

Algebra

Hoyan Mok¹

2020 年 7 月 24 日

¹E-mail: victoriesmo@hotmail.com

目录

目录	i
第一部分 线性代数	1
第一章 群. 环. 域	2
§1 代数运算	2
§2 群	3
§3 环	6
§4 域	8
参考文献	9
符号列表	10
索引	11

第一部分

线性代数

第一章 群. 环. 域

§1 代数运算

Definition 1.1 (二元运算). 集合的 Cartesian 平方到自身的映射 $*$: $X^2 \rightarrow X$ 称为其上的一个二元运算. 通常我们记 $*(a, b) := a * b$. 当 X 上定义了二元运算 $*$ 后, 称 $*$ 定义了 X 上的一种代数结构 $(X, *)$, 也称代数系统.

当指代是明确的时候, 我们将混用集合及其代数结构.

作为习惯, 如果 $\cdot, + \in X^{X^2}$, 我们记 $ab := a \cdot b$ 并称其为 a 和 b 的积, 称 $a + b$ 为 a 和 b 的和. 这些只是约定.

若 $a * b = b * a$ 则称 $*$ 或 $(X, *)$ 是交换的, 而若 $(a * b) * c = a * (b * c)$ 则称 $*$ 或 $(X, *)$ 为结合的.

若 $\exists e \in X$ 满足 $\forall x \in A (e * x = x * e = x)$, 则称其为 $*$ 的一个单位元 (identity), 这时可把 $(X, *)$ 记作 $(X, *, e)$. 可以证明一个代数结构最多只有一个单位元. 乘法单位元通常记为 1, 而加法单位元 (也叫零元) 记为 0.

Definition 1.2 (半群和么半群). 若 $*$ 是结合的, 称 $(X, *)$ 是半群 (semigroup); 若 $*$ 还有一个单位元, 则称 $(X, *, e)$ 是么半群 (monoid).

倘若么半群 $(M, *, e)$ 是有限的 (即其元素有限), 称 $\text{card } M$ 为有限么半群的阶.

作为重要的例子, 置换么半群定义为 $(X^X, \circ, \text{id}_X)$, 有么半群结构的 X^X 通常记作 $M(X)$. 半群中, 括号的位置是不重要的 (可用数学归纳法证明). 通常我们记 $x_1 x_2 \cdots x_n$ 为:

$$\prod_{i=1}^1 x_i = x_1, \prod_{i=1}^{n+1} x_i = \left(\prod_{i=1}^n x_i \right) x_n; \quad (1-1)$$

同理 $x_1 + x_2 + \cdots + x_n$ 为:

$$\sum_{i=1}^1 x_i = x_1, \sum_{i=1}^{n+1} x_i = \left(\sum_{i=1}^n x_i \right) + x_n. \quad (1-2)$$

在半群不交换的场合, 指出递推式右端的顺序是重要的. 这种记法称为**左正规**.

若 $x := x_1 = x_2 = \cdots = x_n$, 记 $\sum_{i=1}^n x_i = nx$, $\prod_{i=1}^n x_i = x^n$, 分别表示 x 的 n 倍和 x 的 n 次幂. 它们满足:

$$nx + mx = (n + m)x, \quad n(mx) = nm x, \quad n, m \in \mathbb{N}_+; \quad (1-3)$$

$$x^n x^m = x^{n+m}, \quad (x^m)^n = x^{nm}, \quad n, m \in \mathbb{N}_+. \quad (1-4)$$

在么半群中, 还可以令 $x^0 = 1, 0x = 0$.

若半群 S 有子集 S' , 使得 $(S', *)$ 是半群, 那么称其为半群 $(S, *)$ 的**子半群**. 同理有么半群 M 的**子么半群** M' .

若半群 $(S, *, e)$ 的元素 a 满足 $\exists a' \in S (aa' = a'a = e)$, 那么称 a 为**可逆的** (invertible), a' 称为其**逆元** (inverse element) 或**逆** (inverse). 通常加法逆元记为 $-a$, 乘法逆元记为 a^{-1} , 且为可逆元素引入 na, a^n 的概念, 其中 $n \in \mathbb{Z}$. 当 n 为负数时, $na = -(-na), a^n = (a^{-n})^{-1}$.

因为群未必是 Abelian, 我们可以也用弱化的**左可逆** $\exists y \text{ s.t. } y * x = 1$ 或**右可逆**的概念.

§2 群

可逆么半群 G 称为**群**, 即:

Definition 2.1 (群). 设有集合 G . 若:

- G1) 定义了二元运算 $\cdot: G^2 \rightarrow G; (x, y) \mapsto xy$.
- G2) 结合性: $\forall x, y, z \in G, (xy)z = x(yz)$.
- G3) 单位元: $\exists e \in G \forall x \in G, xe = ex = x$.
- G4) 可逆性: $\forall x \in G \exists x^{-1} \in G, xx^{-1} = x^{-1}x = e$.

则称 (G, \cdot) 为**群**.

交换群又叫做 **Abelian 群**.

作为重要的例子, 设 X 是一个集合, $S(X) = \{f \in X^X \mid f \text{ 是双射}\}$. 我们断言, $(S(X), \circ, \text{id}_X)$ 是一个群, 称为**变换群**或**置换群**, 其中 \circ 是函数的复合, id_X 是恒等变换. 当它的阶数 $\text{card } X = n$ 是有限的时候, 记 $S_n := S(X)$.

群也有子群的概念. 设 (G, \cdot, e) 是一个群. 当一个集合 $G' \subset G$ 满足:

- SG1) $e \in G'$;
- SG2) $\forall x, y \in G', xy \in G'$;
- SG3) $x \in G' \rightarrow x^{-1} \in G'$,

则称 (G', \cdot, e) 是一个 G 的**子群**. 倘若还有 $G' \neq G$ 则称其为一个**真子群**¹.

¹[1] 等文献把平凡群 $\{e\}$ 也排在真子群的定义外.

Theorem 2.1. 非空的 G' 是群 $(G, \cdot, 1)$ 的子群 $\leftrightarrow \forall x, y \in G' (xy^{-1} \in G')$.

Proof. 根据子群的定义, 它是显然的, 下给出 \leftarrow 的证明:

$$\text{SG1)} \quad \forall x \in G' (xx^{-1} = 1 \in G');$$

$$\text{SG2)} \quad \forall x, y \in G', x1^{-1}1y^{-1-1} = xy \in G';$$

$$\text{SG3)} \quad \forall x \in G', 1x^{-1} = x^{-1} \in G'.$$

□

这里将不加证明地给出:

Lemma 1. 群 G 的子群族 $\mathcal{H} = \{H \mid H \text{ 是 } G \text{ 的子群}\}$ 的交 $\cap \mathcal{H}$ 也是 G 的子群.

设 G 有子集 S , 我们说群 $(G, \cdot, 1)$ 是由 S 生成的, 意思是说 G 没有包含 S 的真子群. 记为 $G = \langle S \rangle$.

Theorem 2.2. $\langle S \rangle = \left\{ \prod_{i=0}^{n-1} s_i \mid \forall i \in n (s_i \in S \vee s_i^{-1} \in S) \right\}$.

Proof. 根据群的定义, 形如 $\prod_{i=0}^{n-1} s_i$ 的将构成一个群. 如果存在一个不能写成这种形式的元素, 那么它们将构成一个真子群, 这和 $\langle S \rangle$ 的定义相违背.

□

我们把半群的公式 (1-4) 推广到整数次幂, 证明在此忽略了.

Theorem 2.3. $\forall g \in G, \forall n, m \in \mathbb{Z},$

$$g^m g^n = g^{m+n}, \quad (g^m)^n = g^{mn}. \quad (2-1)$$

Definition 2.2 (循环群). 设 $(G, \cdot, 1)$ 是一个乘法群, $\exists g_0 \in G$, 使得 $\forall g \in G, \exists n \in \mathbb{Z}, a^n = g$, 那么我们称它是一个循环群, g_0 是一个生成元 (generator), 并记作 $G = \langle g_0 \rangle$.

对于群 G 中任意元素 g , 我们称 $\text{card}\langle g \rangle$ 为元 g 的阶数, 或称 g 为 n 阶元. 而且它将满足:

Theorem 2.4. 任意群 G 中若有 $q \in \mathbb{Z}$ 阶元 g , 则 $\langle g \rangle = \{e, g, \dots, g^{q-1}\}$, 且:

$$g^n = e \leftrightarrow n = kq, \quad n \in \mathbb{Z}. \quad (2-2)$$

证明利用带余除法和定理 2.3, 证明是显然的. 从该定理, 我们可以论断: 循环群都是 Abelian 群.

Definition 2.3 (同构). 两个群 $(G, *)$, (G', \circ) 如若满足: $\exists f: G \rightarrow G'$ s.t.

$$\text{i)} \quad \forall a, b \in G, f(a * b) = f(a) \circ f(b);$$

ii) f 是双射,

则称 f 是一个**同构映射**或**同构** (isomorphism), 并认为两个群是互相**同构**的 (isomorphic), 记为 $G \simeq G'$.

同构关系的自反性, 传递性和对称性是平凡的.

Theorem 2.5. 设群 $(G, *, 1)$, $(G', \circ, 1')$ 被 f 见证同构, 那么 $f(1) = 1'$.

Proof. $\forall g' \in G'$, 记 $g := f^{-1}(g')$, 那么 $f(g) \circ f(1) = f(g * 1) = g' = f(1 * g) = f(1) \circ f(g)$. 从而 $f(1) = 1'$. \square

Theorem 2.6. 设群 $(G, *, 1)$, $(G', \circ, 1')$ 被 f 见证同构, 那么 $\forall g \in G$, $f(g^{-1}) = f(g)^{-1}$.

Proof. $f(g) \circ f(g^{-1}) = f(g * g^{-1}) = f(1) = 1' = f(g^{-1} * g) = f(g^{-1}) \circ f(g)$. \square

Theorem 2.7. $\text{card}\langle g_0 \rangle = \text{card}\langle g'_0 \rangle \rightarrow \langle g_0 \rangle \simeq \langle g'_0 \rangle$.

Proof. 倘若 $\text{card}\langle g_0 \rangle = \infty$, 那么 $\nexists n \in \mathbb{Z} - \{0\}$, s.t. $g_0^n = e$; 这意味着, 存在这样的双射 $f: \mathbb{Z} \rightarrow \langle g_0 \rangle$, 满足 $f(n) = g_0^n$, 见证了 $(\mathbb{Z}, +, 0) \simeq (\langle g_0 \rangle, *, e)$.

如果阶数是有限的, 只需令 $f: g^k \rightarrow g'^k$, 其中 $k = 0, 1, \dots, \text{card}\langle g_0 \rangle$. \square

Theorem 2.8 (Cayley 定理). 设 $(G, *, e)$ 任意 n 阶有限群. $\exists H \subset S_0$ s.t. (H, \circ, id_X) 是 S_n 的子群且 $G \simeq H$.

Proof. 取 $H := \{L_g \mid g \in G\}$, 其中 $L_g: G \rightarrow G; g' \mapsto gg'$ 可以证明是双射. 那么 $L: G \rightarrow H; g \mapsto L_g$ 见证了 $H \simeq G$. \square

若 $\varphi: G \rightarrow G$ 见证了 $G \simeq G$ (如 id_G), 那么称 φ 是群 G 的一个**自同构** (automorphism). 所有自同构组成的集合 $\text{Aut}(G)$ 和其上的函数复合 \circ 构成了 $S(G)$ 的一个子群, 称为 G 的**自同构群**.

自同构群有一特殊的子群 $\text{Inn}(G) := \{I_a: g \mapsto aga^{-1} \mid a \in G\}$, 称为**内自同构群**.

Definition 2.4 (同态). 设有群 $(G, *, e)$ 和 (G', \circ, e') , 映射 $f: G \rightarrow G'$ 若满足

$$\forall a, b \in G, \quad f(a * b) = f(a) \circ f(b),$$

则称其为群 $(G, *)$ 到群 (G', \circ) 的一个**同态** (homomorphism), 也叫**态射** (morphism). 类似映射, 可定义**单态射** (monomorphism), **满态射** (epimorphism).

集合 $\ker f := f^{-1}(\{e'\})$ 叫做同态 f 的**核** (kernel). 群到自身的同态映射称为**自同态** (endomorphism).

同态 f 的核是 G 的子群, 而 G 在同态下的像是 G' 的子群.

Theorem 2.9. 如果同态的核是平凡群 (即, $\ker f = \{e\}$), 那么这个同态是单的.

Proof. 如果 $\exists g_1, g_2 \in G$, s.t. $f(g_1) = f(g_2)$, 那么

$$f(g_1 * g_2^{-1}) = f(g_1) \circ f(g_2^{-1}) = f(g_1) \circ f(g_2)^{-1} \circ f(g_2) \circ f(g_2^{-1}) = e' \circ f(e) = e'$$

从而 $g_1 * g_2^{-1} \in \ker f$, 同理 $g_2^{-1} * g_1 \in \ker f$, 即 $g_1^{-1} = g_2^{-1}$ 或 $g_1 = g_2$, 即: f 是单的. \square

作为例子, 映射

$$f: G \rightarrow \text{Inn}(G); g \mapsto I_g$$

满足同构的条件 i), 因 $f(a) \circ f(b) = I_{ab} = f(ab)$; 但它不一定是双射, 因而是一个同态.

§3 环

Definition 3.1 (环). 集合 R 非空, 其上定义了加法 $+$ 和乘法 \cdot , 且满足:

R1) $(R, +, 0)$ 是阿贝尔群;

R2) (R, \cdot) 是半群;

R3) 乘法对加法有分配律:

$$(a + b)c = ac + bc, \quad c(a + b) = ca + cb$$

对 $\forall a, b, c \in R$ 成立.

那么, 我们称 $(R, +, \cdot)$ 是一个环 (ring)². 而且称 $(R, +)$ 作其加法群, 称 (R, \cdot) 为其乘法半群. 倘若 (R, \cdot) 还有单位元 1, 那么我们称 $(R, +, \cdot)$ 为有单位元的环.

若环 R 非空的子集 L 满足

$$\forall x, y \in L (x - y \in L \wedge xy \in L),$$

则称 L 是 R 的一个子环.

若环的乘法半群是交换的, 则称这个环是一个交换环.

作为例子, $(\mathbb{Z}, +, \cdot)$ 是我们熟悉的整数环, $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ 是它的一个子环 ($n \in \mathbb{Z}$). 交换环 R 上的所有 n 阶方阵之集合 $M_n(R)$ 也是环.

²如果 (R, \cdot) 不结合, 通常称非结合环.

Definition 3.2 (同态). 设 R 和 R' 是两个环, 有一个映射 f 对加法群和乘法半群都是同态 (保持运算), 即:

$$f(x)f(y) = f(xy), \quad f(x) + f(y) = f(x + y),$$

那么, 我们称其为 R 到 R' 的一个**同态或态射**, 集合 $\ker f := \{a \in R \mid f(a) = 0\}$ 称为同态的**核**. 同态 f 的核是 R 的子环. 类似地我们也有**单同态**, **满同态**和**同构**的概念. 两个环同构记为 $R \cong R'$.

设 $(R, +, \cdot)$ 是环, X 是一个集合, 在 R^X 上定义加法和乘法:

$$f + g: x \mapsto f(x) + g(x); \quad fg: x \mapsto f(x)g(x),$$

就得到了**函数环** $(R^X, +, \cdot)$, 其零元是 $0_X: x \mapsto 0$. 如果 R 有单位元 1 , 那么 R^X 也有单位元 $1_X: x \mapsto 1, \forall x \in X$.

作为例子, 考虑到将 $[k]_n \in \mathbb{Z}/\equiv \bmod n$ 映射到 $n^{\mathbb{Z}} \ni \bmod n := \{(m, k) \in \mathbb{Z} \times m \mid n \equiv k \bmod n\}$ 的同构, **模 n 的剩余类环** $(\mathbb{Z}_n, +, \cdot)$ 即可看作函数环 $n^{\mathbb{Z}}$ 的一个交换子环, 其中 $\mathbb{Z}_n := \{[k]_n \mid k \in n\}$. 同构关系让我们也能用剩余类的代表元组成的集合 n 代替剩余类本身进行运算, 这种情况下, n 称为**模 n 的剩余类的导出集**, 我们能用法表和乘法表给出它的代数结构.

Definition 3.3 (整环). 环 R 中, $a \in R$, 如果 $\exists b \in R - \{0\}$ s.t. $ab = 0$, 则称 a 为环 R 的一个**零因子**; 类似则可定义**右零因子**³. 左零因子和右零因子统称**零因子**. 零元 0 则称为**平凡零因子**.

若非平凡的交换环 R 带单位元 $1 \neq 0$, 且没有非平凡零因子, 则称 R 是一个**整环** (entire ring 或 integral domain).

也有将无非平凡左零因子的带单位的非平凡环称为 **domain** 的.

Theorem 3.1 (消去律). 设 R 是带单位元 $1 \neq 0$ 的交换环. 环 R 是整环 $\leftrightarrow \forall x, y, c \in R, cx = cy \wedge c \neq 0 \rightarrow x = y$.

Proof. 如果 R 满足消去律, 那么 $ab = 0 = 0b = a0$ 将给出 $a = 0 \vee b = 0$ 的论断; 如果 R 是整环, 那么 $cx = cy$ 即 $c(x - y) = 0$ 将得出 $c = 0 \vee x = y$; 倘若 $c \neq 0$, 那么这就是消去律. \square

有单位元的环 R 中元素 x 的可逆性往往指关于乘法的可逆性.

Theorem 3.2. 设 R 是带单位元 1 的环, $U(R) := \{x \in R \mid x \text{ 可逆}\}$ 是一个乘法群.

³[1] 中把 0 排除在外了.

Proof. 单位元 1 当然可逆. 由定义可逆元素的逆也是可逆的. 如果 $x, y \in R$ 可逆, 那么

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1 = y^{-1}x^{-1}xy = (xy)^{-1}(xy),$$

即 xy 可逆. □

如果 $U(R) = R - \{0\}$, 那么我们称 R 是一个除环 (division ring), 也称斜域或反对称域 (skew field). 除环没有零因子.

§4 域

交换除环 F 称为域 (field). 群 $P^* = U(P)$ 称为域的乘法群. 如果 $y \neq 0$, 那么我们通常记 $x/y = \frac{x}{y} := xy^{-1}$.

参考文献

- [1] A.I. Kostrikin. *Introduction to Algebra*. Universitext - Springer-Verlag. Springer-Verlag, 1982. ISBN: 9783540907114. URL: <https://www.springer.com/gp/book/9780387907116>.

符号列表

这里列出了笔记中出现的重要符号.

$\langle g_0 \rangle$, 4

$G \simeq G'$, 5

$[k]_n$, 7

$\langle S \rangle$, 4

S_n , 3

$S(X)$, 3

$(X, *)$, 2

$(X, *, e)$, 2

\mathbb{Z}_n , 7

索引

- n 阶元, 4
- Abelian 群, 3
- Cayley 定理, 5
- domain, 7
- 二元运算, 2
- 交换环, 6
- 交换的, 2
- 代数系统, 2
- 代数结构, 2
- 内自同构群, 5
- 函数环, 7
- 分配律, 6
- 剩余类环, 7
- 半群, 2
- 单位元, 2
- 单同态, 7
- 单态射, 5
- 反对称域, 8
- 变换群, 3
- 可逆的, 3
- 右可逆, 3
- 右零因子, 7
- 同态, 5, 7
- 同构, 5, 7
- 同构映射, 5
- 和, 2
- 域, 8
- 子半群, 3
- 子么半群, 3
- 子环, 6
- 子群, 3
- 左可逆, 3
- 左正规, 3
- 平凡群, 3
- 平凡零因子, 7
- 么半群, 2
- 循环群, 4
- 态射, 5, 7
- 整数环, 6
- 整环, 7
- 斜域, 8
- 有限么半群, 2
- 核, 5, 7
- 模 n 的剩余类的导出集, 7
- 模 n 的剩余类环, 7
- 满同态, 7

满态射, 5

环, 6

生成元, 4

真子群, 3

积, 2

结合的, 2

置换幺半群, 2

置换群, 3

群, 3

自同态, 5

自同构, 5

自同构群, 5

逆, 3

逆元, 3

阶, 2

阶数, 4

除环, 8

零元, 2

零因子, 7

非结合环, 6