November 1, 2023

Groups

Table of Contents

---

1. Definitions, examples, and basic properties

1.1. Semigroups, monoids, and groups

1.1.1. Let G be a set. *A binary operation* on G is a mapping $*: G \times G \longrightarrow G$. The result of the application of the operation to elements $a, b \in G$ 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 G is said to be *associative* if $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$. A binary operation $*$ on a set G is said to be *commutative* if $a * b = a * b$ for all $a, b \in G$.

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. In an associative semigroup, when the binary operation is applied sequentially to a sequence of elements, it doesn't matter in which order this is performed: $((a*b)*c)*d = (a*b)*(c*d) = a*((b*c)*d) = \ldots$ (This fact is hard to state rigorously but easy to prove by a sort of induction.) Thus, parentheses can be, and usually are, dropped in such expressions: $a * b * c * d$. (If the semigroup is non-commutative, the order of elements in the expression however matters.)

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

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.*

Proof. Let l be a left neutral element and r be a right neutral element of G. Then $l * r = r$ (since l is left neutral) and $l * r = l$ (since r is right neutral), so $l = r$. It now follows that every left neutral element of G is equal to r (and so to l), and every right neutral element of G is equal to l (and so to r). ■

A semigroup with a neutral element is called *a monoid*.

1.1.5. Let $(G, *)$ be a monoid, with a neutral element e. Let $a \in G$; an element $b \in G$ 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 $b * a = a * b = e$. An element that has an inverse is said to be *invertible*.

Lemma. *If an element a of a monoid has both a left and a right inverses, then these inverses are unique and equal. In particular, if a is invertible, its inverse is unique.*

Proof. Let b be a left inverse and c is a right inverse of a, $ba = ac = e$. Then $b = b * e = b * (a * c) = (b * a) * c = e * c = c$. It now follows that every left inverse of a is equal to c (and so to b), and every right inverse of a is equal to b (and so to c). ■

1.1.6. A monoid in which every element is invertible is called *a group*. (That is, a group is a set with an associative binary operation, a neutral element, and in which every element is invertible.)

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, $((a_1a_2)a_3)a_4 = a_1((a_2a_3)a_4) = a_1(a_2(a_3a_4))$ is written as $a_1a_2a_3a_4$.)

1.1.7. Commutative groups are 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*, and the inverse of an element a is denoted by $-a$.

1.1.8. Lemma. *For any monoid G, the set G^* of invertible elements of G is a group.*

Proof. Since $e \in G^*$ (we have $e^{-1} = e$) and every element of G^* is invertible, it is only to check that the operation of multiplication is defined on G^* and for every $a \in G^*$ one has $a^{-1} \in G^*$ as well. (In other words, that G^* is closed under multiplication and taking inverses.) And indeed, if $a, b \in G^*$, then $b^{-1} * a^{-1}$ is the inverse of $a * b$: $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e$ and $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$, so $a * b \in G^*$. And if $a \in G^*$, then a^{-1} is also invertible with a being its inverse: $a * a^{-1} = a^{-1} * a = e$, so $a^{-1} \in G^*$. ■

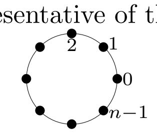
1.1.9. The number of elements in a group G is called *the order* of G and is denoted by $|G|$.

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) Let $n \in \mathbb{N}$. $\mathbb{Z}_n$ is the set $\{0, 1, \ldots, n-1\}$ of residues modulo $n \in \mathbb{N}$. More exactly, $\mathbb{Z}_n$ is the set of classes of equivalence of integers, where $m_1 \sim m_2$ if $m_1 = m_2 \bmod n$; $0, 1, \ldots, n-1$ are just representative of these classes. The operation in $\mathbb{Z}_n$ is addition modulo n: the sum of two residues is the residue of their sum. Under this operation, $\mathbb{Z}_n$ is a group of order n. It is covenient to imagine $\mathbb{Z}_n$ as a discrete circle, where $(n-1) + 1 = 0$.



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

1.2.2. Vectors and matrices

(i) Any vector space, over any field, is an abelian group under addition.

(ii) Let X be a set and G be a group; then the set of functions $f\colon X \longrightarrow G$ is also a group under the operation $(fg)(x) = f(x)g(x)$, $x \in X$.

(iii) Let G be a group, let $n, m \in \mathbb{N}$; the set of $n \times m$-matrices with entries from G is a group under addition.

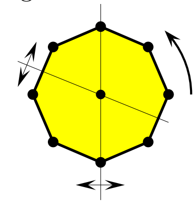
(iv) Let R be any of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_m$ for some m (actually, any *unital ring* – a set with two operations, addition and multiplication, satisfying certain properties), and let $n \in \mathbb{N}$. The set $M_{n,n}(R)$ of $n \times n$-matrices with entries in R under the operation of matrix multiplication is a monoid; the set $\mathrm{GL}_n(R) = M_{n,n}^*(F)$ of invertible $n \times n$-matrices is a (usually nonabelian) group.

1.2.3. Transformations (mappings)

(i) Given a set X, let $\mathcal{F}(X)$ be the set of mappings $X \longrightarrow X$. The operation of composition turns $\mathcal{F}(X)$ 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 $\mathcal{F}(X)$. We will assume the first definition.) The invertible elements of $\mathcal{F}(X)$, 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, usually called *the group of transformations* of X. Such are the group of self-homeomorphisms of a topological space, the group of invertible isometries of a metric space, the *General Linear* group $\mathrm{GL}(V)$ of invertible linear transformations of a vector space V, the *Special Linear* group $\mathrm{SL}(V)$ of linear transformations of a finite dimensional vector space V with determinant 1, the *Orthogonal* group $O(V)$ of linear transformations of a vector space V preserving an inner product on V, the group of Möbius (linear fractional) transformations of the Riemann sphere or of the unit disc, etc.

(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.

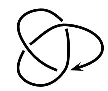


In the case R is a regular n-gon in the plane (with $n \geq 3$), the symmetry group of R is called *the n-th dihedral group* and is denoted by D_{2n} (or D_n, in most books). D_{2n} contains $2n$ elements: n rotations (including the trivial one) and n reflections. D_{2n} permutes the vertices of R and can be viewed as "a subgroup" of S_n.

1.2.4. Set-theoretical groups

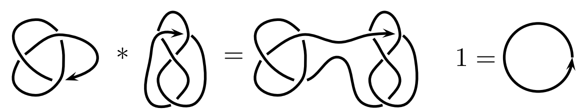
Let X be a set; under the operation $\triangle$ of symmetric difference, $A \triangle B = (A \setminus B) \cup (B \setminus A)$, the power set $\mathcal{P}(X)$ is a group. In this group, $\emptyset$ is the identity, and $A^2 = 1 (= \emptyset)$, so $A^{-1} = A$, for all $A \in \mathcal{P}(X)$. (A group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

1.2.5. Groups, appearing in topology

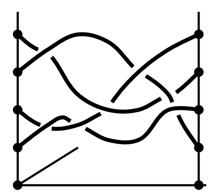


(i) *A knot* is a simple loop in $\mathbb{R}^3$ (that is, a continuous injective mapping $C \longrightarrow \mathbb{R}^3$, where C is a circle) up to *homotopy*: two loops are assumed to represent the same knot if one can be continuously transformed into the other without self-intersections.

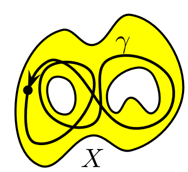
The operation on knots is concatenation; under this operation, the set of knots is a commutative monoid, with the neutral element being "the trivial" knot (a circle). However, it can be shown that no non-trivial knot has an inverse in this monoid.



(ii) *A braid of n strands*, or *an n-braid*, is a collection $\{f_1, \ldots, f_n\}$ of n continuous mappings $[0,1] \longrightarrow \mathbb{R}^2$ with $\{f_1(0), \ldots, f_n(0)\} = \{f_1(1), \ldots, f_n(1)\} = \{(1,0), \ldots, (n,0)\}$, and $f_i(t) \neq f_j(t)$ for all $t \in [0,1]$ and all $i \neq j$, up to homotopy. (That is, two such collections of functions define the same braid if one can be transformed to the other continuously in the space of such collections.) The operation on n-braids is concatenation; under this operation the n-braids form a group, denoted by B_n. (The neutral braid is the collection of constant functions, and the inverse of a braid is its mirror reflection.)



(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 $\gamma \colon [0,1] \longrightarrow X$ 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 and free groups

(i) Given an alphabet (that is, just a set) A, the finte 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 cancelations: any occurences of subwords of the form aa^{-1} or $a^{-1}a$, where $a \in A$, can be deleted. (For example, the word $a_1a_2a_3a_1^{-1}a_1a_3^{-1}a_1$ 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, let's allow replacement of certain subwords by other words; we will then get a group with *relations*. (For example, given the relation $a_1a_2a_1^{-1} = a_2a_3$, we have $a_3a_1a_2a_1 = a_3a_1a_2a_1^{-1}a_1a_1 = a_3a_2a_3a_1a_1$.)

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

1.2.7. Groups, defined by multiplication tables

Given a set G, a group structure on G can be introduced by *a multiplication table*, explcitly 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:

	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

1.3. The cancellation property

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 $b_1 a = b_2 a$, then $b_1 = b_2$.*

Proof. If $ab_1 = ab_2$ then $a^{-1}ab_1 = a^{-1}ab_2$, so $1b_1 = 1b_2$, so $b_1 = b_2$. ■

The cancellation property says that for any $a \in G$, the operations of the left multiplication by a, $x \mapsto ax$, and of the right multiplication by a, $x \mapsto xa$, are injective mappings $G \longrightarrow G$.

1.4. Inverses, powers, and the order of elements

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

Proof. Since $aa^{-1} = 1$, a is the inverse of a^{-1}.

For $a, b \in G$, $(b^{-1}a^{-1})(ab) = b^{-1}1b = b^{-1}b = 1$. By induction on n, $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ for any $a_1, \ldots, a_n \in G$. ■

1.4.2. Let G be a group and let $a \in G$. For any $n \in \mathbb{N}$, we define $a^n = \underbrace{a \cdots a}_{n}$, $a^0 = 1$, $a^{-n} = (a^n)^{-1} = (a^{-1})^n$. Then for any $n, m \in \mathbb{Z}$, $a^{n+m} = a^n a^m$ and $(a^n)^m = a^{nm}$. (This should be proved by induction.)

In additive notation, we write na for $\underbrace{a + \cdots + a}_{n}$ and define $0a = 0$, $(-n)a = -(na)$ for $n \in \mathbb{N}$.

1.4.3. 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: indeed, if $a^n = a^m$ for $n > m$, then $a^{n-m} = 1$. If $|a| = n$, then the sequence $\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots$ is periodic with period n: $\ldots, 1, a, a^2, \ldots, a^{n-1}, 1, a, a^2, \ldots, a^{n-1}, 1, \ldots$

1.5. Isomorphic groups

1.5.1. Two groups (more generally, two sets with a binary operation) G_1 and G_2 are said to be *isomorphic* if there is a bijection $\varphi: G_1 \longrightarrow G_2$ such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G_1$; such a bijection φ is called *an isomorphism*. If G_1 and G_2 are isomorphic, we write $G_1 \cong G_2$.

If G_1 and G_2 are isomorphic groups, with $\varphi: G_1 \longrightarrow G_2$ being the isomorphism, then the multiplication table of G_2 is the same as the multiplication table of G_1 where every element a of G_1 is replaced by the corresponding element $\varphi(a)$ of G_2. We often identify isomorphic groups, considering them to be "the same group" only written in different terms.

1.5.2. Examples. (i) If A and B are two sets of the same cardinality, then the free groups F_A and F_B are isomorphic. Indeed, choose any bijection $A \longrightarrow B$. Given a word in alphabet $A \cup A^{-1}$, replace every "letter" in this word by the corresponding element from $B \cup B^{-1}$; this defines a bijective mapping $F_A \longrightarrow F_B$, under which the product of any two words from F_A goes to the product of their images in F_B. Hence, $F_A \cong F_B$.

In particular, the free groups over any alphabets of cardinality n are all isomorphic; they are denoted by F_n.

(ii) Similarly, the groups S_A of permutations of n-element sets are all isomorphic to the symmetric group S_n.

(iii) The group $\mathrm{GL}_n(F)$ of invertible $n \times n$-matrices over a field F under multiplication is isomorphic to the group $\mathrm{GL}(V)$ of invertible linear transformations of an n-dimensional F-vector space V. Indeed, if a basis in V is chosen, then every invertible linear transformation of V is represented by a non-degenerate (invertible) matrix in this basis, thus we have a one-to-one correspondence between such transformations and invertible $n \times n$-matrices, so that the composition of two transformations corresponds to the product of the corresponding matrices. (The matrix multiplication is defined this way.) Thus, $\mathrm{GL}(V) \cong \mathrm{GL}_n(F)$, and the group $\mathrm{GL}(V)$ is often identified with the group $\mathrm{GL}_n(F)$, and the latter is denoted by $\mathrm{GL}_n(F)$.

1.5.3. 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 $\mathbb{Z}$: the isomorphism is given by $a^n \leftrightarrow n$, $n \in \mathbb{Z}$. (Indeed, this is a bijection, and $a^n a^m = a^{n+m}$ for all n, m.) If $|a| = n$, then this group is isomorphic to $\mathbb{Z}_n$.

1.5.4. For every $n \in \mathbb{N}$ there are only finitely many different $n \times n$ tables over an n-element alphabet, so only finitely many possible multiplication tables for a group of order n, so only finitely many non-isomorphic groups of order n. Here is the list of all, up to isomorphism, groups of orders 1, 2, 3, 4, 6:

(i) There is only one (up to isomorphism) group of order 1, $G = \{1\}$, with the multiplication table $1^2 = 1$.

(ii) There is only one (up to isomorphism) group of order 2, $G = \{1, a\}$, with the multiplication table $1^2 = 1$, $1a = a1 = a$, $a^2 = 1$ (so that $a^{-1} = a$). This group is isomorphic to $\mathbb{Z}_2$.

(iii) Let $|G| = 3$, $G = \{1, a, b\}$. If $a^{-1} = a$, then $b^{-1} = b$, so $a^2 = b^2 = 1$, so ab cannot be defined (it cannot be equal to 1, a, or b). Thus, $a^{-1} = b$, so $ab = 1$. Then $a^2 \neq 1, a$, so $a^2 = b$. Hence, up to isomorphism, there is only one group of order 3, $G = \{1, a, a^2\}$, with $a^3 = 1$. This group is isomorphic to $\mathbb{Z}_3$.

(iv) Let $|G| = 4$, $G = \{1, a, b, c\}$. At least one of a, b, c is the inverse of itself; w.l.o.g. let $a^{-1} = a$, so $a^2 = 1$. Now we have two cases: $b^{-1} = c$ or $b^{-1} = b$.

If $b^{-1} = c$, then $bc = cb = 1$, then $ab = ba \neq 1, a, b$, so $ab = ba = c$. Then $b^2 \neq 1, b, c$, so $b^2 = a$, so $b^3 = ab = c$ and $b^4 = bc = 1$, so $G = \{1.b.b^2, b^3\}$ with $b^4 = 1$.

Let $b^{-1} = b$, then $b^2 = 1$, then also $c^{-1} = c$ so $c^2 = 1$. Then $ab \neq 1, a, b$, so $ab = ba = c$, and similarly $ac = ca = b$ and $bc = cb = a$.

Thus, there are only two nonisomorphic groups of order 4, both abelian: $\{1, b, b^2, b^3\} \cong \mathbb{Z}_4$ and $V_4 = \{1, a, b, c\}$ with $a^2 = b^2 = c^2 = 1$, $ab = ba = c$, $ac = ca = b$, $bc = cb = a$, called *Klein's 4-group*.

(vi) Now let $|G| = 6$, $G = \{1, a, b, c, p, q\}$. At least one of a, b, c, p, q is the inverse of itself; w.l.o.g. let $a^{-1} = a$, so that $a^2 = 1$. W.l.o.g. let $ab = c$, then $ac = a^2 b = b$, then $ap = q$ and $aq = p$. That is, the left multiplication by a (which is a self-bijection of G) acts as follows: $1 \leftrightarrow a$, $b \leftrightarrow c$, $p \leftrightarrow q$. We have two cases:

Case 1. The right multiplication by a is the same as the left multiplication: $ba = c$, $ca = b$, $pa = q$, $qa = p$. (That is, all elements of G commute with a.) $b^2 \neq b, c$, so $b^2 = 1$, a, p, or q.
If $b^2 = 1$, then $cb = ab^2 = a$, so $pb = q = pa$, contradiction.
If $b^2 = a$ then $c = ab = b^3$, so $cb = b^4 = 1$, so $pb = q = pa$, contradiction.
Hence, $b^2 = p$ or q; w.l.o.g. let $b^2 = p$. Then $b^3 = pb \neq p, b, c$ (since $c = ab$), so $b^3 = 1$ or a.
If $b^3 = a$, then the powers of b are 1, b, $b^2 = p$, $b^3 = a$, $b^4 = ab = c$, $b^5 = ap = q$, $b^6 = a^2 = 1$, so $G = \{1, b, b^2, b^3, b^4, b^5\}$ and is isomorphic to $\mathbb{Z}_6$.
If $b^3 = 1$, then $c^2 = (ab)^2 = a^2 b^2 = p$ (since a and b commute) and $c^3 = (ab)^3 = a^3 b^3 = a$; after switching b and c we again get that $G \cong \mathbb{Z}_6$.

Case 2. Now assume that $ba \neq c$; w.l.o.g. $ba = p$, so that the right multiplication by a acts this way: $1 \leftrightarrow a$, $b \leftrightarrow p$, $c \leftrightarrow q$, that is, $pa = b$, $ca = q$, $qa = c$. Then all elements of G are expressible in terms of a and b: these are 1, a, b, $c = ab$, $p = ba$, $q = ap = aba$. (We say that G *is generated* by a and b.) Since $b^2 \neq b, c, p$, we have $b^2 = 1$, a, or p.
Let $b^2 = 1$. Then $bp = b^2 a = a$, so $bc \neq 1, b, c, p, a$, so $bc = q$, that is, $bab = aba$. We can now obtain the complete multiplication table of G: $c^2 = abab = bab^2 = ba = p$, $q^2 = abaaba = abba = a^2 = 1$, $cp = abba = 1$, $bq = baba = abaa = ab = c$, $pq = baaba = a$, etc. (This doesn't prove that such G exists! We need to check that the multiplication we've constructed is associative.)
If $b^2 = a$, then b and a commute, $ba = ab = c$, not p, contradiction.
Finally, if $b^2 = q$, then $c^2 = abab = qb = b^3 \neq b, q, p, c$, so $c^2 = 1$ or a. If $c^2 = a$, then $ca = ac = b \neq q$; hence, $c^2 = 1$. Switching b and c (as well as p and q), we obtain the same (or rather isomorphic) group as above.

Thus, there are at most two nonisomorphic groups of order 6: $\mathbb{Z}_6$ and, perhaps, a nonabelian group $\{1, a, b, ab, ba, aba\}$ with $a^2 = b^2 = 1$ and $aba = bab$. But we know that a nonabelian group of order 6 does exist, namely, S_3 (and $D_6 \cong S_3$).

1.6. Subgroups

1.6.1. 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 $H \leq G$.

1.6.2. 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 replaced by a single one: for any $a, b \in H$, $a^{-1}b \in H$ (in short: $H^{-1}H \subseteq H$).

1.6.3. For any group G, the singleton $1 = \{1\}$ 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*.)

1.6.4. Examples. (i) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ (all groups under addition).

(ii) $\mathbb{R}^*$ (under multiplication) is not a subgroup of $\mathbb{R}$ (under addition).

(iii) For any element a of a group G, the set $\{a^n : n \in \mathbb{Z}\}$ of powers of a is a subgroup of G. called *the subgroup generated by a*.

(iv) For any n and any field F, $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$.

(v) For any n, $D_{2n} \leq S_n$. More exactly, D_{2n} is isomorphic to a subgroup of S_n, consisting of permutations of the vertices of a right n-gon R_n which correspond to symmetries of R_n.

1.6.5. Lemma. *The intersection of any collection of subgroups of a group G is a subgroup of G.*

Proof. Let H_α, $\alpha \in \Lambda$, be a collection of subgroups of G and let $H = \bigcap_{\alpha \in \Lambda} H_\alpha$. Now, if $a, b \in H$, then $a, b \in H_\alpha$ for all α, then $a^{-1}b \in H_\alpha$ for all α, so $a^{-1}b \in H$. ■

1.7. Generating sets and relations

1.7.1. Let G be a group and S be a subset of G. *The subgroup of G generated by S* is the minimal subgroup of G that contains S; this is the intersection of all subgroups of G containing S. This subgroup is denoted by $\langle S \rangle$; if S is a finite or a countable set, $S = \{s_1, \ldots, s_n\}$ or $S = \{s_1, s_2, \ldots\}$, this subgroup is also denoted by $\langle s_1, \ldots, s_n \rangle$ or, respectfully, $\langle s_1, s_2, \ldots \rangle$.

For $S \subseteq G$, the group $\langle S \rangle$ consists of all "words over $S \cup S^{-1}$": the products $s_1 \cdots s_k$ where for each i, $s_i \in S$ or $s_i \in S^{-1}$ (that is, $s_i^{-1} \in S$).

1.7.2. If H and K are two subgroups of a group G, then the group generated by $H \cup K$ is called *the join* of H and K and is denoted by $\langle H, K \rangle$; this is the minimal subgroup of G that contains both H and K.

1.7.3. If $S \subseteq G$ is such that $G = \langle S \rangle$, we say that S *is a generating set of* G, or that S *generates* G. If $G = \langle S \rangle$, then G consists of all words over the alphabet $S \cup S^{-1}$ (but some distinct words may be equal in G). (If no better choice can be seen, as a set of generators one can take all elements of G.)

1.7.4. Examples. (i) $\mathbb{Z} = \langle 1 \rangle$ (where "1" is 1, not the identity of the group $\mathbb{Z}$ (which is 0)!).

(ii) $\mathbb{Z}_n = \langle 1 \rangle$.

(iii) $V_4 = \langle a, b \rangle$ (where V_4 is Klein's 4-group $\{1, a, b, c\}$.)

(iv) For any $n \geq 3$, the dihedral group (the symmetry group of a regular n-gon R_n) D_{2n} is generated by the rotation r by the angle of $2\pi/n$ about the center of R_n and a reflection s with respect to a line passing through the center and one of the vertices of R_n.

(v) For any n, the orthogonal group $O(\mathbb{R}^n)$ is generated by rotations about the coordinate axes of $\mathbb{R}^n$ and a single reflection with respect to a hyperplane.

1.7.5. Let G be generated by a subsets S, $G = \langle S \rangle$. Then every element of G is presented by some words in the alphabet $S \cup S^{-1}$, but distinct words may present the same element: $w_1 \neq w_2$ as words, but $w_1 = w_2$ as elements of G. In this case we call the identity $w_1 = w_2$ *a relation* of G. (For example, if a and b commute in G, then $ab = ba$ is a relation in G.) Clearly, as a set and a group, G is defined by the set of its generators and relations (since the multiplication table in G is a subset of the set of relations). Thus, any group can be seen as a free group (the group of words) with relations.

Let R be a set of relations in G such that all other relations of G can be deduced from the relations from R; let's call R *a complete* set of relations. (If no better choice can be found, as a set of generators one can take all elements of G, and as a set of relations – the complete multiplication table of G.) Then, as a group, G is uniquely defined by S and R; we write $G = \langle S \,|\, R\rangle$ and call it *a presentation of* G. (A more professional definition of $\langle S \,|\, R\rangle$ will be given in 2.2.8.)

1.7.6. Examples. (i) $\mathbb{Z} = \langle 1\rangle$.

(ii) $\mathbb{Z}_n = \langle 1 \,|\, n = 0\rangle$.

(iii) $V_4 = \big\langle a, b \,|\, a^2 = b^2 = 1,\ ab = ba\big\rangle$.

(iv) The free abelian group in two generators is defined as $\langle a, b \,|\, ab = ba\rangle$. (It is easy to see that it is isomorphic to $\mathbb{Z}^2$.) The free abelian group generated by a set S is $\big\langle S \,|\, ab = ba,\ a, b \in S\big\rangle$.

(v) For any $n \geq 3$,

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

1.7.7. Let $G = \langle S \,|\, R\rangle$ be a presentation of a group G. To check that a set $P \subseteq G$ generates G it suffices to check that every element of S can be expressed in terms of elements of P, that is, that $S \leq \langle P\rangle$. Further, if Q is a set of relations in G, then the relation from Q can be deduced from relations from R; if also all relations of R can be deduced from the relations from Q, then Q is a complete set of relations, so that $G = \langle P \,|\, Q\rangle$ is another presentation of G.

1.7.8. If a group G has a finite generating set, G is said to be *finitely generated*; if G has a presentation $\langle S \,|\, R\rangle$ with both S and R being finite, we say that G is *finitely presented*.

1.7.9. Given a group G and a set of generators S of G, *the Cayley graph* $\Gamma(G)$ of G is constructed in the following way: the vertices of $\Gamma(G)$ are the elements of G, and two vertices $a, b \in G$ are connected by an edge if $b = as$ for some $s \in S$. The graph $\Gamma(G)$ is directed and colored: the edge above is directed from a to b and is marked by "s". $\Gamma(G)$ is symmetric: G acts transitively on $\Gamma(G)$ (see Section 4 below). The loops (that is, the closed paths) in $\Gamma(G)$ that start at 1 correspond to the relations in G in the alphabet S.

1.8. Finite groups of matrices

1.8.1. *A field* is a set F with two binary operations, $\cdot$ and $+$, such that F is an abelian group with respect to $+$, $F \setminus \{0\}$ is an abelian group with respect to $\cdot$, and the distributive law holds: $a(b + c) = ab + ac$ for all $a, b, c \in F$. (We will study fields later.)

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 $\mathbb{F}_p$.

1.8.2. Let F be a finite field of q elements. Then for any $n \in \mathbb{N}$, the group $\mathrm{GL}_n(F)$ 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 nonabelian.

1.9. Cyclic groups and their subgroups

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

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

1.9.3. Lemma. *Every subgroup of a cyclic group is cyclic.*

1.9.4. In more details, every nonzero subgroup H of $\mathbb{Z}$ is infinite cyclic, and has form $\langle d\rangle = d\mathbb{Z} = \{\ldots, -d, 0, d, 2d, \ldots\}$ for some $d \in \mathbb{N}$, where d is the minimal positive element of H. The subgroup of $\mathbb{Z}$ generated by elements $m_1, \ldots, m_k$ is the group $\langle d\rangle$ where $d = \gcd(m_1, \ldots, m_k)$.

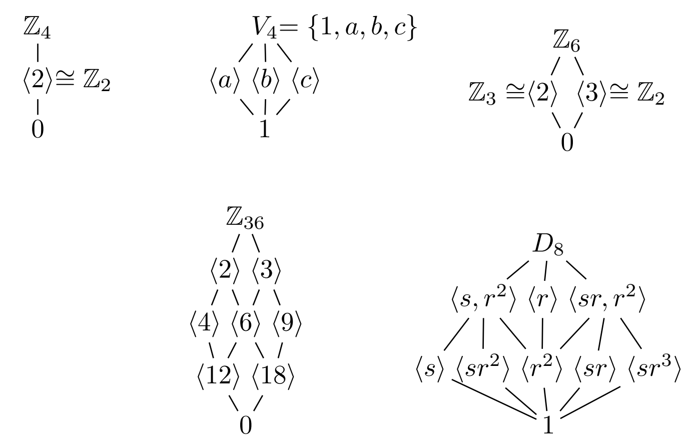
1.9.5. Every nontzero subgroup H of $\mathbb{Z}_n$ is generated by an element d dividing n, $H = \langle d\rangle = d\mathbb{Z}_n = \big\{0, d, 2d, \ldots, \big(\frac{n}{d} - 1\big)d\big\}$, and has order $|H| = n/d$ (so, $\cong \mathbb{Z}_{n/d}$); d is the minimal positive integer such that $d \bmod n \in H$. The subgroup $\langle a_1, \ldots, a_k\rangle$ of $\mathbb{Z}_n$ is the subgroup $\langle d\rangle$ 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.

1.10. The lattice (the diagram) of subgroups of a group

1.10.1. For a group G, *the lattice of subgroups of* G is a diagram (an oriented 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 are 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 $\mathbb{Z}_3^2$ 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:



1.11. Direct products of groups

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

1.11.2. $G_1 \times G_2$ is abelian iff both G_1 and G_2 are abelian.

1.11.3. For any groups G_1 and G_2, $G_1 \times G_2 \cong G_2 \times G_1$. For any groups G_1, G_2, and G_3, $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$.

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

1.11.5. For a group G and $n \in \mathbb{N}$, *the n-th power* G^n of G is the group $\underbrace{G \times \cdots \times G}_{n}$.

1.11.6. Examples. (i) $\mathbb{Z}^2$ is the lattice $\{(n, m) : n, m \in \mathbb{Z}\}$ in $\mathbb{R}^2$.
(ii) $\mathbb{Z}_2^2 \cong V_4$.
(iii) $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ (the element $(1, 1)$ generates $\mathbb{Z}_2 \times \mathbb{Z}_3$).

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 written as a table $\left(\begin{smallmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{smallmatrix}\right)$ where for each j, $i_j = \sigma(j)$.

In this table, the first row is, of course, redundant. But actually, a permutation $\sigma \in S_n$ can be coded by a sequence $[i_1, \ldots, i_n]$ in two ways: either as above, meaning that for every j, $i_j = \sigma(j)$; or as the result of the permutation of $1, \ldots, n$, that is, for every j, i_j is the integer that arrives at the j-th position, $i_j = \sigma^{-1}(j)$. To avoid confusion, I won't use this notation.

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 $|\sigma_1 \sigma_2| = \mathrm{lcm}\big(|\sigma_1|, |\sigma_2|\big)$.

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, $i_1 \leftrightarrow i_2$, 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. The following theorem is easy to believe; we will have it later as a special case of 4.2.6 below:

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

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

1.12.6. Example. For $\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6&7&8\\3&5&4&1&2&8&7&6\end{smallmatrix}\right)$, $\sigma = (1,3,4)(2,5)(6,8)$, and its cycle type is $2, 2, 3$.

1.12.7. It is easy to check that:

Lemma. (i) *For any k and distinct $i_1, \ldots, i_k$ we have $(i_1, \ldots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$.*
(ii) *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. It now follows that:

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

1.12.9. For a transposition $\sigma \in S_n$, *the sign* of σ is defined as $\operatorname{sign}(\sigma) = \operatorname{sign}\prod_{1 \le i < j \le n}(\sigma(j) - \sigma(i))$; this is $(-1)^r$ where r is the number of pairs of elements of $\{1, \ldots, n\}$ whose order is switched by σ. (We assume that 1 stands for $+$ and -1 for $-$.)

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

Proof. In the product $\prod_{1 \le l < j \le n}(\sigma(j) - \sigma(l))$, τ_i only switches the sign of a single factor $(\sigma(j) - \sigma(l))$, – with $\sigma(j) = i$, $\sigma(l) = i+1$, or vice versa. The second statement follows from the first one. ■

1.12.11. It immediately implies that sign is a "multiplicaive" function:

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

1.12.12. For any transposition τ, $\operatorname{sign}(\tau) = -1$. If σ is a product of k transpositions, then $\operatorname{sign}(\sigma) = (-1)^k$. If σ is a k-cycle, then $\operatorname{sign}(\sigma) = (-1)^{k-1}$. For a general $\sigma \in S_n$ of cycle type $k_1, \ldots, k_l$, $\operatorname{sign}(\sigma) = \prod_{j=1}^{l}(-1)^{k_j - 1}$.

1.12.13. Permutations of negative sign are called *odd*, and of positive sign are called *even*. (So, even cycles are odd, and odd are 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 $n!/2$.

1.13. Commuting elements, conjugate elements, the center of the group, and centralizers of elements

Let G be a group.

1.13.1. 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 $aba^{-1}b^{-1} = 1$.

1.13.2. For $a, b \in G$, the elements a and bab^{-1} are said to be *conjugate* in G.

1.13.3. The relation of being conjugate is an equivalence relation: a is conjugate to a, if a_2 is conjugate to a_1 then a_1 is conjugate to a_2, and if a_2 is conjugate to a_1 and a_3 is conjugate to a_2, then a_3 is conjugate to a_1. So, G is partitioned by this relation into equivalence classes, called *conjugacy classes*: two elements of G belong to the same class iff they are conjugate in G.

1.13.4. 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 $[a, b] = 1$.

1.13.5. 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 conjuates except itself, that is, its conjugacy class is the singleton $\{a\}$.

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

1.13.6. 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.
1.13.7. 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, $Z(G) = \bigcap_{b\in G} C_G(b) = \bigcap_{b\in S} C_G(b)$, where S is any set of generators of G.
1.13.8. Example. $C_{D_{2n}}(s) = \{1, s\}$ if n is odd and $\{1, s, r^{n/2}, sr^{n/2}\}$ if n is even; $C_{D_{2n}}(r) = \langle r\rangle$.

---

2. Cosets and factorization

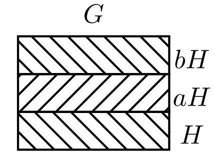
2.1. Cosets and counting principles

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.)
Notice that for any $a \in H$, $aH = Ha = H$, so H is a coset of itself. For any $a \notin H$, $aH \neq H$ and $Ha \neq H$, since $a \in aH$ and $a \in Ha$.
2.1.2. Theorem. *Any two left cosets of H in G either coincide or are disjoint, and thus the left cosets of H partition G. Two elements $a, b \in G$ belong to the same coset iff $aH = bH$ iff $a^{-1}b \in H$.*
Proof. If $aH = bH$ then $b1 = ah$ for some $h \in H$, so $a^{-1}b = h \in H$. Conversely, if $h = a^{-1}b \in H$, then $b = ah$ and $bH = ahH = aH$.
The relation "$a^{-1}b \in H$" between a and b is an equivalence relation: $a^{-1}a = 1 \in H$, if $a^{-1}b \in H$ then $b^{-1}a = (a^{-1}b)^{-1} \in H$, and if $a^{-1}b, b^{-1}c \in H$, then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$. Hence, G is partitioned into equivalence classes of this relation, which are just the left cosets of H. ■
2.1.3. If $aH = bH$, that is, if $a^{-1}b \in H$, we also write $a = b \bmod H$.
2.1.4. Similarly,
Theorem. *Any two right cosets of H in G either coincide or are disjoint, and thus the right cosets of H partition G. Two elements $a, b \in G$ belong to the same coset iff $Ha = Hb$ iff $ab^{-1} \in H$.*
2.1.5. Examples. (i) The cosets of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ are the sets $\overline{k} = n\mathbb{Z} + k$ for $k = 0, 1, \dots, n-1$.
(ii) The cosets of the subgroup (the line) $H = \mathbb{R}u$, where u is a vector in $\mathbb{R}^n$, are the lines $a + \mathbb{R}u$, parallel to H.
(iii) The cosets of the subgroup (the ray) $\mathbb{R}^*_+ = \{x \in \mathbb{R},\ x > 0\}$ of $\mathbb{C}^*$ are the rays $\mathbb{R}^*_+ z_0 = \{z : \arg z = \arg z_0\}$, $z_0 \neq 0$.
(iv) The cosets of the subgroup (the unit circle) $S = \{z : |z| = 1\}$ of $\mathbb{C}^*$ 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 $\{\varphi \in S_X : \varphi(x_1) = x_0\}$, $x_1 \in X$.
2.1.6. The set of left cosets of H in G is denoted by G/H; the set of right cosets of H in G is (sometimes) denoted by ${}_H\backslash G$;
Claim. *The number of right cosets of H in G equals the number of left cosets: $|G/H| = |{}_H\backslash G|$. The mapping $a \mapsto a^{-1}$ maps right cosets to left cosets and vice versa.*
Proof. $(Ha)^{-1} = a^{-1}H^{-1} = a^{-1}H$. ■
The number $|G/H|$ of left (and of right) cosets of H in G is called *the index* of H in G and is denoted by $|G : H|$. In the diagram of subgroups, the edge connecting a group and its subgroup is marked by the index of this subgroup:

$$\begin{array}{c} \mathbb{Z}_6 \\ \big|\,{\scriptstyle 3} \\ \langle 3\rangle \cong \mathbb{Z}_2 \\ \big|\,{\scriptstyle 2} \\ 0 \end{array}$$

2.1.7. All left (and all right) cosets of a subgroup have the same cardinality:

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, $|aH| = |H|$.*



Proof. The inverse mapping $aH \longrightarrow H$ is given by $b \mapsto a^{-1}b$. ∎

2.1.8. As a corollary, we get:

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

2.1.9. Corollary – Lagrange's theorem. *If $|G| < \infty$, then $|H| \mid |G|$.*

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

Proof. The order $|a|$ of an element $a \in G$ is the order of the cyclic group $\langle a \rangle$. ∎

2.1.11. Corollary. *Every finite group of prime order is cyclic.*

Proof. Let $|G|$ be prime. Take any $a \in G \setminus \{1\}$. Then $|a| \mid |G|$ and $|a| \neq 1$, so $|\langle a \rangle| = |a| = |G|$, so $G = \langle a \rangle$. ∎

2.1.12. We now have:

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

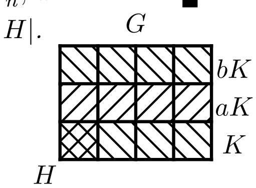
Proof. The group $\mathbb{Z}_p^*$ of nonzero residues modulo p has order $p-1$, so for any $a \in \mathbb{Z}_p^*$, $a^{p-1} = 1$, and $a^p = a$. ∎

2.1.13. And its generalization:

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

Proof. The group $\mathbb{Z}_n^*$ of invertible residues modulo n has order $\varphi(n)$, so for any $a \in \mathbb{Z}_n^*$, $a^{\varphi(n)} = 1$. ∎

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



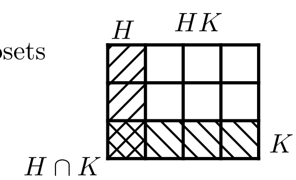
Proof. K is a disjoint union of $|K : H|$ cosets of H, each of $|G : K|$ cosets of K is a copy of K and thus also is a disjoint union of $|K : H|$ cosets of H, and every coset of H in G is contained in one of the cosets of K in G. Hence, the total number $|G : H|$ of cosets of H in G is $|G : K| \cdot |K : H|$. ∎

2.1.15. 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. If a set $S \subseteq G$ is a union of left cosets of a subgroup H of G, under $|S : H|$ we understand the number of these cosets.

2.1.16. The 3rd counting principle. *For $H, K \leq G$ we have $|HK : K| = \big|H : (H \cap K)\big|$ and $\big|HK : (H \cap K)\big| = \big|H : (H \cap K)\big| \cdot \big|K : (H \cap K)\big|$. If $|HK| < \infty$, then $|HK| = |H| \cdot |K| / |H \cap K|$.*

Proof. HK is a disjoint union of left cosets of K and H is a disjoint union of left cosets of $H \cap K$; for $h_1, h_2 \in H$ we have $h_1 K = h_2 K$ iff $h_1^{-1} h_2 \in K$ iff $h_1^{-1} h_2 \in H \cap K$ iff $h_1(H \cap K) = h_2(H \cap K)$. Thus, $|HK : K| = \big|H : (H \cap K)\big|$.

Next, K, and every left coset of K, is a disjoint union of $\big|K : (H \cap K)\big|$ left cosets of $H \cap K$. Thus,



$$\big|HK : (H \cap K)\big| = |HK : K| \cdot \big|K : (H \cap K)\big| = \big|H : (H \cap K)\big| \cdot \big|K : (H \cap K)\big|.$$

And if $|HK| < \infty$, this equality can be rewritten as $|HK|/|H \cap K| = \big(|H|/|H \cap K|\big)\big(|H|/|H \cap K|\big)$, which implies $|HK| = |H| \cdot |K| / |H \cap K|$. ∎

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, $aHa^{-1} = H$. This implies that for every $a \in G$ and $h \in H$, $ah = h'a$ for some $h' \in H$, or, in other words, that $aha^{-1} \in H$; on the other hand, if so, then $aHa^{-1} \subseteq H$ for every $a \in H$, and since also $a^{-1}Ha \subseteq H$, we get that $aHa^{-1} = H$.

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:

$$\begin{array}{c} G \\ \| \\ H \end{array}$$

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 $\{1,(1,2)\}$ 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 $\langle r^k\rangle$ is normal for every k.

2.2.4. Proposition.

(i) *The intersection of any collection of normal subgroups is a normal subgroup.*

(ii) *The join of two (and of any collection of) normal subgroups is a normal subgroup.*

(iii) *If $H \trianglelefteq G$ and $K \leq G$, then $(H\cap K) \trianglelefteq K$; in particular, if $H \leq K \leq G$ and $H \trianglelefteq G$, then $H \trianglelefteq K$.*

(iv) *If $H \leq G$ and $|G:H| = 2$, then $H \trianglelefteq G$.*

Proof.

(i) Let H_α, $\alpha\in\Lambda$, be a collection of normal subgroups of a group G, and let $H=\bigcap_{\alpha\in\Lambda}H_\alpha$. Then for any $a\in G$ and $h\in H$ we have $aha^{-1}\in H_\alpha$ for all $\alpha\in\Lambda$, so $aha^{-1}\in H$.

(ii) Let, again, H_α, $\alpha\in\Lambda$, be a collection of normal subgroups of G, and let H be the join of this family (the minimal subgroup of G generated by the elements of $\bigcup_{\alpha\in\Lambda}H_\alpha$). Then every element h of H has form $h=h_1h_2\cdots h_k$ for some $h_i\in H_{\alpha_i}$, $i=1,\dots,k$. Then

$$aha^{-1} = ah_1h_2\cdots h_ka^{-1} = (ah_1a^{-1})(ah_2a^{-1})\cdots(ah_ka^{-1})\in H$$

since for every i, $ah_ia^{-1}\in H_{\alpha_i}$.

(iii) For every $h\in H\cap K$ and $k\in K$ we have $khk^{-1}\in K$ and $khk^{-1}\in H$, so $khk^{-1}\in H\cap K$.

(iv) If $|G:H|=2$, then, except itself, H has a single left coset $G\setminus H$, which is also the only right coset H distinct from H. So, every left coset of H is a right coset, thus H is normal in G. ■

2.2.5. Let S be a subset of a group; then the intersection of all normal subgroups containing S is a normal subgroup, and is the minimal normal sungroup containing S; it is denoted by $\langle\langle S\rangle\rangle$. This group consists of all products of the form $(a_1s_1a_1^{-1})\cdots(a_ks_ka_k^{-1})$ where for every i, $s_i\in S$ or $s_i^{-1}\in S$, and $a_i\in G$.

2.2.6. If H is a normal subgroup of G, then the set G/H of (left=right) cosets of H in G possesses a group structure. Let's denote the coset aH by $\bar a$; then $G/H=\{\bar a : a\in G\}$. Since H is normal, the product of any two cosets $\bar a,\bar b\in G/H$ is a coset of H as well: $\bar a\bar b=(aH)(bH)=a(Hb)H=a(bH)H=ab(HH)=(ab)H=\overline{ab}\in G/H$. We define the multiplicaiton on G/H this way: for any $\bar a,\bar b\in G$ we define $\bar a\bar b=\overline{ab}$. (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 $\bar 1=H$ of H, and the inverse of a coset $\bar a=aH$ is the coset $\overline{a^{-1}}=a^{-1}H$. Thus, G/H is a group; this group is called *the quotient group*, or *the factor group* of G by H. The order of G/H is $|G:H|$.

Notice that the quotient group G/H is not a subgroup of G. (It may sometimes be isomorphic to a subgroup of G, but, by definition, it is not a subgroup!) G/H may be viewed as G with additional relations: namely, all elements of H are now assumed 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.

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

(ii) $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$. (Notice that $\mathbb{Z}_n$ is not a subgroup of $\mathbb{Z}$, and is not isomorphic to a subgroup of $\mathbb{Z}$!)

(iii) $\mathbb{R}/\mathbb{Z}$ is isomorphic to the group $[0,1)$ with addition modulo 1. (Geometrically, it is a circle.)

(iv) $S_n/A_n\cong\{1,-1\}\cong\mathbb{Z}_2$.

(v) $\mathbb{C}^*/\mathbb{R}^*_+\cong S=\{z\in\mathbb{C}:|z|=1\}$, a circle. (In this case, the quotient group is isomorphic to a subgroup of the group.) Also, $\mathbb{C}^*/S\cong\mathbb{R}^*_+$.

2.2.8. We, actually, already met a situation where elements of a "new" group are equivalence classes of elements of another group. Namely, if a group G is presented by generators and relations, $G=\langle S\,|\,R\rangle$, then it is just the quotient group $F_S/\langle\langle R\rangle\rangle$, 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. (We identify a relation $v=w$ with the element vw^{-1} of G.) This should be used as the "professional" definition of $\langle S\,|\,R\rangle$.

2.2.9. If H is a normal subgroup of G and both H and G/H are finitely generated, then G is finitely generated. Indeed, let $H = \langle S \rangle$ and $G/H = \langle P \rangle$; let π be the projection $G \longrightarrow G/H$. For every $C \in P$ choose $c_C \in \pi^{-1}(C)$ (that is, $c_C \in C$) and put $\widetilde{P} = \{c_C,\ C \in P\}$; then G is generated by $S \cup \widetilde{P}$. Indeed, since G/H is generated by $P = \pi(\widetilde{P})$, for any $a \in G$ there is $b \in \langle \widetilde{P} \rangle$ such that $\pi(a) = \pi(\widetilde{P})$, so $a = bh$ for some $h \in H = \langle S \rangle$.

Conversely, if G is generated by a set S, then any its quotient G/H is generated by the image of S in G/H, so if G is finitely generated so is G/H. It may not be true however that a subgroup of a finitely generated group is finitely generated.

2.2.10. We will also need the following fact:

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 $a^k z$ 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

$$b_1 b_2 = a^{k_1} z_1 a^{k_2} z_2 = a^{k_1+k_2} z_1 z_2 = a^{k_2} z_2 a^{k_1} z_1 = b_2 b_1.$$

■

2.3. Conjugates, normalizers, and centralizers of subgroups

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

2.3.1. The mapping $G \longrightarrow G$ 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: $a(bc)a^{-1} = (aba^{-1})(aca^{-1})$, $b, c \in G$. Hence, it is *an automorphism* of G – an isomorphism $G \longrightarrow G$.

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

2.3.4. Let H be a subgroup of G. We say that an element $a \in G$ *normalizes* H if $aHa^{-1} = H$. 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 $K \leq G$.*

Proof. HK is closed under multiplication: for any $h_1, h_2 \in H$ and $k_1, k_2 \in K$ we have

$$(h_1 k_1)(h_2 k_2) = h_1(k_1 h_2)k_2 = h_1(h' k_1)k_2 = (h_1 h')(k_1 k_2)$$

for some $h' \in H$, so is contained in HK. Also, HK is closed under taking inverses: for any $h \in H$ and $l \in K$,

$$(hk)^{-1} = k^{-1}h^{-1} = h'k^{-1}$$

for some $h' \in H$, so is contained in HK. ■

2.3.6. The group $C_G(H) = \big\{a \in G : aha^{-1} = h \text{ for all } h \in H\big\}$ 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, subnormal 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*. So, a group is solvable if "it is made" of abelian groups.

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 $\mathbb{Z}_p$ for prime p and the groups A_n for $n \geq 5$.

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

The 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.*

The proof of this theorem will be given in subsection 3.4, after we have *isomorphism theorems*.

2.4.6. Examples. (i) The group $\mathbb{Z}_6$ has two different composition series: $0 \trianglelefteq \{0, 3\} \trianglelefteq \mathbb{Z}_6$ with factors (isomorphic to) $\mathbb{Z}_2$ and $\mathbb{Z}_3$, and $0 \trianglelefteq \{0, 2, 4\} \trianglelefteq \mathbb{Z}_6$ with factors (isomorphic to) $\mathbb{Z}_3$ and $\mathbb{Z}_2$.

(ii) The group S_3 has the (unique) composition series $1 \trianglelefteq \langle\sigma\rangle \trianglelefteq S_3$, where σ is a 3-cycle; the factors of this series are (isomorphic to) $\mathbb{Z}_3$ and $\mathbb{Z}_2$. (So, S_3 is "made of" of $\mathbb{Z}_3$ and $\mathbb{Z}_2$, 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 $Z = \big\{1, (1,2)(3,4)\big\} \cong \mathbb{Z}_2$ and $V = \big\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\big\} \cong V_4$. The factors of this series are $\mathbb{Z}_2$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, and $\mathbb{Z}_2$. (So, S_4 is also solvable.)

(iv) The (only) composition series of S_n for $n \geq 5$ is $1 \trianglelefteq A_n \trianglelefteq S_n$. (We will see that for $n \geq 5$, 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, $\mathbb{Z}$ has no finite composition series, and has many different (and with different factors) infinite composition series: in the series $\cdots \trianglelefteq 8\mathbb{Z} \trianglelefteq 4\mathbb{Z} \trianglelefteq 2\mathbb{Z} \trianglelefteq \mathbb{Z}$ all factors are isomorphic to $\mathbb{Z}_2$, in $\cdots \trianglelefteq 27\mathbb{Z} \trianglelefteq 9\mathbb{Z} \trianglelefteq 3\mathbb{Z} \trianglelefteq \mathbb{Z}$ all factors are isomorphic to $\mathbb{Z}_3$, in $\cdots \trianglelefteq 30\mathbb{Z} \trianglelefteq 6\mathbb{Z} \trianglelefteq 2\mathbb{Z} \trianglelefteq \mathbb{Z}$ the factors are isomorphic to $\ldots, \mathbb{Z}_5, \mathbb{Z}_3, \mathbb{Z}_2$.

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 – all finite simple groups have been found. The second part has not.

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

2.5.1. If $\sigma, \rho \in S_n$, then $\sigma\colon i \mapsto j$ iff $\rho\sigma\rho^{-1}\colon \rho(i) \mapsto \rho(j)$. So, if $\sigma = (i_1, \ldots, i_k) \cdots (j_1, \ldots, j_l)$ is the cycle decomposition of σ, then the cycle decomposition of $\rho\sigma\rho^{-1}$ is $\big(\rho(i_1), \ldots, \rho(i_k)\big) \cdots \big(\rho(j_1), \ldots, \rho(j_l)\big)$. 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. Thus, the conjugacy classes in S_n consist of permutations having the same cycle type.

2.5.2. Using 2.5.1, we can now prove the following nice and very important fact:

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

Proof. We do it in three steps:

Claim 1. *A_n is generated by 3-cycles.* Indeed, every even permutation is a product of an even collection of transpositions. Now, the product of two transpositions either has form $(a, b)(c, d)$ with all a, b, c, s distinct, or the form $(a, b)(a, c)$ with distinct a, b, c. And we have $(a, b)(c, d) = (a, c, b)(a, c, d)$ and $(a, b)(a, c) = (a, c, b)$.

Claim 2. *Any two 3-cycles are conjugate in A_n.* Indeed, any two 3-cycles $\sigma_1, \sigma_2 \in A_n$ are conjugate in S_n: $\sigma_2 = \rho\sigma_1\rho^{-1}$ for some $\rho \in S_n$. Now, if ρ is even, we are done; if ρ is odd, let τ be a transposition disjoint with σ_1 (it exists since $n \geq 5$). Then $\rho\tau \in A_5$ and

$$(\rho\tau)\sigma_1(\rho\tau)^{-1} = \rho(\tau\sigma_1\tau^{-1})\rho^{-1} = \rho\sigma_1\rho^{-1} = \sigma_2.$$

Claim 3. *Any nontrivial normal subgroup of A_n contains a 3-cycle.* This is a hard part. Let $N \trianglelefteq A_n$, $N \neq 1$. Take any $\sigma \in N \setminus \{1\}$ and consider the following cases:
(i) The cycle decomposition of σ contains a k-cycle with $k \geq 4$: $\sigma = (a, b, c, d, e, \ldots, z)\delta$ where δ is disjoint from $(a, \ldots, z)$. Put $\rho = (a, b, c) \in A_n$; Since N is normal, it contains the conjugate $\rho\sigma\rho^{-1} = (b, c, a, d, e, \ldots, z)\delta$ of σ, and so, also contains the 3-cycle

$$(\rho\sigma\rho^{-1})\sigma^{-1} = (b, c, a, d, e, \ldots, z)\delta\delta^{-1}(a, b, c, d, e, \ldots, z)^{-1}) = (a, b, d).$$

(ii) The cycle decomposition of σ contains two 3-cycles: $\sigma = (a, b, c)(d, e, f)\delta$ where (a, b, c), (d, e, f), and δ are disjoint. Take $\rho = (a, b, d) \in A_n$ and observe that

$$N \ni (\rho\sigma\rho^{-1})\sigma^{-1} = (b, d, c)(a, e, f)(a, c, b)(d, f, e) = (a, b, e, c, d);$$

then by (i), N contains a 3-cycle.
(iii) σ is a product of a 3-cycle and several (or none) pairwise disjoint and disjoint from σ) transpositions; then σ^2 is a 3-cycle.
(iv) Finally, if $\sigma = (a, b)(c, d)\delta$ where δ is disjoint from (a, b) and (c, d), taking $\rho = (a, b, c) \in A_n$ we get that $\sigma' = \rho\sigma\rho^{-1}\sigma^{-1} = (b, c)(a, d)(a, b)(c, d) = (a, c)(b, d) \in N$. Then taking $\rho' = (a, b, z)$ for some $z \notin \{a, b, c, d\}$ (it exists since $n \geq 5$), we obtain that also

$$\rho'\sigma'(\rho')^{-1}\sigma' = (b, c)(z, d)(a, c)(b, d) = (a, b, z, d, c) \in N.$$

Thus by (i), N contains a 3-cycle. ■

---

3. Homomorphisms of groups

3.1. Homomorphisms

3.1.1. A mapping $\varphi: G \longrightarrow H$ 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*.

3.1.2. Examples. (i) If H is a subgroup of G, then the embedding $H \longrightarrow G$, $a \mapsto a$, is a homomorphism.
(ii) Linear mappings of vector spaces are homomorphisms.
(iii) For any $a \in \mathbb{Z}$, the mapping $\mathbb{Z} \longrightarrow \mathbb{Z}$, $n \mapsto an$, is a homomorphism. More generally, for any group G and an element $a \in G$, the mapping $Z \longrightarrow G$, $n \mapsto a^n$, is a homomorphism. (In fact, any homomorphism $\mathbb{Z} \longrightarrow G$ is of this form.)
(iv) For any $n \in \mathbb{N}$ and a field F, det is a homomorphism $\mathrm{GL}_n(F) \longrightarrow F^*$.
(v) For any $n \in \mathbb{N}$, sign is a homomorphism $S_n \longrightarrow \{-1, 1\}$.
(vi) The mapping $z \mapsto |z|$ is a homomorphism $\mathbb{C}^* \longrightarrow \mathbb{R}^*$.
(vii) The mapping $x \mapsto e^{2\pi i x}$ is a homomorphism $\mathbb{R} \longrightarrow \mathbb{C}^*$.
(viii) If H is a quotient group of a group G, $H = G/N$, then the mapping $G \longrightarrow H$, $a \mapsto \bar{a} = aN$ 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 $F_S \longrightarrow G$, 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.
(x) For every $n \in \mathbb{N}$, there is a natural homomorphism from the group B_n of n-braids to the group S_n: every n-braid connects the set $\{1, \ldots, n\}$ of initial points with the same set $\{1, \ldots, n\}$ of ending points, thereby permuting this set.

3.1.3. Here are some elementary properties of homomorphisms, which are easy to check:
Let $\varphi: G \longrightarrow H$ 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 φ is an isomorphism, then φ^{-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 φ is surjective, then $\varphi(K) \trianglelefteq H$.

3.1.4. If S is a generating set of a group G, then every homomorphism φ of G is uniquely defined by its restriction $\varphi|_S$, that is, by the values $\varphi(a)$, $a \in S$.

3.1.5. Let $\varphi: G \longrightarrow H$ be a homomorphism. The preimage $\varphi^{-1}(1_H) = \{a \in G : \varphi(a) = 1_H\}$ of 1_H is called *the kernel* of φ and is denoted by $\operatorname{Ker}\varphi$. $\operatorname{Ker}\varphi$ is a normal subgroup of G.

3.2. The isomorphism theorems

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

Theorem. *φ is injective iff its kernel is trivial,* $\operatorname{Ker}\varphi = 1$.

3.2.2. As a corollary we get

The 1st isomorphism theorem. *For any homomorphism $\varphi: G \longrightarrow H$, $\varphi(G) \cong G/\operatorname{Ker}\varphi$, where the isomorphism is defined by $\bar{a} \mapsto \varphi(a)$.*

Proof. The cosets of $N = \operatorname{Ker}\varphi$ are in one-to-one correspondence with the elements of $\varphi(G)$, and the mapping $\bar{a} \mapsto \varphi(a)$ is a homomorphism since $\bar{a}\bar{b} = \overline{ab} \mapsto \varphi(ab) = \varphi(a)\varphi(b)$. ∎

3.2.3. It follows that any homomorphism $\varphi: G \longrightarrow H$ is a composition of the (surjective) factorization homomorphism $G \mapsto G/\operatorname{Ker}\varphi$, an isomorphism $G/\operatorname{Ker}\varphi \longrightarrow \varphi(G)$, and the (injective) embedding homomorphism $\varphi(G) \longrightarrow H$.

3.2.4. It also follows that if $\varphi: G \longrightarrow H$ is a group homomorhism, then $|\varphi(G)| = |G : \ker(\varphi)|$. If $|G| < \infty$, this imples that $|\varphi(G)| \bigm| |G|$. (Notice that since $\varphi(G) \leq H$, $|\varphi(G)| \bigm| |H|$ as well.)

3.2.5. Examples. (i) The kernel of the homomorphism $\operatorname{sign}: S_n \longrightarrow \{-1, 1\}$ is the group A_n, so $S_n/A_n \cong \{-1, 1\} \cong \mathbb{Z}_2$.

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

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

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

3.2.6. If a group G is generated by a set S, then the homomorphism $\varphi: F_S \longrightarrow G$, $F_S \ni s_1 \cdots s_k \mapsto s_1 \cdots s_k \in G$, 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.*

3.2.7. 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, $KH/H \cong K/(K \cap H)$:

$$\begin{array}{ccc} & KH & \\ / & & \backslash\!\backslash \\ K & & H \\ \backslash\!\backslash & & / \\ & K \cap H & \end{array}$$

Proof. We know that KH is a group; $H \trianglelefteq KH$ because all elements of K and of H normalize H. We also know that $(K \cap H) \trianglelefteq K$. We have the embedding homomorphism $K \longrightarrow KH$ and, composing it with the factorization homomorphism $KH \longrightarrow (KH)/H$, get a homomorphism $\varphi\colon K \longrightarrow (KH)/H$ defined by $\varphi(k) = kH$, $k \in K$. φ is surjective, since every coset of H in KH has form kH for some $k \in K$. The kernel of φ is $\{k \in K : kH = H\} = K \cap H$. So by The 1st isomorphism theorem 3.2.2, $K/(K \cap H) \cong (KH)/H$. ■

3.2.8. 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 $aK \mapsto (aH)(K/H)$, $a \in G$.*

Proof. The subgroup K/H is normal in G/H since it is the image of the normal subgroup K of G under a surjective (factorization) homomorphism $G \longrightarrow (G/H)$. After factorization of G/H by this subgroup, we get the homomorphism $\varphi\colon G \longrightarrow (G/H)/(K/H)$ with $\varphi(a) = (aH)(K/H)$. φ is surjective since every element of $(G/H)/(K/H)$ has form $(aH)(K/H)$ for some $a \in G$. The kernel of φ consists of elements $a \in G$ such that the coset $(aH)(K/H)$ in the group $(G/H)/(K/H)$ is equal to K/H. This is so iff $aH \in K/H$, that is, iff $a \in K$. Hence, $\ker\varphi = K$ and by The 1st isomorphism theorem 3.2.2, $G/K \cong (G/H)/(K/H)$. ■

3.2.9. The next theorem just summarizes some of the facts we already know. It is not, actually, an "isomorphism theorem", – it does not declare that two groups are isomorphic; it only says that the lattice of subgroups of a quotient group G/H looks exactly like the sublattice of the lattice of subgroups of G located "above H" (that is, of the subgroups of G containing H).

The 4th (lattice) 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 $\overline{K}$ of G/H corresponds to its preimage K in G, and a subgroup K of G containing H corresponds to the subgroup $\overline{K} = K/H$ of G/H. For two subgroups K_1, K_2 of G we have $\overline{K}_1 \leq \overline{K}_2$ iff $K_1 \leq K_2$, in which case $|\overline{K}_2 : \overline{K}_1| = |K_2 : K_1|$; $\overline{K}_1 \trianglelefteq \overline{K}_2$ iff $K_1 \trianglelefteq K_2$, in which case $\overline{K}_2/\overline{K}_1 \cong K_2/K_1$; $\overline{K_1 \cap K_2} = \overline{K}_1 \cap \overline{K}_2$; and $\overline{\langle K_1, K_2\rangle} = \langle \overline{K}_1, \overline{K}_2\rangle$.*

3.3. Reduction of a homomorphism to a quotient group

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

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr] & & H \\ & G/N. \arrow[ur, "\tilde{\varphi}"'] & \end{tikzcd}$$

3.3.2. The following is easy, but important:

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

Proof. In general, if $\varphi\colon X \longrightarrow Y$ is a mapping, X is partitioned, $X = \bigcup_{\alpha \in \Lambda} Z_\alpha$, into subsets Z_α, $\widetilde{X}$ is the set of these subsets, $\widetilde{X} = \{Z_\alpha, \alpha \in \Lambda\}$, and π is the natural projection $X \longrightarrow \widetilde{X}$, then φ reducible to a mapping $\tilde{\varphi}\colon \widetilde{X} \longrightarrow Y$, so that $\varphi = \tilde{\varphi} \circ \pi$, iff φ is constant on each of the sets Z_α:

$$\begin{tikzcd} X \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & Y \\ & \widetilde{X}, \arrow[ur, "\tilde{\varphi}"'] & \end{tikzcd}$$

in which case we put $\tilde{\varphi}(Z_\alpha) = \varphi(x)$ for any element $x \in Z_\alpha$, $\alpha \in \Lambda$.

Thus, in our case, φ is reducible to a mapping $G/N \longrightarrow H$ iff φ is constant on each coset of N in G. This, in particular, implies that $\varphi(H) = \varphi(1) = 1$, so that $H \leq \ker\varphi$. Conversely, if $H \leq \ker\varphi$, then $\varphi(aH) = \varphi(a)\varphi(H) = \varphi(a)1 = \varphi(a)$ for every $a \in G$, thus φ is constant on every the coset of H, and $\tilde{\varphi}$ can be defined. And if so, $\tilde{\varphi}$ is a homomorphism, since for any $a, b \in G$,

$$\tilde{\varphi}(\bar{a}\bar{b}) = \tilde{\varphi}(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \tilde{\varphi}(\bar{a})\tilde{\varphi}(\bar{b}).$$

■

3.3.3. A special case of Theorem 3.3.2 is the following situation: Let G be a group defined by generators and relations, $G = \langle S \,|\, R\rangle$ and let $f\colon S \longrightarrow H$ be a mapping of the set of generators to a group H; is f extendible to a homomorphism $\varphi\colon G \longrightarrow H$, 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.

3.3.4. Example. Dealing with the standard presentation of the dihedral group $D_{2n} = \big\langle r, s \,|\, r^n = s^2 = 1,\ rs = sr^{-1}\big\rangle$, given a group H and elements $a, b \in H$, a homomorphism $D_n \longrightarrow H$ that maps $r \mapsto a$ and $s \mapsto b$ exists iff $a^n = b^2 = 1$ and $ab = ba^{-1}$.

3.4. Proof of the Jordan-Hölder theorem

We may now give the proof of The Jordan-Hölder theorem 2.4.5.

The first part is easy: if G is not simple, it has a nontrivial normal subgroup N. By induction on cardinality, both N and G/N have finite composition series: $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = N$ and $1 = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G/N$. For each i, let $\widetilde{K}_i$ be the preimage of K_i in G; then by The 3rd isomorphism theorem 3.2.8, for each i, $\widetilde{K}_i/\widetilde{K}_{i-1} \cong K_i/K_{i-1}$ is a simple group, thus

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = N = \widetilde{K}_0 \lhd \widetilde{K}_1 \lhd \cdots \lhd \widetilde{K}_m = G$$

is a composition series of G.

The second part is harder. Let us say that two composition series of a group *are equivalent* if they have the same length and the same factors, up to reordering. Let $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$ and $1 = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G$ be two composition series of G. If $H_{n-1} = K_{m-1}$, then by induction on the cardinality of the group, $n = m$ and the series $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1}$ and $1 = K_0 \lhd K_1 \lhd \cdots \lhd K_{m-1}$ are equivelent, and so are $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$ and $1 = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G$. Assume that $H_{n-1} \neq K_{m-1}$. The subgroup $H_{n-1}K_{m-1}$ is normal in G and contains H_{n-1}, thus $H_{n-1}K_{m-1} = G$. (Otherwise $H_{n-1}K_{m-1}/H_{n-1}$ is a normal subgroup of G/H_{n-1}.) Let $L = H_{n-1} \cap K_{m-1}$ and let $1 = L_0 \lhd L_1 \lhd \cdots \lhd L_l = L$ be a composition series of L.

$$\begin{tikzcd}
 & & G \arrow[dl, equal] \arrow[dr, equal] & & \\
 & H_{n-1} \arrow[dl, equal] \arrow[dr, equal] & & K_{m-1} \arrow[dl, equal] \arrow[dr, equal] & \\
H_{n-2} \arrow[d, equal] & & L = H_{n-1} \cap K_{m-1} \arrow[d, equal] & & K_{m-2} \arrow[d, equal] \\
H_{n-3} \arrow[d, equal] & & L_{l-1} \arrow[d, equal] & & K_{m-3} \arrow[d, equal] \\
\vdots \arrow[d, equal] & & \vdots \arrow[d, equal] & & \vdots \arrow[d, equal] \\
H_1 \arrow[drr, equal] & & L_1 \arrow[d, equal] & & K_1 \arrow[dll, equal] \\
 & & 1 & &
\end{tikzcd}$$

Since $H_{n-1}/L \cong G/K_{m-1}$ is simple, $1 = L_0 \lhd L_1 \lhd \cdots \lhd L_l \lhd H_{n-1}$ is a composition series of H_{n-1}, and by induction on the cardinality of the group, is equivalent to $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1}$. Similarly, $1 = L_0 \lhd L_1 \lhd \cdots \lhd L_l \lhd K_{m-1}$ is equivalent to $1 = K_0 \lhd K_1 \lhd \cdots \lhd K_{m-1}$. Firstly, this implies that $n = l + 2 = m$. Next, the factors of the series $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$ are the same as the factors of $1 = L_0 \lhd L_1 \lhd \cdots \lhd L_l$, plus the factor group H_{n-1}/L, plus the factor group G/H_{n-1}; the factors of the series $1 = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G$ are the same as the factors of $1 = L_0 \lhd L_1 \lhd \cdots \lhd L_l$, plus the factor group K_{m-1}/L, plus the factor group G/K_{m-1}. Since, by The 2nd isomorphism theorem 3.2.7, $H_{n-1}/L \cong G/K_{m-1}$ and $G/H_{n-1} \cong K_{m-1}/L$, we obtain that the series $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$ and $1 = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G$ are equivalent. ■

4. Actions of groups on sets and on themselves

4.1. Group actions

4.1.1. Let G be a group and X be a set. *An action* of G on X is a mapping $G\times X\longrightarrow X$, $(a,x)\mapsto ax$, 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 $G\times X\longrightarrow X$, $(a,x)\mapsto xa$, 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 $x\in X$.

4.1.2. Given an action of G on X, every element $a\in G$ defines a mapping $\varphi_a\colon X\longrightarrow X$ 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 $a\in G$, $\varphi_{a^{-1}}=\varphi_a^{-1}$, So, all mappings φ_a are invertible, and we have a homomorphism $\varphi\colon G\longrightarrow S_X$, $a\mapsto\varphi_a$. Conversely, any homomorphism $\varphi\colon G\longrightarrow S_X$ defines an action of G on X by $ax=\varphi_a(x)$.

4.1.3. 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 φ introduced in 4.1.2.) 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 $x_1,\dots,x_n\in X$ and distinct $y_1,\dots,y_n\in X$ there is $a\in G$ such that $ax_i=y_i$ for all $i=1,\dots,n$.)

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

Any two distinct orbits in X are disjoint, and thus orbits partition X: X is a disjoint union of distinct orbits. The action of G on X is transitive if X consists of a unique orbit.

4.1.5. 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 $G_x=G$.

4.1.6. 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: $|Gx|=|G:G_x|$.

4.1.7. 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.

4.1.8. For any $a\in G$ and $x\in X$, the stablizer of the point ax is $G_{ax}=aG_xa^{-1}$, a conjugate of G_x.

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.)

4.1.9. 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 permutations (self-bijections) of X. Such is, for instance, the action of the group $\mathrm{GL}_n(F)$ 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 for 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 $X=\{1,\dots,n\}$. The orbits under this actions are just the cycles from the cycle decomposition of σ.

(v) An action of a group G on a set X induces an action of G on the power set $\mathcal{P}(X)$ of X by $(a,A)\mapsto aA$, $a\in G$, $A\subseteq X$. Also, it induces an action of G on X^k for every k, by $a(x_1,\dots,x_k)=(ax_1,\dots,ax_k)$.

(vi) If G acts on a set X and Y is aother set, then the left action of G on X induces a right action of G on the set of mappings $f\colon X\longrightarrow Y$, by $(fa)(x)=f(ax)$, $a\in G$, $x\in X$.

4.1.10. There is a nice formula for the number of orbits under a finite group action, called *Burnside's lemma* and also *The lemma that is not Burnside's*:

Lemma. *Let G be a finite group acting on a finite set X, for each $a\in G$ let $X^a=\{x\in X: ax=x\}$ (and for every $x\in X$ let G_x be the stabilizer $\{a\in G: ax=x\}$ of x). Then the number of orbits in X under this action equals $\frac{1}{|G|}\sum_{a\in G}|X^a|=\frac{1}{|G|}\sum_{x\in X}|G_x|$.*

Proof. Firstly, we, indeed, have

$$\sum_{a\in G}|X^a| = \#\big\{(a,x)\in G\times X : ax=x\big\} = \sum_{x\in X}|G_x|.$$

And the number of orbits is

$$\sum_{x\in X}\frac{1}{|Gx|} = \frac{1}{|G|}\sum_{x\in X}\frac{|G|}{|Gx|} = \frac{1}{|G|}\sum_{x\in X}|G_x|.$$

■

4.2. The left regular action

Let G be a group.

4.2.1. 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.

4.2.2. The left regular action of G defines an injective homomorphism $G\longrightarrow S_G$. 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.*

4.2.3. Two actions of a group G on sets X and Y are said to be *isomorphic* if there is a bijection $\varphi\colon X\longrightarrow Y$ that "agrees" with the actions: for any $x\in X$ and $a\in G$ one has $\varphi(ax)=a\varphi(x)$. An action of G on a set X is said to be *regular* if for any $x,z\in X$ there is a unique $a\in G$ such that $ax=z$. Clearly, every regular action of G is isomorphic to the left regular action: choose a point $x\in X$ and define $\varphi\colon G\longrightarrow X$ by $\varphi(b)=bx$, $b\in G$; then φ is a bijection and $\varphi(ab)=abx=a\varphi(b)$ for all $a,b\in G$.

4.2.4. Let $H\le G$. 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 $G\longrightarrow S_n$, with kernel $\bigcap_{a\in G}aHa^{-1}$.)

4.2.5. In fact, the action of G on the set G/H of left cosets of a subgroup H is "the most general transitive action", – any transitive action of G is isomorphic to such. Indeed, if G acts transitively on a set X, choose any $x\in X$, let $H=G_x$ (the stablilzer of x), and define $\varphi\colon(G/H)\longrightarrow X$ by $\varphi(bH)=bx$, $b\in G$; then φ is a bijection and satisfies $\varphi(abH)=abx=a\varphi(b)$ for all $a,b\in G$.

4.2.6. In particular, we may now easily justify Theorem 1.12.5 about cyclic decomposition of permutations. Given a permutation σ of a set X, X partitions into a disjoint set of orbits under the action of the cyclic group $Z=\langle\sigma\rangle$, and the action of Z on every orbit $\mathcal{O}$ is isomorphic to the left regular action of Z on the quotient group Z/H where H is a stabilizer of an element of $\mathcal{O}$, that is, is cyclic.

4.2.7. The following is a generalization, in the case of finite groups, of the fact that every subgroup of index two is normal:

Lemma. *If $|G|<\infty$ and a subgroup H of G is such that $p=|G:H|$ is the minimal prime divisor of $|G|$, then $H\trianglelefteq G$.*

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

4.3. The action of a group on itself by conjugations

Let G be a group.

4.3.1. 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 $C_G(b)$.

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

4.3.3. As a corollary, we have the following identity, called *the class equation*: If G is a finite group, then

$$|G| = |Z(G)| + \sum_{i=1}^{k} \bigl|G : C_G(b_i)\bigr|$$

where $b_1, \ldots, b_k$ are representatives of all nontrivial (that is, having more than one element) conjugacy classes in G.

4.3.4. If N is a normal subgroup of G, then, since $aNa^{-1} = N$ for all $a \in G$, G acts on N by conjugations as well. The kernel of this action is the centralizer $C_G(N)$ of N.

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

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

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

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

---

5. The direct product of groups

5.1. The direct product of two groups

5.1.1. Given groups H and K, *The external direct product* is the group $G = H \times K = \bigl\{(h,k) : h \in H,\ k \in K\bigr\}$ with the componentwise multiplication. The subgroup $H \times 1$ of G is isomorphic to H ($(h,1) \leftrightarrow h$), and we identify it with H; likewise, we identify $1 \times K \leq G$ with K. Thus, we consider H and K as subgroups of G.

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

① $hk = kh$ for any $h \in H$ and $k \in K$ (both are equal to (h,k));

② H and K are normal in G;

③ $HK = G$;

④ $H \cap K = 1$;

⑤ every element $a \in G$ is uniquely representable in the form $a = hk$ with $h \in H$ and $k \in K$;

⑥ if $|G| < \infty$, then $|G| = |H| \cdot |K|$;

⑦ For the factorization mapping $\pi\colon G \longrightarrow {}_H\backslash G$ (to the set of right cosets of H), the restriction $\pi|_K$ is a bijection between K and ${}_H\backslash G$.

5.1.3. For any element (h,k) of a direct product $H \times K$, $|(h,k)| = \mathrm{lcm}(|h|, |k|)$.

5.1.4. 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 $\varphi\colon G \longrightarrow H \times K$ 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.)

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

$$\begin{tikzcd}
& H \arrow[dl] \arrow[dr] & \\
G \arrow[rr, "\varphi"] & & H \times K \\
& K \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

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

5.1.6. Proposition. *Let G be a group and let H, K be subgroups of G satisfying the properties ①, ③, and ④ from* 5.1.2. *Then $G = H \times K$.*

Proof. Define a mapping $\psi\colon H \times K \longrightarrow G$ (from the external direct product of K and H!) by $\psi(h,k) = hk$. ψ is a homomorphism by ①: for any $h_1, h_2 \in H$ and $k_1, k_2 \in K$,

$$\psi\big((h_1,k_1)(h_2,k_2)\big) = \psi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \psi(h_1,k_1)\psi(h_2,k_2),$$

and ψ is identical on H and on K:

$$\text{for any } h \in H,\ \psi(h,1) = h, \text{ and for any } k \in K,\ \psi(1,k) = k.$$

By ③, ψ is surjective. By ④, $\ker\psi = 1$: for $h \in H$ and $k \in K$, if $\psi(h,k) = 1$, then $hk = 1$, so $h = k^{-1}$, so $h, k \in H \cap K$, so $(h,k) = 1$. Hence, ψ is an isomorphism. ■

5.1.7. It follows that, given a group G and subgroups $H, K \leq G$, the properties ①, ③, ④ imply the other properties, ②, ⑤, ⑥, and ⑦. We actually have the following implications:

Proposition. *①&③$\Longrightarrow$②; ②&④$\Longrightarrow$①; ⑤$\Longleftrightarrow$③&④; ⑦$\Longleftrightarrow$③&④; and if $|G| < \infty$, ③&④$\Longrightarrow$⑥; ⑤$\Longrightarrow$⑥; ③&⑥$\Longrightarrow$④; ④&⑥$\Longrightarrow$③.*

Proof. ①&③$\Longrightarrow$②: By ③, H and K generate G. and by ①, their elements normalize both H and K, so all elements of G normalize both H and K.

②&④$\Longrightarrow$①: Let $h \in H$ and $k \in K$. By ②, $khk^{-1} \in H$ so $[k,h] = khk^{-1}h^{-1} \in H$, and similarly, $[k,h] \in K$. So, by ③, $[k,h] = 1$, so k and h commute.

③&④$\Longrightarrow$⑤: By ③, every element $a \in G$ is representable in the form $a = hk$ with $h \in H$ and $k \in K$. And if $a = h_1k_1 = h_2k_2$ with $h_1, h_2 \in H$ and $k_1, k_2 \in K$, then $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$, so $h_2^{-1}h_1 = k_2k_1^{-1} = 1$ by ④, so $h_1 = h_2$ and $k_1 = k_2$.

⑤$\Longrightarrow$③&④: Every element $a \in G$ is representable in the form $a = hk$ with $h \in H$ and $k \in K$, so $G = HK$. If $a \in H \cap K$, then $a = a1$ with $a \in H$, $1 \in K$, and also $a = 1a$ with $1 \in H$, $a \in K$; hence, by uniqueness, $a = 1$.

③&④$\Longrightarrow$⑦: By ③ every element of ${}_H\backslash G$ has form Hk for some $k \in K$, so $\pi|_K$ is surjective. And if $a, b \in K$ are such that $\pi(a) = \pi(b)$, that is, $Ha = Hb$, then $ab^{-1} \in H \cap K$, so by ④, $ab^{-1} = 1$, so $a = b$. Thus, $\pi|_K$ is injective.

⑦$\Longrightarrow$③&④: Assume ⑦. Let $a \in G$, put $k = \pi|_K{}^{-1}(\pi(a)) \in K$; then $\pi(k) = \pi(a)$, so $a = hk$, so we have ③. Next, if $a \in H \cap K$, then $\pi|_K(a) = \pi(a) = 1$, so $a = 1$; hence, we have ④.

Now assume that $|G| < \infty$. Then

⑤$\Longrightarrow$⑥ is clear. This also implies ③&④$\Longrightarrow$⑥.

③&⑥$\Longrightarrow$④: since $|H|\cdot|K| = |G| = |HK| = |H|\cdot|K|/|H \cap K|$ (by a counting principle), we get $|H \cap K| = 1$, so $H \cap K = 1$.

④&⑥$\Longrightarrow$③: $|HK| = |H|\cdot|K|/|H \cap K| = |H|\cdot|K| = |G|$, so $G = HK$. ■

5.1.8. As a corollary we obtain plenty of different criteria for a group G to be a direct product of its subgroups H and K: this is so if any of the following combinations of conditions holds: ②&③&④, ①&⑤, ②&⑤, or ②&⑦, and if $|G| < \infty$, ①&③&⑥, ①&④&⑥, ②&③&⑥, or ②&④&⑥.

The properties ②, ③, and ④ together are described by the diagram

$$\begin{array}{ccc} & HK = G & \\ /\!\!/ & & \backslash\!\!\backslash \\ H & & K \\ \backslash\!\!\backslash & & /\!\!/ \\ & H \cap K = 1 & \end{array}$$

Thus, if we have such a diagram of subgroups in G, then $G = H \times K$.

5.1.9. 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 $S = \{z \in \mathbb{C}^* : |z| = 1\}$.

5.1.10. Let $\varphi: G \longrightarrow K$ be a surjective group homomorphism; a homomorphism $\sigma: K \longrightarrow G$ is called *a section* of φ if $\varphi \circ \sigma = \mathrm{Id}_K$. This is the case, σ is an isomorphism between K and $\sigma(K)$.

The fact that ② & ⑦ imply that G is a direct product can be reformulated in the following way:

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

5.2. The central and the relative direct products

5.2.1. Let H and K be groups and let N be "a common central subgroup" of H and K; more generally, let N be a group with embeddings (injective homomorphisms) $\varphi: N \longrightarrow Z(H)$ and $\psi: N \longrightarrow Z(K)$. *The central product* of H and K with respect to N is the group $H *_N K = (H \times K)/D$ where $D = \big\{\big(\varphi(a), \psi(a)^{-1}\big),\ a \in N\big\}$. (That is, in $H \times K$ we identify the elements $(\varphi(a), 1)$ and $(1, \psi(a))$ for all $a \in N$.)

5.2.2. The central product $G = H *_N K$ of H and K with respect to a central subgroup N contains copies of H and K, $H \times 1$ and $1 \times K$. For G, we have the properties ①, ②, and ③, but not ④: H and K are normal in G, $hk = kh$ for all $h \in H$ and $k \in K$, $HK = G$, but $H \cap K = N' \cong N$. (The isomorphism is defined by $(\varphi_1(a), 1) = (1, \varphi_2(a)) \leftrightarrow a$.)

Conversely, if a group G is generated by two commuting subgroups H and K (that is, $G = HK$ and $hk = kh$ for all $h \in H$ and $k \in K$), then G is isomorphic to the central product of H and K with respect to $H \cap K$ (which isomorphism "respects" H and K), and G is said to be *an internal central product* of H and K.

5.2.3. If H and K are finite, $|H *_N K| = |H| \cdot |K|/|N|$.

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

5.2.5. A relative direct product $H \times_N K$ 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.

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

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

5.3. The direct product of several groups

5.3.1. The external direct product of k groups $H_1, \dots, H_k$ is defined similarly, $H_1 \times \cdots \times H_k = \big\{(h_1, \dots, h_n),\ h_i \in H_i,\ i = 1, \dots, k\big\}$, with the componentwise multiplication: $(a_1, \dots, a_n)(b_1, \dots, b_n) = (a_1b_1, \dots, a_nb_n)$. 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.

5.3.2. For any groups $H_1, \dots, H_k$, their "simultaneous" direct product is naturally isomorphic to the "successive" one: $H_1 \times H_2 \times \cdots \times H_{k-1} \times H_k \cong H_1 \times (H_2 \times \cdots \times (H_{k-1} \times H_k) \cdots)$.

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

① for any $i \neq j$, $hh' = h'h$ for any $h \in H_i$ and $h' \in H_j$;

② for every i, $H_i \trianglelefteq G$;

③ $H_1 \cdots H_k = G$;

④ for any i, $H_i \cap (H_1 \cdots H_{i-1}H_{i+1} \cdots H_k) = 1$;

⑤ every element $a \in G$ is uniquely representable in the form $a = h_1 \cdots h_k$ with $h_i \in H_i$ for all i;

⑥ if $|G| < \infty$, then $|G| = |H_1| \cdots |H_k|$;

⑦ with ②: the subgroups H_i are all normal and 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.

5.3.4. Let G be a group and $H_1, \dots, H_k \leq G$. We say that G *is an internal direct product* of $H_1, \dots, H_k$, 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 $\varphi: G \longrightarrow H_1 \times \cdots \times H_k$ such that $\varphi(h_i) = h_i$ for every $h_i \in H_i$ and every i. This implies that the element $(h_1, \dots, h_k)$ of $H_1 \times \cdots \times H_k$ corresponds to the element $h_1 \cdots h_k$ of G.)

5.3.5. Proposition. *Let G be a group and let $H_1, \ldots, H_k \le G$ satisfy the properties ①, ③, and ④ from* 5.3.3*. Then $G = H_1 \times \cdots \times H_k$.*

5.3.6. For the case of several subgroups of a group a statement analogous to Proposition 5.1.7 can also be formulated, but I omit it.

5.4. The 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.

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

5.4.2. 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 $M = \big\{(h_1, \ldots, h_k, 1, 1, 1, \ldots,),\ k \in \mathbb{N},\ h_i \in H_i,\ i = 1, \ldots, k\big\}$ 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 ①–⑦ hold for the direct sum rather than the direct product.

6. The Chinese remainder theorem and classification of finite abelian groups

6.1. The Chinese remainder theorem

6.1.1. The following facts are sometimes referred to as the Chinese remainder theorem:

Theorem. *For any coprime positive integers n and m, $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$, and the element $(1, 1)$ generates this group. Moreover, $\mathbb{Z}_{nm} = \langle m \rangle \times \langle n \rangle$, where $\langle m \rangle = m\mathbb{Z}_{nm} \cong \mathbb{Z}_n$ and $\langle n \rangle = n\mathbb{Z}_{nm} \cong \mathbb{Z}_m$.*

Proof. For every $k \in \mathbb{N}$ we have $k(1, 1) = (k, k)$, and the minimal k such that $(k, k) = 0$ in $\mathbb{Z}_n \times \mathbb{Z}_m$ is $\mathrm{lcm}(n, m) = nm$. So, $(1, 1)$ has order nm, so generates $\mathbb{Z}_n \times \mathbb{Z}_m$, and so this group is cyclic, $\cong \mathbb{Z}_{nm}$.

Since $\mathrm{lcm}(n, m) = nm$, the subgroups $\langle n \rangle$ and $\langle m \rangle$ of $\mathbb{Z}_{nm}$ have trivial intersection. Thus, $\mathbb{Z}_{nm} = \langle n \rangle \times \langle m \rangle$ by ④ and ⑥ from subsection 5.1.2 (and ① of course). ∎

6.1.2. 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 $c = a \bmod n$ and $c = b \bmod m$.*

The theorem says that the homomorphism $\mathbb{Z} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$, $c \mapsto (c \bmod n, c \bmod m)$, 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 $\mathbb{Z}_{nm} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$; since the orders of these groups are equal, this homomorphism is an isomorphism.

6.1.3. 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 $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$.

6.1.4. We also have the following corollary of Theorem 6.1.1:

Lemma. *If elements a and b of a group commute and their orders $n = |a|$ and $m = |b|$ are coprime, then $|ab| = nm$, and $\langle a, b \rangle \cong \mathbb{Z}_{nm}$.*

Proof. Since the orders of the groups $\langle a \rangle$ and $\langle b \rangle$ are coprime, we have $\langle a \rangle \cap \langle b \rangle = 1$, and so $\langle a, b \rangle = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$, with the element ab being the generator of this group. ∎

6.1.5. In the case the orders of a and b are not coprime the situation is more complicated, since $\langle a \rangle \cap \langle b \rangle$ may not be trivial, in which case $\langle a, b \rangle$ is not direct but a central product of $\langle a \rangle$ and $\langle b \rangle$. We will need a special case when $|b| \mid |a|$:

Lemma. *Let elements a and b of a group commute and assume that $m = |b|$ divides $n = |a|$. Let $\big|\langle a \rangle \cap \langle b \rangle\big| = d$; then $\langle a, b \rangle = \langle a \rangle \times \langle c \rangle$ where $c = ba^k$ for some k. and so, $\cong \mathbb{Z}_n \times \mathbb{Z}_{m/d}$.*

Proof. Let $G = \langle a, b \rangle$, then G is commutative, $G = \langle a \rangle *_N \langle b \rangle$ where $N = \langle a \rangle \cap \langle b \rangle \cong \mathbb{Z}_d$, and $|G| = nm/d$. We have $d \bigm| n, m$; let $n = dn'$ and $m = dm'$. The order of (the image) of b in G/N is m', so $b^{m'} \in \langle a \rangle \cap \langle b \rangle$, so $b^{m'} = a^l$ for some l. Since $a^l \in N$, $a^{ld} = 1$, so $n \bigm| ld$, so $n' \bigm| l$, and by our assumption, $m' \bigm| n'$, so $m' \bigm| l$. Put $c = a^{-l/m'}b$, then $\langle a, c \rangle = G$. Since $c^{m'} = a^{-l}b^{m'} = 1$, $|c| \leq m'$; so, $|G| = nm/d = nm' \geq |a| \cdot |c|$, so $|c| = m'$ and $G = \langle a \rangle \times \langle c \rangle \cong \mathbb{Z}_n \times \mathbb{Z}_{m'}$. ■

6.2. The classification of finite abelian groups

6.2.1. 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 $|a_m| \bigm| |a_{m-1}| \bigm| \cdots \bigm| |a_2| \bigm| |a_1|$.*

Proof. Let a_1 be an element of G having the maximal order; let $n_1 = |a_1|$. I claim that for any $b \in G$, $|b| \bigm| n_1$. Indeed, assume that $|b| = k \nmid n_1$, let p be a prime such that $n = p^r n_1'$, $k = p^s k'$ with $s > r$ and $p \nmid n_1', k'$. Then by Lemma 6.1.4, the element $a_1^{p^r} b^{k'}$ has order $p^s n_1' > n_1$, contradiction.

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 $\pi : G \longrightarrow K$ has a section $\sigma : K \longrightarrow G$; this will imply that $G = H_1 \times H_2 \times \cdots \times H_k$, where $H_i = \sigma(K_i)$. We have

$$K = \Big\langle c_2, \ldots, c_m \,\Big|\, c_i c_j = c_j c_i \text{ for all } i, j \text{ and } c_i^{n_i} = 1 \text{ for all } i \Big\rangle.$$

To construct σ, 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 π.

We can choose a_i independently for distinct i. Fix i, and let $b_i \in G$ be such that $\pi(b_i) = c_i$. The group $\pi^{-1}(K_i) = \langle a_1, b_i \rangle$ has order $n_1 n_i$ and is a central product of $\langle a_1 \rangle \cong \mathbb{Z}_{n_1}$ and $\langle b_i \rangle \cong \mathbb{Z}_{n_i}$; since, as we know, $|b_i| \bigm| |a_1|$, by Lemma 6.1.5, $\langle a_1, b_i \rangle = \langle a_1 \rangle \times \langle a_i \rangle$ for some a_i of order n_i and with $\pi(a_i) = \pi(b_i) = c_i$.

We also have that $|a_i| = n_i \bigm| n_1 = |a_1|$ for $i = 2, \ldots, m$, and by induction, $|c_m| \bigm| |c_{m-1}| \bigm| \cdots \bigm| |c_2|$. Since $|a_i| = n_i = |c_i|$ for all i, we have $|a_m| \bigm| |a_{m-1}| \bigm| \cdots \bigm| |a_2| \bigm| |a_1|$. ■

6.2.2. 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 $n_m \bigm| n_{m-1} \bigm| \cdots n_2 \bigm| n_1$. The integers $n_1, \ldots, n_m$ are called *the invariant factors* of G.

Since, by 6.1.3, 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.

6.2.3. 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 divisors 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

$$p_1^{r_{1,1}}, \ldots, p_1^{r_{1,m_1}},\ p_2^{r_{2,1}}, \ldots, p_2^{r_{2,m_2}},\ \ldots,\ p_k^{r_{k,1}}, \ldots, p_k^{r_{k,m_k}},$$

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 $n_m \bigm| n_{m-1} \bigm| \cdots \bigm| n_2 \bigm| n_1$, namely,

$$n_1 = p_1^{r_{1,1}} \cdots p_k^{r_{k,1}},\ n_2 = p_1^{r_{1,2}} \cdots p_k^{r_{k,2}},\ \ldots,\quad n_m = p_1^{r_{1,m}} \cdots p_k^{r_{k,m}},$$

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

6.2.4. 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 $2^3, 3^2, 5, 2^3, 3, 2^2, 5^2, 2, 3$, so that $G \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

Reorder the elementary divisors, grouping, in descending order, those associated with the same prime: $2^3, 2^3, 2^2, 2;\ 3^2, 3, 3;\ 5^2, 5$. 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 $G \cong \mathbb{Z}_{1800} \times \mathbb{Z}_{120} \times \mathbb{Z}_{12} \times \mathbb{Z}_2$.

6.2.5. 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
$$G \cong \big(\mathbb{Z}_{p_1^{r_{1,1}}} \times \cdots \times \mathbb{Z}_{p_1^{r_{1,m_1}}}\big) \times \cdots \times \big(\mathbb{Z}_{p_k^{r_{k,1}}} \times \cdots \times \mathbb{Z}_{p_k^{r_{k,m_k}}}\big),$$
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 $e(G, p_i^s) = p_i^v$, where
$$v = \sum_{\substack{1 \leq j \leq m_i \\ r_{i,j} < s}} r_{i,j} + \#\big\{j : r_{i,j} \geq s\big\} \cdot s.$$
For every i and $s \in \mathbb{N}$ we therefore have
$$\begin{aligned}
&\log_{p_i} e(G, p_i^s) - \log_{p_i} e(G, p_i^{s-1}) \\
&\quad = \sum_{\substack{1 \leq j \leq m_i \\ r_{i,j} < s}} r_{i,j} - \sum_{\substack{1 \leq j \leq m_i \\ r_{i,j} < s-1}} r_{i,j} + \#\big\{j : r_{i,j} \geq s\big\} \cdot s - \#\big\{j : r_{i,j} \geq s-1\big\} \cdot (s-1) \\
&\quad = \#\big\{j : r_{i,j} = s-1\big\} \cdot (s-1) - \#\big\{j : r_{i,j} = s-1\big\} \cdot (s-1) + \#\big\{j : r_{i,j} \geq s\big\} = \#\big\{j : r_{i,j} \geq s\big\}.
\end{aligned}$$
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. ■

6.3. 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.

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

Proof. Let $n_m \mid \cdots \mid n_1$ 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 $\mathbb{Z}_p^* \cong \mathbb{Z}_{n_1}$. ■

6.3.2. 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 $\mathbb{Z}_{p^{r-1}(p-1)}$). For any $r \geq 2$, $\mathbb{Z}_{2^r}^* \cong \mathbb{Z}_{2^{r-2}} \times \mathbb{Z}_2$.*

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 $\mathbb{Z}_{p^r} \longrightarrow \mathbb{Z}_{p^r}/\langle p\rangle \cong \mathbb{Z}_p$ is a homomorphism of the multiplicative groups as well, and induces a surjective homomorphism $\pi\colon \mathbb{Z}_{p^r}^* \longrightarrow \mathbb{Z}_p^*$. 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 6.3.1, 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 $\mathbb{Z}_{2^r}^* \cong \mathbb{Z}_{2^{r-2}} \times \mathbb{Z}_2$. ■

6.3.3. Lemma. *Let $n = p_1^{r_1} \cdots p_k^{r_k}$ 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 $\varphi\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$, appearing in the Chinese remainder theorem, is multiplicative ($\varphi(ab) = \varphi(a)\varphi(b)$), and induces an isomorphism of the multiplicative groups $\mathbb{Z}_n^* \longrightarrow \mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^*$. ■

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

$$\mathbb{Z}^*_{7200} \cong \mathbb{Z}^*_{5^2} \times \mathbb{Z}^*_{3^2} \times \mathbb{Z}^*_{2^5} \cong \mathbb{Z}_{5\cdot4} \times \mathbb{Z}_{3\cdot2} \times \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_2 \cong \mathbb{Z}_{120} \times \mathbb{Z}_4 \times \mathbb{Z}_2^2.$$

---

7. Groups of automorphisms and semidirect products of groups

7.1. Groups of automorphisms

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

7.1.2. If a group G is presented by generators and relations, $G = \langle S \,|\, R\rangle$, then any automorphism φ 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 φ to be an automorphism; if G is infinite, it should also be checked that φ is injective.

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

(ii) $\mathrm{Aut}(\mathbb{Q}) \cong \mathbb{Q}^*$: 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) $\mathrm{Aut}(V_4) \cong S_3$: automorphisms of $V_4 = \{1, a, b, c\}$ act as permutations of the set $\{a, b, c\}$.

(iv) For any n, $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}^*_n$. Indeed, any automorphism φ 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 $\varphi_{k_1}\varphi_{k_2} = \varphi_{k_1k_2}$.

(v) Let $n \geq 3$. Any automorphism of the dihedral group $D_{2n} = \langle r, s \,|\, r^n = s^2 = 1,\ rs = sr^{-1}\rangle$ 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, $\mathrm{Aut}(D_{2n}) = \big\{\varphi_{k,l},\ k \in \mathbb{Z}^*_n,\ l \in \mathbb{Z}_n\big\}$, where $\varphi_{k,l}$ are defined by $\varphi_{k,l}(r) = r^k$, $\varphi_{k,l}(s) = sr^l$. The multiplication on $\mathrm{Aut}(D_{2n})$ is defined by $\varphi_{k_1,l_1}\varphi_{k_2,l_2} = \varphi_{k_1k_2,l_1+k_1l_2}$.

(vi) $\mathrm{Aut}(Q_8) \cong S_4$. It is easy to find all automorphisms of Q_8 and construct the multiplication table of $\mathrm{Aut}(Q_8)$; but it is not immediately clear that this group is actually isomorphic to S_4. One can show however that $\mathrm{Aut}(Q_8)$ is isomorphic to the group of rotations of a cube, which, in its turn, is known to be isomorphic to S_4.

7.1.4. 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 $\mathrm{Aut}(G)$ denoted by $\mathrm{Inn}(G)$.

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

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

7.1.6. Examples. (i) For any abelian group G, $\mathrm{Inn}(G) = 1$ and so, $\mathrm{Out}(G) = \mathrm{Aut}(G)$ (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, $\mathrm{Inn}(D_{2n}) \cong D_{2n}$ if n is odd and $\cong D_{2n}/\langle r^{n/2}\rangle \cong D_n$ if n is even. For all $n > 3$ this is a proper subgroup of $\mathrm{Aut}(D_{2n})$.

(iii) $Z(Q_8) = \{1, -1\}$, so $\mathrm{Inn}(Q_8) \cong Q_8/\{\pm1\} \cong V_4$. So, $\mathrm{Inn}(Q_8)$ is a normal subgroup, isomorphic to V_4, in $\mathrm{Aut}(Q_8) \cong S_4$. (There is only one such.)

(iv) All automorphisms of S_n are inner, $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$, 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 $\mathrm{Out}(S_6) \cong \mathbb{Z}_2$.

7.2. Characteristic subgroups

7.2.1. A subgroup H of a group G is said to be *characteristic* if $\varphi(H) = H$ for all $\varphi \in \mathrm{Aut}(G)$; this is denoted by "$H$ char G".

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

(ii) Every subgroup of $\mathbb{Z}$ and of $\mathbb{Z}_n$, 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 expresssions of the form ..." is characteristic in G; such are the subgroup $\big\langle a^n,\ a \in G \big\rangle$, for any $n \in \mathbb{N}$, and *the commutator*, or *the derived*, subgroup $G_2 = [G,G] = \big\langle [a,b],\ a,b \in G \big\rangle$ (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 $\big\langle a : a^n = 1 \big\rangle$, for any $n \in \mathbb{N}$, and the center $Z(G) = \big\{ a \in G : ab = ba \text{ for all } b \in G \big\}$ of G.

7.2.3. 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 $H \trianglelefteq G$.*

7.3. Semidirect product of groups

7.3.1. 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 $\varphi\colon G \longrightarrow \mathrm{Aut}(H)$, $\varphi(a) = \varphi_a$, with $\ker\varphi = C_G(H)$ (the centralizer of H in G).

7.3.2. 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 $G = H \rtimes K$.

7.3.3. If $G = H \rtimes K$, then, similarly to 5.1.2,
① for any $h \in H$ and $k \in K$, $kh = h'k$, where $h' = khk^{-1} \in H$;
② H is normal in G;
③ $HK = G$;
④ $H \cap K = 1$;
⑤ every element $a \in G$ is uniquely representable in the form $a = hk$ with $h \in H$ and $k \in K$;
⑥ if $|G| < \infty$, then $|G| = |H| \cdot |K|$;
⑦ For the factorization mapping $\pi\colon G \longrightarrow {}_H\backslash G$ (to the set of right cosets of H), the restriction $\pi|_K$ is a bijection between K and ${}_H\backslash G$.

(The only difference with 5.1.2 is that now only one of the subgroups, H, is normal in G, not both). And, exactly as in Proposition 5.1.7, ①&③$\Longrightarrow$②; ②&④$\Longrightarrow$①; ⑤$\Longleftrightarrow$③&④; ⑦$\Longleftrightarrow$③&④; and if $|G| < \infty$, ⑤$\Longrightarrow$⑥; ③&⑥$\Longrightarrow$④; ④&⑥$\Longrightarrow$③. As a corollary we get that for $G = H \rtimes K$ it suffices if any of the following combinations of conditions holds: ①&③&④, ②&③&④, ①&⑤, ②&⑤, ②&⑦, and if $|G| < \infty$, ①&③&⑥, ①&④&⑥, ②&③&⑥, ②&④&⑥.

The properties ②, ③, and ④ together are described by the diagram

$$\begin{array}{ccc} & HK = G & \\ /\!\!/ & & \backslash \\ H & & K \\ \backslash\!\!\backslash & & /\!\!/ \\ & H \cap K = 1 & \end{array}$$

Thus, if we have such a diagram of subgroups in G, then $G = H \rtimes K$.

7.3.4. Also, as in Proposition 5.1.10, the fact that ②&⑦ imply that G is a semidirect product can be reformulated in the following way:

Proposition. *Let $H \trianglelefteq G$, $K = G/H$, and assume that the factorization homomorphism $G \longrightarrow K$ has a section $\sigma\colon K \longrightarrow G$. Then $G = H \rtimes \sigma(K)$.*

7.3.5. 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 τ is any transposition from S_n.
(iv) Let G be the group of nonconstant affine functions $\mathbb{R} \longrightarrow \mathbb{R}$, $G = \big\{ f(x) = ax + b,\ a \in \mathbb{R}^*,\ b \in \mathbb{R} \big\}$, with the operation of composition. Let $H = \{h_b(x) = x + b,\ b \in \mathbb{R}\} \cong \mathbb{R}$, $K = \big\{ k_a(x) = ax,\ a \in \mathbb{R}^* \big\} \cong \mathbb{R}^*$. Then $G = H \rtimes K$, with $k_a h_b k_a^{-1} = h_{ab}$.

7.3.6. If $G = H \rtimes K$, then K acts on H by conjugations, which induces a homomorphism $\varphi: K \longrightarrow \mathrm{Aut}(H)$: 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 thus by homomorphism φ: for $h \in H$ and $k \in K$, $kh = (khk^{-1})k = \varphi_k(h)k$.

7.3.7. Given two groups H and K, it turns out that any homomorphism $\varphi: K \longrightarrow \mathrm{Aut}(H)$, $\varphi(k) = \varphi_k \in \mathrm{Aut}(H)$, $k \in K$, leads to a semidirect product of H and K. Indeed, put $G = H \times K$ as a set, that is, $G = \big\{(h,k),\ h \in H, k \in K\big\}$, and define multiplication on G by

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

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

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

7.3.8. Examples. (i) Let $K = \{1, a\} \cong \mathbb{Z}_2$. For any abelian group H we have a homomorphism $\varphi: K \longrightarrow \mathrm{Aut}(H)$ defined by $\varphi_a(h) = h^{-1}$, $h \in H$. This gives as the semidirect product $G = H \rtimes_\varphi K$, 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 $\mathrm{Aut}(H) = \{\psi_1 = 1, \psi_3, \psi_5, \psi_7\} \cong V_4$, where $\psi_k(a) = a^k$. Let $K = \{1, b\} \cong \mathbb{Z}_2$; there are 4 homomorphisms $K \longrightarrow \mathrm{Aut}(H)$, that map b to any of the elements of $\mathrm{Aut}(H)$, $\varphi_k(b) = \psi_k$, $k = 1, 3, 5, 7$. We then have

$$\begin{aligned}
&H \rtimes_{\varphi_1} K = H \times K = \big\langle a, b \,|\, a^8 = b^2 = 1,\ ba = ab\big\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2;\\
&H \rtimes_{\varphi_3} K = \big\langle a, b \,|\, a^8 = b^2 = 1,\ ba = a^3b\big\rangle, \text{ called } \textit{the quasidihedral group } QD_{16} \text{ (or } SD_{16});\\
&H \rtimes_{\varphi_3} K = \big\langle a, b \,|\, a^8 = b^2 = 1,\ ba = a^5b\big\rangle, \text{ called } \textit{the modular group } M_{16};\\
&H \rtimes_{\varphi_3} K = \big\langle a, b \,|\, a^8 = b^2 = 1,\ ba = a^7b\big\rangle \cong D_{16}.
\end{aligned}$$

(The group, say $\big\langle a, b \,|\, a^8 = b^2 = 1,\ ba = a^2b\big\rangle$ also exists, of course, but it has "hidden" relations: we have $a = b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^2b^{-1} = a^4$, so $a^3 = 1$, so $a = a^9a^{-8} = 1$. 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 $\mathbb{Z}_n \rtimes \mathbb{Z}_m$, one needs a nontrivial homomorphism $\mathbb{Z}_m \longrightarrow \mathbb{Z}_n^*$; 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 $\mathbb{Z}_q \rtimes \mathbb{Z}_p$ exists iff $p \,\big|\, (q-1)$. 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 $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ exists; to construct it, we find an element of order 3 in $\mathbb{Z}_7^*$, which is 2 (and 4), and define (in multiplicative terms) $G = \big\langle a, b \,|\, a^7 = b^3 = 1,\ bab^{-1} = a^2\big\rangle$.

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

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

7.3.10. Example. For any n, $\mathrm{Hol}(\mathbb{Z}_n) = \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ with multiplication $(l_1, k_1)(l_2, k_2) = \big(l_1 + k_1l_2, k_1k_2\big)$. (Notice that this group is isomorphic to the group $\mathrm{Aut}(D_n)$; see 7.1.3(v).)

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

Lemma. *Let H and K be groups, let $\varphi_1, \varphi_2: K \longrightarrow \mathrm{Aut}(H)$ be homomorphisms, and assume that $\varphi_2 = \varphi_1 \circ \rho$ for some $\rho \in \mathrm{Aut}(K)$. Then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.*

(The isomorphism is given by $(h,k) \mapsto (h, \rho^{-1}(k))$.)

7.3.12. Lemma. *Let H and K be groups, let $\varphi_1, \varphi_2 : K \longrightarrow \mathrm{Aut}(H)$ be homomorphisms, and assume that φ_2 and φ_1 are conjugate: there is $\psi \in \mathrm{Aut}(H)$ 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 is given by $(h, k) \mapsto (\psi(h), k)$.)

7.3.13. Lemma. *Let H be a group, K be a cyclic group, and let $\varphi_1, \varphi_2 : K \longrightarrow \mathrm{Aut}(H)$ be homomorphisms such that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$; if $|K| = \infty$, assume additionally that φ_i are injective. Then $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.*

(The isomorphism is defined by $(h, k) \mapsto (\psi(h), k^r)$ where $\psi \in \mathrm{Aut}(H)$ is such that $\psi\varphi_1(K)\psi^{-1} = \varphi_2(K)$ and $r \in \mathbb{Z}_n^*$ if $K \cong \mathbb{Z}_n$, or $r = \pm 1$ if $K \cong \mathbb{Z}$, is such that $\varphi_2(c^r) = \psi\varphi_1(c)\psi^{-1}$ where c is a generator of K.)

---

8. Sylow theorems and groups of small orders

8.1. p-groups

Let p be a prime.

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

8.1.2. Example. The groups Q_8, D_8, M_{16}, QD_{16}, $\mathbb{Z}_{16}$ and $\mathbb{Z}_4 \times \mathbb{Z}_4$ are 2-groups.

8.1.3. 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 $H_2 \subseteq N_G(H_1)$, then also the join H_1H_2 is a p-group.

8.1.4. For any r, the abelian p-group $\mathbb{Z}_{p^r}$ "is made of" r groups isomorphic to $\mathbb{Z}_p$: its composition series is $0 \trianglelefteq \langle p^{r-1}\rangle \trianglelefteq \langle p^{r-2}\rangle \trianglelefteq \cdots \trianglelefteq \langle p\rangle \trianglelefteq \langle 1\rangle = \mathbb{Z}_{p^r}$, with $\langle p^k\rangle \cong \mathbb{Z}_{p^{r-k}}$ and $\langle p^k\rangle/\langle p^k\rangle \cong \mathbb{Z}_p$ for all k.

8.1.5. Lemma. *If G is a p-group, then $Z(G) \neq 1$.*

Proof. 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 $p \,\big|\, |G|$ 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. ■

8.1.6. 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

$$1 \trianglelefteq G^{(1)} \trianglelefteq G^{(2)} \trianglelefteq \cdots \trianglelefteq G^{(d)} = G \tag{8.1}$$

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* (see 9.3); so, we've just proved that p-groups are nilpotent. Since the factors of (8.1) are abelian p-groups, it follows from 8.1.4 that "G is made of cyclic groups of order p": all factors of the composition series of G are isomorphic to $\mathbb{Z}_p$.

8.2. Sylow's theorems

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

8.2.1. 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 $p \not| m$. Then:*

(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^r; these maximal p-subgroups of G are called *Sylow p-subgroups*. The set of Sylow p-subgroups in G is denoted by $\mathrm{Syl}_p(G)$.

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

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

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

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

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

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

(ii) Let $s < r$, $H \leq G$, $|H| = p^s$. I claim that $p^{s+1} \mid |N_G(H)|$. Indeed, assume that this is not so. Let $\mathcal{H}$ be the conjugacy class of H; since $p^r \nmid |N_G(H)|$ and $|\mathcal{H}| = |G|/|N_G(H)|$, we have $p \mid |\mathcal{H}|$. 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 $L' = HH'$ is a p-subgroup with $p^{s+1} \mid |L'|$, and $H' \trianglelefteq L'$. Let $a \in G$ be such that $aH'a^{-1} = H$, put $L = aL'a^{-1}$; then $H \trianglelefteq L$ so $L \leq N_G(H)$, and $p^{s+1} \mid |L|$, which contradicts the assumption that $p^{s+1} \nmid |N_G(H)|$.

It follows that $p \mid |N_G(H)/H|$. Let $\widetilde{K}$ 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 $H \trianglelefteq K$.

(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 KH' is a p-subgroup of G containing both K and H'. But K and H' are maximal p-subgroups of G, so $K = KH' = H'$, 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 HK would be a p-group larger than K), so has cardinality divisible by p. Hence, $n_p = |\mathcal{H}| = 1 \bmod p$.

Finally, $n_p = |G|/|N_G(H)|$. Since $N_G(H) \geq H$, $|N_G(H)| = p^r l$ for some l, so $n_p = m/l$. ■

8.2.2. 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.

8.2.3. Let G be a finite group with $|G| = p_1^{r_1} p_2^{r_2}$, and let $P_1 \in \mathrm{Syl}_{p_1}(G)$, $P_2 \in \mathrm{Syl}_{p_2}(G)$; 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 $n_{p_1} = 1$, then $G = P_1 \rtimes P_2$.

8.2.4. Now let G be a finite group with $|G| = p_1^{r_1} \cdots p_k^{r_k}$, and let $P_i \in \mathrm{Syl}_{p_i}(G)$, $i = 1, \dots, k$. Then $|P_1| \cdots |P_k| = |G|$ and $P_i \cap P_j = 1$ for any $i \neq j$. Moreover, if for some $i_1, \dots, i_l$ the product $H = P_{i_1} \cdots P_{i_l}$ is a group, then for any $j \notin \{i_1, \dots, i_l\}$, $P_j \cap H = 1$. 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 $i = 1, \dots, k-1$, then $G = (P_1 \times \cdots \times P_{k-1}) \rtimes P_k$.

8.2.5. Example. Let G be a group of order $6 = 2 \cdot 3$, let $P \in \mathrm{Syl}_2(G)$ and $Q \in \mathrm{Syl}_3(G)$. We have $n_3 = 1 \bmod 3$ and $n_3 \mid 2$; 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 $G = P \rtimes Q \cong \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2$, where φ is a nontrivial homomorpshim $\mathbb{Z}_2 \longrightarrow \mathrm{Aut}(\mathbb{Z}_3) = \mathbb{Z}_3^*$. There is only one such homomorphism, namely, $1 \mapsto (1 \leftrightarrow 2)$, and G has a presentation $\langle a, b \mid a^3 = b^2 = 1,\ bab^{-1} = a^{-1} \rangle$. 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.

8.2.6. Example. Let G be a group of order $12 = 2^2 \cdot 3$, let $P \in \mathrm{Syl}_2(G)$ and $Q \in \mathrm{Syl}_3(G)$; 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 $n_3 = 1$ and $n_2 \neq 1$, then $G = Q \rtimes P$, which product is induced by a homomorphism $P \longrightarrow \mathrm{Aut}(Q) \cong \mathbb{Z}_2$. If $P \cong \mathbb{Z}_4$, we have a unique such homomorphism, which gives us the group

$$\big\langle a, b \,|\, a^3 = b^4 = 1,\ bab^{-1} = a^2 \big\rangle \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_4.$$

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

$$\big\langle a, b, c \,|\, a^3 = b^2 = c^2 = 1,\ bc = cb, bab = a^2,\ cac = a \big\rangle \cong \mathbb{Z}_3 \rtimes V_4.$$

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 $Q \longrightarrow \mathrm{Aut}(P)$. There is no nontrivial homomorphism $\mathbb{Z}_3 \longrightarrow \mathrm{Aut}(\mathbb{Z}_4^*) \cong \mathbb{Z}_2$, but there is such $\mathbb{Z}_3 \longrightarrow \mathrm{Aut}(V_4) \cong S_3$, which maps the generator of $\mathbb{Z}_3$ to a cyclic permutation of the elements of V_4; the group obtained thereby is

$$\big\langle a, b, c \,|\, a^2 = b^2 = c^3 = 1,\ ab = ba,\ cac^{-1} = b,\ cbc^{-1} = ab \big\rangle \cong V_4 \rtimes \mathbb{Z}_3.$$

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

the group of rotations of a tetrahedron has 4 subgroups of order 3, so it is isomorphic to $V_4 \rtimes \mathbb{Z}_3 \cong A_4$ (which is, actually, clear since it acts as A_4 on the set of vertices of the tetrahedron).

8.2.7. It is interesting that the normalizer of a Sylow subgroup is always *a self-normalizing* subgroup:

Proposition. *If P is a Sylow subgroup of a finite group G, Then $N_G(N_G(P)) = N_G(P)$.*

Proof. P is a normal Sylow's subgroup of $N_G(P)$, so P char $N_G(P)$. Since also $N_G(P) \trianglelefteq N_G(N_G(P))$, we have $P \trianglelefteq N_G(N_G(P))$, so $N_G(N_G(P)) \leq N_G(P)$. ■

8.2.8. If H is a subgroup of a finite group G and $P \in \mathrm{Syl}_p(G)$, then $P \cap H$ doesn't have to be a Sylow p-subgroup of H. However, every Sylow p-subgroup Q of H is a p-group and so, $Q \leq P'$ for some $P' \in \mathrm{Syl}_p(G)$, and then $Q = P' \cap H$. It follows that $n_p(H) \leq n_p(G)$.

It also follows that for any $P \in \mathrm{Syl}_p(G)$, $(aPa^{-1}) \cap H \in \mathrm{Syl}_p(H)$ for some $a \in G$.

8.2.9. Let $H \trianglelefteq G$; in this case we have $P \cap H \in \mathrm{Syl}_p(H)$ for any $P \in \mathrm{Syl}_p(G)$, and $n_p(H) \bigm| n_p(G)$. Indeed, let $a \in G$ be such that $(aPa^{-1}) \cap H = Q \in \mathrm{Syl}_p(H)$; then $a^{-1}Qa \in \mathrm{Syl}_p(H)$ either. But $a^{-1}Qa = a^{-1}\big((aPa^{-1}) \cap H\big)a = P \cap a^{-1}Ha = P \cap H$.

And for any $Q, Q' \in \mathrm{Syl}_p(H)$, the sets $S_Q = \{P \in G : P \cap H = Q\}$ and $S_{Q'} = \{P \in G : P \cap H = Q'\}$ are conjugate: $S_{Q'} = aS_Qa^{-1}$ for $a \in H$ such that $Q' = aQa^{-1}$. Hence $|S_Q| = |S_{Q'}|$, which implies that $n_p(H) \bigm| n_p(G)$.

8.2.10. Now let $N \trianglelefteq G$, $H = G/N$, and $\varphi\colon G \longrightarrow H$ be the projection homomorphism. Let $P \in \mathrm{Syl}_p(G)$, then $Q = \varphi(P)$ is a p-subgroup of H. Let $|G| = p^r m$ and $|N| = p^s k$ where $p \nmid m, k$, then $|H| = p^{r-s}m/k$. We have $|Q| = |NP|/|N| = p^{r-s}l$ for some l; hence, $Q \in \mathrm{Syl}_p(H)$. Conversely, for any $Q \in \mathrm{Syl}_p(H)$, the group $\widetilde{Q} = \varphi^{-1}(Q)$ has order $p^r k$, so any Sylow p-subgroup P of $\widetilde{Q}$ is a Sylow p-subgroup of G with $\varphi(P) = Q$.

It follows that $n_p(H) \leq n_p(G)$. Moreover, $n_p(H) \bigm| n_p(G)$. Indeed, the set $\mathrm{Syl}_p(G)$ is partitioned into sets $S_Q = \{P : \varphi(P) = Q\}$, $Q \in \mathrm{Syl}_p(H)$. For every $Q \in \mathrm{Syl}_p(H)$ we have $S_Q = \mathrm{Syl}_p(\varphi^{-1}(Q))$, and since all subgroups Q from $\mathrm{Syl}_p(H)$ are conjugate, we have that the subgroups $\varphi^{-1}(Q)$ are all conjugate, and so, all have the same number of Sylow p-subgroups.

8.3. Groups of small orders

(More exactly, groups whose orders have ≤ 3 factors.)

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

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

8.3.2. 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 6.3.1. 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 4.2.7, 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 $Z(G) = \{1, a^2\}$. 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 $ba = aba^2 = a^3b$. If $|b| = 2$, we have $G = \big\langle a, b \,|\, a^4 = b^2 = 1,\ ba = a^3b \big\rangle \cong D_8$. If $|b| = 4$, then $b^2 = a^2$, and we have $G = \big\langle a, b \,|\, a^4 = 1,\ b^2 = a^2,\ ba = a^3b \big\rangle \cong Q_8$. ■

Claim. *If $p \geq 3$, then G is isomorphic to one of the following two groups:*

$$\big\langle a, b, c \,|\, a^p = b^p = c^p = 1,\ ba = ab,\ ca = ac,\ cb = abc \big\rangle \cong \mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$$

or

$$\big\langle a, b \,|\, a^{p^2} = b^p = 1,\ ba = a^{p+1}b \big\rangle \cong \mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p.$$

Proof. Assume that $|g| = p$ for all $g \in G$. Let $a, b \in G$ generate G modulo $Z(G)$. a, b don't commute (since otherwise G is abelian); but a, b commute modulo $Z(G)$, so $ba = abc$ where c is a generator of $Z(G) \cong \mathbb{Z}_p$. We then have $\big\langle a, b, c \,|\, a^p = b^p = c^p = 1,\ ac = ca,\ bc = cb,\ ba = abc \big\rangle \cong \mathbb{Z}_p^2 \rtimes \mathbb{Z}_p$.

Now assume that there is $a \in G$ 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 $r \neq 0 \bmod p$. Assume that $|b| = p^2$, then $b^p \in Z(G)$ so $b^p = a^{pk}$ for some k. We then have $(ba^{-k})^p = b^p a^{-kp} c^{-krp(p-1)/2} = 1$ since $c^p = 1$; after replacing b by ba^{-k} we have $|b| = p$. Finally, replacing b by b^s where s is such that $sr = 1 \bmod p$, we get $ba = abc$. Hence, $\big\langle a, b \,|\, a^{p^2} = b^p = 1,\ ba = a^{p+1}b \big\rangle \cong \mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p$. ■

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

8.3.3. Let G be a group of order pq where p and q are prime with $p < q$. If $q \neq 1 \bmod p$, then $G \cong \mathbb{Z}_{pq}$. If $q = 1 \bmod p$, 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 $\big\langle a, b \,|\, a^q = b^p = 1,\ bab^{-1} = a^k \big\rangle$ where k is any element of order p in $\mathbb{Z}_q^*$; all these groups, corresponding to distinct k, are isomorphic. (Indeed, by Lemma 6.3.1, $\mathbb{Z}_q^*$ is cyclic, so it has a single subgroup of order p, and Lemma 7.3.13 applies.)

8.3.4. 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 $G = Q \rtimes P$ where $|Q| = q^k$ and $P \cong \mathbb{Z}_p$.

8.3.5. Let G be a group of order p^2q where p, q are prime with $p < q$. If $n_q = 1$, then $G = Q \rtimes P$ where $Q \cong \mathbb{Z}_q$ and $P \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p^2$, which semidirect products may only be nontrivial if $p \,\big|\, (q-1)$. If $n_q \neq 1$, then $n_q = p^2 = 1 \bmod q$, so $q \,\big|\, (p-1)(p+1)$, which only holds for $p = 2$, $q = 3$, so $|G| = 12$, and $G \cong A_4$ by 8.2.6.

8.3.6. By a *Burnside theorem*, if the order of G has only two prime factors (that is, $|G| = p^k q^l$ 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 $\mathbb{Z}_q$.

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

Claim. $n_r = 1$.

Proof. Assume that $n_r \neq 1$. Then $n_r = pq$ (which, by the way, is only possible if $pq = 1 \bmod r$), 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.

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 group; since $|H| = qr$, R is normal, and so, characteristic in H by 8.3.3. The index $|G : H| = p$ is the minimal prime divisor of G, so by Lemma 4.2.7, $H \trianglelefteq G$. Since $R \operatorname{char} H$, $R \trianglelefteq G$. ■

Let P, Q and R be Sylow p- q- and r-subgroups of G respectively. Since R is normal, $H = QR$ is a subgroup, of index p in G; so, H is normal in G, and $G = H \rtimes P$. And, $H = R \rtimes Q$.

8.3.8. By another *Burnside's theorem*, if the order of G is a square-free integer (that is, $|G| = p_1 \cdots p_k$ 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 $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_k}$.

8.3.9. The minimal positive integer which is not square-free and has ≥ 3 prime factors is $60 = 2^2 \cdot 3 \cdot 5$, and indeed, there exists a simple group of this order, namely, A_5. We can now show that all groups of order $n < 60$ are semidirect products of their Sylow subgroups, with only two exceptions – S_4 and groups of order 48. Indeed, we know that this is true for all groups of orders p^k, pq^k, p^2q, pqr where p, q and r are primes with $p < q < r$. The only problematic groups of order < 60 are those of orders $2^3 \cdot 3 = 24$, $2^3 \cdot 5 = 40$, $2^3 \cdot 7 = 56$, $2^4 \cdot 3 = 48$, and $2^2 \cdot 3^2 = 36$.

For $|G| = 40$ we have $n_5 = 1$. For $|G| = 56$ we have $n_7 = 1$ or 8; but if $n_7 = 8$, then G has $8 \cdot 6 = 48$ elements of order 7, and the remaining 8 elements may only form one subgroup of order 8, thus $n_2 = 1$.

Let $|G| = 24$; I'll show that if both $n_2, n_3 \neq 1$, then $G \cong S_4$. If $n_3 \neq 1$, then $n_3 = 4$. G acts by conjugations on the set $\mathrm{Syl}_3(G)$, which induces a homomorphism $\varphi\colon G \longrightarrow S_4$. If $\ker\varphi = 1$, then $G \cong S_4$; assume that $N = \ker\varphi \neq 1$. Since G acts transitively, $|G : N| \geq 4$, so $|N| \leq 6$. If $|N| = 6$ or 3, then N contains a Sylow 3-subgroup H, so $H \operatorname{char} N \lhd G$, so $H \lhd G$, which contradicts $n_3 \neq 1$. So, $|N| = 2$. Then $\varphi(G)$ is a subgroup of order 12 of S_4, and so, is A_4. A_4 contains a single subgroup V of order 4; for every Sylow 2-subgroup K of G we have $\varphi(K) = V$, so $K \leq \varphi^{-1}(V)$. But $|\varphi^{-1}(V)| = 8$, so $K = \varphi^{-1}(V)$ and so, $n_2 = 1$.

Now let $|G| = 36$; I'll show that if $n_3 \neq 1$, then $n_2 = 1$. Assume that $n_3 = 4$, and let $H \in \mathrm{Syl}_3(G)$; then G acts by conjugations on $\mathrm{Syl}_3(G)$, which induces a homomorphism $\varphi\colon G \longrightarrow S_4$. Let $N = \ker\varphi$; then $|N| \geq |G|/|S_4| = 3$. (This already proves that G is non-simple.) Since G acts transitively, we have $4 \bigm| |G : N|$, so $|N| = 9$ or 3. If $|N| = 9$, then N is a normal Sylow 3-subgroup, which contradicts $n_3 \neq 1$. So, $|N| = 3$, $|G/N| = 12$, and $G/N \cong \varphi(G) = A_4$. G acts on N by conjugations, and $N \cong \mathbb{Z}_3$ acts trivially, so G/N acts on N, which defines a homomorphism $A_{12} \longrightarrow \mathbb{Z}_3^* \cong \mathbb{Z}_2$. However, A_{12} has no subgroup of index 2, so this action is trivial. Hence, $N \leq Z(G)$. Let V be the subgroup of A_4 of order 4, let $W = \varphi^{-1}(V)$. Then W is a group of order 12: and thus is a semidirect product of N and a subgroup L of order 4 with $Z(W) \geq N$, so $W = N \times L$. Hence, W contains a single subgroup of order 4. But every Sylow 2-subgroup of G is contained in $\varphi^{-1}(V)$, so $n_2 = 1$.

Finally, let $|G| = 48$ with $n_2, n_3 \neq 1$; then $n_3 = 4$ or 16. If $n_3 = 16$, there are $16 \cdot 2 = 32$ elements of order 3 in G, and 16 remaning elements may only form a single subgroup of order 16, so $n_2 = 1$ in this case. Assume that $n_3 = 4$. As above, we have a homomorphism $\varphi\colon G \longrightarrow S_4$, with $N = \ker\varphi$ be a subgroup of order 2 or 4. (This already proves that G is non-simple.) If $|N| = 4$ then $\varphi(G) = A_4$, and then $n_2 = 1$. So, $|N| = 2$ and $\varphi(G) = S_4$. Also, N, being normal and of order 2, is contained in the center of G; since S_4 has trivial center, we have that $Z(G) = N$. (And, indeed, there is at least one such group: $S_4 \times \mathbb{Z}_2$.)

8.3.10. It is also 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 $\mathrm{Syl}_2(G)$ of cardinality n_2.

If $n_2 = 3$, we have a nontrivial homomorphism $G \longrightarrow S_3$, which has a nontrivial kernel, and G is not simple.

Now assume that $n_2 = 15$; we will use a "counting elements" method to exclude this case. We have $n_5 = 6$ and $n_3 = 4$ or 10. If $n_3 = 4$, then there is a nontrivial homomorphism $G \longrightarrow S_4$, with a nontrivial kernel; som $b_3 = 10$. Hence, 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 in G; a is contained in a Sylow 2-subgroup of G of order 4. If a commutes with an element b of order 3, then $\langle a, b\rangle \cong \mathbb{Z}_6$. 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 of 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 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 $\varphi\colon G \longrightarrow S_5$; then $\varphi(G)$ is a subgroup of order 60 and so of index 2 in S_5, thus $\varphi(G) = A_5$ and $G \cong A_5$. ■

8.4. Some simple methods for proving the non-simplicity of a finite group

Let G be a finite group, and let p be a prime divisor of $|G|$.

8.4.1. 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 help.

Examples. (i) If $|G| = 99825 = 3 \cdot 5^2 \cdot 11^3$, $n_{11} = 1$ since none of the integers $3, 5, 5^2, 3 \cdot 5, 3 \cdot 5^2$ equals 1 modulo 11.

(ii) Let $|G| = 351 = 3^3 \cdot 13$. 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 $n_3 = 1$.

8.4.2. If G contains a subgroup H of index k, then the action of G by left multiplications on the set G/H of cosets of H induces a nontrivial homomorphism $\varphi\colon G \longrightarrow S_k$. If $k \leq 4$, then even in the case φ is injective, G is isomorphic to a subgroup of a solvable group S_k with $k \leq 4$, so G is not simple. If $k \geq 5$ but $|G|$ doesn't divide $k!$, then φ is not injective, $\ker\varphi \neq 1$, and G is not simple. Moreover, if G is simple, then $\varphi(G)$ must be a subgroup of A_k, so $|G| = |\varphi(G)|$ must divide $k!/2$.

Example. Let $|G| = 30758 = 2 \cdot 7 \cdot 13^3$. A Sylow 13-subgroup of G has index 14, but $|G| \not| \, |14!/2|$ (since $13^3 \not| \, |14!/2|$), so G is not simple.

8.4.3. G acts on the set $\mathrm{Syl}_p(G)$ of cardinality n_p by conjugations, which induces a nontrivial homomorphism $\varphi\colon G \longrightarrow S_{n_p}$. If G is simple, then φ is injective and $\varphi(G) \leq A_{n_p}$. If $n_p \leq 4$, then S_{n_p} is solvable, and G is not simple. If $n_p \geq 5$, $|G|$ is not simple if $|G|$ does not divide $n_p!/2$, or if an element of G acts as an odd permutation.

Examples. (i) Let $|G| = 72 = 2^3 \cdot 3^2$. Since $n_3 = 1$ or 4, G is not simple.

(ii) Let $|G| = 11616 = 2^5 \cdot 3 \cdot 11^2$. If $n_{11} \neq 1$, then $n_{11} = 12$; but $11^2 \not| \, 12!/2$, so G is not simple.

(iii) Let G be a simple group of order $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, then $n_7 = 15$. Let $X = \mathrm{Syl}_7(G)$; the action of G on X by conjugations turns it into a subgroup of A_{15}. Let $P \in X$, $P \cong \mathbb{Z}_7$, and let $N = N_G(H)$; then $|N| = |G|/n_7 = 28$. We then have $P \trianglelefteq N$, $N = P \rtimes Q$ with $Q \cong \mathbb{Z}_4$ or V_4; since $\mathrm{Aut}(P) \cong \mathbb{Z}_6$ has only one element of order 2 and no elements of order 4, in any case there is $b \in Q$ of order 2 that centralizes P, $bab^{-1} = a$ for all $a \in P$. It follows from the proof of the last part of Sylow's theorem that the action of P on X has no fixed points except P itself, so $X \setminus \{P\}$ consists of two disjoint orbits, – two cycles of order 7. b is an element of order 2 that commutes with the action of P, so b must transpose these two orbits and is a product of 7 disjoint transpositions. But then b is an odd permutation, which contradicts our assumption that $G \leq A_{15}$.

8.4.4. Let $P \in \mathrm{Syl}_p(G)$, then $n_p = \big|G : N_G(P)\big|$, 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 with this structure.

Example. Let $|G| = 264 = 2^3 \cdot 3 \cdot 11$, 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 (we can show that) A_{12} has no subgroups isomorphic to $\mathbb{Z}_{22}$ or D_{22}.

8.4.5. 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 $|G| = 36015 = 7^4 \cdot 5 \cdot 3$. Let $P_1, P_2 \in \mathrm{Syl}_7(G)$, and let $H = P_1 \cap P_2$; then $|H| = |P_1| \cdot |P_2|/|P_1 P_2| \geq |P_1| \cdot |P_2|/|G| = 7^8/(7^4 \cdot 15) > 7^2$, so $|H| = 7^3$. Since H has index 7 in P_1 and P_2, by Lemma 4.2.7, $H \trianglelefteq P_1, P_2$, so $P_1, P_2 \leq N = N_G(H)$. So, $|N| \geq |P_1| \cdot |P_2|/|H| = 7^5 > |G|/3$. Hence, $|G : N| \leq 2$; it cannot be 2 since $2 \not| \, |G|$, so $G = N$, $H \triangleleft G$, and G is not simple.

---

9. Commutator calculus, solvable and nilpotent groups

9.1. Commutators and the derived subgroup

Let G be a group, finite or infinite.

9.1.1. 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 $[a, b] = 1$.

9.1.2. 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 $[a, b, c]$.

9.1.3. 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) $[a^{-1}, b] = [b, a]^{a^{-1}}$ for all $a, b \in G$;

(iv) $[ab, c] = [b, c]^a [a, c]$ for all $a, b, c \in G$ (which looks as a sort of "distributive law");

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

9.1.4. For two subsets $A, B \subseteq G$, their *commutator* $[A, B]$ is defined as the subgroup $\big\langle [a, b],\ a \in A,\ b \in B \big\rangle$ of G. We have $[A, B] = 1$ iff $ab = ba$ for all $a \in A$ and $b \in B$.

9.1.5. The group $G' = [G, G]$ is called *the derived subgroup* of G. G' is a characteristic subgroup of G; it is trivial iff G is abelian.

9.1.6. 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 $H \geq G'$.

9.1.7. If $\varphi\colon G \longrightarrow H$ is a group homomorphism, then $\varphi(G') \leq H'$, and if φ 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 π is the factorization mapping, then $K' = \pi(G')$.

9.2. Derived series and solvable groups

9.2.1. For a group G we define $G^{(1)} = G'$, $G'' = G^{(2)} = (G')'$, 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.

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

9.2.3. If a group G is solvable, then any subgroup and any quotient group of G are also solvable. Indeed, if $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$ is a subnormal series with abelian factors then for any $K \leq G$, $1 \trianglelefteq (H_1 \cap K) \trianglelefteq \cdots \trianglelefteq (H_{n-1} \cap K) \trianglelefteq K$ also has abelian factors (as $(H_i \cap K)/(H_{i-1} \cap K)$ is isomorphic to a subgroup of H_i/H_{i-1}), and for any $N \trianglelefteq G$ and $K = G/N$, with $\varphi: G \longrightarrow K$ being the factorization homomorphism, the series $1 \trianglelefteq \varphi(H_1) \trianglelefteq \cdots \trianglelefteq \varphi(H_{n-1}) \trianglelefteq K$ also has abelian factors (as $\varphi(H_i)/\varphi(H_{i-1})$ is isomorphic to a quotient group of H_i/H_{i-1}).

Conversely, if a group G has a normal subgroup H such that both H and $K = G/H$ are solvable, then G itself is solvable. Indeed, if $1 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H$ and $1 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_m = K$ are subnormal series with abelian factors, for each i let $\overline{K}_i$ be the preimage of K_i in G; then $\overline{K}_i/\overline{K}_{i-1} \cong K_i/K_{i-1}$ is abelian, and

$$1 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H \trianglelefteq \overline{K}_1 \trianglelefteq \cdots \trianglelefteq \overline{K}_m = G$$

is a subnormal series with abelian factors in G.

9.2.4. Lemma. *If a subnormal series $\cdots \trianglelefteq H_2 \trianglelefteq H_1 \trianglelefteq H_0 = G$ has abelian factors, then for all i, $H_i \geq G^{(i)}$.*

Proof. Assume by induction that $H_i \geq G^{(i)}$ for some i. Then, since H_i/H_{i+1} is abelian, we have $H_{i+1} \geq H_i' \geq (G^{(i)})' = G^{(i+1)}$.

9.2.5. We therefore have:

Theorem. *A group is solvable iff its derived series degenerates: $G^{(n)} = 1$ for some n.*

Proof. If the dervied series of G degenerates, then it is a finite subnormal series of G with abelian factors, so G is solvable. If G is solvable, let $1 = H_n \trianglelefteq H_{n-1} \trianglelefteq \cdots \trianglelefteq H_1 \trianglelefteq H_0 = G$ be a subnormal series with abelian factors; then $G^{(n)} \leq H_n = 1$, so $G^{(n)} = 1$. ■

9.2.6. A subnormal series of a group G whose all memebers 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 (namely, the derived series).

9.2.7. 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*.

9.2.8. 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 $\mathrm{GL}_n(F)$ of upper-triangular matrices (which have all 0s below the main diagonal) is solvable.

9.2.9. We now have a simpler argument proving that if a group G is solvable, then any its subgroup H and quotient group K are solvable: if $G^{(n)} = 1$ for some n, then $H^{(n)} = 1$ and $K^{(n)} = 1$ as well.

9.3. Central series and nilpotent groups

9.3.1. A normal series $\cdots \trianglelefteq H_i \trianglelefteq H_{i+1} \trianglelefteq \cdots$ of subgroups of a group G is said to be *central* if for every i, $H_{i+1}/H_i \leq Z(G/H_i)$. (That is, for every i, the elements of H_{i+1} commute with all elements of G modulo H_i.) This is equivalent to $[G, H_{i+1}] \leq H_i$.

9.3.2. 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*.

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

$$\text{cyclic groups} \underset{\neq}{\subset} \text{abelian groups} \underset{\neq}{\subset} \text{nilpotent groups} \underset{\neq}{\subset} \text{solvable groups}.$$

9.3.4. Let G be a group; for any subgroup M of any quotient group of G let us denote by $\overline{M}$ the preimage of M in G. *The upper central series* of G is the central series $1 = Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \cdots$ where $Z_1 = Z(G)$, $Z_2 = \overline{Z(G/Z_1)}$, and $Z_{i+1} = \overline{Z(G/Z_i)}$ for all i. (That is, Z_{i+1} consists of all the elements of G that commute with all other elemenets of G modulo Z_i.) The members Z_i of the upper central series of G are characteristic subgroups of G.

9.3.5. *The lower central series* of a group G is the central series $\cdots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G$ where $G_1 = G$, $G_2 = [G,G] = G'$, $G_3 = [G,G']$, and $G_{i+1} = [G,G_i]$ for all i. The members G_i of the lower central series of G are also characteristic subgroups of G.

9.3.6. 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).*

Proof. (i) Let, by induction on i, $H_i \leq Z_i$ for some i. Then, since every element of H_{i+1} commutes with every element of G modulo H_i, it commutes with every element of G modulo Z_i, so is contained in Z_{i+1}.

(ii) Let, by induction on i, $K_i \geq G_i$ for some i. Then, since $[G,K_i] \leq K_{i+1}$, we have $G_{i+1} = [G,G_i] \leq K_{i+1}$. ■

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

9.3.8. 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 $D_{2^{k+1}}$ is k-step nilpotent.

(v) For any field F and $n \in \mathbb{N}$, the subgroup of $\mathrm{GL}_n(F)$ 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 $\left\{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},\ a,b,c \in F\right\}$ is 2-step nilpotent.

9.3.9. 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.

9.3.10. Nilpotent groups have the following property:

Lemma. *If H is a proper subgroup of a nilpotent group G, then $N(H) \neq H$.*

Proof. Let $Z = Z(G)$. If $Z \not\leq H$, then $N_G(H) \neq H$ since $Z \leq N_G(H)$. Assume that $Z \leq H$. Then H/Z is a proper subgroup of G/Z. By induction on the nilpotency class of G, $N_{G/Z}(H/Z) \neq H/Z$. But $N_G(H)$ is the preimage of $N_{G/Z}(H/Z)$ in G, so $N_G(H) \neq H$. ■

9.3.11. 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).

Proof. Every Sylow subgroup of G is nilpotent, and if G is a direct product of its Sylow subgroups, then G is nilpotent.

Assume that G is nilpotent, and let P be one of its Sylow subgroups. By Proposition 8.2.7, $N_G(N_G(P)) = N_G(P)$, so by Lemma 9.3.10, $N_G(P) = G$, that is, P is normal in G. ■

---

10. Subgroups and quotients of free groups

10.0.1. A group F is *free* if it is isomorphic to the group F_A of reduced words in an alphabet $A \cup A^{-1}$; the cardinality of A, that is, the number of free generators of F is called *the rank*, or *the free rank* of F. The rank of a free group is well defined: $F_A \cong F_B$ iff $|A| = |B|$. (Here is an argument for the case the ranks are finite: if $F_n \cong F_m$ for $m < n$, then $\mathbb{Z}^n \cong F_n/F_n' \cong \mathbb{Z}^m \cong F_m/F_m'$. But $\mathbb{Z}^n \not\cong \mathbb{Z}^m$ since the vector space $\mathbb{R}^n$ is spanned by a subgroup isomorphic to $\mathbb{Z}^n$ whereas it cannot be spanned by a subgroup isomorphic to $\mathbb{Z}^m$.)

10.0.2. *The Nielsen-Schreier theorem* says that any subgroup H of a free group F is free; if F has rank n and $|F:H| = k$, then H has rank $k(n-1)+1$.

It is worth mentioning that there is a simple proof of this theorem that uses fundamental groups. (The free group of rank n is the fundamental group of a bouquet of n loops, connected at a single point.)

10.0.3. A free F group is not solvable (unless it is cyclic), but its derived series has a trivial core: $\bigcap_{n=1}^{\infty} F^{(n)} = 1$. Actually, even the lower central series of F has a trivial core: $\bigcap_{n=1}^{\infty} F_n = 1$, so F is "approximable" by nilpotent groups; groups with this property are called *residually nilpotent*.

10.0.4. Every group is representable as a factor of a free group, that is, can be described in terms of generators and relations. However, here the so-called *isomorphism problem* appears, – how to determine whether two different such descriptions actually represent the same group? This problem is proved to be *indecidable* (unsolvable): there is no general algorithm that allows to check whether two groups given by two systems of generators and relations are isomorphic.

10.0.5. Two more related indecidable problems are *the word problem* and *the conjufacy problem*: given two words in terms of generators of a group G (and their inverses), do they represent the same, or conjugate, element(s) of G?