离散数学（2024）作业 18 - 群论导引

离散数学教学组

Problem 1

判断下列集合关于指定的运算是否构成半群和群：

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

「**提示：**(4)(5) 两小题中，形如 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$，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	群
1	$\surd$	$\surd$
2	$\surd$	$\surd$
3	$\surd$	$\times$
4	$\surd$	$\surd$
5	$\surd$	$\times$
6	$\surd$	$\surd$

Problem 2

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

答案：

- 显然 $*$ 是 S 上封闭的二元运算。
- 任意复数 $a, b, c \in S$，有 $(a * b) * c = a * (b * c)$，满足结合律。
- 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，$(S, *)$ 构成群。

Problem 3

设 $(G, *)$ 是一个群，$x \in G$。定义：$a \circ b = a * x * b, \forall a, b \in G$，证明 $(G, \circ)$ 也是群。
答案：

- 显然 $\circ$ 是 G 上封闭的二元运算。
- $\forall a, b, c \in G$，有 $(a \circ b) \circ c = (a * x * b) * x * c = a * x * (b * x * c) = a \circ (b \circ c)$，运算是可结合的。
- $\forall a \in G$，易证 $a \circ x^{-1} = x^{-1} \circ a = a$，所以 x^{-1} 是 $(G, \circ)$ 上的单位元。
- $\forall a \in G$，易证 $a \circ (x^{-1} * a^{-1} * x^{-1}) = (x^{-1} * a^{-1} * x^{-1}) \circ a = x^{-1}$，故 a 的逆元为 $x^{-1} * a^{-1} * x^{-1}$。

综上得证。

Problem 4

证明：设 a 是群 $(G, \circ)$ 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 5

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：

- 由 $gh(h^{-1}g^{-1}) = geg^{-1} = e$ 得证。
- $(g_1 g_2 ... g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} ... g_1^{-1}$

Problem 6

设 G 是一个群，$a, b \in G$ 且 $(ab)^2 = a^2 b^2$。证明：$ab = ba$。
答案： 充分性：$(ab)^2 = a^2 b^2$, 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

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

Problem 7

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： 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。

Problem 8

设 G 是一个有限群，证明：G 中使得 $x^3 = e$ 的元素 x 的个数是奇数。
答案： 令 $S = \{x \in G \mid x^3 = e\}$。由于 G 是有限群，所以 S 为有限集。又因为 $e^3 = e$，所以 $e \in S$，从而 S 不是空集。如果令有 $x \neq e$，使得 $x^3 = e$，则 $(x^{-1})^3 = e$。因为 $x \neq e$，所以 $x^{-1} = x$。这说明 S 中的非单位元（如果有的话）总是成对出现。又因为 $e^3 = e$，所以 G 中使得 $x^3 = e$ 的元素个数是奇数。

Problem 9

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 10

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 $m \equiv m' \pmod n \wedge l \equiv l' \pmod n \Rightarrow ml \equiv m'l' \pmod n$。又因为对任意 $[m]_n, [l]_n \in \mathbb{Z}_n^*$，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。

综上得证。