NIS2312-01 2023-2024 Fall

信息安全的数学基础 (1)

Answer 6-7

2023 年 10 月 13 日

$\mathbb{R}$ 是实数域, $\mathbb{Q}$ 是有理数域, $\mathbb{Z}$ 是整数集合.

Assignment 6

Problem 1

在 $(\mathbb{Z}_{12}, +)$ 中, 求子群 $H = \langle \overline{4} \rangle$ 的所有左陪集.

解: 可知 $H = \{\overline{0}, \overline{4}, \overline{8}\}$, 因此左陪集有

$$\begin{aligned}
\overline{0} + H &= H = \{\overline{0}, \overline{4}, \overline{8}\};\\
\overline{1} + H &= \{\overline{1}, \overline{5}, \overline{9}\};\\
\overline{2} + H &= \{\overline{2}, \overline{6}, \overline{10}\};\\
\overline{3} + H &= \{\overline{3}, \overline{7}, \overline{11}\}.
\end{aligned}$$

Problem 2

设 $H = \{0, \pm 3, \pm 6, \pm 9, \dots\}$. 求子群 H 在 $\mathbb{Z}$ 中的所有左陪集.

解: 子群 H 在 $\mathbb{Z}$ 中的所有左陪集为

$$\begin{aligned}
0 + H &= \{0, \pm 3, \pm 6, \pm 9, \dots\};\\
1 + H &= \{1, 1 \pm 3, 1 \pm 6, 1 \pm 9, \dots\};\\
2 + H &= \{2, 2 \pm 3, 2 \pm 6, 2 \pm 9, \dots\}.
\end{aligned}$$

Problem 3

设 $\operatorname{ord} a = 30$. 问 $\langle a^4 \rangle$ 在 $\langle a \rangle$ 中有多少个左陪集? 试将它们列出.

解: $\operatorname{ord} a^4 = 30/(30, 4) = 15$, 故 $\langle a^4 \rangle$ 在 $\langle a \rangle$ 中有 $30/15 = 2$ 个左陪集. 其中之一为 $e\langle a^4 \rangle$, 因为 $a \notin \langle a^4 \rangle$, 故 a 属于另一个左陪集, 则另一个为 $a\langle a^4 \rangle$.

Problem 4

设 H_1, H_2 是 G 的子群. 证明: $a(H_1 \cap H_2) = aH_1 \cap aH_2$.

解: $\subseteq$: $\forall x \in H_1 \cap H_2$, 都有 $x \in H_1, H_2$, 故 $ax \in aH_1, aH_2$, 即 $ax \in aH_1 \cap aH_2$, 因此 $a(H_1 \cap H_2) \subseteq aH_1 \cap aH_2$;

$\supseteq$: $\forall x \in aH_1 \cap aH_2$, 都有 $x = ah_1 = ah_2$, 其中 $h_1 \in H_1, h_2 \in H_2$. 则 $a^{-1}x \in H_1$, $a^{-1}x \in H_2$, 即 $a^{-1}x \in H_1 \cap H_2$, 那么 $x \in a(H_1 \cap H_2)$, 因此 $a(H_1 \cap H_2) \supseteq aH_1 \cap aH_2$.

综上, $a(H_1 \cap H_2) = aH_1 \cap aH_2$.

Problem 5

设 H 是有限群 G 的子群, K 是 H 的子群. 证明: $[G:K] = [G:H][H:K]$.

解: 根据拉格朗日定理可知, $[G:K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \times \frac{|H|}{|K|} = [G:H][H:K]$.

Problem 6

证明: 15 阶群至多含有一个 5 阶子群.

解: 第一种方法: 假设 5 阶子群至少有 2 个, 分别设为 H, K.

因为 5 是素数, 故 5 阶群是循环群, 即 $H = < h > = \{e, h, h^2, h^3, h^4\}$ 和 $K = < k > = \{e, k, k^2, k^3, k^4\}$, 且元素的阶只有 $1, 5$, 即 5 阶群的元素只有单位元和生成元. 那么任意两个不同的 5 阶群交集为单位元, 否则, H 和 K 有相同的生成元, 则 $H = K$.

故构造集合 $HK = \{hk : h \in H, k \in K\}$, 显然 $HK \subseteq G$, 即 $|HK| \leq |G| = 15$. 现讨论 $|HK|$ 的大小. 假设存在 $h_1, h_2 \in H, k_1, k_2 \in K$, s.t. $h_1k_1 = h_2k_2$, 则 $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$, 即 $h_2 = h_1, k_2 = k_1$. 因此集合 HK 元素数量为 $5 \times 5 = 25 > 15 = |G|$, 矛盾, 故至多含有一个 5 阶子群.

第二种方法: 不妨假设 15 阶群 G 存在两个 5 阶子群 H 和 K. 对 $\forall h \in H, k \in K, hk \in G$

$$
\begin{aligned}
|HK| &= |\bigcup_{h \in H} hK| \\
&= |\{hK | h \in H\}| \cdot |K|
\end{aligned}
$$

不妨设存在对应关系 $\phi : h(H \cap K) \longmapsto hK, \forall h \in H$ 若 $h_1(H \cap K) = h_2(H \cap K)$, 则 $h_1^{-1}h_2 \in H \cap K$ 所以 $h_1^{-1}h_2 \in K$, 即 $h_1K = h_2K$, 所以 ϕ 是一个映射. 若 $h_1K = h_2K$, 则 $h_1^{-1}h_2 \in K$, 而 $h_1, h_2 \in H$, 所以 $h_1^{-1}h_2 \in H$, 即 $h_1^{-1}h_2 \in H \cap K$, 故 $h_1(H \cap K) = h_2(H \cap K)$, 所以 ϕ 是一个单射 $\forall h \in H, hK = \phi(h(H \cap K))$, 所以 ϕ 是一个满射 综上所述,ϕ 是从 $\{h(H \cap K) | h \in H\}$ 到 $\{hK | h \in H\}$ 的一个一一映射. 所以 $|\{hK | h \in H\}| =$

$|\{h(H\cap K)|h\in H\}|$

$$\begin{aligned}|HK| &= |\{hK|h\in H\}|\cdot|K|\\ &= |\{h(H\cap K)|h\in H\}|\cdot|K|\\ &= [H:H\cap K]\cdot|K|\\ &= |H||K|/|H\cap K|\end{aligned}$$

$\forall x\in HK, \exists h\in H, k\in K, s.t. x=hk\in G$ 所以 $|G|\geq|HK|=|H||K|/|H\cap K|$

Assignment 7

Problem 1

证明: 群 G 的中心 $C(G)$ 是 G 的正规子群.

解: $C(G)$ 是群 G 的子群结论在之前的作业中已经证明. 因为 $C(G)=\{a\in G\mid \forall g\in G, ag=ga\}$, 故 $\forall g\in G, \forall a\in C(G)$, 都有 $gag^{-1}=agg^{-1}=a\in C(G)$, 即 $gC(G)g^{-1}\subseteq C(G)$, 因此 $C(G)\lhd G$.

Problem 2

证明: 群的两个正规子群的交或者积都是正规子群.

解: 设群 G 的两个正规子群为 H, K.

两个正规子群的积仍然是子群: 显然 $HK=\{hk: h\in H, k\in K\}$ 是非空的. 对于任意 $h_1k_1, h_2k_2\in HK$, 都有 $h_1,h_2\in H$ 和 $k_1,k_2\in K$, 因此有 $(h_1k_1)(h_2k_2)^{-1}=h_1k_1k_2^{-1}h_2^{-1}$. 由于 $H\lhd G$, 故存在 $h_0\in H$, s.t. $k_1k_2^{-1}h_2^{-1}=h_0k_1k_2^{-1}$, 则 $(h_1k_1)(h_2k_2)^{-1}=h_1h_0k_1k_2^{-1}\in HK$, 故 HK 是 G 的子群. 则对任意 $g\in G$, $\forall hk\in HK$, 都有 $ghkg^{-1}=ghg^{-1}gkg^{-1}\in HK$ 成立, 故 HK 为 G 的正规子群;

显然, 子群的交仍然是子群, 故 $H\cap K<G$ 成立. 对任意 $g\in G$, $\forall x\in H\cap K$, 都有 $gxg^{-1}\in gHg^{-1}=H$, $gxg^{-1}\in gKg^{-1}=K$, 故 $gxg^{-1}\in H\cap K$, 故 $H\cap K$ 为 G 的正规子群.

Problem 3

设 G 为群, H 是 G 的子群. 定义 H 的正规化子 (normalizer) 为

$$N(H)=\{g\in G\mid gHg^{-1}=H\}.$$

证明: $N(H)$ 是 G 的子群, H 是 $N(H)$ 的正规子群.

解: 由于 $e \in N(H)$, 故 $N(H)$ 是非空的. 由 $N(H)=\{g\in G \mid gHg^{-1}=H\}=\{g\in G \mid H=g^{-1}Hg\}=\{g^{-1}\in G \mid gHg^{-1}=H\}$ 可知对任意 $g\in N(H)$ 都有 $g^{-1}\in N(H)$. 且 $\forall x,y\in N(H)$ 都有 $xyH(xy)^{-1}=xyHy^{-1}x^{-1}=xHx^{-1}=H$, 即 $xy\in N(H)$. 故 $N(H)$ 是 G 的子群;

$\forall g\in N(H)$ 都有 $gHg^{-1}=H$, 故 H 是 $N(H)$ 的正规子群.

Problem 4

设 G 为群, $H \triangleleft G$ 且 $[G:H]=m$. 证明: 对每个 $x\in G$ 都有 $x^m\in H$.

解: $H\triangleleft G$ 且 $[G:H]=m$ 可以得到商群 G/H, 且 $|G/H|=m$. 因此商群的任意元素 gH 的阶均整除 m, 即 $\operatorname{ord} gH \mid m$, 故 $(gH)^m=g^mH=H$, 故 $g^m\in H$ 成立.

Problem 5

设 H 是循环群 G 的子群. 证明: G/H 也是循环群.

解: 设 $G=\langle g\rangle$, 则 G 是交换群, 故 $H\triangleleft G$, G/H 是一个群; 那么 $\forall xH\in G/H$, 都有 $x=g^k$, 其中 $k\in\mathbb{Z}$, 则 $xH=g^kH=(gH)^k$, 因此 gH 是群 G/H 的生成元, 即 G/H 也是循环群.

Problem 6

设 $|G|=15$. 证明: 如果 G 有唯一的 3 阶子群和唯一的 5 阶子群, 则 G 是循环群. 将此结果推广到 $|G|=pq$ 的情况, 其中 p,q 为不同的素数.

解: (找到阶为 pq 的元素即可证明循环群) 假设 N 是唯一的 3 阶子群, H 是唯一的 5 阶子群, 故 $N\cap H=\{e\}$, 否则, 存在 $x\in N\cap H$, s.t. $\operatorname{ord}(x)\mid |N|=3$ 和 $\operatorname{ord}(x)\mid |H|=5$, 显然 $\operatorname{ord}(x)=1$, 即 $x=e$.

再证明 $nh=hn$, 其中 $n\in N$ 和 $h\in H$: 由于 $(hn^{-1}h^{-1})^3=e$ 且 N 是唯一的 3 阶子群, 故 $hn^{-1}h^{-1}\in N$, 那么 $nhn^{-1}h^{-1}\in N$. 同理 $nhn^{-1}\in H$, 故 $nhn^{-1}h^{-1}\in H$. 所以 $nhn^{-1}h^{-1}\in N\cap H$, 即 $nhn^{-1}h^{-1}=e$, $nh=hn$.

故 $\operatorname{ord}(nh)=15$, 其中 $n\in N$ 且 $h\in H$ 均非单位元.

给出 $|G|=pq$ 的情况: 假设 N 是唯一的 p 阶子群, H 是唯一的 q 阶子群, 则 $N\cup H$ 中的元素的阶有三种: $1,p,q$ 且元素数量为 $p+q-1<pq$. 因此存在 $x\in G\setminus(N\cup H)$, 显然 $\operatorname{ord} x\neq p,q,1$, 根据拉格朗日定理, G 的元素的阶有 $pq,p,q,1$ 这四种情况, 因此 $\operatorname{ord} x$ 只能为 pq, 即 $G=\langle x\rangle$.

Problem 7* (选做)

设 G 为交换群, $|G|=n$, m 是一个正整数. 证明: 如果 $m\mid n$, 则 G 有 m 阶子群.

解: $n=2$ 时结论成立; 假设结论对阶小于 n 的交换群成立, 则由柯西定理可知, 当 m 为素数时, G 有 m 阶子群, 结论成立; 当 m 不是素数时, 假设 $m=m'p$, 其中 p 是一个素数, 根据柯西定理可知存在 $a \in G$ s.t. $\operatorname{ord} a = p$, 则令 $H=\langle a\rangle$ 为循环群, 则 G/H 为交换群且 $|G/H| = n/p < n$, 那么根据归纳法可知商群 G/H 有阶为 m/p 的子群, 设为 N/H, 有 $N=\{n \in G \mid nH \in N/H\}$ 为所求, 其中 $|N| = m/p \cdot p = m$.

Theorem 1 (Cauchy theorem) *假设 G 是一个有限群, p 是一个素数. 如果 $p \mid |G|$, 那么 G 有阶为 p 的元素.*

Proof 1 *设集合*

$$X=\{(x_1,x_2,\ldots,x_p): x_1x_2\cdots x_p = e, x_i \in G, i=1,2,\ldots,p\}.$$

显然 $|X|=|G|^{p-1}$. 根据 X 的元素是否是循环移位得到的, 可以发现, 这 $|G|^{p-1}$ 个坐标可以划分成 2 种情况, 循环移位 1 次就是自身的 $(x,x,\ldots,x)$ 和循环移位 p 次才能回到自身的: 比如 $(x_1,x_2,\ldots,x_p) \to (x_2,x_3,\ldots,x_p,x_1) \to (x_3,x_4,\ldots,x_p,x_1,x_2) \to \cdots \to (x_p,x_1,x_2,\ldots,x_{p-1})$. 符合第一种情况的元素必然有 $(e,e,\ldots,e)$. 此外, 符合后一种情况的元素数量必然是 p 的倍数, 故不需要循环移位的元素数量是 $|G|^{p-1}-mp$, 同样是 p 的倍数, 即符合 $x^p=e$ 的元素数量大于 1. 又因为 $e^p=e$ 成立, 故存在非单位元 $x_0 \in G$, s.t. $x_0^p=e$.