1. 代数系统的基本概念

该部分有三个需要注意的知识点：

1.1 什么是代数系统？

代数系统的表征形式是一个序偶$<S,\Omega>$，其中 S 是非空元素的集合，叫做该代数系统的定义域，Ω是运算的集合。|S|称为代数系统的阶 。

要判断一个给定的系统是否是代数系统，需要验证：

A. 定义的运算满足映射的唯一性（符合函数的定义）

B. 所有运算都是封闭的 。

例：$<N,\div>$不是一个代数系统，因为自然数集合下的÷运算不满足封闭性；设 S 是一个非空集合，那么$<\rho(S),\cap,\cup>$是一个代数系统，其中$\rho(S)$为 S 的幂集 。

1.2 子代数系统

如果$<S,\Omega>$是一代数系统，取 S 的一个子集$S1\subseteq S$，如果$S1$在所有的运算上都满足封闭性，那么$<S1,\Omega>$也是一个代数系统，称之为$<S,\Omega>$的子代数系统 。

要判断$<S1,\Omega>$是否是$<S,\Omega>$的子代数系统，需要验证：

A. $S1\subseteq S$，并且两个代数系统运算集一样 。

B. 所有运算都是封闭的 。

例：$<N,+,\times>$是代数系统$<I,+,\times>$的子代数系统。其中 N 表示自然数集合，I 表示整数集合 。

1.3 代数系统的同类型

设有两个代数系统$U=<S1,\Omega1>,V=\{S2,\Omega2\}$，如果可以在两者的运算集合$\Omega1,\Omega2$上构造一个双射$\Omega1\rightarrow\Omega2$，并且每个原像和对应的像点运算的元数相同，那么就说代数系统 U 和 V 同类型 。

同类型的概念是讨论同态和同构的基础。

2．代数系统中运算的性质

设代数系统为$<S,\odot,*>$

2.1 运算的定律

结合率：$(\forall x)(\forall y)(\forall z)(x,y,z\in S\rightarrow(x\odot y)\odot z=x\odot(y\odot z))$

交换率：$(\forall x)(\forall y)(x,y\in S\rightarrow x\odot y=y\odot x)$

分配率：

$(\forall x)(\forall y)(\forall z)(x,y,z\in S\rightarrow x\odot(y*z)=(x\odot y)*(x\odot z))$（$\odot$对$*$满足左分配率）

$(\forall x)(\forall y)(\forall z)(x,y,z\in S\rightarrow(y*z)\odot x=(y\odot x)*(z\odot x))$（$\odot$对$*$满足右分配率）

吸收率：

$(\forall x)(\forall y)(x,y\in S\rightarrow x\odot(x*y)=x)$ （$\odot$对$*$满足左吸收率）

$(\forall x)(\forall y)(x,y\in S\rightarrow(x*y)\odot x=x)$ （$\odot$对$*$满足右吸收率）

等幂率：$(\forall x)(x\in S\rightarrow x\odot x=x)$

可约率：设0为零元

$(\forall x)(\forall y)(\forall z)(x,y,z\in S\wedge x\neq 0\wedge(x\odot y=x\odot z)\rightarrow y=z)$（左可约率）

$(\forall x)(\forall y)(\forall z)(x,y,z\in S\wedge x\neq 0\wedge(y\odot x=z\odot x)\rightarrow y=z)$（右可约率）

2.2 运算中的特异元素

么元e：

$(\forall x)(x\in S\rightarrow e_l\odot x=x)$（$e_l$为关于$\odot$的左么元）

$(\forall x)(x\in S\rightarrow x\odot e_r=x)$（$e_r$为关于$\odot$的右么元）

零元0：

$(\forall x)(x\in S\rightarrow 0_l\odot x=0_l)$（$0_l$为关于$\odot$的左零元）

$(\forall x)(x \in S \to x \odot 0_r = 0_r)$（$0_r$ 为关于 $\odot$ 的右零元）

等幂元：$(\exists x)(x \in S \wedge x \odot x = x)$（$x$ 为关于 $\odot$ 的等幂元）

逆元：（设 $x, y \in S, e$ 为关于 $\odot$ 的么元）

$y \odot x = e$（y 为 x 关于 $\odot$ 的左逆元）

$x \odot y = e$（y 为 x 关于 $\odot$ 的右逆元）

可约元：（设 $x \in S \wedge x \neq 0$）

$(\forall y)(\forall z)(y, z \in S \wedge (x \odot y = x \odot z) \to y = z)$（x 是关于 $\odot$ 的左可约元）

$(\forall y)(\forall z)(y, z \in S \wedge (y \odot x = z \odot x) \to y = z)$（x 是关于 $\odot$ 的左可约元）

注意：能寻找到常见代数系统中的特异元素

代数系统	么元	零元	等幂元	逆元	可约元
$<R,+>$	0	无	0	相反数	任何元素
$<R,\times>$	1	0	1，0	除 0 外，为其倒数	除 0 外的任何元素
$<\rho(S),\bigcap>$	S	$\varnothing$	任何元素	除 S 外，其余元素均不可逆	S
$<\rho(S),\bigcup>$	$\varnothing$	S	任何元素	除 $\varnothing$ 外，其余元素均不可逆	$\varnothing$
$<P,\wedge>$	T	F	任何元素	除 T 外，其余元素均不可逆	T
$<P,\vee>$	F	T	任何元素	除 F 外，其余元素均不可逆	F
$<f,\circ>$	I_X 恒等函数	无	I_X	其反函数	所有双射函数

f 是从 n 个元素到自身的双射函数					

2.3 从运算表中判断运算性质的方法

给定代数系统$<S,\odot>$

1. 封闭性：运算表中的每个元素都属于 S 。
2. 交换律：运算表关于主对角线对称 。
3. 等幂律：运算表主对角线上的元素与对应行或者对应列的表头元素相同 。
4. 零元：x 是关于⊙的左零元，当且仅当运算表中 x 所对应的行中每个元素都与 x 相同；x 是关于⊙的右零元，当且仅当运算表中 x 所对应的列中每个元素都与 x 相同 。
5. 么元：x 是关于⊙的左么元，当且仅当运算表中 x 所对应的行中每个元素都与对应的行表头元素相同；x 是关于⊙的右么元，当且仅当运算表中 x 所对应的列中每个元素都与对应的列表头元素相同 。
6. 逆元：x 为关于⊙的左逆元，当且仅当 x 所在行的元素中至少有一个么元，y 为关于⊙的右逆元，当且仅当 y 所在列的元素中至少有一个么元。x 与 y 互为逆元，当且仅当运算表中 x 行 y 列及 y 行 x 列中的元素都为么元 。

例：给定代数系统$<S,\otimes>$，$S=\{a,b,c,d,e\}$，找出下列运算表的特异元素 。

$\otimes$	a	b	c	d	e
a	a	b	c	d	e
b	b	d	a	c	d
c	c	a	b	a	b
d	d	a	c	d	c
e	e	d	a	c	e

么元：a；没有零元；等幂元：a，d，e；

b 、c 互为逆元；d 是 b 的左逆元 。

不满足交换律，不满足等幂律 。

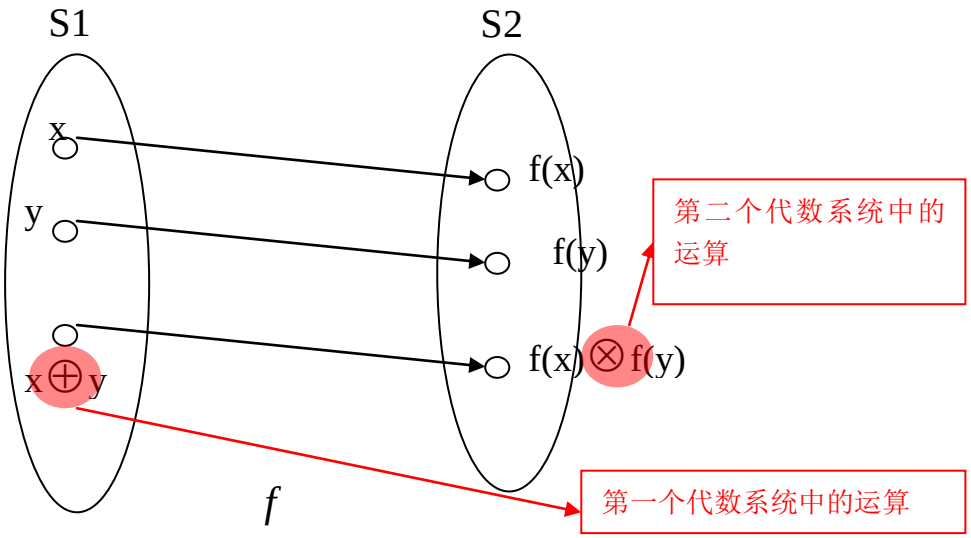
3．代数系统的同态与同构

代数系统的同态和同构是建立在同类型的基础上，在两个代数系统的定义域上构造一个映射，满足**运算的像等于像的运算** 。

3.1 基本概念

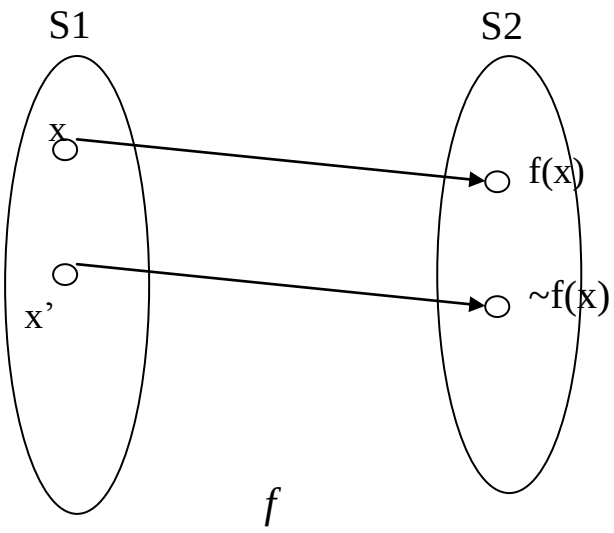
同态：给定代数系统$V1=<S1,\oplus>$，$V2=<S2,\otimes>$，如果这两个代数系统是同类型的，而且可以构造一个函数$f:S1\to S2$，满足$(\forall x)(\forall y)(x\in S1\wedge y\in S1\to f(x\oplus y)=f(x)\otimes f(y))$，那么我们说 V1 和 V2 是同态的，而称 f 为从 V1 到 V2 的同态映射 。

如果用一个图比较直观的观察同态，可以表述如下：



也就是 $f(x\oplus y)=f(x)\otimes f(y)$

如果运算是个一元运算，假设代数系统是$V1=<S1,'>$，$V2=<S2,\sim>$，f 为其对应的同态映射，那么直观图如下：



也就是 $f(x') =\sim f(x)$

由于 f 的类型不同，可以产生不同的映射：

1. f 是满射，f 为两个代数系统之间的满同态映射；
2. f 是单射，f 为两个代数系统之间的单一同态映射；
3. f 是内射，且两代数系统相同，则 f 为两个代数系统之间的自同态映射；
4. f 是双射，f 为两个代数系统之间的同构映射；
5. f 是双射，且两代数系统相同，f 为两个代数系统之间的自同构映射 。

3.2 同态与同构的求解

同态与同构部分要求解的问题一般分为两种：一是求解两个代数系统之间的同态、同构映射；二是证明某一个函数 f 是否是两个代数系统之间的同态、同构映射 。

3.2.1 求解两个代数系统之间的同态、同构映射

一．判定两个代数系统是否同态，并找出一个同态映射

做题步骤：（任何一步不满足，则不同态）

1. 看是否满足同态的前提：两个系统是同类型的；
2. 找到一个映射，所有元素满足运算的像等于像的运算 。

如果遇到这类题目，一定非常简单，因为需要构造映射，这个映射一定是显而易见容易看出的 。

例：是否可以构造代数系统$<N,+>$到$<Z_2,+_2>$的同态映射？

解：首先，这两个代数系统都只有一个二元运算，因此是同类型的 。

构造函数 $f(x)=\begin{cases}1 & x\text{为奇数}\\ 0 & x\text{为偶数}\end{cases}$

任取两个元素 $y,z\in N$

（1）y、z 都为奇数，$f(y+z)=0$，$f(y)=f(z)=1$，

$$f(y)+_2 f(z)=1+_2 1=0=f(y+z)$$

（2）y、z 都为偶数，$f(y+z)=0$，$f(y)=f(z)=0$，

$$f(y)+_2 f(z)=0+_2 0=0=f(y+z)$$

（3）y 为奇数，z 为偶数，$f(y+z)=1, f(y)=1, f(z)=0$

$$f(y)+_2 f(z)=1+_2 0=1=f(y+z)$$

（4）y 为偶数，z 为奇数，$f(y+z)=1, f(y)=0, f(z)=1$

$$f(y)+_2 f(z)=0+_2 1=1=f(y+z)$$

可以看出，无论 y 和 z 如何取值，都满足 $f(y)+_2 f(z)=f(y+z)$，即运算的像等于像的运算 。

因此，可以构造代数系统$<N,+>$到$<Z_2,+_2>$的同态映射 f 为

$$f(x)=\begin{cases}1 & x\text{为奇数}\\ 0 & x\text{为偶数}\end{cases}$$

（完毕）

从过程可以看出，完全是根据两步走的。而且对应的映射也可以很容易的构造 。

二．判定两个代数系统是否同构，并找出一个同构映射

做题步骤：（任何一步不满足，则不同构）

1. **看是否满足同构的前提，即两个代数系统是否是同类型的；**
2. **判断两个代数系统定义域的基数是否相等 。**
3. **查找两个代数系统的性质是否一样：是否都满足交换律、等幂律；是否有么元、零元；等幂元的个数是否相等；和自身互为逆元的元素个数是否相等。如果有的性质**

只有一方有，另一方没有，则两个代数系统不同构。若所有的都满足，继续 。

4. 在两个代数系统间构造一个映射，使得所有元素的运算的像等于像的运算 。

第 4 步有快捷做法：在构造映射的时候，使得代数系统 V1 的么元对应像点为 V2 的么元，V1 的零元对应像点为 V2 的零元，V1 的等幂元像点为 V2 的等幂元；V1 中与自身互为逆元的元素对应像点是 V2 中和自身互为逆元的元素。构造完映射之后，在 V1 的运算表中，将所有的元素换成对应的像点，看生成的新表是否跟 V2 的运算表相同。如果相同，该映射即为从 V1 到 V2 的同构映射 。如果不相同，修改 V1 中非特异元素的映射像点，构造新的映射，再验证……。

如果遇到这类题目，一般情况下非特异元素会很少，映射也很好构造 。

例 1：判断两代数系统$V1=<R,+>$，$V2=<R,\times>$是否同构，若同构，构造其同构映射 。

解：首先，判断两个代数系统是否同类型，两个代数系统都只含有一个二元运算，因此满足同类型 。

第二，判断两个代数系统定义域的基数是否相同，也满足 。

第三，寻找特异元素。V1 中没有零元，V2 中有零元 0 。因此，这两个代数系统不同构 。

例 2：代数系统$V1=<\{1,2,3,4\},\bullet_5>$和$V2=<\{0,1,2,3\},+_4>$是否同构，若同构，构造其同构映射 。

解：首先，判断两个代数系统是否同类型，两个代数系统都只含有一个二元运算，因此满足同类型 。

第二，判断两个代数系统定义域的基数是否相同，都是 4，也满足 。

第三，寻找特异元，为了方便起见，画出其运算表 。

$\bullet_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

V1 和 V2 都有么元，都没有零元，除么元外，都只有一个与自身互为逆元的元素；都没有等

幂元；都满足交换律 。

第四，构造映射 。

么元对应么元：$1\to 0$

与自身互为逆元的元素对应与自身互为逆元的元素：$4\to 2$

剩下两个元素不是特异元素，因此我随意指定一种指派：$2\to 1,3\to 3$

把$\bullet_5$的运算表中元素都换成对应的像点，构造一张新表 。

	0	1	3	2
0	0	1	3	2
1	1	2	0	3
3	3	0	2	1
2	2	3	1	0

为了便于比较跟$+_4$是否一致，调整表头的顺序为 0，1，2，3，如下：（也就是交换表头 2 和 3 所在的列，交换表头 2 和 3 所在的行）

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

可以看出，上表跟$+_4$的运算表完全一致。

因此，代数系统$V1=<\{1,2,3,4\},\bullet_5>$和$V2=<\{0,1,2,3\},+_4>$是同构的，f 为其同构映射，定义如下：$f(1)=0, f(2)=1, f(3)=3, f(4)=2$。

3.2.2 给定一个函数 f，证明 f 是两个代数系统之间的同态、同构映射

这种题，其实跟求同态、同构问题的解法类似，为了清楚起见，给出这类证明题的求解方法 。

一. 证明 f 是 V1 到 V2 的同态映射

做题步骤：

1. 判断两个代数系统是否是同类型的；

2. 看 f 的定义与是否与 V1 的定义域相同，f 的值域是否是 V2 定义域的子集 。

3. 判断所有元素是否满足运算的像等于像的运算 。

例：考察代数系统$U=<N,\bullet>$，$V=<\{0,1\},\bullet>$，其中$\bullet$是普通意义下的乘法运算，定义$f:N\to\{0,1\}$为

$$f(n)=\begin{cases}1 & \text{存在}k\in N,\text{使得}n=2^k\\ 0 & \text{否则}\end{cases}$$

求证：f是 U 到 V 的同态映射。

证明：

首先，U 和 V 都只含有一个二元运算，因此是同类型的；

第二，f的定义域是自然数集合N，值域是$\{0,1\}$，是 V 定义域的子集 。

第三，验证是否运算的像等于像的运算 。

任取$x,y\in N$，分情况讨论：

（1）x 和 y 都可以表示成2^k，设$x=2^{k1},y=2^{k2}$，

那么$f(x\bullet y)=f(2^{k1}\bullet 2^{k2})=f(2^{k1+k2})=1$，$f(x)=f(y)=1$

$$f(x)\bullet f(y)=1\bullet 1=1=f(x\bullet y)$$

（2）x 和 y 都不能表示成2^k，那么$x\bullet y$也不能表示成2^k

$$f(x\bullet y)=0,\ f(x)=f(y)=0$$

$$f(x)\bullet f(y)=0\bullet 0=0=f(x\bullet y)$$

（3） x 可以表示成2^k，y 不能表示成2^k，那么$x\bullet y$也不能表示成2^k

$$f(x\bullet y)=0,\ f(x)=1,f(y)=0$$

$$f(x)\bullet f(y)=1\bullet 0=0=f(x\bullet y)$$

（4）x 不可以表示成2^k，y 能表示成2^k，那么$x\bullet y$也不能表示成2^k

$$f(x\bullet y)=0,\ f(x)=0,f(y)=1$$

$$f(x)\bullet f(y)=0\bullet 1=0=f(x\bullet y)$$

可知，无论 x 和 y 如何取值，都能够保证 $f(x)\bullet f(y)=f(x\bullet y)$。

综上所述， f 是 U 到 V 的同态映射 。

（证毕）

二.　证明 f 是 V1 到 V2 的同构映射

做题步骤：

1.　判断两个代数系统是否是同类型的；

2.　看 f 是不是双射函数，f 的定义与是否与 V1 的定义域相同，f 的值域是否与 V2 定义域相同 。

3.　判断所有元素是否满足运算的像等于像的运算（也就是把 V1 运算表的所有元素换成 f 下对应的像，考察得到的新表是否与 V2 对应的运算表相同）

介于同构中遇到的问题一般是让你构造一个函数，证明两个代数系统是否同构。如果给出了函数，做题的方法就非常简单，因此暂不举例。如果实际中遇到类似问题，按照前面给出的做题步骤求解 。

3.2.3 注意点：为什么在找同态的时候没有利用关系表中特异元素的对应关系？

此处引入这个问题，是为了提醒大家，不要把同态与同构的做题步骤搞混了。在同态中，特异元素不满足对应关系，下面给出例子说明 。

例：代数系统 $<N,+>$和$<Z_3,\oplus>$是同态的，$\oplus$运算定义如下：

$\oplus$	0	1	2
0	0	1	2
1	1	0	2
2	2	2	2

可以证明，如果取

$$f(x)=\begin{cases}1 & x\text{为奇数}\\ 0 & x\text{为偶数}\end{cases}$$

则 f 是$<N,+>$到$<Z_3,\oplus>$的同态映射 。

但是我们发现，$<N,+>$中有么元，没有零元；但是$<Z_3,\oplus>$中有么元，有零元 。

3.3 同态与同构的性质

同态与同构问题研究了两个代数系统之间的关系，如果两个代数系统满足同态性，那么一个代数系统中的某些性质可以平移到另外一个代数系统中 。

下面列举一些主要的性质，具体的证明过程参照前面给出的思路 。

1. 两个代数系统之间的同态映射不唯一 。

2. 满同态映射能够从一个代数系统到另一个代数系统单项保留所有的性质（如交换律、结合律、含零元、含幺元、元素的可逆性等） 。

- 定理 6.3.2 给定<X，⊙，*> ~ <Y，⊕，⊗>且 f 为其满同态映射，则
- (a)如果⊙和*满足结合律，则 ⊕ 和 ⊗ 也满足结合律。
- (b)如果⊙和*满足交换律，则 ⊕ 和 ⊗ 也满足交换律。
- (c)如果⊙对于*或*对于⊙满足分配律，则 ⊕ 对于 ⊗ 或 ⊗ 对于 ⊕ 也相应满足分配律。
- (d)如果⊙对于*或*对于⊙满足吸收律，则 ⊕ 对于 ⊗ 或 ⊗ 对于 ⊕ 也满足吸收律。
- (e)如果⊙和*满足等幂律，则 ⊕ 和 ⊗ 也满足等幂律。
- (f)如果 e_1 和 e_2 分别是关于⊙和*的幺元，则 $f(e_1)$ 和 $f(e_2)$ 分别为关于 ⊕ 和 ⊗ 的幺元。
- (g)如果 θ_1 和 θ_2 分别是关于⊙和*的零元，则 $f(\theta_1)$ 和 $f(\theta_2)$ 分别为关于 ⊕ 和 ⊗ 的零元。
- (h)如果对每个 $x \in X$ 均存在关于⊙的逆元 x^{-1}，则对每个 $f(x) \in Y$ 也均存在关于 ⊕ 的逆元
- $f(x^{-1})$；如果对每个 $z \in X$ 均存在关于*的逆元
- Z^{-1}，则对每个 $f(z) \in Y$ 也均存在关于 ⊗ 的逆元
- $f(z^{-1})$。

3. 两个同构的代数系统其实没有任何差异，只是集合中元素的表示符号以及运算的表示符号不同而已 。同构关系是一个等价关系 。

4. 若 g 是从 V1 到 V2 的同态映射，h 是从 V2 到 V3 的同态映射，那么 $h \circ g$ 是从 V1 到 V3 的同态映射 。

4．同余关系、商代数和积代数

商代数是指由一个大的代数系统可以生成一个小的代数系统，使得我们在讨论问题的时候，不用在基数非常大的代数系统上讨论，而转移到小代数系统上讨论问题 。积代数与之相反，是由 n 个小代数系统生成大的代数系统 。

4.1 基本概念

4.1.1 同余关系

简单的说，就是对所有运算，满足代换性质的等价关系。要注意三点：一，是等价关系；二，满足代换性质；三，不是对某个运算，而是对所有运算都满足代换性质 。

等价关系，我们都已经很清楚了，需要满足自反的 、对称的 、可传递的 。

代换性质，这里给出一个比较直观的感觉方式。假设$<S,\otimes_n>$是一个代数系统，其中，$\otimes_n$是一个 n 元运算，n 可能为 1，2，3，……。代换性质要求，关系 E 满足代换性质，当且仅当任意给定 S 中的元素，满足下列式子：

$$\left.\begin{array}{l} x_1 E y_1 \\ x_2 E y_2 \\ \vdots \quad \vdots \\ x_n E y_n \end{array}\right\} n\text{行}$$

$$\Rightarrow \quad \otimes_n (x_1, x_2, \cdots, x_n) E \otimes_n (y_1, y_2, \cdots, y_n)$$

其中，$\otimes_n(x_1, x_2, \cdots, x_n)$是一种前缀表示法，表示$x_1, x_2, \cdots, x_n$这 n 个元素做 n 元运算$\otimes_n$。

从这个通用的式子我们可以很容易看到常用的一元和二元运算中的代换性质。

一元运算：给定代数系统$<S,\sim>$，关系 E 满足代换性质，当且仅当

$$\left.\begin{array}{l} x_1 E y_1 \end{array}\right\} 1\text{行}$$

$$\Rightarrow \quad \sim x_1 E \sim y_1$$

二元运算：给定代数系统$<S,\oplus>$，关系 E 满足代换性质，当且仅当

$$\left.\begin{array}{l} x_1 E y_1 \\ x_2 E y_2 \end{array}\right\} 2\text{行}$$

$$\Rightarrow \quad x_1 \oplus x_2 E y_1 \oplus y_2$$

4.1.2 商代数

商代数是基于同余关系构造的一个小代数系统。设 R 是代数系统$V =< G,\Omega >$上的同余关系，则称代数系统$< G/R,\Omega_R >$是$V =< G,\Omega >$关于 R 的商代数 。

其中G/R我们在关系那一章已经接触到了，是等价关系 R 划分集合 G 构成的商级 。由于 G 中具有等价关系的元素被划分到同一类了，因此G/R的元素个数一定小于等于 G 的元素个数。这也就是为什么商代数比原代数系统小的原因 。

Ω_R的定义方式如下：假定Ω是一个二元运算，那么$[x]_R \Omega_R [y]_R = [x \Omega y]_R$；假定$\Omega$是一个一元运算，那么$\Omega_R([x]_R) = [\Omega x]_R$。推广到 n 元运算的情况，$\Omega_R([x_1]_R, [x_2]_R \cdots, [x_n]_R) = [\Omega(x_1, x_2, \cdots, x_n)]$。用一句话来形容，就是运算的等价类等于等价类的运算 。

4.1.3 积代数

积代数是由 n 个小的代数系统生成一个大的代数系统，这些小的代数系统必须通型，且都叫做大代数系统的因子代数。大的代数系统定义域是所有小代数系统定义域的笛卡尔乘积，运算是通过小代数系统构造的 。我们一般接触的就是两个只含有一个二元运算或者只含有一个一元运算的代数系统，下面在只含有一个二元运算的代数系统上讨论 。

设$< S,\odot >$和$< T,\oplus >$是同型代数系统，那么它们的积代数为$< S \times T, * >$，其中*定义为：$< s1,t1 > * < s2,t2 > =< s1 \odot s2, t1 \oplus t2 >$，其中$s1, s2 \in S; t1, t2 \in T$。

再举含有一个一元运算的代数系统，设$< S, \sim >$，$< T, ' >$，那么它们的积代数为$< S \times T, \bar{} >$，其中$\bar{}$定义为：$\overline{< s1,t1 >} =< \sim s1, t1' >$，其中$s1 \in S; t1 \in T$。

注意积代数中的运算，序偶的第 i 重用的是第 i 个因子代数系统中的运算。

4.2 同余关系和商代数的性质

4.2.1 同余关系的性质

任何一个同态映射均可诱导出一个同余关系。

设 f 是从 $U=\{G_1,\Omega_1\}$ 到 $V=\{G_2,\Omega_2\}$ 的同态映射，则可由 f 诱导出一个等价关系 R_f，定义如下：对任意的 $x_1,x_2\in G_1$，$x_1R_fx_2$ 当且仅当 $f(x_1)=f(x_2)$。可以证明，该 R_f 是 $U=\{G_1,\Omega_1\}$ 中的同余关系。

4.2.2 商代数的性质

一个代数系统与其商代数同态，并且可以构造该代数系统到商代数的自然同态映射。

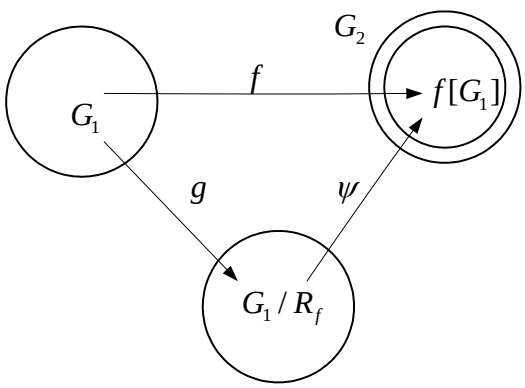
设 R 是代数系统 $V=<G,\Omega>$ 上的同余关系，其关于 R 的商代数是 $<G/R,\Omega_R>$，两个代数系统满足 $<G,\Omega>-<G/R,\Omega_R>$，可以构造其上的自然同态映射 $g:G\to G/R$ 为 $g(x)=[x]_R$。

4.2.3 同余和商代数之间的联系

其实，由前面的性质，商代数和同余之间的关系已经比较明显了。在这里给出整体的描述 。

假定代数系统 $V1=<G_1,\odot>$ 到 $V2=<G_2,*>$ 可以构造一个满同态映射 f，那么可由 f 诱导出一个同余关系 R_f，利用该同余关系可以生成 V1 的商代数，该商代数和 V2 同构 。

为了更直观的了解，引入课本上的一个图：



4.3 求解同余关系、商代数和积代数

4.3.1 同余关系

在同余关系中，最经常遇到的是判定问题，判定一个关系 R 是否是某个代数系统中的同余关系。遇到这类问题，也有固定的解题思路，步骤如下：

1. **判定关系 R 是否是等价关系；**
2. **是否对所有的运算满足代换性质 。**

第 2 步中存在快捷方式，如果你找出一个运算不满足代换性质，则不用继续验证其他运算了。可以直接说关系 R 不是该代数系统中的同余关系。因此，在含有多个运算的代数系统中，如何选择验证顺序很关键，但具体怎么选没有办法给出方法，只能靠你多做练习，积累出来直观的感觉 。

例 1：考察代数系统$V=<I,+,\bullet>$，I 上的关系定义为：iRj，当且仅当$|i|=|j|$。R 是否是 V 上的同余关系？

解：首先，判断 R 是否是一等价关系，根据判定等价关系三步走的方法，依次看是否满足自反 、对称 、可传递 。（此处略去证明过程）

论证了 R 是一等价关系，下面看是否满足代换性质 。

首先选择+运算验证，在二元运算下，需要验证对于任意$x_1,x_2,y_1,y_2\in I$是否

$$\left.\begin{array}{l} x_1Ey_1 \\ x_2Ey_2 \end{array}\right\}\text{2行}$$

$$\Rightarrow \quad x_1+x_2Ey_1+y_2$$

取$x_1=1,x_2=2,y_1=1,y_2=-2$，可知满足x_1Ey_1，x_2Ey_2，但$|x_1+x_2|\neq|y_1+y_2|$，即$x_1+x_2\not Ey_1+y_2$。

可知不满足代换性质 。不用再验证乘法运算了，可以直接得出结论，R 不是 V 上的同余关系 。

（毕）

某些情况下，可能让你找出一个同余关系，特别是让你找出某个同态映射诱导的同余关系，这种题目就更简单了，直接根据 4.2.1 给出的映射方法得出结果（对任意的

$x_1, x_2 \in G_1$，$x_1 R_f x_2$ 当且仅当 $f(x_1) = f(x_2)$）。

例 2：已知代数系统 $U =< N, + >$ 和代数系统 $V =< Z_m, +_m >$ 是同态的，并且可以构造从 U 到 V 的同态映射 $f: N \to Z_m$ 为 $f(x) = x(\mathrm{mod}\, m)$。指出该同态映射诱导的 U 的同余关系 。

解：设该同余关系为 R，则对于任意元素 $x, y \in N$，xRy 当且仅当 $f(x) = f(y)$，即 $x(\mathrm{mod}\, m) = y(\mathrm{mod}\, m)$。

（毕）

注意：有的时候，题目会要求你证明由 f 诱导的关系 R 是同余关系，那么要看清楚题目，根据前面介绍的两个步骤证明 R 是同余关系 。

4.3.2 商代数和积代数

这一部分的主要问题，就是让你求代数系统的商代数以及积代数 。两种代数系统的求解方法有相似点，因此放在一起说明 。步骤如下：

1. 求代数系统的定义域

如果是求商代数的定义域，那就是要求等价关系划分定义域构成的商集，可以利用关系那一章等价类的求法解决；

如果是求积代数的定义域，直接把因子代数的定义域做笛卡尔乘积就可以了。

2. 求代数系统的运算

运算的表示方法有两种，一种是描述性的表示方法，一种是构造运算表，建议定义域比较小的时候用运算表做；定义域很大，短时间无法构造运算表的，用描述性表示法。

再复习一下商代数运算的构造方法：

$[x]_R \Omega_R [y]_R = [x \Omega y]_R$（运算的等价类等于等价类的运算）

积代数运算的构造方法：

$< s1, t1 > * < s2, t2 > =< s1 \odot s2, t1 \oplus t2 >$

例 1：设代数系统为 $< N, + >$，R 是该代数系统的同余关系，并且定义为对于任意元素 $x, y \in N$，xRy 当且仅当 $x(\mathrm{mod}\, 2) = y(\mathrm{mod}\, 2)$，求该代数系统关于 R 的商代数 。

解：设要求解的商代数为$<G,*>$，下面逐一求出定义域和值域 。

首先，任何一个自然数 x， $x(\mathrm{mod}\,2)$ 或等于 0，或等于 1。因此，$G=\{[1]_R,[0]_R\}$

其次，构造运算*，任取 $x,y\in N$，$[x]_R*[y]_R=[x+y]_R$

（1） 如果 x，y 都为奇数，那么 $[x]_R=[1]_R,[y]_R=[1]_R$，$[x+y]_R=[0]_R$

即为 $[1]_R*[1]_R=[0]_R$

（2） 如果 x，y 都为偶数，那么 $[x]_R=[0]_R,[y]_R=[0]_R$，$[x+y]_R=[0]_R$

即为 $[0]_R*[0]_R=[0]_R$

（3） 如果 x 为奇数，y 都为偶数，那么 $[x]_R=[1]_R,[y]_R=[0]_R$，$[x+y]_R=[1]_R$

即为 $[1]_R*[0]_R=[1]_R$

（4） 如果 x 为偶数，y 都为奇数，那么 $[x]_R=[0]_R,[y]_R=[1]_R$，$[x+y]_R=[1]_R$

即为 $[0]_R*[1]_R=[1]_R$

运算表如下：

*	$[0]_R$	$[1]_R$
$[0]_R$	$[0]_R$	$[1]_R$
$[1]_R$	$[1]_R$	$[0]_R$

（毕）

例 2：已知代数系统 $U=<Z_2,+_2>,V=<Z_3,\times_3>$，试构造 U 和 V 的积代数。

解：设 U 和 V 的积代数为 $W=<Z_2\times Z_3,*>$。

其中，$Z_2\times Z_3=\{<0,0>,<0,1>,<0,2>,$
$<1,0>,<1,1>,<1,2>\}$

下面通过运算表构造*运算 。

*	〈0, 0〉	〈0, 1〉	〈0, 2〉	〈1, 0〉	〈1, 1〉	〈1, 2〉
〈0, 0〉	〈0, 0〉	〈0, 0〉	〈0, 0〉	〈1, 0〉	〈1, 0〉	〈1, 0〉
〈0, 1〉	〈0, 0〉	〈0, 1〉	〈0, 2〉	〈1, 0〉	〈1, 1〉	〈1, 2〉

〈0, 2〉	〈0, 0〉	〈0, 2〉	〈0, 1〉	〈1, 0〉	〈1, 2〉	〈1, 1〉
〈1, 0〉	〈1, 0〉	〈1, 0〉	〈1, 0〉	〈0, 0〉	〈0, 0〉	〈0, 0〉
〈1, 1〉	〈1, 0〉	〈1, 1〉	〈1, 2〉	〈0, 0〉	〈0, 1〉	〈0, 2〉
〈1, 2〉	〈1, 0〉	〈1, 2〉	〈1, 1〉	〈0, 0〉	〈0, 2〉	〈0, 1〉

可以看出，〈0, 1〉是么元，0 是 U 的么元，1 是 V 的么元 。

从这里，我们可以推出积代数的特殊性质：

设两个代数系统$<S,\odot>,<T,*>$，它们的积代数是$<S\times T,\oplus>$

（1） 若$<S,\odot>,<T,*>$都是可交换的，则$<S\times T,\oplus>$也是可交换的；

（2） 若$<S,\odot>,<T,*>$含有么元，分别是$e1,e2$，则$<e1,e2>$是$<S\times T,\oplus>$的么元 。

（3） 若$<S,\odot>,<T,*>$含有零元，分别是$0_1,0_2$，则$<0_1,0_2>$是$<S\times T,\oplus>$的么元 。

（4） 若$<S,\odot>$中 x 的逆元是x^{-1}，$<T,*>$中 y 的逆元是y^{-1}，则$<S\times T,\oplus>$中$<x,y>$的逆元是$<x^{-1},y^{-1}>$

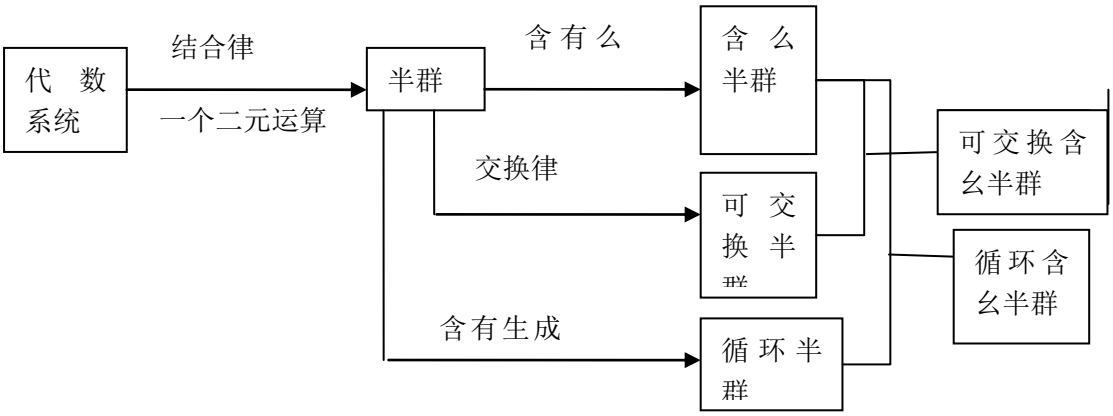
5．特殊的代数系统——半群

半群是一个只含有一个满足结合律的二元运算的代数系统。也是一个代数系统，因此，研究的思路跟代数系统一样，首先是基本概念，然后是运算的性质，然后是同态和同构，最后是商代数以及积代数 。

在半群中，运算的性质已经在定义的时候明确给定了，因此只需要研究基本概念、同态、同构，商代数以及积代数 。下面依照这种思路逐一说明，跟前面的抽象代数系统中一致的性质一笔带过 。

5.1 半群的种类

半群有很多种，在结合律的基础上，如果满足交换律，叫做可交换半群；如果含有么元，叫做含么半群（独异点）；如果有生成元，叫做循环半群。可以通过下图表示出来 。



其中，可交换半群和含么半群可以结合构成可交换含么半群（可交换独异点），循环半群可以和含么半群结合构成循环含么半群（循环独异点） 。

注意：为什么循环半群不和可交换半群合成呢？因为循环半群都是可交换半群 。

5.2 半群的性质及不同半群之间的关系

一．半群

有限半群含有等幂元（有限半群为定义域是有限集合的半群）

二．含么半群

含么半群运算表中任意两行、任意两列都不相同；

含么半群中元素若有逆元，$(a\odot b)^{-1}=b^{-1}\odot a^{-1}$，$(a^{-1})^{-1}=a$

三．循环半群

循环半群都是可交换半群 。

循环半群中可以延伸出来的概念：生成集。用一句话来描述，就是可以用生成集中的元素合成，构造循环半群定义域中的所有元素 。

5.3 半群和含么半群的子半群

半群的子半群跟子代数系统的定义是一致的，因此，验证方法参照 1.2 小结 。

含么半群的子含么半群定义方法与子代数系统不同 。要判断$<S1,\Omega>$是否是半群$<S,\Omega>$的子含么半群，需要验证：

A．$S1\subseteq S$，并且两个代数系统运算集一样 。

B．运算是封闭的 。

C. $S1$中含有$<S,\Omega>$的么元 。

例：设集合$S=\{e,0,1\}$，在 S 中定义二元运算*如下：

*	e	0	1
e	e	0	1
0	0	0	0
1	1	0	1

则$<\{0,1\},*>$是$<S,*>$的子半群，但不是$<S,*>$的子含么半群，$<\{0,e\},*>$是$<S,*>$的子含么半群 。

5.4 半群和含么半群的同态与同构

半群的同态和同构跟代数系统一样，参照第 3 节学习 。

含么半群的同态与同构跟代数系统略有差别。除了要满足运算的像等于像的运算，还要保证第一个代数系统么元的像等于第二个代数系统的么元 。

定义：设$U=<S,*,e_S>$和$V=<T,\otimes,e_T>$是两个含么半群，若存在映射$f:S\to T$，对 S 中任意元素 a 和 b，有

$$f(a*b)=f(a)\otimes f(b)$$
$$f(e_S)=e_T$$

则称 f 是从 U 到 V 的一个含么半群同态映射 。

- **定理 7.2.1** 如果 f 为从$<S,\odot>$到$<T,*>$的半群同态映射，对任意 $a\in S$ 且 $a\odot a = a$，则 $f(a) * f(a) = f(a)$。

5.5 积半群

这一部分跟积代数部分完全相同，性质也跟积代数部分相同，如要研究性质，详见 4.3.2 小节最后 。

5.6 做题思路

这一部分遇到的题，大部分是比较简单的判断某一代数系统是否是半群/含么半群/循环半群，并找出对应的特异元素。做题方法参见 2.3 小节 。

第二种可能的题目是判断一个半群是否是另一个的子半群/子含么半群，判断方法在 5.3 小节已经讨论过了 。

另外一种题目就是判定同态、同构，求同余关系、积代数等等。这部分的做题方法与抽象代数部分也完全一样，只是在对含么半群的做题中，论证同态同构问题的时候在判断运算的像等于像的运算后面，加上一条，第一个半群的么元的像为第二个半群的么元 。别的都完全一致 。

其实，只要掌握了第 1 至第 4 节的做题方法，基本上可以直接用在半群上，只需要偶尔增加条件即可 。

6．特殊的代数系统——群

群是半群的加强，**每个元素都含有逆元的含么半群**叫做群 。因此，说道底，群是一种含么半群，因此，含么半群的所有性质都可以平移到群中 。在本节讨论的时候，省略了讨论群的子群，群的同态 、同构，积群，因为这些部分跟 5.3,5.4,5.5 是完全一致的 。但要注意，群的同态与同构讨论的时候只需要满足运算的像等于像的运算就可以了，它自身已经保证了么元 、逆元和子群。本节主要讨论群的概念以及群的性质 。

6.1 群的概念

如果$<G,*>$是独异点并且 G 中的每个元素都含有逆元，那么$<G,*>$为群 。

如果单独把群具有的性质列出来，在做判定问题的时候，需要注意以下四点：

（1）$<G,*>$是一代数系统，*为二元运算；

（2）*满足结合律；

（3）$<G,*>$含有么元；

（4）每个 G 中的元素都含有逆元 。

原则上来说，要论证一个代数系统是否是群，必须对以上四点逐个验证，但实际应用中我们发现，利用群的某些性质，可以很简单的把一些代数系统排出群的范围，给我们的判定带来方便 。

例：$<Z,+>$是群，$<Q,\times>$不是群，仅是含么半群，因为 0 没有逆元 。

定义域为有限集合的群叫有限群；无限集合的叫无限群；定义域只含有一个元素的叫平凡群。

6.2 群的性质

首先回忆一下 5.2 小节含么半群的性质，同样也适用于群。除此之外，群有其自身的性质 。

6.2.1 一般的群的性质

在下列性质中均设对应的群是$<G,*>$

1. 如果 G 的基数大于 1，则群无零元；
2. 群中仅有唯一的等幂元，是么元；
3. 群满足可约律；

$$a*b=a*c\Rightarrow b=c$$
$$b*a=c*a\Rightarrow b=c$$

4. 群中方程的解是唯一的；

方程$a*x=b$，解得$x=a^{-1}*b$

方程$x*a=b$，解得$x=b*a^{-1}$

5. 群中元素的 n 次幂定义为

$$a^n=\begin{cases}e & n=0\\ a^{n-1}*a & n>0\\ (a^{-1})^m & n<0,\ \text{且n=-m}\end{cases}$$

- 5、**定理 7.4.5** 设$<G,\odot>$为群，则
- ① $\forall a\in G,\ (a^{-1})^{-1}=a$

- ② $\forall a$， $\forall\ b\in G$，$(a\odot b)^{-1} = b^{-1}\odot a^{-1}$
- ③ $\forall a\in G$，m，$n\in Z$，有 $a^m\odot a^n = a^{m+n}$
- ④ $\forall a\in G$，m，$n\in Z$，有$(a^m)^n = a^{mn}$

⑤ 若<G，$\odot$>为 Abel 群（可交换群），则$(a\odot b)^n = a^n\odot b^n$

6. 取群中任意元素 a，|a|=k，p 为整数，$a^p = e$ 当且仅当 p 是 k 的整数倍；

（|a|表示的意义不是绝对值，而是 a 的阶，它是使$a^n = e$ 的最小正整数 n）

定理 7.4.7 给定群<G，$\odot$>，

$a\in G$，且| a | = k，p 为整数，则 a^p=e iff $p|k$。

推论：若 a^n = e 且没有 n 的因子 d (1＜d＜n)使 a^d = e，则 n 为 a 的阶。

7. $|a|=|a^{-1}|$（两者的阶相等）

6.2.2Abel 群的性质

$<G,*>$是群，在群的基础上，如果满足交换律，那么$<G,*>$称为 Abel 群 。

除了群的性质，Abel 群也有其自身的性质：$<G,*>$是 Abel 群当且仅当 $(a*b)^2 = a^2*b^2$。

6.3 置换群和对称群

这部分单独拿出来讲，是因为置换群和循环群也有其独特的特点，他们的定义域都是从一个集合 X 到 X 的双射函数的集合，运算是函数的合成运算 。

这部分需要注意以下几点：

1. 置换

设 X 是个非空集合，那么从 X 到 X 的双射函数叫做 X 的置换（又看到了双射函数的另一种叫法）。把恒等映射 $f(x)=x$ 叫做 X 的恒等置换或者么置换。我们知道，双射函数都

是有反函数的，把 f 的反函数 f^{-1} 叫做 f 的反置换 。

2．置换的合成

在置换的基础上，定义了置换的合成。设 p_i, p_j 是 X 的两种置换。把 X 中的元素先进行 p_i 置换再进行 p_j 置换的操作叫做两个置换的复合，表示成 $p_i \Diamond p_j$，可以看出**置换的复合运算跟关系的合成顺序是一样的，跟函数的合成顺序正好相反** 。

3．对称群和置换群

X 的所有置换构成一个集合，表示成 P_X ，则称 $<P_X, \Diamond>$ 为对称群，其实，N 个元素的对称群是同构的，仅是元素的表示方式不同而已，因此，通常用 $<S_{|X|}, \Diamond>$ 表示对称群，|X| 表示 X 中元素的个数 。

如果 $G \subseteq S_{|X|}$ 并且 $<G, \Diamond>$ 可构成群（满足群的定义），那么称 $<G, \Diamond>$ 为置换群。（注意，对称群是置换群，置换群不一定是对称群 。）

这部分涉及到的题目基本上就是求对称群，后面一节给出具体例子 。

- **定义 7.5.3** 令<Q, ◇>是一置换群
- 且 $Q \subseteq S_{|X|}$。
- 称 $R = \{<a, b> \mid a, b \in X \wedge p \in Q \wedge p(a) = b\}$ 为由<Q, ◇>所诱导的 X 上的二元关系。

定理 7.5.2 由置换群<Q, ◇>诱导的 X 上的二元关系是一等价关系。

一般地说来，由 n 个元素的集合而构成的所有 $n!$ 个 n 阶置换的集合 S_n 与复合置换运算◇构成群<S_n, ◇>，它便是 n 次 $n!$ 阶对称群。

6.4 做题思路

这一部分，有三种题目比较常见：第一，判定某一代数系统是否是群；第二，求某一集合的对称群；第三，求某个群的子群。其余题型，像同态 、同构的验证，积代数，跟前面章节的做题方法是一样的，不再累述。只需要注意一点，群是含幺元半群，因此，求子群 、

同态 、同构的时候不要忘了对么元的判定 。

6.4.1 判断某一代数系统是否是群

在 6.1 小节介绍群的概念的时候，已经给出了一般的判定方法：

（1）$<G,*>$是一代数系统，*为二元运算；

（2）*满足结合律；

（3）$<G,*>$含有么元；

（4）每个 G 中的元素都含有逆元 。

实际上，我们在讨论群的性质的时候，得知群没有零元，只有一个等幂元，因此，如果发现该代数系统含有零元，或者除么元外还有其它的等幂元，那就没有必要从那四步一步一步进行了，可以直接判定该代数系统不是群 。

例 1：判断$<Z_3,+_3>$，$<Z_3,\times_3>$是否是群？

解：$<Z_3,+_3>$是群，$<Z_3,\times_3>$不是，因为含有零元 0。

例 2：判断$<\rho(S),\bigcap>$，$<\rho(S),\bigcup>$是否是群？

解：都不是群，因为两个系统都含有零元 。

6.4.2 求集合 X 的对称群

这一部分的题目，X 的基数不会大，因为 X 上构造的双射函数是 n！个 。

例：设 $X=\{a,b,c\}$，求 X 的对称群 。

解：X 有 6 个置换，分别用 $p_1,p_2,\cdots,p_6$ 表示，设

$$
\begin{array}{llll}
X: & a & b & c \\
 & \downarrow & \downarrow & \downarrow \\
p_1: & a & b & c \\
p_2: & a & c & b \\
p_3: & b & a & c \\
p_4: & b & c & a \\
p_5: & c & a & b \\
p_6: & c & b & a
\end{array}
$$

设$<S_3,\Diamond>$是 X 的对称群，则$S_3=\{p_1,p_2,\cdots,p_6\}$，构造运算表◊如下：

$\Diamond$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_4	p_3	p_6	p_5
p_3	p_3	p_5	p_1	p_6	p_2	p_4
p_4	p_4	p_6	p_2	p_5	p_1	p_3
p_5	p_5	p_3	p_6	p_1	p_4	p_2
p_6	p_6	p_4	p_5	p_2	p_3	p_1

从表中可以看到，含有么元p_1，与自身互为逆元的四个：p_1，p_2，p_3，p_6；有两个元素互为逆元，为p_4，p_5。

从运算中可以看出，恒等置换是对称群的么元 。

6.4.3 求一个群的子群

设$<G,*>$是群，如果 G 中有 n 个元素，那么 G 的子集有2^n个元素，要求$<G,*>$的子群，原则上需要讨论这2^{n-1}个非空集合（子群含有原群的么元）中的元素，跟*作运算是否满足群的概念要求 。试想，如果 n=6，则2^{n-1}=32，运算结果非常大 。

拉格朗日定理指出：

（1） 任何素数阶群除自身外，只含有平凡子群 。

（2） 任何非素数阶群仅可能含有因子阶子群 。（6 的因子：1，6，2，3）

这两条为我们解决这一问题铺平的道路，下面给出一个例子 。

例 1：求$<Z_6,+_6>$的所有子群 。

解：这是一个 6 阶群，只可能含有 1，2，3，6 阶子群 。

我们先构造$+_6$的运算表：

$+_6$	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

由子群的定义知道，子群中一定要含有原群的么元，因此，1 阶子群是$<\{0\},+_6>$，6 阶子群是$<Z_6,+_6>$。剩下的，是 2 阶和 3 阶子群 。

再分析表中的元素，0 是么元，0，3 的逆元是自身；1 和 5 互为逆元，2 和 4 互为逆元 。

2 阶子群中，含有么元 0，加入的 1 个元素必须有逆元，因此只能加入逆元是自身的元素——3。考察$<\{0,3\},+_6>$，满足封闭性，因此是子群 。

3 阶子群中，含有么元 0，加入两个元素，有两种方式：一是加入非么元的两个等幂元；二是加入互为逆元的两个元素 。这里只能用第二种方案 。

考虑$<\{0,1,5\},+_6>$，由于$1+_61=2$，不满足封闭性，因此排除；

考察$<\{0,2,4\},+_6>$，满足封闭性，因此是子群 。

综上所述，$<Z_6,+_6>$有四个子群，分别是$<\{0\},+_6>$，$<Z_6,+_6>$，$<\{0,3\},+_6>$，$<\{0,2,4\},+_6>$。（毕）

例 2：求 6.4.2 小节的例子中对称群的子群 。

解：这也是一个 6 阶群，只可能含有 1，2，3，6 阶子群 。1 阶和 6 阶不用再讨论了，只用看 2 阶和 3 阶子群 。

为了清楚起见，把运算表复制下来：

$\Diamond$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_4	p_3	p_6	p_5
p_3	p_3	p_5	p_1	p_6	p_2	p_4
p_4	p_4	p_6	p_2	p_5	p_1	p_3
p_5	p_5	p_3	p_6	p_1	p_4	p_2
p_6	p_6	p_4	p_5	p_2	p_3	p_1

p_1是么元，p_1，p_2，p_3，p_6的逆元是自身，p_4和p_5互为逆元 。

2阶子代数：$<\{p_1,p_2\},\Diamond>,<\{p_1,p_3\},\Diamond>,<\{p_1,p_6\},\Diamond>$，都满足封闭性

3 阶子代数：可能有$<\{p_1,p_4,p_5\},\Diamond>,<\{p_1,p_2,p_3\},\Diamond>,<\{p_1,p_2,p_6\},\Diamond>,$
$<\{p_1,p_3,p_6\},\Diamond>$。其中，$<\{p_1,p_2,p_3\},\Diamond>$中$p_2\Diamond p_3=p_4$，不满足封闭性；
$<\{p_1,p_2,p_6\},\Diamond>$中$p_2\Diamond p_6=p_5$，不满足封闭性。$<\{p_1,p_3,p_6\},\Diamond>$中
$p_3\Diamond p_6=p_4$，不满足封闭性 。

综上所述，共有 6 个子群，分别是：$<\{p_1\},\Diamond>$，$<S_3,\Diamond>$，
$<\{p_1,p_2\},\Diamond>,<\{p_1,p_3\},\Diamond>,<\{p_1,p_6\},\Diamond>$，$<\{p_1,p_4,p_5\},\Diamond>$。