

Algebra

Hoyan Mok¹

2020 年 7 月 22 日

¹E-mail: victoriesmo@hotmail.com

B

目录

Contents	i
第一章 群. 环. 域	1
§1 代数运算	1
§2 群	2
参考文献	4
符号列表	5
索引	6

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, $na = -(-na), a^n = (a^{-n})^{-1}$.

§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.

我们把半群的公式 (1-4) 推广到整数次幂, 证明在此忽略了.

¹[1] 等文献把平凡群 $\{e\}$ 也排在真子群的定义外.

Theorem 2.1. $\forall g \in G, \forall n, m \in \mathbb{Z},$

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

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 2.2. 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 2.1, 证明是显然的.

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

- i) $\forall a, b \in G, f(a * b) = f(a) \circ f(b);$
- ii) f 是双射,

则称 f 是一个同构映射或同构, 并认为两个群是互相同构的, 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 2.3. 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 2.4. 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 2.5. $\text{card}\langle g_0 \rangle = \text{card}\langle g'_0 \rangle \rightarrow \langle g_0 \rangle \simeq \langle g'_0 \rangle$.

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 2.6 (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. 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.

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.

$\langle g_0 \rangle$, 3

$G \simeq G'$, 3

S_n , 2

$S(X)$, 2

$(X, *)$, 1

$(X, *, e)$, 1

索引

n 阶元, 3

Abelian 群, 2

Cayley 定理, 3

二元运算, 1

交换的, 1

代数系统, 1

代数结构, 1

半群, 1

单位元, 1

变换群, 2

可逆的, 2

同构, 3

同构映射, 3

和, 1

子半群, 2

子么半群, 2

子群, 2

左正规, 2

平凡群, 2

么半群, 1

循环群, 3

有限么半群, 1

生成元, 3

真子群, 2

积, 1

结合的, 1

置换么半群, 1

置换群, 2

群, 2

自同构, 3

逆, 2

逆元, 2

阶, 1

阶数, 3

零元, 1