Abstract Algebra Note

Author: isomo

Date: December 27, 2024

Contents

Chapter 1 Group Theory **1**

1.1 Monoid Group 1

Chapter 2 Ring Theory **4**

Chapter 3 Polynomial Theory **5**

Chapter 4 Field Theory **6**

Chapter 1 Group Theory

1.1 Monoid Group

Definition 1.1 (monoid)

We say that $(S, *)$ is a monoid if the binary operation satisfies the associative law and has an identity element. That is,

$$\forall x, y, z \in S, \quad x * (y * z) = (x * y) * z$$

and

$$\exists e \in S, \forall x \in S, \quad e * x = x * e = x$$

♣

Definition 1.2 (commutative monoid)

We say that $(S, *)$ is a commutative monoid if it is a monoid and the operation satisfies the commutative law. That is,

$$\forall x, y \in S, \quad x * y = y * x$$

♣

Proposition 1.1 (unique of identity element)

Let $(S, \cdot)$ be a monoid. Then the identity element is unique.

♠

Proof Suppose that e and e' are both identity elements of S. Then

$$e = e \cdot e' = e'$$

so $e = e'$. □

Proposition 1.2 (expand of associative law)

Let $x_1, \ldots, x_n, y_1, \ldots, y_m \in S$. Then

$$x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot y_1 \cdot y_2 \cdot \ldots \cdot y_m = (x_1 \cdot x_2 \cdot \ldots \cdot x_n) \cdot (y_1 \cdot y_2 \cdot \ldots \cdot y_m)$$

♠

Proof We prove this by induction on n.

Base Case ($n = 1$): When $n = 1$, the statement simplifies to:

$$x_1 \cdot y_1 \cdot y_2 \cdot \ldots \cdot y_m = x_1 \cdot (y_1 \cdot y_2 \cdot \ldots \cdot y_m)$$

This is clearly true by the associative property of multiplication.

Inductive Step: Assume the statement holds for $n = k$, that is:

$$x_1 \cdot x_2 \cdot \ldots \cdot x_k \cdot y_1 \cdot y_2 \cdot \ldots \cdot y_m = (x_1 \cdot x_2 \cdot \ldots \cdot x_k) \cdot (y_1 \cdot y_2 \cdot \ldots \cdot y_m)$$

We need to show that the statement holds for $n = k + 1$. Consider:

$$x_1 \cdot x_2 \cdot \ldots \cdot x_k \cdot x_{k+1} \cdot y_1 \cdot y_2 \cdot \ldots \cdot y_m$$

By the associative property, we can regroup the terms as:

$$(x_1 \cdot x_2 \cdot \ldots \cdot x_k \cdot x_{k+1}) \cdot (y_1 \cdot y_2 \cdot \ldots \cdot y_m)$$

Using the inductive hypothesis on the first k terms, we have:

$$(x_1 \cdot x_2 \cdot \ldots \cdot x_k) \cdot x_{k+1} \cdot (y_1 \cdot y_2 \cdot \ldots \cdot y_m) = (x_1 \cdot x_2 \cdot \ldots \cdot x_k \cdot x_{k+1}) \cdot (y_1 \cdot y_2 \cdot \ldots \cdot y_m)$$

Thus, the statement holds for $n = k + 1$.

□

Proposition 1.3

Let $x \in S$ and $m, n \in \mathbb{N}$. Then

$$x^{m+n} = x^m \cdot x^n$$

♠

Proof We will prove this in three steps:

Step 1: First, recall from Proposition 1.2 that for any elements in S:

$$x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot y_1 \cdot y_2 \cdot \ldots \cdot y_m = (x_1 \cdot x_2 \cdot \ldots \cdot x_n) \cdot (y_1 \cdot y_2 \cdot \ldots \cdot y_m)$$

Step 2: Now, consider the special case where all elements are equal to x:

- Let $x_1 = x_2 = \ldots = x_m = x$
- Let $y_1 = y_2 = \ldots = y_n = x$

Step 3: By definition of exponentiation in a monoid:

$$\begin{aligned} x^{m+n} &= \underbrace{x \cdot x \cdot \ldots \cdot x}_{m+n \text{ times}} \\ &= (\underbrace{x \cdot x \cdot \ldots \cdot x}_{m \text{ times}}) \cdot (\underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}}) \\ &= x^m \cdot x^n \end{aligned}$$

Therefore, we have proved that $x^{m+n} = x^m \cdot x^n$ for all $x \in S$ and $m, n \in \mathbb{N}$. □

Definition 1.3 (Submonoid)

Let $(S, \cdot)$ be a monoid. If $T \subset S$, we say that $(T, \cdot)$ is a submonoid of $(S, \cdot)$ if:

1. *The identity element $e \in T$*
2. *T is closed under multiplication, that is:*

$$\forall x, y \in T, \quad x \cdot y \in T$$

♣

Proposition 1.4

If $(T, \cdot)$ is a submonoid of $(S, \cdot)$, then $(T, \cdot)$ is a monoid.

♠

Proof We need to verify two properties:

1. The operation is associative in T:
   Since $T \subset S$ and $\cdot$ is associative in S, it is also associative in T.
2. T has an identity element:
   By definition of submonoid, the identity element $e \in T$.

Therefore, $(T, \cdot)$ satisfies all properties of a monoid. □

Definition 1.4 (Monoid Homomorphism)

Let $(S, \cdot)$ and $(T, *)$ be monoids, and let $f : S \to T$ be a mapping. We say f is a monoid homomorphism if f preserves multiplication and maps the identity element to the identity element. That is:

1. *For all $x, y \in S$:*

$$f(x \cdot y) = f(x) * f(y)$$

2. *For the identity elements $e \in S$ and $e' \in T$:*

$$f(e) = e'$$

♣

Remark While a homomorphism preserves operations, an isomorphism represents complete structural equivalence. An isomorphism is first a **bijective mapping**, meaning it establishes a one-to-one correspondence between elements - essentially “relabeling” elements uniquely. Beyond being bijective, an isomorphism preserves operations under this relabeling, implying that the only difference between two structures (like monoids) is their labeling.

Example 1.1 Different Types of Monoid Maps Let’s examine several maps between monoids:

1. **A homomorphism that is not an isomorphism:** Consider $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by $f(n) = 2n$
   - Preserves operation: $f(a + b) = 2(a + b) = 2a + 2b = f(a) + f(b)$
   - Is injective: $f(a) = f(b) \implies 2a = 2b \implies a = b$
   - Not surjective: odd numbers are not in the image
   - Therefore: homomorphism but not isomorphism
2. **Another non-isomorphic homomorphism:** Consider $h : (\mathbb{Z}, +) \to (\mathbb{Z}_2, +)$ defined by $h(n) = n \bmod 2$
   - Preserves operation: $h(a + b) = (a + b) \bmod 2 = (a \bmod 2 + b \bmod 2) \bmod 2 = h(a) + h(b)$
   - Not injective: $h(0) = h(2) = 0$
   - Surjective: image is all of $\mathbb{Z}_2$
   - Therefore: homomorphism but not isomorphism
3. **An isomorphism:** Consider $g : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by $g(n) = -n$
   - Preserves operation: $g(a + b) = -(a + b) = -a + (-b) = g(a) + g(b)$
   - Bijective: one-to-one correspondence
   - Has inverse function: $g^{-1}(n) = -n$
   - Therefore: isomorphism
4. **An isomorphism between different monoids:**
   - Homomorphisms preserve structure but may ”collapse” elements
   - Isomorphisms preserve both structure and distinctness of elements
   - The same set can have different monoid structures that are isomorphic

Chapter 2　Ring Theory

Chapter 3 Polynomial Theory

Chapter 4   Field Theory