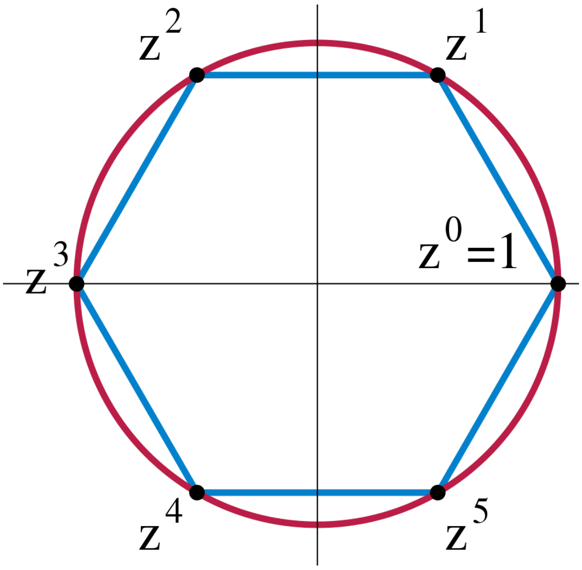
Abstract Algebra

Ji Yong-Hyeon



Ji Yong-Hyeon
May 22, 2023

Contents

Contents

Chapter 1

Introduction to Groups

1.1 Basic Axioms and Examples

Group

Definition 1.1. A **group** G is a non-empty set with a binary operation $*: G \times G \to G$ such that

(0) (Closure) $a, b \in G \implies a * b \in G$;

(1) (Associativitiy) $\forall a, b, c \in G : (a * b) * c = a * (b * c)$;

(2) (Identity) $\exists e \in G : \forall a \in G : a * e = e * a = a$;

(3) (Inverse) $\forall a \in G : \exists a^{-1} : a^{-1} * a = aa^{-1} = e$.

Remark 1.1. In particular, if

$$\forall a, b \in G : a * b = b * a,$$

G is called **abelian**.

Remark 1.2.

- If $|G| < \infty$, G is finite.
- If $|G| = \infty$, G is infinite.

Example 1.1. $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $* = +$ are groups so that $e = 0$ and $a^{-1} = -a$.

Example 1.2. Is $\mathbb{N} = \{1, 2, 3, \cdots\}$ a group? No $1 \in \mathbb{N}$ and $-1 \notin \mathbb{N}$. But $\mathbb{N}$ is a semi-group (i.e., a set with an associative binary operation).

Example 1.3. $G = \mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$ with $* = \cdot$ are groups so that $e = 1$ and $a^{-1} = \frac{1}{a}$. Note that $\mathbb{Z}^\times = \mathbb{Z} \setminus \{0\}$ is not a group under $\cdot$ since $\frac{1}{2} \in \mathbb{Z}$.

Example 1.4 (Finite Group).

- Modular group $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \cdots, n-1\}$ with $+_n$.
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in (\mathbb{Z}/n\mathbb{Z}) : (a, n) = 1\}$ where $(a, n) = \gcd(a, n)$ is a group under $\cdot_n$.

  Proof. Since $(a, n) = 1$, $\exists x, y \in \mathbb{Z}$ s.t. $ax + ny = 1$. Take mod n on both sides:

  $$\begin{aligned} ax &\equiv 1 \pmod{n}, \\ a^{-1} &\equiv x \pmod{n}. \end{aligned}$$

  ☐

Basic Properties of a Group

Proposition 1.1. *Let G be a group with $*$ (normally omitted). Then*

(1) $\exists! e \in G$;

(2) $\exists! a^{-1}$

(3) $\forall a \in G : \left(a^{-1}\right)^{-1} = a$

(4) $\forall a, b \in G : ab^{-1} = b^{-1}a^{-1}$

(5) (Generalized Associative Law) for any $a_1, a_2, \ldots, a_n \in G$, the value of $a_1 * a_2 * \cdots * a_n$ is independent of how the expression is bracketed.

Proof. content... ☐

Advanced Properties of a Group

Proposition 1.2. *Let G be a group and $a, b, u, v \in G$. Then*

(1) (Left Cancellation) $au = av \implies u = v$

(2) (Right Cancellation) $ua = va \implies u = v$

(3) $ab = e \implies ba = e$

Proof. (1) $au = av \implies a^{-1}(au) = a^{-1}(av) \implies (a^{-1}a)u = (a^{-1}a)v \implies u = v$.

(2)

(3) $ab = e \implies a^{-1}(ab) = a^{-1}e \implies b = a^{-1} \implies ba = e$.

☐

Order

Definition 1.2. Let G be a group and $a \in G$. The **order** of a is the smallest positive integer $n \in \mathbb{N}$ such that $a^n = 1 = e_G$ where $a^n = a \cdots a \cdots a$ (n copies of a). It is denoted by $|a|$ (or $\operatorname{ord}(a)$). If such an integer n does not exists, the order of a is called infinite denoted by $|a| = \infty$.

Example 1.5.

- Let $G = (\mathbb{Z}, +)$. Then $|0| = 0$ and $|n| = \infty$ for $n \neq 0$.
- $G = (\mathbb{Z}/10\mathbb{Z}, +)$. Then $|0| = 0$, $|1| = |3| = |7| = |9| = 10$, $|5| = 2$ and $|2| = |4| = |6| = |8| = 5$.
- $G = ((\mathbb{Z}/10\mathbb{Z})^{\times} = \{1, 3, 7, 9\}, \cdot)$. Then $|9| = 1$ and $|3| = |7| = 4$.

Exercise

Let G be a group. (1, 5, ~~6~~, 11, 12, 13, 14, 20, 21, 22, 25, 31)

1. Determine which of the following binary operations are associative:

(a) the operation $*$ on $\mathbb{Z}$ defined by $a * b = a - b$

(b) the operation $*$ on $\mathbb{R}$ defined by $a * b = a + b + ab$

(c) the operation $*$ on $\mathbb{Q}$ defined by $a * b = \dfrac{a+b}{5}$

(d) the operation $*$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) * (c, d) = (ad + bc, bd)$

(e) the operation $*$ on $\mathbb{Q} \setminus \{0\}$ defined by $a * b = \dfrac{a}{b}$.

Sol. (a) Note that

$$
\begin{aligned}
(a * b) * c &= (a - b) * c = a - b - c, \\
a * (b * c) &= a * (b - c) = a - b + c.
\end{aligned}
$$

Because $(a-b-c) \neq (a-b+c)$ in general, the operation is not associative.'

(b) Note that

$$
\begin{aligned}
(a * b) * c = (a + b + ab) * c \quad &= (a + b + ab) + (c) + (ac + bc + abc) \\
&= a + b + c + ab + bc + ca + abc,
\end{aligned}
$$

$$
\begin{aligned}
a * (b * c) = a * (b + c + bc) \quad &= (a) + (b + c + bc) + (ab + ac + abc) \\
&= a + b + c + ab + bc + ca + abc.
\end{aligned}
$$

Thus the operation is associative.

(c) Note that

$$
\begin{aligned}
(a * b) * c &= \left(\frac{a+b}{5}\right) * c = \frac{\frac{a+b}{5} + c}{5} = \frac{a + b + 5c}{25}, \\
a * (b * c) &= a * \left(\frac{b+c}{5}\right) = \frac{a + \frac{b+c}{5}}{5} = \frac{5a + b + c}{25}.
\end{aligned}
$$

Because $\frac{a+b+5c}{25} \neq \frac{5a+b+c}{25}$ in general, the operation is not associative.

(d) Note that

$$
\begin{aligned}
[(a, b) * (c, d)] * (e, f) &= (ad + bc, bd) * (e, f) \\
&= ((ad + bc)f + bde, bdf) = (adf + bcf + bde, bdf),
\end{aligned}
$$

$$
\begin{aligned}
(a, b) * [(c, d) * (e, f)] &= (a, b) * (de + cf, df) \\
&= (adf + (de + cf)b, bdf) = (adf + bde + bcf, bdf).
\end{aligned}
$$

Thus the operation is associative.

(e) Note that

$$(a * b) * c = \left(\frac{a}{b}\right) * c = \frac{\frac{a}{b}}{c} = \frac{a}{bc},$$
$$a * (b * c) = a * \left(\frac{b}{c}\right) = \frac{a}{\frac{b}{c}} = \frac{ac}{b}.$$

Because $\frac{a}{bc} \neq \frac{ac}{b}$ in general, the operation is not associative.

□

2. Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

Sol. In the case of $\mathbb{Z}/n\mathbb{Z}$ under multiplication, the identity element is $[1]_n$[1], and associativity and closure hold. However, the inverses condition does not hold.

To show this, consider the equivalence class $[0]_n \in \mathbb{Z}/n\mathbb{Z}$. Clearly

$$a * [0]_n = [0]_n \quad (\forall a \in \mathbb{Z}/n\mathbb{Z}).$$

Thus, $[0]_n$ has no multiplicative inverse.

Therefore, $\mathbb{Z}/n\mathbb{Z}$ under multiplication is not a group for $n > 1$. □

3. Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

Sol.

Element	0	1	2	3	4	5	6	7	8	9	10	11
Order	1	12	6	4	3	12	2	12	3	4	6	12

□

4. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{7}, \overline{-7}, \overline{13}$.

Sol. Note that

$$(\mathbb{Z}/12\mathbb{Z})^\times = \{a \in \mathbb{Z}/12\mathbb{Z} : (a, 12) = 1\} = \{1, 5, 7, 11\}.$$

Then

Element	$\overline{1}$	$\overline{-1}$	$\overline{5}$	$\overline{7}$	$\overline{-7}$	$\overline{13}$
Order	1	2	2	2	2	1

[1]the equivalence class of 1 modulo n.

$\square$

5. Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: $\overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.

Sol.

Element	$\overline{1}$	$\overline{2}$	$\overline{6}$	$\overline{9}$	$\overline{10}$	$\overline{12}$	$\overline{-1}$	$\overline{-10}$	$\overline{-18}$
Order	36	18	6	4	18	3	36	18	2

$\square$

6. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^{\times}$: $\overline{1}, \overline{-1}, \overline{5}, \overline{13}, \overline{-13}, \overline{17}$.

Sol. Note that

$(\mathbb{Z}/36\mathbb{Z})^{\times} = \{a \in \mathbb{Z}/36\mathbb{Z} : (a, 36) = 1\} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.

Then

Element	$\overline{1}$	$\overline{-1}$	$\overline{5}$	$\overline{13}$	$\overline{-13}$	$\overline{17}$
Order	1	2	6	3	3	3

$\square$

7. For x an element in G show that x and x^{-1} have the same order.

Sol. Assume $x^n = e$. Then

$$(x^{-1})^n = x^{-n} = (x^n)^{-1} = e^{-1} = e.$$

Therefore, the order of x^{-1} is also n. $\square$

8. Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.

Sol. Let $n = 2m + 1$ for some $m \in \mathbb{Z}$. Note that

$$(x^2)^m = x^{2m} = x^{n-1} = x^n x^{-1} = ex^{-1} = x^{-1}.$$

Thus

$$x = (x^{-1})^{-1} = (x^{2m})^{-1} = x^{2(-m)}.$$

So we have that $x = (x^2)^k$ for $k = -m$. $\square$

9. If x and g are elements of the group G, prove that $|x| = \left|g^{-1}xg\right|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Sol. Let's denote $y = g^{-1}xg$. Let $n = |x|$, then $x^n = e$. Using the group property of associativitiy, y^n can be rewritten as:

$$\begin{aligned} y^n = (g^{-1}xg)^n &= \underbrace{(g^{-1}xg)(g^{-1}xg)\cdots(g^{-1}xg)}_{n \text{ times}} \\ &= g^{-1}x(gg^{-1})x(gg^{-1})x\cdots(gg^{-1})xg \\ &= g^{-1}x^n g \\ &= g^{-1}eg \\ &= g^{-1}g \\ &= e. \end{aligned}$$

Thus, $|x| = n = \left|g^{-1}xg\right|$.

To deduce that $|ab| = |ba|$, we apply the previous result with $x = ab$ and $g = a$:

$$\begin{aligned} |ab| &= \left|a^{-1}(ab)a\right| && \text{by previous result} \\ &= \left|(a^{-1}a)ba\right| \\ &= |ba|. \end{aligned}$$

□

10. Prove that if $x^2 = 1$ for all $x \in G$ then G abelian.

Sol. We are given that for all $x \in G$, $x^2 = e$ where e is the identity element of G. We need to show that G is abelian, i.e., for all $a, b \in G$, $ab = ba$.

Given any $a, b \in G$, consider the product $aba^{-1}b^{-1}$:

$aba^{-1}b^{-1} = abe = ab$ since $a^{-1} = a$ and $b^{-1} = b$.

Then we multiply by b^{-1} and a^{-1} from the right:

$ab = aba^{-1}b^{-1}b^{-1}a^{-1} = abab = (ab)^2 = e$.

Multiply by ba from the left:

$ba = (ba)ab = ba(ab) = ba$.

So, $ab = ba$ for all $a, b \in G$, and thus G is abelian, as required. This completes the proof. □

11. Prove that any finite group G of even order contains an element of order 2. [Hint: Let $t(G)$ be the set $\left\{g \in G : g \neq g^{-1}\right\}$. Show that $t(G)$ has an even number of element and every non-identity element of $G \setminus t(G)$ has order 2.]

Sol. Let's denote by $|G|$ the order of G, i.e., the number of elements in G. By assumption, $|G|$ is even.

We know that for any group, G, the inverse of each element is also in G, and each element pairs uniquely with its inverse.

Consider the set $t(G) = g \in G : g \neq g^{-1}$. Since each element in $t(G)$ and its inverse are distinct, we can pair them up, meaning the total number of elements in $t(G)$ is even.

Now consider the set $G \setminus t(G)$, which are all the elements of G not in $t(G)$. This set consists of all elements that are their own inverse, i.e., for all $g \in G \setminus t(G)$, we have $g = g^{-1}$.

The identity element, e, is in $G \setminus t(G)$, since $e = e^{-1}$.

Now, let's consider a non-identity element $x \in G \setminus t(G)$. Since x is in this set, we have $x = x^{-1}$, and so $x^2 = x \cdot x^{-1} = e$. Therefore, the order of x is 2.

Now, since $|G|$ is even and $|t(G)|$ is even, the number of elements in $G \setminus t(G)$ must be even as well. But we know that at least one element in $G \setminus t(G)$ is the identity. So, there must be at least one other element in $G \setminus t(G)$, and by the previous paragraph, this element must have order 2.

Therefore, any finite group of even order contains an element of order 2, completing the proof. □

Chapter 2

Introduction

2.1 What is group theory?

Group theory is a branch of mathematics that studies groups, which are sets of elements that have a binary operation defined between them. The operation must satisfy certain properties, such as closure, associativity, identity, and invertibility. Groups arise naturally in many areas of mathematics, physics, chemistry, and computer science.

In group theory, we study the properties of groups and the relationships between different groups. Some of the main topics in group theory include:

- Group structure and classification
- Subgroups and quotient groups
- Homomorphisms and isomorphisms
- Group actions and representations
- Group cohomology and other algebraic topological concepts

Group theory has many applications in various areas of mathematics, physics, and other sciences. For example, group theory is used in cryptography to create secure encryption schemes, and in particle physics to study the fundamental symmetries of the universe.

Overall, group theory is a rich and fascinating area of mathematics with many important applications and connections to other fields of study.

2.2 History of group theory

Group theory has its roots in several branches of mathematics, including number theory, geometry, and algebra. The study of symmetry in geometry and crystallography played a key role in the development of group theory.

One of the earliest pioneers of group theory was Evariste Galois, a French mathematician who made important contributions to the theory of equations and the study of groups in the early 19th century. His work laid the foundation for the modern theory of groups.

In the late 19th century, the German mathematician Felix Klein developed the theory of transformation groups, which became a major area of research in group theory. Klein's work on continuous groups, such as Lie groups, also had important applications in physics.

The Russian mathematician Sophus Lie made significant contributions to the study of Lie groups and their applications in geometry and physics. Lie's work on the theory of continuous groups has had a profound impact on many areas of mathematics and science.

In the 20th century, group theory became an important tool in many areas of mathematics, including algebraic geometry, number theory, and topology. The study of finite groups, in particular, has become a major area of research, with important applications in coding theory, cryptography, and other areas.

Today, group theory continues to be a vibrant and active area of research, with new insights and discoveries being made all the time. It remains an essential tool for understanding the symmetries and structures that underlie many areas of mathematics, science, and engineering.

2.3 Applications of group theory

Group theory has numerous applications in mathematics, science, and engineering. Here are some examples:

2.3.1 Coding Theory

Group theory has important applications in coding theory, which is used in the design of error-correcting codes for digital communication. By using the symmetries of codes and their generators, coding theorists can construct efficient and reliable codes that are resistant to errors and noise.

2.3.2 Cryptography

Group theory is also used in cryptography, which is the science of secure communication. By using the properties of certain groups, cryptographers can design encryption algorithms that are difficult to break, ensuring the confidentiality and integrity of sensitive information.

2.3.3 Computer Graphics

Group theory is used in computer graphics to study the symmetries of shapes and images. By understanding these symmetries, computer graphics designers can create visually appealing and aesthetically pleasing images and animations.

2.4 Catgories

Category

Definition 2.1. A category $\mathbf{C}$ consists of:

1. A collection of objects Obj($\mathbf{C}$)
2. For each pair of objects $A, B \in \text{Obj}(\mathbf{C})$, a collection of morphisms $\text{Hom}\mathbf{C}(A, B)$
3. For each object $A \in \text{Obj}(\mathbf{C})$, an identity morphism $\text{Id}_A \in \text{Hom}\mathbf{C}(A, A)$
4. For each triple of objects $A, B, C \in \text{Obj}(\mathbf{C})$, a composition operation $\circ : \text{Hom}\mathbf{C}(B, C) \times \text{Hom}\mathbf{C}(A, B) \to \text{Hom}\mathbf{C}(A, C)$

such that the following axioms hold:

1. Composition is associative: $f \circ (g \circ h) = (f \circ g) \circ h$ for all morphisms f, g, h that can be composed.
2. Identity morphisms are identity elements for composition: $\text{Id}_A \circ f = f$ and $f \circ id_A = f$ for all morphisms f that can be composed with Id_A.

A collection of objects: denoted by C. These objects can be anything: sets, groups, topological spaces, etc. They are often written in uppercase letters such as A, B, C, etc.

A collection of morphisms: denoted by $\text{Hom}(A, B)$, where A and B are objects in the category. These morphisms are often written as $f : A \to B$. The morphisms represent some kind of relationship or transformation between the objects. The collection of morphisms is required to satisfy the following axioms:

Identity: For every object A in the category, there exists a unique morphism $1_A : A \to A$ called the identity morphism, such that for any morphism $f : A \to B$, we have $f \circ 1_A = f$ and $1_B \circ f = f$.

Associativity: For any objects A, B, and C in the category, and any morphisms $f : A \to B$, $g : B \to C$, and $h : C \to D$, we have $(h \circ g) \circ f = h \circ (g \circ f)$.

A composition operation: denoted by $\circ$. This operation takes two morphisms $f : A \to B$ and $g : B \to C$ and produces a new morphism $g \circ f : A \to C$. The composition operation is required to be associative, meaning that $(h \circ g) \circ f = h \circ (g \circ f)$.

$$A \xrightarrow{f} B \xrightarrow{g} C$$

1. The category of sets, where the objects are sets and the morphisms are functions between those sets.
2. The category of groups, where the objects are groups and the morphisms are group homomorphisms between those groups.

3. The category of topological spaces, where the objects are topological spaces and the morphisms are continuous functions between those spaces.

4. The category of vector spaces, where the objects are vector spaces and the morphisms are linear transformations between those spaces.

5. The category of finite sets, where the objects are finite sets and the morphisms are functions between those sets.

6. The category of graphs, where the objects are graphs and the morphisms are graph homomorphisms between those graphs.

7. The category of categories, where the objects are categories and the morphisms are functors between those categories.

8. The category of simplicial sets, where the objects are simplicial sets and the morphisms are simplicial maps between those sets.

9. The category of algebraic structures, where the objects are algebraic structures such as groups, rings, and fields, and the morphisms are structure-preserving maps between those structures.

10. The category of schemes, where the objects are schemes and the morphisms are morphisms of schemes.

Chapter 3

Basic Concepts

3.1 Definition of a group

Group

Definition 3.1. A **group** is a set G equipped with a binary operation $\cdot : G \times G \to G$ that satisfies the following axioms:

1. **Closure:** $g, h \in G \implies g \cdot h \in G$.
2. **Associativity:** $g, h, k \in G \implies (g \cdot h) \cdot k = g \cdot (h \cdot k)$.
3. **Identity Element:** $\exists e \in G : [g \in G \implies g \cdot e = e \cdot g = g]$.
4. **Inverse Element:** $g \in G \implies [\exists g^{-1} \in G : [g \cdot g^{-1} = g^{-1} \cdot g = e]]$.

For example, the set of integers $\mathbb{Z}$ equipped with addition is a group. This is because addition satisfies the closure, associativity, identity element, and inverse element axioms. The identity element is 0, and the inverse of an integer n is $-n$.

3.2 Subgroups

A subgroup H of a group G is a subset of G that is also a group under the same group operation as G. In other words, H must satisfy the following conditions:

1. The identity element of G is in H.
2. If x and y are in H, then their product xy is also in H.
3. If x is in H, then its inverse x^{-1} is also in H.

Here are some examples of subgroups:

- The trivial subgroup, consisting only of the identity element.
- The whole group G itself.

- The center of G, consisting of all elements that commute with every element in G.
- The cyclic subgroup generated by an element g of G, denoted $\langle g \rangle$.
- The subgroup of the symmetric group S_n consisting of all permutations that fix a particular element.

Here are some exercises to practice working with subgroups:

1. Let G be a group, and let H and K be subgroups of G. Prove that $H \cap K$ is a subgroup of G.
2. Let G be a group, and let H and K be subgroups of G. Prove that $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G.
3. Let G be a group, and let H be a subgroup of G. Prove that H is normal in G if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.

3.2.1 Normal subgroups

3.3 Generators

3.4 Cyclic groups

3.5 Homomorphisms

Chapter 4

Group Actions

4.1 Definitions and Examples

4.2 Orbit-Stabilizer Theorem

4.3 Applications

Chapter 5

Sylow Theorems

5.1 Sylow's First Theorem

5.2 Sylow's Second Theorem

5.3 Sylow's Third Theorem

5.4 Applications

Chapter 6

Finite Abelian Groups

6.1 Classification

6.2 Invariant Factors and Elementary Divisors

Chapter 7

Solvable and Nilpotent Groups

7.1 Definitions and Examples

7.2 Properties

7.3 Applications

Chapter 8

Representation Theory

8.1 Definitions and Examples

8.2 Schur's Lemma

8.3 Maschke's Theorem

8.4 Character Theory

Chapter 9

Group Cohomology

9.1 Definitions and Examples

9.2 Cohomology of Groups

9.3 Applications

Chapter 10

Appendix

10.1 Basic Algebraic Structures

10.2 Category Theory