}_n(F) = \text{GL}(F^n)$ of invertible linear transformations of an $n$-dimensional $F$-vector space.

#### 1.4.3. If an element $a$ of a group $G$ has an infinite order, then the group $\{a^n, n \in \mathbb{Z}\}$ of its powers is isomorphic to $\mathbb{Z}$ (under the isomorphism $a^n \leftrightarrow n$); if $|a| = n$, then this group is isomorphic to $\mathbb{Z}_n$.

### 1.5. Subgroups

#### 1.5.1. Let $G$ be a group. A nonempty subset $H$ of $G$ is said to be a subgroup of $G$ if $H$ is a group under multiplication (that is, the operation) in $G$; (in some books) this is written as $H \leq G$.

#### 1.5.2. For a subset $H$ of $G$ to be a subgroup, $H$ must be closed under multiplication in $G$: for any $a, b \in H$, $ab \in H$ (in short: $HH \subseteq H$); contain $1_G$; and for every $a \in H$ contain the inverse of $a$: $a^{-1} \in H$ (in short: $H^{-1} \subseteq H$). All these conditions can be reduced to a single one: for any $a, b \in H$, $a^{-1}b \in H$ (in short: $H^{-1}H \subseteq H$).

#### 1.5.3. For any group $G$, the singleton $\{1\}$ and $G$ itself are subgroups of $G$; these subgroups are called trivial (and all other are called nontrivial). (Or, only 1 is said to be trivial, and the subgroups $H \neq G$ are said to be proper.)

#### 1.5.4. Lemma. The intersection of any collection of subgroups of a group $G$ is a subgroup of $G$. 


1.6. Generating sets and relations

1.6.1. Let $G$ be a group and $A$ be a subset of $G$. The subgroup of $G$ generated by $A$ is the minimal subgroup of $G$ that contains $A$; this is the intersection of all subgroups of $G$ containing $A$. This subgroup is denoted by $⟨A⟩$; if $A$ is a finite or a countable set, $A = \{a_1, \ldots, a_n\}$ or $A = \{a_1, a_2, \ldots\}$, this subgroup is also denoted by $⟨a_1, \ldots, a_n⟩$ or, respectively, $⟨a_1, a_2, \ldots⟩$.

For $A \subseteq G$, the group $⟨A⟩$ consists of all “words over $A ∪ A^{-1}$”: the products $c_1 \cdots c_k$ where for each $i$, $c_i \in A$ or $c_i^{-1} \in A$.

1.6.2. If $A \subseteq G$ is such that $G = ⟨A⟩$, we say that $A$ is a generating set of $G$, or that $A$ generates $G$.

If $G = ⟨A⟩$, then $G$ consists of all words over the alphabet $A ∪ A^{-1}$ (but some distinct words may be equal in $G$). Thus, any group can be seen as a free group with relations. (If no better choice is seen, as a set of generators one can take all elements of $G$, and as a set of relations – the complete multiplication table of $G$.) The group $G$ with a set $A$ of generators and a set $R$ of relations is written as $⟨A \ | \ R⟩$, which is called a presentation of $G$. ($R$ does not have to be the set of all relations of $G$; it suffices if all other relations in $G$ follow from those in $R$.)

1.6.3. Examples.

(i) $\mathbb{Z}_n = \{1 \mid n = 0\}$ (where “1” is 1 mod $n$, not the identity of the group $\mathbb{Z}_n$ (which is 0)).

(ii) The free abelian group in two generators is defined as $⟨a, b \mid ab = ba⟩$.

(iii) For any $n \geq 3$, the dihedral group (the symmetry group of a regular $n$-gon $R_n$) is

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$$

(where $r$ is a rotation by the angle of $2\pi/n$ about the center of $R_n$ and $s$ is a reflection with respect to a line passing through the center and, say, one of the vertices of $R_n$).

1.7. Cyclic groups and their subgroups

1.7.1. A group generated by a single element, $G = ⟨a⟩$, is called cyclic. If $|a| = \infty$, then $G \cong \mathbb{Z}$, if $|a| = n$, then $G \cong \mathbb{Z}_n$.

1.7.2. A finite group $G$ of order $n$ is cyclic iff it contains an element of order $n$.

1.7.3. Lemma. Every subgroup of a cyclic group is cyclic.

1.7.4. In more details, every subgroup $H$ of $\mathbb{Z}$ is infinite cyclic, and has form $⟨d⟩ = d\mathbb{Z} = \{\ldots, -d, 0, d, 2d, \ldots\}$ for some $d \in \mathbb{N}$; the subgroup of $\mathbb{Z}$ generated by elements $m_1, \ldots, m_k$ is the group $⟨d⟩$ where $d = \gcd(m_1, \ldots, m_k)$.

1.7.5. Every subgroup $H$ of $\mathbb{Z}_n$ is generated by an element $d$ dividing $n$, $H = ⟨d⟩ = d\mathbb{Z}_n = \{0, d, 2d, \ldots, (\frac{n}{d} - 1)d⟩$, and has order $|H| = n/d$ (so, $\cong \mathbb{Z}_n/d$). The subgroup $⟨a_1, \ldots, a_k⟩$ of $\mathbb{Z}_n$ is the subgroup $⟨d⟩$ where $d = \gcd(a_1, \ldots, a_k, n)$. In particular, an element $a \in \mathbb{Z}_n$ generates $\mathbb{Z}_n$ iff $\gcd(a, n) = 1$; if $n$ is prime, then $\mathbb{Z}_n$ is generated by any its nonzero element.

1.8. Direct products of groups

1.8.1. Let $G_1$, $G_2$ be two groups. The group $G_1 × G_2 = \{(a_1, a_2) : a_1 \in G_1, a_2 \in G_2\}$ with multiplication defined by $(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2)$ is called the direct product of $G_1$ and $G_2$. The identity in $G_1 × G_2$ is the element $(1_{G_1}, 1_{G_2})$, the inverse $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$.

1.8.2. $G_1 × G_2$ is abelian iff both $G_1$ and $G_2$ are abelian.

1.8.3. For any groups $G_1$ and $G_2$, $G_1 × G_2 \cong G_2 × G_1$. For any groups $G_1$, $G_2$, and $G_3$, $(G_1 × G_2) × G_3 \cong G_1 × (G_2 × G_3)$.

1.8.4. Given $k$ groups $G_1, \ldots, G_k$, the direct product $G_1 × \cdots × G_k$ is defined as the set $\{(a_1, \ldots, a_k) : a_1 \in G_1, \ldots, a_k \in G_k\}$ with the componentwise multiplication $(a_1, \ldots, a_k)(b_1, \ldots, b_k) = (a_1b_1, \ldots, a_kb_k)$. This group is isomorphic to $\left(\cdots ((G_1 × G_2) × G_3) × \cdots × G_{k-1}\right) × G_k$.

1.8.5. For a group $G$ and $n \in \mathbb{N}$, the $n$-th power $G^n$ of $G$ is the group $\underbrace{G × \cdots × G}_n$.

1.8.6. Examples.

(i) $\mathbb{Z}^2$ is the lattice $\{(n, m) : n, m \in \mathbb{Z}\}$ in $\mathbb{R}^2$.  

5
(ii) \(V_4 \cong \mathbb{Z}_2^2\).
(iii) \(\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6\).

1.9. Finite groups of matrices

1.9.1. There exist finite fields. For example, for every prime integer \(p\), \(\mathbb{Z}_p\) is a field (all its nonzero elements are invertible under multiplication); this field is denoted by \(F_p\).

1.9.2. Let \(F\) be a finite field of \(q\) elements. Then for any \(n \in \mathbb{N}\), the group \(\text{GL}_n(F)\) of invertible \(n \times n\)-matrices under multiplication has \((q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})\) elements. For every \(F\) and every \(n \geq 2\) this group is noncommutative.

1.10. The lattice of subgroups of a group

1.10.1. For a group \(G\), the lattice of subgroups of \(G\) is a diagram (a graph), whose vertices are subgroups of \(G\), and if \(H < K \leq G\) then \(K\) is located above \(H\) in this diagram, and if there is no subgroups \(L\) with \(H < L < K\), then \(H\) and \(K\) are connected by an edge.

Isomorphic groups have identical lattices of subgroups; the converse is not true. (For instance, the groups \(\mathbb{Z}_2^2\) and \(\mathbb{Z}_2^3\) have identical lattices of subgroups.)

1.10.2. The lattices of subgroups of \(\mathbb{Z}_4, V_4, \mathbb{Z}_6, S_3, \mathbb{Z}_{36}, D_8, Q_8\) are:

\[
\begin{align*}
\mathbb{Z}_4 & : \langle 2 \rangle \cong \mathbb{Z}_2 \\
\langle a \rangle & \langle b \rangle \langle c \rangle \\
0 & 1
\end{align*}
\]

\[
\begin{align*}
V_4 & = \{1, a, b, c\} \\
\langle a \rangle & \langle b \rangle \langle c \rangle \\
\langle 1 \rangle & \langle 0 \rangle
\end{align*}
\]

\[
\begin{align*}
\mathbb{Z}_6 & : \langle 2 \rangle \cong \mathbb{Z}_2 \\
\langle a \rangle & \langle b \rangle \langle c \rangle \\
0 & 1
\end{align*}
\]

\[
\begin{align*}
\mathbb{Z}_{36} & : \langle 2 \rangle \langle 3 \rangle \\
\langle 4 \rangle & \langle 6 \rangle \langle 9 \rangle \\
\langle 12 \rangle & \langle 18 \rangle \\
0 & 1
\end{align*}
\]

\[
\begin{align*}
S_3 & = \{1, \tau_1, \tau_2, \tau_3, \sigma, \sigma^2\} \\
\langle \tau_1 \rangle & \langle \tau_2 \rangle \langle \tau_3 \rangle \langle \sigma \rangle \\
\langle 1 \rangle & \langle 0 \rangle
\end{align*}
\]

\[
\begin{align*}
D_8 & : \langle s, r^2 \rangle \langle r \rangle \langle sr, r^2 \rangle \\
\langle s \rangle & \langle sr^2 \rangle \langle r \rangle \langle sr \rangle \langle sr^3 \rangle \\
\langle 1 \rangle & \langle 0 \rangle
\end{align*}
\]

\[
\begin{align*}
Q_8 & : \langle i \rangle \langle j \rangle \langle k \rangle \\
\langle -1 \rangle & \langle 0 \rangle
\end{align*}
\]

1.11. Commuting elements, conjugate elements, the center, and the centralizers of elements

Let \(G\) be a group.

1.11.1. Two elements \(a\) and \(b\) of \(G\) are said to commute if \(ab = ba\). \(a\) and \(b\) commute iff \(bab^{-1} = a\) iff \(aba^{-1} = a\) iff \(aba^{-1}b^{-1} = 1\).

1.11.2. The elements \(a\) and \(bab^{-1}\) are said to be conjugate in \(G\).

1.11.3. The relation of being conjugate is an equivalence relation, and thus partitions \(G\) into disjoint equivalence classes, called conjugacy classes: two elements of \(G\) belong to the same class iff they are conjugate in \(G\).

1.11.4. For two elements \(a, b\) of a group \(G\), the element \([a, b] = aba^{-1}b^{-1}\) is called the commutator of \(a\) and \(b\). Thus, \(a\) and \(b\) commute iff \([a, b] = 1\).

1.11.5. Let \(G\) be a group. The center of \(G\) is the subgroup \(Z(G) = \{a \in G : ab = ba\ \text{for all} \ b \in G\}\) of \(G\). An element \(a \in G\) is contained in \(Z(G)\) iff \(a\) has no conjugates (except itself), that is, its conjugacy class is the singleton \(\{a\}\).

We have \(Z(G) = G\) iff \(G\) is abelian.

1.11.6. Examples.
(i) \(Z(S_3) = 1\) (the center is trivial).
(ii) \(Z(D_{2n}) = 1\) if \(n\) is odd and \(\{1, r^{n/2}\}\) if \(n\) is even.
1.11.7. For an element \( b \in G \), the **centralizer** of \( b \) is the subgroup \( C_G(b) = \{a \in G : ab = ba\} \) of \( G \).

We have \( C_G(b) = G \) iff \( b \in Z(G) \).

For any group \( G \), \( Z(G) = \bigcap_{b \in G} C_G(b) = \bigcap_{a \in A} C_G(b) \), where \( A \) is any set of generators of \( G \).

**Example.** \( C_{D_{2n}}(s) = \{1, s\} \) if \( n \) is odd and \( \{1, s, r^{n/2}, sr^{n/2}\} \) if \( n \) is even; \( C_{D_{2n}}(r) = \langle r \rangle \).

1.12. **The symmetric group** \( S_n \)

1.12.1. The symmetric group \( S_n \) is the group of self-bijection of the \( n \)-element set \( \{1, 2, \ldots, n\} \) (and is isomorphic to the group of self-bijections of any other \( n \)-element set), with the operation of composition. The elements of \( S_n \) are called **permutations**. The order of \( S_n \) is \( n! \).

1.12.2. A permutation \( \sigma \in S_n \) can be coded as a sequence \([i_1, \ldots, i_n]\) in two ways: either as a mapping \([1, \ldots, n] \mapsto [1, \ldots, n] \), meaning that for every \( j \), \( i_j = \sigma(j) \); or as a permutation, meaning \([i_1, \ldots, i_n]\) is the result of permutation of \(1, \ldots, n \), that is, for every \( j \), \( i_j \) is the integer that arrives at the \( j \)-th position, \( i_j = \sigma^{-1}(j) \).

1.12.3. Two permutations \( \sigma_1, \sigma_2 \in S_n \) are said to be disjoint if the sets \( \{i : \sigma_1(i) \neq i\} \) and \( \{j : \sigma_2(j) \neq j\} \) are disjoint. Disjoint permutations commute, \( \sigma_1 \sigma_2 = \sigma_2 \sigma_1 \), and \(|\sigma_1 \sigma_2| = |\sigma_1| \cdot |\sigma_2|\).

1.12.4. A permutation of the form \( i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1 \), where \( i_1, \ldots, i_k \) are all distinct, is called **cyclic of length** \( k \), or a \( k \)-cycle. Every 1-cycle is a trivial permutation. 2-cycles are called transpositions. A cycle \( i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1 \) is written as \((i_1, i_2, \ldots, i_k)\).

1.12.5. **Theorem.** Every permutation is uniquely (up to permutation of factors) representable as a product of disjoint cyclic permutations.

The representation of a permutation \( \sigma \) as a product of (nontrivial) disjoint cycles is called the **cycle decomposition** of \( \sigma \); the cycle decomposition of the identity is \((1)\). The sequence of lengths of the cycles appearing in the cycle decomposition of \( \sigma \) (in the increasing order) is called the **cycle type** of \( \sigma \).

1.12.6. **Example.** For \( \sigma = (1, 2, 3, 4, 5, 6, 7, 8), \sigma = (1, 3, 4)(2, 5)(6, 8) \), and its cycle type is 2, 2, 3.

1.12.7. **Lemma.** For any \( k \) and distinct \( i_1, \ldots, i_k \) we have \((i_1, \ldots, i_k) = (i_1, i_2)(i_2, i_3)\cdots(i_{k-1}, i_k)\). For any \( i \) and \( j \) with \( i < j \), \((i, j) = (i, i+1)(i+1, i+2)\cdots(j-2, j-1)(j-1, j)(j-2, j-1)\cdots(i+1, i+2)(i, i+1)\).

1.12.8. **Theorem.** For any \( n \), \( S_n \) is generated by transpositions. Moreover, \( S_n \) is generated by transpositions of the form \( \tau_i = (i, i+1), i = 1, \ldots, n-1 \).

1.12.9. For a transposition \( \tau \in S_n \), the **sign** of \( \tau \) is defined as \( \text{sign}(\tau) = \text{sign} \prod_{1 \leq i < j \leq n}(\sigma(j) - \sigma(i)); \) this is \((-1)^r\) where \( r \) is the number of pairs of elements of \( \{1, \ldots, n\} \) whose order is switched by \( \sigma \).

1.12.10. **Lemma.** For every \( i < n \), let \( \tau_i = (i, i+1) \). Then for any \( \sigma \in S_n \) and any \( i \), \( \text{sign}(\tau_i \sigma) = -\text{sign}(\sigma) \). Hence for \( \sigma = \tau_{i_1} \cdots \tau_{i_k} \) we have \( \text{sign}(\sigma) = (-1)^k \).

1.12.11. **Theorem.** For any \( \sigma_1, \sigma_2 \in S_n \), \( \text{sign}(\sigma_1 \sigma_2) = \text{sign}(\sigma_1) \text{sign}(\sigma_2) \).

1.12.12. For any transposition \( \tau \), \( \text{sign}(\tau) = -1 \). If \( \sigma \) is a product of \( k \) transpositions, then \( \text{sign}(\sigma) = (-1)^k \). If \( \sigma \) is a \( k \)-cycle, then \( \text{sign}(\sigma) = (-1)^{k-1} \).

1.12.13. Permutations of negative sign are called **odd**, and of positive sign are called **even**. The product of two even or two odd permutations is even, and the product of an even and an odd permutations is odd.

1.12.14. The even permutations from \( S_n \) form a subgroup, called the **alternating group** and denoted by \( A_n \). The order of \( A_n \) is \( n! / 2 \).

---

2. **Factorization and homomorphisms**

2.1. **Cosets and counting principles**

Let \( G \) be a group and \( H \) be a subgroup of \( G \).

2.1.1. For \( a \in G \), the set of the form \( ah = \{ah : h \in H\} \) is called a left coset of \( H \) in \( G \); the set of the form \( Ha = \{ha : h \in H\} \) is called a right coset of \( H \) in \( G \). (If \( G \) is abelian, then left cosets = right cosets.)
2.1.2. Theorem. Any two left cosets of $H$ in $G$ either coincide or are disjoint, and thus left cosets partition $G$. Two elements $a, b \in G$ belong to the same coset iff $aH = bH$ iff $a^{-1}b \in H$.

And similarly,

Theorem. Any two right cosets of $H$ in $G$ either coincide or are disjoint, and thus right cosets partition $G$. Two elements $a, b \in G$ belong to the same coset iff $Ha = Hb$ iff $ab^{-1} \in H$.

2.1.3. Examples.
(i) The cosets of the subgroup $\mathbb{Z}$ are the sets $\mathbb{Z} = n\mathbb{Z} + k$ for $k = 0, 1, \ldots, n - 1$.
(ii) The cosets of the subgroup $R$ are the lines $a + Ru$, parallel to $H$.
(iii) The cosets of the subgroup $S$ are the rays $\mathbb{R}^+_u = \{x \in \mathbb{R}, x > 0\}$ of $\mathbb{C}^+$ and the rays $\mathbb{R}^+_u z_0 = \{z : \arg z = \arg z_0\}$, $z_0 \neq 0$.
(iv) The cosets of the subgroup $S$ are the circles $Sz = \{z : |z| = |z_0|\}$, $z_0 \neq 0$.
(v) Let $X$ be a set, $S_X$ be the group of permutations of $X$, $x_0 \in X$, and $H = \{\varphi \in S_X : \varphi(x_0) = x_0\}$. Then left cosets of $H$ in $S_X$ are the sets of the form $\{\varphi \in S_X : \varphi(x_0) = x_1\}$, $x_1 \in X$, and right cosets are the sets of the form $\{x_1 \in X : \varphi(x_1) = x_0\}$.

2.1.4. Theorem. For any left coset $aH$ of $H$, the mapping $h \mapsto ah$, $h \in H$, is a bijection between $H$ and $aH$. In particular, $|aH| = |H|$. 

2.1.5. Corollary – Lagrange’s theorem. If $|G| < \infty$, then $|H| \mid |G|$.

2.1.6. Corollary. If $|G| < \infty$, then for any $a \in G$, $|a| \mid |G|$; hence, $a^{|G|} = 1$.

2.1.7. Corollary. Every finite group of prime order is cyclic.

2.1.8. Corollary – Fermat’s little theorem. If $p$ is a prime integer and $p \nmid a \in \mathbb{N}$, then $a^p = a \mod p$.

2.1.9. Corollary – Euler’s theorem. If $a, n \in \mathbb{N}$ are relatively prime, then $a^{\varphi(n)} = 1 \mod n$.

2.1.10. The number of (left) cosets of $H$ in $G$ is called the index of $H$ in $G$ and is denoted by $|G : H|$.

Claim. The number of right cosets of $H$ in $G$ equals the number of left cosets; the mapping $a \mapsto a^{-1}$ maps right cosets to left cosets and vice versa.

2.1.11. The 1st counting principle. If $|G| < \infty$, then $|G| = |H| \cdot |G : H|$.

2.1.12. The 2nd counting principle. If $H \leq K \leq G$, then $|G : H| = |G : K| \cdot |K : H|$.

2.1.13. If $H$ and $K$ are subgroups of $G$, by $HK$ we understand the set $\{hk : h \in H, k \in K\}$; this may not be a subgroup of $G$, but is a union of right cosets of $H$, and is a union of left cosets of $K$. By $|HK : (H \cap K)|$ we understand the number of (left or right) cosets of $H \cap K$ in $HK$.

The 3rd counting principle. If $H, K \leq H$, then $|HK : (H \cap K)| = |H : (H \cap K)| \cdot |K : (H \cap K)|$. If $|HK| < \infty$, then $|HK| = |H| \cdot |H|/|H \cap K|$.

2.2. Normal subgroups and factorization

2.2.1. A subgroup $H$ of a group $G$ is said to be normal if the left cosets of $H$ in $G$ are its right cosets, that is, if for every $a \in G$, $aH = Ha$, or equivalently, $aHa^{-1} = H$.

The normality of $H$ in $G$ is denoted by $H \trianglelefteq G$. In subgroup diagrams, the normality of $H$ in $G$ is denoted by a double line connecting $G$ and $H$:

\[
\begin{array}{c}
G \\
\hline
H
\end{array}
\]

2.2.2. A subgroup $H$ of a group $G$ is normal iff it is a union of conjugacy classes in $G$.

2.2.3. Examples.
(i) If $G$ is an abelian group, then every subgroup of $G$ is normal.
(ii) The subgroup $\{e, (1, 2)\}$ is not normal in $S_3$, the subgroup $\{1, (1, 2, 3), (1, 3, 2)\}$ is.
(iii) In $D_{2n}$, $\langle s \rangle$ is not normal, but $\langle p^k \rangle$ is normal for every $k$.

2.2.4. Lemma.
(i) The intersection of any collection of normal subgroups is a normal subgroup.
(ii) The join of any collection of normal subgroups is a normal subgroup.
(iii) If $H \leq G$ and $K \leq H$, then $(H \cap K) \leq K$; in particular, if $H \leq K \leq G$ and $H \leq G$, then $H \leq K$.

(iv) If $H \leq G$ and $[G : H] = 2$, then $H \leq G$.

2.2.5. If $H \leq G$, then for any two cosets of $H$, their product is a coset of $H$ as well: $(aH)(bH) = (ab)H$.

Under this multiplication the cosets of $H$ form a group, with $H$ being the identity and $a^{-1}H$ being the inverse of a coset $aH$, $a \in G$. This group is called the quotient group, or the factor group of $G$ by $H$, and is denoted by $G/H$. The order of $G/H$ is $|G : H|$.

Notice that $G/H$ is not a subgroup of $G$. (It may sometimes look like (be isomorphic to) a subgroup of $G$, but, by definition, it is not a subgroup!) Elements of $G/H$ are subsets of $G$, namely, the cosets of $H$ in $G$. If we denote the coset $aH$ by $\bar{a}$, then the elements of $G/H = \{a : a \in G\}$, that is, $G/H$ consists of the same elements as $G$, of which some are identified: we have $\bar{a} = \bar{b}$ if $aH = bH$; we also write $a = b \mod H$ in this case. For an element $C$ of $G/H$, for every $a \in C$ we have $C = \bar{a}$; any such $a$ is called a representative of $C$.

$G/H$ may also be viewed as $G$ with additional relations: namely, all elements of $H$ are now declared to be equal to $1$. This implies that all elements of any coset $aH$ of $H$ are now equal (to $\bar{a}$) in $G/H$.

The multiplication in $G/H$ is inherited from $G$: we have $\bar{a}\bar{b} = \bar{ab}$. That is, to multiply two elements (two cosets) from $G/H$, we take any representatives of these two cosets, multiply them, and take the coset of the product; since $H$ is normal, the result will not depend on the choice of the representatives. The identity in $G/H$ is the coset $1 = H$ of $H$, and the inverse of a coset $\bar{a} = aH$ is the coset $\bar{a}^{-1} = a^{-1}H$.

2.2.6. Examples.

(i) For any group $G$, $G/G = \{\bar{1}\}$ and $G/1 = \{\{a\} : a \in G\} \cong G$.

(ii) $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

(iii) $S_n/A_n \cong \mathbb{Z}_2$.

(iv) $C^*/\mathbb{Z}_{\mathbb{Z}^+} \cong \{z \in \mathbb{C} : |z| = 1\}$, a circle.

2.2.7. A group $G$ presented by generators and relations, $G = \langle S \mid R \rangle$, can be formally defined as the factor $F_S/\langle\langle R \rangle\rangle$, where $F_S$ is the free group over $S$ and $\langle\langle R \rangle\rangle$ is the minimal normal subgroup of $F_S$ containing $R$ (the intersection of all subgroups containing $R$).

2.2.8. The following fact will be useful:

Lemma. If $G/Z(G)$ is cyclic, then $G$ is abelian. (And so, actually, $G = Z(G)$.)

Proof. Let $a \in G$ be such that its image in $G/Z(G)$ generates this group. Then every element of $G$ has form $a^kz$ for some $k \in \mathbb{Z}$ and $z \in Z(G)$, and for any two elements $c_1 = a^{k_1}z_1$, $c_2 = a^{k_2}z_2$, with $z_1, z_2 \in Z(G)$, we have $b_1b_2 = a^{k_1}z_1a^{k_2}z_2 = a^{k_1+k_2}z_1z_2 = a^{k_2}z_2a^{k_1}z_1 = b_2b_1$.

2.3. Conjugation, normalizers and centralizers

Let $G$ be a group and let $a \in G$.

2.3.1. The mapping $G \rightarrow G$ defined by $b \mapsto aba^{-1}$, $b \in G$, is called conjugation by $a$; for $b \in G$, the element $aba^{-1}$ is said to be a conjugate of $b$ by $a$.

2.3.2. Conjugation by $a$ is a self-bijection of $G$ (its inverse is the conjugation by $a^{-1}$), and preserves multiplication: $a(bc) = (ab)a^{-1}$, $b, c \in G$. Hence, it is an automorphism of $G$ – an isomorphism $G \rightarrow G$.

It follows that conjugations preserve all properties of elements, subsets, and subgroups of $G$: for any $b \in G$, $|a^{-1}b| = |b|$, elements $b$ and $c$ of $G$ commute iff their conjugates commute, $H \subseteq G$ is a subgroup of $G$ iff $aHa^{-1}$ is a subgroup of $G$, $|aHa^{-1}| = |H|$, $|G : (aHa^{-1})| = |G : H|$, etc.

2.3.3. For a subgroup $H$ of $G$ and an element $a \in G$, the subgroup $aHa^{-1}$ is said to be conjugate to $H$. $H$ is a normal subgroup of $G$ iff it has no conjugates except itself.

The set of subgroups conjugate to $H$ is called the conjugacy class of $H$. $H$ is normal in $G$ iff its conjugacy class is $\{H\}$. 

$\blacksquare$
2.3.4. Let $H$ be a subgroup of $G$. We say that an element $a \in G$ normalizes $H$ is $aHa^{-1} = H$. The set $N_G(H) = \{a \in G : aHa^{-1} = H\}$ of elements of $G$ normalizing $H$ is called the normalizer of $H$ in $G$. $N_G(H)$ is a subgroup of $G$, namely, the maximal subgroup of $G$ containing $H$ and in which $H$ is normal: we have $H \trianglelefteq N_G(H) \leq G$. $H$ is a normal subgroup of $G$ iff $N_G(H) = G$.

2.3.5. Proposition. If $H$ and $K$ are subgroups of $G$ and $K$ normalizes $H$ (that is, $K \leq N_G(H)$), then $HK$ is a subgroup of $G$ (and so, is the join of $H$ and $K$). In particular, if $H \trianglelefteq G$, then $HK$ is a subgroup of $G$ for every $K \leq G$.

2.3.6. The group $C_G(H) = \{a \in G : aHa^{-1} = h$ for all $h \in H\}$ is called the centralizer of $H$ in $G$. We have $C_G(H) \leq N_G(H)$ and $C_G(H) \cap H = Z(H)$.

2.4. Simple groups and composition series

2.4.1. Let $G$ be a group, $H$ be a normal subgroup of $G$, and $K = G/H$; then, informally, we can see $G$ as a group “made of” $H$ and $K$.

2.4.2. Let $G$ be a group; a nested sequence $1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = G$ of subgroups of $G$ such that for each $i$, $H_{i-1}$ is normal in $H_i$ is called a subnormal series in $G$; the quotient groups $G_i = H_i/H_{i-1}$, $i = 1, \ldots, n$, are called the factors of this series. (Informally, $G$ is “made of” the groups $G_i$, $i = 1, \ldots, n$.)

2.4.3. A group that is “made of” abelian groups, that is, has a subnormal series with abelian factors, is said to be solvable.

2.4.4. A group is said to be simple if it has no normal subgroups. (Simple groups are considered as “non-decomposable”, and play a role of blocks of which another groups are made.) Examples of simple groups are the groups $Z_p$ for prime $p$ and the groups $A_n$ for $n \geq 5$.

2.4.5. A subnormal series in $G$ with simple factors is called a composition series of $G$.

Jordan-Hölder theorem. Every finite group has a (finite) composition series. This series may not be unique, but the factors of this series are defined uniquely up to reordering.

2.4.6. Examples.

(i) The group $Z_6$ has two different composition series: $0 \trianglelefteq \{0,3\} \trianglelefteq Z_6$ with factors (isomorphic to) $Z_2$ and $Z_3$, and $0 \trianglelefteq \{0,2,4\} \trianglelefteq Z_6$ with factors (isomorphic to) $Z_3$ and $Z_2$.

(ii) The group $S_3$ has the (unique) composition series $1 \trianglelefteq \langle \sigma \rangle \trianglelefteq S_3$, where $\sigma$ is a 3-cycle; the factors of this series are (isomorphic to) $Z_3$ and $Z_2$. (So, $S_3$ is “made of” of $Z_3$ and $Z_2$, and is a solvable group.)

(iii) The group $S_4$ has the composition series $1 \trianglelefteq Z \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$, where $Z = \{1, (1,2)(3,4)\} \trianglelefteq Z_2$ and $V = \{(1,1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \trianglelefteq V_4$. The factors of this series are $Z_2$, $Z_2$, $Z_3$, and $Z_2$. (So, $S_4$ is also solvable.)

(iv) The (only) composition series of $S_n$ for $n \geq 5$ is $1 \trianglelefteq A_n \trianglelefteq S_n$ (if we assume that $A_n$ is a simple group). So, $S_n$ for $n \geq 5$ is not solvable.

(v) For infinite groups the Jordan-Hölder theorem does not hold. For example, $Z$ has no finite composition series, and has many different (and with different factors) infinite composition series: in the series $\cdots \trianglelefteq 8Z \trianglelefteq 4Z \trianglelefteq 2Z \trianglelefteq Z$ all factors are isomorphic to $Z_2$, in $\cdots \trianglelefteq 27Z \trianglelefteq 9Z \trianglelefteq 3Z \trianglelefteq Z$ all factors are isomorphic to $Z_3$, in $\cdots \trianglelefteq 30Z \trianglelefteq 6Z \trianglelefteq 2Z \trianglelefteq Z$ the factors are isomorphic to $\ldots, Z_5, Z_3, Z_2$.

2.4.7. The Hölder program of studying finite groups was:

(i) to find all (up to isomorphism, of course) finite simple groups;

(ii) and to describe all ways two groups can be “connected” (that is, given groups $H$ and $K$, describe all groups $G$ that contain $H$ as a normal subgroup so that $G/H \cong K$).

The first part of the program has been fulfilled, the second is not even close to fulfillment...

2.5. Conjugacy classes in $S_n$ and simplicity of $A_n$ for $n \geq 5$

2.5.1. If $\sigma, \rho \in S_n$, then $\sigma: i \mapsto j$ iff $\rho \sigma \rho^{-1}: \rho(i) \mapsto \rho(j)$. So, if $\sigma = (i_1, \ldots, i_k) \cdots (j_1, \ldots, j_l)$ is the cycle decomposition of $\sigma$, then the cycle decomposition of $\rho \sigma \rho^{-1}$ is $(\rho(i_1), \ldots, \rho(i_k)) \cdots (\rho(j_1), \ldots, \rho(j_l))$. This implies that conjugate permutations have the same cycle type, and conversely, if two permutations from $S_n$ have the same cycle type, then they are conjugate in $S_n$. 
2.5.2. Using 2.5.1, we can prove:

**Theorem.** For \( n \geq 5 \), \( A_n \) is a simple group.

Here is the idea of (one possible) proof of this theorem:

(i) Show that \( A_n \) is generated by 3-cycles.
(ii) Show that any two 3-cycles are conjugate in \( A_n \).
(iii) Show that any nontrivial normal subgroup of \( A_n \) contains a 3-cycle.

2.6. Homomorphisms of groups

2.6.1. A mapping \( \varphi : G \rightarrow H \) from a group \( G \) to a group \( H \) is said to be a homomorphism if \( \varphi(ab) = \varphi(a)\varphi(b) \) for every \( a, b \in G \). A bijective homomorphism is called an isomorphism.

2.6.2. Examples.

(i) If \( H \) is a subgroup of \( G \), then the embedding \( H \hookrightarrow G, a \mapsto a \), is a homomorphism.
(ii) Linear mappings of vector spaces are homomorphisms.
(iii) For any \( a \in \mathbb{Z} \), the mapping \( \mathbb{Z} \rightarrow \mathbb{Z}, n \mapsto an \), is a homomorphism. More generally, for any group \( G \) and an element \( a \in G \), the mapping \( \mathbb{Z} \rightarrow G, n \mapsto a^n \), is a homomorphism. (In fact, any homomorphism \( \mathbb{Z} \rightarrow G \) is of this form.)
(iv) For any \( n \in \mathbb{N} \) and a field \( F \), det is a homomorphism \( \text{GL}_n(F) \rightarrow F^* \).
(v) For any \( n \in \mathbb{N} \), sign is a homomorphism \( S_n \rightarrow \{-1,1\} \).
(vi) The mapping \( z \mapsto |z| \) is a homomorphism \( \mathbb{C}^* \rightarrow \mathbb{R}^* \).
(vii) The mapping \( x \mapsto e^{2\pi ix} \) is a homomorphism \( \mathbb{R} \rightarrow \mathbb{C}^* \).
(viii) If \( H \) is a quotient group of a group \( G \), \( H = G/N \), then the mapping \( G \rightarrow H, a \mapsto \bar{a} = aN \) is a homomorphism, called the factorization, or the projection homomorphism.
(ix) Let \( S \) be a subset of a group \( G \), and let \( F_S \) be the free group on the set \( S \), We then have a natural homomorphism \( F_S \rightarrow G \), which maps a word \( s_1 \cdots s_k \), with \( s_i \in S \cup S^{-1} \) for all \( i \), to the element \( s_1 \cdots s_k \) of \( G \).

2.6.3. Here are some elementary properties of homomorphisms:

Let \( \varphi : G \rightarrow H \) be a homomorphism; then

(i) \( \varphi(1_G) = 1_H \).
(ii) For any \( a \in G \), \( \varphi(a^{-1}) = \varphi(a)^{-1} \), and for any \( n \in \mathbb{Z} \), \( \varphi(a^n) = (\varphi(a))^n \).
(iii) The composition of two homomorphisms is a homomorphism.
(iv) If \( \varphi \) is an isomorphism, then \( \varphi^{-1} \) is also an isomorphism.
(v) If \( K \) is a subgroup of \( G \), then \( \varphi(K) \) is a subgroup of \( H \); in particular, \( \varphi(G) \leq H \).
(vi) If \( L \) is a subgroup of \( H \), then \( \varphi^{-1}(L) \) is a subgroup of \( G \).
(vii) If \( L \) is a normal subgroup of \( H \), then \( \varphi^{-1}(L) \) is a normal subgroup of \( G \).
(viii) If \( K \) is a normal subgroup of \( G \), then \( \varphi(K) \) may not be normal in \( H \); however, it is normal in \( \varphi(G) \). In particular, if \( \varphi \) is surjective, then \( \varphi(K) \leq H \).

2.6.4. Let \( \varphi : G \rightarrow H \) be a homomorphism. The preimage \( \varphi^{-1}(1_H) = \{ a \in G : \varphi(a) = 1_H \} \) of \( 1_H \) is called the kernel of \( \varphi \) and is denoted by \( \text{Ker} \varphi \). \( \text{Ker} \varphi \) is a normal subgroup of \( G \).

2.7. The isomorphism theorems

2.7.1. Let \( \varphi : G \rightarrow H \) be a homomorphism and \( N = \text{Ker} \varphi \); then the fibers of \( \varphi \) (that is, the preimages of elements of \( \varphi(G) \)) are cosets of \( N \); two elements \( a, b \in G \) have the same image, \( \varphi(a) = \varphi(b) \), if \( aN = bN \). It follows that

**Theorem.** \( \varphi \) is injective iff its kernel is trivial, \( \text{Ker} \varphi = 1 \).

2.7.2. As a corollary we get

**The 1st isomorphism theorem.** For any homomorphism \( \varphi : G \rightarrow H \), \( \varphi(G) \cong G/\text{Ker} \varphi \), where the isomorphism is defined by \( \bar{a} \mapsto \varphi(a) \).
2.7.3. It follows that any homomorphism $\varphi: G \to H$ is a composition of the (surjective) factorization homomorphism $G \mapsto G/\operatorname{Ker}\varphi$, an isomorphism $G/\operatorname{Ker}\varphi \to \varphi(G)$, and an (injective) embedding $\varphi(G) \to H$.

2.7.4. Examples.

(i) The kernel of the homomorphism sign: $S_n \to \{−1, 1\}$ is the group $A_n$, so $S_n/A_n \cong \{−1, 1\} \cong \mathbb{Z}_2$.

(ii) The kernel of the (surjective) homomorphism det: $\mathrm{GL}_n(F) \to F^*$ is the special linear group $\mathrm{SL}_n(F) = \{ A \in \mathrm{Mat}_{n \times n}(F) : \det A = 1 \}$, so $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^*$.

(iii) For the homomorphism $\varphi: \mathbb{C}^* \to \mathbb{R}^*$, $\varphi(z) = |z|$, we have $\operatorname{Ker}\varphi = S = \{ z : |z| = 1 \}$ and $\varphi(\mathbb{C}^*) = \mathbb{R}_+$. So, $\mathbb{C}^*/S \cong \mathbb{R}_+^\ast (\cong \mathbb{R})$.

(iv) For the homomorphism $\varphi: \mathbb{R} \to \mathbb{C}^*$, $\varphi(x) = e^{2\pi ix}$, we have $\operatorname{Ker}\varphi = \mathbb{Z}$ and $\varphi(\mathbb{R}) = S = \{ z : |z| = 1 \}$. So, $\mathbb{R}/\mathbb{Z} \cong S$.

2.7.5. If a group $G$ is generated by a set $S$, then the homomorphism $\varphi: F_S \to G$, $F_S \ni s_1 \cdots s_k \mapsto s_1 \cdots s_k \in G$, is surjective. So, $G \cong F_S/N$, where $N$ is the normal subgroup that consists of all “relations” of $G$. We obtain:

**Theorem.** Every group is (isomorphic to) a quotient group of a free group. If a group is generated by $n$ elements, then it is (isomorphic to) a factor of $F_n$.

2.7.6. **The 2nd isomorphism theorem.** Let $H, K$ be subgroup of a group $G$ such that $K$ normalizes $H$, $K \leq N_G(H)$. Then $(K \cap H) \trianglelefteq K$ and $(KH)/H \cong K/(K \cap H)$, where the isomorphism is (naturally) defined by $kH \mapsto k(K \cap H)$, $k \in K$.

In the subgroup diagram below, $KH/H \cong K/(K \cap H)$:

\[
\begin{array}{ccc}
KH & \downarrow & K \\
K \cap H & \downarrow & \hline \\
& K \cap H & \\
\end{array}
\]

2.7.7. **The 3rd isomorphism theorem.** Let $H$ and $K$ be normal subgroups of a group $G$ such that $H \leq K$. Then $K/H \trianglelefteq G/H$ and $G/K \cong (G/H)/(K/H)$, where the isomorphism is (naturally) defined by $aK \mapsto (aH)(K/H)$, $a \in G$.

2.7.8. **The 4th isomorphism theorem.** Let $H$ be a normal subgroup of a group $G$. Then the subgroups of $G/H$ are in 1-to-1 correspondence with the subgroups of $G$ containing $H$: a subgroup $K$ of $G/H$ corresponds to its preimage in $G$, and a subgroup $K$ of $G$ containing $H$ corresponds to the subgroup $K = KH$ of $G/H$. For two subgroups $K_1, K_2$ of $G$ we have $K_1 \leq K_2$ iff $K_1 \leq K_2$, in which case $|K_2:K_1| = |K_2:K_1|$; $K_1 \trianglelefteq K_2$ iff $K_1 \trianglelefteq K_2$, in which case $K_2/K_1 \cong K_2/K_1$; $K_1 \cap K_2 = K_1 \cap K_2$; and $(K_1,K_2) = (K_1 \cap K_2)$. It follows that the lattice of subgroups of $G/H$ is isomorphic to (looks exactly like) the lattice of subgroups of $G$ “above $H$” (containing $H$).

2.8. Reduction of a homomorphism to a quotient group

2.8.1. Let $\varphi: G \to H$ be a group homomorphism and let $N \trianglelefteq G$. A homomorphism $\overline{\varphi}: G/N \to H$ is called a reduction of $\varphi$ if $\bar{\varphi}(\bar{a}) = \varphi(a)$ for every $a \in G$ (where $\bar{a}$ stands for the coset $aN$).

2.8.2. **Theorem.** Let $N$ be a normal subgroup of a group $G$; a homomorphism $\varphi: G \to H$ can be reduced to a homomorphism $G/N \to H$ iff $N \leq \ker\varphi$.

2.8.3. A special case of Theorem 2.8.2 is the following situation: Let $G$ be a group defined by generators and relations, $G = \langle S \mid R \rangle$ and let $f: S \to H$ be a mapping of the set of generators to a group $H$; is $f$ extendible to a homomorphism $\varphi: G \to H$, so that $\varphi(s) = f(s)$ for all $s \in S$? The answer is “yes” iff all relations from $R$ are satisfied in $H$: for any relation $s_1 \cdots s_k = s_{k+1} \cdots s_n$ from $R$ we must have $f(s_1) \cdots f(s_k) = f(s_{k+1}) \cdots f(s_n)$ in $H$.

2.8.4. **Example.** Dealing with the standard presentation of the dihedral group $D_{2n} = \langle r,s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$, given a group $H$ and elements $a,b \in H$, a homomorphism $D_n \to H$ that maps $r \mapsto a$ and $s \mapsto b$ exists iff $a^n = b^2 = 1$ and $ab = ba^{-1}$.
3. Actions of groups on sets and on themselves

3.1. Group actions

3.1.1. Let $G$ be a group and $X$ be a set. An action of $G$ on $X$ is a mapping $G \times X \rightarrow X$, $(a,x) \mapsto ax$, such that $(ab)x = a(bx)$ for all $a, b \in G$, $x \in X$, and $1x = x$ for all $x \in X$. I’ll call the elements of $X$ points.

This was, actually, the definition of a left action; a right action is a mapping $G \times X \rightarrow X$, $(a,x) \mapsto xa$, satisfying $x(ab) = (xa)b$ for all $a, b \in G$ and $x \in X$ (in the product $ab$, $a$ acts first), and $x1 = x$ for all $x \in X$.

3.1.2. Given an action of $G$ on $X$, every element $a \in G$ defines a mapping $\varphi_a : X \rightarrow X$ by $\varphi_a(x) = ax$, $x \in X$. By definition, for any $a, b \in G$ we have $\varphi_{ab} = \varphi_a \circ \varphi_b$. It follows that for any $a, b \in G$, $\varphi_{ab} = \varphi_b^{-1} \circ \varphi_a$, So, all mappings $\varphi_a$ are invertible, and we have a homomorphism $\varphi : G \rightarrow S_X$, $a \mapsto \varphi_a$. Conversely, any homomorphism $\varphi : G \rightarrow S_X$ defines an action of $G$ on $X$ by $ax = \varphi_a(x)$.

3.1.3. For an action of a group $G$ on a set $X$, the kernel of this action is the set of elements of $G$ that act identically on $X$, (This is just the kernel of the homomorphism $\varphi$ introduced in 3.1.2.) An action of a group $G$ on a set $X$ is said to be faithful if its kernel is trivial.

An action of $G$ on $X$ is said to be transitive if for any $x, y \in X$ there is $a \in G$ such that $ax = y$. (More generally, for $n \in \mathbb{N}$, an action is said to be $n$-transitive if for any distinct $x_1, \ldots, x_n \in X$ and distinct $y_1, \ldots, y_n \in X$ there is $a \in G$ such that $ax_i = y_i$ for all $i = 1, \ldots, n$.)

3.1.4. Let $G$ act on $X$. For a point $x \in X$, the orbit of $x$ under this action is the set $Gx = \{ax, a \in G\}$.

Two orbits in $X$ are either equal or disjoint, and thus the orbits partition $X$. A group action is transitive, the kernel of the action is $\{1\}$, and its stabilizer is $\{e\}$.

3.1.5. For a point $x \in X$, the stabilizer of $x$ in $G$ is the subgroup $G_x = \{a \in G : ax = x\}$. A point $x$ is said to be a fixed point of $G$ if $Gx = \{x\}$, that is, if $G_x = G$.

3.1.6. Two elements $a, b \in G$ map $x$ to the same point, $ax = bx$, iff $aG_x = bG_x$; thus the orbit $Gx$ of $x$ is in a 1-1 correspondence with the left cosets of $G_x$ in $G$. In particular, the cardinality of the orbit of a point equals the index of its stabilizer: $|Gx| = |G : G_x|$.

3.1.7. If the action of $G$ is transitive, then $|X| = |G : G_x|$ for any $x \in X$. In the general case, $|X| = \sum_{x \in S} |G : G_x|$, where $S \subseteq X$ is a set of representatives of all distinct orbits in $X$.

3.1.8. For any $a \in G$, the stabilizer of the point $ax$ is $G_{ax} = aG_xa^{-1}$.

In the case the action of $G$ is transitive, the kernel of the action is $\bigcap_{a \in G} aG_xa^{-1}$ for any point $x \in X$. (This is the maximal normal subgroup of $G$ that is contained in $G_x$.)

3.1.9. Examples.

(i) An action of a group $G$ on a set $X$ appears naturally when $G$ is a subgroup of the group $S_X$ of self-bijections of $X$. Such is, for instance, the action of the group $GL_n(F)$ on the $n$-dimensional vector space $F^n$. This action is transitive and faithful.

(ii) The multiplicative group $F^*$ of a field $F$ naturally acts on any $F$-vector space $V$ by left multiplications, $(a, u) \mapsto au$. The orbits of this action are 1-dimensional subspaces of $V$ with 0 excluded; the orbit of 0 $\in V$ is $\{0\}$.

(iii) The group $D_{2n}$ naturally acts on the plane $\mathbb{R}^2$. The orbits are either $2n$-gons or $n$-gons (except the orbit of 0, which is $\{0\}$).

(iv) For any $\sigma \in S^n$ we have an action of the cyclic group $\langle \sigma \rangle$ on $X = \{1, \ldots, n\}$. The orbits under this actions are just the cycles from the cycle decomposition of $\sigma$.

(v) An action of a group $G$ on a set $X$ induces an action of $G$ on the power set $P(X)$ of $X$ by $(a, A) \mapsto aA$, $a \in G$, $A \subseteq X$.

3.2. The left regular action

Let $G$ be a group.

3.2.1. $G$ naturally acts on itself by multiplication, $(a, b) \mapsto ab$. This action is called the left regular action. This action is faithful and transitive; the stabilizer of every point is trivial.
3.2.2. The left regular action of $G$ defines an injective homomorphism $G \to S_G$. We therefore obtain:

**Cayley’s theorem.** Every group $G$ is isomorphic to a subgroup of a group of permutations, namely, of $S_G$. If $|G| = n$, then $G$ is isomorphic to a subgroup of $S_n$.

3.2.3. Let $H \leq G$. Then the left regular action of $G$ induces an action of $G$ on the set of left cosets of $H$, $(a, bH) \mapsto abH$.

This action is transitive, but may not be faithful; the stabilizer of the point $aH$ is the group $aHa^{-1}$, and the kernel of the action is $\bigcap_{a \in G} aHa^{-1}$. (Thus, if $|G : H| = n$, the action defines a homomorphism $G \to S_n$, with kernel $\bigcap_{a \in G} aHa^{-1}$.)

3.2.4. The following fact is useful:

**Lemma.** If $|G| < \infty$ and a subgroup $H$ of $G$ is such that $p = |G : H|$ is the minimal prime divisor of $|G|$, then $H \not\leq G$.

**Proof.** The action of $G$ by left multiplications on the set of left cosets of $H$ defines a nontrivial homomorphism $\varphi : G \to S_p$. The only common factor of $|G|$ and $|S_p| = p!$ is $p$, so $|\varphi(G)| = p$. So, $|G : \ker(\varphi)| = p$; since $\ker(\varphi) \leq H$, we have $\ker(\varphi) = H$, so $H$ is normal. ■

3.3. The action of a group on itself by conjugations

Let $G$ be a group.

3.3.1. $G$ acts on itself by conjugations: $(a, b) \mapsto aba^{-1}$.

This action may not be faithful and is never transitive: its kernel is the center of $G$; the orbits are conjugacy classes in $G$, the stabilizer of $b \in G$ is its centralizer $C_G(b)$.

3.3.2. It follows that for any $b \in G$ the cardinality of the conjugacy class of $b$ (the number of elements conjugate to $b$) is $|G : C_G(b)|$. The conjugacy class of $b$ is the singleton $\{b\}$ if $b \in Z(G)$.

3.3.3. Also $G$ acts by conjugations on the set of its subgroups: for $a \in G$ and $H \leq G$, $(a, H) \mapsto aHa^{-1}$. The orbit of any $H \leq G$ is the conjugacy class of $H$.

3.3.4. Let $H \leq G$, and consider the action of $G$ on the conjugacy class of $H$.

This action is transitive (of course), the stabilizer of $H$ is its normalizer $N_G(H)$, the kernel of the action is $\bigcap_{a \in G} aN_G(H)a^{-1}$.

3.3.5. It follows that for any $H \leq G$ the cardinality of the conjugacy class of $H$ is $|G : N_G(H)|$.

4. Direct product of groups

4.1. Direct products of two groups

4.1.1. Given groups $H$ and $K$, The external direct product is the group $H \times K = \{(h, k) : h \in H, k \in K\}$ with the componentwise multiplication.

4.1.2. Let $G = H \times K$, with $H$ and $K$ being considered as subgroups of $G$. Then $H$ and $K$ satisfy the following properties:

- $hk = kh$ for any $h \in H$ and $k \in K$ (both are equal to $(h, k)$);
- $H$ and $K$ are normal in $G$;
- $HK = G$;
- $H \cap K = 1$;
- every element $a \in G$ is uniquely representable in the form $a = hk$ with $h \in H$ and $k \in K$;
- if $|G| < \infty$, then $|G| = |H| \cdot |K|$;
- $G/H \cong K$; moreover, for the factorization homomorphism $\pi : G \to G/H$, $\pi|_K$ is an isomorphism between $K$ and $G/H$.

4.1.3. For any element $(h, k)$ of a direct product $H \times K$, $|(h, k)| = |h| \cdot |k|$.
4.1.4. Let $G$ be a group and $H, K \leq G$. We say that $G$ is an internal direct product of $H$ and $K$, and write (again) $G = H \times K$, if $G$ is isomorphic to the (external) direct product $H \times K$ under an isomorphism that is identical on $H$ and $K$. (That is, there is an isomorphism $\varphi: G \to H \times K$ such that $\varphi(h) = h$ and $\varphi(k) = k$ for every $h \in H$ and $k \in K$. This implies that the element $(h, k)$ of $H \times K$ corresponds to the element $hk$ of $G$.)

4.1.5. The fact that an isomorphism $\varphi: G \to H$ is identical on $H$ and $K$ can be expressed in the language of diagrams, by saying that the diagram

$$
\begin{array}{c}
G \\
\downarrow \varphi \\
H \times K \\
\uparrow K
\end{array}
$$

is commutative, meaning that the composition of $\varphi$ with the embedding of $H$ into $G$ equals the embedding of $H$ into $H \times K$, and the same for $K$.

4.1.6. Proposition. Let $G$ be a group and let $H, K$ be subgroups of $G$ satisfying the properties 0, $\Theta$, and $\Theta$ from 4.1.2. Let $O$. Then $G = H \times K$.

4.1.7. It follows that, given a group $G$ and a subgroup $H, K \leq G$, the properties 0, $\Theta$, $\Theta$ imply the other properties, $\Theta$, $\Theta$, $\Theta$, and $\Theta$. We actually have the following implications:

- Proposition. $\Theta$ implies $\Theta$; $\Theta$ implies $\Theta$; $\Theta$ implies $\Theta$, and if $|G| < \infty$, $\Theta$ implies $\Theta$; $\Theta$ implies $\Theta$; $\Theta$ implies $\Theta$, and if $|G| < \infty$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$.

4.1.8. As a corollary we get that $G = H \times K$ is also true if any of the following combinations of conditions holds: $\Theta$ implies $\Theta$; $\Theta$ implies $\Theta$; $\Theta$ implies $\Theta$, and if $|G| < \infty$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$, $\Theta$ implies $\Theta$.

4.1.9. Examples.

(i) $\mathbb{Z}_6 = \{0, 2, 4\} \times \{0, 3\}$.

(ii) $\mathbb{R}^* = \{-1, 1\} \times \mathbb{R}_+^*$.

(iii) $\mathbb{C}^* = S \times \mathbb{R}_+^*$, where $S = \{z \in \mathbb{C}^* : |z| = 1\}$.

4.1.10. Let $\varphi: G \to K$ be a surjective group homomorphism; a homomorphism $\sigma: K \to G$ is called a section of $\varphi$ if $\varphi \sigma = \text{Id}_K$. This is the case, $\sigma$ is an isomorphism between $K$ and $\sigma(K)$.

The fact that $\Theta$ implies direct product can be reformulated in the following way:

- Proposition. Let $H \trianglelefteq G$, $K = G/H$, and assume that the factorization homomorphism $G \to K$ has a section $\sigma$ such that $\sigma(K) \trianglelefteq G$. Then $G \cong H \times K$ (external product); more exactly, $G = H \times \sigma(K)$ (internal product).

4.2. A relative direct product

4.2.1. Let $H$ and $K$ be groups with surjective homomorphisms $\varphi: H \to N$ and $\psi: K \to N$ to a group $N$ (which, therefore, is isomorphic to a quotient group of $H$ and of $K$). A relative direct product $H \times_K K$ of $H$ and $K$ over $N$ is the subgroup $\{(h, k) : h \in H, k \in K, \varphi(h) = \psi(k)\}$ of $H \times K$.

4.2.2. A relative direct product $H \times_K K$ does not, generally speaking, contain $H$ and $K$ as subgroups. It however has surjective homomorphisms onto $K$ and $H$, with kernels $\ker \varphi \times 1$ and $1 \times \ker \psi$ respectively.

4.2.3. If $H$ and $K$ are finite groups, then $|H \times_K K| = |H| \cdot |K|/|N|$.

4.2.4. Example. Let $n, m \in \mathbb{N}$, $d = \gcd(n, m)$ and $l = \lcm(n, m)$. Then $\mathbb{Z}_d$ is a quotient group of both $\mathbb{Z}_n$ and $\mathbb{Z}_m$, and $\mathbb{Z}_n \times_{\mathbb{Z}_d} \mathbb{Z}_m \cong \mathbb{Z}_d$.

4.3. Direct product of several groups

4.3.1. The external direct product of $k$ groups $H_1, \ldots, H_k$ is defined similarly, $H_1 \times \cdots \times H_k = \{(h_1, \ldots, h_n), h_i \in H_i, i = 1, \ldots, k\}$, with the componentwise multiplication: $(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$. For each $i$, $H_i$ is identified with the subgroup $1 \times \cdots \times 1 \times H_i \times 1 \times \cdots \times H_k$ of the product.

4.3.2. For any groups $H_1, \ldots, H_k$, their "simultaneous" direct product is naturally isomorphic to the "successive" one: $H_1 \times H_2 \times \cdots \times H_k \cong H_1 \times (H_2 \times \cdots \times (H_k-1 \times H_k) \cdots)$.

4.3.3. If $G = H_1 \times \cdots \times H_k$ and with $H_i$ being considered as subgroups of $G$, we have:

- $\Theta$ for any $i \neq j$, $h h' = h' h$ for any $h \in H_i$ and $h' \in H_j$;
- $\Theta$ for every $i$, $H_i \leq G$.

15
The properties

\[ O \]

for any \( i \), \( H_i \cap (H_1 \cdots H_{i-1}H_{i+1} \cdots H_k) = 1 \);

\[ \Theta \]
ev\( \text{very element } a \in G \text{ is uniquely representable in the form } a = h_1 \cdots h_k \text{ with } h_i \in H_i \text{ for all } i; \)

\[ \Theta \]
if \( |G| < \infty \), then \( |G| = |H_1| \cdots |H_k| \);

\[ \Theta \]
for any \( i \), \( G/(H_1 \cdots H_{i-1}H_{i+1} \cdots H_k) \cong H_i \); moreover, the isomorphism is given by the factorization homomorphism, restricted on \( H_i \).

4.3.4. Let \( G \) be a group and \( H_1, \ldots, H_k \leq G \). We say that \( G \) is an internal direct product of \( H_1, \ldots, H_k \), and write \( G = H_1 \times \cdots \times H_k \), if \( G \) is isomorphic to the (external) direct product \( H_1 \times \cdots \times H_k \) under an isomorphism that is identical on each \( H_i \). (That is, there is an isomorphism \( \varphi : G \to H_1 \times \cdots \times H_k \) such that \( \varphi(h_i) = h_i \) for every \( h_i \in H_i \) and every \( i \). This implies that the element \((h_1, \ldots, h_k)\) of \( H_1 \times \cdots \times H_k \) corresponds to the element \( h_1 \cdots h_k \) of \( G \).

4.3.5. Proposition. Let \( G \) be a group and let \( H_1, \ldots, H_k \leq G \) satisfy the properties \( O\), \( \Theta \), and \( \Theta \) from 4.3.3. Then \( G = H_1 \times \cdots \times H_k \).

4.4. Direct product of infinitely many groups

To simplify notation, I’ll only discuss countable collection of groups, but uncountable collections can be considered as well.

4.4.1. The direct product of a sequence \( H_1, H_2, \ldots \) of groups is the group \( \prod_{i=1}^\infty H_i = \{(h_1, h_2, \ldots), \ h_i \in H_i, \ i = 1, 2, \ldots \} \), with the componentwise multiplication: \((a_1, a_2, \ldots)(b_1, b_2, \ldots) = (a_1b_1, a_2b_2, \ldots)\).

4.4.2. The group \( \prod_{i=1}^\infty H_i \) is not generated by the groups \( H_i \) (unless all but finitely many of these groups are trivial). The group, generated by \( H_1, H_2, \ldots \) is the normal subgroup \( M = \{(h_1, \ldots, h_k, 1, 1, 1, \ldots), \ k \in \mathbb{N}, \ h_i \in H_i, \ i = 1, \ldots, k \} \) of \( \prod_{i=1}^\infty H_i \). The group \( M \) is sometimes called the direct sum of \( H_i \); this is definitely so if the groups \( H_i \) are abelian and are written additively, in which case \( M \) is denoted by \( \bigoplus_{i=1}^\infty H_i \). The properties \( O\), \( \Theta \) hold for the direct sum rather than the direct product.

5. The Chinese remainder theorem and a complete classification of finite abelian groups

5.1. The Chinese remainder theorem

5.1.1. The following fact is sometimes referred to as the Chinese remainder theorem:

Theorem. For any coprime positive integers \( n \) and \( m \), \( \mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm} \). Moreover, \( \mathbb{Z}_{nm} = \langle m \rangle \times \langle n \rangle \), where \( \langle m \rangle = m\mathbb{Z}_{nm} \cong \mathbb{Z}_n \) and \( \langle n \rangle = n\mathbb{Z}_{nm} \cong \mathbb{Z}_m \).

5.1.2. Actually, the Chinese remainder theorem is the following statement:

The Chinese remainder theorem. Let \( n, m \in \mathbb{N} \) be coprime. Then for any \( a, b \in \mathbb{Z} \) there exists \( c \in \mathbb{Z} \) such that \( c = a \mod n \) and \( c = b \mod m \).

The theorem says that the homomorphism \( \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m, \ c \mapsto (c \mod n, c \mod m) \), is surjective. Indeed, since \( n \) and \( m \) are coprime, the kernel of this homomorphism is the subgroup \( \langle nm \rangle = nm\mathbb{Z} \) of \( \mathbb{Z} \), so by the first isomorphism theorem it induces an injective homomorphism \( \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m \); since the orders of these groups are equal, this homomorphism is an isomorphism.

5.1.3. Let \( n \in \mathbb{N}, n = p_1^{r_1} \cdots p_k^{r_k} \), where \( p_i \) are distinct primes and \( r_i \in \mathbb{N} \). Applying the Chinese remainder theorem several times, we get that \( \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} \).

5.2. The classification of finite abelian groups

5.2.1. The fundamental theorem of finite abelian groups – existence. Every finite abelian group \( G \) is a direct product of cyclic subgroups, \( G = H_1 \times \cdots \times H_m \), \( H_i = \langle a_i \rangle \) for some \( a_i \in G, \ i = 1, \ldots, m \). Moreover, the elements \( a_i \) can be chosen so that \( |a_m| \mid |a_{m-1}| \mid \cdots \mid |a_2| \mid |a_1| \).
Proof. Let \( a_1 \) be an element of \( G \) having the maximal order; let \( n_1 = |a_1| \). I claim that for any \( b \in G \), \( |b| \mid n_1 \). Indeed, assume that \( |b| = k \mid n_1 \), let \( p \) be a prime such that \( n = p^n a_1^k \), \( k = p^k \), with \( s > r \) and \( p \nmid a_1^s \). Then the element \( a_1^s b^k \) has order \( p^n a_1^k > n_1 \), contradiction. (Indeed, since the orders \( |a_1^p| = n_1', \) and \( |b^k| = p^r \) are coprime, the groups \( \langle a_1^p \rangle \cong \mathbb{Z}_{n_1} \) and \( \langle b^k \rangle \cong \mathbb{Z}_{p^r} \) have trivial intersection, so their join is their direct product.)

Now, let \( H_1 = \langle a_1 \rangle \). By induction on \( |G| \), the group \( K = G/H_1 \) is a direct product of cyclic subgroups: \( K = K_2 \times \cdots \times K_m \) where for each \( i = 2, \ldots, m \), \( K_i = \langle c_i \rangle \). I claim that the factorization homomorphism \( \pi: G \rightarrow K \) has a section \( \sigma: K \rightarrow G \); this will imply that \( G = H_1 \times H_2 \times \cdots \times H_k \), where \( H_i = \sigma(K_i) \). We have

\[
K = \left\{ c_2, \ldots, c_m \mid c_i c_j = c_j c_i \text{ for all } i, j \text{ and } c_i^{n_i} = 1 \text{ for all } i \right\}.
\]

To construct \( \sigma \), we need to find elements \( a_2, \ldots, a_m \) such that \( \pi(a_i) = c_i \) and \( a_i^{n_i} = 1 \), \( i = 2, \ldots, m \); then the homomorphism defined by \( \sigma(c_i) = a_i \), \( i = 2, \ldots, m \), is well defined and is a section of \( \pi \).

We can choose \( a_i \) independently for distinct \( i \). Fix \( i \), and let \( b_i \in G \) be such that \( \pi(b_i) = c_i \). Then \( b_i^{n_i} \in H_1 \) (and \( n_i \) is the minimal such positive integer); let \( b_i^{n_i} = a_i \). Let \( d = \gcd(n_i, l) \); then \( b_i^{n_i} = n_i/d \) and \( |b_i| = n_i/n_i/d \). (Indeed, if \( b_i^{n_i} = 1 \), then \( n = n_i l \) for some \( k \), so \( b_i^{n_i} = a_i \), and \( k = |a_i| = n_i/d \).)

We also have that \( |a_i| = |a_i| \), and by induction, \( |c_m| \mid |c_{m-1}| \cdots |c_2| \), so \( |a_m| \mid |a_{m-1}| \cdots |a_2| \) (since \( |a_i| = n_i = |c_i| \) for all \( i \)).

5.2.2. So, every abelian group \( G \) is isomorphic to a product \( \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m} \), where the orders \( n_i = |a_i|, i = 1, \ldots, m \), of the elements \( a_i \) from the theorem satisfy \( n_{m} \mid n_{m-1} \mid \cdots n_2 \mid n_1 \). The integers \( n_1, \ldots, n_m \) are called the invariant factors of \( G \).

Since, by 5.1.3, for each \( i \), \( \mathbb{Z}_{n_i} \) is isomorphic to a direct product of cyclic groups of the form \( \mathbb{Z}_{p^r} \) where \( p \) is a prime, we get that \( G \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} \) for some (not necessarily distinct) prime integers \( p_1, \ldots, p_k \) and \( r_1, \ldots, r_k \in \mathbb{N} \). The integers \( p_1^{r_1}, \ldots, p_k^{r_k} \) are called the elementary divisors of \( G \).

5.2.3. A representation of a finite abelian group \( G \) as a direct product of cyclic groups, \( G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_l} \), is not, generally speaking, unique. But given such a decomposition, it is easy to find the elementary divisor of \( G \) – these are the factors of the prime decompositions of the integers \( d_1, \ldots, d_l \). And the invariant factors of \( G \) can be easily recovered from the elementary divisors: if the elementary divisors are

\[
p_1^{r_1,1} \cdots p_1^{r_1,m_1}, p_2^{r_2,1} \cdots p_2^{r_2,m_2}, \ldots, p_k^{r_k,1} \cdots p_k^{r_k,m_k},
\]

where \( p_i \) are distinct primes and for each \( i \), \( r_{i,1} \geq r_{i,2} \geq \cdots \geq r_{i,k_i} \), there is only one way we can multiply them to get \( n_1, \ldots, n_m \) with \( n_m \mid n_{m-1} \mid \cdots n_2 \mid n_1 \), namely,

\[
n_1 = p_1^{r_1,1} \cdots p_k^{r_k,1}, n_2 = p_1^{r_1,2} \cdots p_k^{r_k,2}, \ldots, n_m = p_1^{r_1,m} \cdots p_k^{r_k,m},
\]

where \( m = \max(m_1, \ldots, m_k) \) and I assume that \( r_{i,l} = 0 \) for \( l > m_i \).

5.2.4. Example. Let \( G \cong \mathbb{Z}_{360} \times \mathbb{Z}_{24} \times \mathbb{Z}_{100} \times \mathbb{Z}_6 \). Since \( 360 = 2^3 \cdot 3^2 \cdot 5, 24 = 2^3 \cdot 3, 100 = 2^2 \cdot 5^2 \), and \( 6 = 2 \cdot 3 \), the elementary divisors of \( G \) are \( 2^3, 3^2, 5, 2^3, 3, 2^2, 5^2, 2, 3, 3, 2 \), so that \( G \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \).

Recorder the elementary divisors, grouping, in descending order, those associated with the same prime: \( 2^3, 2^2, 2; 3^2, 3, 3; 5^2, 5 \). We now get the invariant factors of \( G \): \( 2^3 \cdot 3^2 \cdot 5^2 = 1800, 2^3 \cdot 3 \cdot 5 = 120, 2^2 \cdot 3 = 12, 2 \), so that \( G \cong \mathbb{Z}_{1800} \times \mathbb{Z}_{120} \times \mathbb{Z}_{12} \times \mathbb{Z}_2 \).

5.2.5. The fundamental theorem of finite abelian groups – uniqueness. For every finite abelian group, its invariant factors and its elementary divisors are uniquely defined. So, two finite abelian groups are isomorphic iff they have the same collection of invariant factors, and iff they have the same collection of elementary divisors.
Proof. Let $G$ be a finite abelian group. The passages from the invariant factors to the elementary divisors and back are inverses of each other, so it suffices to prove that the elementary divisors of $G$ are uniquely defined.

Let

$$G \cong \left( \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_1 \cdot r_1} \right) \times \cdots \times \left( \mathbb{Z}_{p_k} \times \cdots \times \mathbb{Z}_{p_k \cdot r_k} \right),$$

where $p_1, \ldots, p_k$ are distinct primes and $r_{i,j} \in \mathbb{N}$. For any group $H$ and $n \in \mathbb{N}$ let

$$e(H, n) = \#\{a \in H : a^n = 1\}.$$

For any prime $p$, $r \in \mathbb{N}$, and $s \geq 0$ we have $e(\mathbb{Z}_{p^r}, p^s) = p^s$ if $s \leq r$ and $= p^r$ if $s > r$, and $e(\mathbb{Z}_{p^r}, q^s) = 1$ for any prime $q \neq p$. Thus for any $i \in \{1, \ldots, k\}$ and $s \geq 0$ we have $e(G, p_i^s) = p_i^s$, where

$$v = \sum_{1 \leq j \leq m_i, r_{i,j} < s} r_{i,j} + \#\{j : r_{i,j} \geq s\} \cdot s.$$

For every $i$ and $s \in \mathbb{N}$ we therefore have

$$\log_{p_i} e(G, p_i^s) - \log_{p_i} e(G, p_i^{s-1}) = \sum_{1 \leq j \leq m_i, r_{i,j} < s} r_{i,j} - \sum_{1 \leq j \leq m_i, r_{i,j} < s-1} r_{i,j} + \#\{j : r_{i,j} \geq s\} \cdot s - \#\{j : r_{i,j} \geq s - 1\} \cdot (s-1) = \#\{j : r_{i,j} = s - 1\} \cdot (s-1) - \#\{j : r_{i,j} = s - 1\} \cdot (s-1) + \#\{j : r_{i,j} \geq s\} = \#\{j : r_{i,j} \geq s\}.$$

Since the numbers $e(G, p_i^s)$ are defined by $G$, the collection of exponents $r_{i,j}$ is also uniquely defined by $G$. □

5.3. The groups $\mathbb{Z}_n^*$.

For $n \in \mathbb{N}$, $\mathbb{Z}_n^*$ is a finite abelian group (of order $\varphi(n)$), and thus is a direct product of cyclic subgroups; the factorization of $\mathbb{Z}_n^*$ can be easily determined, based on the following lemmas.

5.3.1. Lemma. For any prime $p$, $Z^*_p$ is a cyclic group (and so, is isomorphic to $Z_{p-1}$).

Proof. Let $n_m = \cdots = n_1$ be the invariant factors of $\mathbb{Z}_p^*$, so that $\mathbb{Z}_p^* \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ and $n_1 \cdots n_m = p-1$. Then $a^{n_1} = 1$ for all nonzero $a \in \mathbb{Z}_p^*$, that is, the polynomial $x^{n_1} - 1$ has $p-1$ roots in $\mathbb{Z}_p$. But $\mathbb{Z}_p = \mathbb{F}_p$ is a field, thus any polynomial of degree $d$ with coefficients from $\mathbb{Z}_p$ has at most $d$ roots. Hence, $p-1 \leq n_1$, so $p-1 = n_1$, $m = 1$, and $\mathbb{Z}_p^* \cong \mathbb{Z}_{n_1}$. □

5.3.2. Lemma. For any $r \in \mathbb{N}$ and any prime $p \geq 3$ the group $\mathbb{Z}_{p^r}^*$ is cyclic (and so, is isomorphic to $Z_{p^r-1}$).

Proof. Let $p \geq 3$ and $r \in \mathbb{N}$. Then $|\mathbb{Z}_{p^r}^*| = p^{r-1}(p-1)$. Since $p \nmid (p-1)$, $\mathbb{Z}_{p^r}$ is a direct product $P \times H$ of its $p$-component $P$ (which is a subgroup of order $p^{r-1}$ that consists of all elements of orders $p^k$, $k \geq 0$) and a subgroup $H$ of order $p-1$. It is easy to check that the element $p+1$ has order $p^{r-1}$, so $P$ is cyclic, generated by $p+1$.

The factorization mapping $\mathbb{Z}_{p^r} \rightarrow \mathbb{Z}_{p^r}/(p) \cong \mathbb{Z}_p$ is a homomorphism of the multiplicative groups as well, and induces a surjective homomorphism $\pi : \mathbb{Z}_{p^r}^* \rightarrow \mathbb{Z}_p^*$. Since the orders $|P|$ and $|\mathbb{Z}_{p}^*|$ are coprime, $\pi(P) = 1$, so $\pi_H$ is surjective, and since $|H| = |\mathbb{Z}_{p}^*|$, is an isomorphism between $H$ and $\mathbb{Z}_{p}^*$. Hence, by Lemma 5.3.1, $H$ is also cyclic, and by the Chinese remainder theorem, $\mathbb{Z}_{p^r}^* = P \times H$ is cyclic.

For $p = 2$ and $r \geq 2$, the group $\mathbb{Z}_{2^r}^*$ is not cyclic, since it has 3 elements of order 2: $-1$ and $2^{r-1} \pm 1$. However, it is easy to see that the element $5 = 1 + 2^2$ has order $2^{r-2}$, so $\mathbb{Z}_{2^r}^* \cong \mathbb{Z}_{2^{r-2}} \times \mathbb{Z}_2$. □

5.3.3. Lemma. Let $n = p_1^{k_1} \cdots p_k^{k_k}$ be the prime factorization of $n \in \mathbb{N}$. Then $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^*$.

Proof. The isomorphism $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$, appearing in the Chinese remainder theorem, is multiplicative $(\varphi(ab) = \varphi(a)\varphi(b))$, and induces an isomorphism of the multiplicative groups $\mathbb{Z}_n^* \rightarrow \mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^*$. □
6. Groups of automorphisms and semidirect products of groups

6.1. Groups of automorphisms

6.1.1. Let $G$ be a group; the automorphisms of $G$ (that is, the isomorphisms $G \to G$) under the operation of composition form a group, called the group of automorphisms of $G$ and denoted by $\text{Aut}(G)$.

6.1.2. If a group $G$ is presented by generators and relations, $G = \langle S \mid R \rangle$, then any automorphism $\varphi$ of $G$ is defined by its action, $\varphi(s)$, on the generators $s \in S$; the elements $\varphi(s)$ must generate $G$ and satisfy all the relations from $R$ (that is, it must be that $\varphi(r) = 1$ for all $r \in R$). If $G$ is a finite group, this is enough for $\varphi$ to be an automorphism; if $G$ is infinite, it should also be checked that $\varphi$ is injective.

6.1.3. Examples.

(i) $\text{Aut}(\mathbb{Z}) = \{1, \varphi\}$ where $\varphi(m) = -m$, $m \in \mathbb{Z}$. So, $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

(ii) $\text{Aut}(\mathbb{Q}) \cong \mathbb{Q}^*$: any automorphism of $\mathbb{Q}$ has form $\varphi_r(s) = rs$, $s \in \mathbb{Q}$, for some $r \in \mathbb{Q}^*$, and we have $\varphi_{r_1}\varphi_{r_2} = \varphi_{r_1r_2}$.

(iii) $\text{Aut}(V_4) \cong S_3$: automorphisms of $V_4 = \{1, a, b, c\}$ act as permutations of the set $\{a, b, c\}$.

(iv) For any $n$, $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$. Indeed, any automorphism $\varphi$ of $\mathbb{Z}_n$ is uniquely defined by the element $\varphi(1)$, which has to be a generators of $\mathbb{Z}_n$. So, the automorphisms have form $\varphi_k(m) = km$, $m \in \mathbb{Z}_n$, with $k \in \mathbb{Z}_n^*$, and $\varphi_k\varphi_{k'} = \varphi_{kk'}$.

(v) Let $n \geq 3$. Any automorphism of the dihedral group $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1}\rangle$ maps $r$ to an element of order $n$, that is, to $r^k$ with $k \in \mathbb{Z}_n^*$, and $s$ to one of the elements $sr^l$, $l \in \mathbb{Z}_n$; it is easy to check that the elements $r^k$ and $sr^l$ generate $D_{2n}$ and satisfy the relations for $r$ and $s$. So, $\text{Aut}(D_{2n}) = \{\varphi_k, l \mid k \in \mathbb{Z}_n^*, l \in \mathbb{Z}_n\}$, where $\varphi_k, l$ are defined by $\varphi_k(r) = r^k$, $\varphi_k(l)(s) = sr^l$. The multiplication on $\text{Aut}(D_{2n})$ is defined by $\varphi_{k_1, l_1}\varphi_{k_2, l_2} = \varphi_{k_1+k_2, l_1+l_2}$.

(vi) $\text{Aut}(Q_8) \cong S_4$. (It is easy to find all automorphisms of $Q_8$ and construct the multiplication table of $\text{Aut}(Q_8)$; but it is not immediately clear that this group is actually isomorphic to $S_4$.)

6.1.4. Let $G$ be a group. Every element $a \in G$ defines an automorphism of $G$ by conjugation, $\varphi_a(b) = aba^{-1}$. Automorphisms of $G$ of this form are called inner; they form a subgroup of $\text{Aut}(G)$ denoted by $\text{Inn}(G)$.

We have a homomorphism $\Phi: G \to \text{Aut}(G)$, $\Phi(a) = \varphi_a$. By definition, the image of $\Phi$ is $\text{Inn}(G)$, and $\ker \Phi = Z(G)$. Thus, $\text{Inn}(G) \cong G/Z(G)$.

6.1.5. $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$; the quotient group $\text{Aut}(G)/\text{Inn}(G)$ is called the group of outer automorphisms of $G$ and is denoted by $\text{Out}(G)$. (Actually, the elements of $\text{Out}(G)$ are not automorphisms of $G$, but automorphisms of $G$ up to inner automorphisms.)

6.1.6. Examples.

(i) For any abelian group $G$, $\text{Inn}(G) = 1$ and so, $\text{Out}(G) = \text{Aut}(G)$ (all automorphisms of $G$ are outer).

(ii) $Z(D_{2n}) = 1$ if $n$ is odd and $= \{1, r^{n/2}\}$ if $n$ is even. So, $\text{Inn}(D_{2n}) \cong D_{2n}$ if $n$ is odd and $\cong D_{2n}/(r^{n/2}) \cong D_n$ if $n$ is even. For all $n > 3$ this is a proper subgroup of $\text{Aut}(D_{2n})$.

(iii) $Z(Q_8) = \{1, -1\}$, so $\text{Inn}(Q_8) \cong Q_8/\{\pm 1\} \cong V_4$. So, $\text{Inn}(Q_8)$ is a normal subgroup, isomorphic to $V_4$, in $\text{Aut}(Q_8) \cong S_4$. (There is only one such.)

(iv) All automorphisms of $S_n$ are inner, $\text{Aut}(S_n) = \text{Inn}(S_n)$, for all $n \neq 6$. For $n = 6$, there is an outer automorphism of $S_6$: it maps transpositions to permutations of the cycle type 2, 2, 2, and we have $\text{Out}(S_6) \cong \mathbb{Z}_2$.

6.2. Characteristic subgroups

6.2.1. A subgroup $H$ of a group $G$ is said to be characteristic if $\varphi(H) = H$ for all $\varphi \in \text{Aut}(G)$; this is denoted by “$H$ char $G$”.

6.2.2. Examples.

(i) If $H$ is the only subgroup of $G$ of a certain order or index, then $H$ char $G$. 

---

5.3.4. Example. For $7200 = 5^2 \cdot 3^3 \cdot 2^5$ we have

$$\mathbb{Z}_{7200} \cong \mathbb{Z}_{5^2} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_{2^5} \cong \mathbb{Z}_{5 \cdot 4} \times \mathbb{Z}_{3 \cdot 2} \times \mathbb{Z}_2 \cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_2 \cong \mathbb{Z}_{40} \times \mathbb{Z}_{12} \times \mathbb{Z}_2^2.$$
(ii) Every subgroup of \(Z\) and of \(Z_n\), for any \(n\), is characteristic.

(iii) \(\langle a \rangle\) is not a characteristic subgroup of \(V_4 = \{1, a, b, c\}\) (but is normal).

(iv) For any \(n\), \(\langle r \rangle\) char \(D_{2n}\), and every subgroup of \(\langle r \rangle\) is also characteristic in \(D_{2n}\).

(v) For any \(n\), \(A_n\) char \(S_n\).

(vi) Any subgroup of a group \(G\) consisting of, or generated by, “all expressions of the form ...” is characteristic in \(G\); such are the subgroup \(\langle a^n, a \in G \rangle\), for any \(n \in \mathbb{N}\), and the commutator, or the derived, subgroup \(G_2 = [G, G] = \langle [a, b], a, b \in G \rangle\) (where \([a, b] = aba^{-1}b^{-1}\)).

(vii) Also, any subgroup of a group \(G\) consisting of, or generated by, all elements of \(G\) satisfying certain equations, is characteristic in \(G\); such are, for examples, the subgroup \(\langle a : a^n = 1 \rangle\), for any \(n \in \mathbb{N}\), and the center \(Z(G) = \{a \in G : ab = ba\} \text{ for all } b \in G\) of \(G\).

6.2.3. Proposition. Every characteristic subgroup is normal. The intersection and the join of any collection of characteristic subgroups is characteristic. If \(H\) char \(K\) char \(G\) then \(H\) char \(G\), and if \(H\) char \(K \trianglelefteq G\), then \(H \trianglelefteq G\).

6.3. Semidirect product of groups

6.3.1. Let \(G\) be a group and \(H \trianglelefteq G\). Then \(G\) acts on \(H\) by conjugations: for \(a \in G\), the mapping \(\varphi_a(h) = aha^{-1}, h \in H\), is an automorphism of \(H\). So, we have a homomorphism \(\varphi: G \to \text{Aut}(H), \varphi(a) = \varphi_a\), with \(\ker \varphi = C_G(H)\) (the centralizer of \(H\) in \(G\)).

6.3.2. Let \(G\) be a group with subgroups \(H\) and \(K\) such that \(H\) is normal in \(G\), \(H \cap K = 1\), and \(HK = G\); we then say that \(G\) is an (internal) semidirect product of \(H\) and \(K\), and write \(G = H \rtimes K\).

6.3.3. If \(G = H \rtimes K\), then, similarly to 4.1.2,

(i) for any \(h \in H\) and \(k \in K\), \(kh = h'k\), where \(h' = khk^{-1} \in H\);

(ii) \(H\) is normal in \(G\);

(iii) \(HK = G\);

(iv) \(H \cap K = 1\);

(v) every element \(a \in G\) is uniquely representable in the form \(a = hk\) with \(h \in H\) and \(k \in K\);

(vi) if \(|G| < \infty\), then \(|G| = |H| \cdot |K|\);

(vii) \(G/H \cong K\); moreover, for the factorization homomorphism \(\pi: G \to G/H, \pi|_K\) is an isomorphism between \(K\) and \(G/H\).

And, as in Proposition 4.1.7, \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), \(\triangleleft \leftrightarrow \triangleleft \& \triangleleft\), \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), and if \(|G| < \infty\), \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\). As a corollary we get that \(G = H \rtimes K\) if any of the following combinations of conditions holds: \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), and if \(|G| < \infty\), \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\), and \(\triangleleft \& \triangleleft \Rightarrow \triangleleft\).

6.3.4. Also, as in Proposition 4.1.10, the fact that \(\triangleleft \& \triangleleft\) imply semidirect product can be reformulated in the following way:

Proposition. Let \(H \triangleleft G\), \(K = G/H\), and assume that the factorization homomorphism \(G \to G/H\) has a section \(\sigma: K \to G\). Then \(G = H \rtimes \sigma(K)\).

6.3.5. Examples.

(i) The direct product is a special case of a semidirect product.

(ii) For any \(n\), \(D_{2n} = \langle r \rangle \rtimes \langle s \rangle\).

(iii) For any \(n\), \(S_n = A_n \rtimes \langle \tau \rangle\), where \(\tau\) is any transposition from \(S_n\).

(iv) Let \(G\) be the group of nonconstant affine functions \(\mathbb{R} \to \mathbb{R}, G = \{f(x) = ax + b, a \in \mathbb{R}^*, b \in \mathbb{R}\}\), with the operation of composition. Let \(H = \{h_b(x) = x + b, b \in \mathbb{R}\} \cong \mathbb{R}, K = \{k_a(x) = ax, a \in \mathbb{R}^*\} \cong \mathbb{R}^*\). Then \(G = H \rtimes K\), with \(k_a h_b k_a^{-1} = h_{ab}\).

6.3.6. If \(G = H \rtimes K\), then \(K\) acts on \(H\) by conjugations, which induces a homomorphism \(\varphi: K \to \text{Aut}(H)\): for \(k \in K\), \(\varphi(k) = \varphi_k\) defined by \(\varphi_k(h) = khk^{-1}, h \in H\). The multiplication in \(G\) is completely defined by \(H, K\), and this homomorphism \(\varphi\): for \(h \in H\) and \(k \in K\), \(hk = (khk^{-1})k = \varphi_k(h)k\).
6.3.7. Given two groups $H$ and $K$, it turns out that any homomorphism $\varphi : K \longrightarrow \text{Aut}(H)$, $\varphi(k) = \varphi_k \in \text{Aut}(H)$, $k \in K$, leads to a semidirect product of $H$ and $K$. Indeed, put $G = H \times K$ as a set, that is, $G = \{(h, k), \ h \in H, k \in K\}$, and define multiplication on $G$ by

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi_{k_1}(h_2), k_1k_2).$$

Then $G$ is a group, the set $\bar{H} = H \times 1$ is a normal subgroup of $G$ (isomorphic to $H$), the set $\bar{K} = 1 \times K$ is a subgroup of $G$ (isomorphic to $K$), and $G = \bar{H} \rtimes \bar{K}$. The obtained group $G$ is called the (external) semidirect product of $H$ and $K$ induced by $\varphi$ and is denoted by $H \rtimes_{\varphi} K$.

The groups $H$ and $K$ are identified, respectively, with the subgroups $\bar{H}$ and $\bar{K}$ of $G$; we then have $G = H \rtimes K$ ("internally"), so that for any $h \in H$ and $k \in K$ we have $khk^{-1} = \varphi_k(h)$.

6.3.8. Examples.

(i) Let $K = \{1, a\} \cong \mathbb{Z}_2$. For any abelian group $H$ we have a homomorphism $\varphi : K \longrightarrow \text{Aut}(H)$ defined by $\varphi_a(h) = h^{-1}$, $h \in H$. This gives as the semidirect product $G = H \rtimes_a K$, in which $ah = h^{-1}a$ for all $h \in H$. For $H \cong \mathbb{Z}_n$, the obtained group is isomorphic to $D_{2n}$.

(ii) Let $H$ be a cyclic group of order 8, $H = \langle a \rangle \cong \mathbb{Z}_8$. Then $\text{Aut}(H) = \{\psi_1 = 1, \psi_3, \psi_5, \psi_7\} \cong V_4$, where $\psi_k(a) = a^k$. Let $K = \{1, b\} \cong \mathbb{Z}_2$; there are 4 homomorphisms $K \longrightarrow \text{Aut}(H)$, that map $b$ to any of the elements of $\text{Aut}(H)$, $\varphi_k(b) = \psi_k$, $k = 1, 3, 5, 7$. We then have

- $H \rtimes_{\varphi_1} K = H \times K = \langle a, b \mid a^8 = b^2 = 1, ba = ab \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$;
- $H \rtimes_{\varphi_3} K = \langle a, b \mid a^8 = b^2 = 1, ba = a^3b \rangle$, called the quasidihedral group $QD_{16}$ (or $SD_{16}$);
- $H \rtimes_{\varphi_5} K = \langle a, b \mid a^8 = b^2 = 1, ba = a^5b \rangle$, called the modular group $M_{16}$;
- $H \rtimes_{\varphi_7} K = \langle a, b \mid a^8 = b^2 = 1, ba = a^7b \rangle \cong D_{16}$.

(The group, say $\langle a, b \mid a^8 = b^2 = 1, ba = a^2b \rangle$ also exists, of course, but it has "hidden" relations: we have $a = b^2ab^{-2} = b(bab^{-1})b^{-1} = b^2b^{-1} = a^4$, so $a^3 = 1$, so $a = a^8a^{-8} = 1$. So, this group is not really constructed from $H$ and $K$, since it does not contain $H$ as a subgroup. The problem here is that the mapping $a \mapsto bab^{-1} = a^2$ is not an automorphism of $H$.)

(iii) To construct a nonabelian semidirect product $H \rtimes K$, one needs a nontrivial homomorphism $\mathbb{Z}_m \rightarrow \mathbb{Z}^*_n$, such a homomorphism exists iff the integers $m$ and $|\mathbb{Z}_n^*| = \varphi(n)$ are not coprime. In particular, if $p$ and $q$ are prime integers, a nonabelian semidirect product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ exists iff $p \divides (q - 1)$. So, the only semidirect product $\mathbb{Z}_5 \rtimes \mathbb{Z}_3$ is the direct product $\mathbb{Z}_5 \times \mathbb{Z}_3$, whereas a nonabelian semidirect product $\mathbb{Z}_5 \rtimes \mathbb{Z}_3$ exists; to construct it, we find an element of order 3 in $\mathbb{Z}_5^*$, which is 2 (and 4), and define (in multiplicative terms) $G = \langle a, b \mid a^2 = b^3 = 1, bab^{-1} = a^2 \rangle$.

(iv) Let $p \in \mathbb{N}$ be prime and $A = \begin{pmatrix} a & b \\ b & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_p)$ have order $n$. Then a nonabelian semidirect product $\mathbb{Z}_p^2 \rtimes \mathbb{Z}_n$ can be defined (multiplicatively) by $\langle a, b, c \mid a^n = b^p = c^n = 1, ab = ba, cac^{-1} = a^\gamma b^\delta, bcbc^{-1} = a^\beta b^\delta \rangle$. (Of course, this example generalizes to the case of the group $\mathbb{Z}_p^k$ and a matrix $A \in \text{GL}_k(\mathbb{F}_p)$, for any $k$.)

6.3.9. Let $H$ be a group; the holomorph of $H$ is the group $\text{Hol}(H) = H \rtimes \text{Aut}(H)$, where the semidirect product is induced by the identity homomorphism $\text{Aut}(H) \longrightarrow \text{Aut}(H)$. (This means that $\text{Hol}(H) = H \times \text{Aut}(H)$ as a set, with multiplication defined by $(h_1, \varphi_1)(h_2, \varphi_2) = (h_1\varphi_1(h_2), \varphi_1\varphi_2)$.)

6.3.10. Example. For any $n$, $\text{Hol}(\mathbb{Z}_n) = \mathbb{Z}_n \rtimes \mathbb{Z}^*_n$ with multiplication $(l_1, k_1)(l_2, k_2) = (l_1 + k_1l_2, k_1k_2)$. (Notice that this group is isomorphic to the group $\text{Aut}(D_n)$; see 6.1.3(v).)

6.3.11. It may happen that distinct homomorphisms $\varphi_1, \varphi_2 : K \longrightarrow \text{Aut}(H)$ produce isomorphic semidirect products $H \rtimes K$. Here are two such situations:

Lemma. Let $H$ and $K$ be groups, let $\varphi_1, \varphi_2 : K \longrightarrow \text{Aut}(H)$ be homomorphisms, and assume that $\varphi_2$ and $\varphi_1$ are conjugate: there is $\psi \in \text{Aut}(H)$ such that $\varphi_2(k) = \psi\varphi_1(k)\psi^{-1}$ for all $k \in K$. Then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.

(The isomorphism has form $(h, k) \mapsto (\psi(h), k)$.)
6.3.12. Lemma. Let $H$ be a group, $K$ be a cyclic group, and let $\varphi_1, \varphi_2: K \rightarrow \text{Aut}(H)$ be homomorphisms such that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\text{Aut}(H)$; if $|K| = \infty$, assume additionally that $\varphi_i$ are injective. Then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.

(The isomorphism has form $(h, k) \mapsto (\psi(h), k^r)$ where $\psi \in \text{Aut}(H)$ is such that $\psi\varphi_1(H)\psi^{-1} = \varphi_2(H)$ and $r \in \mathbb{N}$.)

7. Sylow theorems and groups of small orders

7.1. $p$-groups

Let $p$ be a prime.

7.1.1. A finite group $G$ is called a $p$-group if $|G|$ is a power of $p$, $|G| = p^r$ for some $r \in \mathbb{N}$.

7.1.2. Example. The groups $Q_8$, $D_8$, $M_{16}$, $QD_{16}$, $Z_{16}$ and $Z_4 \times Z_4$ are 2-groups.

7.1.3. If $G$ is a $p$-group, then for any $a \in G$, $|a| = p^l$ for some $l \geq 0$. Any subgroup and any factorgroup of a $p$ group is a $p$-group. If $H_1$ and $H_2$ are $p$-subgroups of a group $G$, then the intersection $H_1 \cap H_2$ is a $p$-group, and if $H_2 \subseteq N_G(H_1)$, the also the join $H_1H_2$ is a $p$-group.

7.1.4. For any $r$, the $p$-group $Z_{p^r}$ “is made of” $r$ groups isomorphic to $Z_p$: its composition series is $0 \leq \langle p^{r-1} \rangle \leq \langle p^{r-2} \rangle \leq \cdots \leq \langle p \rangle \leq \langle 1 \rangle = Z_{p^r}$, with $\langle p^k \rangle \cong Z_{p^{k-1}}$ and $\langle p^k \rangle / \langle p^{k+1} \rangle \cong Z_p$ for all $k$.

7.1.5. If $G$ is a $p$-group, then $Z(G) \neq 1$. (Indeed, let $G = \bigcup_{i=1}^{k} C_i$ be the partition of $G$ into conjugacy classes. Then for each $i$, $|C_i| = 1$ or $|C_i|$ is divisible by $p$. Since $p \mid |G|$ and the class of 1 is the singleton $\{1\}$, there are other singleton classes in $G$: the union of these singletons is the center of $G$.) Assume that $Z(G) \neq G$ and put $G^{(1)} = Z(G)$; then $G/G^{(1)}$, is also a $p$-group, so $Z(G/G^{(1)}) \neq 1$; let $G^{(2)}$ be the preimage of $Z(G/G^{(1)})$ in $G$. Etc.; we get a subnormal series

$$1 \trianglelefteq G^{(1)} \trianglelefteq G^{(2)} \trianglelefteq \cdots \trianglelefteq G^{(d)} = G$$

(7.1)

of $G$ where for each $k$, $G^{(k+1)}/G^{(k)} = Z(G/G^{(k)})$. Such a series is called central; groups possessing finite central series are called nilpotent. (So, we’ve just proved that $p$-groups are nilpotent.) Since the factors of (7.1) are abelian $p$-groups, it follows from 7.1.4 that “$G$ is made of cyclic groups of order $p^d$”: all factors of the composition series of $G$ are isomorphic to $Z_p$.

7.2. Sylow’s theorems

This is a theorem, or a set of four theorems, giving a lot of information about $p$-subgroups of finite groups:

7.2.1. Sylow’s theorems. Let $G$ be a finite group, $|G| = n$, let $p$ be a prime divisor of $n$, let $n = p^r m$ with $p \nmid m$.

(i) For any $s \leq r$ there exists a subgroup $H \leq G$ with $|H| = p^s$.

In particular, there are subgroups of $G$ of order $p^s$; these maximal $p$-subgroups of $G$ are called Sylow $p$-subgroups. The set of Sylow $p$-subgroups in $G$ is denoted by $\text{Syl}_p(G)$.

(ii) For any $s < r$ and any subgroup $H \leq G$ with $|H| = p^s$ there exists a subgroup $K \leq G$ with $|K| = p^{s+1}$ such that $H \trianglelefteq K$.

In particular, every $p$-subgroup of $H$ of $G$ is contained in a Sylow $p$-subgroup of $G$.

(iii) All Sylow $p$-subgroups are conjugate.

(So, $\text{Syl}_p(G)$ is a conjugacy class of subgroups.

(iv) Let $n_p$ be the number of Sylow $p$-subgroups of $G$, $n_p = |\text{Syl}_p(G)|$. Then $n_p = 1 \mod p$ and $n_p \mid m$.

Proof.
(i) Let \( s \leq r \). Consider the set \( A = \{ A \subseteq G, |A| = p^s \} \). We have

\[
|A| = \binom{n}{p^s} = \frac{p^s m (p^s m - 1) (p^s m - 2) \cdots (p^s m - p^s + 1)}{p^s (p^s - 1) (p^s - 2) \cdots 1} = \frac{p^{r-s} m (p^s m - 1) (p^s m - 2) \cdots (p^s m - p^s + 1)}{(p^s - 1) (p^s - 2) \cdots 1}.
\]

No factor in the numerator or the denominator of this quotient is divisible by \( p^s \), and for every \( k = 1, \ldots, p^s - 1 \) one has \( p^s m - k = p^s - k \mod p^s \); hence, all appearances of \( p \) in the numerator and the denominator cancel, and we get \( |A| = p^{r-s} M \) with \( p \nmid M \).

\( G \) acts on \( A \) by left multiplications, and \( A \) partitions into orbits under this action; since \( p^{r-s+1} \nmid |G| \), there is a set \( A \in A \) such that the orbit \( O(A) \) has cardinality \( p^k l, p \nmid l \), with \( k \leq r - s \). Let \( H = G_A \), the stabilizer of \( A \) in \( G \); then \( |H| = |G|/|O(A)| = p^k m / (p^k l) = p^{-k} (m/l) \) where \( r - k \geq s \), so \( p^s \nmid |H| \). On the other hand, \( H \) preserves \( A \), so acts on \( A \) by left multiplications, and for any \( a \in A \) the mapping \( H \rightarrow A, h \mapsto h a \), is injective; hence, \( |H| \leq |A| = p^s \). It follows that \( |H| = p^s \).

(ii) Let \( s < r \), \( H \leq G \), \( |H| = p^s \). Let \( \mathcal{H} \) be the conjugacy class of \( H \); then \( |\mathcal{H}| = |G|/|N_G(H)| \). I claim that \( p^{s+1} \nmid |N_G(H)| \). Indeed, assume that this is not so; then \( p \nmid |\mathcal{H}| \). Consider the action of \( H \) on \( \mathcal{H} \) by conjugations. Under this action, \( \mathcal{H} \) partitions into several orbits. The orbit of \( H \) itself is the singleton \( \{ H \} \), thus there are other singleton orbits in \( \mathcal{H} \); let \( \{ H' \} \) be such. Then \( H \) normalizes \( H' \), so \( H' = H H' \) is a \( p \)-subgroup with \( p^{s+1} \nmid |L'| \), and \( H' \leq L' \). Let \( a \in G \) be such that \( a H' a^{-1} = H \), put \( L = a L a^{-1} \); then \( H \trianglelefteq L \) so \( L \leq N_G(H) \), and \( p^{s+1} \nmid |L| \), which contradicts the assumption that \( p^{s+1} \nmid |N_G(H)| \).

It follows that \( p \nmid |N_G(H)/H| \). Let \( \tilde{K} \) be a subgroup of order \( p \) in \( N_G(H)/H \) (which exists by (i)), and let \( K \) be its preimage in \( N_G(H) \). Then \( |K| = p^{s+1} \) and \( H \leq K \).

(iii) Let \( K \) and \( H \) be two Sylow \( p \)-subgroups of \( G \). Let \( \mathcal{H} \) be the conjugacy class of \( H \); it consists of Sylow \( p \)-subgroups of \( G \) conjugate to \( H \). We have \( |\mathcal{H}| = |G|/|N_G(H)| \) and since \( N_G(H) \geq H, p \nmid |\mathcal{H}| \). Under the action of \( K \) by conjugations \( \mathcal{H} \) partitions into orbits of cardinality either 1 or divisible by \( p \); since \( p \nmid |\mathcal{H}| \), there is a singleton orbit \( \{ H' \} \) in \( \mathcal{H} \). This means that \( K \) normalizes \( H' \), so \( K H' \) is a \( p \)-subgroup of \( G \) containing both \( K \) and \( H' \). But \( K \) and \( H' \) are maximal \( p \)-subgroups of \( G \), so \( K = K H' = H' K \), and \( K \in \mathcal{H} \).

(iv) Let \( \mathcal{H} \) be the set of Sylow \( p \)-subgroups of \( G \). Let \( H \in \mathcal{H}, H \) acts on \( \mathcal{H} \) by conjugations. Under this action the orbit of \( H \) is \( \{ H \} \). For any \( K \in \mathcal{H} \) distinct from \( H \), the orbit of \( K \) is not a singleton (otherwise \( H K K = K \) would be a \( p \)-group larger than \( K \)), so has cardinality divisible by \( p \). Hence, \( n_p = |H| = 1 \mod p \).

Finally, \( n_p = |G|/|N_G(H)| \). Since \( N_G(H) \geq H, |N_G(H)| = p^{s+1}l \) for some \( l \), so \( n_p = m/l \).

7.2.2. Let \( G \) be a finite group and \( p \) be a prime divisor of \( |G| \). If \( n_p = 1 \), that is, \( G \) has a single Sylow \( p \)-subgroup, then this subgroup is normal and, moreover, characteristic; it consists of all elements of \( G \) whose order is a power of \( p \).

If \( n_p \neq 1 \), then Sylow \( p \)-subgroups of \( G \) are not normal; their union (which is not a subgroup) consists of all elements of \( G \) whose order is a power of \( p \).

7.2.3. Let \( G \) be a finite group with \( |G| = p_1^{s_1} p_2^{s_2} \), and let \( P_1 \subseteq \text{Syl}_{p_1}(G), P_2 \subseteq \text{Syl}_{p_2}(G) \); then \( P_1 \cap P_2 = 1 \) and \( |P_1| \cdot |P_2| = |G| \). If both \( n_{p_1} = n_{p_2} = 1 \), then \( G = P_1 \times P_2 \). If only \( n_{p_i} = 1 \), then \( G = P_1 \rtimes P_2 \).

7.2.4. Now let \( G \) be a finite group with \( |G| = p_1^{s_1} \cdots p_k^{s_k} \), and let \( P_i \subseteq \text{Syl}_{p_i}(G), i = 1, \ldots, k \). Then \( |P_1| \cdots |P_k| = |G| \) and \( P_1 \cap P_2 = 1 \) for any \( i \neq j \). Moreover, if for some \( i_1, \ldots, i_l \) the product \( H = P_{i_1} \cdots P_{i_l} \) is a group, then for any \( j \notin \{ i_1, \ldots, i_l \}, P_j \cap H = 1 \). It follows that if \( n_{p_i} = 1 \) for all \( i \), then \( G = P_1 \times \cdots \times P_k \); if \( n_{p_i} = 1 \) for all \( i = 1, \ldots, k-1 \), then \( G = (P_1 \times \cdots \times P_{k-1}) \rtimes P_k \).

7.2.5. Example. Let \( G \) be a group of order 6 = 2 \cdot 3 \), let \( P \in \text{Syl}_2(G) \) and \( Q \in \text{Syl}_3(G) \). We have \( n_3 = 1 \mod 3 \) and \( n_3 = 2 \); it follows that \( n_3 = 1 \). If also \( n_2 = 1 \), then \( G = P \times Q \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \). If \( n_2 \neq 1 \), then \( G = P \rtimes Q \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \). There is only one such homomorphism, namely, \( 1 \mapsto (1 \mapsto 2) \), and \( G \) has a presentation \( \langle a, b | a^3 = b^2 = 1, bab^{-1} = a^{-1} \rangle \).

Since such a nonabelian group \( G \) is unique (up to isomorphism), it must be isomorphic to \( S_3 \); and indeed, \( S_3 \) has a presentation above. So, up to isomorphism, the only groups of order 6 are \( \mathbb{Z}_6 \) and \( S_3 \).
7.2.6. Example. Let $G$ be a group of order $12 = 2^2 \cdot 3$, let $P \in \text{Syl}_2(G)$ and $Q \in \text{Syl}_3(G)$; then $Q \cong \mathbb{Z}_3$ and $P \cong \mathbb{Z}_4$ or $P \cong V_4 \cong \mathbb{Z}_2^2$.

If $n_2 = n_3 = 1$, then $G = P \times Q$ is abelian, and is isomorphic to $\mathbb{Z}_{12}$ or $\mathbb{Z}_6 \times \mathbb{Z}_2$.

If $n_2 = 1$ and $n_2 \neq 1$, then $G = Q \rtimes P$, which product is induced by a homomorphism $P \longrightarrow \text{Aut}(Q) \cong \mathbb{Z}_2$. If $P \cong \mathbb{Z}_4$, we have a unique such homomorphism, which gives us the group
\[
\langle a, b \mid a^3 = b^4 = 1, bab^{-1} = a^2 \rangle \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_4.
\]

If $P \cong V_4$, we have three homomorphisms $V_4 \longrightarrow \mathbb{Z}_2$, but they all are obtained from each other by “changing notation” in (by an automorphism of) $V_4$, and produce groups isomorphic to
\[
\langle a, b, c \mid a^3 = b^2 = c^2 = 1, bc = cb, bab = a^2, cac = a \rangle \cong \mathbb{Z}_3 \rtimes V_4.
\]

Assume that $n_3 \neq 1$; then $n_3 = 4$. Any two Sylow 3-subgroups of $G$ have trivial intersection, so $G$ totally has $4 \times 2 = 8$ elements of order 3. The remaining 4 elements of $G$ may only form one subgroup of order 4, so $n_2 = 1$. Thus, $G = P \rtimes Q$. This product is induced by a nontrivial homomorphism $Q \longrightarrow \text{Aut}(P)$. There is no nontrivial homomorphism $\mathbb{Z}_3 \rightarrow \text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$, but there is such $\mathbb{Z}_3 \rightarrow \text{Aut}(V_4) \cong S_3$, which maps the generator of $\mathbb{Z}_3$ to a cyclic permutation of the elements of $V_4$; the group obtained thereby is
\[
\langle a, b, c \mid a^3 = b^2 = c^3 = 1, ab = ba, cac^{-1} = b, bc^{-1} = ab \rangle \cong V_4 \rtimes \mathbb{Z}_3.
\]

So, up to isomorphism, there are 2 abelian and 3 nonabelian groups of order 12, $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$, $\mathbb{Z}_3 \rtimes V_4$, and $V_4 \rtimes \mathbb{Z}_3$. Now, given a group of order 12, we can easily determine which of these groups it is isomorphic to:

the group $A_4$ has 4 subgroups of order 3, so $A_4 \cong V_4 \rtimes \mathbb{Z}_3$;

the group $D_{12}$ has a single subgroup of order 3 and no elements of order 4, so $D_{12} \cong \mathbb{Z}_3 \rtimes V_4$;

the direct product $S_3 \times \mathbb{Z}_2$ also has a single subgroup of order 3 and no elements of order 4, so $D_{12}$;

the group of rotations of a tetrahedron has 4 subgroups of order 3, so it is isomorphic to $V_4 \rtimes \mathbb{Z}_3 \cong A_4$

(there is, actually, clear since it acts as $A_4$ on the set of vertices of the tetrahedron).

7.3. Groups of small orders

(More exactly, groups whose orders have $\leq 3$ factors.)

7.3.1. If $|G| = p$, then $G \cong \mathbb{Z}_p$.

If $|G| = p^2$, then $G$ is abelian, $G \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_2^p$.

7.3.2. Let $|G| = p^3$. If $G$ is abelian, then $G \cong \mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, or $\mathbb{Z}_p^3$.

Let $G$ be nonabelian, then $Z(G) \neq G$. If $|Z(G)| = p^2$, then $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic, and $G$ is abelian by Lemma 5.3.1. If $|Z(G)| = p$, then $|G/Z(G)| = p^2$, and if $G/Z(G) \cong \mathbb{Z}_{p^2}$, then $G$ is again cyclic.

So, $|Z(G)| = p$, $Z(G) \cong \mathbb{Z}_p$, and $G/Z(G) \cong \mathbb{Z}_p^2$. Also by Lemma 3.2.4, any subgroup of $G$ of order $p^2$ is normal.

Claim. If $p = 2$, then $G \cong D_8$ or $Q_8$.

Proof. It cannot be that $g^2 = 1$ for all $g \in G$ since in this case $G$ is abelian. Let $a \in G$ be such that $|a| = 4$, then $Z(G) = \langle a^2 \rangle$. Let $b \in G \setminus \langle a \rangle$, then $G = \langle a, b \rangle$. $a, b$ don’t commute (since otherwise $G$ is abelian); but $a, b$ commute modulo $Z(G)$, so $ba = ab a^2 = a^3 b$. If $|b| = 2$, we have $G = \langle a, b \mid a^4 = b^2 = 1, ba = a^3 b \rangle \cong D_8$.

If $|b| = 4$, then $b^2 = a^2$, and we have $G = \langle a, b \mid a^4 = 1, a^2 = b^2, ba = a^3 b \rangle \cong Q_8$. $\blacksquare$

Claim. If $p \geq 3$, then $G$ is isomorphic to one of the following two groups:
\[
\langle a, b, c \mid a^p = b^p = c^p = 1, ba = ab, ca = ac, cb = abc \rangle \cong \mathbb{Z}_p^2 \rtimes \mathbb{Z}_p
\]

or
\[
\langle a, b \mid a^{p^2} = b^p = 1, ba = a^{p+1} b \rangle \cong \mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p.
\]

Proof. Assume that $|G| = p$ for all $g \in G$. Let $b, c \in G$ generate $G$ modulo $Z(G)$. $b, c$ don’t commute (since otherwise $G$ is abelian); but $b, c$ commute modulo $Z(G)$, so $cb = bca$ where $a$ is a generator of $Z(G) \cong \mathbb{Z}_p$.

We then have $\langle a, b, c \mid a^p = b^p = c^p = 1, ba = ab, ca = ac, cb = abc \rangle \cong \mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$.

Now assume that there is a $a \in G$ with $|a| = p^2$. Let $c = a^p$, then $c$ is a generator of $Z(G) \cong \mathbb{Z}_p$. Let $b \in G \setminus Z(G)$. Since $a, b$ don’t commute but commute modulo $Z(G)$, we have $ba = abc^r$ for some $r \neq 0 \mod p$.

Assume that $|b| = p^r$, then $b^p \in Z(G)$ so $b^p = a^{ek}$ for some $k$. We then have $(ba^{-k})^p = b^p a^{-k r p^{-1}/2} a^{-k p^{-1}/2} = 1$ since $e^p = 1$; after replacing $b$ by $ba^{-k}$ we have $|b| = p$. Finally, replacing $b$ by $b^s$ where $s$ is the such that $sr = 1 \mod p$, we get $ba = abc$. Hence, $\langle a, b \mid a^{p^2} = b^p = 1, ba = a^{p+1} b \rangle \cong \mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p$. $\blacksquare$

The Heisenberg group $\left\{ \begin{pmatrix} 1 & m & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid m, n, k \in \mathbb{Z}_p \right\}$ over $\mathbb{Z}_p$ is isomorphic to the first of these groups, $\mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$. 

24
Let $G$ be a group of order $pq$ where $p$ and $q$ are prime with $p < q$. If $q \neq 1 \mod p$, then $G \cong \mathbb{Z}_{pq}$.

If $q = 1 \mod p$, then either $G$ is cyclic, $\cong \mathbb{Z}_{pq}$, or $G$ is nonabelian, $\cong \mathbb{Z}_q \rtimes \mathbb{Z}_p$, and has a presentation $\langle a, b \mid a^q = b^p = 1, bab^{-1} = a^k \rangle$ where $k$ is any element of order $p$ in $\mathbb{Z}_q^\ast$; all these groups, corresponding to distinct $k$, are isomorphic. (Indeed, by Lemma 5.3.1, $\mathbb{Z}_{pq}$ is cyclic, so it has a single subgroup of order $p$, and Lemma 6.3.12 applies.)

Let $G$ be a group of order $pq^k$ where $p, q$ are prime with $p < q$ and $k \in \mathbb{N}$. Then $n_q = 1$, so $G \cong Q \rtimes P$ where $|Q| = q^k$ and $P \cong \mathbb{Z}_p$.

Let $G$ be a group of order $p^2q$ where $p, q$ are prime with $p < q$. If $n_q = 1$, then $G \cong Q \rtimes P$ where $Q \cong \mathbb{Z}_q$ and $P \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_q^2$, which semidirect products may only be nontrivial if $p \mid (q-1)$. If $n_q \neq 1$, then $n_q = p^2 = 1 \mod q$, so $q \mid (p-1)(p+1)$, which only holds for $p = 2, q = 3$, so $|G| = 12$, and $G \cong A_4$ by 7.2.6.

By a Burnside theorem, if the order of $G$ has only two prime factors (that is, $|G| = p^kq^l$ where $p, q$ are distinct primes), then $G$ is not simple. It follows, by induction on $|G|$, that $G$ is solvable, made of $k$ copies of the group $\mathbb{Z}_p$ and $l$ copies of the group $\mathbb{Z}_q$.

Let $G$ be a group of order $pqr$ where $p, q, r$ are prime with $p < q < r$.

**Claim.** $n_r = 1$.

**Proof.** If $n_r \neq 1$, then $n_r = pq$ (which is, in fact, only possible if $pq = 1 \mod r$), and the set $B_r = \{a \in G : |a| = r\}$ has cardinality $pq(r-1)$. If $n_q \neq 1$, then $n_q = r$ or $n_q = pr$, and the set $B_q = \{a \in G : |a| = q\}$ has cardinality $\geq r(q-1)$. So, if both $n_r, n_q \neq 1$, we have

$$|B_r| + |B_q| \geq pq(r-1) + r(q-1) = pqr + r(q-1) - qp > pqr = |G|,$$

which is impossible.

If $n_r = 1$, we are done. Assume that $n_q = 1$. Let $R$ be a Sylow $r$-subgroup and $Q$ be the Sylow $q$-subgroup. Since $Q$ is normal, $H = QR$ is a subgroup of $G$; since $|H| = qr$, $R$ is normal in $G$ by 7.3.3. The index $|G : H| = p$ is the minimal prime divisor of $G$, so by Lemma 3.2.4, $H \trianglelefteq G$. Since $R$ char $H$, $R \trianglelefteq G$.

**7.3.8. By a Burnside theorem,** if the order of $G$ is a square-free integer (that is, $|G| = p_1 \cdots p_l$ where $p_i$ are distinct primes), then $G$ is not simple. It follows, by induction on $|G|$, that $G$ is solvable, made of the groups $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_l}$.

The minimal positive integer which is not square-free and has $\geq 3$ prime factors is $60 = 2^2 \cdot 3 \cdot 5$, and indeed, there exists a simple group of this order, namely, $A_5$. It is worth proving that $A_5$ is the only simple group of order 60.

**Claim.** If $G$ is a simple group of order 60, then $G \cong A_5$.

**Proof.** Since $G$ is simple, $n_2 \neq 1$, so $n_2 = 3, 5$ or 15. $G$ acts on the set Syl$_2(G)$ of cardinality $n_2$.

Now assume that $n_2 = 15$; we will use a “counting elements” method to exclude this case. We have $n_5 = 6$ and $n_3 = 10$ (the case $n_3 = 4$ is impossible since there is no nontrivial homomorphism $G \rightarrow S_4$); so, $G$ contains $10 \cdot 2 + 6 \cdot 4 = 44$ elements of order 3 and 5, and only 16 elements of other orders. Let $a$ be an element of order 2 and $b$ is contained in a Sylow 2-subgroup of $G$ of order 4. If $a$ commutes with an element $b$ of order 3, then $(a, b) \cong \mathbb{Z}_6$. Then, since Sylow 3-subgroups are all conjugate, each of 10 Sylow 3-subgroups of $G$ is contained in a cyclic group of order 6, which has 2 elements of order 6; so there are $10 \cdot 2 = 20$ such elements in $G$, which is impossible. Similarly, if $a$ commutes with an element if order 5, then $G$ contains $6 \cdot 4 = 24$ elements of order 10, which is also impossible. Hence, the centralizer $C_G(a)$ of $a$ does not contain elements of order 3 or 5, so, it is a 2-group but the Sylow 2-subgroup $P$ containing 2 is abelian, so $C_G(a) = P$. This implies that every Sylow 2-subgroup of $G$ is uniquely defined by any of its element of order 2, so these subgroups have pairwise trivial intersections, and their union contains 45 elements, which is impossible.

Finally, if $n_2 = 5$, we have an injective homomorphism $\varphi : G \rightarrow S_5$; then $\varphi(G)$ is a subgroup of order 60 and so of index 2 in $S_5$, thus $\varphi(G) = A_5$ and $G \cong A_5$. ■
7.4. Some simple methods of proving that a finite group is not simple

Let \( G \) be a finite group, and let \( p \) be a prime divisor of \( |G| \).

7.4.1. If \( n_p = 1 \), then the Sylow \( p \)-subgroup of \( G \) is normal, and \( G \) is not simple. To show that \( n_p = 1 \), the last part of Sylow’s theorem and counting elements of certain orders in \( G \) sometimes helps.

Examples.

(i) If \( |G| = 3 \cdot 5^2 \cdot 11^3 \), \( n_{11} = 1 \) since none of the integers \( 3, 5, 5^2, 3 \cdot 5, 3 \cdot 5^2 \) equals 1 modulo 11.

(ii) Let \( |G| = 3^4 \cdot 13 \). If \( n_{13} \neq 1 \), then \( n_{13} = 27 \), and \( G \) has \( 3^3 \cdot 12 \) elements of order 13. The remaining \( 3^3 \) elements of \( G \) may form only one Sylow 3-subgroup, so \( n_3 = 1 \).

7.4.2. \( G \) acts on the set \( \text{Syl}_p(G) \) of cardinality \( n_p \) by conjugations, which induces a nontrivial homomorphism \( \varphi : G \rightarrow S_n_p \). If \( G \) is simple, then \( \varphi \) is injective and \( \varphi(G) \leq A_n_p \). But this is impossible if \( |G| \) does not divide \( n_p! / 2 \), or if an element of \( G \) acts as an odd permutation.

Examples.

(i) Let \( |G| = 2^3 \cdot 3^2 \). If \( G \) is simple, then \( n_3 = 4 \), and \( G \) is isomorphic to a subgroup of \( A_4 \), which is impossible since \( |G| > 12 \).

(ii) Let \( |G| = 2^5 \cdot 3 \cdot 11^2 \). If \( G \) is simple, then \( n_{11} = 12 \), and \( G \) is isomorphic to a subgroup of \( A_{12} \); but \( 11^2 \nmid 12 \), so this is impossible.

7.4.3. Let \( P \in \text{Syl}_p(G) \), then \( n_p = |G : N_G(P)| \), so \( |N_G(P)| = |G|/n_p \). Also, \( P \) is a normal subgroup of \( N_G(P) \), which gives some additional information about the structure of \( N_G(P) \). To prove that \( G \) is simple, it suffices to show that \( A_{n_p} \) cannot contain a group of this structure.

Example. Let \( |G| = 2^3 \cdot 3 \cdot 11 \), and assume that \( G \) is simple. Then \( n_{11} = 12 \), and \( |N_G(P)| = |G|/12 = 22 \). Thus, \( N_G(P) \cong \mathbb{Z}_{22} \) or \( D_{22} \). But (it can be shown that) \( A_{12} \) has no subgroups isomorphic to \( \mathbb{Z}_{22} \) or to \( D_{22} \).

7.4.4. It is sometimes possible to show that the normalizer of the intersection of two Sylow \( p \)-subgroups coincides with \( G \), so this intersection is normal in \( G \).

Example. Let \( |G| = 7^3 \cdot 2^2 \cdot 3 \). Let \( P_1, P_2 \in \text{Syl}_7(G) \), and let \( H = P_1 \cap P_2 \); then \( |H| = |P_1| \cdot |P_2| / |P_1 P_2| \leq \frac{|P_1| \cdot |P_2|}{|G|} = \frac{7^3}{(7^3 \cdot 12)} > 7^3 \), so \( |H| = 7^3 \). Since \( H \) has index 7 in \( P_1 \) and \( P_2 \), by Lemma 3.2.4, \( H \leq P_1, P_2 \), so \( P_1, P_2 \leq N_G(H) \), and \( |N_G(H)| \geq |P_1| \cdot |P_2| / |H| = 7^5 > |G|/2 \). So, \( N_G(H) = G \), and \( H \trianglelefteq G \).

8. Commutator calculus, solvable and nilpotent groups

8.1. Commutators and the derived subgroup

Let \( G \) be a group, finite or infinite.

8.1.1. For \( a, b \in G \), the commutator of \( a \) and \( b \) is the element \( [a, b] = aba^{-1}b^{-1} \) of \( G \). (In some books, \([a, b] = a^{-1}b^{-1}ab\).)

We have \( ab = [a, b]ba \) (two elements can be “switched” modulo their commutator). The commutator illuminates “the noncommutativity” between \( a \) and \( b \): \( ab = ba \) iff \([a, b] = 1\).

8.1.2. The commutator is a binary operation on \( G \), \( (a, b) \mapsto [a, b] \). This operation is, however, not associative: \([a, b, c] \neq [a, [b, c]] \) generally speaking. The expression \([a, b, c] \) is denoted by \([a, b, c] \).

8.1.3. For \( a, b \in G \), the conjugate \( bab^{-1} \) of \( a \) by \( b \) is denoted by \( a^b \). (In some books, \( a^b = b^{-1}ab \).) In this notation, commutators satisfy the following equalities:

(i) \( a^b = [b, a]a \);

(ii) \([b, a] = [a, b]^{-1} \) for all \( a, b \in G \);

(iii) \([a^{-1}, b] = [b, a]^{-1} \) for all \( a, b \in G \);

(iv) \([a, b, c] = [b, c]^{-1}[a, c] \) for all \( a, b, c \in G \) (which looks as a sort of “distributive law”);

(v) the Hall-Witt identity: \( [a, b, c][b, c, a][c, a, b] = 1 \) for all \( a, b, c \in G \) (this is what we have instead of associativity).

8.1.4. For two subsets \( A, B \subseteq G \), their commutator \([A, B] \) is defined as the subgroup \( \langle [a, b], \ a \in A , \ b \in B \rangle \) of \( G \). We have \([A, B] = 1 \) iff \( ab = ba \) for all \( a \in A \) and \( b \in B \).
8.1.5. The group $G' = [G, G]$ is called the derived subgroup of $G$. $G'$ is a characteristic subgroup of $G$; it is trivial if $G$ is abelian.

8.1.6. The group $G/G'$ is abelian, and $G'$ is the minimal subgroup of $G$ with this property: If $H \trianglelefteq G$ is such that $G/H$ is abelian, then $H \geq G'$.

8.1.7. If $\varphi : G \to H$ is a group homomorphism, then $\varphi(G') \leq H'$, and if $\varphi$ is surjective, then $\varphi(G') = H'$. If $H$ is a subgroup of $G$, then $H' \leq H \cap G'$; if $K$ is a quotient group of $G$ and $\pi$ is the factorization mapping, then $K' = \pi(G')$.

8.2. Derived series and solvable groups

8.2.1. For a group $G$ we define $G^{(1)} = G'$, $G^{(n)} = (G^{(n)})'$, and $G^{(i+1)} = (G^{(i)})'$ for all $i$. For every $i$, the $i$-th derived subgroup $G^{(i)}$ is characteristic in $G$. The series $\ldots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$ is called the derived series of $G$.

The derived series may degenerate after finitely many steps: $G^{(n)} = 1$ for some $n$; may stabilize after finitely many steps: $G^{(n+1)} = G^{(n)} \neq 1$ for some $n$; and (in the case $|G| = \infty$) may be infinitely decreasing.

8.2.2. A group $G$ is said to be solvable if it has a finite subnormal series $1 = H_n \trianglelefteq H_{n-1} \trianglelefteq \ldots \trianglelefteq H_1 \trianglelefteq H_0 = G$ with abelian factors ($H_i/H_{i+1}$ are abelian groups for all $i$).

8.2.3. If a subnormal series $\ldots \trianglelefteq H_2 \trianglelefteq H_1 \trianglelefteq H_0 = G$ has abelian factors, then for all $i$, $H_i \geq G^{(i)}$. We therefore have:

Theorem. A group is solvable iff its derived series degenerates.

8.2.4. A subnormal series of a group $G$ whose all members are normal subgroups of $G$ is called a normal series. It follows that if a group is solvable, then it has a finite normal series with abelian factors.

8.2.5. If $G$ is a solvable group, the minimal $n$ for which $G^{(n)} = 1$ is called the solvability degree or the solvability class of $G$, and $G$ is said to be $n$-step solvable.

8.2.6. Examples.

(i) 1-step solvable groups are the abelian groups.

(ii) A group $G$ is 2-step solvable iff it has an abelian normal subgroup $H$ such that $G/H$ is also abelian. In particular, any semidirect product of two abelian groups is 2-step solvable.

(iii) The groups $S_3$, $Q_8$ and $D_{2n}$ for all $n$ are 2-step solvable. The group $S_4$ is 3-step solvable. $S_n$ for $n \geq 5$ are not solvable.

(iv) For any field $F$ and $n \in \mathbb{N}$, the subgroup of GL$_n(F)$ of upper-triangular matrices (which have all 0s below the main diagonal) is solvable.

8.2.7. If a group $G$ is solvable, then any subgroup and any quotient group of $G$ are also solvable. Conversely, if a group $G$ has a normal subgroup $H$ such that both $H$ and $G/H$ are solvable, then $G$ itself is solvable.

8.3. Central series and nilpotent groups

8.3.1. A normal series $\ldots \trianglelefteq H_i \trianglelefteq H_{i+1} \trianglelefteq \ldots$ of subgroups of a group $G$ is said to be central if for every $i$, $H_i/H_{i+1} \leq Z(G/H_{i+1})$.

8.3.2. A group $G$ is said to be nilpotent if it possesses a finite central series. The minimal length $n$ of such a series is called the nilpotency degree or the nilpotency class of $G$, and $G$ is said to be $n$-step nilpotent.

8.3.3. Abelian groups are nilpotent of degree 1. For any $n$, $n$-step nilpotent groups are $n$-step solvable, but not vice versa:

cyclic groups $\subset$ abelian groups $\subset$ nilpotent groups $\subset$ solvable groups.

8.3.4. Let $G$ be a group; for any subgroup $M$ of any quotient group of $G$ let us denote by $\hat{M}$ the preimage of $M$ in $G$. The upper central series of $G$ is the central series $1 = Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \ldots$ where $Z_i = Z(G/Z_{i-1})$.

8.3.5. The lower central series of a group $G$ is the central series $\ldots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G$ where $G_1 = G' = [G, G]$, $G_2 = [G, G_1]$, and $G_{i+1} = [G, G_i]$ for all $i$. The members $G_i$ of the lower central series of $G$ are characteristic subgroups of $G$.

8.3.6. Lemma. Let $G$ be a group.
(i) For any central series \( 1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \) of \( G \) we have \( H_i \leq Z_i \) (where \( Z_i \) is the \( i \)-th term of the upper central series of \( G \)).

(ii) For any central series \( \cdots \trianglelefteq K_3 \trianglelefteq K_2 \trianglelefteq K_1 = G \) of \( G \) we have \( K_i \geq G_i \) (where \( G_i \) is the \( i \)-th term of the lower central series of \( G \)).

8.3.7. As a corollary of Lemma 8.3.6 we get that a group \( G \) is nilpotent iff its upper central series is finite \( (Z_n = G \) for some \( n \)), and iff its lower central series is finite \( (G_n = 1 \) for some \( n \)), in which case \( n \) is the nilpotency class of \( G \).

8.3.8. Examples.

(i) 1-step nilpotent groups are abelian groups. A group \( G \) is 2-step nilpotent iff \( G \) is nonabelian but \( G/Z(G) \) is abelian.

(ii) The groups \( Q_8 \) and \( D_8 \) are 2-step nilpotent. The group \( S_3 \) is not nilpotent.

(iii) For any prime \( p \), any \( p \)-group is nilpotent.

(iv) The group \( D_{2n} \) is nilpotent iff \( n = 2^k \) for some \( k \); the group \( D_{2k+1} \) is \( k \)-step nilpotent.

(v) For any field \( F \) and \( n \in \mathbb{N} \), the subgroup of \( GL_n(F) \) of \( n \times n \) strictly upper-triangular matrices (which have all 1s on the main diagonal and all 0s below the main diagonal) is \((n-1)\)-step nilpotent. In particular, the Heisenberg group \( \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \ a, b, c \in F \} \) is 2-step nilpotent.

8.3.9. Any subgroup and any quotient group of a nilpotent group are nilpotent. The converse is not true; the maximum we can say is that the direct product of nilpotent groups is nilpotent.

8.3.10. For finite groups there is a simple criterion of nilpotency:

**Theorem.** A finite group \( G \) is nilpotent iff it is a direct product of its Sylow subgroups (which means that all Sylow subgroups of \( G \) are normal).

---

9. Some facts about free groups