



抽象代数

作者: 邹文杰

组织: 无

时间: 2024/10/25

版本: ElegantBook-4.5

自定义: 信息



宠辱不惊, 闲看庭前花开花落;
去留无意, 漫随天外云卷云舒.

目录

第一章 群论 I——Group Theory I	1
1.1 么半群	1
1.2 群	5
1.3 有限群	13
1.4 正规子群	22
1.5 群作用	27
1.6 群论与数论	32
第二章 环论——Ring Theory I	39
2.1 环	39
2.2 环同态	42
2.3 理想	49
2.4 素理想与极大理想	54
2.5 环的局部化	60

第一章 群论 I——Group Theorey I

1.1 么半群

定义 1.1 (代数运算/二元运算)

设 A 是一个非空集合, 若对 A 中任意两个元素 a, b , 通过某个法则 “ \cdot ”, 有 A 中唯一确定的元素 c 与之对应, 则称法则 “ \cdot ” 为集合 A 上的一个**代数运算 (algebraic operation)** 或**二元运算**. 元素 c 是 a, b 通过运算 “ \cdot ” 作用的结果, 将此结果记为 $a \cdot b = c$.

定义 1.2 (半群和交换半群)

非空集合 S 和 S 上满足结合律的二元运算 \cdot 所形成的代数结构叫做**半群**. 此即

$$\forall x, y, z \in S, x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

这个半群记成 (S, \cdot) 或者简记成 S , 运算 $x \cdot y$ 也常常简写成 xy . 此外, 如果半群 (S, \cdot) 中的运算 “ \cdot ” 又满足交换律, 则 (S, \cdot) 叫做**交换半群**. 此即

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

$$\forall x, y \in S, x \cdot y = y \cdot x.$$

注 像通常那样令 $x^2 = x \cdot x, x^{n+1} = x^n \cdot x (= x \cdot x^n, n \geq 1)$.

定义 1.3 (么元素)

设 S 是半群, 元素 $e \in S$ 叫做半群 S 的**么元素 (也叫单位元 (unit element) 或恒等元 (identity))**, 是指对每个 $x \in S, xe = ex = x$.

命题 1.1 (么元素存在必唯一)

如果半群 (S, \cdot) 中有么元素, 则么元素一定唯一. 我们将半群 (S, \cdot) 中这个唯一的么元素 (如果存在的话) 通常记作 1_S 或者 1 .

证明 因若 e' 也是么元素, 则 $e' = e'e = e$. □

定义 1.4 (含么半群和交换含么半群)

如果半群 (S, \cdot) 含有么元素, 则 (S, \cdot) 称为**(含) 么半群**. 此即

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

$$\exists e \in S, \forall x \in S, e \cdot x = x \cdot e = x.$$

此外, 如果么半群 (S, \cdot) 中的运算 “ \cdot ” 又满足交换律, 则 (S, \cdot) 叫做**交换么半群**. 此即

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

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

$$\forall x, y \in S, x \cdot y = y \cdot x.$$

例题 1.1 $(M_n(\mathbb{R}), \cdot)$ 是一个含么 (乘法) 半群.

证明 $\forall A, B, C \in (M_n(\mathbb{R}), \cdot)$, 则不妨设 $A = (a_{ij})_{n \times n}, B = (b_{ij})_{n \times n}, C = (c_{ij})_{n \times n}$. 再设 $A \cdot B = (d_{ij})_{n \times n}, B \cdot C =$

$(e_{ij})_{n \times n}, (A \cdot B) \cdot C = (f_{ij})_{n \times n}, A \cdot (B \cdot C) = (g_{ij})_{n \times n}$. 于是

$$d_{ij} = \sum_{k=1}^n a_{ik} b_{kl}, e_{ij} = \sum_{k=1}^n b_{ik} c_{kl}.$$

其中 $i, j = 1, 2, \dots, n$.

从而

$$\begin{aligned} f_{ij} &= \sum_{l=1}^n d_{il} c_{lj} = \sum_{l=1}^n \left(\sum_{k=1}^n a_{ik} b_{kl} \right) \cdot c_{lj} = \sum_{l=1}^n \sum_{k=1}^n a_{ik} b_{kl} c_{lj}, \\ g_{ij} &= \sum_{k=1}^n a_{ik} e_{kj} = \sum_{k=1}^n a_{ik} \cdot \left(\sum_{l=1}^n b_{kl} c_{lj} \right) = \sum_{k=1}^n \sum_{l=1}^n a_{ik} b_{kl} c_{lj}. \end{aligned}$$

由二重求和号的可交换性, 可知 $f_{ij} = g_{ij}, \forall i, j \in \{1, 2, \dots, n\}$. 故 $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.

记 $I_n = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \in M_n(\mathbb{R})$, 于是 $\forall X \in M_n(\mathbb{R})$, 则不妨设 $X = (x_{ij})_{n \times n}, I_n = (\delta_{ij})_{n \times n}$. 其中 $\delta_{ij} = \begin{cases} 1, & \text{当 } i = j \text{ 时,} \\ 0, & \text{当 } i \neq j \text{ 时} \end{cases}$. 再设 $I_n \cdot X = (x'_{ij})_{n \times n}, X \cdot I_n = (x''_{ij})_{n \times n}$, 于是由矩阵乘法的定义可知

$$\begin{aligned} x'_{ij} &= \sum_{k=1}^n x_{ik} \delta_{kj} = x_{ij} \delta_{jj} = x_{ij}, \\ x''_{ij} &= \sum_{k=1}^n \delta_{ik} x_{kj} = \delta_{ii} x_{ij} = x_{ij}. \end{aligned}$$

故 $x'_{ij} = x''_{ij} = x_{ij}, \forall i, j \in \{1, 2, \dots, n\}$. 从而 $X = I_n \cdot X = X \cdot I_n$. 因此 I_n 是 $(M_n(\mathbb{R}), \cdot)$ 的单位元. 综上所述, $(M_n(\mathbb{R}), \cdot)$ 是一个含么 (乘法) 半群. \square

定义 1.5 (么半群中多个元素的乘积)

设 (S, \cdot) 是一个么半群, 令 $x_1, \dots, x_n \in S$, 我们递归地定义

$$x_1 \cdot x_2 \cdots x_n = (x_1 \cdot x_2 \cdots x_{n-1}) \cdot x_n$$

令 $x \in S, n \in \mathbb{N}$. 若 $n > 0$, 我们定义 $x^n = x \cdots x$, 而 $x^0 = e$.


定义 1.6 (广义结合律)

设 S 是一个非空集合, “ \cdot ” 是一个二元运算, 若对于任意有限多个元素 $x_1, x_2, \dots, x_n \in S$, 乘积 $x_1 \cdot x_2 \cdots x_n$ 的任何一种 “有意义的加括号方式” (即给定的乘积的顺序) 都得出相同的值.

命题 1.2

设 S 是一个非空集合, “ \cdot ” 是一个满足结合律的二元运算, 令 $x_1, \dots, x_n, y_1, \dots, y_m \in S$, 则

$$x_1 \cdot x_2 \cdots x_n \cdot y_1 \cdot y_2 \cdots y_m = (x_1 \cdot x_2 \cdots x_n) \cdot (y_1 \cdot y_2 \cdots y_m) \quad (1.6)$$

 **笔记** 根据这个命题, 我们就可以得到一个半群 (S, \cdot) 一定满足广义结合律, 只要 $x_1, \dots, x_n \in S$ 的 \cdot 运算顺序是固定的, 无论怎么添加括号, 我们都可以利用这个命题的结论, 将括号重排至从前往后依次乘的顺序而保持结果不变. 所以, 如果一个集合上的二元运算有结合律, 我们就可以在连续元素的乘积中不加括号, 也可以按照我们的需要随意加括号.

证明 对 m 做数学归纳. 当 $m = 1$ 时, 由定义 1.5 直接得到. 接下来, 假设

$$x_1 \cdot x_2 \cdots x_n \cdot y_1 \cdot y_2 \cdots y_k = (x_1 \cdot x_2 \cdots x_n) \cdot (y_1 \cdot y_2 \cdots y_k)$$

则由“ \cdot ”满足结合律, 我们有

$$\begin{aligned} & x_1 \cdot x_2 \cdots x_n \cdot y_1 \cdot y_2 \cdots y_{k+1} \\ &= ((x_1 \cdot x_2 \cdots x_n) \cdot (y_1 \cdot y_2 \cdots y_k)) \cdot y_{k+1} \\ &= (x_1 \cdot x_2 \cdots x_n) \cdot ((y_1 \cdot y_2 \cdots y_k) \cdot y_{k+1}) \\ &= (x_1 \cdot x_2 \cdots x_n) \cdot (y_1 \cdot y_2 \cdots y_{k+1}) \end{aligned}$$

□

推论 1.1

令 $x \in S, m, n \in \mathbb{N}$, 则

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

♥

证明 令命题 1.2 中的所有 x_i 和 y_j 都等于 x 即可得到.

□

定义 1.7 (子么半群)

令 (S, \cdot) 是一个么半群, 若 $T \subset S, e \in T$, 且 T 在乘法下封闭, 即

$$\begin{aligned} & e \in T, \\ & \forall x, y \in T, x \cdot y \in T. \end{aligned}$$

则我们称 (T, \cdot) 是 (S, \cdot) 的一个**子么半群**

♣

命题 1.3 (子么半群也是么半群)

若 (T, \cdot) 是 (S, \cdot) 的一个子么半群, 则 (T, \cdot) 是个么半群.

♠

证明 就二元运算的定义而言, 子群第一个条件 (封闭性) 就满足了, 这使得我们后面的谈论是有意义的. 首先, 结合律对于 S 中元素都满足, 当然对 T 中元素也满足 (T 是子集). 接下来, 类似地, e 对于所有 S 中元素都是单位元, 固然对于 T 中元素亦是单位元.

□

定义 1.8 (两个么半群的直积)

令 $(G, \cdot_1), (G', \cdot_2)$ 是两个么半群, 我们记 $(G \times G', *)$ 为 (G, \cdot_1) 和 (G', \cdot_2) 的**直积**. 满足对于 $(x, y), (x', y') \in G \times G'$, 有

$$(x, y) * (x', y') = (x \cdot_1 x', y \cdot_2 y').$$

♣

命题 1.4 (两个么半群的直积仍是么半群)

若 $(G, \cdot_1), (G', \cdot_2)$ 是两个么半群, 则它们的直积 $(G \times G', *)$ 还是一个么半群.

♠

证明 封闭性: 因为 G 在 \cdot_1 下封闭, G' 在 \cdot_2 下封闭, 而 $G \times G'$ 的元素乘积是逐坐标定义的, 则 $G \times G'$ 在 $*$ 下也是封闭的.

结合律: 同样, 逐坐标有结合律, 故整体也有结合律.

单位元: 设 e, e' 分别是 $(G, \cdot_1), (G', \cdot_2)$ 的单位元, 则不难想象, (e, e') 是直积的单位元. 对于任意 $(x, y) \in G \times G'$, 我们有 $(x, y) * (e, e') = (x \cdot_1 e, y \cdot_2 e') = (x, y)$, 另一边也是同理, 这就证明了 (e, e') 是直积的单位元.

□

定义 1.9 (一族么半群的直积)

令 $(G_i, \cdot_i)_{i \in I}$ 是一族么半群, 其中 I 是一个指标集. 我们记它们的**直积**为 $(\prod_{i \in I} G_i, *)$. 满足对于 $(x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} G_i$, 有

$\prod_{i \in I} G_i$, 有

$$(x_i)_{i \in I} * (y_i)_{i \in I} = (x_i \cdot_i y_i)_{i \in I}.$$

命题 1.5 (一族么半群的直积仍是么半群)

若 $(G_i, \cdot_i)_{i \in I}$ 是一族么半群, 则它们的直积 $(\prod_{i \in I} G_i, *)$ 还是一个么半群.

证明 证明与命题 1.4 同理.. 封闭性与结合律是显然的. 单位元是 $(e_i)_{i \in I}$. □

命题 1.6 (一族交换么半群的直积仍是交换么半群)

若 $(G_i, \cdot_i)_{i \in I}$ 是一族交换么半群, 则它们的直积 $(\prod_{i \in I} G_i, *)$ 还是一个交换么半群.

证明 由命题 1.5 可知 $(\prod_{i \in I} G_i, *)$ 还是一个么半群. 下面证明它还是交换么半群.

由 $(G_i, \cdot_i)_{i \in I}$ 是一族交换么半群可得, 对 $\forall (x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} G_i$, 都有

$$(x_i)_{i \in I} \cdot (y_i)_{i \in I} = (x_i \cdot_i y_i)_{i \in I} = (y_i \cdot_i x_i)_{i \in I} = (y_i)_{i \in I} \cdot (x_i)_{i \in I}.$$

故 $(\prod_{i \in I} G_i, *)$ 还是一个交换么半群. □

定义 1.10 (么半群同态)

假设 $(S, \cdot), (T, *)$ 是两个么半群, 且 $f: S \rightarrow T$ 是一个映射, 我们称 f 是一个**么半群同态**, 当 f 保持了乘法运算, 且把单位元映到了单位元. 此即

$$\begin{aligned} \forall x, y \in S, f(x \cdot y) &= f(x) * f(y), \\ f(e) &= e'. \end{aligned}$$

其中, e 和 e' 分别是 (S, \cdot) 和 $(T, *)$ 的单位元. ♣

定义 1.11 (由子集生成的子么半群)

假设 (S, \cdot) 是一个么半群, 而 $A \subset S$ 是一个子集. 我们称 S 中所有包含了 A 的子么半群的交集为**由 A 生成的子么半群**, 记作 $\langle A \rangle$. 此即

$$\langle A \rangle = \bigcap \{T \subset S : T \supset A, T \text{ 是子么半群}\}.$$

命题 1.7 (由子集生成的子么半群是包含了这个子集的最小的子么半群)

假设 (S, \cdot) 是一个么半群, 而 $A \subset S$ 是一个子集. 则 $\langle A \rangle$ 也是一个子么半群. 因此, 这是包含了 A 的最小的子么半群. ♣

注 这里说的“最小”, 指的是在包含关系下最小的, 也就是, 它包含于所有包含 A 的子么半群.

证明 要证明 $\langle A \rangle$ 是子么半群, 只需要证明它包含了 e , 并在乘法运算下封闭. 首先, 因为族中每一个 T , 作为子么半群, 都会包含 e ; 因此 $\langle A \rangle$ 作为这些集合的交集也会包含 e , 这就证明了第一点. 而对于第二点, 我们首先假设 $x, y \in \langle A \rangle$, 而想要证明 $x \cdot y \in \langle A \rangle$. 注意到, 因为 $x, y \in \langle A \rangle$, 任取一个包含了 A 的子么半群 T (族中的集合), 我们都有 $x, y \in T$, 于是有 $x \cdot y \in T$. 而 $x \cdot y \in T$ 对于所有这样的 T 都成立, 我们就有 $x \cdot y$ 属于它们的交集, 也就是 $\langle A \rangle$. 这样, 我们就证明了第二点. 综上, 由一个么半群 S 的任意子集 A 生成的子么半群都确实是一个子么半群. □

定义 1.12 (幺半群同构)

假设 $(S, \cdot), (T, *)$ 是两个幺半群, 且 $f: S \rightarrow T$ 是一个映射, 我们称 f 是一个**幺半群同构**, 当 f 是一个双射, 且是一个同态.

$$\begin{aligned} f & \text{ 是双射,} \\ \forall x, y \in S, f(x \cdot y) &= f(x) * f(y), \\ f(e) &= e'. \end{aligned}$$

其中, e 和 e' 分别是 (S, \cdot) 和 $(T, *)$ 的单位元.



注 容易验证同构是一个等价关系.

命题 1.8 (幺半群同构的逆是幺半群同态)

若 $f: (S, \cdot) \rightarrow (T, *)$ 是一个幺半群同构, 则 $f^{-1}: T \rightarrow S$ 是一个幺半群同态. 因此, f^{-1} 也是个幺半群同构.



证明 令 $x', y' \in T$, 我们只需证明 $f^{-1}(x' * y') = f^{-1}(x') \cdot f^{-1}(y')$. 为了方便起见, 根据 f 是一个双射, 从而存在 $x, y \in S$, 使得 $x = f^{-1}(x'), y = f^{-1}(y')$, 并且 $f(x) = x', f(y) = y'$. 我们只需证明 $f^{-1}(x' * y') = x \cdot y$. 而由于 f 是幺半群同态, 所以 $f(x \cdot y) = f(x) * f(y) = x' * y'$. 反过来说, $f^{-1}(x' * y') = x \cdot y = f^{-1}(x') \cdot f^{-1}(y')$. 这就证明了这个命题.

□

1.2 群

定义 1.13

令 (S, \cdot) 是一个幺半群, $x \in S$. 我们称 x 是**可逆的**, 当且仅当

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

其中 y 被称为 x 的**逆元**, 记作 x^{-1} .

**命题 1.9 (逆元存在必唯一)**

令 (S, \cdot) 是一个幺半群. 假设 $x \in S$ 是可逆的, 则其逆元唯一. 也就是说, 如果 $y, y' \in S$ 都是它的逆元, 则 $y = y'$.



证明 假设 y, y' 都是 x 的逆元. 则 $y \cdot x = e, x \cdot y' = e$. 从而

$$y = y \cdot e = y \cdot x \cdot y' = e \cdot y' = y'.$$

□

定义 1.14 (群)

令 (G, \cdot) 是一个幺半群, 若 G 中所有元素都是可逆的, 则我们称 (G, \cdot) 是一个**群**. 换言之, 若 \cdot 是 G 上的一个二元运算, 则我们称 (G, \cdot) 是个**群**, 或 G 对 \cdot 构成群, 当这个运算满足结合律, 存在单位元, 且每个元素具有逆元. 再进一步展开来说, 同样等价地, 若 \cdot 是 G 上的一个二元运算, 则我们称 (G, \cdot) 是个**群**, 当

$$\begin{aligned} \forall x, y, z \in G, x \cdot (y \cdot z) &= (x \cdot y) \cdot z, \\ \exists e \in G, \forall x \in G, x \cdot e &= e \cdot x = x, \\ \forall x \in G, \exists y \in G, x \cdot y &= y \cdot x = e. \end{aligned}$$



命题 1.10

令 (G, \cdot) 是一个群, 令 $x \in G$, 则 $(x^{-1})^{-1} = x$.



证明 方便起见, 我们令 $y = x^{-1}$, 于是有 $x \cdot y = y \cdot x = e$. 我们要证明 $y^{-1} = x$, 而这就是 $y \cdot x = x \cdot y = e$, 显然成立. 这就证明了逆元的逆元是自身. \square

命题 1.11

令 (G, \cdot) 是一个群, 令 $x, y \in G$, 则 $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.



证明 我们利用定义来证明. 一方面, 利用广义结合律, $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = e$; 另一方面, 同理可以得到另一边的等式 $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = e$, 这就告诉我们 $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. \square

定义 1.15

设 (G, \cdot) 是一个群, 且 $x \in G$. 若 $n \in \mathbb{N}_1$, 我们定义 $x^{-n} = (x^{-1})^n$, 另外定义 $x^0 = e$.

**命题 1.12**

设 (G, \cdot) 是一个群, 且 $x \in G$. 则满足

- (1) $x^{-n} = (x^{-1})^n = (x^n)^{-1}, \forall n \in \mathbb{Z}$.
- (2) $x^{m+n} = x^m \cdot x^n, \forall m, n \in \mathbb{Z}$.
- (3) $x^{mn} = (x^m)^n = (x^n)^m, \forall m, n \in \mathbb{Z}$.



证明

(1) (i) 当 $n = 0$ 时, 结论显然成立.

(ii) 当 $n \in \mathbb{N}_1$ 时, 只需证明 $(x^{-1})^n = (x^n)^{-1}$ 即可. 注意到

$$\begin{aligned} x^n \cdot (x^{-1})^n &= \left(\underbrace{x \cdots x}_{n \uparrow} \right) \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{n \uparrow} \right) = e, \\ (x^n)^{-1} \cdot x^n &= \left(\underbrace{x^{-1} \cdots x^{-1}}_{n \uparrow} \right) \cdot \left(\underbrace{x \cdots x}_{n \uparrow} \right) = e. \end{aligned}$$

故根据逆元的定义可知结论成立.

(iii) 当 n 为负整数时, 令 $m = -n$, 则 $m \in \mathbb{N}_1$. 从而我们只需证 $x^m = (x^{-1})^{-m} = (x^{-m})^{-1}$ 即可. 根据定义 1.15 可得

$$\begin{aligned} x^{-m} \cdot x^m &= (x^{-1})^m \cdot x^m = \left(\underbrace{x^{-1} \cdots x^{-1}}_{m \uparrow} \right) \cdot \left(\underbrace{x \cdots x}_{m \uparrow} \right) = e, \\ x^m \cdot x^{-m} &= x^m \cdot (x^{-1})^m = \left(\underbrace{x \cdots x}_{m \uparrow} \right) \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{m \uparrow} \right) = e. \end{aligned}$$

故根据逆元的定义可知 $x^m = (x^{-m})^{-1}$. 又由定义 1.15 可知, $(x^{-1})^{-m} = ((x^{-1})^{-1})^m = x^m$. 故结论成立.

(2) 首先注意到,

(i) 如果 $m, n \in \mathbb{N}_1$, 则由推论 1.1 就立刻得到这个性质. 若 m 或 n 是 0, 利用单位元的性质也是显然的. 从而我们只需证明当 m, n 至少有一个小于 0 时, $x^{m+n} = x^m \cdot x^n$. 故我们可以不失一般性, 假设 $m < 0$, 记 $m' = -m$, 则 $x^m = x^{-m'} = (x^{-1})^{m'}$.

(ii) 若 $n < 0$, 记 $n' = -n$, 则同理, $x^n = (x^{-1})^{n'}$, 故 $x^{m+n} = (x^{-1})^{m'+n'}$, 这里 $m', n' \in \mathbb{N}_1$, 于是就有

$$x^{m+n} = (x^{-1})^{m'+n'} = (x^{-1})^{m'} (x^{-1})^{n'} = x^m x^n,$$

因此得证了.

(iii) 若 $0 < n < m'$, 则 $x^{m+n} = x^{-(m'-n)} = (x^{-1})^{m'-n}$. 而 $x^m \cdot x^n = (x^{-1})^{m'} \cdot x^n$. 于是

$$\begin{aligned} x^{m+n} &= x^m \cdot x^n \\ \Leftrightarrow (x^{-1})^{m'-n} &= (x^{-1})^{m'} \cdot x^n \\ \Leftrightarrow \underbrace{x^{-1} \cdots x^{-1}}_{m'-n \uparrow} &= \left(\underbrace{x^{-1} \cdots x^{-1}}_{m' \uparrow} \right) \cdot x^n \end{aligned}$$

对上式两边左乘 $x^{m'-n}$, 得到

$$\begin{aligned} x^{m+n} &= x^m \cdot x^n \Leftrightarrow \underbrace{x^{-1} \cdots x^{-1}}_{m'-n \uparrow} = \left(\underbrace{x^{-1} \cdots x^{-1}}_{m' \uparrow} \right) \cdot x^n \\ \Leftrightarrow x^{m'-n} \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{m'-n \uparrow} \right) &= x^{m'-n} \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{m' \uparrow} \right) \cdot x^n \\ \Leftrightarrow \left(\underbrace{x \cdots x}_{m'-n \uparrow} \right) \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{m'-n \uparrow} \right) &= \left(\underbrace{x \cdots x}_{m'-n \uparrow} \right) \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{m' \uparrow} \right) \cdot x^n \\ \Leftrightarrow e = \left(\underbrace{x^{-1} \cdots x^{-1}}_{n \uparrow} \right) \cdot x^n &\Leftrightarrow e = (x^n)^{-1} \cdot x^n \end{aligned}$$

上式最后一个等式显然成立, 故此时结论成立.

(iv) 若 $n \geq m'$, 则 $x^{m+n} = x^{n-m'}$. 而 $x^m \cdot x^n = (x^{-1})^{m'} \cdot x^n$. 于是

$$\begin{aligned} x^{m+n} &= x^m \cdot x^n \\ \Leftrightarrow x^{n-m'} &= (x^{-1})^{m'} \cdot x^n \\ \Leftrightarrow \underbrace{x \cdots x}_{n-m' \uparrow} &= (x^{-1})^{m'} \cdot \left(\underbrace{x \cdots x}_{n \uparrow} \right) \end{aligned}$$

对上式两边右乘 $(x^{-1})^{n-m'}$, 得到

$$\begin{aligned} x^{m+n} &= x^m \cdot x^n \Leftrightarrow \underbrace{x \cdots x}_{n-m' \uparrow} = (x^{-1})^{m'} \cdot \left(\underbrace{x \cdots x}_{n \uparrow} \right) \\ \Leftrightarrow \left(\underbrace{x \cdots x}_{n-m' \uparrow} \right) \cdot (x^{-1})^{n-m'} &= (x^{-1})^{m'} \cdot \left(\underbrace{x \cdots x}_{n \uparrow} \right) \cdot (x^{-1})^{n-m'} \\ \Leftrightarrow \left(\underbrace{x \cdots x}_{n-m' \uparrow} \right) \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{n-m' \uparrow} \right) &= (x^{-1})^{m'} \cdot \left(\underbrace{x \cdots x}_{n \uparrow} \right) \cdot \left(\underbrace{x^{-1} \cdots x^{-1}}_{n-m' \uparrow} \right) \\ \Leftrightarrow e = (x^{-1})^{m'} \cdot \left(\underbrace{x \cdots x}_{m' \uparrow} \right) &\Leftrightarrow e = (x^{-1})^{m'} \cdot x^{m'} \end{aligned}$$

上式最后一个等式显然成立, 故此时结论成立.

(3) 先证 $x^{mn} = (x^m)^n$. 对 $\forall m \in \mathbb{Z}$, 固定 m , 对 n 使用数学归纳法. 当 $n = 1$ 时, 结论显然成立. 假设当 $n = k$ 时, 结论成立, 即 $x^{mk} = (x^m)^k$. 则由 (2) 的结论可得

$$x^{m(k+1)} = (x^m)^{k+1} = (x^m)^k \cdot x^m = (x^m)^{k+1}.$$

故由数学归纳法可知 $x^{mn} = (x^m)^n, \forall n \in \mathbb{Z}$. 再由 m 的任意性可知 $x^{mn} = (x^m)^n, \forall m, n \in \mathbb{Z}$. 同理可证 $x^{nm} = (x^n)^m, \forall m, n \in \mathbb{Z}$. 由于 $x^{nm} = x^{mn}, \forall m, n \in \mathbb{Z}$. 因此 $x^{mn} = (x^m)^n = (x^n)^m, \forall m, n \in \mathbb{Z}$.

□

定义 1.16 (Abel 群)

若 (G, \cdot) 是一个群, 我们称它是 **Abel 群**, 或 **交换群**, 当该运算满足交换律, 即

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

**例题 1.2 常见的群**

1. 我们称只有一个元素的群为**平凡群**, 记作 e . 其中的二元运算是 $e \cdot e = e$.
2. 常见的加法群有 $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ 等. 这些加法群分别称为整数加群、有理数加群、实数加群、复数加群.
3. 常见的乘法群有 $(\mathbb{Q}^\times, +)$, $(\mathbb{R}^\times, +)$, $(\mathbb{C}^\times, +)$ 等, 其中 $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, 类似地定义其余两个集合. 这些乘法群分别称为有理数乘群、实数乘群、复数乘群.
4. 在向量空间中, n 维欧式空间对加法构成群即 $(\mathbb{R}^n, +)$. 类似地 $(\mathbb{C}^n, +)$, $(\mathbb{Q}^n, +)$, $(\mathbb{Z}^n, +)$ 也是群. 对于这些群, 单位元都是零向量, 加法逆元则是对每个坐标取相反数, 如 (x_1, \dots, x_n) 的加法逆元是 $(-x_1, \dots, -x_n)$.
5. 所有的 $m \times n$ 矩阵也对加法构成群, 单位元都是零矩阵, 加法逆元则是对每一项取相反数. 对于 $n \times n$ 的实矩阵加法群, 我们记作 $(M(n, \mathbb{R}), +)$, 类似地我们将 $n \times n$ 的复矩阵加法群记作 $(M(n, \mathbb{C}), +)$.

证明 证明都是显然的. □

引理 1.1

令 (S, \cdot) 是一个么半群, 令 G 是其所有可逆元素构成的子集, 则 (G, \cdot) 是个群. ♥

注 我们称呼么半群中的可逆元素为“**单位**”, 因此 G 是由所有该运算下的单位构成的集合 (在这里甚至是群).

证明 首先结合律完全继承自 S , 不需要证明. 而单位元是可逆的, 因此 $e \in G$. 剩下要证明 G 中每个元素都有 (G 中的) 逆元, 而这几乎是显然的. 假设 $x \in G$, 则 x 是可逆元素, 我们取 $y \in S$, 使得 $x \cdot y = y \cdot x = e$ (这里要注意我们只能首先保证 y 在全集 S 中). 接下来我们要证明 $y \in G$, 即 y 可逆, 而这是显然的, 因为 x 正是它的逆. 所以 $y \in G$. 这样, 就证明了 (G, \cdot) 是个群. □

定义 1.17 (子群)

设 (G, \cdot) 是一个群, 且 $H \subset G$. 我们称 H 是 G 的**子群**, 记作 $H < G$, 当其包含了单位元, 在乘法和逆运算下都封闭, 即

$$\begin{aligned} e &\in H, \\ \forall x, y \in H, x \cdot y &\in H, \\ \forall x \in H, x^{-1} &\in H. \end{aligned}$$

**命题 1.13 (子群也是群)**

令 (G, \cdot) 是一个群. 若 H 是 G 的子群, 则 (H, \cdot) 也是个群. ♠

证明 就二元运算的良好定义性而言, 子群第一个条件 (封闭性) 就满足了, 这使得我们后面的谈论是有意义的. 首先, 结合律肯定满足, 因为它是个子集. 其次, 根据子群的第二个条件, $e \in H$ 是显然的. 再次, 我们要证明每个 H 中元素有 H 中的逆元, 而这是子群的第三个条件. □

推论 1.2 (子群的传递性)

若 (G, \cdot) 是一个群, 且 $H < G, K < H$, 则一定有 $K < G$. 因此我们可以将 $H < G, K < H$ 简记为 $K < H < G$. ♥

证明 证明是显然的. □

命题 1.14 (子群的等价条件)

设 (G, \cdot) 是一个群, $H \subset G$, 则 (H, \cdot) 是子群等价于

$$\begin{aligned} e &\in H, \\ \forall x, y \in H, x \cdot y^{-1} &\in H. \end{aligned}$$

♠

证明 设 (H, \cdot) 是子群. 令 $x, y \in H$, 利用逆元封闭性得到 $y^{-1} \in H$, 再利用乘法封闭性得到 $x \cdot y^{-1} \in H$.

反过来, 假设上述条件成立. 令 $x \in H$, 则 $e \cdot x^{-1} = x^{-1} \in H$, 这证明了逆元封闭性. 接下来, 令 $x, y \in H$, 则利用逆元封闭性, $y^{-1} \in H$, 故 $x \cdot (y^{-1})^{-1} = x \cdot y \in H$. 这就证明了乘法封闭性.

综上, 这的确是子群的等价条件. □

命题 1.15 (子群的任意交仍是子群)

设 G 是一个群, $(N_i)_{i \in I}$ 是一族 G 的子群, 则它们的交集仍然是 G 的子群, 即

$$\bigcap_{i \in I} N_i \leq G.$$

♠

证明 首先, 设 e 是 G 的单位元, 则由子群对单位元封闭可知, $e \in N_i, \forall i \in I$. 从而 $e \in \bigcap_{i \in I} N_i$.

其次, 对 $\forall x, y \in \bigcap_{i \in I} N_i$, 都有 $x, y \in N_i, \forall i \in I$. 根据子群对逆元封闭可知, $y^{-1} \in N_i, \forall i \in I$. 于是再由子群对乘法封闭可知, $xy^{-1} \in N_i, \forall i \in I$. 故 $xy^{-1} \in \bigcap_{i \in I} N_i$.

综上, $\bigcap_{i \in I} N_i \leq G$. □

定义 1.18 (一般线性群)

我们对于那些 $n \times n$ 可逆实矩阵构成的乘法群, 称为 **(实数上的) n 阶一般线性群**, 记作 $(GL(n, \mathbb{R}), \cdot)$. 由于一个矩阵可逆当且仅当其行列式不为零, 因此

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

♣

定义 1.19 (特殊线性群)

我们将由那些行列式恰好是 1 的 $n \times n$ 实矩阵构成的乘法群称为 **(实数上的) n 阶特殊线性群**, 记作 $(SL(n, \mathbb{R}), \cdot)$, 即

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

♣

命题 1.16

$(SL(n, \mathbb{R}), \cdot)$ 是个群. ♠

证明 根据定义, $SL(n, \mathbb{R})$ 首先是 $GL(n, \mathbb{R})$ 的子集, 那么只要证明它是子群即可. 首先, 乘法单位元单位矩阵的行列式恰好是 1 (这也是为什么我们定义特殊线性群是行列式是 1 的矩阵构成的群的原因), 这就证明了 $I \in SL(n, \mathbb{R})$ ($I = I_n$ 指的是 n 阶单位矩阵). 另外, 我们要证明 $SL(n, \mathbb{R})$ 在乘法下封闭. 令 A, B 是两个行列式为 1 的 $n \times n$ 实矩阵. 由于行列式满足 $\det(AB) = \det(A)\det(B)$, 因此 AB 的行列式也是 1, 也就在特殊线性群中. 这就证明了特殊线性群确实是个群. 至于逆元封闭性, 我们利用 $\det(A^{-1}) = \frac{1}{\det(A)}$. 假设 $\det(A) = 1$, 则 $\det(A^{-1}) = 1$, 于是 $A^{-1} \in SL(n, \mathbb{R})$. 综上, 特殊线性群确实是个群. □

定义 1.20 (群同态)

令 $(G, \cdot), (G', *)$ 是两个群, 且 $f: G \rightarrow G'$ 是一个映射. 我们称 f 是一个**群同态**, 当其保持了乘法运算, 即

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

命题 1.17

若 $f: (G, \cdot) \rightarrow (G', *)$ 是一个群同态, 则 $f(e) = e', f(x^{-1}) = f(x)^{-1}$.



笔记 也就是说, f 不仅把乘积映到乘积, 而且把单位元映到单位元, 把逆元映到逆元. 在这个意义下, 实际上 f 将所有群 G 的“信息”都保持到了 G' 上, 包括单位元, 乘法和逆元. 至于结合律 (或者更基础的封闭性), 显然两边本来就有, 就不必再提.

证明 首先, 因为 $e \cdot e = e$, 所以利用同态的性质, $f(e) = f(e \cdot e) = f(e) * f(e)$. 这时, 两边同时左乘 $f(e)^{-1}$, 就可以各约掉一个 $f(e)$, 得到 $e' = f(e)$, 这就证明了 f 把单位元映到单位元.

另一方面, 令 $x \in G$, 则 $e' = f(e) = f(x \cdot x^{-1}) = f(x) * f(x^{-1})$. 同理 $e' = f(x^{-1}) * f(x)$. 于是由定义, $f(x^{-1})$ 就是 $f(x)$ 的逆元, 即 $f(x^{-1}) = f(x)^{-1}$. 这就证明了这个命题. \square

定义 1.21 (群同态的核与像)

令 $f: (G, \cdot) \rightarrow (G', *)$ 是一个群同态, 则我们定义 f 的**核**与**像**, 记作 $\ker(f)$ 与 $\text{im}(f)$, 分别为

$$\ker(f) = \{x \in G : f(x) = e'\} \subset G,$$

$$\text{im}(f) = \{y \in G' : \exists x \in G, y = f(x)\} = \{f(x) : x \in G\} \subset G'.$$

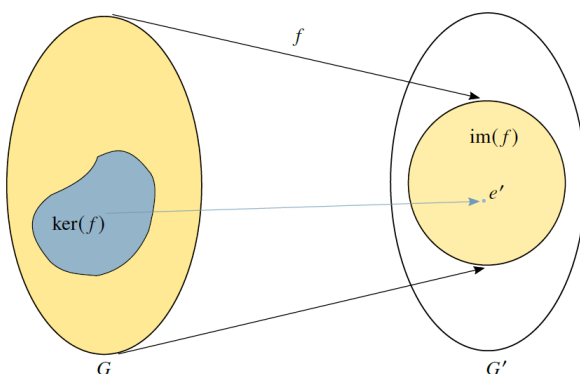


图 1.1: 群同态的核与像示意图

命题 1.18

令 $f: (G, \cdot) \rightarrow (G', *)$ 是一个群同态, 则核是定义域的子群, 像是陪域的子群, 即

$$\ker(f) < G, \quad \text{im}(f) < G'.$$

注 根据群同构第一定理进一步可知, $\ker f \triangleleft G$. 但是注意同态的像 ($\text{im}(f)$) 未必是 G' 的正规子群, 往往只是普通的子群.

证明 先证明第一个子群关系. 我们利用 $f(e) = e'$ 来说明 $e \in \ker(f)$. 接着, 设 $x, y \in \ker(f)$, 只需证明 $xy^{-1} \in \ker(f)$. 利用同态的性质, $f(xy^{-1}) = f(x)f(y)^{-1} = e'e'^{-1} = e'$, 这就证明了 $xy^{-1} \in \ker(f)$. 第一个子群关系得证.

再证明第二个子群关系. 同样由于 $f(e) = e'$, 我们有 $e' \in \text{im}(f)$. 接着, 设 $y = f(x), y' = f(x') \in \text{im}(f)$, 只需证明 $yy'^{-1} \in \text{im}(f)$. 同样利用同态的性质, $yy'^{-1} = f(x)f(x')^{-1} = f(xx'^{-1}) \in \text{im}(f)$. 第二个子群关系也得证. 这样我们就证完了整个命题. \square

例题 1.3 证明: $(SL(n, \mathbb{R}), \cdot) < (GL(n, \mathbb{R}), \cdot)$.

证明 由命题??可知, $\det : GL(n, \mathbb{R}) \rightarrow (\mathbb{R}^\times, \cdot)$ 是一个乘法群同态. 注意到 $\ker(\det) = (SL(n, \mathbb{R}), \cdot)$, 因此由命题 1.18 可知, $(SL(n, \mathbb{R}), \cdot) = \ker(\det) < (GL(n, \mathbb{R}), \cdot)$. \square

定义 1.22 (满同态与单同态)

令 $f : (G, \cdot) \rightarrow (G', *)$ 是一个群同态, 我们称 f 是一个**满同态**当 f 是满射, 称 f 是一个**单同态**当 f 是单射.

命题 1.19

令 $f : (G, \cdot) \rightarrow (G', *)$ 是一个群同态, 则

1. f 是一个单同态当且仅当 $\ker(f) = \{e\}$. 也就是说, 一个群同态是单的当且仅当核是平凡的.
2. f 是一个满同态当且仅当 $\text{im}(f) = G'$. 也就是说, 一个群同态是满的当且仅当值域等于陪域.

证明

1. 假设 f 是单的, 那么因为 $f(e) = e'$, 因此若 $f(x) = e'$, 则利用单射的性质我们一定有 $x = e$, 这就证明了核是平凡的.(这个方向是显然的)
另一个方向不那么显然. 我们假设 $\ker(f) = \{e'\}$. 假设 $x, x' \in G$, 使得 $f(x) = f(x')$, 我们只须证明 $x = x'$. 在这里, 我们同时右乘 $f(x')^{-1}$, 得到 $f(x)f(x')^{-1} = f(xx'^{-1}) = e'$. 而因为核是平凡的, 所以必须有 $xx'^{-1} = e$. 接下来同时右乘 x' , 我们就得到 $x = x'$. 这就证明了这个命题.
2. 因为 f 是满同态, 所以对 $\forall a' \in G'$, 都存在 $a \in G$, 使得 $f(a) = a'$. 故 $a' \in \text{im}(f)$. 因此 $G' \subset \text{im}(f)$. 又显然有 $\text{im}(f) \subset G'$. 故 $\text{im}(f) = G'$.

\square

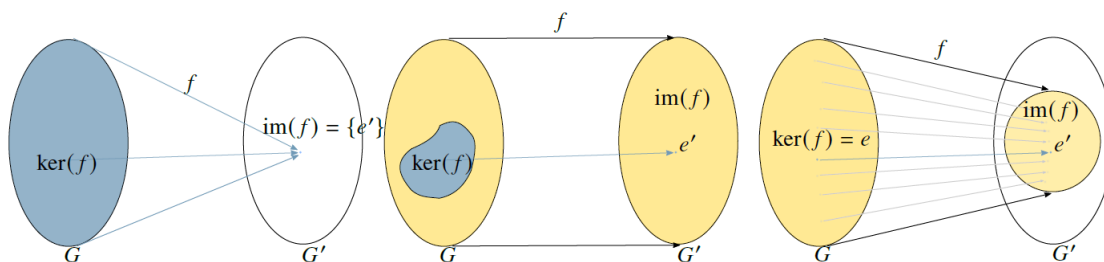


图 1.2: 平凡群, 满同态和单同态示意图

例题 1.4 证明: $\det : GL(n, \mathbb{R}) \rightarrow (\mathbb{R}^\times, \cdot)$ 是一个乘法群同态, 并且是满同态, $\ker(\det) = SL(n, \mathbb{R})$.

证明 设 $A, B \in GL(n, \mathbb{R})$, 则由行列式的 Laplace 定理可知 $\det(AB) = \det(A)\det(B)$. 故 \det 是群同态.

任取 $a \in \mathbb{R}^\times$, 令 $C = \begin{pmatrix} a & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$, 则 $C \in GL(n, \mathbb{R})$ 并且 $\det(C) = a$. 故 \det 是满同态.

一方面, 任取 $N \in SL(n, \mathbb{R})$, 则 $\det(N) = 1$, 从而 $N \in \ker(\det)$. 于是 $SL(n, \mathbb{R}) \subset \ker(\det)$. 另一方面, 任取 $M \in \ker(\det)$, 则 $\det(M) = 1$, 从而 $M \in SL(n, \mathbb{R})$. 于是 $\ker(\det) \subset SL(n, \mathbb{R})$. 故 $\ker(\det) = SL(n, \mathbb{R})$. \square

定义 1.23 (群同构)

令 $f : (G, \cdot) \rightarrow (G', *)$ 是一个映射, 我们称 f 是一个**群同构**, 当 f 既是一个双射, 又是一个群同态. 简单来说, 同构就是双射的同态.

命题 1.20 (群同构的逆也是群同构)

若 $f : (G, \cdot) \rightarrow (G', *)$ 是一个群同构, 则 f^{-1} 也是群同构.

证明 因为 f^{-1} 也是双射, 所以我们只须证明 f^{-1} 是群同态. 令 $x', y' \in G'$, 设 $x' = f(x), y' = f(y)$. 则 $x' * y' = f(x \cdot y), x = f^{-1}(x'), y = f^{-1}(y')$, 故 $f^{-1}(x' * y') = x \cdot y = f^{-1}(x') \cdot f^{-1}(y')$. 这就完成了证明. \square

定义 1.24 (两个群的直积)

令 $(G, \cdot_1), (G', \cdot_2)$ 是两个群, 我们记 $(G \times G', *)$ 为 (G, \cdot_1) 和 (G', \cdot_2) 的直积. 满足对于 $(x, y), (x', y') \in G \times G'$, 有

$$(x, y) * (x', y') = (x \cdot_1 x', y \cdot_2 y').$$

命题 1.21 (两个群的直积仍是群)

若 $(G, \cdot_1), (G', \cdot_2)$ 是两个群, 则它们的直积 $(G \times G', *)$ 还是一个群.

证明 封闭性: 因为 G 在 \cdot_1 下封闭, G' 在 \cdot_2 下封闭, 而 $G \times G'$ 的元素乘积是逐坐标定义的, 则 $G \times G'$ 在 $*$ 下也是封闭的.

结合律: 同样, 逐坐标有结合律, 故整体也有结合律.

单位元: 设 e, e' 分别是 $(G, \cdot_1), (G', \cdot_2)$ 的单位元, 则不难想象, (e, e') 是直积的单位元. 对于任意 $(x, y) \in G \times G'$, 我们有 $(x, y) * (e, e') = (x \cdot_1 e, y \cdot_2 e') = (x, y)$, 另一边也是同理, 这就证明了 (e, e') 是直积的单位元.

逆元: 对于任意 $(x, y) \in G \times G'$, 设 x^{-1}, y^{-1} 分别是 x, y 的逆元, 则同样不难想象, (x^{-1}, y^{-1}) 是 (x, y) 的逆元. \square

定义 1.25 (一族群的直积)

令 $(G_i, \cdot_i)_{i \in I}$ 是一族群, 其中 I 是一个指标集. 我们记它们的直积为 $(\prod_{i \in I} G_i, *)$. 满足对于 $(x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} G_i$, 有

$$(x_i)_{i \in I} * (y_i)_{i \in I} = (x_i \cdot_i y_i)_{i \in I}.$$

命题 1.22 (一族群的直积仍是群)

若 $(G_i, \cdot_i)_{i \in I}$ 是一族群, 则它们的直积 $(\prod_{i \in I} G_i, *)$ 还是一个群.

笔记 最经典的例子就是通过 n 个实数加群 $(\mathbb{R}, +)$ 直积得到的 $(\mathbb{R}^n, +)$.

证明 证明与命题 1.21 同理. 封闭性与结合律是显然的. 单位元是 $(e_i)_{i \in I}$, 而 $(x_i)_{i \in I}$ 的逆元是 $(x_i^{-1})_{i \in I}$. \square

命题 1.23 (一族 Abel 群的直积仍是 Abel 群)

若 $(G_i, \cdot_i)_{i \in I}$ 是一族 Abel 群, 则它们的直积 $(\prod_{i \in I} G_i, *)$ 还是一个 Abel 群.

证明 由命题 1.22 可知 $(\prod_{i \in I} G_i, *)$ 还是一个群. 下面证明它还是 Abel 群.

由 $(G_i, \cdot_i)_{i \in I}$ 是一族 Abel 群可得, 对 $\forall (x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} G_i$, 都有

$$(x_i)_{i \in I} \cdot (y_i)_{i \in I} = (x_i \cdot_i y_i)_{i \in I} = (y_i \cdot_i x_i)_{i \in I} = (y_i)_{i \in I} \cdot (x_i)_{i \in I}.$$

故 $(\prod_{i \in I} G_i, *)$ 还是一个 Abel 群. \square

定义 1.26 (投影映射)

若 $(G_i, \cdot_i)_{i \in I}$ 是一族群, $j \in I$ 是任意指标, 我们定义映射到指标 j 的**投影映射**为

$$p_j : \prod_{i \in I} G_i \rightarrow G_j.$$

对于 $(x_i)_{i \in I}$, 我们称 $p_j((x_i)_{i \in I}) = x_j$ 为 $(x_i)_{i \in I}$ 的**投影**.

命题 1.24 (投影映射是群同态)

若 $(G_i, \cdot_i)_{i \in I}$ 是一族群, $j \in I$ 是任意指标, 则投影映射 $p_j : \prod_{i \in I} G_i \rightarrow G_j$ 是个群同态.

证明 令 $(x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} G_i$, 则

$$p_j((x_i)_{i \in I}) = x_j, \quad p_j((y_i)_{i \in I}) = y_j$$

$$p_j((x_i)_{i \in I} * (y_i)_{i \in I}) = p_j((x_i \cdot_i y_i)_{i \in I}) = x_j \cdot_j y_j = p_j((x_i)_{i \in I}) \cdot_j p_j((y_i)_{i \in I}).$$

□

1.3 有限群

定义 1.27 (有限群)

设 (G, \cdot) 是一个群. 我们称 G 是一个**有限群**, 若 G 是有限的.

定义 1.28 (元素的阶)

设 (G, \cdot) 是一个群, 若 $x \in G$, 则 x (在 G 中) 的**阶**, 记作 $|x|$, 定义为那个最小的正整数 $n \in \mathbb{N}_1$, 使得 $x^n = e$. 若这样的 n 不存在, 则记 $|x| = \infty$.

命题 1.25 (有限群的每个元素的阶必有限)

若 (G, \cdot) 是有限群, 且 $x \in G$, 则 $|x| < \infty$. 换言之, 有限群的每一个元素通过自乘有限多次, 都可以得到单位元.

证明 我们用反证法, 假设 $|x| = \infty$, 那么根据定义, 对于任意的 $n \in \mathbb{N}_1$, 我们都有 $x^n \neq e$. 我们要说明的是, 这会导致一个事实, 就是所有的 $x^n (n \in \mathbb{N}_1)$ 都是不同的. 假设但凡有一对 $n \neq m \in \mathbb{N}_1$ 使得 $x^n = x^m$, 不失一般性我们假设 $n > m$. 则通过反复的消元 (两边反复右乘 x^{-1}), 我们可以得到 $x^{n-m} = e$, 其中 $n-m \in \mathbb{N}_1$, 而这与假设是矛盾的, 因为我们假设 x 的阶是无穷的. 因此, 这个事实是对的——所有的 $x^n (n \in \mathbb{N}_1)$ 都是不同的, 从而 G 中有无穷多个元素, 这与 G 是有限群矛盾. 这就证明了这个命题.

命题 1.26

设 (G, \cdot) 是一个群, 任取 $x \in G$. 则

$$\begin{aligned} f : (\mathbb{Z}, +) &\rightarrow (G, \cdot) \\ n &\mapsto x^n \end{aligned}$$

是一个群同态.

证明 取定 $x \in G$. 令 $m, n \in \mathbb{Z}$, 我们只须证明 $f(m+n) = f(m) \cdot f(n)$, 也即 $x^{m+n} = x^m \cdot x^n$. 于是根据命题 1.12(1) 就能立即得到结论.

□

定义 1.29 (由 x 生成的群)

设 (G, \cdot) 是一个群, 且 $x \in G$, 则 $\langle x \rangle$, 被称为由 x 生成的群, 定义为

$$\langle x \rangle = \{x^n : n \in \mathbb{Z}\}.$$

命题 1.27

设 (G, \cdot) 是一个群, 且 $x \in G$, 则 $\langle x \rangle < G$.

证明 记

$$\begin{aligned} f : (\mathbb{Z}, +) &\rightarrow (G, \cdot) \\ n &\mapsto x^n \end{aligned}$$

由命题 1.26 可知 f 是一个群同态. 注意到 $\text{im } f = \langle x \rangle$, 即 $\langle x \rangle$ 是 f 的同态像. 从而由命题 1.18 可知, $\langle x \rangle = \text{im } f < G$.

□

定义 1.30 (由 S 生成的群)

设 (G, \cdot) 是一个群, 且 $S \subset G$. 则由 S 生成的群, 记作 $\langle S \rangle$, 定义为

$$\langle S \rangle = \bigcap \{H \subset G : H \supset S, H < G\}$$

命题 1.28

令 (G, \cdot) 是一个群, 且 $S \subset G$, 则 $\langle S \rangle < G$.

笔记 这个命题表明: G 中由 S 生成的子群, 确实是包含了 S 的最小子群.

证明 在这里, 我们只要证明其包含单位元, 在乘法和逆元下封闭.

根据定义, $\langle S \rangle$ 是由所有包含了 S 的 G 中子群全部取交集得到的.

单位元: 每个这样的子群 H 都包含单位元, 故它们的交集也包含单位元.

乘法封闭性: 设 $x, y \in \langle S \rangle$, 任取一个包含了 S 的子群 H , 则 $x, y \in H$. 因为 H 是子群, 故 $xy \in H$, 所以由 H 的任意性可知 $xy \in \langle S \rangle$.

逆元封闭性: 设 $x \in \langle S \rangle$, 任取一个包含了 S 的子群 H , 则 $x \in H$. 因为 H 是子群, 故 $x^{-1} \in H$, 所以由 H 的任意性可知 $x^{-1} \in \langle S \rangle$. □

定义 1.31 (循环群)

令 (G, \cdot) 是一个群. 若存在 $x \in G$, 使得 $G = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$, 则 G 被称为一个循环群, 而 x 被称为 G 的一个生成元.

若 G 还是一个有限群, 则我们称 G 为有限循环群. 若 G 不是有限群, 则我们称 G 为无限循环群.

注 我们一般用 C_n 表示 n 阶循环群.

笔记 有限循环群与无限循环群示意图如下:

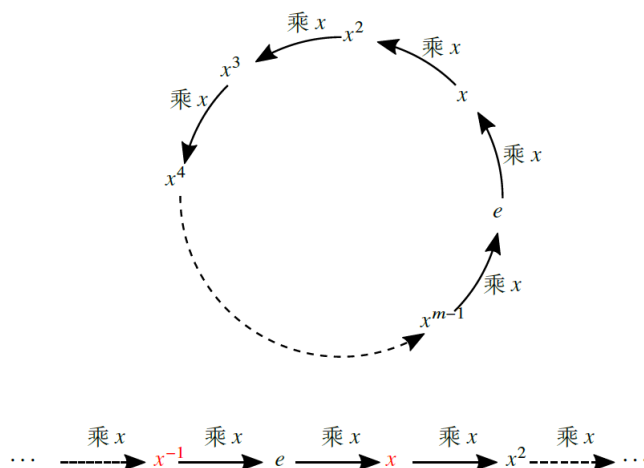


图 1.3: 有限循环群和无限循环群

命题 1.29

设 (G, \cdot) 是一个群, 对 $\forall x \in G$, 都有 $\langle x \rangle = \langle \{x\} \rangle$.



笔记 这个命题表明: 由 x 生成的群就是由子集 $\{x\}$ 生成的子群.

证明 根据定义和性质, $\langle \{x\} \rangle$ 是包含了 $\{x\}$ 的最小的子群. 因此要证明这个最小的子群就是 $\langle x \rangle$, 我们只须证明两点. 一, $\langle x \rangle$ 是个子群; 二, 如果一个子群 H 包含了 $\{x\}$, 那么它一定要包含整个 $\langle x \rangle$.

首先, 由命题 1.27 可知 $\langle x \rangle$ 是个子群. 这就证明了第一点.

第二点几乎也是显然的. 我们设 H 是个子群, 且 $x \in H$. 那么根据子群包含单位元, 且有乘法和逆元的封闭性, 我们有 $e \in H$, 并且递归地, 对于 $\forall n \in \mathbb{N}_1$, 都有 $x^n = x \cdots x \in H, x^{-n} = x^{-1} \cdots x^{-1} \in H$. 这就证明了 $H \supset \langle x \rangle$. \square

命题 1.30

设 $G = \langle x \rangle$ 是有限循环群, 并且 $|x| = n$, 则 $G = \{e, x, x^2, \dots, x^{n-1}\}$, 并且 $\{e, x, x^2, \dots, x^{n-1}\}$ 中的这些元素是两两不同的. 我们称这样的有限循环群的阶是 n .

证明 我们来证明两件事. 第一, 每一个 G 中元素都可以写成从 0 开始的前 n 项幂的形式; 第二, 从 0 开始的前 n 项幂是两两不同的.

我们来证明第一点. 任取 G 中元素 x^m , 其中 $m \in \mathbb{Z}$. 根据带余除法, 存在 $q \in \mathbb{Z}, 0 \leq r \leq n-1$, 使得 $m = qn + r$. 那么因为 $x^n = e$, 所以 $x^m = x^{qn+r} = (x^n)^q \cdot x^r = x^r$, 而这就属于从 0 开始的前 n 项幂.

我们来证明第二点. 用反证法, 假设 $0 \leq m' < m \leq n-1$, 使得 $x^m = x^{m'}$, 则 $x^{m-m'} = e$. 其中 $1 \leq m-m' \leq n-1 < n$, 可是 $n = |x|$ 是最小的正整数 k 使 $x^k = e$, 这就导致了矛盾.

综上所述, $G = \{e, x, x^2, \dots, x^{n-1}\}$, 其中枚举法中的这些元素是两两不同的. \square

命题 1.31

对于任意的 $n \in \mathbb{N}_1$, 所有 n 阶的循环群都是互相同构的.

证明 设 $G = \langle x \rangle, G' = \langle y \rangle$ 都是 n 阶循环群. 令

$$f: G \rightarrow G', x^m \mapsto y^m$$

则对 $\forall x^{m_1}, x^{m_2} \in G$, 其中 $1 \leq m_1, m_2 \leq n-1$. 我们都有

$$f(x^{m_1}x^{m_2}) = f(x^{m_1+m_2}) = y^{m_1+m_2} = y^{m_1}y^{m_2} = f(x^{m_1})f(x^{m_2}).$$


因此 f 是个同态映射. 此外, 它是个双射, 因为我们可以明确地找到其逆映射

$$f^{-1}(y^m) = x^m$$

这样, f 既是双射, 也是同态, 这就证明了 f 是个同构. \square

命题 1.32

设 $G = \langle x \rangle$ 是无限循环群, 则 $x^n (n \in \mathbb{Z})$ 是两两不同的, 且 G 只有两个生成元, 分别是 x 与 x^{-1} . \blacktriangle


 **笔记** 显然, $(\mathbb{Z}, +)$ 就是一个无限循环群, 生成元是 1 或 -1.

证明 首先证明 $x^n (n \in \mathbb{Z})$ 是两两不同的. 假设有两个相同, 不失一般性假设 $m > n \in \mathbb{Z}, x^m = x^n$, 则 $x^{m-n} = e$, 故 x 是有有限阶的. 这就矛盾了.

接着, 如果 $x^n (n \in \mathbb{Z})$ 可以生成这个群, 那么 $x \in \langle x^n \rangle$, 于是存在 $m \in \mathbb{Z}$ 使得 $x = (x^n)^m$, 于是 $x^{nm-1} = e$. 由于 x 是无限阶的, 所以 $nm = 1$, 那么这样的 n 只能是 ± 1 . 另外, 显然 x^{-1} 也可以生成这个群. 这就证明了恰好是这两个生成元. \square

命题 1.33

所有的无限循环群是彼此同构的. 进而所有的无限循环群 $\langle x \rangle (|x| = \infty)$ 都同构于整数加群 $(\mathbb{Z}, +)$. \blacktriangle

 **笔记** 这个命题告诉我们: 要研究无限循环群, 只要研究整数加群 $(\mathbb{Z}, +)$ 就可以了.

证明 设 $G = \langle x \rangle, G' = \langle y \rangle$ 都是无限循环群. 令

$$f: G \rightarrow G', x^m \mapsto y^m$$

则对 $\forall x^{m_1}, x^{m_2} \in G$, 其中 $m_1, m_2 \in \mathbb{Z}$. 我们都有

$$f(x^{m_1} x^{m_2}) = f(x^{m_1+m_2}) = y^{m_1+m_2} = y^{m_1} y^{m_2} = f(x^{m_1}) f(x^{m_2}).$$

因此 f 是个同态映射. 此外, 它是个双射, 因为我们可以明确地找到其逆映射

$$f^{-1}(y^m) = x^m$$

这样, f 既是双射, 也是同态, 这就证明了 f 是个同构. \square

命题 1.34

令 $G = \langle x \rangle$ 是一个 n 阶循环群. 假设 $1 \leq m \leq n$, 则 x^m 的阶为

$$|x^m| = \frac{n}{\gcd(n, m)}.$$

证明 设 $1 \leq m \leq n-1$, 我们希望找到最小的正整数 k 使得 $(x^m)^k = x^{mk} = e$. 由于 $|x| = n$, 故这等价于 $n \mid mk$. 接下来我们要利用简单的初等数论. 通过同时除以 n 和 m 的最大公因数, 我们得到

$$\frac{n}{\gcd(n, m)} \mid \frac{m}{\gcd(n, m)} \cdot k$$

而因为 $\frac{n}{\gcd(n, m)}$ 和 $\frac{m}{\gcd(n, m)}$ 是互素的, 所以这个条件进一步等价于

$$\frac{n}{\gcd(n, m)} \mid k$$

也就是说, 最小的这个正整数 k 正是 $\frac{n}{\gcd(n, m)}$. 这就完成了证明. \square

命题 1.35

令 $G = \langle x \rangle$ 是一个 n 阶循环群, 则 $x^m (1 \leq m \leq n)$ 是个生成元, 当且仅当

$$\gcd(m, n) = 1.$$

根据欧拉 ϕ 函数的定义, 这些生成元的个数正是 $\phi(n)$. \blacktriangle

证明 若 x^m 是一个生成元, 则由 G 是一个 n 阶循环群可知, $|x^m| = n$. 从而由命题 1.34 可知, $\gcd(m, n) = \frac{n}{|x^m|} = 1$.

若 $\gcd(m, n) = 1$, 则由命题 1.34 可知, $|x^m| = \frac{n}{\gcd(n, m)} = n$. 从而

$$(x^m)^n = e, (x^m)^{n+1} = (x^m)^n x = x, \dots, (x^m)^{2n-1} = (x^m)^n x^{n-1} = x^{n-1}.$$

又由命题 1.30 可知 $G = \{e, x, \dots, x^{n-1}\}$. 于是

$$G = \{e, x, \dots, x^{n-1}\} = \{(x^m)^n, (x^m)^{n+1}, \dots, (x^m)^{2n-1}\} = \{(x^m)^n : n \in \mathbb{Z}\}.$$

因此 $G = \langle x^m \rangle$, 故 x^m 是 G 的生成元. □

定义 1.32 (群的阶)

设 (G, \cdot) 是一个群, 则 G 的阶, 记作 $|G|$, 定义为 G 的集合大小 (元素的个数).

定义 1.33 (子群的阶)

设 (G, \cdot) 是一个群, H 是 G 的子群, 则 H 的阶, 记作 $|H|$, 定义为 H 的集合大小 (元素的个数). 若 H 是无限群则记 $|H| = \infty$.

定义 1.34 (左陪集)

设 G 是一个群, $H < G$ 是一个子群, $a \in G$. 则称 aH 是 H 的一个 (由 a 引出的) **左陪集**, 定义为

$$aH = \{ax : x \in H\}.$$

称 aH 是 H 的一个 (由 a 引出的) **右陪集**, 定义为

$$Ha = \{xa : x \in H\}.$$

注 aH, Ha 一般来说不是 G 的子群.

我们只讨论左陪集的性质和结论, 右陪集的性质与左陪集类似.

引理 1.2

令 G 是一个有限群, $H < G$ 是一个子群, $a \in G$. 令

$$f : H \rightarrow aH, x \mapsto ax.$$

则 f 是一个双射. 特别地, $|H| = |aH|$.



笔记 这个引理表明: 陪集的大小都是一样的.

证明 证法一: 根据 f 的定义易知 f 是满射. 若 $f(h_1) = f(h_2)$, 则

$$ah_1 = ah_2 \Rightarrow a^{-1}ah_1 = a^{-1}ah_2 \Rightarrow h_1 = h_2.$$

故 f 也是单射. 因此 f 是双射.

证法二: 令

$$g : aH \rightarrow H, k \mapsto a^{-1}k.$$

设 $k \in aH$, 则存在 $h \in H$, 使得 $k = ah$. 则 $g(k) = g(ah) = a^{-1}ah = h \in H$. 故 g 是良定义的. 注意到

$$g \circ f = \text{id}_H, \quad f \circ g = \text{id}_{aH}.$$

故 g 是 f 的逆映射. 因此 f 是双射. □

命题 1.36

设 G 是一个有限群, $H < G$ 是一个子群, $a, b \in G$. 则左陪集 aH 和 bH 要么相等, 要么无交. 也就是说, 我们有 $aH = bH$, 或 $aH \cap bH = \emptyset$.

证明 假设 $aH \cap bH \neq \emptyset$, 则可设 $ah_1 = bh_2 \in aH \cap bH$, 其中 $h_1, h_2 \in H$. 我们只须证明 $aH = bH$, 而根据对称性,

我们只须证明 $aH \subset bH$ 即可. 任取 aH 中的元素 $ah (h \in H)$, 则由 $ah_1 = bh_2$ 可知, $a = bh_2h_1^{-1}$. 从而

$$ah = (bh_2h_1^{-1})h = b(h_2h_1^{-1}h) \in bH$$

这就完成了证明. □

定义 1.35 (商集)

设 G 是一个非空集合, $H \subset G$ 是一个子集合. 则商集 G/H 定义为

$$G/H = \{aH : a \in G\}.$$

商集 $H \backslash G$ 定义为

$$H \backslash G = \{Ha : a \in G\}.$$

我们把商集 G/H 的大小 (所含元素的个数) 称为 H 在 G 中的指数, 记为 $[G : H]$, 即

$$[G : H] = |G/H|.$$

定理 1.1

设 G 是一个有限群, $H < G$ 是一个子群, 则商集 $G/H = \{aH : a \in G\}$ 就是 G 的一个分拆, 即

$$G = \bigsqcup_{i=1}^{[G:H]} a_i H = \bigsqcup_{a \in G} aH.$$

证明 一方面, 设 $x \in G$, 取 $a = x$, 则 $x = xe = ae \in xH$. 另一方面, 由命题 1.36 可知, 对 $\forall aH, bH \in G/H$, 都有 aH 和 bH 要么相等, 要么无交. 故商集 $G/H = \{aH : a \in G\}$ 就是 G 的一个分拆. □

 笔记

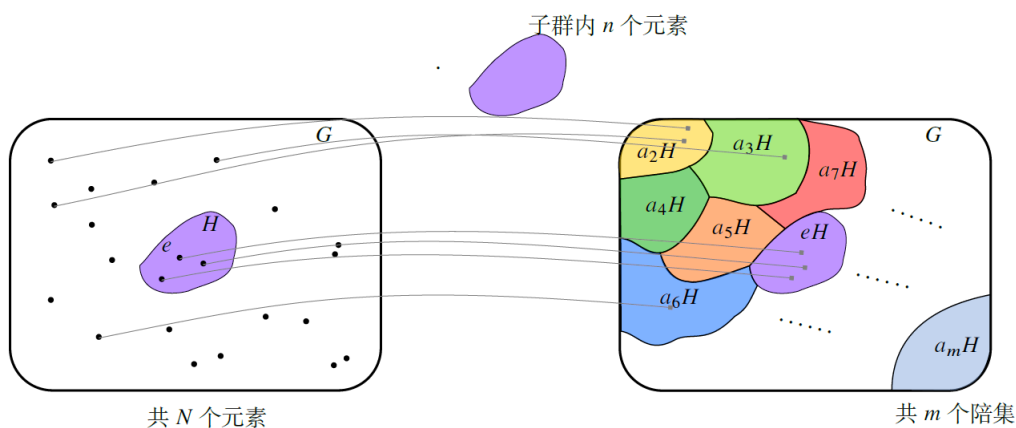


图 1.4: 左陪集示意图

定理 1.2 (Lagrange 定理)

设 G 是一个有限群, $H < G$ 是一个子群, 则

$$|G| = [G : H]|H|.$$

进而 $[G : H] = \frac{|G|}{|H|}$. 特别地,

$$|H| \mid |G|.$$

证明 由定理 1.1 可知 $G = \bigsqcup_{i=1}^{[G:H]} a_i H$, 从而

$$|G| = \sum_{i=1}^{[G:H]} |a_i H|.$$

又由引理 1.2 可知 $|a_i H| = |H|$. 故

$$|G| = [G:H]|H|.$$

□

例题 1.5 设 (G, \cdot) 是一个群, 若 $|G| = p$ 是素数, 则不存在任何非平凡子群.

证明 设 $H < G$, 则由 Lagrange 定理可知 $|H| \mid |G|$, 即 $|H| \mid p$. 从而 $|H| = 1$ 或 p , 于是 $H = \{e\}$ 或 G .

□

引理 1.3

设 G 是一个群, $H < G$ 是一个子群, $x, y, a, b \in G$, 则

$$(1) xH \subset yH \Leftrightarrow axHb \subset ayHb.$$

$$(2) Hx \subset Hy \Leftrightarrow aHxb \subset aHyb.$$

$$(3) xH \subset Hy \Leftrightarrow axHb \subset aHyb.$$

进一步, 我们有

$$(4) xH = yH \Leftrightarrow axHb = ayHb.$$

$$(5) Hx = Hy \Leftrightarrow aHxb = aHyb.$$

$$(6) xH = Hy \Leftrightarrow axHb = aHyb.$$

♡

证明

(4) \Rightarrow : 若 $xH = yH$, 则要证 $axHb = ayHb$, 根据对称性, 只须证 $axHb \subset ayHb$. 任取 $axhb \in axHb$, 其中 $h \in H$, 则由 $xH = yH$ 及 $xh \in xH$ 可知, 存在 $h' \in H$, 使得 $xh = yh'$. 从而 $axhb = ayh'b \in ayHb$. 故 $axHb \subset ayHb$.

\Leftarrow : 若 $axHb = ayHb$, 则要证 $xH = yH$, 根据对称性, 只须证 $xH \subset yH$. 任取 $xh \in xH$, 其中 $h \in H$, 则由 $axHb = ayHb$ 及 $axhb \in axHb$ 可知, 存在 $h' \in H$, 使得 $axhb = ayh'b$. 从而 $xh = a^{-1}axhbb^{-1} = a^{-1}ayh'bb^{-1} = yh' \in yH$. 故 $xH \subset yH$.

(5) \Rightarrow : 若 $Hx = Hy$, 则要证 $aHxb = aHyb$, 根据对称性, 只须证 $aHxb \subset aHyb$. 任取 $ahxb \in aHxb$, 其中 $h \in H$, 则由 $Hx = Hy$ 及 $hx \in Hx$ 可知, 存在 $h' \in H$, 使得 $hx = h'y$. 从而 $ahxb = ah'yb \in aHyb$. 故 $aHxb \subset aHyb$.

\Leftarrow : 若 $aHxb = aHyb$, 则要证 $Hx = Hy$, 根据对称性, 只须证 $Hx \subset Hy$. 任取 $hx \in Hx$, 其中 $h \in H$, 则由 $aHxb = aHyb$ 及 $ahxb \in aHxb$ 可知, 存在 $h' \in H$, 使得 $ahxb = ah'yb$. 从而 $hx = a^{-1}ahxb b^{-1} = a^{-1}ah'yb b^{-1} = h'y \in Hy$. 故 $Hx \subset Hy$.

(6) \Rightarrow : 若 $xH = Hy$, 则要证 $axHb = aHyb$, 根据对称性, 只须证 $axHb \subset aHyb$. 任取 $axhb \in axHb$, 其中 $h \in H$, 则由 $xH = Hy$ 及 $xh \in xH$ 可知, 存在 $h' \in H$, 使得 $xh = h'y$. 从而 $axhb = ah'yb \in aHyb$. 故 $axHb \subset aHyb$.

\Leftarrow : 若 $axHb = aHyb$, 则要证 $xH = Hy$, 根据对称性, 只须证 $xH \subset Hy$. 任取 $xh \in xH$, 其中 $h \in H$, 则由 $axHb = aHyb$ 及 $axhb \in axHb$ 可知, 存在 $h' \in H$, 使得 $axhb = ah'yb$. 从而 $xh = a^{-1}axhbb^{-1} = a^{-1}ah'yb b^{-1} = h'y \in Hy$. 故 $xH \subset Hy$.

根据上述 (4)(5)(6) 的证明过程就能直接得到 (1)(2)(3) 的证明.

□

引理 1.4


设 G 是一个群, $H < G$ 是一个子群, $x \in G$, 则我们有充要条件

$$xH = H \iff x \in H.$$

一般地, 对于 $x, y \in G$, 我们有充要条件

$$xH = yH \iff y^{-1}x \in H \iff x^{-1}y \in H \iff x \in yH \iff y \in xH.$$

♡

 **笔记** 同理可知对右陪集也有相同的结论.

证明 对于 $x \in G$, 一方面, 设 $xH = H$, 则 $x = xe \in xH = H$, 因此 $x \in H$.

另一方面, **证法一**: 设 $x \in H$, 任取 $xh \in xH$, 则根据乘法封闭性可知 $xh \in H$. 故 $xH \subset H$. 任取 $h \in H$, 则根据乘法封闭性和逆元封闭性可知 $x^{-1}h \in H$, 从而 $h = xx^{-1}h \in xH$. 故 $H \subset xH$. 因此 $xH = H$.

证法二: 设 $x \in H$, 则 $x = xe \in xH$. 从而 $xH \cap H \neq \emptyset$. 于是由 **命题 1.36** 可知 $xH = H$.

综上, 我们就有 $xH = H \iff x \in H$.

一般地, 对于 $x, y \in G$, 由 **引理 1.3** 可知 $xH = yH \iff y^{-1}xH = H \iff H = x^{-1}yH$, 又由上述证明可知

$$y^{-1}xH = H \iff y^{-1}x \in H, x^{-1}yH = H \iff x^{-1}y \in H.$$


故 $xH = yH \iff y^{-1}x \in H \iff x^{-1}y \in H$. 下证 $xH = yH \iff x \in yH \iff y \in xH$.


一方面, 设 $xH = yH$, 则 $x = xe \in xH = yH$, 因此 $x \in yH$. 另一方面, 设 $x \in yH$, 则 $x = ye \in xH$. 从而 $xH \cap yH \neq \emptyset$. 于是由 **命题 1.36** 可知 $xH = yH$. 故 $xH = yH \iff x \in yH$. 同理可证 $xH = yH \iff y \in xH$. \square

推论 1.3

(1) 设 G 是一个群, $H < G$ 是一个子群, $a \in G$, 则

$$axH = aH \iff x \in H.$$

(2) 设 G 是一个群, $K < H < G$, $a_1, a_2 \in G$, $b_1, b_2 \in H$. 若 $a_1b_1K = a_2b_2K$, 则 $a_1H = a_2H$. 

 **笔记** 同理可知对右陪集也有相同的结论.

证明

(1) 由 **引理 1.3** 可知

$$axH = aH \iff xH = H.$$

又由 **引理 1.4** 可知

$$xH = H \iff x \in H.$$

故

$$axH = aH \iff x \in H.$$

(2) 由 **引理 1.4** 可知 $b_2^{-1}a_2^{-1}a_1b_1 \in K$, 从而存在 $k \in K$, 使得 $b_2^{-1}a_2^{-1}a_1b_1 = k$, 于是 $a_2^{-1}a_1 = b_2kb_1^{-1} \in H$. 再根据 **引理 1.4** 可知 $a_1H = a_2H$. \square

命题 1.37

令 $K < H < G$ 是三个有限群, 则

$$[G : K] = [G : H][H : K].$$


证明 **证法一**: 由 **Lagrange 定理** 可得

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H][H : K].$$

证法二: 设 $G/H = \{a_iH\}_{i \in I}$, $H/K = \{b_jK\}_{j \in J}$, 其中 $I = \{1, 2, \dots, [G : H]\}$, $J = \{1, 2, \dots, [H : K]\}$. 则 $|I| = [G : H]$, $|J| = [H : K]$.

先证明 $G/K = \{a_ib_jK\}_{i \in I, j \in J}$. 因为 $G/K = \{xK : x \in G\}$, 所以任取 $xK \in G/K$, 都有 $x \in G$. 由 **定理 1.1** 可知 $G = \bigsqcup_{i=1}^{[G:H]} a_iH$, 从而存在 $i \in I$, 使得 $x \in a_iH$. 于是存在 $h \in H$, 使得 $x = a_ih$. 再由 **定理 1.1** 可知 $H = \bigsqcup_{j=1}^{[H:K]} b_jK$, 因此存在 $j \in J$, 使得 $h \in b_jK$. 进而存在 $k \in K$, 使得 $h = b_jk$. 于是 $x = a_ih = a_ib_jk$. 故由推论可得

$$xK = a_ib_jkK = a_ib_jK.$$

再由 xK 的任意性可知 $G/K = \{a_i b_j K\}_{i \in I, j \in J}$.

再证明 $\{a_i b_j K\}_{i \in I, j \in J}$ 两两互异 (集合中不含重复元素). 设 $a_i b_j K = a_{i'} b_{j'} K$, 则由推论 1.3(2) 可知, $a_i H = a_{i'} H$. 又因为 $G/H = \{a_i H\}_{i \in I}$, 所以 $\{a_i H\}_{i \in I}$ 两两互异, 从而 $a_i = a_{i'}$. 于是由引理 1.3 可得

$$a_i b_j K = a_{i'} b_{j'} K \Leftrightarrow a_i b_j K = a_i b_{j'} K \Leftrightarrow a_i^{-1} a_i b_j K = a_i^{-1} a_i b_{j'} K \Leftrightarrow b_j K = b_{j'} K.$$

又因为 $H/K = \{b_j K\}_{j \in J}$, 所以 $\{b_j K\}_{j \in J}$ 两两互异, 因此 $b_j = b_{j'}$. 故 $\{a_i b_j K\}_{i \in I, j \in J}$ 两两互异 (集合中不含重复元素).

综上, $G/K = \bigsqcup_{i \in I} \bigsqcup_{j \in J} a_i b_j K$. 因此根据定义 1.35 可知

$$[G : K] = |I| \cdot |J| = [G : H][H : K].$$

□

定义 1.36 (两个子群的乘积)

设 G 是一个群, 且 $H, K < G$, 定义 H 和 K 的乘积为

$$HK = \{hk : h \in H, k \in K\}.$$

♣

注 两个子群的乘积不一定是子群.

命题 1.38

令 (G, \cdot) 是一个群. 若 $H, K < G$ 是两个有限子群, 则

$$|HK| = \frac{|H||K|}{|H \cap K|}, \text{ 也即 } |HK||H \cap K| = |H||K|.$$

其中 HK 未必是 G 的子群, 也不一定是群.

♠

证明 证法一: 不考虑重复性, HK 产生 $|H||K|$ 个元素, 其中存在 $hk = h'k', h \neq h', k \neq k'$ 的情况.

现在分析产生相同乘积的 (h, k) 组合个数, 对 $\forall t \in H \cap K$, 都有 $ht = (ht)(t^{-1}k)$. 从而一方面, 对 $\forall t_1, t_2 \in H \cap K$ 且 $t_1 \neq t_2$, 都有 $ht_i \in H, t_i^{-1}k \in K (i = 1, 2), (ht_1, t_1^{-1}k) \neq (ht_2, t_2^{-1}k)$, 但 $(ht_1)(t_1^{-1}k) = hk = (ht_2)(t_2^{-1}k)$. 于是 HK 中产生相同乘积的不同 (h, k) 组合至少有 $|H \cap K|$ 个.

另一方面, 我们有

$$\begin{aligned} hk = h'k' &\iff t = h^{-1}h' = k(k')^{-1} \in H \cap K \\ &\iff \exists t \in H \cap K \text{ s.t. } h' = ht, k' = t^{-1}k. \end{aligned}$$

因此 HK 中产生相同乘积的不同 (h, k) 组合最多有 $|H \cap K|$ 个. 综上, HK 中产生相同乘积的不同 (h, k) 组合恰好有 $|H \cap K|$ 个. 故 $|HK| = \frac{|H||K|}{|H \cap K|}$.

证法二 (有待考察): 原命题等价于证明

$$\frac{|HK|}{|K|} = \frac{|H|}{|H \cap K|}.$$

因为 $H \cap K < H$, 我们可以假设 $H/(H \cap K) = \{a_i(H \cap K)\}_{i \in I}$, 其中 $a_i \in H (i \in I)$ 是两两不同的. 我们只须证明 $HK/K = \{a_i K\}_{i \in I}$, 并且 HK/K 中的重复元对应的指标与 $H/(H \cap K)$ 相同. 再根据 $H/(H \cap K)$ 和 HK/K 的指标集相同都是 I 就能得到两个商集 $H/(H \cap K)$ 和 HK/K 所含元素的个数相等.

任取 $hkK = hK \in HK/K$, 其中 $h \in H$, 故存在 $i \in I$ 使得 $h \in a_i(H \cap K)$. 假设 $h = a_i x$, 其中 x 既在 H , 也在 K . 这样, $hkK = hK = a_i xK = a_i K$, 因为 $x \in K$. 这就证明了第一点.

接着, 假设 $a_i K = a_j K$, 其中 $i, j \in I$. 我们只须证明 $a_i(H \cap K) = a_j(H \cap K)$. 根据引理 1.4 可知 $a_j^{-1} a_i \in K$, 可是 $a_i = a_j \in H$, 于是 $a_j^{-1} a_i \in H \cap K$. 同样根据引理 1.4, 我们知道 $a_i(H \cap K) = a_j(H \cap K)$. 这就证明了第二点.

综上所述, 两个商集 $H/(H \cap K)$ 和 HK/K 所含元素的个数相等. 显然 H 是一个群, 于是由 Lagrange 定理及商

集的性质可得

$$\frac{|HK|}{|K|} \stackrel{?}{=} [HK : K] = [H : H \cap K] = \frac{|H|}{|H \cap K|}.$$

□

注 尽管 HK 不需要成为一个群, 但是 HK/K 完全可以通过 $H/(H \cap K)$ 来明确地构造出来, 它们的大小相等, 这就完成了这个命题的证明.

1.4 正规子群

定义 1.37 (正规子群)

令 (G, \cdot) 是一个群, 且 $N \subset G$. 我们称 N 是个**正规子群**, 记作 $N \triangleleft G$, 若

N 是个子群,

$$\forall a \in G, aN = Na.$$


♣

注 注意 $aN = Na \Leftrightarrow an = na, \forall n \in N$. 虽然 $an = na, \forall n \in N \Rightarrow aN = Na$, 但是 $aN = Na \not\Leftrightarrow an = na, \forall n \in N$. 实际上, $aN = Na \Leftrightarrow \exists n, n' \in N$ s.t. $an = n'a$.

引理 1.5

设 H 是一个么半群, 则 $HH = H$.

♡

 **笔记** 因为群也是么半群, 所以这个引理对群也成立.

证明 一方面, 对 $\forall h_1, h_2 \in H$, 根据乘法封闭性 (乘法是 H 上的代数运算), 都有 $h_1 h_2 \in H$. 故 $HH \subset H$.

另一方面, 设 $h \in H$, 则 $h = he \in HH$, 其中 e 是 H 的单位元. 故 $H \subset HH$. 因此 $HH = H$. □

命题 1.39

令 (G, \cdot) 是一个群, 且 $N \triangleleft G, a, b \in G$, 则

$$(aN) \cdot (bN) = (ab)N.$$

是良定义的.

♣

注 因为陪集代表元的不唯一性可能导致上述乘积运算结果不唯一, 所以上述乘积运算不一定是良定义的, 需要给出证明.

结论 元素与群 (其实只要满足结合律的半群就足够了) 的乘积满足广义结合律. 例如: 设 G 是一个群, 若 $H, K < G, a, b \in G$, 则

$$aHbK = (aH)(bK) = a((Hb)K) = a(H(bK)) = (a(Hb))K = ((aH)b)K.$$

$$abHK = (ab)(HK) = a((bH)K) = a(b(HK)) = ((ab)H)K.$$

.....

即两个陪集相乘可以看作一个陪集或两个陪集的乘积的陪集等.

证明 证法一: 设 $aN = a'N, bN = b'N$, 则由引理 1.4 可知 $a^{-1}a', b^{-1}b' \in N$, 我们只须证明 $abN = a'b'N$, 即 $(ab)^{-1}a'b' = b^{-1}a^{-1}a'b' \in N$. 首先中间这个部分, 即 $a^{-1}a'$, 是在 N 中的. 接着, 利用 N 是个正规子群, 再结合引理 1.3, 我们可以得到 $b^{-1}Nb = N$, 因此, $b^{-1}a^{-1}a'b' \in b^{-1}Nb' = N$. 进一步地, 由引理 1.4 可得 $abN = a'b'N$. 这就证明了良定义性.

证法二: 事实上, 这个乘法可以简单地理解成子集乘法, 即 $(aN)(bN) = \{xy : x \in aN, y \in bN\}$. 我们只须说明, 这从集合意义上, 等于 abN . 而这几乎是显然的. 由于 $Nb = bN$ 及引理 1.5, 我们有 $aNbN = abNN = abN$. 这样, 既然从集合意义上相等, 那么自然就是良定义的 (因为我们不必选取单位元). □

命题 1.40 (商群)

令 (G, \cdot) 是一个群, 且 $N \triangleleft G$, 则 $(G/N, \cdot)$ 构成一个群, 称为 $(G$ 在 N 上的) **商群**, 其中的单位元是 $eN = N$, 每个陪集 aN 的逆元是 $a^{-1}N$.

证明 由命题 1.39 可知商群 $(G/N, \cdot)$ 的乘法是良定义的.

封闭性: 对 $\forall aN, bN \in (G/N, \cdot)$, 其中 $a, b \in G$, 根据 G 对乘法的封闭性可得 $ab \in G$, 从而 $(aN)(bN) = abN \in (G/N, \cdot)$.

结合律: 令 $a, b, c \in G$, 则利用乘法的定义, $(aNbN)cN = (abN)(cN) = ((ab)c)N$. 利用 G 对乘法的结合律, 得到这是等于 $(a(bc))N$ 的. 类似地, 这最终等于 $aN(bNcN)$.

单位元: 令 $a \in G$, 则 $aNeN = (ae)N = aN$, 类似地 $eNaN = aN$.

逆元: 令 $a \in G$, 则 $aNa^{-1}N = (aa^{-1})N = eN$, 类似地 $a^{-1}NaN = eN$.

综上, 若 $N \triangleleft G$, 则 G/N 在这个自然的乘法下构成群, 称为一个商群. \square

引理 1.6 (正规子群的等价条件)

令 (G, \cdot) 是一个群, 且 $N < G$, 则下列命题等价

- (1) N 是 G 的正规子群, 即 $\forall a \in G, aN = Na$.
- (2) $\forall a \in G, aNa^{-1} = N$.
- (3) $\forall a \in G, aNa^{-1} \subset N$.
- (4) $\forall a \in G, \forall n \in N, ana^{-1} \in N$.

证明 显然 (3) 和 (4) 等价.

(1) \Leftrightarrow (2): 一方面, 设 N 是 G 的正规子群. 则由引理 1.3 可得 $\forall a \in G, aNa^{-1} = N$.

另一方面, 设 (2) 成立. 则由引理 1.3 可得 $\forall a \in G, aN = Na$.

(1) \Leftrightarrow (3): 一方面, 设 N 是 G 的正规子群. 令 $a \in G$, 则 $aN = Na$. 同时右乘 a^{-1} 并取一半的包含关系, 我们得到了 $aNa^{-1} \subset N$.

另一方面, 设 (3) 成立. 令 $a \in G$, 则由 $aNa^{-1} \subset N$ 及引理 1.3 得到 $aN \subset Na$, 由 $a^{-1}N(a^{-1})^{-1} \subset N$ 及引理 1.3 得到 $Na \subset aN$. 因此, $aN = Na$. \square

例题 1.6 证明: $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$.

证明 显然 $SL(n, \mathbb{R}) < GL(n, \mathbb{R})$. 任取 $A \in GL(n, \mathbb{R}), N \in SL(n, \mathbb{R})$, 都有

$$\det(ANA^{-1}) = \frac{\det(A)\det(N)}{\det(A)} = \det(N) = 1.$$

从而 $ANA^{-1} \in SL(n, \mathbb{R})$. 故 $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$. \square

命题 1.41 (正规子群的任意交还是正规子群)

设 $(N_i)_{i \in I}$ 是一族 G 的正规子群, 则它们的交集仍然是 G 的正规子群, 即

$$\bigcap_{i \in I} N_i \triangleleft G.$$

证明 首先, 由子群的任意交仍是子群可知 $\bigcap_{i \in I} N_i < G$. 因此我们只需证明正规性. 利用正规子群的等价条件 (3) 可知, 对 $\forall a \in G, \forall n \in \bigcap_{i \in I} N_i$, 我们只须证明 $ana^{-1} \in \bigcap_{i \in I} N_i$ 即可. 任取 $i \in I$, 则 $n \in N_i$. 由于 $N_i \triangleleft G$, 我们有 $ana^{-1} \in N_i$. 因此, 由 i 的任意性可知 $ana^{-1} \in \bigcap_{i \in I} N_i$. 这就证明了 $\bigcap_{i \in I} N_i \triangleleft G$. \square

命题 1.42

令 (G, \cdot) 是一个群, 则

$$\{e\} \triangleleft G,$$

$$G \triangleleft G.$$

证明 平凡群: 怎么乘都是单位元, 所以对乘法封闭; 包含单位元; 唯一的元素的逆元还是单位元; 在这个群中, a 的左右陪集都是 $a\{e\} = \{e\}a = \{a\}$. 因此, $\{e\} \triangleleft G$.

整个群: 子群是显然的; 在整个群 G 中, 每个元素的左右陪集都是全集, 即 $aG = Ga = G$, 这是因为 $a \in G$. 因此, $G \triangleleft G$ (推论 1.3). \square

推论 1.4

(1) 若 G 是一个群, e 是其单位元, 则 $G/\{e\}$ 同构于 G , 即 $G/\{e\} \cong G$.

(2) 若 G 是一个群, 则 G/G 是平凡群, 即 $G/G = \{e\}$.

证明

(1) 令

$$f: G \rightarrow G/\{e\}, a \mapsto a\{e\} = \{a\}.$$

显然 f 是双射. 对 $\forall a, b \in G$, 我们都有

$$f(ab) = \{ab\} = ab\{e\} = (a\{e\})(b\{e\}) = \{a\}\{b\} = f(a)f(b).$$

因此 f 也是同态映射. 于是 f 是同构映射. 故 $G/\{e\} \cong G$.

(2) 由命题 1.40 及命题 1.42 可知 G/G 是一个群. 注意到 $\forall a \in G$, 都有 $aG = G$. 因此 $G/G = G$. 于是 $|G/G| = 1$. 故 $G/G = \{e\}$. \square

命题 1.43

令 (G, \cdot) 是个阿贝尔群, 则子群就是正规子群, 正规子群也就是子群, 即

$$H < G \iff H \triangleleft G$$

证明 \Leftarrow : 由于正规子群都是子群, 故显然成立.

\Rightarrow : 根据阿贝尔群满足交换律可知 $aH = \{ah : h \in H\} = \{ha : h \in H\} = Ha$. \square

定理 1.3 (群同构第一定理)

设 $f: G \rightarrow G'$ 是一个群同态, 则 $\ker(f) \triangleleft G$, 且 G 在 $\ker(f)$ 上的商群同构于 $\text{im}(f)$, 即

$$G/\ker(f) \cong \text{im}(f).$$

特别地, 若 f 是满同态, 则

$$G/\ker(f) \cong G'.$$

若 f 是单同态, 则

$$G/\{e\} \cong G \cong \text{im}(f).$$

若 G 是有限群, 则

$$\frac{|G|}{|\ker(f)|} = |\text{im}(f)|, \text{ 也即 } |G| = |\ker(f)||\text{im}(f)|.$$

注 要注意, 同态的像 $(\text{im}(f))$ 未必是 G' 的正规子群, 往往只是普通的子群.

证明 根据命题 1.19 和 Lagrange 定理, 这三条推论都是显然的, 唯一要说明的是 $G/\{e\}$ 为什么同构于 G , 这由推论 1.4(1) 可直接得到. 这就意味着我们只须证明原命题即可.

首先要说明每个同态的核都是定义域的正规子群. 我们只须证明, 若 $a \in G, n \in \ker(f)$, 则 $ana^{-1} \in \ker(f)$. 注意到

$$f(ana^{-1}) = f(a)e'f(a)^{-1} = e'.$$

因此 $ana^{-1} \in \ker(f)$. 这就证明了 $\ker(f) \triangleleft G$.

接下来, 我们要找到一个从商群 $G/\ker(f)$ 到像集 $\text{im}(f)$ 的同构映射. 我们称这个映射叫 $\tilde{f} : G/\ker(f) \rightarrow \text{im}(f)$, 对于 $a \in G$, 定义为

$$\tilde{f}(a\ker(f)) = f(a).$$

为了方便起见, 在不会引起歧义的情况下, 我们令 $N = \ker(f)$, 也即

$$\tilde{f}(aN) = f(a).$$

考虑到陪集代表元的不唯一性, 我们要证明良定义性. 假设 $aN = a'N$, 或 $a^{-1}a' \in N$, 只须证明 $f(a) = f(a')$, 而这是因为

$$f(a') = f(aa^{-1}a') = f(a)f(a^{-1}a') = f(a)f(eN) = f(a)e' = f(a).$$

其中 e 是 G 的单位元, e' 是 G' 的单位元. 这就证明了良定义性.

接下来, 我们要证明 \tilde{f} 既是同态, 也是双射 (单射 + 满射).

同态: 令 $a, b \in G$, 则 $\tilde{f}(aN) = f(a), \tilde{f}(bN) = f(b)$, 而由 $N = \ker f \triangleleft G$ 及 f 是一个群同态可得

$$\tilde{f}((aN)(bN)) = \tilde{f}(abN) = f(ab) = f(a)f(b) = \tilde{f}(aN)\tilde{f}(bN).$$

这就证明了 \tilde{f} 是一个同态.

单射: 只须证明 $\ker(\tilde{f}) = \{N\}$. 设 $\tilde{f}(aN) = e'$, 则根据定义, $f(a) = e'$, 故 $a \in \ker(f) = N$, 所以 $aN = N$, 这就证明了 \tilde{f} 是一个单射.

满射: 令 $a' \in \text{im}(f)$, 取 $a \in G$ 使得 $a' = f(a)$. 因此, $\tilde{f}(aN) = f(a) = a'$, 这就证明了 \tilde{f} 是一个满射.

综上所述, \tilde{f} 是一个从商群 $G/\ker(f)$ 到像集 $\text{im}(f)$ 的同构. 作为结论,

$$G/\ker(f) \cong \text{im}(f).$$

这就完成了整个命题的证明. □

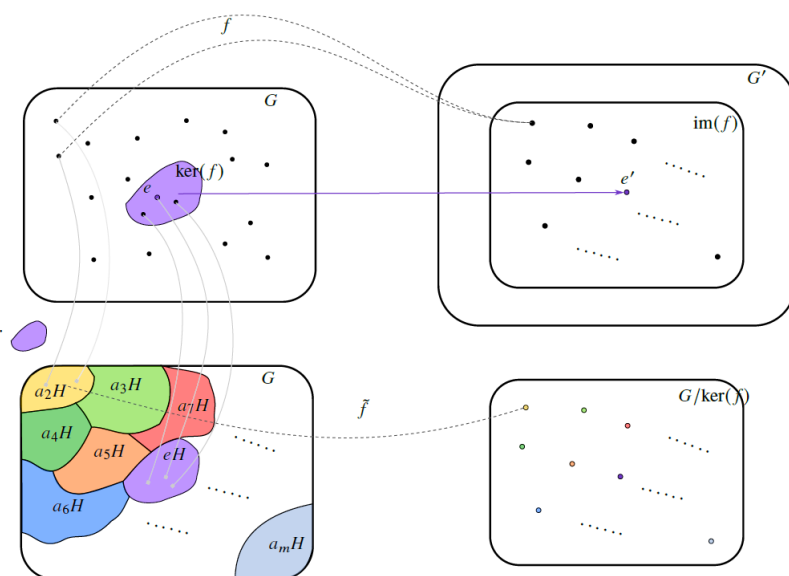


图 1.5: 群同构第一定理示意图

例题 1.7 证明: $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R}^\times$.

证明 由命题 1.4 可知

$$\det : GL(n, \mathbb{R}) \rightarrow \mathbb{R}^\times.$$

是个满同态, 且 $\ker(\det) = SL(n, \mathbb{R})$, 故由群同构第一定理, 我们有

$$SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R}) \text{ 且 } GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R}^\times.$$

□

推论 1.5

设 G 是有限群, $f: G \rightarrow G'$ 是一个群同态, 则

$$|\operatorname{im} f| \mid \gcd(|G|, |G'|).$$

♡

证明 由群同构第一定理可知, $|\operatorname{im} f| \mid |G|$. 由 Lagrange 定理可知, $|\operatorname{im} f| \mid |G'|$. 故

$$|\operatorname{im} f| \mid \gcd(|G|, |G'|).$$

□

例题 1.8 设 $f: C_{12} \rightarrow C_{35}$ 是一个群同态, 求证: f 是平凡同态, 即对 $\forall x \in C_{12}$, 都有 $f(x) = e$, 也即 $\operatorname{im} f = \{e\}$, 其中 e 是 C_{35} 的单位元.

证明 由推论 1.5 可知, $|\operatorname{im} f| \mid \gcd(12, 35) = 1$. 又因为 $\operatorname{im} f < G'$, 所以 $\operatorname{im} f = \{e\}$.

□

引理 1.7

设 (G, \cdot) 是一个群, 且 $N \triangleleft G, H < G$. 则 $HN < G$.

♡

证明 设 e 是 G 的单位元, 则由 $N \triangleleft G, H < G$ 可知, $e \in N \cap H$. 从而 $e = ee \in HN$.

对 $\forall h_1 n_1, h_2 n_2 \in HN$, 其中 $h_1, h_2 \in H, n_1, n_2 \in N$. 由 $N \triangleleft G, H < G$ 可得

$$h_1 n_1 (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 n_1 h_2^{-1} n_2^{-1} = h_1 h_2^{-1} n_1 n_2^{-1} \in HN.$$

故 $HN < G$.

□

定理 1.4 (群同构第二定理)

设 (G, \cdot) 是一个群, 且 $N \triangleleft G, H < G$. 则 $H \cap N \triangleleft H, N \triangleleft HN$, 且

$$H/(H \cap N) \cong HN/N.$$

这和之前两个子群乘积的阶的公式是类似的.

♡

注 由引理 1.7 可知 $HN < G$. 故此时 $N \triangleleft HN$ 是有意义的.

证明 第一, 要证明 $H \cap N \triangleleft H$. 令 $h \in H$, 而 $x \in H \cap N$, 则 $h x h^{-1} \in H$, 而且因为 $N \triangleleft G, h x h^{-1} \in N$, 因此 $h x h^{-1} \in H \cap N$.

第二, 要证明 $N \triangleleft HN$. 令 $hn \in HN$, 而 $n' \in N$. 则由引理 1.6(2) 可得 $h n n' (hn)^{-1} = h (n n' n^{-1}) h^{-1} \in h N h^{-1} = N$.

第三, 要证明 $H/(H \cap N) \cong HN/N$. 令 $f: H \rightarrow HN/N$, 定义为

$$f(h) = hN.$$

这显然是良定义的 (若 $h = h' \in H$, 则 $h^{-1} h' = e \in N$, 从而 $f(h) = hN = h'N = f(h')$). 又由 $N \triangleleft G$ 及引理 1.5 可知, 对 $\forall h_1, h_2 \in H$, 都有

$$f(h_1 h_2) = h_1 h_2 N = h_1 h_2 N N = h_1 N h_2 N = f(h_1) f(h_2).$$

故 f 是同态的. 根据 $HN/N = \{hnN : h \in H, n \in N\} = \{hN : h \in H\}$ 可知, f 还是个满同态.

接下来, 根据引理 1.4 可知, f 的核是 $\ker(f) = \{h \in H : hN = eN\} = \{h \in H : h \in N\} = H \cap N$. 因此, 根据群同

构第一定理,

$$H/(H \cap N) \cong HN/N.$$

这就证明了群同构第二定理. □

引理 1.8

设 (G, \cdot) 是一个群, 且 $N \triangleleft G, M \triangleleft G, M < N$, 则 $M \triangleleft N$. ♥

证明 令 $n \in N \subset G, m \in M$, 则由 $M \triangleleft G$ 可知, $nmn^{-1} \in M$. 因此由引理 1.6 可知 $M \triangleleft N$. □

定理 1.5 (群同构第三定理)

设 (G, \cdot) 是一个群, 且 $N \triangleleft G, M \triangleleft G, M < N$. 则 $N/M \triangleleft G/M$, 且

$$(G/M)/(N/M) \cong G/N. \quad \heartsuit$$

证明 首先显然有 $N/M \subset G/M$. 由引理 1.8 可知 $M \triangleleft N$. 因此 N/M 是个商群. 因为这两个都是群, 所以对单位元、乘法和逆元都有封闭性. 因此就有 $N/M < G/M$. 接下来我们可以先证明正规性, 这也几乎是显然的. 令 $nM \in N/M (n \in N), gM \in G/M (g \in G)$, 则由 $M \triangleleft N, N \triangleleft G$ 可得

$$(gM)(nM)(gM)^{-1} = (gng^{-1})M \in \{nM : n \in N\} = N/M.$$

因此 $N/M \triangleleft G/M$.

那么, 我们要定义 $f : G/M \rightarrow G/N$, 定义为

$$f(gM) = gN.$$

要证明良定义性. 假设 $gM = g'M$, 则 $g^{-1}g' \in M$, 故 $g^{-1}g' \in N$, 所以 $gN = g'N$.

同态是显然的: 对 $\forall gM, g'M \in G/M$, 都有

$$f(gMg'M) = f(gg'M) = gg'N = gNg'N = f(gM)f(g'M).$$

满同态几乎也是显然的. 任取 $gN \in G/N (g \in G)$, 则 $f(gM) = gN$.

最后, 注意到

$$\ker(f) = \{gM : f(gM) = gN = eN\} = \{gM : g \in N\} = N/M.$$

于是根据群同构第一定理, 这就告诉我们

$$(G/M)/(N/M) \cong G/N.$$

综上所述, 我们就证明了群同构第三定理. □

1.5 群作用

定义 1.38 (置换群 (对称群))

令 S 是一个集合, 则 S 上的**置换群** (或**对称群**), 记作 $(\text{Perm}(S), \circ)$, 由所有 S 到自身的双射构成, 而这里的运算是映射的复合运算. 此即

$$\text{Perm}(S) = \{f : S \rightarrow S \text{ 双射}\}. \quad \clubsuit$$

证明 首先, 映射的复合是满足结合律的. 这是根据定义立刻可知的.

单位元是恒等映射, 记作 id , 对所有 $s \in S$, 定义为

$$\text{id}(x) = x.$$

故显然有, 对所有 $f \in \text{Perm}(S), f \circ \text{id} = \text{id} \circ f = f$.

逆元是根据双射可知的. 假如 f 是一个从 S 到自身的双射, 则存在其逆映射 f^{-1} , 使得 $f \circ f^{-1} = f^{-1} \circ f = \text{id}$.

综上所述, $(\text{Perm}(S), \circ)$ 是个群, 称为 S 上的置换群 (或对称群). \square

例题 1.9 设 $S = \{1, 2, \dots, n\}$, 记 $S_n = \text{Perm}(S) = \{f : S \rightarrow S \text{ 双射}\}$. 证明: $|S_n| = n!$.

证明 设 $f : S \rightarrow S$ 是双射, 我们逐个定义 f 的像. 首先, $f(1)$ 有 n 种不同的取法, 取定 $f(1)$ 以后, $f(2)$ 就只有 $n-1$ 种不同的取法, 否则 $f(1) = f(2)$ 与双射矛盾. 依此类推, 可知 $f(i)$ 就只有 $n+1-i$ 种不同的取法, $i = 1, 2, \dots, n$. 故 f 就有 $n!$ 种不同的取法, 即 $|S_n| = n!$. \square

命题 1.44

令 (G, \cdot) 是一个群, 我们定义

$$\phi : (G, \cdot) \rightarrow (\text{Perm}(G), \circ), x \mapsto \phi_x.$$

其中 $\phi_x : G \rightarrow G, y \mapsto xy$. 则 ϕ 是个群同态.

证明 证明是很简单的. 令 $x, y \in G$, 对于 $z \in G$, 我们有

$$(\phi_x \circ \phi_y)(z) = x(yz) = (xy)z = \phi_{xy}(z)$$

由于这对于所有 $z \in G$ 都成立, 故

$$\phi_x \circ \phi_y = \phi_{xy}$$

即

$$\phi(xy) = \phi(x) \circ \phi(y)$$

这就证明了 $\phi : G \rightarrow \text{Perm}(G)$ 是个群同态. \square

定义 1.39 (群作用)

令 (G, \cdot) 是一个群, S 是一个非空集合, 而 $\phi : G \rightarrow \text{Perm}(S)$. 若 ϕ 是一个群同态, 则我们说 ϕ 是 G 在 (集合) S 上的群作用.

命题 1.45 (群作用的等价条件)

设 G 是一个群, S 是一个非空集合.

(1) 若 ϕ 是 G 在 S 的群作用, 记 $\text{Perm}(S) = \{\phi_x : x \in G\}$, 则一定满足

$$\forall s \in S, e \cdot s = s, \text{ 即 } \forall s \in S, \phi_e(s) = s.$$

$$\forall x, y \in G, \forall s \in S, x \cdot (y \cdot s) = (xy) \cdot s, \text{ 即 } \forall x, y \in G, \forall s \in S, \phi_x(\phi_y(s)) = (\phi_x \circ \phi_y)(s) = \phi_{xy}(s).$$

(2) 若 $\phi : G \times S \rightarrow S$ 是满足

$$\forall s \in S, e \cdot s = s, \text{ 即 } \forall s \in S, \phi(e, s) = s.$$

$$\forall x, y \in G, \forall s \in S, x \cdot (y \cdot s) = (xy) \cdot s, \text{ 即 } \forall x, y \in G, \forall s \in S, \phi(x, \phi(y, s)) = \phi(xy, s).$$

的映射, 则一定存在一个 G 在 S 上的群作用 $\tilde{\phi}$.

注 在不引起歧义的情况下, 我们用 $x \cdot s$, 甚至 xs , 来代表 $\phi_x(s)$, 或 $\phi(x, s)$ (其中 $x \in G, s \in S$).

笔记 命题中的第一条性质, 是说明 ϕ 是良定义的 (ϕ_x 是双射), 而第二条性质是说明 ϕ 是同态. 二者缺一不可. 这两条性质加起来, 就是群作用的定义.

证明

(1) 若 ϕ 是一个群作用, 则显然利用同态的性质我们有第二条. 而根据同态把单位元映到单位元, 我们有 $\phi_e = \text{id}$, 即对所有 $s \in S, es = s$. 这就证明了 (1).

(2) 对 $\forall x \in G$, 令

$$\phi_x : S \rightarrow S, s \mapsto \phi(x, s) = xs,$$

$$\phi_{x^{-1}} : S \rightarrow S, s \mapsto \phi(x^{-1}, s) = x^{-1}s.$$

从而由假设可知, 对 $\forall s \in S$, 都有

$$\phi_x \circ \phi_{x^{-1}}(s) = xx^{-1}s = es = s,$$

$$\phi_{x^{-1}}(s) \circ \phi_x = x^{-1}xs = es = s.$$

因此 $\phi_{x^{-1}}$ 是 ϕ_x 的逆映射, 故对 $\forall x \in G, \phi_x$ 都是双射. 于是 $\{\phi_x : x \in G\} \subset \text{Perm}(S)$. 令

$$\tilde{\phi} : G \rightarrow \text{Perm}(S), x \mapsto \phi_x.$$

由假设可知, 对 $\forall x, y \in G, \forall s \in S$, 都有

$$x \cdot (y \cdot s) = (xy) \cdot s \Leftrightarrow (\phi_x \circ \phi_y)(s) = \phi_{xy}(s).$$

因此 $\phi_{xy} = \phi_x \phi_y, \forall x, y \in G$. 故 $\tilde{\phi}(xy) = \tilde{\phi}(x)\tilde{\phi}(y), \forall x, y \in G$. 即 $\tilde{\phi}$ 是群同态. 进而 $\tilde{\phi}$ 就是 G 在 S 上的一个群作用.

□

定义 1.40 (左乘作用)

设 (G, \cdot) 是一个群, 我们对 $x \in G$, 定义 $\phi_x \in \text{Perm}(G)$, 对 $y \in G$, 定义为

$$\phi_x(y) = xy.$$

则 $\phi : G \rightarrow \text{Perm}(G)$, 对 $x \in G$, 定义为 $\phi(x) = \phi_x$, 被称为 G 的左乘作用.

♣

命题 1.46

设 (G, \cdot) 是一个群, 则 G 的左乘作用是 G 在自身的一个群作用.

♣

证明 首先, 我们要说明 ϕ_x 是双射, 而这是显然的, 因为其逆是 $\phi_{x^{-1}}$. 而这是因为, 对于 $y \in G$,

$$(\phi_x \circ \phi_{x^{-1}})(y) = \phi_x(x^{-1}y) = x(x^{-1}y) = y$$

$$(\phi_{x^{-1}} \circ \phi_x)(y) = \phi_{x^{-1}}(xy) = x^{-1}(xy) = y$$

这样, $\phi : G \rightarrow \text{Perm}(G)$ 就是良定义的. 接下来, 我们证明 ϕ 是个同态. 令 $x, y \in G, z \in G$, 则

$$(\phi_x \circ \phi_y)(z) = \phi_x(yz) = x(yz) = (xy)z = \phi_{xy}(z)$$

这对所有 $z \in G$ 都成立, 故

$$\phi_{xy} = \phi_x \circ \phi_y$$

即

$$\phi(xy) = \phi(x) \circ \phi(y)$$

这就证明了左乘作用确实是一个群在自身的群作用.

□

定义 1.41 (共轭作用)

设 (G, \cdot) 是一个群, 我们对 $x \in G$, 定义 $\phi_x \in \text{Perm}(G)$, 对 $y \in G$, 定义为

$$\phi_x(y) = xyx^{-1}.$$

则 $\phi : G \rightarrow \text{Perm}(G)$, 对 $x \in G$, 定义为 $\phi(x) = \phi_x$, 被称为 G 的共轭作用.

♣

命题 1.47

设 (G, \cdot) 是一个群, 则 G 的共轭作用是 G 在自身的一个群作用.

♣

证明 首先, 我们要说明 ϕ_x 是双射, 而这是显然的, 因为其逆是 $\phi_{x^{-1}}$. 而这是因为, 对于 $y \in G$,

$$(\phi_x \circ \phi_{x^{-1}})(y) = \phi_x(x^{-1}yx) = x(x^{-1}yx)x^{-1} = y$$

$$(\phi_{x^{-1}} \circ \phi_x)(y) = \phi_{x^{-1}}(xyx^{-1}) = x^{-1}(xyx^{-1})x = y$$

这样, $\phi: G \rightarrow \text{Perm}(G)$ 就是良定义的. 接下来, 我们证明 ϕ 是个同态. 令 $x, y \in G, z \in G$, 则

$$(\phi_x \circ \phi_y)(z) = \phi_x(yzy^{-1}) = x(yzy^{-1})x^{-1} = (xy)z(xy)^{-1} = \phi_{xy}(z)$$

这对所有 $z \in G$ 都成立, 故

$$\phi_{xy} = \phi_x \circ \phi_y$$

即

$$\phi(xy) = \phi(x) \circ \phi(y)$$

这就证明了共轭作用确实是一个群在自身的群作用. □

命题 1.48

令 (G, \cdot) 是一个群, $x \in G$, 则 $\phi_x: G \rightarrow G$, 对 $y \in G$, 定义为

$$\phi_x(y) = xyx^{-1}.$$

是一个群 G 的自同构 (即到自身的同构).

证明 由命题 1.47 的证明可知 ϕ_x 一定是双射, 因为它的逆是 $\phi_{x^{-1}}$. 因此我们只须证明 ϕ_x 本身还是个同态 (不是说 ϕ 是同态, 而是说每个 ϕ_x 是同态). 因此我们令 $y, z \in G$, 只须证明 $\phi_x(yz) = \phi_x(y)\phi_x(z)$. 而这是因为

$$\phi_x(y)\phi_x(z) = (xyx^{-1})(xzx^{-1}) = x(yz)x^{-1} = \phi_x(yz).$$

恰好约掉. 这就证明了共轭作用下的每一个 ϕ_x 都是群 G 的自同构. □

定义 1.42 (内自同构与外自同构)

设 (G, \cdot) 是一个群, 则一个 G 的 (由 $x \in G$ 引出的) **内自同构**, 指的是 $\phi_x: G \rightarrow G$, 对 $y \in G$, 定义为

$$\phi_x(y) = xyx^{-1}.$$

而其他所有 G 上的自同构, 则称为 G 上的**外自同构**.

定义 1.43 (轨道与稳定化子)

令 $\phi: (G, \cdot) \rightarrow (\text{Perm}(S), \circ)$ 是一个 G 在 S 的群作用. 若 $s \in S$. 则我们定义 s 的**轨道**, 记作 $\text{Orb}(s)$, 定义为

$$\text{Orb}(s) = \{s' \in S : \exists x \in G, s' = xs\} = \{xs : x \in G\}.$$

我们定义 s 的**稳定化子**, 记作 $\text{Stab}(s)$, 定义为

$$\text{Stab}(s) = \{x \in G : xs = s\}.$$

命题 1.49

令 $\phi: (G, \cdot) \rightarrow (\text{Perm}(S), \circ)$ 是一个 G 在 S 的群作用, 而 $s, s' \in S$, 则 $\text{Orb}(s)$ 与 $\text{Orb}(s')$ 要么相等, 要么无交.

因此, S 可以写成轨道的无交并, $S = \bigsqcup_{s \in S} \text{Orb}(s) = \bigsqcup_{s \in S} \{xs : x \in G\}$.

证明 假设它们有交集, 即假设 $s'' \in \text{Orb}(s) \cap \text{Orb}(s')$. 进一步, 我们找到 $x, x' \in G$, 使得 $s'' = xs = x's'$. 根据对称性, 我们只须证明 $\text{Orb}(s) \subset \text{Orb}(s')$.

任取 $ys \in \text{Orb}(s) (y \in G)$, 则

$$ys = (yx^{-1})xs = (yx^{-1})x's' = (yx^{-1}x')s' \in \text{Orb}(s')$$

根据对称性, 我们就知道 $\text{Orb}(s) = \text{Orb}(s')$.

又因为对 $\forall s \in S$, 都有 $s = es$, 其中 e 是 $\text{Perm}S$ 的单位元, 即恒等映射. 故 $s \in \text{Orb}(s) \subset \{\text{Orb}(s) : s \in S\}$. □

命题 1.50

令 $\phi: (G, \cdot) \rightarrow (\text{Perm}(S), \circ)$ 是一个 G 在 S 的群作用, 而 $s \in S$, 则 s 的稳定化子是 G 的子群, 即

$$\text{Stab}(s) < G$$

♣

证明 一, $es = s$. 二, 若 $x, y \in \text{Stab}(s)$, 则 $(xy)s = x(ys) = xs = s$. 三, 若 $xs = s$, 则左乘 x^{-1} (两边同时作用 x^{-1}), 得到 $x^{-1}s = s$. □

引理 1.9

令 $\phi: (G, \cdot) \rightarrow (\text{Perm}(S), \circ)$ 是一个 G 在 S 的群作用, $s \in S, x, y \in G$, 则 $xs = ys$ 当且仅当 $x^{-1}y \in \text{Stab}(s)$. ♡

证明 对 $xs = ys$ 两边同时左乘 x^{-1} (两边同时作用 x^{-1}), 就显然了. □

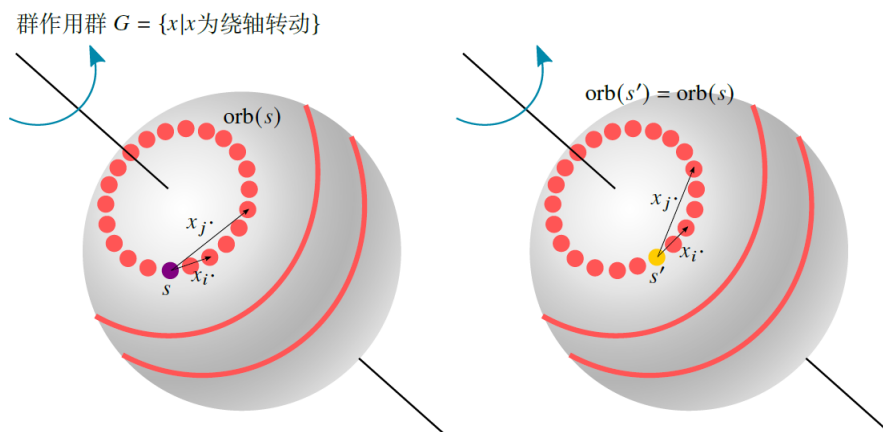


图 1.6: 群作用与轨道

定理 1.6 (轨道 - 稳定化子定理)

令 $\phi: (G, \cdot) \rightarrow (\text{Perm}(S), \circ)$ 是一个 G 在 S 的群作用, $s \in S$, 则存在 $G/\text{Stab}(s)$ 到 $\text{Orb}(s)$ 的双射. 特别地, 若 G 是有限群, 则

$$|G| = |\text{Stab}(s)| \cdot |\text{Orb}(s)|.$$

♡

证明 令 $f: G/\text{Stab}(s) \rightarrow \text{Orb}(s)$, 定义为 $f(x \text{Stab}(s)) = xs$.

首先证明 f 是良定义的. 根据引理 1.9, 若 $x \text{Stab}(s) = y \text{Stab}(s)$, 则由引理 1.4 可知 $x^{-1}y \in \text{Stab}(s)$, 故 $xs = ys$. 根据 $\text{Orb}(s)$ 的定义, f 显然是一个满射.

单射则是再次利用引理 1.9. 若 $xs = ys$, 则 $x^{-1}y \in \text{Stab}(s)$, 故 $x \text{Stab}(s) = y \text{Stab}(s)$.

假如 G 是有限群, 则同时取集合大小, 由定理 1.2 就得到了

$$|G| = |\text{Stab}(s)| \cdot |\text{Orb}(s)|$$

综上, 我们就证明了轨道 - 稳定化子定理. □

定义 1.44

二面体群 D_{2n} , 它是由所有正 n 边形到自身的对称变换所构成的.

对称变换就是把自身映到自身, 而且是保距的.

保距指的是, 原先距离相同的点, 变换后距离仍然相同. ♣

笔记 如图 1.7 中的例子.

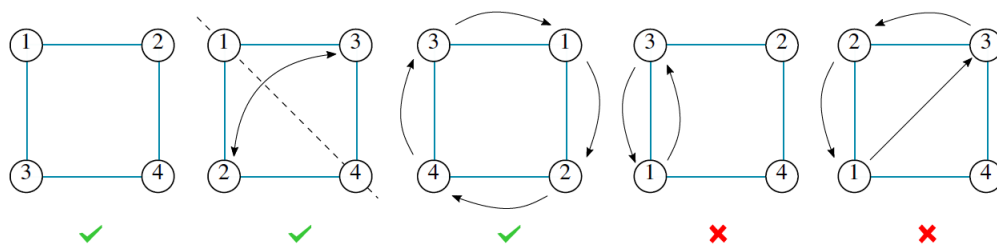


图 1.7: 置换群中的对称变换

例题 1.10 $|D_{2n}| = 2n$.

笔记 事实上, 每一个对称变换由其 n 个顶点的像唯一确定, 因为其余的点都可以通过顶点来找到位置. 很明显, D_{2n} 中的元素都是个轴对称图形, 有 n 个翻折变换; 这还是个中心对称图形, 有 n 个旋转变换. 由此可知, 二面体群 D_{2n} 就是恰好由 n 个翻折变换和 n 个旋转变换所组成的群.

证明 任取正多边形的一个顶点 s , 考虑其轨道 $\text{Orb}(s)$. 最多只有 n 个顶点可以去, 而 n 个旋转变换恰好带 s 去了这些顶点, 因此 $|\text{Orb}(s)| = n$.

接下来, 考虑其稳定化子 $\text{Stab}(s)$. 如果 $x \in D_{2n}$ 把 s 映射到 s , 但又有保证是一个等距变换, 则 s 相邻的两个顶点一定要被映射到这两个顶点. 其中一个是恒等变换, 而另一个是沿 s 所在的对称轴的翻折变换. 不难看出, 这两个是唯一的 s 的稳定化子. 因此 $|\text{Stab}(s)| = 2$.

根据定理 1.6, $|D_{2n}| = |\text{Orb}(s)| \cdot |\text{Stab}(s)| = 2n$. 这就证明了这个命题. \square

1.6 群论与数论

定义 1.45 (整除)

令 $n \in \mathbb{Z} \setminus \{0\}$, 而 $m \in \mathbb{Z}$. 我们说 n 整除 m , 记作 $n \mid m$, 若

$$m \in n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$$

命题 1.51

若 $n \in \mathbb{Z}$, 则 $(n\mathbb{Z}, +) \triangleleft (\mathbb{Z}, +)$.

注 这里的加法和乘法都是通常意义下的整数加法和整数乘法.

证明 令 $f: \mathbb{Z} \rightarrow \mathbb{Z}$, 对 $m \in \mathbb{Z}$, 定义为

$$f(m) = mn.$$

则对 $\forall m_1, m_2 \in (\mathbb{Z}, +)$, 都有

$$f(m_1 + m_2) = (m_1 + m_2)n = m_1n + m_2n = f(m_1) + f(m_2).$$

故 f 是 $(\mathbb{Z}, +)$ 到 $(\mathbb{Z}, +)$ 的群同态. 因此由命题 1.18 可知 $n\mathbb{Z} = \text{im}(f) < \mathbb{Z}$. 又因为 $(\mathbb{Z}, +)$ 是阿贝尔群, 因此由命题 1.43 可知 $(n\mathbb{Z}, +) \triangleleft (\mathbb{Z}, +)$. \square

命题 1.52

若 $(A, +) < (\mathbb{Z}, +)$, 则存在 $n \in \mathbb{N}_0$, 使得 $A = n\mathbb{Z}$.

证明 (i) 若 $A = \{0\}$, 则 $A = 0\mathbb{Z}$.

(ii) 若 $A \neq \{0\}$, 则由 $(A, +) < (\mathbb{Z}, +)$ 可知, A 在加法逆元下封闭. 从而 $A \cap \mathbb{N}_1 \neq \emptyset$, 否则 $A \subset \mathbb{Z} - \mathbb{N}_1$ 且 $A \neq \{0\}$, 于是任取 $x \in A \subset \mathbb{Z} - \mathbb{N}_1$ 且 $x \neq 0$, 则其加法逆元 $-x \in A$, 但 $-x \in \mathbb{N}_1$, 这与 $A \subset \mathbb{Z} - \mathbb{N}_1$ 矛盾!

令 $n = \min(A \cap \mathbb{N}_1)$ (n 的良定义是因为良序公理), 则 $n \in A$. 我们断言 $A = n\mathbb{Z}$.


注意到 $n\mathbb{Z} = \{nm : m \in \mathbb{Z}\} = \langle n \rangle$, 故我们只需证 $A = \langle n \rangle$.

任取 $m \in \mathbb{Z}$, 则由 $n \in A$ 及 A 在加法下封闭可知, $nm = \underbrace{n + n + \cdots + n}_{m \uparrow} \in A$. 故 $\langle n \rangle \subset A$.

任取 $a \in A$, 假设 $a \notin n\mathbb{Z}$, 则由带余除法可知, 存在 $q, r \in \mathbb{Z}$, 使得 $a = qn + r$, 其中 $0 \leq r \leq n-1$. 因为 $a \notin n\mathbb{Z}$, 所以 $r \neq 0$. 又 $qn \in \langle n \rangle \subset A, a \in A$. 故由 A 对加法和加法逆元封闭可知, $r = a - qn \in A$. 而 $1 \leq r \leq n-1 < n$, 这与 $n = \min(A \cap \mathbb{N}_1)$ 矛盾! 故 $a \in n\mathbb{Z}$. \square

推论 1.6

任意的无限循环群 $\langle x \rangle$ ($|x| = \infty$) 的子群都是形如 $\langle x^n \rangle = \{x^{nm} : m \in \mathbb{Z}\}$ 的形式, 进而都是正规子群.

即对任意的无限循环群 $\langle x \rangle$ ($|x| = \infty$), 任取 $A < \langle x \rangle$, 则一定存在 $n \in \mathbb{Z}$, 使得 $A = \langle x^n \rangle = \{x^{nm} : m \in \mathbb{Z}\}$, 并且 $A \triangleleft \langle x \rangle$. 

证明 由命题 1.33 可知, 任意无限循环群 $\langle x \rangle$ ($|x| = \infty$) 都同构于整数加群 $(\mathbb{Z}, +)$, 故 A 一定同构于 \mathbb{Z} 的某一子群. 于是由命题 1.52 可知, 存在 $n \in \mathbb{Z}$, 使得 A 同构于 $n\mathbb{Z}$. 因此 $A = \langle x^n \rangle = \{x^{nm} : m \in \mathbb{Z}\}$. 又由命题 1.51 可知 $n\mathbb{Z} \triangleleft \mathbb{Z}$. 故 $A \triangleleft \langle x \rangle$. \square

定义 1.46 (同余 (模 n))

设 $n \in \mathbb{N}_1$, 而 $a, b \in \mathbb{Z}$. 我们说 a 同余 b (模 n), 记作 $a \equiv b \pmod{n}$, 若

$$a + n\mathbb{Z} = b + n\mathbb{Z},$$

或

$$a - b \in n\mathbb{Z}.$$

或

$$n \mid (a - b).$$

或

a 和 $b \pmod{n}$ 的余数相同.



证明 $n \mid (a - b) \Leftrightarrow a - b \in n\mathbb{Z}$ 是显然的. 由引理 1.4 可知 $a + n\mathbb{Z} = b + n\mathbb{Z} \Leftrightarrow a - b \in n\mathbb{Z}$. 下证 $a - b \in n\mathbb{Z} \Leftrightarrow a$ 和 $b \pmod{n}$ 的余数相同.

\Rightarrow : 由 $a - b \in n\mathbb{Z}$ 可知, 存在 $m \in \mathbb{Z}$, 使得 $a - b = nm$. 从而 $a = b + nm$. 由带余除法可知, 存在 $q, r \in \mathbb{Z}$, 使得 $b = qn + r$, 其中 $0 \leq r \leq n-1$. 于是

$$a = b + nm = (q + m)n + r.$$

故 a 和 $b \pmod{n}$ 的余数都是 r .

\Leftarrow : 由 a 和 $b \pmod{n}$ 的余数相同可知, 存在 $q, p, r \in \mathbb{Z}$, 使得

$$a = qn + r, \quad b = pn + r.$$

其中 $0 \leq r \leq n-1$. 于是 $a - b = (q - p)n \in n\mathbb{Z}$.


综上所述, a 同余 b (模 n) 是良定义的. \square

命题 1.53 (同余 (模 n) 是 (\mathbb{Z}) 上的) 等价关系)

设 $n \in \mathbb{N}_1$, 对 $\forall a, b, c \in \mathbb{Z}$, 都满足

自反性: $a \equiv a \pmod{n}$.

对称性: 若 $a \equiv b \pmod{n}$, 则 $b \equiv a \pmod{n}$.

传递性: 若 $a \equiv b \pmod{n}, b \equiv c \pmod{n}$, 则 $a \equiv c \pmod{n}$. 

证明 自反性: 由 $a + n\mathbb{Z} = a + n\mathbb{Z}$ 可知 $a \equiv a \pmod{n}$.

对称性: 由 $a \equiv b \pmod{n}$ 可知 $a + n\mathbb{Z} = b + n\mathbb{Z}$, 从而 $b + n\mathbb{Z} = a + n\mathbb{Z}$, 故 $b \equiv a \pmod{n}$.

传递性: 由 $a \equiv b \pmod{n}, b \equiv c \pmod{n}$ 可知 $a + n\mathbb{Z} = b + n\mathbb{Z}, b + n\mathbb{Z} = c + n\mathbb{Z}$. 从而 $a + n\mathbb{Z} = c + n\mathbb{Z}$. 故 $a \equiv c \pmod{n}$. \square

命题 1.54

设 $n \in \mathbb{N}_1, a \in \mathbb{Z}$, 记在同余 $(\text{mod } n)$ 的等价关系下以 a 为代表元的等价类为 $\bar{a} = [a]$, 则

$$\bar{a} = [a] = a + n\mathbb{Z}.$$

证明 若 $b \in \bar{a}$, 则 $a \equiv b \pmod{n}$. 从而 $a + n\mathbb{Z} = b + n\mathbb{Z}$. 于是 $b = b + 0 \in b + n\mathbb{Z} = a + n\mathbb{Z}$. 故 $\bar{a} \subset a + n\mathbb{Z}$.

若 $b \in a + n\mathbb{Z}$, 则存在 $m \in \mathbb{Z}$, 使得 $b = a + nm$. 从而 $a - b = nm \in n\mathbb{Z}$. 故 $a \equiv b \pmod{n}$. 因此 $b \in \bar{a}$. 故 $a + n\mathbb{Z} \subset \bar{a}$.

综上, $\bar{a} = a + n\mathbb{Z}$. \square

定义 1.47 (模 n 的同余类)

令 $n \in \mathbb{N}_1$, 则 \mathbb{Z}_n 定义为

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}.$$

\mathbb{Z}_n 中的每个元素, 被称为一个模 n 的同余类.

 **笔记** 不难发现, $0, \dots, n-1$ 分别代表了 n 个同余类. 并且由命题 1.51 及商群的定义可知 \mathbb{Z}_n 是一个商群.

命题 1.55

$(\mathbb{Z}_n, +)$ 是一个 Abel 群.

证明 设 $a + n\mathbb{Z}, b + n\mathbb{Z} \in \mathbb{Z}_n$, 由命题 1.51 可知 $n\mathbb{Z} \triangleleft \mathbb{Z}$. 从而


$$\begin{aligned} a + n\mathbb{Z} + b + n\mathbb{Z} &= a + b + n\mathbb{Z} + n\mathbb{Z} \\ &= b + a + n\mathbb{Z} + n\mathbb{Z} \\ &= b + n\mathbb{Z} + a + n\mathbb{Z}. \end{aligned}$$

故 $(\mathbb{Z}_n, +)$ 是一个 Abel 群. \square

命题 1.56

$$\mathbb{Z}_n = \{k + n\mathbb{Z} : 0 \leq k \leq n-1\}$$

其中枚举法 (上述集合) 中的这些陪集是两两不同的.

 **笔记** 这个命题和命题 1.54 表明:

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, n-1 + n\mathbb{Z}\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

证明 首先证明这里列完了所有的陪集. 令 $m \in \mathbb{Z}$, 根据带余除法, 我们可以找到 $q \in \mathbb{Z}$, 以及 $0 \leq r \leq n-1$, 使得

$$m = qn + r.$$

由于

$$qn \in n\mathbb{Z},$$

因此 $m + n\mathbb{Z} = r + n\mathbb{Z} \in \{k + n\mathbb{Z} : 0 \leq k \leq n-1\}$. 这就证明了最多只有这 n 个同余类.

接下来证明这 n 个同余类是互异的. 假如 $k + n\mathbb{Z} = k' + n\mathbb{Z}$, 其中 $0 \leq k, k' \leq n-1$, 则 $k - k' \in n\mathbb{Z}$. 但是 $-(n-1) \leq k - k' \leq (n-1)$. 而在这个范围内唯一 n 的倍数就是 0, 于是 $k - k' = 0$, 或 $k = k'$. 这就证明了这 n 个同余类是互异的.


综上所述,

$$\mathbb{Z}_n = \{k + n\mathbb{Z} : 0 \leq k \leq n-1\}.$$

□

命题 1.57

令 $n \in \mathbb{N}_1$, 则 \mathbb{Z}_n 是个 n 阶循环群.

 **笔记** 由命题 1.31 可知, 给定 n , 所有 n 阶循环群都是同构的. 因此我们只要研究了 \mathbb{Z}_n , 就研究了所有的有限循环群.

证明 我们只须证明 \mathbb{Z}_n 是一个循环群即可, 也即 $\mathbb{Z}_n = \langle 1 + n\mathbb{Z} \rangle$. 任取 $A \in \mathbb{Z}_n$, 则由命题 1.56 可知, $A = k + n\mathbb{Z}$, 其中 $0 \leq k \leq n-1$. 又由命题 1.51 可知 $(n\mathbb{Z}, +) \triangleleft (\mathbb{Z}, +)$. 从而

$$\underbrace{(1 + n\mathbb{Z}) + \cdots + (1 + n\mathbb{Z})}_{k \text{ 个}} = k + n\mathbb{Z} = A.$$

(注意 0 个 $1 + n\mathbb{Z}$ 相加规定为 $0 + n\mathbb{Z} = n\mathbb{Z}$). 因此 $\mathbb{Z}_n = \langle 1 + n\mathbb{Z} \rangle$. 而由命题 1.56 可知, 这个群又是 n 阶的, 因此是 n 阶循环群. □

定义 1.48

定义乘法 $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n, (a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) \mapsto ab + n\mathbb{Z}$. 也即 $\overline{a} \cdot \overline{b} \mapsto \overline{ab}$.

♣

证明 设 $\overline{a} = \overline{a'} \in \mathbb{Z}_n, \overline{b} = \overline{b'} \in \mathbb{Z}_n$, 则

$$a + n\mathbb{Z} = a' + n\mathbb{Z}, \quad b + n\mathbb{Z} = b' + n\mathbb{Z}.$$

从而 $(a - a'), (b - b') \in n\mathbb{Z}$. 于是存在 $k, l \in \mathbb{Z}$, 使得

$$a' - a = kn, \quad b' - b = ln.$$

因此

$$a'b' - ab = (a + kn)(b + ln) - ab = aln + bkn + kln^2 = n(al + bk + ln^2) \in n\mathbb{Z}.$$

故 $a'b' + n\mathbb{Z} = ab + n\mathbb{Z}$, 即 $\overline{a'b'} = \overline{ab}$. 故上述定义的乘法是良定义的. □

命题 1.58

(\mathbb{Z}_n, \cdot) 是个交换幺半群.

♣

证明 我们先证明乘法是良定义的. 假设 $a' + n\mathbb{Z} = a + n\mathbb{Z}, b' + n\mathbb{Z} = b + n\mathbb{Z}$. 故 $a' = a + nk, b' = b + nl$, 其中 $k, l \in \mathbb{Z}$. 我们只须证明 $a'b' - ab \in n\mathbb{Z}$. 而这是因为

$$a'b' - ab = (a + nk)(b + nl) - ab = anl + bnk + n^2kl = n(al + bk + nkl) \in n\mathbb{Z}.$$

单位元显然是 $1 + n\mathbb{Z}$. 这是因为 $(a + n\mathbb{Z})(1 + n\mathbb{Z}) = a + n\mathbb{Z}$.

结合律也是显然的, 因为 (\mathbb{Z}, \cdot) 是幺半群, 所以设 $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, 都有

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{abc} = abc + n\mathbb{Z} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot (\overline{b} \cdot \overline{c}).$$

交换律, 设 $\overline{a}, \overline{b} \in \mathbb{Z}_n$, 则 $\overline{a} \cdot \overline{b} = \overline{ab} = ab + n\mathbb{Z} = ba + n\mathbb{Z} = \overline{ba}$.

这样, 我们就证明了 (\mathbb{Z}_n, \cdot) 是个幺半群. □

定义 1.49

令 $n \in \mathbb{N}_2$, 则 \mathbb{Z}_n^\times , 定义为由 (\mathbb{Z}_n, \cdot) 中所有可逆元素构成的群. 即

$$\mathbb{Z}_n^\times = \{k + n\mathbb{Z} : 0 \leq k \leq n-1, \exists l \in \mathbb{Z}, kl \equiv 1 \pmod{n}\}$$

也即

$$\mathbb{Z}_n^\times = \{\bar{k} : 0 \leq k \leq n-1, \exists \bar{l} \in \mathbb{Z}_n, \bar{k} \cdot \bar{l} \equiv \bar{1} \pmod{n}\}.$$

♣

注 由引理 1.1 可知上述定义的 \mathbb{Z}_n^\times 确实是一个群. 故上述定义是良定义的.

引理 1.10 (Bézout 定理)

若 $a, b, c \in \mathbb{N}_1$, 则 $ax + by = c$ 有整数解 x, y 当且仅当 $\gcd(a, b) \mid c$.

特别地, 对任意 $a, b \in \mathbb{N}_1$, 我们可以找到 $x, y \in \mathbb{Z}$, 使得 $\gcd(a, b) = ax + by$.

♡

证明

□

命题 1.59

设 $n \in \mathbb{N}_2$, 则

$$\mathbb{Z}_n^\times = \{k + n\mathbb{Z} : 1 \leq k \leq n-1, \gcd(k, n) = 1\} = \{\bar{k} : 1 \leq k \leq n-1, \gcd(k, n) = 1\}.$$

因此

$$|\mathbb{Z}_n^\times| = \phi(n).$$

特别地, 若 p 是一个素数, 则

$$\mathbb{Z}_p^\times = \{1 + p\mathbb{Z}, 2 + p\mathbb{Z}, \dots, (p-1) + p\mathbb{Z}\} = \{\bar{k} : 1 \leq k \leq p-1\}.$$

因此

$$|\mathbb{Z}_p^\times| = p-1.$$

♠

证明 我们只须证明, 若 $0 \leq k \leq n-1$, 则

$$(\exists l \in \mathbb{Z}, kl \equiv 1 \pmod{n}) \iff \gcd(k, n) = 1.$$

分两类情况. 若 $k = 0$, 则显然左边是错的, 而右边甚至是没有定义的, 当然也是错的. 即便你考虑 k 是 n 的倍数, 那么 $\gcd(k, n) = n$, 也是错的. 若 $1 \leq k \leq n-1$, 则

$$\exists l \in \mathbb{Z}, kl \equiv 1 \pmod{n}.$$

$$\iff \exists l \in \mathbb{Z}, \exists m \in \mathbb{Z}, kl + mn = 1.$$

$$\iff \gcd(k, n) = 1.$$

其中第一个充要条件是因为同余的定义, 第二个充要条件是因为引理 1.10. 这样我们就证明了 \mathbb{Z}_n^\times 是由那些 n 互素的数所在的陪集所构成的. 特别地, 这样的陪集的数量就是由欧拉 ϕ 函数给出的, 即

$$\phi(n) = |\{1 \leq k \leq n-1 : \gcd(k, n) = 1\}|.$$

接下来, 若 p 是一个素数, 则

$$\gcd(k, p) = 1 \iff p \nmid k.$$

当然, 从 1 到 $p-1$ 的这些数, 都和 p 互素. 因此

$$\mathbb{Z}_p^\times = \{1 + p\mathbb{Z}, 2 + p\mathbb{Z}, \dots, (p-1) + p\mathbb{Z}\}.$$

故

$$|\mathbb{Z}_p^\times| = p-1.$$

这就证明了这个命题.

□

引理 1.11

令 (G, \cdot) 是个有限群, 则对任意 $a \in G, a^{|G|} = e$.



证明 令 $\langle a \rangle$ 是由 a 生成的循环子群. 则由 **Lagrange 定理** 可知,

$$|\langle a \rangle| \mid |G|$$

而由 **命题 1.30** 我们知道

$$|a| = |\langle a \rangle|$$

因此,

$$a^{|G|} = (a^{|a|})^{|G|/|a|} = e^{|G|/|a|} = e$$

这就证明了这个引理. □

定理 1.7 (Fermat 小定理)

令 p 是一个素数, 而 $p \nmid a$, 则

$$a^{p-1} \equiv 1 \pmod{p}$$

同时左乘 a , 也可以得到

$$a^p \equiv a \pmod{p}$$



笔记 不妨设 $1 \leq a \leq p-1$ 的原因:

假设结论对 $1 \leq a \leq p-1$ 已经成立, 则当 $a \in \mathbb{Z}$ 时, 由带余除法可知, 存在 $m, r \in \mathbb{Z}$ 且 $1 \leq r \leq p-1$, 使得

$$a = mp + r.$$

于是 $1 \leq r = a - mp \leq p-1$ 且 $p \nmid a$. 从而由假设可知

$$(a - mp)^{p-1} = r^{p-1} \equiv 1 \pmod{p}.$$

即

$$(a - mp)^{p-1} - 1 \in p\mathbb{Z}.$$

因此存在 $s \in \mathbb{Z}$, 使得

$$(a - mp)^{p-1} - 1 = ps \iff a^{p-1} + Q(p) - 1 = ps.$$

其中 $Q(p) = (a - mp)^{p-1} - a^{p-1}$. 注意到 $Q(p)$ 的每一项 p 的次数都至少为 1, 故 $p \mid Q(p)$. 进而

$$a^{p-1} - 1 = ps - Q(p) \in p\mathbb{Z}.$$

因此 $a^{p-1} \equiv 1 \pmod{p}$.

证明 根据 (\mathbb{Z}_p, \cdot) 中乘法的良定义性和 $p \nmid a$, 我们不失一般性, 假设

$$1 \leq a \leq p-1.$$

从而 $\bar{a} \in \mathbb{Z}_p^\times$ (实际上, 由 $p \nmid a$ 就直接可以得到 $\bar{a} \in \mathbb{Z}_p^\times$). 根据 **引理 1.11**, 可得

$$\overline{a^{p-1}} = \bar{a}^{p-1} = \bar{a}^{|\mathbb{Z}_p^\times|} = \bar{1}.$$

此即

$$a^{p-1} \equiv 1 \pmod{p}.$$

同时左乘后的结论是显然的. 综上所述, 我们用群论证明了费马小定理. □

定理 1.8 (Euler 定理)

令 $n \in \mathbb{N}_2$, 而 $\gcd(a, n) = 1$, 则

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$



注 注意, 当 $n = p$ 的时候, 欧拉定理就退化为费马小定理.

笔记 这个定理叫欧拉定理, 这也在一定程度上解释了为什么 ϕ 函数被称为欧拉函数. 欧拉定理显然是费马小定理的推广 (当 p 为素数时, 就有 $\phi(p) = p - 1$). 通过群论来证明的思路是一致的.

注 这里不妨设 $1 \leq a \leq n - 1, \gcd(a, n) = 1$ 的原因与费马小定理的证明类似.

证明 首先, 根据 (\mathbb{Z}_n, \cdot) 中乘法的良定义性和 $\gcd(a, n) = 1$, 我们不失一般性, 假设

$$1 \leq a \leq n - 1, \gcd(a, n) = 1.$$

从而 $\bar{a} \in \mathbb{Z}_n^\times$ (实际上, 由 $n \nmid a$ 就直接可以得到 $\bar{a} \in \mathbb{Z}_n^\times$). 利用引理 1.11, 可得

$$\overline{a^{\phi(n)}} = \bar{a}^{\phi(n)} = \bar{a}^{|\mathbb{Z}_n^\times|} = \bar{1}.$$

此即

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

这就证明了欧拉定理. □

定理 1.9 (Wilson 定理)

若 p 是一个奇素数 (即除了 2 以外的素数), 则

$$(p - 1)! \equiv -1 \pmod{p}.$$

其中 $!$ 表示阶乘.



证明 我们令 p 是一个奇素数, 故 \mathbb{Z}_p^\times 包含 $p - 1$ (偶数) 个元素. 我们希望将逆元进行配对. 注意到每一个元素都对应了一个逆元. 而元素和逆元相等当且仅当这个元素的平方是单位元, 即

$$\bar{a} = \bar{a}^{-1} \iff \bar{a}^2 = \bar{1} \iff a^2 \equiv 1 \pmod{p}.$$

而这就是

$$p \mid (a^2 - 1) = (a - 1)(a + 1).$$

所以要么 $p \mid (a - 1)$, 要么 $p \mid (a + 1)$. 即 $a \equiv \pm 1 \pmod{p}$. 这就等价于 $a \equiv 1$ 或 $a \equiv p - 1 \pmod{p}$. 这就说明了所有逆元是自己的元素恰好是 $\bar{1}$ 和 $\overline{p-1}$ 这两个. 我们去掉这两个元素, 剩下 $p - 3$ (偶数) 个元素一定是两两配对的. 因此剩下所有元素的乘积是 1. 因此

$$\overline{(p-1)!} = \bar{1} \cdot \overline{(p-1)} \cdot \underbrace{\bar{1} \cdots \bar{1}}_{\frac{p-3}{2} \text{ 个}} = \overline{p-1} = \overline{-1}.$$

即 $(p - 1)! \equiv -1 \pmod{p}$. 这就证明了威尔逊定理. □

第二章 环论——Ring Theorey I

2.1 环

定义 2.1 (环)


我们称 $(R, +, \cdot)$ 是一个**环**, 当 $(R, +)$ 是个阿贝尔群, (R, \cdot) 是个么半群, 且乘法对加法有左右分配律, 即

$$\forall a, b, c \in R, a(b+c) = ab+ac,$$

$$\forall a, b, c \in R, (a+b)c = ac+bc.$$



注 我们把环 $(R, +, \cdot)$ 中的加法单位元记作 0 , 乘法单位元记作 1 . 对任意的 $a \in R$, 我们将 a 的加法逆元记作 $-a$, 乘法逆元记作 a^{-1} .

 **笔记** 最常见的环是整数环 $(\mathbb{Z}, +, \cdot)$.

定义 2.2 (交换环)

设 $(R, +, \cdot)$ 是一个环, 我们称 R 是一个**交换环**, 当 R 对乘法有交换律, 即

$$\forall a, b \in R, ab = ba.$$

也即 (R, \cdot) 是一个交换么半群.



例题 2.1

1. $(\mathbb{Z}_n, +, \cdot)$ 是一个交换环.
2. $(M(n, \mathbb{R}), +, \cdot)$ 是一个环 (不是交换环).

证明

1. 由**命题 1.55**可知 $(\mathbb{Z}_n, +)$ 是一个 Abel 群. 又由**命题 1.58**可知 (\mathbb{Z}_n, \cdot) 是一个交换么群. 因此我们只须证明分配律即可. 对 $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, 都有

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a}(\overline{b+c}) = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c}.$$

$$(\bar{a} + \bar{b})\bar{c} = (\overline{a+b})\bar{c} = \overline{(a+b)c} = \overline{ac+bc} = \overline{ac} + \overline{bc} = \bar{a}\bar{c} + \bar{b}\bar{c}.$$

综上, $(\mathbb{Z}_n, +, \cdot)$ 是一个交换环.

2. $(M(n, \mathbb{R}), +, \cdot)$ 是一个环的证明是显然的.

□

命题 2.1

设 $(R, +, \cdot)$ 是一个环, 而 $a, b, c \in R$, 则

- (1) $a0 = 0a = 0$,
- (2) $a(-b) = (-a)b = -(ab)$,
- (3) $(-a)(-b) = ab$.



证明

- (1) 首先, 利用分配律,

$$a0 = a(0+0) = a0 + a0.$$

因此 $a0 = 0$. 根据对称性, $0a = a$.

- (2) 根据对称性, 我们只须证明 $a(-b) = -(ab)$. 而这是因为

$$a(-b) + ab = a(-b+b) = a0 = 0.$$

(3) 利用两次 (2) 的结论和命题 1.10, 我们就得到

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab.$$


□

定义 2.3 (零环)

有一个重要的环是零环, 它是最平凡的环, 即 $(0, +, \cdot)$, 也记作 $\{0\}$. 它只有一个元素, 既是加法单位元也是乘法单位元, 定义为

$$\begin{aligned} 00 &= 0, \\ 0 + 0 &= 0. \end{aligned}$$

♣

 **笔记** 很容易检验这是一个环.

命题 2.2 (零环的充要条件)

设 $(R, +, \cdot)$ 是一个环, 则 $R = \{0\}$ 当且仅当 $0 = 1$.

♠

证明 必要性 (\Rightarrow) 是显然的.

我们来证明充分性 (\Leftarrow). 假设 $0 = 1$, 我们只须证明对所有 $a \in R$, 都有 $a = 0$. 由命题 2.1 可知

$$a = a1 = a0 = 0$$

这就证明了这个命题.

□

定义 2.4 (单位及所有单位构成的群)

设 $(R, +, \cdot)$ 是一个环, 则 (R^\times, \cdot) 是由 R 中所有乘法可逆元素构成的群. R 中的乘法可逆元素又被称为 R 中的**单位**.

♣

注 由引理 1.1 可知, R 中所有乘法可逆元素构成了一个群. 故上述 (R^\times, \cdot) 的定义是良定义的.

命题 2.3

设 $(R, +, \cdot)$ 是一个环, 若 $R \neq \{0\}$, 则 0 一定不是单位, 1 一定是单位.

♠

证明 因为 $R \neq \{0\}$, 所以由命题 2.2 可知 $0 \neq 1$. 于是对 $\forall a \in R$, 由命题 2.1 可知 $a \cdot 0 = 0 \neq 1$. 故 0 一定没有逆元, 即 0 不是单位.

由于 $1 \cdot 1 = 1$, 因此 1 的逆元就是其自身, 故 1 一定是单位.

□

定义 2.5 (除环)

设 $(R, +, \cdot)$ 是一个环, 我们称 $(R, +, \cdot)$ 是一个**除环**, 若

$$R \setminus \{0\} = R^\times$$

也即, 所有非零元素都是单位.

♣

命题 2.4 (除环的充要条件)

$(R, +, \cdot)$ 是一个除环, 当且仅当同时满足下面三个条件

- (i) $(R, +)$ 是一个 Abel 群,
- (ii) $(R \setminus \{0\}, \cdot)$ 是一个群,
- (iii) 乘法对加法有左右分配律.

♠

证明 根据定义, 这是显然的.

□

定义 2.6 (交换的除环)

设 $(R, +, \cdot)$ 是一个除环, 我们称 $(R, +, \cdot)$ 是一个**交换的除环**, 当 R 对乘法有交换律, 即

$$\forall a, b \in R, ab = ba.$$

即 (R, \cdot) 是一个交换么半群. 也即 $(R \setminus \{0\}, \cdot) = (R^\times, \cdot)$ 是一个 Abel 群.

定义 2.7 (域)

设 $(R, +, \cdot)$ 是一个环, 我们称 $(R, +, \cdot)$ 是一个**域**, 若它是一个交换的除环.

命题 2.5 (域的充要条件)

$(R, +, \cdot)$ 是一个域, 当且仅当同时满足下面三个条件

- (i) $(R, +)$ 是一个 Abel 群,
- (ii) $(R \setminus \{0\}, \cdot)$ 是一个 Abel 群,
- (iii) 乘法对加法有左右分配律.

证明 根据定义, 这是显然的. □

命题 2.6


设 $(R, +, \cdot)$ 是一个域, 则 $0 \neq 1$.

证明 反证, 假设 $0 = 1$, 则对 $\forall a \in R$, 由命题 2.1 可知 $a = 1 \cdot a = 0 \cdot a = 0$. 从而 $R = \{0\}$. 于是 $R \setminus \{0\} = \emptyset$. 而空集一定不是 Abel 群, 故 $R \setminus \{0\} = \emptyset$ 一定不是 Abel 群, 而由命题 2.5 可知 $R \setminus \{0\} = \emptyset$ 是 Abel 群, 矛盾! □

定义 2.8 (子环)

设 $(R, +, \cdot)$ 是一个环, 而 $S \subset R$. 我们称 S 是 R 的**子环**, 记作 $S < R$, 若同时满足下面三个条件


- (i) $0, 1 \in S$,
- (ii) $\forall a, b \in S, a + b, ab \in S$,
- (iii) $\forall a \in S, -a \in S$.

 **笔记** 事实上, 这就是说 $(S, +)$ 是 $(R, +)$ 的子群, (S, \cdot) 是 (R, \cdot) 的子么半群. 又因为 $(R, +)$ 是 Abel 群, 所以 $(S, +)$ 一定是 $(R, +)$ 的正规子群.

引理 2.1 (子环的充要条件)

设 $(R, +, \cdot)$ 是一个环, 而 $S \subset R$, 则 $S < R$ 当且仅当

$$\begin{aligned} 1 &\in S, \\ \forall a, b \in S, a - b, ab &\in S. \end{aligned}$$

 **笔记** 例如 $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$.

证明 假如满足了这两个条件, 那么 $0 = 1 - 1 \in S$. 而 $-a = 0 - a \in S, a + b = a - (-b) \in S$. 这就证明了这是子环. 另一个方向是显然的. 假如 S 是子环, 那么 $a - b = a + (-b) \in S$. □

命题 2.7 (子环仍是环)

设 $(R, +, \cdot)$ 是一个环, S 是其子环, 则 $(S, +, \cdot)$ 也是环.

证明 由子环的定义可知 S 对加法和乘法满足封闭性, 从而加法和乘法是 S 上代数运算. 于是再结合 $0, 1 \in S$ 且 $S \subset R$, 将 $(R, +, \cdot)$ 的性质照搬过来即可. □

定义 2.9 (由子集生成的子环)

设 $(R, +, \cdot)$ 是一个环, 而 $A \subset R$, 则 A 生成的子环, 记作 $\langle A \rangle$, 定义为所有包含了 A 的子环的交集, 即

$$\langle A \rangle = \bigcap \{S \subset R : S \supset A, S < R\}.$$

命题 2.8 (由子集生成的子环仍是子环)

设 $(R, +, \cdot)$ 是一个环, 而 $A \subset R$, 则 $\langle A \rangle < R$.

证明 首先这个集族是非空的, 因为 R 本身就是一个包含了 A 的子环.

接下来, 我们利用上面的引理. 令 S 是一个包含了 A 的子环. 因为 1 在每一个这样的 S 中, 所以 $1 \in \langle A \rangle$.

令 $a, b \in \langle A \rangle$, 则 $a - b, ab$ 在每一个这样的 S 中, 因为每一个 S 都是子环. 因此 $a - b, ab \in \langle A \rangle$.

综上所述, $\langle A \rangle < R$. □

定义 2.10 (环的直积)

设 $((R_i, +_i, \cdot_i)_{i \in I})$ 是一族环. 我们定义这一族环的直积, 为 $(\prod_{i \in I} R_i, +, \cdot)$. 对于 $(x_i)_{i \in I}, (y_i)_{i \in I} \in \prod_{i \in I} R_i$, 我们

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i +_i y_i)_{i \in I} \quad (2.1)$$

$$(x_i)_{i \in I} \cdot (y_i)_{i \in I} = (x_i \cdot_i y_i)_{i \in I} \quad (2.2)$$

命题 2.9 (环的直积仍是环)

设 $((R_i, +_i, \cdot_i)_{i \in I})$ 是一族环, 则它们的直积 $(\prod_{i \in I} R_i, +, \cdot)$ 还是一个环.

证明 由命题 1.5 和命题 1.23 可知, 么半群和 Abel 群对直积是保持的, 从而我们立刻知道 $\prod_{i \in I} R_i$ 对加法构成 Abel 群, 对乘法构成么半群. 因此只须检验乘法对加法的左右分配律. 根据对称性, 我们只证明左分配律.

由于 $((R_i, +_i, \cdot_i)_{i \in I})$ 是一族环, 因此 $((R_i, +_i, \cdot_i)_{i \in I})$ 的乘法对加法有左分配律. 故令 $(x_i)_{i \in I}, (y_i)_{i \in I}, (z_i)_{i \in I} \in \prod_{i \in I} R_i$, 则

$$\begin{aligned} (x_i)_{i \in I} \cdot ((y_i)_{i \in I} + (z_i)_{i \in I}) &= (x_i \cdot_i (y_i +_i z_i))_{i \in I} = (x_i \cdot_i y_i +_i x_i \cdot_i z_i)_{i \in I} \\ &= (x_i \cdot_i y_i)_{i \in I} + (x_i \cdot_i z_i)_{i \in I} = (x_i)_{i \in I} \cdot (y_i)_{i \in I} + (x_i)_{i \in I} \cdot (z_i)_{i \in I}. \end{aligned}$$

因此, $(\prod_{i \in I} R_i, +, \cdot)$ 是一个环. 这就证明了这个命题. □

2.2 环同态

定义 2.11 (环同态)

设 $(R, +, \cdot), (R', +', *)$ 都是环, $f: (R, +, \cdot) \rightarrow (R', +', *)$ 是一个映射, 我们说 f 是个环同态, 若

- (i) $f(1) = 1'$,
- (ii) $f(a + b) = f(a) +' f(b), \forall a, b \in R$.
- (iii) $f(ab) = f(a) * f(b), \forall a, b \in R$.

注 未来, 在不引起歧义的情况下, 我们会忽略两个环中加法与乘法的区别, 都记作 $+$ 和 \cdot , 称环同态是

$$f: (R, +, \cdot) \rightarrow (R', +, \cdot).$$

命题 2.10

设 $(R, +, \cdot), (R', +', *)$ 都是环, $f: (R, +, \cdot) \rightarrow (R', +', *)$ 是一个映射, 则 f 是环同态等价于 f 既是加法的群同态, 又是乘法的幺半群同态. 进而, f 对加法保持逆元和单位元.

证明 根据环同态的定义可直接得到, f 是环同态等价于 f 既是加法的群同态, 又是乘法的幺半群同态.. 再由命题 1.17 可知, f 对加法保持逆元和单位元. \square

定义 2.12 (环同态的核与像)

设 $f: (R, +, \cdot) \rightarrow (R', +', *)$ 是一个环同态, 则我们定义 f 的**核与像**, 记作 $\ker(f)$ 与 $\text{im}(f)$, 分别为

$$\ker(f) = \{x \in R : f(x) = 0'\} \subset R,$$

$$\text{im}(f) = \{y \in R' : \exists x \in R, y = f(x)\} = \{f(x) : x \in R\} \subset R'.$$

注 注意核在大多数情况下不会是一个子环.

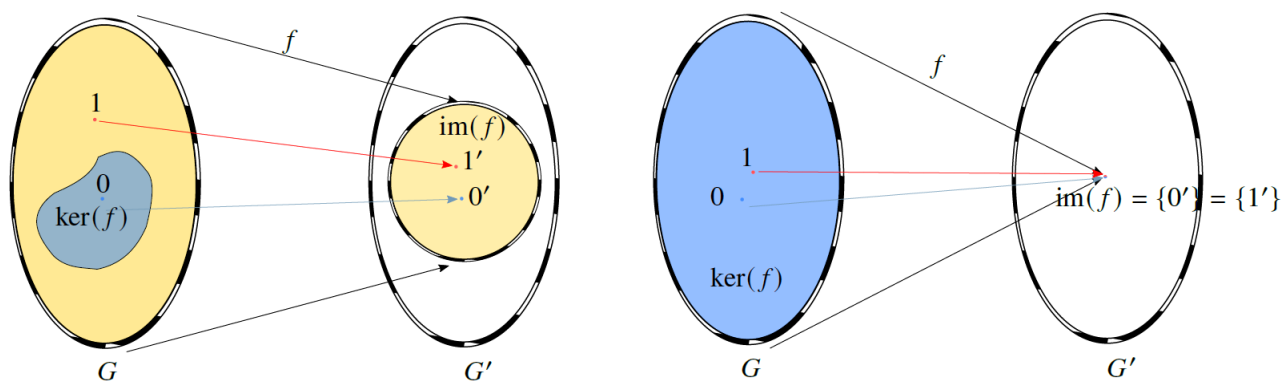


图 2.1: 环同态的核与像示意图

定义 2.13 (满同态与单同态)

设 $f: (R, +, \cdot) \rightarrow (R', +', *)$ 是一个环同态, 我们称 f 是一个**满同态**当 f 是满射, 称 f 是一个**单同态**当 f 是单射.

命题 2.11

设 $f: (R, +, \cdot) \rightarrow (R', +', *)$ 是一个环同态, 则

1. f 是一个单同态当且仅当 $\ker(f) = \{0\}$. 也就是说, 一个环同态是单的当且仅当核是平凡的.
2. f 是一个满同态当且仅当 $\text{im}(f) = R'$. 也就是说, 一个环同态是满的当且仅当值域等于陪域.

证明 证明与命题 2.11 类似. \square

定义 2.14 (理想)

设 $(R, +, \cdot)$ 是一个环, 而 $I \subset R$. 我们定义, 称 I 是 R 的**左理想**, 若

$$(I, +) < (R, +),$$

$$\forall r \in R, \forall a \in I, ra \in I.$$

即 $RI \subset I$, 也即 $RI = I$. 也等价于 $SI = I, \forall S \subset R$.

类似地, 我们称 I 是 R 的**右理想**, 若

$$(I, +) < (R, +),$$

$$\forall a \in I, \forall r \in R, ar \in I.$$

即 $IR \subset I$, 也即 $IR = I$. 也等价于 $IS = I, \forall S \subset R$.

如果 I 既是左理想又是右理想, 我们就称 I 是 R 的一个理想, 记作 $I \triangleleft R$.



注 因为 $(R, +)$ 是 Abel 群, 所以 $(I, +)(R, +)$ 的子群等价于 $(I, +)$ 是 $(R, +)$ 的正规子群.

笔记 理想的第二条性质表明: 理想在乘法下“吸收”了整个环到理想上, 也就是说

$$RI \subset I, IR \subset I.$$

其中子集的乘法, 定义为所有元素乘积的集合. 而显然有 $I \subset RI, IR$. 故

$$\forall r \in R, \forall a \in I, ra \in I \Leftrightarrow RI \subset I \Leftrightarrow RI = I,$$

$$\forall r \in R, \forall a \in I, ar \in I \Leftrightarrow IR \subset I \Leftrightarrow IR = I.$$

引理 2.2

(1) 设 $(R, +, \cdot)$ 是一个环, $H < R$, 则 $HH = H$.

(2) 设 $(R, +, \cdot)$ 是一个环, $H \triangleleft R$, 则 $HH = H$.



证明

(1) 一方面, 根据 $H < R$ 可知, H 是 R 的一个乘法子么半群. 于是由引理 1.5 可知, 对 $\forall h_1, h_2 \in H$, 都有 $h_1 h_2 \in H$. 故 $HH \subset H$.

另一方面, 设 $h \in H, e$ 是 R 的乘法单位元. 则 $h = he \in HH$. 故 $H \subset HH$.

综上, $HH = H$.

(2) 一方面, 对 $\forall h_1, h_2 \in H$, 根据 $H \triangleleft R$ 的定义及 $h_1 \in R$ 可知, $h_1 h_2 \in H$. 故 $HH \subset H$.

另一方面, 设 $h \in H, e$ 是 R 的乘法单位元. 则 $h = he \in HH$. 故 $H \subset HH$.

综上, $HH = H$.



引理 2.3 (理想是整个环的充要条件)

(1) 设 $(R, +, \cdot)$ 是一个环, 而 $I \triangleleft R$. 则 $I < R$ 当且仅当 $I = R$.

(2) 设 $(R, +, \cdot)$ 是一个环, 1 是其乘法单位元, $I \triangleleft R$, 则 $1 \in I$ 当且仅当 $I = R$.

(3) 设 $(R, +, \cdot)$ 是一个环, 1 是其乘法单位元, $I \triangleleft R$, 则 $R^\times \cap I \neq \emptyset$ 当且仅当 $I = R$.



证明

(1) 充分性是显然的, 因为一个环当然是自己的子环.

我们来证明必要性. 设 $I < R$, 则特别地, $1 \in I$. 可是 $I \triangleleft R$, 因此对任何 $r \in R$, 我们有

$$r = r \cdot 1 \in I.$$

这就证明了 $I = R$.

综上所述, 一个理想是子环当且仅当它是整个环.

(2) 充分性是显然的. 下证必要性.

由 $I \triangleleft R$ 可知 $I \subset R$. 因为 $1 \in I$, 且 $I \triangleleft R$, 所以 $\forall r \in R$, 都有 $r = r \cdot 1 \in I$. 因此 $R \subset I$.

综上, 我们就有 $I = R$.

(3) 充分性是显然的. 下证必要性.

设 $a \in R^\times \cap I$, 则 a 是 R 中的一个单位. 从而存在 $b \in R$, 使得 $ab = 1$. 又由 $I \triangleleft R$ 可知, $1 = ab \in I$. 于是由 (2) 可知 $I = R$.



命题 2.12 (理想的任意交还是理想)

设 $(R, +, \cdot)$ 是一个环, $(N_i)_{i \in I}$ 是一族 R 的理想, 则它们的交集仍然是 R 的理想, 即

$$\bigcap_{i \in I} N_i \triangleleft R.$$

证明 一方面, 由条件可知, $((N_i)_{i \in I}, +)$ 是一族 $(R, +)$ 的子群. 从而由命题 1.15 可知 $(\bigcap_{i \in I} N_i, +)$ 仍是 $(R, +)$ 的子群.

另一方面, 对 $\forall r \in R, \forall n \in \bigcap_{i \in I} N_i$, 都有 $n \in N_i, \forall i \in I$. 又因为对 $\forall i \in I, N_i$ 都是 R 的理想, 所以 $rn \in N_i, \forall i \in I$. 从而 $rn \in \bigcap_{i \in I} N_i$. 同理可证 $nr \in \bigcap_{i \in I} N_i$.

综上, $\bigcap_{i \in I} N_i$ 仍然是 R 的理想. □

命题 2.13

设 $(R, +, \cdot)$ 是一个交换环, 则 I 是一个左理想当且仅当 I 是一个右理想, 又当且仅当 I 是一个理想.

证明 根据交换环对乘法的交换律, 这是显然的. □

命题 2.14

设 $n \in \mathbb{N}_1$, 则 $n\mathbb{Z}$ 是 \mathbb{Z} 的理想, 即

$$n\mathbb{Z} \triangleleft \mathbb{Z}.$$

证明 首先, 由命题 1.51 我们知道 $(n\mathbb{Z}, +)$ 是 $(\mathbb{Z}, +)$ 的 (加法) 正规子群.

其次, 注意到 \mathbb{Z} 是一个交换环, 故根据命题 2.13 可知, 我们只须证明 $n\mathbb{Z}$ 是 \mathbb{Z} 的左理想, 也即 $\mathbb{Z} \cdot n\mathbb{Z} \subset n\mathbb{Z}$. 要证明 $\mathbb{Z} \cdot n\mathbb{Z} \subset n\mathbb{Z}$, 我们只须令 $m \in \mathbb{Z}, nk \in n\mathbb{Z} (k \in \mathbb{Z})$, 只要证明 $mnk \in n\mathbb{Z}$ 即可. 而这是因为

$$mnk = n(mk) \in n\mathbb{Z}.$$

综上所述, 这就证明了 $n\mathbb{Z}$ 是 \mathbb{Z} 的理想. □

引理 2.4

设 $n \in \mathbb{N}_1$, 我们要定义映射 $f: (\mathbb{Z}, +, \cdot) \rightarrow (\mathbb{Z}_n, +, \cdot)$. 对 $m \in \mathbb{Z}$, 我们定义

$$f(m) = m + n\mathbb{Z}.$$

则 f 是一个环同态, 而 $\ker(f) = n\mathbb{Z} \triangleleft R$. ♥

证明 先证明 f 是加法的群同态.

设 $a, b \in \mathbb{Z}$, 由命题 1.51 可知, $(n\mathbb{Z}, +) \triangleleft (\mathbb{Z}, +)$. 从而

$$f(a) + f(b) = a + n\mathbb{Z} + b + n\mathbb{Z} = a + b + n\mathbb{Z} = f(a + b).$$

故 f 是加法的群同态.

下面证明 f 是乘法的幺半群同态.

第一, $f(1) = 1 + n\mathbb{Z}$ 是 \mathbb{Z}_n 的乘法单位元.

第二, 设 $m, m' \in \mathbb{Z}$, 则利用上一章中我们证明过的 \mathbb{Z}_n 对乘法的良定义性, 我们有

$$f(m)f(m') = (m + n\mathbb{Z})(m' + n\mathbb{Z}) = mm' + n\mathbb{Z} = f(mm').$$

故 f 是乘法的幺半群同态.

综上所述, f 是一个从 \mathbb{Z} 到 \mathbb{Z}_n 的环同态.

注意到

$$\ker f = \{m \in \mathbb{Z} : f(m) = n\mathbb{Z} = \bar{0}\} = \{m \in \mathbb{Z} : \bar{m} = m + n\mathbb{Z} = n\mathbb{Z} = \bar{0}\} = \{m \in \mathbb{Z} : m \in n\mathbb{Z}\} = n\mathbb{Z}.$$

因此由命题 2.14 可知 $\ker(f) = n\mathbb{Z} \triangleleft R$. □

命题 2.15 (环同态的核是理想并且像是子环)

设 $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$ 是一个环同态, 则 f 的核是 R 的理想, f 的像是 R' 的子环. 此即,

$$\begin{aligned}\ker(f) &= \{a \in R : f(a) = 0'\} \triangleleft R, \\ \operatorname{im}(f) &= \{b \in R' : \exists a \in R, b = f(a)\} = \{f(a) \in R' : a \in R\} < R'.\end{aligned}$$

证明 我们先证明 $\ker(f) \triangleleft R$. 根据群同态的性质, 由群同构第一定理, 我们知道 $\ker(f)$ 是加法的 (正规) 子群. 为了方便起见, 令 $I = \ker(f)$. 我们只须证明 $RI \subset I$ 以及 $IR \subset I$.

令 $a \in R, b \in I = \ker(f)$, 故 $f(b) = 0'$. 因此, $f(ab) = f(a)f(b) = f(a)0' = 0'$, 从而 $ab \in \ker(f) = I$. 这就证明了 $RI \subset I$. 而另一个包含关系同理可证. 这样, 我们就证明了 $\ker(f) \triangleleft R$.

我们再证明 $\operatorname{im}(f) < R'$. 第一, $1' = f(1) \in \operatorname{im}(f)$.

第二, 令 $a', b' \in \operatorname{im}(f)$, 不妨设 $a' = f(a), b' = f(b)$. 只须证明 $a' - b', a'b' \in \operatorname{im}(f)$. 而由 f 对加法是群同态可知, f 保持加法逆元和加法. 由 f 对乘法是幺半群同态可知, f 保持乘法. 于是就有

$$\begin{aligned}a' - b' &= f(a) - f(b) = f(a - b) \in \operatorname{im}(f), \\ a'b' &= f(a)f(b) = f(ab) \in \operatorname{im}(f).\end{aligned}$$

这就证明了 $\operatorname{im}(f) < R'$.

综上所述, 我们证明了这个命题. □

定义 2.15 (商环)

设 $(R, +, \cdot)$ 是一个环, 而 $I \triangleleft R$. 我们定义 R 对 I 的商环, 定义为 $(R/I, +, \cdot)$, 其中

$$R/I = \{a + I : a \in R\}.$$

而加法和乘法分别对 $a + I, b + I \in R/I (a, b \in R)$, 定义为

$$\begin{aligned}(a + I) + (b + I) &= (a + b) + I, \\ (a + I)(b + I) &= (ab) + I.\end{aligned}$$

证明 我们需要证明上述定义是良定义的, 即证上述的加法和乘法是良定义的, 且商环 $(R, +, \cdot)$ 是一个环.

注意到 $(R, +)$ 是 Abel 群, 又因为 I 是 R 的理想, 所以 $(I, +)$ 是 $(R, +)$ 的子群. 从而由命题 1.43 可知 $(I, +)$ 是 $(R, +)$ 的正规子群. 根据命题 1.39 可知, 正规子群 I 的陪集的加法是良定义的, 即上述加法是良定义的.

我们要证明商环对乘法是良定义的. 令 $a + I = a' + I, b + I = b' + I$, 即 $a - a' \in I, b - b' \in I$. 我们只须证明 $ab + I = a'b' + I$, 即 $ab - a'b' \in I$. 而这是因为

$$ab - a'b' = (ab - a'b) + (a'b - a'b') = (a - a')b + a'(b - b') \in IR + RI \subset I + I = I.$$

其中倒数第二个包含关系是根据理想对乘法的“吸引”性质, 而最后一个等号是根据引理 1.5 及 $(I, +) < (R, +)$. 这样, 我们就证明了商环对乘法是良定义的.

接下来, 要证明商环是个环, 其实只要将 R 上环的结构 (利用良定义性) 照搬过来即可.

利用 I 对加法构成正规子群, 因此利用命题 1.40 可知, R/I 对加法构成群. 我们只须证明 R/I 对乘法构成幺半群, 且乘法对加法有左右分配律.

乘法单位元是 $1 + I$, 因为对任意 $a + I (a \in R)$, 我们有

$$(a + I)(1 + I) = (1 + I)(a + I) = a + I.$$

R/I 对乘法有结合律, 这是因为对任意 $a + I, b + I, c + I (a, b, c \in R)$, 由 $(R, +, \cdot)$ 是一个环可得

$$((a + I)(b + I))(c + I) = (ab + I)(c + I) = (ab)c + I = a(bc) + I = (a + I)((b + I)(c + I)).$$

最后, 我们要证明乘法对加法有左右分配律. 利用对称性, 我们只证明左分配律. 对任意 $a + I, b + I, c + I (a, b, c \in R)$,

由 $(R, +, \cdot)$ 是一个环可得

$$\begin{aligned}(a + I)((b + I) + (c + I)) &= (a + I)((b + c) + I) = a(b + c) + I \\ &= (ab + ac) + I = (a + I)(b + I) + (a + I)(c + I).\end{aligned}$$

综上所述, 我们就证明了 R/I 是个环. 这个环被叫做 R 对 I 的商环. □

定义 2.16 (环同构)

设 $(R, +, \cdot), (R', +, \cdot)$ 都是环, $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$ 是一个映射, 我们称 f 是一个**环同构**, 若 f 既是双射, 又是环同态.

引理 2.5

设 $(R, +, \cdot), (R', +, \cdot)$ 都是环, $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$ 是一个映射, 则 f 是环同构, 当且仅当 f 对加法是群同构, 而对乘法是么半群同构.

证明 必要性是显然的. 下证充分性.

由于 f 对加法是群同构, 而对乘法是么半群同构, 因此 f 是双射, 且 f 既对加法是群同态, 又对乘法是么半群同态. 于是由**命题 2.10**可知 f 是环同态. 又因为 f 是双射, 所以 f 是环同构. □

引理 2.6

设 $(R, +, \cdot), (R', +, \cdot)$ 都是环, $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$ 是个环同构, 则 f^{-1} 是个环同态, 进而也是环同构.

证明 由 f 是个环同构可知, f 既对加法是群同态, 又对乘法是么半群同态. 从而由**命题 1.8**和**命题 1.20**可知, f^{-1} 既对加法是群同态, 又对乘法是么半群同态. 于是由**命题 2.10**可知 f^{-1} 是环同态. 又因为 f^{-1} 是双射, 所以 f^{-1} 是环同构. □

定理 2.1 (环同构第一定理)

设 $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$ 是一个环同态, 则 R 对 $\ker(f)$ 构成的商环, 同构于 $\text{im}(f)$. 此即,

$$R/\ker(f) \cong \text{im}(f).$$

证明 令 $\tilde{f}: R/\ker(f) \rightarrow \text{im}(f)$, 对 $a + \ker(f)$, 定义为

$$\tilde{f}(a + \ker(f)) = f(a).$$

我们根据**群同构第一定理**中对 \tilde{f} 的证明同理可证 \tilde{f} 是良定义的, 且对加法构成群同构. 要证明 \tilde{f} 是环同构, 只须证明它对乘法是么半群同态.

单位元: 由**商环的定义**及**命题 2.15**可知, $R/\ker(f)$ 的乘法单位元是 $1 + \ker f$ 且 $\text{im}(f) < R'$, 从而 $\text{im}(f)$ 的乘法单位元就是 R' 的乘法单位元. 由 \tilde{f} 的定义及 f 是环同态可得 $\tilde{f}(1 + \ker f) = f(1) = 1'$.

保持乘法: 令 $a + \ker(f), b + \ker(f) \in R/\ker(f)$ ($a, b \in R$), 则

$$\tilde{f}((a + \ker(f))(b + \ker(f))) = \tilde{f}(ab + \ker(f)) = f(ab) = f(a)f(b) = \tilde{f}(a + \ker(f))\tilde{f}(b + \ker(f)).$$

综上所述, \tilde{f} 给出了一个从商环 $R/\ker(f)$ 到像 $\text{im}(f)$ 的环同构. 这就证明了这个定理. □

定理 2.2 (环同构第二定理)

设 $(R, +, \cdot)$ 是一个环, 而 $S < R, I \triangleleft R$. 则 $S + I < R, S \cap I \triangleleft S, I \triangleleft S + I$, 且

$$S/(S \cap I) \cong (S + I)/I.$$

证明 我们先证明 $S + I < R$. 对加法而言, 由 $S < R, I \triangleleft R$ 可知 $(S, +) < (R, +), (I, +) < (R, +)$, 又因为 $(R, +)$ 是 Abel 群, 所以 $(S, +), (I, +) \triangleleft (R, +)$. 从而由**引理 1.7**可知 $(S + I, +) < (R, +)$. 因此我们只须证明 $S + I$ 对乘法构成么半群, 即对乘法是封闭的, 且包含单位元. 第一, $1 = 1 + 0 \in S + I$. 第二, 只须证明 $(S + I)(S + I) \subset (S + I)$. 由**引理 2.2**可知

$II = I$, 由引理 1.5 可知 $SS = S, I + I = I$. 根据 $I \triangleleft R$ 可知 $IS, SI = I$. 于是再利用 R 的乘法对加法满足左右分配律可得

$$(S + I)(S + I) = SS + SI + IS + II = S + I + I + I = S + I.$$

我们再证明 $S \cap I \triangleleft S$. 由命题 1.15 可知, $S \cap I$ 对加法构成子群. 我们只须证明 $S \cap I$ 对乘法的“吸收”性, 即 $(S \cap I)S \subset S \cap I$, 及 $S(S \cap I) \subset S \cap I$. 根据对称性, 我们只证明前面这个包含关系. 由 $SS = S, IS = I$ 可得

$$(S \cap I)S \subset SS = S, (S \cap I)S \subset IS = I \Leftrightarrow (S \cap I)S = S \cap IS = S \cap I.$$

根据对称性, $S \cap I \triangleleft S$.

我们接着证明 $I \triangleleft S + I$. 我们已经证明了 $S + I \triangleleft R$, 因此 $S + I$ 对加法构成 Abel 群, 又 $I \subset S + I (0 \in S, I = 0 + I \subset S + I)$, 故 $(I, +) \leq (S + I, +)$. 于是我们只须证明 $I(S + I) \subset I$, 及 $(S + I)I \subset I$. 根据对称性, 我们只证明前面这个包含关系. 由 $I \triangleleft R$ 及 $S + I \triangleleft R$ 可得

$$I(S + I) = IS + II = I + I = I.$$

根据对称性, $I \triangleleft S + I$.

我们最后证明 $S/(S \cap I) \cong (S + I)/I$. 和群同构第二定理的证明一样, 我们定义 $f: S \rightarrow (S + I)/I$, 对 $a \in S$, 定义为

$$f(a) = a + I \in (S + I)/I.$$

先证 f 是良定义的. 设 $a = a' \in S$, 则 $a - a' = 0 \in I$, 从而 $f(a) = a + I = a' + I = f(a')$. 故 f 是良定义的. 显然 f 是满射, 又由群同构第二定理的证明可知, f 对加法构成群同态, 且 $\ker(f) = \{a \in S : a + I = I\} = \{a \in S : a \in I\} = S \cap I$. 因此我们只要证明 f 对乘法是么半群同态, 就可以利用环同构第一定理证明这个命题了. 而这是显然的, 因为若 $a, b \in S$, 则

$$f(a)f(b) = (a + I)(b + I) = ab + I = f(ab).$$

因此, 由环同构第一定理, 我们得到了

$$S/(S \cap I) \cong (S + I)/I.$$

综上所述, 我们就证明了这个命题. □

引理 2.7

设 $(R, +, \cdot)$ 是一个环, $I \triangleleft R, J \triangleleft R$, 且 $I \subset J$, 则 $I \triangleleft J$. ♥

证明 第一, 由 $I \triangleleft R$ 可知 $(I, +) \leq (R, +)$, 从而 I 对单位、加法和逆元都封闭. 又 $I \subset J$, 故 $(I, +) \leq (J, +)$.

第二, 由 $J \triangleleft R$ 可知 $J \subset R$. 于是由 $I \triangleleft R$ 可得 $IJ = JI = I$.

综上, $I \triangleleft J$. □

定理 2.3 (环同构第三定理)

设 $(R, +, \cdot)$ 是一个环, 而 $I, J \triangleleft R$, 且 $I \subset J$. 则 $J/I \triangleleft R/I$, 且

$$(R/I)/(J/I) \cong R/J. \quad \text{♥}$$

证明 首先, 由引理 2.7 可知 $I \triangleleft J$. 故 J/I 是一个商环. 由 $I, J \triangleleft R$ 可知 $R/I, R/J$ 也是商环. 我们先证明 $J/I \triangleleft R/I$. 对加法而言 J/I 和 R/I 都是群, 从而它们都对单位元、加法和逆元封闭. 又 $J/I \subset R/I$, 故 J/I 是 R/I 的加法子群. 我们只须证明 $(J/I)(R/I) \subset J/I$, 及 $(R/I)(J/I) \subset J/I$. 根据对称性, 我们证明前面这个包含关系. 因为 $J \triangleleft R$, 所以

$$(J/I)(R/I) = (JR)/I \subset J/I.$$

这就证明了 $J/I \triangleleft R/I$.

和群同构第三定理一样, 我们令 $f: R/I \rightarrow R/J$, 对 $a + I (a \in R)$, 定义为

$$f(a + I) = a + J.$$

根据群同构第三定理的证明, 同理可知 f 是一个良定义的满射, 对加法构成群同态, 且 $\ker(f) = J/I$. 因此我们只要证明 f 对乘法是么半群同态, 就可以利用环同构第一定理证明这个命题了. 而这是显然的, 因为若 $a+I, b+I \in R/I(a, b \in R)$, 则

$$f(a+I)f(b+I) = (a+J)(b+J) = ab+J = f(ab+I).$$

又因为 $f(1+I) = 1+J$. 因此, 由环同构第一定理, 我们得到了

$$(R/I)/(J/I) \cong R/J. \quad (2.3)$$

综上所述, 我们就证明了这个命题. \square

2.3 理想

定义 2.17 (由子集生成的理想)

设 $(R, +, \cdot)$ 是一个环, 而 $A \subset R$. 则 (A) , 称为由 A 生成的理想, 定义为所有 R 中包含 A 的理想的交集, 即

$$(A) = \bigcap \{I \subset R : I \supset A, I \triangleleft R\}.$$

 **笔记** 因为 $R \triangleleft R$ 且 $A \subset R$, 所以 $R \subset (A)$. 故 $(A) \neq \emptyset$.

命题 2.16 (生成的理想还是理想)

设 $(R, +, \cdot)$ 是一个环, 而 $A \subset R$, 则 $(A) \triangleleft R$.

证明 首先, 取交集的集族非空, 因为整个环 R 是包含了 A 的一个理想 (对加法构成子群, 且“吸收”了乘法).

由于集族中每一个理想都是加法子群. 因此根据命题 1.15 可知, 它们的交还是加法子群. 我们只须检验乘法的“吸收”性, 即 $R(A) \subset (A)$, 及 $(A)R \subset (A)$. 根据对称性, 我们证明第一个包含关系. 假设 $r \in R, a \in (A)$, 则对于任意集族中的理想 I , 我们都有 $a \in I$. 故 $ra \in I$. 这对于任意这样的理想 I 都是成立的, 因此 $ra \in (A)$. 这就证明了 (A) 是 R 的子环. \square

定义 2.18

设 $(R, +, \cdot)$ 是一个环, 而 $a \in R$, 则我们定义

$$(a) = (\{a\}).$$

称为由 a 生成的主理想. 一般地, 若一个理想能被一个元素生成, 我们就称其为主理想.

对于 $a_1, \dots, a_n \in R$, 我们定义

$$(a_1, \dots, a_n) = (\{a_1, \dots, a_n\}).$$

一般地, 若一个理想能被有限个元素生成, 我们就称其为有限生成的理想. \clubsuit

命题 2.17

设 $(R, +, \cdot)$ 是一个交换环, 而 $a \in R$, 则

$$(a) = Ra = \{ra : r \in R\}.$$

一般地, 若 $a_1, \dots, a_n \in R$, 则

$$(a_1, \dots, a_n) = Ra_1 + \dots + Ra_n = \{r_1a_1 + \dots + r_na_n : r_1, \dots, r_n \in R\}.$$

注 若 $(R, +, \cdot)$ 是环, 但不是交换环, 则上述结论仍成立. 但是我们还可以同理得到, 当 $m = 1, 2, \dots, n$ 时, 都有

$$(a_1, \dots, a_n) = Ra_1 + \dots + Ra_m + a_{m+1}R + \dots + a_nR.$$

故此时与 (a_1, \dots, a_n) 相等的集合就有 2^m 种不同的形式.

如果 $(R, +, \cdot)$ 是一个交换环, 那么当 $m = 1, 2, \dots, n$ 时, 都有

$$(a_1, \dots, a_n) = Ra_1 + \dots + Ra_m + a_{m+1}R + \dots + a_nR = Ra_1 + \dots + Ra_n.$$

这样在交换环下 (a_1, \dots, a_n) 的形式就能够统一起来.

证明 显然有限生成的理想是主理想的特例, 故我们只须证明第二个等式.

要证明 $(A) = I$, 我们只须证明两点. 一, I 是包含 A 的理想 (即 $(A) \subset I$); 二, 每一个包含 A 的理想都会包含 I (即 $\forall H \in (A)$, 都有 $I \subset H$. 也即 $I \subset (A)$).

首先, 要证明 $Ra_1 + \dots + Ra_n$ 是个理想. 对加法而言, $0 = 0a_1 + \dots + 0a_n \in Ra_1 + \dots + Ra_n$, 而且对 $r_1a_1 + \dots + r_na_n, s_1a_1 + \dots + s_na_n (r_i, s_i \in R)$, 我们有

$$(r_1a_1 + \dots + r_na_n) - (s_1a_1 + \dots + s_na_n) = (r_1 - s_1)a_1 + \dots + (r_n - s_n)a_n \in Ra_1 + \dots + Ra_n.$$

因此 $Ra_1 + \dots + Ra_n$ 对加法构成子群.

接下来, 根据对称性, 我们只须证明 $R(Ra_1 + \dots + Ra_n) \subset (Ra_1 + \dots + Ra_n)$. 而这是因为

$$R(Ra_1 + \dots + Ra_n) = RRa_1 + \dots + RRa_n = Ra_1 + \dots + Ra_n.$$

这样, 我们就证明了 $Ra_1 + \dots + Ra_n$ 是个理想, 而且显然包含 $\{a_1, \dots, a_n\}$.

另一方面, 设 I 是一个包含了 a_1, \dots, a_n 的理想, 那么根据加法的封闭性及乘法的“吸收”性,

$$I \supset Ra_1 + \dots + Ra_n.$$

综上所述, 这就证明了这个命题. □

定义 2.19 (理想的加法)

设 $(R, +, \cdot)$ 是一个环, 而 $I, J \triangleleft R$, 则

$$I + J = \{a + b : a \in I, b \in J\}.$$

命题 2.18 (理想的加法还是理想)

设 $(R, +, \cdot)$ 是一个环, 而 $I, J \triangleleft R$, 则 $I + J$ 还是个理想, 即

$$I + J \triangleleft R.$$

证明 由引理 1.7 可知 $(I + J, +) < (R, +)$. 因此我们只须证明乘法的“吸收”性.

$$R(I + J) = RI + RJ \subseteq I + J,$$

$$(I + J)R = IR + JR \subseteq I + J.$$

这就证明了

$$I + J \triangleleft R.$$

□

命题 2.19

设 $(R, +, \cdot)$ 是一个环, 而 $I, J \triangleleft R$, 则 $I + J$ 是由 $I \cup J$ 生成的理想, 即

$$I + J = (I \cup J).$$

证明 首先, 由命题 2.18 可知 $I + J$ 是一个理想. 而 $I + J \supset I + \{0\} = I$, 同理 $I + J \supset J$, 故 $I + J \supset I \cup J$. 这就证明了 $I + J$ 是一个包含了 $I \cup J$ 的理想.

接着, 如果 K 是包含了 $I \cup J$ 的理想, 则 $K \supset I, K \supset J$, 那么根据加法封闭性, 我们当然有

$$K \supset I + J.$$

综上所述, 我们就证明了

$$I + J = (I \cup J).$$

□

定义 2.20 (理想的乘法)

设 $(R, +, \cdot)$ 是一个交换环, 而 $I, J \triangleleft R$, 则

$$IJ = (\{ab : a \in I, b \in J\}) = (I \cdot J).$$

上面的圆括号表示生成的理想.

♣

注 由命题 2.16 可知, 上述定义的 IJ 仍是 R 的一个理想.

命题 2.20

设 $(R, +, \cdot)$ 是一个交换环, 而 $I, J \triangleleft R$, 则

$$IJ = \{a_1b_1 + \cdots + a_nb_n : a_1, \cdots, a_n \in I, b_1, \cdots, b_n \in J\}.$$

♣

注 若 $(R, +, \cdot)$ 是环, 但不是交换环, 则上述结论仍成立. 但是我们还可以同理得到, 当 $m = 1, 2, \cdots, n$ 时, 都有

$$IJ = \{(a_1b_1 + \cdots + a_mb_m) + (b_{m+1}a_{m+1} + \cdots + b_na_n) : a_1, \cdots, a_n \in I, b_1, \cdots, b_n \in J\}.$$

故此时与 IJ 相等的集合就有 2^m 种不同的形式.

如果 $(R, +, \cdot)$ 是一个交换环, 那么当 $m = 1, 2, \cdots, n$ 时, 都有

$$\begin{aligned} IJ &= \{a_1b_1 + \cdots + a_nb_n : a_1, \cdots, a_n \in I, b_1, \cdots, b_n \in J\} \\ &= \{(a_1b_1 + \cdots + a_mb_m) + (b_{m+1}a_{m+1} + \cdots + b_na_n) : a_1, \cdots, a_n \in I, b_1, \cdots, b_n \in J\}. \end{aligned}$$

这样在交换环下 IJ 的形式就能够统一起来.

证明 首先, 如果 K 是交换环 R 中包含了 $\{ab : a \in I, b \in J\}$ 的理想, 则根据加法的封闭性,

$$K \supset \{a_1b_1 + \cdots + a_nb_n : a_1, \cdots, a_n \in I, b_1, \cdots, b_n \in J\}.$$

故 $\{a_1b_1 + \cdots + a_nb_n : a_1, \cdots, a_n \in I, b_1, \cdots, b_n \in J\} \subset IJ$.

接着, 我们要证明 $A = \{a_1b_1 + \cdots + a_nb_n : a_1, \cdots, a_n \in I, b_1, \cdots, b_n \in J\}$ 确实是包含了 $\{ab : a \in I, b \in J\}$ 的一个 R 上的理想. 包含关系是显然的, 这就是有限和中只有一项的特例.

我们先证明加法是子群. $0 = 00 + \cdots + 00 \in A$, 而且对于 $a_1b_1 + \cdots + a_nb_n, c_1d_1 + \cdots + c_md_m \in A$, 其中 $a_i, c_i \in I, b_i, d_i \in J$. 由 $I, J \triangleleft R$ 可知 $-c_i \in I, a_ib_i \in I, (-c_i)d_i \in J$. 于是我们有

$$\begin{aligned} (a_1b_1 + \cdots + a_nb_n) - (c_1d_1 + \cdots + c_md_m) &= a_1b_1 + \cdots + a_nb_n + (-c_1)d_1 + \cdots + (-c_m)d_m \\ &= (a_1b_1 + \cdots + a_nb_n) \cdot 1 + 1 \cdot ((-c_1)d_1 + \cdots + (-c_m)d_m) + 0 + \cdots + 0 \in A. \end{aligned}$$

故 $(A, +)$ 是 $(R, +)$ 的子群. 我们再证明乘法的“吸收性”. 根据对称性, 我们只证“左吸收性”. 令 $a_1b_1 + \cdots + a_nb_n \in A$, 而 $\forall r \in R$, 都有 $ra_i \in I$, 不妨令 $a'_i = ra_i \in I$, 则

$$r(a_1b_1 + \cdots + a_nb_n) = ra_1b_1 + \cdots + ra_nb_n = a'_1b_1 + \cdots + a'_nb_n \in A.$$

综上所述, 由交换环中的两个理想 I, J 的乘积所生成的理想, 就是它们元素乘积的有限和所构成的集合. □

命题 2.21 (理想关于加法和乘法的运算律)

设 $(R, +, \cdot)$ 是一个交换环, 而 $I, J, K \triangleleft R$, 则满足

- (1) $I + J = J + I$;
- (2) $I + (J + K) = (I + J) + K$;
- (3) $I(J + K) = IJ + IK$;
- (4) $I(JK) = (IJ)K$;

$$(5) I = RI = IR.$$

证明

- (1) 由 $(R, +)$ 是一个 Abel 群可直接得到 $I + J = J + I$.
 (2) 由 $(R, +)$ 是一个 Abel 群也可直接得到 $I + (J + K) = (I + J) + K$.
 (3) 一方面, $I(J + K) \supset I(J + \{0\}) = IJ$, 同理 $I(J + K) \supset IK$. 又 $I(J + K)$ 是 R 上的理想, 故根据 $I(J + K)$ 对加法的封闭性可得 $I(J + K) \supset IJ + IK$.

另一方面, 令 $\sum_i (a_i(b_i + c_i)) \in I(J + K)$, 则

$$\sum_i (a_i(b_i + c_i)) = \sum_i (a_i b_i) + \sum_i (a_i c_i) \in IJ + IK.$$

因此 $I(J + K) \subset IJ + IK$.

- (4) 根据对称性, 我们只证明 $I(JK) \subset (IJ)K$. 因为理想的乘积是由元素乘积的集合所生成的, 故只须证明 $\{ad : a \in I, d \in JK\} \subset (IJ)K$. 令 $a \in I, d = \sum_i (b_i c_i) \in JK$. 则

$$ad = a \sum_i (b_i c_i) = \sum_i ((ab_i) c_i).$$

其中 $ab_i \in IJ$, 故 $ad \in (IJ)K$. 因此 $I(JK) \subset (IJ)K$.

- (5) 我们只证明 $I = RI$. 一方面, 根据理想的定义, $I \supset RI$. 另一方面, $I = 1I \subset RI$, 因为 $1 \in R$.

□

引理 2.8

设 $(R, +, \cdot)$ 是一个交换环, 而 $I, J \triangleleft R$, 则

$$IJ \subset I \cap J \subset I + J$$

♡

证明 证明是简单的. 因为 R 是一个交换环, 而 I 是一个理想, 故

$$IJ \subset IR = I.$$

对 J 是类似的, 故

$$IJ \subset I \cap J.$$

另外, $I \cap J \subset I$, 而且 $I \cap J \subset J$, 故

$$I \cap J \subset (I \cup J) = I + J.$$

这就证明了这个引理.

□

引理 2.9

设 $(R, +, \cdot)$ 是一个交换环, 而 $I, J \triangleleft R$, 则

$$(I \cap J)(I + J) \subset IJ.$$

♡

证明 证明是不难的. 由命题 2.20 可知 $(I \cap J)(I + J) = \{\sum_i (a_i(b_i + c_i)) : a_i \in I \cap J, b_i \in I, c_i \in J\}$. 于是任取 $\sum_i (a_i(b_i + c_i)) \in (I \cap J)(I + J)$, 则 $a_i(b_i + c_i) \in (I \cap J) \cdot (I + J)$, 其中 $a_i \in I \cap J, b_i \in I, c_i \in J$, 从而

$$\sum_i (a_i(b_i + c_i)) = \sum_i (a_i b_i) + \sum_i (a_i c_i) \subset JI + IJ = IJ + IJ = IJ.$$

第一个等号是因为 R 中的乘法对加法满足分配律, 倒数第二个等号是根据交换环对乘法的交换律, 最后一步是根据理想的乘积对加法的封闭性. 这就证明了这个命题.

□

命题 2.22

设 $(R, +, \cdot)$ 是一个交换环, 而 $I, J, K \triangleleft R$, 则

$$I \cap (J + K) \supset I \cap J + I \cap K$$

特别地, 如果 $J \subset K$, 则

$$I \cap (J + K) = I \cap J + I \cap K$$

♠

证明 因为 $I \cap (J + K) \supset I \cap J$, 且 $I \cap (J + K) \supset I \cap K$, 又 $I \cap (J + K)$ 构成 R 的加法子群, 从而对加法封闭. 所以

$$I \cap (J + K) \supset I \cap J + I \cap K.$$

这就证明了第一点.

接下来, 我们假设 $J \subset K$. 我们只须证明

$$I \cap (J + K) \subset I \cap J + I \cap K.$$

而这是因为

$$I \cap (J + K) \subset I \cap (K + K) = I \cap K \subset I \cap J + I \cap K.$$

这就证明了这个命题. □

定义 2.21 (理想的互素)

设 $(R, +, \cdot)$ 是一个交换环, 而 $I, J \triangleleft R$. 我们称 I, J **互素**, 若其和为整个环, 即

$$I + J = R.$$

♣

命题 2.23 (两个理想互素的充要条件)

设 $(R, +, \cdot)$ 是一个交换环, 而 $I, J \triangleleft R$. 则 I, J 互素, 当且仅当

$$\exists a \in I, \exists b \in J, a + b = 1.$$

♠

证明 一方面, 若 $I + J = R$, 则根据引理 2.3 可知 $1 \in R = I + J$, 故存在 $a \in I, b \in J$, 使得 $a + b = 1$.

另一方面, 假设 $a + b = 1 (a \in I, b \in J)$, 则对任何 $r \in R$,

$$r = r1 = r(a + b) = ra + rb \in RI + RJ = I + J$$

这就证明了 $I + J \subset R$. 而由 R 对加法封闭, 显然有 $R \subset I + J$. 故 $R = I + J$. 综上所述, 两个理想互素当且仅当 1 可以写成这两个理想中元素的和. □

命题 2.24

设 $(R, +, \cdot)$ 是一个交换环, 而 $I, J \triangleleft R$ 互素, 则

$$IJ = I \cap J.$$

♠

证明 由引理 2.8 可知

$$IJ \subset I \cap J.$$

故只须证明

$$I \cap J \subset IJ.$$

由 I, J 互素可知 $I + J = R$. 又由命题 2.12 可知 $I \cap J$ 仍是 R 的理想, 从而 $I \cap J = (I \cap J)R$. 于是由引理 2.9 可得

$$I \cap J = (I \cap J)R = (I \cap J)(I + J) \subset IJ.$$

这就证明了这个命题. □

命题 2.25

设 $(R, +, \cdot)$ 和 $(R', +, \cdot)$ 是两个交换环, $f: (R, +, \cdot) \rightarrow (R', +, \cdot)$ 是一个环同态, 而 $I' \triangleleft R'$, 则 $f^{-1}(I') \triangleleft R$.

证明 就加法子群而言, 由命题 2.10 可知 $0 = f^{-1}(0) \in R$, 并且若 $a = f^{-1}(a'), b = f^{-1}(b') \in f^{-1}(I')$, 则

$$\begin{aligned} f(a - b) &= f(a) + f(-b) = f(a) - f(b) = a' - b' \\ \Rightarrow a - b &= f^{-1}(a' - b') \in f^{-1}(I'). \end{aligned}$$

就乘法的“吸收”性来说, 根据对称性, 我们只须证明 $Rf^{-1}(I') \subset f^{-1}(I')$, 对 $\forall r \in R, x \in f^{-1}(I')$, 有 $f(x) \in I'$. 由 f 是环同态可知, $f(rx) = f(r)f(x)$. 又由 I' 是 R' 的理想且 $f(r) \in R'$, 因此 $f(rx) = f(r)f(x) \in I'$. 于是 $rx \in f^{-1}(I')$. 这样, 我们就证明了这个命题, 即交换环中, 理想在环同态下的原像还是理想. \square

2.4 素理想与极大理想

定义 2.22 (整环)

设 $(R, +, \cdot)$ 是一个环, 则我们称 R 是个**整环**, 若它是个非零交换环, 且没有零因子, 即

$$\begin{aligned} R &\neq \{0\}, \\ R &\text{是个交换环}, \\ \forall a, b \in R, (ab = 0 &\implies a = 0 \text{ 或 } b = 0). \end{aligned}$$

若 $a \neq 0$ 且 $a \in R$ 满足 $\exists b \neq 0$ 且 $b \in R$ 使得 $ab = 0$, 我们就称 a 为 R 的一个**零因子**.

引理 2.10

若 p 是一个素数, $a, b \in \mathbb{Z}$, 则

$$p \mid ab \iff p \mid a \text{ 或 } p \mid b$$

证明 见初等数论. \square

定义 2.23 (合数)

除了 1 和其本身外还有其他正因数的大于 1 的正整数就称为**合数**. 此即大于 1 的不是素数的正整数.

引理 2.11

若 n 是一个合数, 则存在 $a, b \in \mathbb{Z}$, 使得

$$n \mid ab, n \nmid a, n \nmid b.$$

证明 证明是简单的. 若 n 是一个合数, 我们可以取一个非平凡分解 $n = ab$, 其中 $a, b \neq \pm 1$. 则 $n \mid ab$, 可是 $|n| > |a|$, 故 $n \nmid a$ (因为若一个数整除另一个数, 则这个数的绝对值必须小于等于另一个数). 同理 $n \nmid b$. 这样, 我们就证明了这个引理. \square

定义 2.24 (素理想)

设 $(R, +, \cdot)$ 是一个交换环, 而 $\mathfrak{p} \triangleleft R$, 则我们称 \mathfrak{p} 是个**素理想**, 若

$$\begin{aligned} \forall a, b \in \mathbb{Z}, (ab \in \mathfrak{p} &\iff a \in \mathfrak{p} \text{ 或 } b \in \mathfrak{p}), \\ \mathfrak{p} &\neq R. \end{aligned}$$

例题 2.2 证明: $p\mathbb{Z}$ 是整数环 $(\mathbb{Z}, +, \cdot)$ 的素理想, 而 $m\mathbb{Z}$ 不是整数环 $(\mathbb{Z}, +, \cdot)$ 的素理想, 其中 p 是素数, m 是合数.

证明 首先由命题 2.14 可知 $p\mathbb{Z}, m\mathbb{Z}, \mathbb{Z}$ 都是 \mathbb{Z} 的理想.

由引理 2.10 可知, 对 $\forall a, b \in \mathbb{Z}$

$$ab \in p\mathbb{Z} \Leftrightarrow p \mid ab \Leftrightarrow p \mid a \text{ 或 } p \mid b \Leftrightarrow a \in p\mathbb{Z} \text{ 或 } b \in p\mathbb{Z}.$$

故 $p\mathbb{Z}$ 是整数环 $(\mathbb{Z}, +, \cdot)$ 的素理想.

而由引理 2.11 可知

$$ab \in m\mathbb{Z} \Leftrightarrow m \mid ab \Rightarrow m \nmid a \text{ 且 } m \nmid b \Leftrightarrow a \notin m\mathbb{Z} \text{ 或 } b \notin m\mathbb{Z}.$$

故 $m\mathbb{Z}$ 不是整数环 $(\mathbb{Z}, +, \cdot)$ 的素理想.

又因为素理想一定不是整个环, 所以 \mathbb{Z} 也不是整数环 $(\mathbb{Z}, +, \cdot)$ 的素理想. □

命题 2.26

若 $m, n \in \mathbb{N}_1$, 由命题 2.14 可知 $m\mathbb{Z}, n\mathbb{Z}$ 一定是整数环的理想. 则

$$m\mathbb{Z} \text{ 和 } n\mathbb{Z} \text{ 互素} \iff m, n \text{ 互素}.$$

证明 由理想互素的定义和命题 2.3 可知

$$\begin{aligned} m\mathbb{Z} \text{ 和 } n\mathbb{Z} \text{ 互素} &\iff m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z} \\ &\iff 1 \in m\mathbb{Z} + n\mathbb{Z} \\ &\iff \exists k, l \in \mathbb{Z}, \text{ s.t. } 1 = mk + nl \end{aligned}$$

又由 Bézout 定理可知

$$\exists k, l \in \mathbb{Z}, \text{ s.t. } 1 = mk + nl \iff \gcd(m, n) = 1 \iff m, n \text{ 互素}$$

故

$$m\mathbb{Z} \text{ 和 } n\mathbb{Z} \text{ 互素} \iff m, n \text{ 互素}.$$

□

命题 2.27 (素理想的充要条件)

设 $(R, +, \cdot)$ 是一个交换环, 而 $\mathfrak{p} \triangleleft R$. 则 \mathfrak{p} 是一个素理想, 当且仅当商环 R/\mathfrak{p} 是一个整环.

证明 先证必要性. 令 \mathfrak{p} 是一个素理想. 因为 R 是交换环, 则显然 R/\mathfrak{p} 也是交换环. 因为对 $a, b \in R$, 我们有

$$(a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p} = ba + \mathfrak{p} = (b + \mathfrak{p})(a + \mathfrak{p}).$$

而且因为 $\mathfrak{p} \neq R$, 所以任取 $r \in R - \mathfrak{p}$, 则 $r + \mathfrak{p} \in R/\mathfrak{p}$. 注意到 $\mathfrak{p} \in R/\mathfrak{p}$, 且 $r \notin \mathfrak{p}$, 因此 $r + \mathfrak{p} \neq \mathfrak{p}$. 故 R/\mathfrak{p} 中此时至少有两个互异的元素, 即 R/\mathfrak{p} 不是零环.

我们只须证明 R/\mathfrak{p} 中没有零因子. 假设

$$(a + \mathfrak{p})(b + \mathfrak{p}) = 0 + \mathfrak{p} \Leftrightarrow ab + \mathfrak{p} = \mathfrak{p} \Leftrightarrow ab \in \mathfrak{p}.$$

根据 \mathfrak{p} 是素理想, 不失一般性假设 $a \in \mathfrak{p}$. 则

$$a + \mathfrak{p} = 0 + \mathfrak{p}.$$

这就证明了 R/\mathfrak{p} 是一个整环.

再证充分性. 假设 R/\mathfrak{p} 是一个整环. 类似地, 我们知道因为 R/\mathfrak{p} 不是零环, 所以 $\mathfrak{p} \neq R$. 否则 $R/\mathfrak{p} = R/R = 0 + R$, 只含一个元素, 与 R/R 不是零环矛盾.

再令 $a, b \in R$, 使得 $ab \in \mathfrak{p}$, 则

$$ab + \mathfrak{p} = (a + \mathfrak{p})(b + \mathfrak{p}) = 0 + \mathfrak{p}.$$

由于 R/\mathfrak{p} 是一个整环, 故不失一般性假设 $a + \mathfrak{p} = 0 + \mathfrak{p}$, 这就证明了 $a \in \mathfrak{p}$, 即 \mathfrak{p} 是一个素理想. □

定义 2.25 (极大理想)

设 $(R, +, \cdot)$ 是一个交换环, 而 $\mathfrak{m} \triangleleft R$. 则我们称 \mathfrak{m} 是一个**极大理想**, 若 $\mathfrak{m} \neq R$, 且它是个极大的理想, 即对于任意 $I \triangleleft R$, 如果 $I \supsetneq \mathfrak{m}$, 则

$$I = R.$$

这就是说, 唯一严格大于 \mathfrak{m} 的理想, 是整个环.

命题 2.28 (极大理想的充要条件)

设 $(R, +, \cdot)$ 是一个交换环, 而 $\mathfrak{m} \triangleleft R$. 则 \mathfrak{m} 是一个极大理想, 当且仅当商环 R/\mathfrak{m} 是一个域.

证明 先证必要性. 令 \mathfrak{m} 是一个极大理想. 因为 R 是交换环, 从而对 $a, b \in R$, 我们有

$$(a + \mathfrak{m})(b + \mathfrak{m}) = ab + \mathfrak{m} = ba + \mathfrak{m} = (b + \mathfrak{m})(a + \mathfrak{m}).$$

所以 R/\mathfrak{m} 是交换环, 因此我们只须证明每个非零元素都有逆元. 令 $a + \mathfrak{m} \in R/\mathfrak{m}$ 且 $a + \mathfrak{m} \neq 0 + \mathfrak{m}$, 也就是说 $a \notin \mathfrak{m}$. 只须证明存在 $b + \mathfrak{m} \in R/\mathfrak{m}$ ($b \in R$), 使得 $ab + \mathfrak{m} = 1 + \mathfrak{m}$. 等价地, 我们只须证明存在 $b \in R, m \in \mathfrak{m}$, 使得

$$1 = ab + m.$$

由**命题 2.17**可知 $\mathfrak{m} + (a) = \mathfrak{m} + Ra$, 又因为 $a \notin \mathfrak{m}$, 所以 $\mathfrak{m} + (a) = \mathfrak{m} + Ra$ 是一个严格包含了 \mathfrak{m} 的理想. 因为 \mathfrak{m} 是极大理想, 所以 $\mathfrak{m} + Ra = R$. 右边取 $1 \in R$, 我们就得到了, 存在 $b \in R, m \in \mathfrak{m}$, 使得 $1 = ab + m$, 这就证明了必要性.

再证充分性. 如果 R/\mathfrak{m} 是一个域, \mathfrak{m} 是一个极大理想, 那么对于任意理想 $I \supsetneq \mathfrak{m}$. 由**命题 2.6**可知 $0 \neq 1$, 从而 $0 + \mathfrak{m} \neq 1 + \mathfrak{m}$, 于是 $1 \notin \mathfrak{m}$. 故 $\mathfrak{m} \neq R$, 否则, 由**命题 2.3**可知 $1 \in \mathfrak{m}$ 矛盾!

再任取 $a \in I - \mathfrak{m}$. 则 $a + \mathfrak{m} \neq 0 + \mathfrak{m}$. 由于 R/\mathfrak{m} 是一个域, 故 $a + \mathfrak{m}$ 有逆元, 即存在 $b \in R$, 使得 $(a + \mathfrak{m})(b + \mathfrak{m}) = 1 + \mathfrak{m}$. 因此, 也存在 $m \in \mathfrak{m}$, 使 $1 = ab + m$. 因此, 对任意 $r \in R$, 由 I 和 \mathfrak{m} 都是 R 的理想可知

$$r = r(ab + m) = rab + rm \in Ib + \mathfrak{m} \subset I + \mathfrak{m} = I.$$

这就证明了 $I \subset R$. 又因为 $I \subset R$, 所以 $I = R$. 因此 \mathfrak{m} 是一个极大理想.

综上所述, 我们就证明了这个命题. □

引理 2.12 (域一定是整环)

设 $(R, +, \cdot)$ 是一个域, 则 R 是一个整环.

证明 由域的定义可知, 一个域当然是一个交换环. 又由**命题 2.6**可知 $0 \neq 1$, 故 $0, 1 \in R$, 因此 $R \neq \{0\}$. 令 $a, b \in R$, 使 $ab = 0$. 我们只须证明 $a = 0$ 或 $b = 0$.

假设 $a \neq 0, b \neq 0$, 而 $ab = 0$. 由 R 是域可知, 存在 $c, d \in R$, 使 $ac = bd = 1$. 则

$$1 = 1 \cdot 1 = acbd = abcd = 0 \cdot cd = 0.$$

而由**命题 2.6**可知 $0 \neq 1$ 矛盾! 因此每一个域都是整环. □

命题 2.29

设 $(R, +, \cdot)$ 是一个交换环, 则每一个极大理想都是素理想.

证明 **证法一:** 令 \mathfrak{m} 是一个极大理想, 则 R/\mathfrak{m} 是一个域. 根据**引理 2.12**可知, R/\mathfrak{m} 是一个整环, 再利用**命题 2.27**可知 \mathfrak{m} 是一个素理想. 这就证明了这个命题.

证法二: 令 \mathfrak{m} 是一个极大理想. 假设 $a, b \in R$, 使得 $ab \in \mathfrak{m}$, 我们只须证明 $a \in \mathfrak{m}$ 或 $b \in \mathfrak{m}$. 用反证法, 假设 $a, b \notin \mathfrak{m}$. 则由**命题 2.17**可知 $\mathfrak{m} + (a) = \mathfrak{m} + Ra$, 又因为 $a \notin \mathfrak{m}$, 所以 $\mathfrak{m} + (a) = \mathfrak{m} + Ra$ 是一个严格包含了 \mathfrak{m} 的理想. 因为 \mathfrak{m} 是极大理想, 这就迫使

$$R = \mathfrak{m} + Ra.$$

从而由 $1 \in R$ 可知, 存在 $m \in \mathfrak{m}$ 与 $r \in R$, 使

$$1 = m + ra.$$

则由于 $ab \in \mathfrak{m}$ 及 \mathfrak{m} 是一个理想, 我们有

$$b = bm + r(ab) \in \mathfrak{m} + r\mathfrak{m} \subset \mathfrak{m} + \mathfrak{m} = \mathfrak{m}.$$

可是这与 $b \notin \mathfrak{m}$ 相矛盾. 因此, \mathfrak{m} 是一个素理想. □

定义 2.26 (模理想同余)

设 $(R, +, \cdot)$ 是一个交换环, 而 $I \triangleleft R$. 令 $a, b \in R$, 我们称 a, b 模 I 同余, 记作

$$a \equiv b \pmod{I}$$

若它们的差在 I 中, 即

$$a - b \in I$$

或等价地,

$$a + I = b + I$$

命题 2.30 (模理想同余是一个等价关系)

设 $(R, +, \cdot)$ 是一个交换环, 而 $I \triangleleft R$. 令 $a, b, c \in R$, 则

- (1) $a \equiv a \pmod{I}$.
- (2) 若 $a \equiv b \pmod{I}$, 则 $b \equiv a \pmod{I}$.
- (3) 若 $a \equiv b \pmod{I}$, $b \equiv c \pmod{I}$, 则 $a \equiv c \pmod{I}$.

证明

- (1) 因为 $a - a = 0 \in I, (I, +) < (R, +)$, 所以 $a \equiv a \pmod{I}$.
- (2) 由 $a \equiv b \pmod{I}$ 可知 $a - b \in I$. 于是由 $(I, +) < (R, +)$ 可知 $b - a = -(a - b) \in I$. 故 $b \equiv a \pmod{I}$.
- (3) 由 $a \equiv b \pmod{I}, b \equiv c \pmod{I}$ 可知 $a - b, b - c \in I$. 从而由 $(I, +) < (R, +)$ 可知 $a - c = (a - b) + (b - c) \in I$. 故 $a \equiv c \pmod{I}$. □

定义 2.27

设 $(R, +, \cdot)$ 是一个交换环, 而 $I \triangleleft R$. 令 $a, b \in R$, 令 $a \in R$, 我们定义 a 在模 I 同余关系下的等价类为

$$\bar{a} = \{b \in R : b \equiv a \pmod{I}\}.$$

命题 2.31

设 $(R, +, \cdot)$ 是一个交换环, 而 $I \triangleleft R, a \in R$, 则

$$\bar{a} = \{b \in R : b \equiv a \pmod{I}\} = a + I.$$

进而, $R/I = \{a + I : a \in R\}$ 就是 R 在模 I 同余关系下的一个分拆. ◆

证明 根据定义 2.27 可知

$$\bar{a} = \{b \in R : b \equiv a \pmod{I}\} = \{b \in R : b - a \in I\} = \{b \in R : b \in a + I\} = a + I.$$

□

命题 2.32 (模理想同余的基本性质)

设 $(R, +, \cdot)$ 是一个交换环, 而 $I \triangleleft R$. 令 $n \in \mathbb{N}_1, a, b, c, d \in R$. 若

$$a \equiv b \pmod{I}$$

$$c \equiv d \pmod{I}$$

则

$$a + c \equiv b + d \pmod{I}$$

$$ac \equiv bd \pmod{I}$$

$$a^n \equiv b^n \pmod{I}$$

进而, $f(a) \equiv f(b) \pmod{I}$. 其中 $f(x)$ 是关于 x 的多项式.



注 一个关系若对加法、乘法和幂次都成立, 则它就一定对多项式也成立.

证明 由 $a \equiv b \pmod{I}, c \equiv d \pmod{I}$ 可知 $a - b, c - d \in I$.

第一条, 因为 $(I, +) < (R, +), (R, +)$ 是 Abel 群, 所以 $(a + c) - (b + d) = (a - b) + (c - d) \in I$. 故 $a + c \equiv b + d \pmod{I}$.

第二条, 由 $a - b, c - d \in I$ 可知存在 $r, s \in I$, 使得 $a = b + r, c = d + s$. 从而由 I 是 R 的理想可得

$$ac - bd = (b + r)(d + s) - bd = bs + rd + rs \in I.$$

故 $ac \equiv bd \pmod{I}$.

第三条, 结合数学归纳法, 反复利用第二条结论即可得到 $a^n \equiv b^n \pmod{I}$. □

定理 2.4 (中国剩余定理)

设 $(R, +, \cdot)$ 是一个交换环, 而 $(I_i)_{1 \leq i \leq n}$ 是一族两两互素的理想, 即对任何 $i \neq j$ 都有 $I_i + I_j = R$. 则对任何 $a_1, \dots, a_n \in R$, 都存在 $x \in R$, 使

$$x \equiv a_1 \pmod{I_1},$$

...

$$x \equiv a_n \pmod{I_n}.$$



证明 令 $a = (a_1, \dots, a_n)$, 则

$$a = a_1(1, 0, \dots, 0) + \dots + a_n(0, \dots, 0, 1).$$

假如 $x_i (1 \leq i \leq n)$ 分别满足

$$x_i \equiv 1 \pmod{I_i}.$$

$$\text{若 } j \neq i, x_i \equiv 0 \pmod{I_j}.$$

则根据模理想同余的基本性质可知, $x = a_1x_1 + \dots + a_nx_n$ 就一定满足了同余方程组

$$x \equiv a_1 \pmod{I_1},$$

...

$$x \equiv a_n \pmod{I_n}.$$

因此我们只须证明对任何 $1 \leq i \leq n$, 我们能找到 $x_i \in R$, 使得

$$x_i \equiv 1 \pmod{I_i},$$

$$\text{若 } j \neq i, x_i \equiv 0 \pmod{I_j}.$$

不失一般性, 我们假设 $i = 1$. 由于 I_1 与 $I_j (j \neq 1)$ 都互素, 特别地, $1 \in I_1 + I_j (j \neq 1)$. 则存在 $b_j \in I_1, c_j \in I_j (j \neq 1)$,

使得

$$b_2 + c_2 = 1,$$

...

$$b_n + c_n = 1.$$

令 $x_1 = c_2 \cdots c_n \in R$. 则对任何 $j \neq 1$, 由 $I_j \triangleleft R$, 我们有

$$c_2 \cdots c_j \cdots c_n \in I_j.$$

即

$$x_1 \equiv c_2 \cdots c_j \cdots c_n \equiv 0 \pmod{I_j}.$$

并且

$$1 - c_2 \cdots c_n = (b_2 + c_2) \cdots (b_n + c_n) - (c_2 \cdots c_n).$$

根据分配律, 将上式展开后, 上面的每一项都包含至少某个 $b_i \in I_1$ 作为因子, 因此

$$1 - c_2 \cdots c_n \in I_1.$$

于是

$$x_1 = c_2 \cdots c_n \equiv 1 \pmod{I_1}.$$

这就完成了 x_1 的构造. 类似地, 我们可以构造出所有的 $x_i (1 \leq i \leq n)$, 因此

$$x \equiv a_1 x_1 + \cdots + a_n x_n.$$

给出了原命题所需的解.

综上所述, 我们通过线性性对原同余方程组进行了化简, 并不失一般性地证明了 $i = 1$ 的情形, 这就完成了中国剩余定理的证明. \square

命题 2.33 (中国剩余定理推论)

设 $(R, +, \cdot)$ 是一个交换环, 而 $(I_i)_{1 \leq i \leq n}$ 是一族两两互素的理想, 即对任何 $i \neq j$ 都有 $I_i + I_j = R$. 则

$$\begin{aligned} \pi : R &\rightarrow \prod_{i=1}^n (R/I_i), \\ \pi(a) &= (a + I_1, \cdots, a + I_n). \end{aligned}$$

是个满同态. 特别地,

$$R / \bigcap_{i=1}^n I_i \simeq \prod_{i=1}^n (R/I_i).$$

因此在以上条件下, π 是个同构当且仅当

$$\bigcap_{i=1}^n I_i = \{0\}.$$



证明 π 的每一个坐标都是环同态, 因此 π 也是环同态. 根据中国剩余定理的证明可知, 对任意 $(a_1 + I_1, \cdots, a_n + I_n) \in \prod_{i=1}^n (R/I_i)$, 都存在 $a \in R$, 使得

$$\begin{aligned} a &\equiv a_i \pmod{I_i} \quad (i = 1, 2, \cdots, n) \iff a + I_i = a_i + I_i \quad (i = 1, 2, \cdots, n) \\ &\iff \pi(a) = (a + I_1, \cdots, a + I_n) = (a_1 + I_1, \cdots, a_n + I_n). \end{aligned}$$

故 π 是个满同态. 我们只须找到 π 的核即可. 根据 π 的定义,

$$\begin{aligned} \pi(a) = 0 &\iff \forall i, a + I_i = 0 + I_i \\ &\iff \forall i, a \in I_i \end{aligned}$$

$$\iff a \in \bigcap_{i=1}^n I_i.$$

因此 $\ker \pi = \bigcap_{i=1}^n I_i$. 根据环同构第一定理, 这就证明了

$$R / \bigcap_{i=1}^n I_i \simeq \prod_{i=1}^n (R / I_i).$$

因此在以上的条件下, π 是同构当且仅当 π 是单的, 当且仅当 $\ker(\pi) = \{0\}$, 当且仅当

$$\bigcap_{i=1}^n I_i = \{0\}.$$

因此, 最特殊的情况即 R 中有有限多个两两互素且总的交集为 $\{0\}$ 的理想. 在这种情况下,

$$R \simeq \prod_{i=1}^n (R / I_i).$$

综上所述, 我们证明了这个命题. □

推论 2.1

设 $n \in \mathbb{N}_1$, 由算术基本定理可知, n 存在素幂因子分解, 即存在 p_1, p_2, \dots, p_m 两两互素, $\alpha_1, \alpha_2, \dots, \alpha_m \in \mathbb{N}_1$, 使得

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}.$$

则

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \mathbb{Z}_{\prod_{i=1}^m p_i^{\alpha_i}} \cong \prod_{i=1}^m \mathbb{Z}_{p_i^{\alpha_i}}.$$



证明 由命题 2.24 可知

$$n\mathbb{Z} = \prod_{i=1}^m p_i^{\alpha_i} \mathbb{Z} = \bigcap_{i=1}^m (p_i^{\alpha_i} \mathbb{Z}).$$

从而由中国剩余定理推论可知

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z} / \bigcap_{i=1}^m (p_i^{\alpha_i} \mathbb{Z}) \cong \prod_{i=1}^m (\mathbb{Z} / p_i^{\alpha_i} \mathbb{Z}) = \prod_{i=1}^m \mathbb{Z}_{p_i^{\alpha_i}}.$$



2.5 环的局部化