NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Answer 10-11

2023 年 10 月 27 日

Assignment 10

Problem 1

设 $\sigma = (1\ 2\ 3\ 4\ 5\ 6) \in S_6$, 求 $\langle\sigma\rangle$.

解: $\langle\sigma\rangle = \{(1), (1\ 2\ 3\ 4\ 5\ 6), (1\ 3\ 5)(2\ 4\ 6), (1\ 4)(2\ 5)(3\ 6), (1\ 5\ 3)(2\ 6\ 4), (1\ 6\ 5\ 4\ 3\ 2)\}$.

Problem 2

证明: $(i_1\ i_2\ \cdots\ i_r)^{-1} = (i_r\ i_{r-1}\ \cdots\ i_1)$.

解: 当 $n \in \mathbf{Z} \setminus \{i_1, i_2, \ldots, i_r\}$ 时, $(i_1\ i_2\ \cdots\ i_r)(i_r\ i_{r-1}\ \cdots\ i_1)(n) = n$ 是显然的, 因此考虑 $n \in \{i_1, i_2, \ldots, i_r\}$ 的情况:

不失一般性的假设 $n = i_m$, 其中 $1 \le m \le r$, 因此 $(i_r\ i_{r-1}\ \cdots\ i_1)(n) = i_{m-1}$, 故 $(i_1\ i_2\ \cdots\ i_r)(i_r\ i_{r-1}\ \cdots\ i_1)(n) = (i_1\ i_2\ \cdots\ i_r)(i_{m-1}) = i_m = n$. 显然对所有的 $n \in \{i_1, i_2, ..., i_r\}$ 成立, 故 $(i_1\ i_2\ \cdots\ i_r)(i_r\ i_{r-1}\ \cdots\ i_1) = (1)$, 即

$$(i_1\ i_2\ \cdots\ i_r)^{-1} = (i_r\ i_{r-1}\ \cdots\ i_1).$$

Problem 3

设 $\sigma \in S_n$. 证明:

$$\sigma\,(i_1\ i_2\ \cdots\ i_r)\,\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_r)).$$

解: 首先考虑 $m = \sigma(i) \notin \{\sigma(i_n) | n = 1, 2, \ldots, r\}$ 的情况: 此时 $\sigma^{-1}(m) \notin \{i_n \mid n = 1, 2, ..., r\}$, 即轮换 $(i_1\ i_2\ \cdots\ i_r)(\sigma^{-1}(m)) = \sigma^{-1}(m)$, 因此等式左边对 m 作用的结果仍是 m, 此时等式右边也是 m.

其次考虑等式两边对 $\sigma(i_1)$ 的作用情况: 等式左边为 $\sigma\,(i_1\ i_2\ \cdots\ i_r)\,\sigma^{-1}(\sigma(i_1)) = \sigma(i_2)$, 等式右边为 $\sigma(i_2)$. 等式两边对其他的 $\sigma(i_n)$ 其中 $n = 2, 3, ..., r$ 的作用情况是一样的.

Problem 4

设 σ 为一个 n 阶置换, 集合 $X = \{1, 2, ..., n\}$. 在 X 中, 规定关系 "$\sim$":

$$k \sim l \iff \text{存在 } r \in \mathbf{Z}, \text{ 使 } \sigma^r(k) = l.$$

(1) 证明: $\sim$ 是 X 的一个等价关系;

(2) 证明: $k \sim l$ 的充分必要条件是 k 与 l 属于 σ 的同一个轮换;

(3) 对于置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 6 & 8 & 9 & 1 & 7 & 10 & 4 & 5 \end{pmatrix},$$

试确定集合 $X = \{1, 2, ..., 10\}$ 的所有等价类.

解:

(1) 因为 $\sigma^0(k) = k$, 故反身性成立;

如果 $k \sim l$, 那么 $\sigma^r(k) = l$, 故 $\sigma^{-r}(l) = k$, 因此 $l \sim k$, 故对称性成立;

如果 $j \sim k, k \sim l$, 那么有 $1, r_2 \in \mathbf{Z}$ 使得 $\sigma^{r_1}(j) = k$ 和 $\sigma^{r_2}(k) = l$, 故 $\sigma^{r_1+r_2} = l$, 即 $j \sim l$, 因此传递性成立.

所以 $\sim$ 是 X 上的一个等价关系;

(2) 将 σ 表示为不相交轮换的乘积 $\sigma_1\sigma_2\cdots\sigma_n$:

$\Rightarrow$: 因为 $k \sim l$, 那么 $\sigma^r(k) = \sigma_1^r\sigma_2^r\cdots\sigma_n^r(k) = l$, 因此 k 和 l 必然等于 $\sigma_i^r(k)$, 其中 $1 \le i \le n$;

$\Leftarrow$: 假如 k 和 l 属于同一个 σ_i, 那么有 $\sigma_i^r(k) = l$, 因此有 $\sigma_i^r(k) = (\sigma_1\sigma_2\cdots\sigma_i\cdots\sigma_n)^r(k) = \sigma_r(k) = l$, 即 $k \sim l$.

(3) 有 $\sigma = (1\ 3\ 6)(2)(4\ 8\ 10\ 5\ 9)(7)$, 故等价类是 $\{1, 3, 6\}, \{2\}, \{4, 8, 10, 5, 9\}, \{7\}$.

Assignment 11

Problem 1

证明或否定 $\mathbf{Z} \oplus \mathbf{Z}$ 是循环群.

解: 假设 $\mathbf{Z} \oplus \mathbf{Z}$ 是循环群, 生成元为 (a, b), 故有 $(m, n) = k(a, b)$, 当 $m = 0, n \neq 0$ 时, 有 $a = 0$, 当 $m \neq 0, n = 0$ 时, 有 $b = 0$, 因此生成元为 $(0, 0)$, 矛盾. 故 $\mathbf{Z} \oplus \mathbf{Z}$ 不是循环群.

Problem 2

假设 $G_1 \cong H_1,\ G_2 \cong H_2$. 证明: $G_1 \times G_2 \cong H_1 \times H_2$.

解: 假设 $\phi_1(G_1) = G_2$ 且 $\phi_2(H_1) = H_2$. 因此构造

$$\begin{aligned} \phi: \quad G_1 \times G_2 &\longrightarrow H_1 \times H_2 \\ (a,b) &\longmapsto (\phi_1(a), \phi_2(b)), \quad \forall a \in G_1, b \in G_2. \end{aligned}$$

(1) 显然 ϕ 是 $G_1 \times G_2$ 到 $H_1 \times H_2$ 的映射;

(2) 假设有 $(a,b),(a',b') \in G_1 \times G_2$, 使得 $\phi(a,b) = \phi(a',b')$, 即 $(\phi_1(a), \phi_2(b)) = (\phi_1(a'), \phi_2(b'))$. 因为 ϕ_1, ϕ_2 都是单射, 故 $a = a', b = b'$, 于是 $(a,b) = (a',b')$, 则 ϕ 为单射;

(3) 对 $\forall (h,k) \in H_1 \times H_2$, 由于 ϕ_1, ϕ_2 都是满射, 因此 $\exists a \in G_1, b \in G_2$, 使得 $\phi_1(a) = h, \phi_2(b) = k$, 故 $\phi(a,b) = (\phi_1(a), \phi_2(b)) = (h,k)$, 因此 ϕ 是满射;

(4) $\forall (a,b),(a',b') \in G_1 \times G_2$ 都有

$$\begin{aligned} \phi((a,b)(a',b')) =& \phi(aa', bb') = (\phi_1(aa'), \phi_2(bb')) \\ =& (\phi_1(a)\phi_1(a'), \phi_2(b)\phi_2(b')) \\ =& (\phi_1(a), \phi_2(b))(\phi_1(a'), \phi_2(b')) \\ =& \phi(a,b)\phi(a',b'). \end{aligned}$$

因此 ϕ 是 $G_1 \times G_2$ 到 $H_1 \times H_2$ 的同构映射, 故 $G_1 \times G_2 \cong H_1 \times H_2$.

Problem 3

在 $\mathbf{Z}$ 中, 设 $H = \langle 3 \rangle,\ K = \langle 5 \rangle$. 证明: $\mathbf{Z} = H + K$. 请问 $\mathbf{Z}$ 与 $H \oplus K$ 同构吗?

解: $\mathbf{Z}$ 的生成元是 1, 且 $(3,5) = 1$, 即 $\exists a, b \in \mathbf{Z}$ 满足 $3a + 5b = 1$, 因此 $\forall z \in \mathbf{Z}$, 都有

$$z = z \cdot 1 = z \cdot (3a + 5b) = 3az + 5bz \in H + K.$$

同时 $H + K \subseteq \mathbf{Z}$, 故 $Z = H + K$.

假设 $Z \cong H \oplus K$, 那么有 $H \oplus K \cong H + K$, 即有同构映射 $\phi : H \oplus K \to H + K$, 即 $\phi(h,k) = h + k$. 注意到 $15 \in H \cap K$, 因此有 $\phi(0,15) = 0 + 15 = 15 + 0 = \phi(15,0)$, 不满足单射, 故不同构.

第二部分也可以通过第一题和第二题的结论证明: 有 $\mathbf{Z} \cong H$ 和 $\mathbf{Z} \cong K$, 故 $\mathbf{Z} \oplus \mathbf{Z} \cong H \oplus K \cong \mathbf{Z}$, 与第一题结论矛盾, 故两者不同构.

Problem 4

证明: $U(15)$ 同构于 $U(3) \times U(5)$.

解: [书上的参考答案, 但不推荐] 利用书上定理 2.4.5 可知, 证明 $U(3) \cong H$, $U(5) \cong K$ 和 $U(15)$ 是 H 和 K 的内直积即可. $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$. 因为 $U(5)$ 为 4 阶循环群, 故寻找 $U(15)$ 中的一个 4 阶元素 (因为 $U(15)$ 不是循环群且阶为 8, 故其元素的阶只能有 $1, 2$ 和 4, 因此 $\forall x \in U(15)$, 只要 $x^2 \neq 1$, 则 $\mathrm{ord}(x) = 4$.) 显然 2 是符合条件的, 当然 7 同样符合条件, 我们给出后者的情况: 因此 $K = \langle 7 \rangle = \{1, 7, 4, 13\}$, H 同构于 $U(3)$ 是个 2 阶循环群, 故找一个不在 K 中且阶为 2 的元素即可, 可以发现 11 符合条件, 故 $H = \langle 11 \rangle = \{1, 11\}$. 又因为 $G = HK$ 且 $H \cap K = \{e\}$, 则 $U(15)$ 的内直积为 HK 且有 $H \cong U(3)$, $K \cong U(5)$. 故 $U(15)$ 同构于 $U(3) \times U(5)$.

解: (推荐) 构造

$$\begin{aligned} \phi: \ U(15) &\longrightarrow U(3) \times U(5) \\ n &\longmapsto (n \pmod 3, n \pmod 5), \text{ 其中 } n \text{ 和 } 15 \text{ 互素.} \end{aligned}$$

(1) 显然 ϕ 是一个映射;

(2) 假设有 $n_1, n_2 \in U(15)$ 使得 $\phi(n_1) = \phi(n_2)$, 那么 $(n_1 \pmod 3, n_1 \pmod 5) = (n_2 \pmod 3, n_2 \pmod 5)$, 故 $n_1 - n_2 \equiv 0 \pmod 3$, $n_1 - n_2 \equiv 0 \pmod 5$, 即 $3 \mid n_1 - n_2, 5 \mid n_1 - n_2$ 且 $0 \leq n_1 - n_2 \leq 14$, 故 $n_1 = n_2$, 即 ϕ 是单射;

(3) 因为 $|U(15)| = 8 = 2 \times 4 = |U(3)| \times |U(5)|$, 故 ϕ 是满射;

(4) $\forall n_1, n_2 \in U(15)$, 都有 $\phi(n_1 n_2) = (n_1 n_2 \pmod 3, n_1 n_2 \pmod 5) = (n_1 \pmod 3, n_1 \pmod 5)(n_2 \pmod 3, n_2 \pmod 5) = \phi(n_1)\phi(n_2)$, 其中第二个等号成立是因为 $(p, ab) = 1 \Rightarrow (p, a) = 1$ 且 $(p, b) = 1$.

综上, ϕ 是从 $U(15)$ 到 $U(3) \times U(5)$ 的同构映射, 故 $U(15)$ 同构于 $U(3) \times U(5)$.

Problem 5

设 $G = G_1 \times G_2 \times \cdots \times G_n$, 每个 a_i 是 G_i 中的有限阶元素. 证明:

$$\mathrm{ord}(a_1, a_2, \ldots, a_n) = [\mathrm{ord}\, a_1, \mathrm{ord}\, a_2, \ldots, \mathrm{ord}\, a_n].$$

解: 设 $d = [\mathrm{ord}\, a_1, \mathrm{ord}\, a_2, \ldots, \mathrm{ord}\, a_n]$, 那么 $(a_1, a_2, \ldots, a_n)^d = (a_1^d, a_2^d, \ldots, a_n^d) = (e_1, e_2, \ldots, e_n)$, 故 $\mathrm{ord}(a_1, a_2, \ldots, a_n) \mid [\mathrm{ord}\, a_1, \mathrm{ord}\, a_2, \ldots, \mathrm{ord}\, a_n]$;

假设 $d' \in \mathbf{Z}$ 使得 $(a_1, a_2, \ldots, a_n)^d = (e_1, e_2, \ldots, e_n)$, 那么 $a_i^{d'} = e_i$, 故 $\mathrm{ord}\, a_i \mid d'$, 因此 $d \mid d'$.

综上 $\mathrm{ord}(a_1, a_2, \ldots, a_n) = [\mathrm{ord}\, a_1, \mathrm{ord}\, a_2, \ldots, \mathrm{ord}\, a_n]$.