NIS2312-1 Spring 2021-2022

信息安全的数学基础 (1)

Answer 4

2022 年 3 月 17 日

Problem 1

H 中有单位元 e, 因此 $g \in gH$, 同时 g 也在 H 的一个右陪集中. 显然 $g \in Hg$, 又因为不同陪集不相交, 故这个右陪集一定是 Hg.

Problem 2

1. 考虑 $x_1x_2\cdots x_{p-1}$, 因为 $x_1x_2\cdots x_{p-1}x_p = 1$, 故 $x_1x_2\cdots x_{p-1} = x_p^{-1}$, 即 $p-1$ 个元素可以确定剩下的一个元素, 因此仅需要考虑 $x_1, x_2, \ldots, x_{p-1}$ 这 $p-1$ 个元素的取值范围, 显然是 $|G|^{p-1}$.

2. 反身性: $\forall x \in S$, x 经过 0 次循环移位 (置换) 仍是 x; 对称性: 对任意 $x, y \in S$, 如果 x 经过 i 次置换得到 y, 那么 y 可以经过 $p-i$ 次置换得到 x; 传递性: $\forall x, y, z \in S$, 如果 x 经过 i 次置换得到 y, 那么 y 可以经过 j 次置换得到 z, 显然 x 可以经过 $i+j \mod p$ 次置换得到 z. 因此 $\sim$ 是一个等价关系.

   显然 $x = (x_1, x_2, \ldots, x_p) = (1, 1, \ldots, 1)$ 是满足 $x_1x_2\cdots x_p = 1$ 的, 此时 x 所在等价类仅有 1 个元素. 注意到如果 $x = (x_0, x_0, \ldots, x_0)$ 是一个元素数量为 1 的等价类, 我们可以得到 $x_0^p = 1$.

   如果一个 x 中有 2 个元素不同, 显然在这个等价类中有 p 个元素.

3. 由之前的结论可知, $p \mid |S| = |G|^{p-1}$, 且 $|S| =\geq np + r$, 其中 n 是元素数量是 p 的等价类的数量, r 是等价类元素数量为 1 的数量. 因此 $p \mid r$, 所以存在 $r = p > 1$ 个元素数量为 1 的等价类, 显然能得到存在元素 $x^p = 1$, i.e. $\mathrm{ord}(x) = p$.

Problem 3

1. 封闭性, S_k 中置换的复合仍然是置换; 逆元, S_k 中置换的逆仍在 S_k 中; 因此是子群.

2. 同样的可以证明 S_n 中, 有一个子群, 子群内的置换分别独立地作用在集合 $\{1, 2, \ldots, k\}$ 和 $\{k+1, k+2, \ldots, n\}$ 上, 此子群阶为 $k!(n-k)!$. 再利用拉格朗日定理, 可以确定 $k!(n-k)! \mid |S_n| = n!$, 所以二项式系数是整数.

Problem 4

因为 $7 \nmid 30$, 故 G 中没有 7 阶子群.

5 阶子群是循环群, 所以这些子群两两相交于单位元, 因此假设有 n 个子群, 则有公式 $n(5-1)+1 \leq 30$, 可以得到 $n \leq 7$.

Problem 5

先证明 HK 是一个群: 封闭性是 $\forall hk, h'k' \in HK$, 有 $hkh'k' = hh'kk' \in HK$, 剩下的结合, 单位元, 逆元同样类似在此不证明了.

再证明 $H \cap K < HK$: 显然的, 子群的交仍然是子群.

现证明正规性: $\forall hk \in HK$, 有 $hkH \cap K(hk)^{-1} = hkH \cap Kk^{-1}h^{-1}$, 因为 $H \triangleleft G$, 所以 $H \cap K \triangleleft G$, 故 $hkH \cap K(hk)^{-1} = hkH \cap Kk^{-1}h^{-1} \in hH \cap Kh^{-1} = H \cap K$.

Problem 6

1. $\forall h_0, h_1 \in H$, 有 $gh_0g^{-1}(gh_1g^{-1})^{-1} = gh_0g^{-1}gh_1^{-1}g^{-1} = gh_0h_1^{-1}g^{-1} \in gHg^{-1}$, 因此 $gHg^{-1} < G$. 显然 $|gH| = |H|$, 否则有 $x, y \in H$ s.t. $gx = gy$, 即 $x = y$. 同理得到 $|gHg^{-1}| = |gH|$, 证毕.

2. 由于 $|gHg^{-1}| = |H| = n$ 且 H 是唯一的 n 阶子群, 所以 $H = gHg^{-1}$, 即 $H \triangleleft G$.

Problem 7

1. $Z(G) < G$ 在之前作业证明过, 因此仅证明正规性: $\forall g \in G$, 我们有 $gZ(G)g^{-1} = Z(G)gg^{-1} = Z(G)$, 证毕.

2. 循环群有 $G/Z(G) = \langle xZ(G) \rangle$, 其中 $x \in G$ 且 $xZ(G)$ 是一个陪集. 因此对于 $g, h \in G$ 有 $g \in (xZ(G))^n = x^nZ(G), h \in x^mZ(G)$, 其中 $n, m \in \mathbf{Z}$. 所以 $gh = x^nZ(G)x^mZ(G) = x^mZ(G)x^nZ(G) = hg$. 故 G 是阿贝尔群.

3. 如果 $|G| = pq$, 那么 $|G|/|Z(G)| = 1, p, q, pq$ 中的一个, $1, pq$ 的情况过于简单不再叙述. 假设 $|G|/|Z(G)| = p$, 那么 $G/Z(G)$ 是一个循环群, 所以 G 是一个阿贝尔群, 因此 $Z(G) = G$, i.e. $|G|/|Z(G)| = 1$ 与假设矛盾. 另一个情况类似不再叙述.

Problem 8

1. 显然是的, 对任意 $m \in GL_n(\mathbf{R})$, 有 $|mSL_n(\mathbf{R})m^{-1}| = |m||m^{-1}| = 1$, 即 $mSL_n(\mathbf{R})m^{-1} = SL_n(\mathbf{R})$, 是正规子群. 商群是 $\{mSL_n(\mathbf{R}) \mid |m|$各不相同$\}$ 同构于 $\mathbf{R}^*$

2. 显然是的, $\forall (x,y) \in A \times B$, 有 $(x,y)(a,1)(x,y)^{-1} = (xax^{-1}, 1) \in H$. 商群 $\{(1,b)H \mid b \in B\}$ 同构于 B, 注意陪集首里面的 1 可以换成任意 A 中元素.

3. 证明显然的. 商群直接看的话可能不好看出来, 当然写一写陪集就能看出陪集的问题了. 可以构造一个满同态, $f : A \times A \to H$, 使得 $f(x,y) = xy^{-1}$, 显然 $ker(f) = H$. 这里商群 $\{(a,1)H \mid a \in G\}$

4. 同样是明显的. 商群 $\{H, -H\} \cong \mathbf{Z}_2$

5. 如果 $[G : H] = 2$, 可以将 G 写为 $H \cup aH$ 和 $H \cup Ha$, 其中 $a \in G \setminus H$. 所以 $Ha = aH$, i.e. $H \triangleleft G$.

6. 不满足传递性: $H = \{(\sigma, \sigma) \mid \sigma \in A_3\} \triangleleft A_3 \times A_3 \triangleleft S_3 \times S_3$, 但是 H 不是 $S_3 \times S_3$ 的正规子群.

7. $\forall g \in G$, $[x,y] \in H$ 有 $g^{-1}x^{-1}y^{-1}xyg = g^{-1}x^{-1}gg^{-1}y^{-1}gg^{-1}xgg^{-1}yg$, 令 $u = g^{-1}xg, v = g^{-1}yg$, 可以得到 $g^{-1}x^{-1}y^{-1}xyg = u^{-1}v^{-1}uv \in H$, 因此是正规子群.