● 填空题：

1、设 A={2,4,6}，A 上的二元运算*定义为：a*b=max{a,b}，则在独异点<A,*>中，单位元是(　　)，零元是(　　)。

答：2，6

2、设 A={3,6,9}，A 上的二元运算*定义为：a*b=min{a,b}，则在独异点<A,*>中，单位元是(　　)，零元是(　　)；

答：9，3

3、设 a 是 12 阶群的生成元， 则 a^2 是(　　)阶元素，a^3 是(　　)阶元素。

答： 6,4

4、群<G,*>的幂等元是(　　)，有(　　)个。

答：单位元，1

5、设 a 是 10 阶群的生成元， 则 a^4 是(　　)阶元素，a^3 是(　　)阶元素。

答：5，10

6、素数阶群一定是(　　)群，它的生成元是(　　)。

答：循环群，任一非单位元

7、<H,,∗>是<G,,∗>的子群的充分必要条件是(　　)。

答：<H,,∗>是群 或 $\forall a, b \in G$，$a*b\in H$，$a^{-1}\in H$ 或 $\forall a,b \in G$，$a*b^{-1}\in H$

8、在一个群〈G,*〉中，若 G 中的元素 a 的阶是 k，则 a^{-1} 的阶是(　　)。

答：k

9、在自然数集 N 上，下列哪种运算是可结合的？（　　）

(1) a*b=a-b　(2) a*b=max{a,b}　(3) a*b=a+2b　(4) a*b=|a-b|

答：(2)

10、设 G 是所有 3 位二进制数构成的集合，关于异或运算，G 中的幺元是（　　），011 的逆元是（　　）。

答：000，011

11、10 阶群的子群的阶数只可能是（　　）。

答：1,2,5,10

12、设 G 是群，a∈G，若|a|=12，则$|a^9|$=（　　）。

答：4

13、设 A 是集合，P(A)是 A 的幂集，则代数系统<P(A)，$\oplus$>中幺元是（　　　　）；对任意 T∈P(A)，T 的逆元是（　）。

答：∅,T

二、选择题

1、在 N 上定义几个二元运算，其中不满足结合律的是（　　）。

A. a * b = a　　　　B. a*b=a+b-5

C. a*b=a+3b　　　　D. a*b=max{a，b}

答：C

2. 下面 4 个代数系统中构成群的是（　　）。

A. <N，+>　　　　B. {R^+，×}

C. <P(A)，U>　　　　D. <A^A，∘>

答：B

3. <Z^*_{13}，$\otimes_{13}$>是群，下面子集中（　　）不是它的子群。

A. {1，2，4，8}　　　　B. {1，12}

C. {1，3，9}　　　　D. {1，5，8，12}

答：A.

4. 下面集合关于相应的加法和乘法运算构成域的是（　　）。

A. {a+b$\sqrt[3]{3}$| a，b∈Z}　　　　B. {a+bi| a，b∈Q}

C. {a+b$\sqrt{2}$| a，b∈Z}　　　　D.{$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ | a，b，c，d∈Z}

答：B.

5. 下面关于循环群性质的描述，错误的是（　）。

A. 循环群必是交换群

B. 循环群的子群仍然是循环群

C. 设 G 是 n 阶循环群，a∈G，则 a 是生成元当且仅当 a 的阶数是 n

D. 循环群的生成元一定是唯一的

答：D.

6. 设 G 是群，e 是幺元，a，b，c∈G，则下面关于子群的性质描述错误的是（　　）。

A. 若 ab=b，则必有 a=e　　　　B. 若 b≠c，有可能 ab=ac

C. G 有唯一的幂等元　　　　D．aG=Ga

答：B.

7、6 阶有限群的任何子群一定不是（　　）。

A.2 阶　　B.3 阶　　C. 4 阶　　D. 6 阶

答：C.

证明题：

1、求循环群 $C_{12}=\{e,a,a^2,\ldots,a^{11}\}$ 中 $H=\{e,a^4,a^8\}$ 的所有右陪集。

解：

因为 $|C_{12}|=12$，$|H|=3$，所以 H 的不同右陪集有 4 个：H，$\{a,a^5,a^9\},\{a^2,a^6,a^{10}\},\{a^3,a^7,a^{11}\}$。

2、求下列置换的运算：

解：

（1）$\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$

（2）$\begin{pmatrix}1&2&3&4&5&6\\4&5&2&6&3&1\end{pmatrix}^3=\begin{pmatrix}1&2&3&4&5&6\\4&5&2&6&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5&6\\4&5&2&6&3&1\end{pmatrix}^2$

$=\begin{pmatrix}1&2&3&4&5&6\\4&5&2&6&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5&6\\6&3&5&1&2&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$

5、试求出 8 阶循环群 G=<a>的所有生成元和所有子群。

解：

设 G 是 8 阶循环群，a 是它的生成元。则 $G=\{e,a,a^2,..,a^7\}$。由于 a^k 是 G 的生成元的充分必要条件是 k 与 8 互素，故 a,a^3,a^5,a^7 是 G 的所有生成元。

因为循环群的子群也是循环群，且子群的阶数是 G 的阶数的因子，故 G 的子群只能是 1 阶的、2 阶的、4 阶的或 8 阶的

1 阶子群：{e}

2 阶子群：$\{e, a^4\}$

4 阶子群：$\{e, a^2, a^4, a^6\}$

8 阶子群：$G=\{e,a,a^2,..,a^7\}$

6、设$<G,\circ>$是群，$a\in G$。令 $H=\{x\in G|a\circ x=x\circ a\}$。试证：H 是 G 的子群。

证明：

$\forall c, d\in H$，$c\circ a=a\circ c$，$d\circ a=a\circ d$。故 $(c\circ d)\circ a=c\circ(d\circ a)=c\circ(a\circ d)=(c\circ a)\circ d=(a\circ c)\circ d=a\circ(c\circ d)$。从而 $c\circ d\in H$。

由于 $c\circ a=a\circ c$,且满足消去律，所以 $a\circ c^{-1}=c^{-1}\circ a$。故 $c^{-1}\in H$。

从而 H 是 G 的子群。

7、设 G={1，3，5，7}，关于模 8 乘法运算，列出运算表，说明 G 构成群。

8、证明：有限群中阶大于 2 的元素的个数一定是偶数。

证明：

设$<G,\circ>$是有限群，则$\forall a\in G$，有$|a|=|a^{-1}|$。且当 a 阶大于 2 时，$a\neq a^{-1}$。故阶数大于 2 的元素成对出现，从而其个数必为偶数。

9、证明：偶数阶群中阶为 2 的元素的个数一定是奇数。

证明：

设$<G,\circ>$是偶数阶群，则由于群的元素中阶为 1 的只有一个单位元，阶大于 2 的元素是偶数个，剩下的元素中都是阶为 2 的元素。故偶数阶群中阶为 2 的元素一定是奇数个。

10、试求$<Z_6,\oplus_6>$中每个元素的阶。

解：

0 是$<Z_6,\oplus_6>$中关于$\oplus_6$的单位元。则$|0|=1$；$|1|=|5|=6$，$|2|=|4|=3$，$|3|=2$。

11、Z 上的二元运算*定义为：$\forall a,b\in Z$，a*b=a+b-2。试证：<Z,*>为群。

证明：

（1）$\forall a,b,c\in I$，(a*b)*c=(a*b)+c-2=(a+b-2)+c-2=a+b+c-4, a*(b*c)=a+(b*c)-2=a+(b+c-2)-2=a+b+c-4。故(a*b)*c= a*(b*c)，从而*满足结合律。

（2）记 e=2。对$\forall a\in I$，a*2=a+2-2=a=2+a-2=2*a.。故 e=2 是 I 关于运算*的单位元。

（3）对$\forall a\in I$，因为 a*（4-a）=a+4-a-2=2=e=4-a+a-2=(4-a)*a。故 4-a

是 a 关于运算*的逆元。

综上所述，$<I,*>$为群。

12、设$<S,\cdot>$为半群，$a\in S$。令 $S_a=\{a^i \mid i\in Z^+\}$。试证$<S_a,\cdot>$是$<S,\cdot>$的子半群。

证明：

$\forall b$，$c\in S_a$，则存在 $k,l\in I_+$，使得 $b=a^k,c=a^l$。从而 $b\cdot c=a^k\cdot a^l=a^{k+l}$。因为 $k+l\in I_+$，所以 $b\cdot c\in S_a$，即 S_a 关于运算·封闭。故$<S_a,\cdot>$是$<S,\cdot>$的子半群。

13、证明在元素不少于两个的群中不存在零元。

证明：（用反证法证明）

设在素不少于两个的群$<G,*>$中存在零元θ。对$\forall a\in G$，由零元的定义有 $a*\theta=\theta$。

$\because$ $<G,*>$是群，$\therefore$关于*消去律成立。$\therefore$ $a=e$。即 G 中只有一个元素，这与$|G|\geq 2$ 矛盾。故在元素不少于两个的群中不存在零元。

14、证明在一个群中单位元是惟一的。

证明：

设 e_1,e_2 都是群〈G,*〉的单位元。　　则 $e_1=e_1*e_2=e_2$。

所以单位元是惟一的。

15、设 a 是一个群〈G，*〉的生成元，则 a^{-1} 也是它的生成元。

证明：

$\forall x\in G$，因为 a 是〈G，*〉的生成元，所以存在整数 k，使得 $x=a^k$。

故 $x=((a^k)^{-1})^{-1}=((a^{-1})^k)^{-1}=(a^{-1})^{-k}$。从而 a^{-1} 也是〈G，*〉的生成元。

17、代数系统$<G,*>$是一个群，则 G 除单位元以外无其它幂等元。

证明：

设 e 是该群的单位元。若 a 是$<G,*>$的等幂元，即 $a*a=a$。

因为 $a*e=a$，所以 $a*a=a*e$。由于运算*满足消去律，所以 $a=e$。

即 G 除单位元以外无其它等幂元。

19、设半群$<S,\cdot>$中消去律成立，则$<S,\cdot>$是可交换半群当且仅当$\forall a,b\in S$，$(a\cdot b)^2=a^2\cdot b^2$。

证明：

$\Rightarrow$ $\forall a,b\in S$，$(a\cdot b)^2=(a\cdot b)\cdot(a\cdot b)=((a\cdot b)\cdot a)\cdot b$

$=(a\cdot(a\cdot b))\cdot b=((a\cdot a)\cdot b)\cdot b=(a\cdot a)\cdot(b\cdot b)=a^2\cdot b^2$;

$\Leftarrow \forall a,b\in S$，因为（$a\cdot b$）$^2=a^2\cdot b^2$，所以 $(a\cdot b)\cdot(a\cdot b)=(a\cdot a)\cdot(b\cdot b)$。故 $a\cdot((b\cdot a)\cdot b)=a\cdot(a\cdot(b\cdot b))$。由于 $\cdot$满足消去律，所以 $(b\cdot a)\cdot b=a\cdot(b\cdot b)$，即 $(b\cdot a)\cdot b=(a\cdot b)\cdot b$。从而 $a\cdot b=b\cdot a$。故满足交换律。

20、设群$<G,\star>$除单位元外每个元素的阶均为 2，则$<G,\star>$是交换群。

证明：

对任一 $a\in G$，由已知可得 $a*a=e$，即 $a^{-1}=a$。

对任一 $a,b\in G$，因为 $a*b=(a*b)^{-1}=b^{-1}*a^{-1}=b*a$，所以运算*满足交换律。

从而＜G,*＞是交换群。

21、设 H 和 K 都 是 G 的子群。证明：$H\cap K$ 也是 G 的子群。

证明：

因为 H 和 K 都 是 G 的不变子群，所以 $H\cap K$ 是 G 的子群。对$\forall a\in G$，$h\in H\cap K$，有 $a\cdot h\cdot a^{-1}\in a\cdot H\cdot a^{-1}$，$h\cdot a^{-1}\in a\cdot K\cdot a^{-1}$。因为 H 和 K 都 是 G 的不变子群，所以 $a\cdot h\cdot a^{-1}\in H$ 且 $a\cdot h\cdot a^{-1}\in K$。从而 $a\cdot h\cdot a^{-1}\in H\cap K$。故 $H\cap K$ 是 G 的不变子群。

22、设群 G 的中心为 C（G）$=\{a\in G|\forall x\in G, a\cdot x=x\cdot a\}$。证明 C（G）是 G 的子群。

证明：

先证 C（G）是 G 的子群。

$\forall a,b\in$ C（G），对$\forall x\in G$,有 $a\cdot x=x\cdot a$，$b\cdot x=x\cdot b$。故（$a\cdot b$）$\cdot x= a\cdot(b\cdot x)=a\cdot(x\cdot b)=(a\cdot x)\cdot b=(x\cdot a)\cdot b=x\cdot(a\cdot b)$, $a^{-1}\cdot x=x\cdot a^{-1}$。从而 $a\cdot b$，$a^{-1}\in$ C（G）。 故 C（G）是 G 的子群。

23、设$<G,\cdot>$是没有非平凡子群的有限群。试证：G 是平凡群或质数阶的循环群。

证明：

若 G 是平凡群，则结论显然成立。

否则设$<G,\cdot>$的阶为 n。任取 $a\in G$ 且 $a\neq e$,记 H=（a）(由 a 生成的 G 的子群)。显然 $H\neq\{e\}$，且 G 没有非平凡子群，故 H=G。从而 G 一定是循环群，且 a 是 G 的生成元。

若 n 是合数，则存在大于 1 的整数 k,m，使得 n=mk。记

$H=\{e,a^k,(a^k)^2,\ldots,(a^k)^{m-1}\}$，易证 H 是 G 的子群，但 $1<|H|=m<n$，故 H 是 G 的非平凡子群。这与已知矛盾。从而 n 是质数。

故 G 是质数阶的循环群。

综上所述，G 是平凡群或质数阶的循环群。

24、设 H 和 K 都是 G 的有限子群，且|H|与|K|互质。试证：$H\cap K=\{e\}$。

证明：

用反证法证明。

若 $H\cap K\neq\{e\}$。则 $H\cap K$ 是一个元素个数大于 1 的有限集。

先证 $H\cap K$ 也是 G 的子群，从而也是 H 和 K 的子群。

$\forall a,b\in H\cap K$,则 $a,b\in H$ 且 $a,b\in K$。因为 H 和 K 都是 G 的子群，故 $a ƀ,a^{-1}\in H$ 且 $a ƀ,a^{-1}\in K$。从而 $a ƀ\in H\cap K,a^{-1}\in H\cap K$。故 $H\cap K$ 是 G 的子群，从而也是 H 和 K 的子群。

由拉格朗日定理可知，$|H\cap K|$是|H|和|K|的因子，这与已知矛盾。

25、素数阶循环群的每个非单位元都是生成元。

证明：

设<G,*>是 p 阶循环群，p 是素数。

对 G 中任一非单位元 a。设 a 的阶为 k,则 $k\neq 1$。

由拉格朗日定理，k 是 p 的正整因子。因为 p 是素数，故 k=p。即 a 的阶就是 p，即群 G 的阶。故 a 是 G 的生成元。

26、设<G,●>是有限群，|G|＝n，则$\forall a\in G$，$|a|\leq n$。

证明：

$\forall a\in G$，由封闭性及|G|=n 可知 $a,a^2,\ldots,a^n,a^{n+1}$ 中必有相同的元素，不妨设为 $a^k=a^m,k<m$。 由消去律得 $a^{m-k}=e$。从而$|a|\leq m-k\leq n$。

27、有限群 G 的每个元素的阶均能整除 G 的阶。

证明：

设|G|=n，$\forall a\in G$，则|a|=m。令 $H=\{e,a,a^2,\ldots,a^{m-1}\}$。

则 H 是 G 的子群且|H|=m。由 **Lagrange 定理知|H|能整除|G|，故 a 的阶能整除 G 的阶。**

28、在一个群<G,*>中，若 G 中的元素 a 的阶是 k，即|a|=k，则 a^{-1} 的阶也是 k。

证明：

因为$|a|=k$，所以$a^k=e$。即（a^{-1}）$^k=(a^k)^{-1}=e$。

从而a^{-1}的阶是有限的，且$|a^{-1}|\leq k$。

同理可证，a 的阶小于等于$|a^{-1}|$。

故a^{-1}的阶也是 k。

29、设 e 是奇数阶交换群<G,*>的单位元，则 G 的所有元素之积为 e。

证明：

设$G=\langle\{e,a_1,a_2,\ldots,a_{2n}\},*\rangle$，n 为正整数。

因为 G 的阶数为奇数 2n+1，所以由拉格朗日定理知 G 中不存在 2 阶元素，即除了单位元 e 以外，G 的所有元素的阶都大于 2。故对 G 中的任一非单位元 a，它的逆元a^{-1}不是它本身，且 G 中不同的元素有不同的逆元。

由此可见，G 中的 2n 个非单位元构成互为逆元的 n 对元素。因为 G 是交换群，故 G 的所有元素之积可变成单位元和 n 对互为逆元的元素之积的积，从而结果为 e。

30、设$S=Q\times Q$，Q 为有理数集合，*为 S 上的二元运算：对任意$\langle a,b\rangle$，$\langle c,d\rangle\in S$，有

$$\langle a,b\rangle*\langle c,d\rangle=\langle ac,ad+b\rangle,$$

求出 S 关于二元运算*的单位元，以及当$a\neq 0$时，<a,b>关于*的逆元。

解：

设 S 关于*的单位元为<a,b>。根据*和单位元的定义，对$\forall\langle x,y\rangle\in S$，有

$$\langle a,b\rangle*\langle x,y\rangle=\langle ax,ay+b\rangle=\langle x,y\rangle,\ \langle x,y\rangle*\langle a,b\rangle=\langle ax,xb+y\rangle=\langle x,y\rangle。$$

即$ax=x,\ ay+b=y,\ xb+y=y$对$\forall x,y\in Q$都成立。解得$a=1,b=0$。

所以 S 关于*的单位元为<1,0>。

当$a\neq 0$时，设<a,b>关于*的逆元为<c,d>。根据逆元的定义，有

$$\langle a,b)*\langle c,d\rangle=\langle ac,ad+b\rangle=\langle 1,0\rangle$$

$$\langle c,d)*\langle a,b\rangle=\langle ac,cb+d\rangle=\langle 1,0\rangle$$

即$ac=1,ad+b=0,cb+d=0$。解得$c=\frac{1}{a},d=-\frac{b}{a}$。

所以<a,b>关于*的逆元为$\langle\frac{1}{a},-\frac{b}{a}\rangle$。