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

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 $f : \mathbb{Z} \to \mathbb{Z}$, 对 $m \in \mathbb{Z}$, 定义为

$$f(m) = mn.$$

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

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

故 f 是 $(\mathbb{Z}, +)$ 到 $(\mathbb{Z}, +)$ 的群同态. 因此由命题**??**可知 $n\mathbb{Z} = \mathrm{im}(f) < \mathbb{Z}$. 又因为 $\mathbb{Z}$ 是阿贝尔群, 因此由命题**??**可知 $n\mathbb{Z} \lhd \mathbb{Z}$. □

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 $A \cap \mathbb{N}_1 \neq \varnothing$, 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 $0 \leqslant r \leqslant n - 1$. 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 $1 \leqslant r \leqslant n - 1 < n$, 这与 $n = \min(A \cap \mathbb{N}_1)$ 矛盾! 故 $a \in n\mathbb{Z}$. □

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 $A = \langle x^n \rangle = \{x^{nm} : m \in \mathbb{Z}\}$, 并且 $A \lhd \langle x \rangle$.

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 $(\mathbb{Z}, +)$, 故 A 一定同构于 $\mathbb{Z}$ 的某一子群. 于是由命题 0.2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 0.1可知 $n\mathbb{Z} \lhd \mathbb{Z}$. 故 $A \lhd \langle x \rangle$. □

定义 0.2 (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 $a \equiv b \bmod n$, 若

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

或

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

或

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

或

$$a\text{和}b(\mathrm{mod}\ n)\text{的余数相同}.$$

证明 $n\mid(a-b)\Leftrightarrow a-b\in n\mathbb{Z}$ 是显然的. 由引理??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 $b(\mathrm{mod}\ n)$ 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 $0\leqslant r\leqslant n-1$. 于是

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

故 a 和 $b(\mathrm{mod}\ n)$ 的余数都是 r.

$\Leftarrow$: 由 a 和 $b(\mathrm{mod}\ n)$ 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 $0\leqslant r\leqslant n-1$. 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. □

命题 0.3 (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: $a\equiv a(\mathrm{mod}\ n)$.

对称性: 若 $a\equiv b(\mathrm{mod}\ n)$, 则 $b\equiv a(\mathrm{mod}\ n)$.

传递性: 若 $a\equiv b(\mathrm{mod}\ n), b\equiv c(\mathrm{mod}\ n)$, 则 $a\equiv c(\mathrm{mod}\ n)$.

证明 自反性: 由 $a+n\mathbb{Z}=a+n\mathbb{Z}$ 可知 $a\equiv a(\mathrm{mod}\ n)$.

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

传递性: 由 $a\equiv b(\mathrm{mod}\ n), b\equiv c(\mathrm{mod}\ n)$ 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 $a\equiv c(\mathrm{mod}\ n)$. □

命题 0.4

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

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

证明 若 $b\in\overline{a}$, 则 $a\equiv b(\mathrm{mod}\ n)$. 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 $\overline{a}\subset a+n\mathbb{Z}$.

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 $a\equiv b(\mathrm{mod}\ n)$. 因此 $b\in\overline{a}$. 故 $a+n\mathbb{Z}\subset\overline{a}$.

综上,$\overline{a}=a+n\mathbb{Z}$. □

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,$0, \cdots, n-1$ 分别代表了 n 个同余类. 并且由命题 0.1可知 $\mathbb{Z}_n$ 是一个商群.

命题 0.5

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

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 0.4表明:

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1+n\mathbb{Z}, \cdots, n-1+n\mathbb{Z}\} = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}.$$

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 $0 \leqslant r \leqslant n-1$, 使得

$$m = qn + r.$$

由于

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

因此 $m + n\mathbb{Z} = r + n\mathbb{Z} \in \{k + n\mathbb{Z} : 0 \leqslant k \leqslant n-1\}$. 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 $0 \leqslant k, k' \leqslant n-1$, 则 $k - k' \in n\mathbb{Z}$. 但是 $-(n-1) \leqslant k - k' \leqslant (n-1)$. 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,

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

□

命题 0.6

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

笔记 由命题??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 0.5可知,$A = k + n\mathbb{Z}$, 其中 $0 \leq k \leq n-1$. 又由命题 0.1可知 $(n\mathbb{Z}, +) \lhd (\mathbb{Z}, +)$. 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 0.5可知, 这个群又是 n 阶的, 因此是 n 阶循环群. □

定义 0.4

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

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

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 0.7

$(\mathbb{Z}_n, \cdot)$ 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

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

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 0.5

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

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

也即

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

注 由引理**??**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 0.1 (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 0.8

设 $n \in \mathbb{N}_2$, 则

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

因此

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

特别地, 若 p 是一个素数, 则

$$\mathbb{Z}_p^\times = \{1 + p\mathbb{Z}, 2 + p\mathbb{Z}, \cdots, (p - 1) + p\mathbb{Z}\} = \{\overline{k} : 1 \leqslant k \leqslant p - 1\}.$$

因此

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

证明 我们只须证明, 若 $0 \leqslant k \leqslant n - 1$, 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 $1 \leqslant k \leqslant n - 1$, 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 0.1. 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

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

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

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

故

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

这就证明了这个命题. □

引理 0.2

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,

$$|\langle a \rangle| \,\big|\, |G|$$

而由命题??我们知道

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

因此,

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

这就证明了这个引理. □

定理 0.1 (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 $1 \leqslant a \leqslant p-1$ 的原因:

假设结论对 $1 \leqslant a \leqslant p-1$ 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 $1 \leqslant r \leqslant p-1$, 使得

$$a = mp + r.$$

于是 $1 \leqslant r = a - mp \leqslant p-1$ 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

$$1\leqslant a\leqslant p-1.$$

从而 $\overline{a}\in\mathbb{Z}_p^\times$(实际上, 由 $p\nmid a$ 就直接可以得到 $\overline{a}\in\mathbb{Z}_p^\times$). 根据引理 0.2, 可得

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

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 0.2 (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 $1\leqslant a\leqslant n-1, \gcd(a,n)=1$ 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

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

从而 $\overline{a}\in\mathbb{Z}_n^\times$(实际上, 由 $n\nmid a$ 就直接可以得到 $\overline{a}\in\mathbb{Z}_n^\times$). 利用引理 0.2, 可得

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

此即

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

这就证明了欧拉定理. □

定理 0.3 (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

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

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$p-1 \pmod p$. 这就说明了所有逆元是自己的元素恰好是 $\overline{1}$ 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

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

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