

0.1 群论与数论

定义 0.1 (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 0.1

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??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??可知 $n\mathbb{Z} \triangleleft \mathbb{Z}$. \square

命题 0.2

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, $nm = \underbrace{n + n + \cdots + n}_{m \text{ 个}} \in A$. 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 0.1

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 $A = \langle x^n \rangle$, 并且 $A \triangleleft \langle x \rangle$. \heartsuit

证明 由命题??可知, 任意无限循环群 $\langle x \rangle$ ($|x| = \infty$) 都同构于整数加群 $(\mathbb{Z}, +)$. \square

定义 0.2 (同余 (模 n))

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

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


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

定义 0.3 (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。

命题 0.3

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

其中枚举法中的这些陪集是两两不同的。

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,

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

□