Problem Set 18: 群论导引

提交截止时间：5 月 13 日 10:00

Problem 1

判断下列集合关于指定的运算是否构成半群, 幺半群和群：

1. a 是正实数, G = {a^n |n ∈ Z}, 运算是普通乘法.
   封闭性：存在，$\forall x, y \in Z, a^x \circ a^y = a^{m+n} \in G$
   结合性：存在，$\forall x, y, z \in Z, (a^x \circ a^y) \circ a^z = a^{x+y+z} = a^x \circ (a^y \circ a^z)$
   单位元：存在，$\forall x \in Z, a^0 \circ a^x = a^x$,故$a^0$为单位元
   可逆性：存在，$\forall x \in Z, a^x \circ a^{-x} = a^0 = e$

```
故<G, *>为群
```

2. Q+ 为正有理数, 运算是普通乘法.
   封闭性： 存在，∀ x, y ∈ Q+, x ∘ y = x * y ∈ G
   结合性： 存在，∀ x, y, z ∈ Q+, (x ∘ y) ∘ Q+ = x * y * z = x ∘ (y ∘ z)
   单位元： 存在，∀ x ∈ Q+, 1 ∘ x = x, 故1为单位元
   可逆性： 存在，∀ x ∈ Q+, x ∘ 1/x = 1 = e

```
故<Q+, *>为群
```

3. Q+ 为正有理数, 运算是普通加法.
   封闭性： 存在，∀ x, y ∈ Q+, x ∘ y = x + y ∈ G
   结合性： 存在，∀ x, y, z ∈ Q+, (x ∘ y) ∘ Q+ = x + y + z = x ∘ (y ∘ z)
   单位元： 不存在，∀ x ∈ Q+, 0 ∘ x = x, 故0为单位元，但0 ∉ Q+

```
故<Q+, +>为半群
```

4. 一元实系数多项式的集合关于多项式的加法.
   令$f(a) = \sum_{i=0}^{n} a * x^i (a \in R)$
   封闭性：存在，$f(a) \circ f(b) = f(a+b)$
   结合性：存在，$\forall x, y, z \in Q+, (f(x) \circ f(y)) \circ f(z) = f(x) \circ f(y) \circ f(z) = f(x) \circ (f(y) \circ f(z))$
   单位元：存在，$\forall x \in Q+, f(0) \circ f(x) = f(x)$
   可逆性：存在，$\forall x \in Q+, f(x) \circ f(-x) = 1 = e$

```
故<Y, +>为群
```

5. 一元实系数多项式的集合关于多项式的乘法.
   令$f(a) = \sum_{i=0}^{n} a_i * x^i (a_i \in R)$
   封闭性：存在，$f(a) \circ f(b) \in Y$
   结合性：存在，$\forall x, y, z \in R, (f(x) \circ f(y)) \circ f(z) = f(x) \circ f(y) \circ f(z) = f(x) \circ (f(y) \circ f(z))$
   单位元：存在，$\forall x \in R, 1 \circ f(x) = f(x)$,故1为单位元
   可逆性：不存在，找不到一个一元实系数多项式x使得$x \circ f(a) == 1$

$6.U_n = x|x \in C \wedge x^n = 1, n$为某个给定正整数,$C$为复数集合,运算是复数乘法.
封闭性：存在，$\forall a, b \in U, a \circ b = c, c^n = a^n * b^n$
结合性：存在，$\forall x, y, z \in U, (a \circ b) \circ c = a * b * c = a \circ (b \circ c)$
单位元：存在，$\forall x \in R, 1 \circ f(x) = f(x)$,故1为单位元
可逆性：存在，$\forall x \in C, \exists 1/x \in U, x \circ 1/x = 1$

```
故<U, *>为一个群
```

Problem 2

S = {a, b, c}, ∗ 是 S 上的二元运算, 且 ∀x, y ∈ S, x ∗ y = x.

1. 证明 S 关于 ∗ 运算构成半群.
   封闭性： 存在，∀ x, y ∈ S, x ∘ y = x, x ∈ S
   结合性： 存在，∀ x, y, z ∈ U, (a ∘ b) ∘ c = a = a ∘ (b ∘ c)

```
故<S, *>为一个半群
```

2. 试判断 S 成为幺半群的条件.

```
若a = e, 则 a ∘ b = a, b ∘ a = b, a = b
又因为a的任意性，所以S任何条件下都不存在单位元
```

Problem 3

证明：有单位元且满足消去律的有限半群一定是群。

```
由题意可知，该群是幺半群
又因为∀a, b ∈ G, a ∘ b = a ∘ c -> b = c
所以∃ x, x ∘ a ∘ b = x ∘ a ∘ c = b = c
故x ∘ a = e
所以x为a的逆元，存在可逆性
故命题得证
```

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$g! = e$且$g = g^{-1}$

```
令 S = {x | ∀ x ∈ G, x != e, ∃ y ∈ G, x != y, x ∘ y = e}
显然|S|为偶数且e ∉ S,
又因为|G|为偶数
则∃ y ∈ G, y ∉ S ∧ y != e ∧ y = y ^ (-1)
```

Problem 5

证明：设 a 是群 ⟨G, ∘⟩ 的幂等元, 则 a 一定是单位元. 注：a 为群 ⟨G, ∘⟩ 的幂等元指 a ∘ a = a

```
a ∘ a = a = a ∘ e
根据消去律
a = e
```

Problem 6

(结合律) 假定集合 S 上定义的二元操作∘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 ∈ S, 那么可能会有的情况有
a∘b. ∘c∘d. , a∘(b∘c.)∘d, a∘(b∘c. ∘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
s1 s2 ...sn ∈ S, 任意括号嵌套顺序下的结果都等同于 (...((s1∘s2 . ∘s3)...)∘sn).
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. .

```
当 n = 2 时。由于∘ 满足结合律，所以 (a1 ∘ a2) 的结果不变

假设对于任意的 k 个元素的序列 a1, a2, ..., ak，无论如何放置括号，嵌套运算结果都是相同

一个包含 k+1 个元素的序列 a1, a2, ..., ak+1这个序列可以被划分成两个部分(a1, a2, ..., ai) 和 (ai+1, ai+2, ..., ak+1),
根据假设，对于这两个部分的嵌套运算，无论如何放置括号，其结果都是相同的。
由于二元操作 ∘ 满足结合律，将这两个结果进行一次运算所得到的结果也是不变的。
因此，无论如何放置括号，整个序列 a1, a2, ..., ak+1 的嵌套运算的结果都是相同的。
```

Problem 7

(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
$b \in [a]_n \Leftrightarrow a \equiv b(modn)$
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Z^n, Z/nZ等. 例如$Z/nZ = [0]_2, [1]_2$. 对于正整数n,
我们记扩展的加法为
$[a]_n + [b]_n := [a+b]_n$.
易证Zn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$Z_n^* := [m]_n \in Z_n | gcd(m,n) = -1$. 证明：$Z_n^*$在扩展乘法下构成一个群.

封闭性：对任意$[m]_n, [l]_n \in Z_n^*$, 有$gcd(m,n) = 1, gcd(l,n) = 1$, 所以$gcd(lm,n) = 1$.因此扩展乘法在$Z_n^*$上封闭
结合性：由乘法结合性可以直接得到扩展乘法的结合性.
单位元：单位元为$[1]n$对任意$[m]n \in Z_n^*$, 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

Problem 8

对没有单位元的半群 M , 是否一定能在其中加入一个新元素 e 使得 M ∪ {e} 是含有单位元 e 的半群?

```
S = {a, b, c}, ∗ 是 S 上的二元运算, 且 ∀x, y ∈ S, x ∗ y = x.
由第二题可知
<S, *>无法加入一个新元素，使之成为幺半群。
```

Problem 9

设 M 是有单位元 e 的半群, a, b 是 M 中的可逆元, 试证 ab 也是 M 的可逆元。

```
因为a, b 为M中的可逆元，所以 a ^ (-1) ∈ M ∧ b ^ (-1) ∈ M
所以b ^ (-1) ∘ a ^ (-1) ∈ M
故(ba) ^ (-1) ∈ M
又因为ab ∘ (ba) ^ (-1) = e
所以ab也是可逆元
```