

1. Definition, examples, and elementary properties of groups.

Definition: A set G with an operation $\cdot$ is called a group if:

- (1) $\forall a, b \in G: a \cdot b \in G$
- (2) $\forall a, b, c \in G: a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- (3) $\exists e \in G: \forall a \in G: a \cdot e = e \cdot a = a$
- (4) $\forall a \in G \exists a^{-1} \in G: a \cdot a^{-1} = a^{-1} \cdot a = e$

The element e is usually called the *identity element*, and a^{-1} the *inverse of the element a* .

The proper notation for a group is $(G, \cdot)$, but it is often denoted simply by G when the operation is clear from the context.

Examples:

1. $(\mathbb{Z}, +)$.

Let us prove that the set of integers with addition is a group:

- 1) Clearly, if $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$.
- 2) Clearly, $a + (b + c) = (a + b) + c$.
- 3) Here the number 0 plays the role of e . Indeed, $\forall a \in \mathbb{Z}: a + 0 = 0 + a = a$.
- 4) For an integer a , the number $-a$ plays the role of a^{-1} . Verily, $a + (-a) = -a + a = 0$.

Thus all 4 properties hold, so $(\mathbb{Z}, +)$ is a group.

2. $(\mathbb{Z}, \cdot)$

Let us check whether the set of integers with multiplication is a group.

- 1) Clearly, if $a, b \in \mathbb{Z}$, then $a \cdot b \in \mathbb{Z}$.
- 2) Clearly, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- 3) Here the number 1 plays the role of e . Indeed, $\forall a \in \mathbb{Z}: a \cdot 1 = 1 \cdot a = a$.
- 4) The existence of an inverse, however, is a problem. We need $\forall a \in \mathbb{Z} \exists a^{-1}$ such that $a \cdot a^{-1} = 1$. But then $a^{-1} = \frac{1}{a}$. Remember that the inverse must also belong to the group, so $\frac{1}{a} \in \mathbb{Z} \Rightarrow a = \pm 1$. Thus only 2 elements of the set of integers are invertible under multiplication, so the fourth part of the definition of a group does not hold.

Thus $(\mathbb{Z}, \cdot)$ is not a group.

Exercise: Check whether the following are groups:

$(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0, 2, \frac{1}{2}\}, \cdot)$, $(\mathbb{Q} \setminus \{0, 2, \frac{1}{2}\}, \cdot)$,
 $(\mathbb{R} \setminus \{0\}, \div)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n \setminus \{0\}, \cdot)$, $(S_n, \circ)$, $(A_n, \circ)$,
(the set of isometries taking a triangle to itself, $\circ$).

By definition, every group has at least one identity element. A natural question arises: how many can there be? The answer is that **the identity element is unique** in every group. Let us prove this:

Suppose there are two elements $e_1, e_2 \in G$ with the properties of an identity. Then $e_1 \cdot e_2 = e_1 = e_2$. Thus they are actually the same element. This is what we wanted to prove.

Exercise: Prove that every element of every group has a unique inverse.

2. Subgroups.

Definition: A subgroup H of a group G with operation $\cdot$ is a subset $H \subseteq G$ that is a group under the same operation $\cdot$.

The assertion that a subset H of a group G is a subgroup is conventionally written with the same symbol as an ordinary subset: $H \subseteq G$. This is convenient and causes no confusion, since the meaning is always clear from the context.

Examples:

1. $(2\mathbb{Z}, +)$

Let us check that the set of even integers with addition is a group.

- 1) If a, b are even numbers, then $a + b$ is also even.
- 2) Clearly, $a + (b + c) = (a + b) + c$ for both even and odd numbers (in fact, associativity holds automatically for subsets of a group, provided the first group property holds, and need not be checked).
- 3) 0 is even, so it belongs to $2\mathbb{Z}$ and plays the role of the identity element.
- 4) If a is even, then $-a$ is also even, so every $a \in 2\mathbb{Z}$ has an even inverse.

Thus all the group axioms hold, so $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

2. $(\mathbb{Z} \setminus 2\mathbb{Z}, +)$.

Let us check whether the set of all odd numbers is a subgroup of $(\mathbb{Z}, +)$.

- 1) If a, b are odd, then $a + b$ is even.

Thus the very first group axiom fails, so the set of odd numbers is not a subgroup of the group $\mathbb{Z}$.

Proposition. A subset H of a group G is a subgroup if and only if it is closed under multiplication and taking inverses, that is, $\forall a, b \in H$

- (1) $a \cdot b \in H$;
- (2) $a^{-1} \in H$.

Corollary. The intersection of any collection of subgroups is a subgroup.

Exercise: Find some subgroups in each of the groups considered so far.

Definition: The *left coset* of an element a of a group G with operation $\cdot$ modulo a subgroup H is the set $aH = \{a \cdot h \mid h \in H\}$.

Similarly, the *right coset* of an element a is the set $Ha = \{h \cdot a \mid h \in H\}$.

The construction of right and left cosets, which at first sight seem rather unnatural and unnecessary, leads to one of the most important theorems in group theory: Lagrange's theorem. Let us prove it.

Lemma: Left (right) cosets of a group G modulo the same subgroup H are either disjoint or equal. (In other words, distinct aH do not intersect.)

Proof: Let us prove that if two cosets aH and bH intersect, then in fact $aH = bH$.

Let $c \in aH \cap bH$. Then $c = a \cdot h_1 = b \cdot h_2$, where $h_1, h_2 \in H$. But then $a = b \cdot h_2 \cdot h_1^{-1}$. Now multiply this equality on the right by an arbitrary element $h \in H$, obtaining $a \cdot h = b \cdot h_2 \cdot h_1^{-1} \cdot h$. But $h_2 \cdot h_1^{-1} \cdot h = h_0 \in H$. Thus $a \cdot h = b \cdot h_0$, and since h was arbitrary, we obtain the inclusion $aH \subseteq bH$. The reverse inclusion is proved similarly by interchanging the roles of a and b . Thus $aH = bH$, as required.

We are now ready to state and prove Lagrange's theorem.

Lagrange's theorem: In a finite group G , the order of any subgroup H divides the order of G . (The order is the number of elements in a group or subgroup, and is denoted by $|\cdot|$.)

Proof: Every element a of the group G belongs to some coset (for example, to aH , since $e \in H$). Suppose two elements of aH coincide (that is, there are $h_1 \neq h_2 \in H$ such that $a \cdot h_1 = a \cdot h_2$). Multiplying this equality on the left by a^{-1} gives $h_1 = h_2$, a contradiction. Thus the elements $a \cdot h$ are distinct for all $h \in H$, and hence $|aH| = |H| \forall a \in G$. We therefore know that all cosets contain the same number $|H|$ of elements, are disjoint, and have union equal to the whole group G . It follows immediately that $|G| = k|H|$, or, in other words, $|G| \div |H|$, as required.

Definition: The order $\text{ord}(a)$ of an element a of a group G is a natural number n such that $a^n = e$ (if no such n exists, we put $\text{ord}(a) = \infty$).

Corollary of Lagrange's theorem: In a finite group, the orders of all elements are finite and divide the order of the group.

Exercise: Prove the corollary.

Hint: Think of the simplest possible subgroup containing the element a .

The cosets of a group modulo a subgroup are, generally speaking, not particularly interesting sets. There are, however, situations in which things are much more interesting.

Definition: A subgroup H of a group G is called *normal* if $\forall g \in G, h_1 \in H \exists h_2 \in H$ such that $g \cdot h_1 \cdot g^{-1} = h_2$, or, equivalently, $g \cdot h_1 = h_2 \cdot g$.

The phrase “the subgroup H is normal in the group G ” is written $H \triangleleft G$ (or $G \triangleright H$).

Examples:

1. In any group, the subgroup consisting only of the identity is normal. Indeed, $\forall g \in G, g \cdot e \cdot g^{-1} = e$, so this subgroup is normal by definition.

2. In any group, the subgroup equal to the whole group is normal. Indeed, $\forall g_1, g_2 \in G, g_1 \cdot g_2 \cdot g_1^{-1} \in G$, as required.

3. Suppose a group G satisfies $\forall g_1, g_2 \in G, g_1 \cdot g_2 = g_2 \cdot g_1$. (Such groups are called *abelian*, or *commutative*.) Let us prove that every subgroup of an abelian group is normal.

Indeed, let G be abelian and $H \subseteq G$. Take any $g \in G$ and $h \in H$. Then $g \cdot h \cdot g^{-1} = g \cdot (h \cdot g^{-1}) = (h \cdot g^{-1}) \cdot g = h \cdot (g^{-1} \cdot g) = h \in H$. This proves the assertion.

Notice that most of the groups we have considered are abelian.

Exercise: Find some normal subgroups in the nonabelian groups considered earlier.

Definition: The set $Z = \{h \in G \mid \forall g \in G, h \cdot g = g \cdot h\}$ is called the *center* of the group G .

Exercise: Prove that $Z \triangleleft G$ for every group G .

Let us now see what is useful about cosets of a group modulo a normal subgroup. Let $H \triangleleft G$. For two elements $g_1, g_2 \in G$, consider their cosets g_1H and g_2H and take an arbitrary representative from each: $g_1 \cdot h_1 \in g_1H$ and $g_2 \cdot h_2 \in g_2H$. Let us see what happens when we multiply them: $g_1 \cdot h_1 \cdot g_2 \cdot h_2 = g_1 \cdot (h_1 \cdot g_2) \cdot h_2 = g_1 \cdot (g_2 \cdot h) \cdot h_2 = (g_1 \cdot g_2) \cdot (h \cdot h_2) \in g_1 \cdot g_2H$ (h is some element of H whose existence follows from the normality of H). This calculation shows that the cosets gH also form a group under the “same” operation. Indeed, eH plays the role of the identity, and $g^{-1}H$ is the inverse of gH . We thus obtain the following:

Definition: The group of cosets of a group G modulo a normal subgroup H is called the *quotient group* of G by H and is denoted by G/H .

Remark: The group of cosets modulo a normal subgroup is in no sense a subgroup of G .

Exercise: Explore the structure of the quotient groups by the normal subgroups we considered earlier.

3. Homomorphisms.

Definition: A map f from a group $(G, \cdot)$ to a group $(H, \heartsuit)$ is called a *homomorphism* if $\forall g_1, g_2 \in G, f(g_1 \cdot g_2) = f(g_1) \heartsuit f(g_2)$.

Here $\heartsuit$ denotes the operation in the other group. For convenience, we will also denote it by $\cdot$ below, without meaning that it is the same operation as in G .

Examples:

1. From any group G , we can construct a homomorphism to the one-element group simply by mapping every $g \in G$ to e .

2. From any group to itself, we can construct a homomorphism using the identity map.

3. Let us construct a homomorphism from $\mathbb{Z}$ to $2\mathbb{Z}$ using a function f such that $\forall k \in \mathbb{Z} f(k) = 2k$.

Let us check that this is indeed a homomorphism. We have $f(n+k) = 2(n+k) = 2n+2k = f(n) + f(k)$, as required.

4. Let us check whether $f(x) = x^2$ is a homomorphism from the group $\mathbb{R}$ to itself.

$f(x+y) = (x+y)^2 = x^2 + y^2 + 2xy = f(x) + f(y) + 2xy$. Thus squaring is not a homomorphism in this case.

Exercise: Is

- (1) $f(x) = x + 1$ a homomorphism from the group $\mathbb{Z}$ to itself;
- (2) $f(x) = x^2$ a homomorphism from the group $\mathbb{R} \setminus \{0\}$ to itself;
- (3) $f(\sigma) = \text{the number of disjoint cycles}$ a homomorphism from S_n to $\mathbb{Z}$;
- (4) $f(\sigma) = \text{sgn}(\sigma)$ a homomorphism of the group S_n ;
- (5) $f(n) = n \pmod{m}$ a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_m$;
- (6) $f(g) = gH$ a homomorphism from G to the quotient group G/H ?

Exercise: Prove that a homomorphism satisfies $f(e) = e$ and $f(g^{-1}) = f(g)^{-1} \forall g \in G$.

Let a homomorphism f from a group G to a group H be given.

Definition 1: The set $A = \{g \in G \mid f(g) = e\}$ is called the *kernel* of the homomorphism f and is denoted by $\text{Ker}(f)$.

Definition 2: The set $B = \{h \in H \mid h = f(g)\}$ is called the *image* of the homomorphism f and is denoted by $\text{Im}(f)$.

Proposition: $\text{Im}(f)$ is a subgroup of H , and $\text{Ker}(f)$ is a **normal** subgroup of G .

Proof: Let us prove that $\text{Ker}(f) \triangleleft G$. Associativity clearly holds, since it holds throughout G . Now let $g_1, g_2 \in G$. Then $f(g_1) = f(g_2) = e$. Consider $g_1 \cdot g_2$ and apply f to this element. We obtain $f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2) = e \cdot e = e$. Thus if $g_1, g_2 \in \text{Ker}(f)$, then $g_1 \cdot g_2 \in \text{Ker}(f)$ as well.

The exercise gives $f(e) = e$ (that is, $e \in \text{Ker}(f)$) and $f(g^{-1}) = f(g)^{-1}$ (if $g \in \text{Ker}(f)$, this gives $f(g^{-1}) = f(g)^{-1} = e^{-1} = e$. Thus if $g \in \text{Ker}(f)$, then $g^{-1} \in \text{Ker}(f)$ as well).

We have proved that $\text{Ker}(f)$ is a subgroup of G . Let us prove normality.

Let $x \in \text{Ker}(f), g \in G$. Consider the element $g^{-1} \cdot x \cdot g$ and apply f to it. We obtain $f(g^{-1} \cdot x \cdot g) = f(g^{-1}) \cdot f(x) \cdot f(g) = f(g)^{-1} \cdot e \cdot f(g) = e$. It follows that $g^{-1} \cdot x \cdot g \in \text{Ker}(f) \forall g \in G$. By definition, this means that $\text{Ker}(f)$ is a normal subgroup of G , as required.

Exercise: Prove that $\text{Im}(f)$ is a subgroup of H .

Exercise: Find the kernels and images of the homomorphisms we considered.

Definition: A bijective homomorphism f from a group G to a group H is called an *isomorphism* of these groups. In this case, G and H are said to be *isomorphic*, and we write $G \simeq H$.

Exercise: Are the following groups isomorphic:

- (1) $\mathbb{Z}$ and $\mathbb{R}$;
- (2) $\mathbb{R}$ and $\mathbb{R} \setminus \{0\}$;
- (3) S_n and $\mathbb{Z}_n$?

Fundamental theorem on homomorphisms: Let f be a homomorphism from a group G to a group H . Then $G/\text{Ker}(f) \simeq \text{Im}(f)$.

Exercise: Determine which groups are isomorphic to one another in the examples of homomorphisms we considered.

Exercise: Try to prove the fundamental theorem on homomorphisms.

4. Specifying a group by generators.

In many situations, when considering a group, we would like a limited, convenient set of elements in terms of which we can express all the other elements of the group.

Definition Let M be an arbitrary subset of a group G . Consider the intersection of all subgroups of G containing M : this is the subgroup generated by M . (Clearly, the same subgroup may have different generating sets.)

We denote the subgroup generated by M by $\langle M \rangle$. If the subgroup generated by M equals the entire group G , then M is a generating set for G .

Theorem. If M is a subset of a group G , then $\langle M \rangle = \{a_1^{\epsilon_1} \cdots a_s^{\epsilon_s} \mid a_i \in M, \epsilon_i = \pm 1, s = 1, 2, \dots\} = H$.

Proof. The subgroup $\langle M \rangle$ contains all $a_i \in M$, their products, and their inverses, and hence the entire set H ; therefore $H \subset \langle M \rangle$. But by *Proposition 1*, H is a subgroup containing $\langle M \rangle$, so the definition of the subgroup generated by M gives $\langle M \rangle \subset H$. Thus $\langle M \rangle = H$.

Examples: $\mathbb{Z}, \mathbb{Q}, S_n, \mathbb{Z}/n\mathbb{Z}$.

Relations. When specifying a subgroup by generating sets, we must take into account how multiplication works among the elements of the generating set: there may be conditions on products of certain elements. For example, if a is an element of the generating set M and a^{-1} is its inverse, then $a \cdot a^{-1} = 1$. There may also be other conditions on products of elements of M , for example, $a \cdot b \cdot c^{-1} \cdot a^{-1} \cdot d = d \cdot a^{-1}$; notice that by successively multiplying both sides of the equation on the left by the inverse of the first element on the right, we can always write these conditions in the form “a product of some elements equals the identity.” Such conditions on multiplication are called *relations* in the group. Relations of the form $a \cdot a^{-1} = 1$, which hold in every group, are called *trivial* relations.

Examples:

- (1) An abelian group is a group in which the relations $\forall a, b, a \cdot b \cdot a^{-1} \cdot b^{-1} = 1$ hold, or, equivalently, $a \cdot b = b \cdot a$.
- (2) The cyclic group $\mathbb{Z}/n\mathbb{Z}$ of order n is an abelian group generated by one element a , with the additional relation $a^n = 1$. Consequently, every element b of this group satisfies $b^n = 1$.

5. Equivalence

Definition, which you need not ponder here. An equivalence relation between objects is a relation “ $\sim$ ” satisfying three properties:

- (1) $a \sim a$ (Reflexivity);
- (2) If $a \sim b$, then $b \sim a$ (Symmetry);
- (3) If $a \sim b$ and $b \sim c$, then $a \sim c$ (Transitivity).

If a relation $\sim$ on an arbitrary set A satisfies all three properties, then $\sim$ is called an *equivalence relation* on this set, and elements $a \sim b$ are said to be equivalent. Informally, an equivalence relation generalizes equality of two elements: elements are equivalent when they are the same in some sense, so they should satisfy the basic properties satisfied by identical objects.

Examples.

- (1) Equality of two numbers is an equivalence relation; moreover, equality of other objects (for example, geometric figures) is an equivalence relation.
- (2) Congruence modulo a fixed modulus (also a generalization of equality), $a \equiv b$, is an equivalence relation.
- (3) Geometric similarity is an equivalence relation; the relation $\parallel$ of parallelism of two lines or two planes is an equivalence relation.

- (4) The relation " $<$ " (a strict linear order) on the rational numbers is NOT an equivalence relation: it is transitive, but not reflexive ($a < a$ is false) and not symmetric.
- (5) The relation " $\leq$ " (a non-strict linear order) on the real numbers is NOT an equivalence relation: indeed, it is reflexive and transitive, but not symmetric ($a \leq b$ does not imply $b \leq a$).

Definition Fix a particular equivalence relation on a set X . The equivalence class of an element a is the set of all elements equivalent to a , denoted by $[a] = \{x \in X \mid x \sim a\}$.

An equivalence class can itself be regarded as an element of a set (the set of equivalence classes of elements of X). Moreover, if an operation " $\cdot$ " is defined on X and preserves equivalence (that is, if $a \sim b$ and $x \sim y$, then $a \cdot b \sim x \cdot y$), we can define a compatible operation on the set of equivalence classes as well.

6. On the free group

Important example 1. Consider the set of words in the letters of a finite alphabet

$\{a_1, a_2, \dots, a_m, a_1^{-1}, a_2^{-1}, \dots, a_m^{-1}\}$ (that is, elements of the form $a_{i_1}^{k_1} \dots a_{i_s}^{k_s}$, where the k_j are integers indicating the number of consecutive identical elements), with the following equivalence relation: words are equivalent if they can be transformed into one another by successively inserting or deleting pieces of the form $x^k x^{-k}$ or $x^{-k} x^k$.

Introduce multiplication of words as follows: if u and v are two words, their product $u \cdot v = uv$ is the word obtained by appending v to the right of u (this operation is called *concatenation*). It is easy to check that this operation preserves equivalence of the elements in *important example 1*: if we could insert and delete several trivial pieces in parts of words to make them equal, we can do the same when the words are appended to one another. We can therefore take the set of equivalence classes of words as our set (so that we do not have distinct "identical", that is, equivalent, elements), and perform the same operations on them as on the words themselves. To avoid cumbersome notation, we will continue to write the words themselves (usually in reduced form, that is, without trivial pieces of the form $x^k x^{-k}$).

Exercise. Prove that every word has exactly one reduced form, that is, a form without pieces $x^k x^{-k}$ that can be deleted.

It is easy to see that in a group with generators $a_1, a_2, \dots, a_m$, every element can be written as a word over the corresponding alphabet (possibly in more than one way); and if the group has no relations other than trivial ones, it can be written uniquely as a reduced word (in other words, uniquely assigned the equivalence class of its words, since we have seen that an equivalence class determines a unique reduced word). We are ready to introduce the following:

Definition A free group is a group generated by a set M whose generators satisfy no relations other than trivial ones.

Theorem. For every set of generators $M = \{a_i \mid i \in I\}$, there exists a free group generated by this set; it consists of all reduced words over this alphabet (or, equivalently, the equivalence classes of such words defined above), with the operation of "gluing" (concatenation).

Proof. The identity element is the empty word (the equivalence class of any trivial word, for example, $[aa^{-1}]$; the inverse of $a_{i_1}^{k_1} \dots a_{i_s}^{k_s}$ is $a_{i_s}^{-k_s} \dots a_{i_1}^{-k_1}$. It remains to check that all group axioms hold.

Exercise. Free groups with two or more generators are noncommutative.

Important example 2. Suppose a collection of relations (possibly not just trivial ones), that is, equalities between certain words, is given on the elements of the alphabet $\{a_1, a_2, \dots, a_m, a_1^{-1}, a_2^{-1}, \dots, a_m^{-1}\}$. Introduce a new equivalence relation on the words of *important example 1*: words are equivalent if one can be transformed into the other by replacing some pieces with equal ones (according to the relations). As in *important example 1*, we can define "gluing" on the equivalence classes of these words, and then prove that they form a group.

Definition. Let ψ be a set of relations on a set M . The group generated by the generating set M and the set of defining relations ψ is the group $\langle M \mid \psi \rangle$ of equivalence classes of words (constructed using the defining relations ψ), with concatenation as its operation.

In particular, trivial relations ψ generate a free group.

7. The universal property.

The free group generated by a set M is, in a sense, the most general group generated by this set. Here is what this means:

Theorem. (Universal property): Denote the free group generated by M by F . Then for any group G and any map of sets $f : M \longrightarrow G$, there exists a unique group homomorphism $\phi : F \longrightarrow G$ satisfying $\forall m \in M$ $f(m) = \phi(m)$. In other words, the diagram commutes.

$$\begin{array}{ccc} M & \longrightarrow & F \\ & \searrow f & \downarrow \phi \\ & & G \end{array}$$

Exercise: Prove the theorem.

In fact, the universal property can be taken as the definition of a free group.

Remark: If we take M to be a generating set of G (denote it by E) and define f by $\forall g \in E$ $f(g) = g$, we find that there is a surjective homomorphism $\phi : F \longrightarrow G$ from the free group generated by the same generating set as G . Then the fundamental theorem on homomorphisms gives $G \simeq F/\text{Ker}\phi$.

Thus any group with generating set E is a quotient of the free group generated by E by some normal subgroup.