1 半群和幺半群

先介绍半群, 再介绍幺半群, 再介绍群. 半群是最秃的, 群没那么秃.

1.1 半群

定义 1.1 (代数运算)**.** S 上的代数运算 f 的定义为

$$f\colon S \times S \to S \tag{1}$$

仅此而已. $f(a,b)$ 记为 ab, 如果不引起歧义的话.

定义 1.2 (Semigroup)**.** 如果 S 上有一个运算 f, 其满足结合律:

$$(ab)c = a(bc) \tag{2}$$

那么 S 并上这个运算 f .viz $\{S; f\}$ [1], 称为半群.

1.2 幺半群

定义 1.3 (identity, monoid)**.** 存在一个 e 使得 $\forall a \in A(ea = a)$, 则称 e 为左幺元, 如果满足的是 $\forall a \in A(ae = a)$, 那么 e 称为右幺元. e 既是左幺元又是右幺元的话, e 是幺元. 存在幺元的半群称为幺半群.[2]

Example 1.4. *对于 A 集合上的变换, 其天然是一个幺半群.*

Example 1.5. *存在只有左幺元而没有右幺元的半群. 考虑运算为右投影映射的半群, 不难验证其只有左幺元而没有右幺元.*

2 群

定义 2.1 (逆)**.** 对于一个幺半群, 对于 a 若是存在 b 使得 $ab = e$, 则称 b 为 a 的左逆. 类似的, 也有右逆的定义. 如果左逆等于右逆, 则称 b 为 a 的逆.

[1]写为 (S, f) 也行

[2]幺半群的集合常用符号 M 来表示. M for momoid

定义 2.2 (群)**.** 若是每一个元素都有逆, 那么这个幺半群称为群.

Example 2.3. 集合 A 上的双射自然构成了一个群. 进一步讨论见 *Example 2.14*.

Example 2.4 (四元数)**.**

Remark 2.5. 若是一个幺半群元素既有左逆又有右逆, 那么他有逆.

证明.

$$b_l = b_l e = b_l(ab_r) = (b_l a)b_r = eb_r = b_r$$

□

Remark 2.6. 逆元唯一.

证明. 设 b, b' 均为逆元. 证明过程同上. □

定理 2.7 (群的等价条件)**.** 半群若是 1. 有左幺元, 2. 每个元素有左逆, 则其为群.

证明. 设 a 的左逆为 b, b 的左逆为 c.

$$a = ea = cba = c(ba) = ce \tag{3}$$

$$ab = (ce)b = c(eb) = cb = e \tag{4}$$

$ab = e$ 说明 b 是 a 的逆. 于是有 $c = a$, 带入 $a = ce$ 有 $a = ae$, 说明 e 是幺元. 于是该半群为群. □

Remark 2.8. 有些书上, 采用这种描述来定义群.

定理 2.9. 半群满足形如 $ax = b, yc = d$ (其中 x, y 为变量) 的方程均有解, 则其为群.

证明. 验证定理 2.7 的条件. 因为 $a \in G$, $xa = a$ 有解, 设解为 e .viz $ea = a$, 对于任意的 b, $ax = b$ 有解, 设解为 c .viz $ac = b$. 那么

$$eb = e(ac) = (ea)c = ac = b \tag{5}$$

则 e 为左幺元. 并且显然, 每个元素都有左逆, 根据定理 2.7, 该半群为群. □

定理 2.10 (满足消去律的半群)**.** 有限半群若满足消去律 (左右消去律), 则其为群.

Example 2.11. 存在半群使得其有左幺元且有右逆, 但不是群, 甚至不是幺半群. 见 *Example 1.5*

证明. □

Example 2.12. 数域 $\mathbb{R}$ 或者 $\mathbb{C}$ 上的 n 阶可逆矩阵的全体和矩阵乘法构成了一个群, 记为 $GL_n(\mathbb{R})$, 读作一般线性群. 同时还有特殊线性群 $SL_n(\mathbb{R})$ 表示的是行列式为 1 的可逆矩阵群, $\mathbb{R}$ 上的 SL_n 群也可写为 $O(n)$, 读作正交矩阵群.

Example 2.13. 设幺半群为 $(M, \cdot)$, 设 $U(M) = \{a \mid a \text{ 可逆}\}$[3], 则 $(U(M), \cdot)$ 为群[4]

Example 2.14 (置换群, 对称群)**.** 对于双射变换, 其构成一个群, 称为置换群或者是对称群. 当我们考虑有限集合上的双射变换的时候, 能够看出为什么称为置换群. 每一个双射变换都是一个置换. 写作 φ, 比如说, 对于集合 $M = \{1, 2, 3\}$, 一个置换可以写为:

$$\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \varphi' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \tag{6}$$

Example 2.15 (模 n 群)**.** 不知道叫什么名字姑且这么叫了. 设 $\bar{a} = \{b \mid b \equiv a \pmod n\}$, 定义运算 $*$: $\bar{a} * \bar{b} = \overline{a+b}$, 设 $\mathbb{Z}_n = \{\bar{a} \mid a \in Z\}$, 则 $(\mathbb{Z}_n, *)$ 是一个群, 且是交换群.

Example 2.16 (n 次单位根)**.** $\mathbb{C}_n = \{e^{\frac{2\pi \mathrm{i} a}{n}} \mid 0 \le a \le n-1\}$. 对于任意的 $c \in \mathbb{C}_n$, 满足 $c^n = 1$, 因此称为 n 次单位根.

3 同态

[3] U for uniform, I guess.

[4] 这里对于数域的强调很可能是没有必要的