离散考前练习

1、Solve the recurrence relation $a_n=a_{n-1}+a_{n-2}$ with $a_0=a_1=1$ using generating function.

2、Determine the number of the terms in the expansion of

$(x_1+x_1+\cdots+x_{10})^{20}$.

3、将 m 个无区别的球，放入 n 个有区别的盒子，在允许有空盒和不允许有空盒两种情况下分别讨论可能的放法数。

4、求 n 元集合到 m 元集合单射、满射、双射的个数。

5、用容斥原理求 1~n 中与 n 互素的元素个数。

6、<G,*>是个群，x∈G，定义 G 中的运算“Δ”为 aΔb=a*x*b，对∀a,b∈G，证名<G, Δ>也是群。

证明：1）∀a,b∈G，aΔb=a*x*b∈G，运算是封闭的。

2）∀a,b,c∈G，（aΔb）Δc=（a*x*b）*x*c=a*x*（b*x*c）=aΔ（bΔc），运算是可结合的。

3）∀a∈G，设 E 为Δ的单位元，则 aΔE=a*x*E=a，得 $E=x^{-1}$，存在单位元。

4）∀a∈G，aΔ $x^{-1}*a^{-1}*x^{-1}=a*x*x^{-1}*a^{-1}*x^{-1}=x^{-1}=E$，

$x^{-1}*a^{-1}*x^{-1}$Δ a = $x^{-1}*a^{-1}*x^{-1}*x*a=x^{-1}=E$，a 的逆元为 $x^{-1}*a^{-1}*x^{-1}$，每个元素都有存在。所以<G, Δ>也是个群

7、设<G,*>是有限交换群，a,b∈G，|a|=m,|b|=n,m,n 是整数，且 GCD（m,n）=1 即 m,n 互素，证明：|ab|=mn

证明：设|ab|=k，因为$(ab)^{mn}$= (ab)(ab)…(ab)=$(a^m)^n(b^n)^m$=e,所以 k|mn,

e=$((ab)^k)^m=(ab)^{km}=(a^{km})(b^{km})=b^{km}$, 所以 n|km,由于 GCD（m,n）=1，所以 n|k

同理可求，所以 m|k.

所以有 mn|k，mn=k ,|ab|=mn

8、设<S，+，•>是环，1 是其乘法幺元，在 S 上定义运算 □ 和 □：

$a\oplus b=a+b+1$，$a\odot b=a+b+a\cdot b$。

（1）证明<S，⊕，⊙>是一个环。

（2）给出<S，⊕，⊙>的关于运算 ⊕ 和 ⊙ 的单位元。

证明：（1）对任意 a、b、$c\in S$,

则（$a\oplus b$）$\oplus c=a\oplus b+c+1=a+b+c+1+1$,

$a\oplus$（$b\oplus c$）$=a+b\oplus c+1=a+b+c+1+1$,

于是（$a\oplus b$）$\oplus c=a\oplus$（$b\oplus c$），即⊕满足结合律。

$a\oplus b=a+b+1=b+a+1=b\oplus a$，所以⊕是可交换的。

$a\oplus$（-1）$=a+$（-1）$+1=a=$（-1）$\oplus a$,

所以-1 是 ⊕ 单位元。

$a\oplus$（$-1-1-a$）$=a+$（$-1-1-a$）$+1=-1=$（$-1-1-a$）$\oplus a$,

所以$-1-1-a$ 是 a 的逆元。

综上可知，<S，⊕>是一个交换群。

（2）（$a\odot b$）$\odot c=a\odot b+c+$（$a\odot b$）$\cdot c=a+b+a\cdot b+c+$（$a+b+a\cdot b$）$\cdot c$

$=a+b+a\cdot b+c+a\cdot c+b\cdot c+a\cdot b\cdot c$

$a\odot$（$b\odot c$）$=a+b\odot c+a\cdot$（$b\odot c$）

$=a+b+c+b\cdot c+a\cdot$（$b+c+b\cdot c$）

$=a+b+c+b\cdot c+a\cdot b+a\cdot c+a\cdot b\cdot c$

所以（$a\odot b$）$\odot c=a\odot$（$b\odot c$），即⊙满足结合律。

又 $a\odot 0=a+0+a\cdot 0=a$，

$0\odot a=0+a+0\cdot a=a$，

0 是 ⊙ 单位元

因而〈S，⊙〉是有幺元的半群。

a⊙（b⊕c）＝a＋b⊕c＋a·（b⊕c）

＝a＋b＋c＋1＋a·（b＋c＋1）＝2a＋b＋c＋a·b＋a·c＋1

（a⊙b）⊕（a⊙c）＝a⊙b＋a⊙c＋1＝a＋b＋a·b＋a＋c＋a·c＋1

＝2a＋b＋c＋a·b＋a·c＋1

a⊙（b⊕c）＝（a⊙b）⊕（a⊙c），

所以 ⊙ 对 ⊕ 满足分配律。

从而<S，⊕，⊙>是一个环。

9、设 G 是一个群,e 是 G 的单位元,H 是 G 的子群. 如下定义关系 R：$\forall a_1,a_2 \in G, < a_1,a_2 > \in R \Leftrightarrow a_1ea_2^{-1} \in H.$ 证明 R 是 G 上的等价关系.

证明: 对于任意的 a∈G，∵ $aea^{-1}=e\in H$， ∴ <a,a> ∈ R，故 R 是自反的。

对于任意的 a，b∈G，若<a,b>∈ R，

∴ $aeb^{-1}\in H$，∴$(aeb^{-1})^{-1}=(ab^{-1})^{-1}=ba^{-1}\in H$，

∴ <b,a> ∈ R，故 R 是对称的。

对于任意的 a,b,c∈G，若<a,b> ∈ R，<b,c> ∈ R， ∴ $aeb^{-1}\in H$ 且 $bec^{-1}\in H$，

∴ $(aeb^{-1})(bec^{-1})=ac^{-1}\in H$， ∴ <a,c> ∈ R，故 R 是传递的

10、<G,*>是个群，u∈G，定义 G 中的运算“Δ”为 $a\Delta b=a*u^{-1}*b$，对任意 a,b∈G，求证：<G, Δ>也是群。

证明：1）∀a,b∈G，$a\Delta b=a*u^{-1}*b\in G$，运算是封闭的。

2）∀a,b,c∈G，（aΔb）Δc=（$a*u^{-1}*b$）$*u^{-1}*c=a*u^{-1}*$（$b*u^{-1}*c$）=aΔ（bΔc），运算是可结合的。

3）∀a∈G，设 E 为Δ的单位元，则 $a\Delta E=a*u^{-1}*E=a$，得 E=u，存在单位元。

4）∀a∈G，$a\Delta x=a*u^{-1}*x=E$，$x=u*a^{-1}*u$，则 $x\Delta a=u*a^{-1}*u*u^{-1}*a=u=E$，每个元素都有逆元。

所以<G, Δ>也是个群

11、证明有限群中阶（周期）大于 2 的元素的个数必定是偶数。

证明 x 与其逆元 x-1 的周期相同，又当 x 的周期大于 2 时，x≠x-1。定义映射 f: x→x-1,是群中的双射函数，所以阶大于 2 的元素成对出现（x 与其逆元 x-1 是一对），故其个数必定是偶数。

12、 证明 n 阶循环群的子群的个数恰为 n 的正因子数。

证明：对 n 的每一正因子 d，令 $k=\frac{n}{d}$, $b=a^k$, $H=\{e, b, b^2, \cdots, b^{d-1}\}$。

因为$|a|=n$,所以 $b^d=(a^k)^d=a^{kd}=a^n=e$ 且$|b|=d$。

从而 H 中的元素是两两不同的，易证 H≤G。

故$|H|=d$。所以是 G 的一个 d 阶子群。

设 H_1是 G 的任一 d 阶子群。则由定理 5.4.4 知，$H_1=(a^m)$，其中 a^m是 H_1中 a 的最小正幂，且$|H|=\frac{n}{m}$。因为$|H|=d$，所以 $m=\frac{n}{d}=k$，即 $H=H_1$。从而 H 是 G 的惟一 d 阶子群。

13、证明：对于剩余环〈Zn，＋n，×n 〉，n 是素数当且仅当 Zn 中无零因子。

证明：（1）⇐

设 $\mathbf{Z}_n$ 中无零因子，往证 n 是素数。假设 n 不是素数，则存在整数 n_1，n_2，使

$$n=n_1n_2 \qquad 1<n_1\leq n_2<n$$

因此 $[n_1]\neq[0]$，$[n_2]\neq[0]$，但 $[n_1]\times_n[n_2]=[0]$. 即 $[n_1]$，$[n_2]$ 是 $\mathbf{Z}_n$ 的一对零因子，矛盾。所以，n 是素数。

（2）⇒

设 n 是素数，若〈$\mathbf{Z}_n$，$+_n$，$\times_n$〉中有零因子 $[i]$，$[j]\in\mathbf{Z}_n$，使得 $[i]$，$[j]\neq[0]$，$[i]\times_n[j]=[0]$，则 $[ij]=[0]$，因而 $n\mid ij$. 由于 n 是素数，故 $n\mid i$ 或 $n\mid j$. 即 $[i]=[0]$ 或 $[j]=[0]$，矛盾。所以，〈$\mathbf{Z}_n$，$+_n$，$\times_n$〉中无零因子。

14、假设<X,*>是一个代数系统，*是 X 上的二元运算。如果*运算是可结合的，并且对任意的 x,y∈X，当 x*y=y*x 时，有 x=y。证明 X 中每个元素都是幂等元。

证明：对任意的元素 x∈X，由于*运算可结合，所以有 (x*x)*x=x*(x*x)

由题设条件可知 x*x=x

由 x 的任意性则每个元素都是等幂元。

15、假设<X,⊕,⊗>是一个代数系统，⊕和⊗分别是 X 上的二元运算。若对任意的 x,y∈X，有 x⊕y=x。证明：⊗对于⊕是可分配的。

证明：对任意的 x,y,z∈X，

$x\otimes(y\oplus z)=x\otimes y$

$\quad= (x\otimes y)\oplus(x\otimes z)$

而 $(y\oplus z)\otimes x=y\otimes x$

$= (y\otimes x)\oplus(z\otimes x)$

证毕。

16、假设<X,*>和<Y, ⊗>是两个代数系统，*和⊗分别是 X 和 Y 上的二元运算，并且满足结合律和交换律。f1 和 f2 都是代数系统 X 到 Y 的同态映射。令：$h:X\to Y$，对任意的 $x\in X$，$h(x)=f1(x)\otimes f2(x)$。证明 h 是代数系统 X 到 Y 的同态映射

证明：由 h 的定义可知 h 是 X 到 Y 的函数

对任意的 $x,y\in X$

$h(x*y)=f1(x*y)\otimes f2(x*y)$

$=(f1(x)\otimes f1(y))\otimes(f2(x)\otimes f2(y))$

由于运算⊗满足结合律和交换律，

所以上式 $=(f1(x)\otimes f2(x))\otimes(f1(y)\otimes f2(y))=h(x)\otimes h(y)$

h 对于运算保持。

所以 h 是代数系统 X 到 Y 的同态映射。

证毕

17、假设<G,*>是一个群，|G|=2n。证明 G 中至少有一个周期为 2 的元素。

证明：因为群<G,*>中的元素互逆，即元素 a 的逆元是 a’，a’的逆元是 a。因而 G 中逆元不等于自身的元素必为偶数个（包括零个）。

但是 G 包含偶数个元素，因此 G 的逆元等于自身的元素个数也必为偶数个，而 G 的单位元 e 的逆元是其本身，所以 G 中至少还有另一个元素 a 其逆元是它本身，即 $a^{-1}=a$。

从而 $a^2=a*a=a*a^{-1}=e$，并且 $e\neq a$。

即 a 是一个周期为 2 的元素

所以至少存在一个周期为 2 的元素。

18、已知 G={1,2,3,4,5,6}，$\times_7$为模 7 乘法，试说明<G, $\times_7$>是否构成群？是否为循环群？若是，生成元是什么？它是否有子群？若有，子群是什么？

解：列出运算表如下：

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

由运算表和模 7 乘法的性质可知<G,$\times_7$>是群。是循环群，生成元是 3，5。

它有子群，子群是：< G,$\times_7$>，< {1},$\times_7$>，< {1,6},$\times_7$>，< {1,2,4},$\times_7$>

19、假设 f, g 是群<X, *>到群<Y, ⊗>的同态映射。证明<H, *>是群<X, *>的子群，其中 H={x|x∈X ,并且 f(x)=g(x)}。

证明：由 H 的定义可知 H⊆X。假设 e_x 是群<X,*>的单位元，e_y 是<Y, ⊗>的单位元　　由 f,g 是群<X,*>到群<Y, ⊗>的同态映射可知 $f(e_x)= e_y=g(e_x)$　　从而 $e_x\in H$，故 H 非空。对于任意的 a, b∈H，则有 f(a)=g(a)，f(b)=g(b)

由 f,g 是群<X,*>到群<Y, ⊗>的同态映射可知 $f(b^{-1})=(f(b))^{-1}=(g(b))^{-1}=g(b^{-1})$

因此 $f(a*b^{-1})=f(a)\otimes f(b^{-1})=g(a)\otimes g(b^{-1})=g(a*b^{-1})$

所以 $a*b^{-1}\in H$

因此<H,*>是群<X,*>的子群。

证毕。

20、假设<X, *>是一个代数系统，*是 X 上的二元运算。对任意的 x, y, z, w∈X，有 x*x=x，并且(x*y)*(z*w)=(x*z)*(y*w)。证明：x*(y*z)=(x*y)*(x*z)

证明：对任意的 x,y,z∈X

有 x*x=x

所以 x*(y*z)= (x*x)*(y*z)=(x*y)*(x*z) （由已知条件）

证毕。

21、假设 S={a,b,c}，X=<{∅,S},∩,∪,~>，Y=<{{a,b},S},∩,∪,~>。二元运算符∩,∪和一元运算符~分别是集合的交、并、补运算。问 X 和 Y 是否同构？为什么？

答：X 和 Y 不同构。因为 Y=<{{a,b},S},∩,∪,~>不是代数系统，补运算~关于集合{{a,b},S}不封闭。如果存在 X 和 Y 同构，则 X 是代数系统，Y 一定是代数系统。由上可知产生矛盾。

22、假设<G, *>是一个群。证明对于任意的 a, b∈G，存在唯一的 x∈G，使得 a*x=b。

证明：由于<G,*>是一个群，所以对于任意元素 $a,b\in G$，逆元 $a'\in G$ 存在，并且

$x=a'*b\in G$，使得 $a*x=a*(a'*b)=(a*a')*b=b$

假若还存在另一个元素 $c\in G$，使得 $a*c=b$

则 $c=e*c=(a'*a)*c=a'*(a*c)=a'*b=x$

所以 x 唯一。

证毕。

23、设<S,*>是一个含幺半群，e 是单位元。证明若任意的 $x\in S$，有 $x*x=e$，则<S,*>是阿贝尔群。

证明：对于任意的 $x\in S$，有 $x*x=e$，因此 $x^{-1}=x$，所以<S,*>是群。

对任意的 $x,y\in S$

$x*y= x^{-1}*y^{-1}=(y*x)^{-1}=y*x$

所以<S,*>是阿贝尔群

证毕。

24、已知 G={0,1,2,3,4,5}，$+_6$为模 6 加法，试说明<G,$+_6$>是否构成群？是否为循环群？若是，生成元是什么？它是否有子群？若有，子群是什么？

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

解：由运算表和模 6 加法的性质可知<G,$+_6$>是群。是循环群，生成元是 1，5。

它有子群，子群是：< G,$+_6$>，< {0},$+_6$>，< {0,3},$+_6$>，< {0,2,4},$+_6$>

25、假设<G,*>是群，C={a | a∈G, 并且对 $\forall x\in G$, $a*x = x*a$}，证明<C,*>是<G,*>的子群。

证明：（1）因为<G,*>是群，所以存在单位元 e。

对 $\forall x\in G$，有 $e*x = x*e = x$

所以 $e\in C$，即 C 是非空的。

又由 C 的定义可知：$C\subseteq G$。

（2）对 $\forall a,b\in C$，有 $a*x = x*a$ 和 $b*x = x*b$

而 $(a*b)*x = a*(b*x) = a*(x*b) = (a*x)*b = (x*a)*b = x*(a*b)$

所以 $a*b\in C$

又对 $\forall a\in C$，有 $a*x = x*a$

又有 $a^{-1}*a*x = a^{-1}*x*a$ 所以 $x = a^{-1}*x*a$

而 $x*a^{-1}= a^{-1}*x*a*a^{-1} = a^{-1}*x$

所以 $a^{-1} \in C$