



代数笔记

作者: isomo

时间: December 28, 2024

前言

抽象代数笔记，主要的面向还是自我的学习，写作上的风格也是信息密度较低，冗余啰嗦的。

第一次接触是，一本英文的抽象代数的书，多是定理的证明，看着很慢，也没有感觉到什么实际的应用。但是时间也花了不少，为此我们想找找中文的资料，看看有没有更好的学习方式。一去小破站上搜一下视频，发现了 **maki** 讲抽象代数的视频，配合讲义，深入浅出，很棒的工作。但是内容上来说，还是有些不太完善的地方。在刷到一个推荐学习代数的书之后，李文威老师的《代数学方法》，为此我们在此基础上记录一些笔记，以便后续的学习。后续参考资料还有变化的话，会及时更新。

目录

第 1 章 Group Theory	1
1.1 Monoid Group	1
1.2 Group	4
第 2 章 Ring Theory	8
第 3 章 Ring Theory	9
第 4 章 Ring Theory	10
第 5 章 Ring Theory	11
第 6 章 Ring Theory	12
第 7 章 Polynomial Theory	13
第 8 章 Field Theory	14

第 1 章 Group Theory

1.1 Monoid Group

定义 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

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



定义 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,

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



命题 1.1 (unique of identity element)

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



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

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

so $e = e'$.



命题 1.2 (expand of associative law)

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

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



证明 We prove this by induction on n .

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

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

This is clearly true by the associative property of multiplication.

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

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

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

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

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

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

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

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

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

命题 1.3

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

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

证明 We will prove this in three steps:

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

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

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

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

Step 3: By definition of exponentiation in a monoid:

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

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

定义 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:

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

命题 1.4

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

证明 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. □

定义 1.4 (Monoid Homomorphism)

Let (S, \cdot) and $(T, *)$ be monoids, and let $f : S \rightarrow T$ 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 $e' \in T$:

$$f(e) = e'$$



注 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.

例题 1.1 Different Types of Monoid Maps Let's examine several maps between monoids:

1. **A homomorphism that is not an isomorphism:** Consider $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ 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. **Non-isomorphic homomorphism:** Consider $h : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_2, +)$ 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

定义 1.5 (Generated Submonoid)

Let (S, \cdot) be a monoid and $A \subset S$ be a subset. The submonoid generated by A , denoted by $\langle A \rangle$, is defined as the intersection of all submonoids of S containing A . That is:

$$\langle A \rangle = \bigcap \{T \subset S : T \supset A, T \text{ is a submonoid}\}$$

**命题 1.5**

Let (S, \cdot) be a monoid and $A \subset S$ be a subset. Then $\langle A \rangle$ is also a submonoid. Therefore, it is the smallest submonoid containing A .



证明 We will prove this in two steps:

Step 1: Show $\langle A \rangle$ contains the identity element

Let $\{T_\alpha\}_{\alpha \in I}$ be the collection of all submonoids containing A . Each T_α contains the identity e (by definition of submonoid), Therefore $e \in \bigcap_{\alpha \in I} T_\alpha = \langle A \rangle$

Step 2: Show closure under multiplication

Let $x, y \in \langle A \rangle = \bigcap_{\alpha \in I} T_\alpha$, Then $x, y \in T_\alpha$ for all $\alpha \in I$. Since each T_α is a submonoid, $x \cdot y \in T_\alpha$ for all

$\alpha \in I$, Therefore $x \cdot y \in \bigcap_{\alpha \in I} T_\alpha = \langle A \rangle$.

□

定义 1.6 (Monoid Isomorphism)

Let (S, \cdot) and $(T, *)$ be monoids, and let $f : S \rightarrow T$ be a mapping. We say f is a monoid isomorphism if f is bijective and a homomorphism. That is:

1. f is bijective (one-to-one and onto)
2. For all $x, y \in S$:

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

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

$$f(e) = e'$$



命题 1.6

If $f : (S, \cdot) \rightarrow (T, *)$ is a monoid isomorphism, then $f^{-1} : T \rightarrow S$ is a monoid homomorphism. Therefore, f^{-1} is also a monoid isomorphism.



证明 Since f is an isomorphism, f^{-1} exists and is bijective. We need to show:

1. f^{-1} preserves operation:

$$\begin{aligned} f^{-1}(a * b) &= f^{-1}(f(f^{-1}(a)) * f(f^{-1}(b))) \\ &= f^{-1}(f(f^{-1}(a) \cdot f^{-1}(b))) \\ &= f^{-1}(a) \cdot f^{-1}(b) \end{aligned}$$

2. f^{-1} preserves identity:

$$f^{-1}(e') = e \text{ where } e' \text{ and } e \text{ are identity elements}$$

Therefore, f^{-1} is both a homomorphism and bijective, making it an isomorphism.

□

1.2 Group

定义 1.7 (Invertible Element)

Let (S, \cdot) be a monoid and $x \in S$. We say x is invertible if and only if

$$\exists y \in S, x \cdot y = y \cdot x = e$$

where y is called the inverse of x , denoted as x^{-1} .



命题 1.7 (Uniqueness of Inverse)

Let (S, \cdot) be a monoid. If $x \in S$ is invertible, then its inverse is unique. That is, if $y, y' \in S$ are both inverses of x , then $y = y'$.



证明 Let y and y' be inverses of x . Then:

$$\begin{aligned}
 y &= y \cdot e \\
 &= y \cdot (x \cdot y') \\
 &= (y \cdot x) \cdot y' \\
 &= e \cdot y' \\
 &= y'
 \end{aligned}$$

Therefore, the inverse is unique. □

定义 1.8 (Group)

Let (G, \cdot) be a monoid. We say it is a group if every element in G is invertible.

Equivalently, if \cdot is a binary operation on G , we say (G, \cdot) is a group, or G forms a group under \cdot , when this operation satisfies:

1. Associativity: For all $x, y, z \in G$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

2. Identity element: There exists $e \in G$ such that for all $x \in G$

$$x \cdot e = e \cdot x = x$$

3. Inverse elements: For each $x \in G$, there exists $y \in G$ such that

$$x \cdot y = y \cdot x = e$$



命题 1.8

Let (G, \cdot) be a group and $x \in G$. Then $(x^{-1})^{-1} = x$. ♠

证明 Let $y = x^{-1}$. Then:

$$y \cdot x = x \cdot y = e$$

This shows that x is the inverse of $y = x^{-1}$. Therefore, $(x^{-1})^{-1} = x$. □

命题 1.9 (Inverse of Product)

Let (G, \cdot) be a group and $x, y \in G$. Then $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. ♠

证明 We will show that $y^{-1} \cdot x^{-1}$ is the inverse of $x \cdot y$:

$$\begin{aligned}
 (x \cdot y)(y^{-1} \cdot x^{-1}) &= x \cdot (y \cdot y^{-1}) \cdot x^{-1} \\
 &= x \cdot e \cdot x^{-1} \\
 &= x \cdot x^{-1} \\
 &= e
 \end{aligned}$$


Similarly, $(y^{-1} \cdot x^{-1})(x \cdot y) = e$. Therefore, $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. □

定义 1.9 (Abelian Group)

Let (G, \cdot) be a group. We say it is an abelian group, or commutative group, if the operation satisfies the commutative law:

$$\forall x, y \in G, \quad x \cdot y = y \cdot x$$

**引理 1.1**

Let (S, \cdot) be a monoid and let G be the subset of all invertible elements in S . Then (G, \cdot) is a group. 

证明 We need to verify three group axioms:

1. Closure: If $x, y \in G$, then $x \cdot y \in G$ (as product of invertible elements is invertible)
2. Identity: $e \in G$ (as e is invertible)
3. Inverse: If $x \in G$, then $x^{-1} \in G$ (by definition of invertible elements)

Associativity is inherited from S . Therefore, (G, \cdot) is a group. □

定义 1.10 (General Linear Group)

The group of $n \times n$ invertible real matrices under matrix multiplication is called the general linear group of degree n over the real numbers, denoted as $(GL(n, \mathbb{R}), \cdot)$. Since a matrix is invertible if and only if its determinant is nonzero:

$$GL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) : \det(A) \neq 0\}$$

**定义 1.11 (Special Linear Group)**

The special linear group of degree n over the real numbers is the group of $n \times n$ real matrices with determinant exactly 1 under matrix multiplication, denoted as $(SL(n, \mathbb{R}), \cdot)$. That is:

$$SL(n, \mathbb{R}) = \{A \in M(n, \mathbb{R}) : \det(A) = 1\}$$

**定义 1.12 (Subgroup)**

Let (G, \cdot) be a group and $H \subset G$. We say H is a subgroup of G , denoted as $H < G$, if it contains the identity element and is closed under multiplication and inverse operations. That is:

1. $\forall x, y \in H, \quad x \cdot y \in H$ (closure under multiplication)
2. $\forall x \in H, \quad x^{-1} \in H$ (closure under inverse)
3. $e \in H$ (contains identity)

**命题 1.10**

Let (G, \cdot) be a group. If H is a subgroup of G , then (H, \cdot) is also a group. 

证明 Since H is a subgroup:


1. Associativity: Inherited from G
2. Identity: $e \in H$ by definition of subgroup
3. Inverse: For all $x \in H, x^{-1} \in H$ by definition of subgroup
4. Closure: For all $x, y \in H, x \cdot y \in H$ by definition of subgroup

Therefore, (H, \cdot) satisfies all group axioms. □

命题 1.11

For convenience, we can combine the first two conditions of a subgroup definition 1.12 into one, reducing to two conditions:

1. $\forall x, y \in H, \quad x \cdot y^{-1} \in H$
2. $e \in H$

These conditions are equivalent to the original subgroup definition. 


证明

$(\Rightarrow) \forall y \in H, y^{-1} \in H$, then the closure under multiplication, $\forall x, y, y^{-1} \in H, x \cdot y^{-1} \in H$

$(\Leftarrow) \forall x, y \in H, x \cdot y^{-1} \in H$, let $x = e$, then have $\forall y \in H, y^{-1} \in H$; so $\forall x, y^{-1} \in H, x \cdot (y^{-1})^{-1} \in H$,

then $x \cdot y \in H$. □

命题 1.12

$(SL(n, \mathbb{R}), \cdot)$ is a group. 


证明 We verify the group axioms:

1. Closure: If $A, B \in SL(n, \mathbb{R})$, then $\det(AB) = \det(A) \det(B) = 1 \cdot 1 = 1$, so $AB \in SL(n, \mathbb{R})$
2. Identity: The identity matrix $I_n \in SL(n, \mathbb{R})$ since $\det(I_n) = 1$
3. Inverse: If $A \in SL(n, \mathbb{R})$, then $\det(A^{-1}) = \frac{1}{\det(A)} = 1$, so $A^{-1} \in SL(n, \mathbb{R})$
4. Associativity: Inherited from matrix multiplication

Therefore, $(SL(n, \mathbb{R}), \cdot)$ is a group. □


定义 1.13 (Group Homomorphism)

Let (G, \cdot) and $(G', *)$ be groups, and let $f : G \rightarrow G'$ be a mapping. We say f is a group homomorphism if it preserves the operation, that is:

$$\forall x, y \in G, \quad f(x \cdot y) = f(x) * f(y)$$


命题 1.13

Let $f : (G, \cdot) \rightarrow (G', *)$ be a group homomorphism. Then:

1. $f(e) = e'$ (preserves identity)
 2. $f(x^{-1}) = f(x)^{-1}$ (preserves inverses)
- 

证明

1. For identity element:

$$\begin{aligned} f(e) * f(e) &= f(e \cdot e) = f(e) \quad \text{left multiply by } f(e)^{-1} \\ \therefore f(e) &= e' \end{aligned}$$

2. For inverse elements:

$$\begin{aligned} f(x) * f(x^{-1}) &= f(x \cdot x^{-1}) = f(e) = e' \quad \text{left multiply by } f(x)^{-1} \\ \therefore f(x^{-1}) &= f(x)^{-1} \end{aligned}$$

□

第 2 章 Ring Theory

第 3 章 Ring Theory

第 4 章 Ring Theory

第 5 章 Ring Theory

第 6 章 Ring Theory

第 7 章 Polynomial Theory

第 8 章 Field Theory