离散数学第十六次作业-群论导引

Problem 1

判断下列集合关于指定的运算是否构成半群, 独异点和群:

(1) a 是正实数, $G=\{a^n|n\in\mathbb{Z}\}$, 运算是普通乘法.

(2) $\mathbb{Q}^+$ 为正有理数, 运算是普通乘法.

(3) $\mathbb{Q}^+$ 为正有理数, 运算是普通加法.

(4) 一元实系数多项式的集合关于多项式的加法.

(5) 一元实系数多项式的集合关于多项式的乘法.

(6) $U_n=\{x|x\in\mathbb{C}\wedge x^n=1\}$, n 为某个给定正整数, $\mathbb{C}$ 为复数集合, 运算是复数乘法.

注: (4) (5) 两小题中, 形如 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, 只有 x 一个变元, 系数均为实数的多项式, 叫做一元实系数多项式.

答案:

	半群	独异点	群
(1)	√	√	√
(2)	√	√	√
(3)	√	×	×
(4)	√	√	√
(5)	√	√	×
(6)	√	√	√

Problem 2

$S=\{a,b,c\}$, $*$ 是 S 上的二元运算, 且 $\forall x,y\in S$, $x*y=x$.

(1) 证明 S 关于 $*$ 运算构成半群.

(2) 试判断 S 成为独异点的条件.

答案:

(1) 运算显然是封闭的. 因为 $\forall x, y, z \in S$, $(x * y) * z = x * y = x$ 且 $x * (y * z) = x * y = x$. 所以结合律成立. 综上, S 关于 $*$ 运算构成半群.

(2) 若存在 $e \in S$, 使得 e 为 S 中的单位元, 必有 $a * e = e * a = a$, 而 $\forall x, y \in S$, $x * y = x$, 那么 $e * a = e$, 于是得到 $e = a$. 因此如果存在单位元, 这个单位元必然与每个元素相同. 因此 S 成为独异点当且仅当 $a = b = c$.

Problem 3

设 A 是一个非空集合, 定义: $a \circ b = a, \forall a, b \in A$. 试证明: $\langle A, \circ \rangle$ 是一个半群.

答案: 显然 $\circ$ 是 A 上的二元运算. 对于任意的 $a, b, c \in A$, 由

$$(a \circ b) \circ c = a \circ c = a, a \circ (b \circ c) = a \circ b = a,$$

恒有

$$(a \circ b) \circ c = a \circ (b \circ c).$$

即结合律成立, 所以 $\langle A, \circ \rangle$ 是一个半群.

Problem 4

设 G 是一个群, 并且 $|G|$ 为偶数, 证明 G 中必定存在一个元素 g 满足 $g \neq e$ 且 $g = g^{-1}$

答案: 归谬法, 假定不存在这样的 g. 则每个非单位元元素都与其逆不同. 由条件知 G 有限, 则可以使用选择公理和群论公理, 每次从中取出一个非单位元元素和它的逆, 最终会只剩单位元 (因为逆元唯一, 不会剩余一个单位元和一个非单位元) . 那么 G 中有奇数个元素, 与条件矛盾.

直接使用配对法也可算对.

Problem 5

证明: 设 a 是群 $\langle G, \circ \rangle$ 的幂等元, 则 a 一定是单位元.

答案: 由条件有 $a \circ a = a$, 因为 G 是群, 任何一个元素都有逆元. 等式两边同乘 a 的逆元, 有

$$a^{-1} \circ (a \circ a) = a^{-1} \circ a.$$

由于运算可结合, 得到

$$a = e \circ a = (a^{-1} \circ a) \circ a = a^{-1} \circ (a \circ a) = a^{-1} \circ a = e.$$

即 a 一定是单位元.

Problem 6

(结合律) 假定集合 S 上定义的二元操作 $\circ$ 满足结合律. 我们知道二元操作只定义在两个元素上, 当参与运算的元素超过两个时, 会有很多种不同的顺序, 比如, 假定 $a, b, c, d \in S$, 那么可能会有的情况有

$$(a \circ b) \circ (c \circ d), (a \circ (b \circ c)) \circ d, a \circ ((b \circ c) \circ d)$$

等等, 注意到**每一步只进行一次运算**. 证明：无论我们怎么放置括号, 这种嵌套运算的最终结果是不变的. 即证明对 $s_1 s_2 ... s_n \in S$, 任意括号嵌套顺序下的结果都等同于 $((...((s_1 \circ s_2) \circ s_3)...) \circ s_n)$.

(提示：使用数学归纳法, 基础情况是 $n = 2$, 手动尝试一下从 $n = 4$ 到 $n = 5$ 的情况).

答案：对 n 进行归纳, $n = 2$ 时, 只有一种情况, 得证.

归纳假设在 $n = k$ 时, 结论成立. 尝试证明 $n = k + 1$ 的情况.

由于每一步只进行一次运算, 考虑最先进行的运算, 设为 $(s_i \circ s_{i+1})$, 其中 $1 \leq i \leq k$. 设 $(s_i \circ s_{i+1}) = s_j \in S$.

应用归纳假设,

$$\begin{aligned} \text{原式} &= (...((...((s_1 \circ s_2) \circ s_3)... \circ s_j) \circ s_{i+2})...s_{k+1}) \\ &= (...((...((s_1 \circ s_2) \circ s_3)... \circ (s_i \circ s_{i+1})) \circ s_{i+2})...s_{k+1}) \\ &= (...((...((s_1 \circ s_2) \circ s_3)... \circ s_i) \circ s_{i+1})...s_{k+1}) \end{aligned}$$

得证

Problem 7

证明对任意群 G 以及 $g, h \in G$ 我们有 $(gh)^{-1} = h^{-1}g^{-1}$. 对于正整数 n, 给出 $(g_1 g_2 ... g_n)^{-1}$ 的一个形式.

答案:

$$gh(h^{-1}g^{-1}) = geg^{-1} = e$$

$$(g_1 g_2 ... g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} ... g_1^{-1}$$

Problem 8

(数论) 我们知道, 在整数集合 Z 上的同余关系是一个等价关系. 我们用记号 $[a]_n$ 表示 a 的模 n 同余类. 即

$$b \in [a]_n \Leftrightarrow a \equiv b \pmod{n}.$$

模 n 同余类构成的集合是一个重要的概念, 有许多记法, 例如 $\mathbb{Z}_n, \mathbb{Z}/n\mathbb{Z}$ 等. 例如 $\mathbb{Z}/n\mathbb{Z} = \{[0]_2, [1]_2\}$. 对于正整数 n, 我们记扩展的加法为

$$[a]_n + [b]_n := [a + b]_n.$$

易证 $\mathbb{Z}_n$ 在扩展加法下构成一个群. 类似地, 扩展乘法为

$$[a]_n \times [b]_n := [a \times b]_n.$$

现在令 $\mathbb{Z}_n^* := \{[m]_n \in \mathbb{Z}_n | \gcd(m, n) = 1\}$. 证明: $\mathbb{Z}_n^*$ 在扩展乘法下构成一个群.

答案: 首先, 我们有 $m \equiv m' \pmod{n} \wedge l \equiv l' \pmod{n} \Rightarrow ml \equiv m'l' \pmod{n}$, 故扩展乘法为良定义的操作. 对任意 $[m]_n, [l]_n \in \mathbb{Z}_n^*$, 我们有 $\gcd(m, n) = 1, \gcd(l, n) = 1$, 所以 $\gcd(lm, n) = 1$. 因此扩展乘法在 $\mathbb{Z}_n^*$ 上封闭. 由乘法结合性可以直接得到扩展乘法的结合性. 单位元为 $[1]_n$ 对任意 $[m]_n \in \mathbb{Z}_n^*$, 由贝祖定理, 因为 $\gcd(m, n) = 1$, 故存在 k, r 使得 $km + rn = 1$, 即 $[k]_n \times [m]_n = [km]_n = [1]_n$, 存在逆元.

Problem 7

设 $i = \sqrt{-1}$, $S = \{1, -1, i, -i\}$, 证明 $\langle S, * \rangle$ 构成群, 其中 $*$ 为复数域上的乘法运算.

答案: $V = \langle S, * \rangle$ 是代数系统. 任意复数 $a, b, c \in S$, 有 $(a * b) * c = a * (b * c)$, 则 V 为半群. 任意复数 $a \in S$, 有 $1 * a = a * 1 = a$, 则 $1 \in S$ 是关于 $*$ 运算的单位元. $\forall a \in S$, 有 $aa^{-1} = e = 1$, 则 $a^{-1} \in S$. 综上, $\langle S, * \rangle$ 构成群.

Problem 10

证明: G 为交换群当且仅当 $\forall a, b \in G$, 有 $(ab)^2 = a^2b^2$.

答案: 充分性: $(ab)^2 = a^2b^2$, 即 $(ab)(ab) = (aa)(bb)$, 由结合律得: $a(ba)b = a(ab)b$, 由消去律得 $ba = ab$.

必要性: G 是交换群, 因此 $\forall a, b \in G$, 有 $ab = ba$, 那么

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = a^2b^2$$