

Groups

TS. Nguyễn Việt Đông

1

Groups

- 1. Introduction
- 2. Normal subgroups, quotient groups.
- 3. Homomorphism.

2

1. Introduction

- 1.1. Binary Operations
- 1.2. Definition of Groups
- 1.3. Examples of Groups
- 1.4. Subgroups

3

1. Introduction

- 1.1. Binary Operations
- 1.2. Definition of Groups
- 1.3. Examples of Groups
- 1.4. Subgroups

4

1. Introduction

1.1. Binary Operations

A *binary operation* on a set is a rule for combining two elements of the set. More precisely, if S is a nonempty set, a binary operation on S is a mapping $f : S \times S \rightarrow S$. Thus f associates with each ordered pair (x,y) of element of S an element $f(x,y)$ of S . It is better notation to write $x \cdot y$ for $f(x,y)$, referring to \cdot as the binary operation.

5

1. Introduction

1.2. Definition of Groups

A *group* (G, \cdot) is a set G together with a binary operation \cdot satisfying the following axioms.

- (i) The operation \cdot is associative; that is, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
- (ii) There is an *identity element* $e \in G$ such that $e \cdot a = a \cdot e = a$ for all $a \in G$.
- (iii) Each element $a \in G$ has an *inverse element* $a^{-1} \in G$ such that $a^{-1} \cdot a = a \cdot a^{-1} = e$.

6

1. Introduction

If the operation is commutative, that is,

$$\text{if } a \cdot b = b \cdot a \quad \text{for all } a, b \in G,$$

the group is called **commutative or abelian, in honor of the mathematician Niels Abel**.

7

1. Introduction

1.3. Examples of Groups

- **Example 1.3.1.** Let G be the set of complex numbers $\{1, -1, i, -i\}$ and let \cdot be the standard multiplication of complex numbers. Then (G, \cdot) is an abelian group. The product of any two of these elements is an element of G ; thus G is closed under the operation. Multiplication is associative and commutative in G because multiplication of complex numbers is always associative and commutative. The identity element is 1, and the inverse of each element a is the element $1/a$. Hence

$$1^{-1} = 1, (-1)^{-1} = -1, i^{-1} = -i, \text{ and } (-i)^{-1} = i.$$

8

1. Introduction

- **Example 1.3.2.** The set of all rational numbers, \mathbb{Q} , forms an abelian group $(\mathbb{Q}, +)$ under addition. The identity is 0, and the inverse of each element is its negative. Similarly, $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all abelian groups under addition.
- **Example 1.3.3.** If \mathbb{Q}^* , \mathbb{R}^* , and \mathbb{C}^* denote the set of nonzero rational, real, and complex numbers, respectively, (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) , and (\mathbb{C}^*, \cdot) are all abelian groups under multiplication.

9

1. Introduction

- **Example 1.3.4.** A translation of the plane \mathbb{R}^2 in the direction of the vector (a, b) is a function $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by $f(x, y) = (x + a, y + b)$. The composition of this translation with a translation g in the direction of (c, d) is the function $f \circ g: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, where $f \circ g(x, y) = f(g(x, y)) = f(x + c, y + d) = (x + c + a, y + d + b)$. This is a translation in the direction of $(c + a, d + b)$. It can easily be verified that the set of all translations in \mathbb{R}^2 forms an abelian group, under composition. The identity is the identity transformation $1_{\mathbb{R}^2}: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, and the inverse of the translation in the direction (a, b) is the translation in the opposite direction $(-a, -b)$.

10

1. Introduction

- **Example 1.3.5.** If $S(X)$ is the set of bijections from any set X to itself, then $(S(X), \circ)$ is a group under composition. This group is called the symmetric group or permutation group of X .

11

1. Introduction

- **Proposition 1.3.1.** If a, b , and c are elements of a group G , then
 - (i) $(a^{-1})^{-1} = a$.
 - (ii) $(ab)^{-1} = b^{-1}a^{-1}$.
 - (iii) $ab = ac$ or $ba = ca$ implies that $b = c$. (cancellation law)

12

1. Introduction

- 1.4. Subgroups

It often happens that some subset of a group will also form a group under the same operation. Such a group is called a *subgroup*. If (G, \cdot) is a group and H is a nonempty subset of G , then (H, \cdot) is called a *subgroup* of (G, \cdot) if the following conditions hold:

- (i) $a \cdot b \in H$ for all $a, b \in H$. (*closure*)
- (ii) $a^{-1} \in H$ for all $a \in H$. (*existence of inverses*)

13

1. Introduction

- Conditions (i) and (ii) are equivalent to the single condition:
(iii) $a \cdot b^{-1} \in H$ for all $a, b \in H$.

Proposition 1.4.2. *If H is a nonempty finite subset of a group G and $ab \in H$ for all $a, b \in H$, then H is a subgroup of G .*

Example 1.4.1 In the group $(\{1, -1, i, -i\}, \cdot)$, the subset $\{1, -1\}$ forms a subgroup because this subset is closed under multiplication

14

1. Introduction

- **Example 1.4.2** .The group \mathbb{Z} is a subgroup of \mathbb{Q} , \mathbb{Q} is a subgroup of \mathbb{R} , and \mathbb{R} is a subgroup of \mathbb{C} . (Remember that addition is the operation in all these groups.)
- However, the set $\mathbb{N} = \{0, 1, 2, \dots\}$ of nonnegative integers is a subset of \mathbb{Z} but not a subgroup, because the inverse of 1, namely, -1 , is not in \mathbb{N} . This example shows that Proposition 1.4.2 is false if we drop the condition that H be finite.
- The relation of being a subgroup is transitive. In fact, for any group G , the inclusion relation between the subgroups of G is a partial order relation.

15

1. Introduction

- **Definition.** Let G be a group and let $a \in G$. If $a^k = 1$ for some $k \geq 1$, then the smallest such exponent $k \geq 1$ is called the *order* of a ; if no such power exists, then one says that a has *infinite order*.
- **Proposition 1.4.3** . *Let G be a group and assume that $a \in G$ has finite order k . If $a^n = 1$, then $k \mid n$. In fact, $\{n \in \mathbb{Z} : a^n = 1\}$ is the set of all the multiples of k .*

16

1. Introduction

- **Definition.** If G is a group and $a \in G$, write $\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\text{all powers of } a\}$.

It is easy to see that $\langle a \rangle$ is a subgroup of G .

$\langle a \rangle$ is called the *cyclic subgroup* of G generated by a . A group G is called *cyclic* if there is some $a \in G$ with $G = \langle a \rangle$; in this case a is called a *generator* of G .

- **Proposition 1.4.4.** If $G = \langle a \rangle$ is a cyclic group of order n , then a^k is a generator of G if and only if $\gcd(k, n) = 1$.
- **Corollary 1.4.5.** The number of generators of a cyclic group of order n is $\phi(n)$.

17

1. Introduction

- **Proposition 1.4.6.** Let G be a finite group and let $a \in G$. Then the order of a is the number of elements in $\langle a \rangle$.
- **Definition.** If G is a finite group, then the number of elements in G , denoted by $|G|$, is called the **order of G** .

18

2. Normal subgroups, quotient groups

- 2.1. Cosets
- 2.2. Theorem of Lagrange
- 2.3. Normal Subgroups
- 2.4. Quotient Groups

19

2. Normal subgroups, quotient groups

- **2.1. Cosets**
- Let (G, \cdot) be a group with subgroup H . For $a, b \in G$, we say that a is **congruent to b modulo H** , and write $a \equiv b \pmod{H}$ if and only if $ab^{-1} \in H$.
- **Proposition 2.1.1.** The relation $a \equiv b \pmod{H}$ is an equivalence relation on G . The equivalence class containing a can be written in the form $Ha = \{ha \mid h \in H\}$, and it is called a **right coset of H in G** . The element a is called a **representative of the coset Ha** .

20

2.Normal subgroups,quotient groups

- **Example 2.1.1.** Find the right cosets of A_3 in S_3 .

Solution. One coset is the subgroup itself $A_3 = \{(1), (123), (132)\}$. Take any element not in the subgroup, say (12). Then another coset is $A_3(12) = \{(12), (123)(12), (132)(12)\} = \{(12), (13), (23)\}$. Since the right cosets form a partition of S_3 and the two cosets above contain all the elements of S_3 , it follows that these are the only two cosets.

In fact, $A_3 = A_3(123) = A_3(132)$ and $A_3(12) = A_3(13) = A_3(23)$.

21

2.Normal subgroups,quotient groups

- **Example 2.1.2.** Find the right cosets of $H = \{e, g^4, g^8\}$ in $C_{12} = \{e, g, g^2, \dots, g^{11}\}$.

• *Solution.* H itself is one coset. Another is $Hg = \{g, g^5, g^9\}$. These two cosets have not exhausted all the elements of C_{12} , so pick an element, say g^2 , which is not in H or Hg . A third coset is $Hg^2 = \{g^2, g^6, g^{10}\}$ and a fourth is $Hg^3 = \{g^3, g^7, g^{11}\}$. Since $C_{12} = H \cup Hg \cup Hg^2 \cup Hg^3$, these are all the cosets

22

2.Normal subgroups,quotient groups

- **2.2.Theorem of Lagrange**
- As the examples above suggest, every coset contains the same number of elements. We use this result to prove the famous theorem of Joseph Lagrange (1736–1813).
- **Lemma 2.2.1.** There is a bijection between any two right cosets of H in G.

Proof. Let Ha be a right coset of H in G. We produce a bijection between Ha and H, from which it follows that there is a bijection between any two right cosets.

Define $\psi: H \rightarrow Ha$ by $\psi(h) = ha$. Then ψ is clearly surjective. Now suppose that $\psi(h_1) = \psi(h_2)$, so that $h_1a = h_2a$. Multiplying each side by a^{-1} on the right, we obtain $h_1 = h_2$. Hence ψ is a bijection.

23

2.Normal subgroups,quotient groups

- **Theorem 2.2.2.** Lagrange's Theorem. If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

Proof. The right cosets of H in G form a partition of G, so G can be written as a disjoint union

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k \text{ for a finite set of elements } a_1, a_2, \dots, a_k \in G.$$

By Lemma 2.2.1, the number of elements in each coset is $|H|$. Hence, counting all the elements in the disjoint union above, we see that $|G| = k|H|$. Therefore, $|H|$ divides $|G|$.

24

2.Normal subgroups,quotient groups

- If H is a subgroup of G , the number of distinct right cosets of H in G is called the *index of H in G* and is written $|G : H|$. The following is a direct consequence of the proof of Lagrange's theorem.
- **Corollary 2.2.3.** *If G is a finite group with subgroup H , then $|G : H| = |G|/|H|$.*
- **Corollary 2.2.4.** *If a is an element of a finite group G , then the order of a divides the order of G .*

25

2.Normal subgroups,quotient groups

- 2.3.Normal Subgroups
- Let G be a group with subgroup H . The *right cosets* of H in G are equivalence classes under the relation $a \equiv b \pmod H$, defined by $ab^{-1} \in H$. We can also define the relation L on G so that aLb if and only if $b^{-1}a \in H$. This relation, L , is an equivalence relation, and the equivalence class containing a is the *left coset* $aH = \{ah|h \in H\}$. As the following example shows, the left coset of an element does not necessarily equal the right coset.

26

2.Normal subgroups,quotient groups

- **Example 2.3.1.** Find the left and right cosets of $H = A_3$ and $K = \{(1), (12)\}$ in S_3 .
- *Solution.* We calculated the right cosets of $H = A_3$ in Example 2.1.1.
 Right Cosets
 $H = \{(1), (123), (132)\}; H(12) = \{(12), (13), (23)\}$
 Left Cosets
 $H = \{(1), (123), (132)\}; (12)H = \{(12), (23), (13)\}$
 In this case, the left and right cosets of H are the same.
- However, the left and right cosets of K are not all the same.
 Right Cosets
 $K = \{(1), (12)\}; K(13) = \{(13), (132)\}; K(23) = \{(23), (123)\}$
 Left Cosets
 $K = \{(1), (12)\}; (23)K = \{(23), (132)\}; (13)K = \{(13), (123)\}$

27

2.Normal subgroups,quotient groups

- Definition:** A subgroup H of a group G is called a *normal subgroup* of G if $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$.
- Proposition 2.3.1.** *$Hg = gH$, for all $g \in G$, if and only if H is a normal subgroup of G .*
- Proof.* Suppose that $Hg = gH$. Then, for any element $h \in H$, $hg \in Hg = gH$. Hence $hg = gh_1$ for some $h_1 \in H$ and $g^{-1}hg = g^{-1}gh_1 = h_1 \in H$. Therefore, H is a normal subgroup.
- Conversely, if H is normal, let $hg \in Hg$ and $g^{-1}hg = h_1 \in H$. Then $hg = gh_1 \in gH$ and $Hg \subseteq gH$. Also, $ghg^{-1} = (g^{-1})^{-1}hg^{-1} = h_2 \in H$, since H is normal, so $gh = h_2g \in Hg$. Hence, $gH \subseteq Hg$, and so $Hg = gH$.

28

2.Normal subgroups,quotient groups

- If N is a normal subgroup of a group G , the left cosets of N in G are the same as the right cosets of N in G , so there will be no ambiguity in just talking about the cosets of N in G .
- **Theorem 2.3.2.** *If N is a normal subgroup of (G, \cdot) , the set of cosets $G/N = \{Ng \mid g \in G\}$ forms a group $(G/N, \cdot)$, where the operation is defined by $(Ng_1) \cdot (Ng_2) = N(g_1 \cdot g_2)$. This group is called the quotient group or factor group of G by N .*

29

2.Normal subgroups,quotient groups

- *Proof.* The operation of multiplying two cosets, Ng_1 and Ng_2 , is defined in terms of particular elements, g_1 and g_2 , of the cosets. For this operation to make sense, we have to verify that, if we choose different elements, h_1 and h_2 , in the same cosets, the product coset $N(h_1 \cdot h_2)$ is the same as $N(g_1 \cdot g_2)$. In other words, we have to show that multiplication of cosets is well defined. Since h_1 is in the same coset as g_1 , we have $h_1 \equiv g_1 \pmod{N}$. Similarly, $h_2 \equiv g_2 \pmod{N}$. We show that $Nh_1h_2 = Ng_1g_2$. We have $h_1g_1^{-1} = n_1 \in N$ and $h_2g_2^{-1} = n_2 \in N$, so $h_1h_2(g_1g_2)^{-1} = h_1h_2g_2^{-1}g_1^{-1} = n_1g_1n_2g_2g_2^{-1}g_1^{-1} = n_1g_1n_2g_1^{-1}$. Now N is a normal subgroup, so $g_1n_2g_1^{-1} \in N$ and $n_1g_1n_2g_1^{-1} \in N$. Hence $h_1h_2 \equiv g_1g_2 \pmod{N}$ and $Nh_1h_2 = Ng_1g_2$. Therefore, the operation is well defined.

30

2.Normal subgroups,quotient groups

- The operation is associative because $(Ng_1 \cdot Ng_2) \cdot Ng_3 = N(g_1g_2) \cdot Ng_3 = N(g_1g_2)g_3$ and also $Ng_1 \cdot (Ng_2 \cdot Ng_3) = Ng_1 \cdot N(g_2g_3) = Ng_1(g_2g_3) = N(g_1g_2)g_3$.
- Since $Ng \cdot Ne = Nge = Ng$ and $Ne \cdot Ng = Ng$, the identity is $Ne = N$.
- The inverse of Ng is Ng^{-1} because $Ng \cdot Ng^{-1} = N(g \cdot g^{-1}) = Ne = N$ and also $Ng^{-1} \cdot Ng = N$.
- Hence $(G/N, \cdot)$ is a group.

31

2.Normal subgroups,quotient groups

- **Example 2.3.1.** $(\mathbb{Z}_n, +)$ is the quotient group of $(\mathbb{Z}, +)$ by the subgroup $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$.
- *Solution.* Since $(\mathbb{Z}, +)$ is abelian, every subgroup is normal. The set $n\mathbb{Z}$ can be verified to be a subgroup, and the relationship $a \equiv b \pmod{n\mathbb{Z}}$ is equivalent to $a - b \in n\mathbb{Z}$ and to $n \mid a - b$. Hence $a \equiv b \pmod{n\mathbb{Z}}$ is the same relation as $a \equiv b \pmod{n}$. Therefore, \mathbb{Z}_n is the quotient group $\mathbb{Z}/n\mathbb{Z}$, where the operation on congruence classes is defined by $[a] + [b] = [a + b]$. $(\mathbb{Z}_n, +)$ is a cyclic group with 1 as a generator. When there is no confusion, we write the elements of \mathbb{Z}_n as $0, 1, 2, 3, \dots, n - 1$ instead of $[0], [1], [2], [3], \dots, [n - 1]$.

32

3.Homomorphisms.

- 3.1.Definition of Homomorphisms
- 3.2.Examples of Homomorphisms
- 3.3.Theorem on Homomorphisms

33

3.Homomorphisms

- 3.1.Definition of Homomorphisms
- If (G, \cdot) and $(H, *)$ are two groups, the function $f : G \rightarrow H$ is called a *group homomorphism* if

$$f(a \cdot b) = f(a) * f(b) \text{ for all } a, b \in G.$$
- We often use the notation $f : (G, \cdot) \rightarrow (H, *)$ for such a homomorphism. Many authors use *morphism* instead of *homomorphism*.
- A *group isomorphism* is a bijective group homomorphism. If there is an isomorphism between the groups (G, \cdot) and $(H, *)$, we say that (G, \cdot) and $(H, *)$ are *isomorphic* and write $(G, \cdot) \cong (H, *)$.

34

3.Homomorphisms

- 3.2.Examples of Homomorphisms
 - The function $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$, defined by $f(x) = [x]$ is the group homomorphism.
 - Let \mathbb{R} be the group of all real numbers with operation addition, and let \mathbb{R}^+ be the group of all positive real numbers with operation multiplication. The function $f : \mathbb{R} \rightarrow \mathbb{R}^+$, defined by $f(x) = e^x$, is a homomorphism, for if $x, y \in \mathbb{R}$, then

$$f(x + y) = e^{x+y} = e^x e^y = f(x) f(y).$$
 Now f is an isomorphism, for its inverse function $g : \mathbb{R}^+ \rightarrow \mathbb{R}$ is $\ln x$. Therefore, the additive group \mathbb{R} is isomorphic to the multiplicative group \mathbb{R}^+ . Note that the inverse function g is also an isomorphism:

$$g(xy) = \ln(xy) = \ln x + \ln y = g(x) + g(y).$$

35

3.Homomorphisms

- 3.3.Theorem on Homomorphisms
- **Proposition 3.3.1.** Let $f : G \rightarrow H$ be a group morphism, and let e_G and e_H be the identities of G and H , respectively. Then
 - (i) $f(e_G) = e_H$.
 - (ii) $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.
- *Proof.* (i) Since f is a morphism, $f(e_G)f(e_G) = f(e_G e_G) = f(e_G) = f(e_G)e_H$. Hence (i) follows by cancellation in H .
- (ii) $f(a) f(a^{-1}) = f(a a^{-1}) = f(e_G) = e_H$ by (i). Hence $f(a^{-1})$ is the unique inverse of $f(a)$; that is $f(a^{-1}) = f(a)^{-1}$.

36

3. Homomorphisms

- If $f: G \rightarrow H$ is a group morphism, the *kernel* of f , denoted by $\text{Ker}f$, is defined to be the set of elements of G that are mapped by f to the identity of H . That is, $\text{Ker}f = \{g \in G \mid f(g) = e_H\}$
- **Proposition 3.3.2.** Let $f: G \rightarrow H$ be a group morphism. Then:
 - (i) $\text{Ker}f$ is a normal subgroup of G .
 - (ii) f is injective if and only if $\text{Ker}f = \{e_G\}$.
- **Proposition 3.3.3.** For any group morphism $f: G \rightarrow H$, the image of f , $\text{Im}f = \{f(g) \mid g \in G\}$, is a subgroup of H (although not necessarily normal).

37

3. Homomorphisms

- **Theorem 3.3.4. Morphism Theorem for Groups.** Let K be the kernel of the group morphism $f: G \rightarrow H$. Then G/K is isomorphic to the image of f , and the isomorphism $\psi: G/K \rightarrow \text{Im}f$ is defined by $\psi(Kg) = f(g)$.
- This result is also known as the **first isomorphism theorem**.
- *Proof.* The function ψ is defined on a coset by using one particular element in the coset, so we have to check that ψ is well defined; that is, it does not matter which element we use. If $Kg' = Kg$, then $g' \equiv g \pmod{K}$ so $g \cdot g^{-1} = k \in K = \text{Ker}f$. Hence $g \cdot = kg$ and so $f(g \cdot) = f(kg) = f(k)f(g) = e_H f(g) = f(g)$. Thus ψ is well defined on cosets.

38

3. Homomorphisms

- The function ψ is a morphism because $\psi(Kg_1Kg_2) = \psi(Kg_1g_2) = f(g_1g_2) = f(g_1)f(g_2) = \psi(Kg_1)\psi(Kg_2)$.
- If $\psi(Kg) = e_H$, then $f(g) = e_H$ and $g \in K$. Hence the only element in the kernel of ψ is the identity coset K , and ψ is injective. Finally, $\text{Im}\psi = \text{Im}f$, by the definition of ψ . Therefore, ψ is the required isomorphism between G/K and $\text{Im}f$.

39

3. Homomorphisms

- **Example 3.3.1. Show that the quotient group \mathbb{R}/\mathbb{Z} is isomorphic to the circle group $W = \{e^{i\theta} \in \mathbb{C} \mid \theta \in \mathbb{R}\}$.**
- Solution.* The set W consists of points on the circle of complex numbers of unit modulus, and forms a group under multiplication. Define the function $f: \mathbb{R} \rightarrow W$ by $f(x) = e^{2\pi ix}$. This is a morphism from $(\mathbb{R}, +)$ to (W, \cdot) because $f(x+y) = e^{2\pi i(x+y)} = e^{2\pi ix} \cdot e^{2\pi iy} = f(x) \cdot f(y)$. The morphism f is clearly surjective, and its kernel is $\{x \in \mathbb{R} \mid e^{2\pi ix} = 1\} = \mathbb{Z}$. Therefore, the morphism theorem implies that $\mathbb{R}/\mathbb{Z} \cong W$.

40