NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Answer 5

2023 年 10 月 8 日

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

子群的判别条件:

Theorem 1 *设 G 是群, H 是群 G 的$\boxed{\text{非空子集}}$, 则 H 成为群 G 的子群的充分必要条件是*

(1) 对$\boxed{\text{任意}}$$a, b \in H$, 有 $ab \in H$;

(2) 对$\boxed{\text{任意}}$$a \in H$, 有 $a^{-1} \in H$.

上述验证子群的两个条件可以用一个条件代替:

Theorem 2 *设 G 是群, H 是群 G 的$\boxed{\text{非空子集}}$, 则 H 成为群 G 的子群的充分必要条件是对$\boxed{\text{任意}}$的 $a, b \in H$, 有 $ab^{-1} \in H$.*

上述两个子群判别定理中无子群运算结合律和单位元的验证.

Problem 1

在 $\mathbb{Z}_{10}$ 中, 令 $H = \{\overline{2}, \overline{4}, \overline{6}, \overline{8}\}$. 证明: H 关于剩余类的乘法构成群. H 是 $(\mathbb{Z}_{10}, \cdot)$ 的子群吗? 为什么?

解:

(1) 直接计算可以发现 H 关于剩余类的乘法是封闭的;

(2) 剩余类的乘法满足结合律, 所以 H 的乘法也满足结合律;

(3) 可以验证

$$\overline{2} \cdot \overline{6} = \overline{12} = \overline{2}$$
$$\overline{4} \cdot \overline{6} = \overline{24} = \overline{4}$$
$$\overline{6} \cdot \overline{6} = \overline{36} = \overline{6}$$
$$\overline{8} \cdot \overline{6} = \overline{48} = \overline{8}$$

故 $\overline{6}$ 是 H 的单位元;

(4) 从上述等式可以发现 H 中的每个元素都是可逆的.

综上 H 是一个群.

但 H 不是 $(\mathbb{Z}_{10},\cdot)$ 的子群: 因为 $(\mathbb{Z}_{10},\cdot)$ 不构成群 ($\bar{1}$ 是单位元, 但 $\bar{2}$ 无逆元).

Problem 2

设 $G=\mathrm{GL}_2(\mathbb{R})$, $H=\{A\in G\mid \det(A)\text{是 3 的整数幂次}\}$. 证明: H 是 G 的子群.

解: 显然 H 是 G 的非空集合. 假设任意 $A,B\in H$, 那么存在 $m,n\in\mathbb{Z}$ 使得 $\det(A)=3^m,\det(B)=3^n$. 因此

$$\det(AB^{-1})=\det(A)\det(B^{-1})=\det(A)\det(B)^{-1}=3^m3^{-n}=3^{m-n}.$$

故 $AB^{-1}\in H$, 因此 H 为 G 的子群.

Problem 3

设 G 是交换群, m 是固定的整数. 令 $H=\{a\in G\mid a^m=e\}$. 证明: H 是 G 的子群.

解: 因为 $e^m=e$ 故 $e\in H$, 即 H 是 G 的非空子集. 设任意 $a,b\in H$, 则 $a^m=b^m=e$. 因此

$$(ab^{-1})^m=a^m(b^{-1})^m=a^m(b^m)^{-1}=e.$$

故 $ab^{-1}\in H$, 因此 H 为 G 的子群.

Problem 4

设 H 是 G 的子群. 证明: 对任意的 $g\in G$, 集合 $gHg^{-1}=\{ghg^{-1}\mid h\in H\}$ 是 G 的子群.

解: 因为 $e\in H$, 则 $e=geg^{-1}\in gHg^{-1}$, 故 gHg^{-1} 非空. 此外 gHg^{-1} 是 G 的子集. 设任意的 $h_1,h_2\in H$, 故 $x=gh_1g^{-1}\in gHg^{-1},y=gh_2g^{-1}\in gHg^{-1}$. 因此

$$xy^{-1}=gh_1g^{-1}(gh_2g^{-1})^{-1}=gh_1g^{-1}gh_2^{-1}g^{-1}=gh_1h_2^{-1}g^{-1}\in gHg^{-1}.$$

其中 $h_1h_2^{-1}\in H$ 是因为 H 为 G 的子群. 故集合 $gHg^{-1}=\{ghg^{-1}\mid h\in H\}$ 是 G 的子群.

Problem 5

设 a 是群 G 的元素. 定义 a 在 G 中的中心化子 (centralizer) 为

$$C(a)=\{g\in G\mid ga=ag\}.$$

证明: $C(a)$ 是 G 的子群.

解: 显然 $e \in C(a)$, 故 $C(a)$ 是群 G 的非空子集. 假设任意 $g_1, g_2 \in C(a)$, 则 $g_1 a = a g_1, g_2 a = a g_2$, 整理得到 $g_1 g_2 a = g_1 a g_2 = a g_1 g_2$, 故 $g_1 g_2 \in C(a)$; 同时假设任意 $g \in C(a)$, 则 $ga = ag$, 整理得到 $g^{-1} g a = g^{-1} a g = a \Rightarrow g^{-1} a g g^{-1} = a g^{-1}$, 即 $g^{-1} a = a g^{-1}$, 故 $g^{-1} \in C(a)$. 因此, $C(a)$ 是 G 的子群.

Problem 6

设 G 的群. 证明: $C(G) = \bigcap_{a \in G} C(a)$ (即 G 的中心是所有形如 $C(a)$ 的子群的交).

解:

- $\subseteq$ 对任意 $x \in G$, $g \in C(G)$, 都有 $gx = xg$, 因此 $g \in C(x)$, 故 $C(G) \subseteq C(x)$, 由于 x 任意, 则 $C(G) \subseteq \bigcap_{x \in G} C(x)$;
- $\supseteq$ 设任意 $g \in \bigcap_{a \in G} C(a)$, 则 $g \in C(a)$, 其中 $a \in G$. 因此 $ag = ga$, 由于 a 任意, 则 $g \in C(G)$, 故 $\bigcap_{a \in G} C(a) \subseteq C(G)$.

综上, $C(G) = \bigcap_{a \in G} C(a)$.

Problem 7

设 G 的群, $a \in G$. 证明: $C(a) = C(a^{-1})$.

解: $\forall a, g \in G$, 有 $ag = ga \Leftrightarrow g a^{-1} = a^{-1} g$, 故

$$C(a) = \{g \mid ga = ag\} = \{g \mid g a^{-1} = a^{-1} g\} = C(a^{-1}).$$

Problem 8

设 H, K 是 G 的两个子群. 证明: 当且仅当 $H \subseteq K$ 或 $K \subseteq H$ 时, $H \cup K$ 是 G 的子群. 利用此结论证明, 群 G 不能被它的两个真子群所覆盖. G 能被它的三个真子群所覆盖吗?

解: 不是一般性的, 仅证明 $H \subseteq K$ 的情况.

充分性: 假设 $H \subseteq K$, 则 $H \cup K = K$ 显然是 G 的子群;

必要性: 假设 $H \cup K < G$. 如果 $H \subseteq K$, 则结论成立. 因此假设 $H \nsubseteq K$, 则假设 $h \in H \setminus K$, 故 $hkk^{-1} = h \in H$. 由 $H \cup K < G$, 有 $h \in H, k \in K$ 且 $hk \in H$ 或 $hk \in K$. 如果 $hk \in K$, 则 $h = hkk^{-1} \in K$ 与假设矛盾, 故 $hk \in H$, 故 $k = h^{-1} hk \in H$, 即 $K \subseteq H$.

如果 G 能被它的两个真子群覆盖, 那么假设为 $G = H \cup K$, 则 $G = H$ 或 $G = K$, 与真子群的性质矛盾, 故群 G 不能被它的两个真子群所覆盖.

G 能被它的三个真子群所覆盖, 举例:

1. 克莱因加法群 $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$, 三个真子群分别是 $\{(0,0),(0,1)\}$, $\{(0,0),(1,0)\}$ 和 $\{(0,0),(1,1)\}$.

2. $U(8) = \{\overline{1},\overline{3},\overline{5},\overline{7}\}$, 运算是剩余类的乘法, 其三个真子群分别是 $\{\overline{1},\overline{3}\}$, $\{\overline{1},\overline{5}\}$ 和 $\{\overline{1},\overline{7}\}$.

3. 可将 1 和 2 抽象为: $G = \{e,a,b,c\}$, 其中 e 为单位元, 运算满足 $a^2 = b^2 = c^2 = e$ 和 $ab = c$ (余下的 $ac = ca = b$ 等可由已知条件推导得到).

Problem 9

设群 K 由元素 a, b 和关系 $a^2 = b^2 = e, ab = ba$ 所定义. 试给出群 K 的乘法表 (乘法表定义见 Page 11).

解:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e