NIS2312-1 Spring 2021-2022

信息安全的数学基础 (1)

Answer 3

2022 年 3 月 17 日

Problem 1

$$\mathbf{Z}_3[x] = \left\{a_0 + a_1x + a_2x^2 + \cdots \mid a_i \in \mathbf{Z}_3, i = 0, 1, 2, \dots\right\}$$

所以

$$\mathbf{Z}_3[x]/\langle x^2+1\rangle = \left\{a_0 + a_1x + \langle x^2+1\rangle \mid a_i \in \mathbf{Z}_3, i = 0, 1\right\}$$

这里 a_i 中的 i 只能取 $0, 1$ 是因为理想 $\langle x^2+1\rangle$ 会让二次及以上的单项式降次 (处于同一个陪集中), 比如

$$x^2 + x + 1 + \langle x^2+1\rangle = x + (x^2+1) + \langle x^2+1\rangle = x + \langle x^2+1\rangle$$

1.2. 不是 (写这两道小题是因为有人做错了...)

3 该映射不是 $\mathbf{Z}_8$ 到 $\mathbf{Z}_2\times\mathbf{Z}_2\times\mathbf{Z}_2$ 的同构映射, 因为不保持运算, 举例: $dec2bin(7+1) = dec2bin(0) = (0,0,0) \neq dec2bin(7) + dec2bin(1) = (1,1,1) + (0,0,1) = (1,1,0)$.

4 对称群作用的集合元素数量相等的话, 对称群是同构的.

7 注意到 $a = 1$ 为单位元的时候, 是一个恒等映射显然是同构映射.

Problem 2

证明群之间不同构, 可以有几种: 一个是循环群一个不是; 两个群的阶不相等; 两个群中元素阶相等的元素数量不同;

1. 乘法群 $\mathbf{R}^*$ 和乘法群 $\mathbf{C}^*$ 不同构: 假设同构, 那么存在一个同构映射 $f : \mathbf{C}^* \to \mathbf{R}^*$ 使得 $f(i)^4 = f(i^4) = f(1) = 1$, 那么 $\mathrm{ord}(f(i)) = 4$, 但是在 $\mathbf{R}^*$ 中没有四阶的元素.
2. 加法群 $\mathbf{Z}$ 和 $\mathbf{Q}$ 不同构: 假设同构, 那么有同构映射 $f : \mathbf{Q} \to \mathbf{Z}$ 使得 $f(1) \in \mathbf{Z}$, 所以对任意 n 有 $f(1/n) = f(1)/n \in \mathbf{Z}$, 显然 $f(1) = 0$, 矛盾, 因为将非单位元映射到单位元了.

也可以这样证明: $\exists n \in \mathbf{Q}$ 使得 $f(n) = 1$, 所以 $f(n/2) = 1/2 \notin \mathbf{Z}$ 矛盾.

或者证明 $\mathbf{Z}$ 是循环群 (显然的), 但 $\mathbf{Q}$ 不是循环群: 如果 $\mathbf{Q}$ 是循环群, a 是生成元, 那么有整数 n 使得 $na = a/2 \to n = 1/2$ 不是整数, 矛盾.

3. 这里证明只需写出 $\mathbf{Z}_2 \times \mathbf{Z}_2$ 不是循环群即可, 比如所有的非单位元元素都 2 阶的.

4. 构造映射: $f : G \times H \to H \times G$ 使得 $f((g,h)) = (h,g)$, 其中 $g \in G, h \in H$.

   (1) 是一个映射, 因为 $f((g,h)) = (h,g) \in H \times G$

   (2) 单射: 若 $(g_1,h_1) \neq (g_2,h_2)$, 显然 $f((g_1,h_1)) = (h_1,g_1) \neq f((g_2,h_2)) = (h_2,g_2)$

   (3) 满射: $\forall (h,g) \in H \times G$, 都有 $(g,h) \in G \times H$ 使得 $f((g,h)) = (h,g)$.

   (4) 保持运算: $\forall (g_1,h_1),(g_2,h_2) \in G \times H$, 都有 $f((g_1,h_1)(g_2,h_2)) = f((g_1g_2,h_1h_2)) = (h_1h_2,g_1g_2) = (h_1,g_1)(h_2,g_2) = f((g_1,h_1))f((g_2,h_2))$

5. 证明 $\mathbf{Z}_n \times \mathbf{Z}_m$ 是循环群: 部分同学仅仅写出 $mn(1,1) = (0,0)$ 就说这是生成元, 这是不对的! 生成元的定义是按照元素的阶, 元素的阶为 n 还要证明小于 n 的整数无法使得元素的幂为单位元.

   显然 $mn(1,1) = (0,0)$, 所以如果 $\mathrm{ord}((1,1)) = k$, 那么 $k \mid mn$; 同时假设 $k = mn/d$, 其中 $d \in \mathbf{Z}$ 是 mn 的因子, 因此 $m \mid mn/d$ 和 $n \mid mn/d$, 所以 $n/d, m/d \in \mathbf{Z}$, 显然只有 $d = 1$ 满足条件. 因此 $k = mn$. 故 $\mathrm{ord}((1,1)) = mn$, 又因为 $|\mathbf{Z}_n \times \mathbf{Z}_m| = mn$, 就能得到结论群是个循环群.

Problem 3

群中的每一个元素的阶均不为 0, 且单位元是其中惟一的阶为 1 的元素。因为任一阶大于 2 的元素和它的逆元的阶相等。且当一个元素的阶大于 2 时，其逆元和它本身不相等。故阶大于 2 的元素是成对的。从而阶为 1 的元素与阶大于 2 的元素个数之和是奇数。因为该群的阶是偶数，从而它一定有阶为 2 的元素。

Problem 4

凯莱定理的推广: 仅证明 $GL_n(\mathbf{F}_2)$ 同构于置换矩阵即可. 置换矩阵是 $GL_n(F)$ 的子群, 其中 F 是任意域 (题目中我给出的是 $\mathbf{F}_2$, 实际上通常用的是 $\mathbf{R}$, 域的概念暂时不需要掌握). 证明是显然的...

考虑映射 $\phi : S_n \to P_{n\times n}$, 后者是 n 阶置换矩阵, 映射的方式为: 给定 $\tau \in S_n$, $\phi(\tau)$ 的第 i 列第 $\tau(i)$ 行为 1, 此外 1 所在的行和列其他位置全部为 0.

1. 显然这个是一个映射: $(\phi(i), i)$ 处为 1, 同时矩阵各行各列都只有一个 1, 因此 $\phi(\tau)$ 是一个置换矩阵.

2. 映射是一个单映射: 显然的.

3. 满映射同样显然的.

4. 保持运算: 对于任意 $\tau, \sigma \in S_n$, 有 $\phi(\tau \circ \sigma)_{ij} = 1$ 当且仅当 $i = \tau \circ \sigma(j)$, 其他情况是 0. 对于置换矩阵的乘法运算, $(\phi(\tau)\phi(\sigma))_{ij} = \sum_{k=1}^{n} \phi(\tau)_{ik}\phi(\sigma)_{kj}$. 而 $\phi(\tau)_{ik} = 1$ 当且仅当 $i = \tau(k)$, $\phi(\sigma)_{kj} = 1$ 当且仅当 $k = \sigma(j)$. 所以 $\phi(\tau)_{ik}\phi(\sigma)_{kj} = 1$ 当且仅当 $i = \tau(k), k = \sigma(j)$, 也就是 $i = \tau \circ \sigma(j)$. 并且 $(\phi(\tau)\phi(\sigma))_{ij} \leq 1$ 因为不存在多个 k 使得 $\tau(k) = i$.

因此映射 ϕ 是一个同构映射.

Problem 5

参考欧拉公式, 书上 11 页

$\mathbf{Z}_2 33$ 的生成元数量是 $\phi(233) = 232$ $\mathbf{Z}_4 900$ 的生成元数量是 $\phi(4900) = 1680$

推论 1: 因为 $(n, r) = d$, 所以 $d \mid r$, 故 $\langle a^r \rangle \subseteq \langle a^d \rangle$. 同时因为 $(n, r) = d$, 则存在 $u, v \in \mathbf{Z}$ 使得 $d = un + vr$. 于是 $a^d = a^{un+vr} = a^{vr} \in \langle a^r \rangle$. 证毕.

推论 2: (1) 如果 $|G| = \infty$, 因为对任意的 $r_1 > r_2 > 0$, 有 $r_1 \nmid r_2$, 所以 $a^{r_2} \notin \langle a^{r_1} \rangle$, 于是 $\langle a^{r_1} \rangle \neq \langle a^{r_2} \rangle$. 另一方面, 对任意的 $r > 0$, 显然 $a^r \notin \langle a^0 \rangle = \langle e \rangle$, 所以又有

$$\langle a^r \rangle \neq \langle e \rangle.$$

由此得 G 的全部子群为

$$\left\{ \left\langle a^d \right\rangle \mid d = 0, 1, 2, \cdots \right\}.$$

(2) 如果 $|G| = n$, 从上题知道对 $d = (n, r)$, 有 $\langle a^r \rangle = \left\langle a^d \right\rangle$

又如果 $d_1 > d_2$ 为 n 的两个不同的正因子, 则 $d_1 \nmid d_2$, 于是 $a^{d_2} \notin \left\langle a^{d_1} \right\rangle$, 从而

$$\left\langle a^{d_1} \right\rangle \neq \left\langle a^{d_2} \right\rangle.$$

另一方面, 对 n 的任一正因子 $d < n$, 显然 $a^d \neq e$, 所以又有

$$\left\langle a^d \right\rangle \neq \langle e \rangle.$$

而

$$\langle e \rangle = \langle a^n \rangle$$

由此得 G 的全部子群为

$$\left\{ \left\langle a^d \right\rangle \mid d \text{ 为} n \text{ 的正因子} \right\}.$$

Problem 6

假设 $\sigma = (123\cdots m)$, 于是 $\sigma^i(k) = k+i$, 且 $\sigma^i(k+i) = k+2i$, 因此 $\sigma^i : k \mapsto k+i \mapsto k+2i \mapsto \cdots k+(m-1)i \mapsto k$. 显然此时 σ^i 是一个 m-轮换, 当且仅当上式元素均不相同, i.e. $k + xi \neq k + yi \mod m$, 其中 $x, y \in \{0, 1, \ldots, m-1\}$, 也就是 $(x-y)i \neq 0 \mod m$, 即 $x = y$.

其实利用 probblem 5 的推论 1 就好

Problem 7

使用书上的公式 $(F1)$, 书上 46 页, 结果分别是 $(1\ 3), (1\ 4\ 2\ 7), (1\ 2)(4\ 7)$

Problem 8

(F2)(F3) 的证明完全可以硬算, S_n 子群更是简单 (偶置换和偶置换复合肯定还是偶置换, 逆也是偶置换) ... 略过