5.7 陪集与拉格朗日定理

定义5-7.1 设<G,*>是群，A和B是G的非空子集(A,B∈$\mathscr{P}$(G))，则记AB={a*b|a∈A,b ∈B}为A和B的积；

记A^{-1}={a^{-1}|a ∈A}为A的逆。

例

设 群<I,+>，A={1}，B={0，2}，则

AB={1，3}，A^{-1}={-1}。

陪集

定义5-7.2:设<H,*>是群<G,*>的子群，元素 $a \in G$，则称 $\{a\}H=\{a*h \mid h \in H\}$ 为元素a所确定的子群<H,*>的左陪集，

$H\{a\}=\{h*a \mid h \in H\}$ 称为元素a所确定的子群<H,*>的右陪集。

简记为aH或Ha，a称为代表元素。

(注：重点讨论左陪集)

例1. 求出$<N_6,+_6>$关于子群$<\{0,3\},+_6>$的所有左陪集和右陪集，其中$N_6=\{0,1,2,3,4,5\}$。

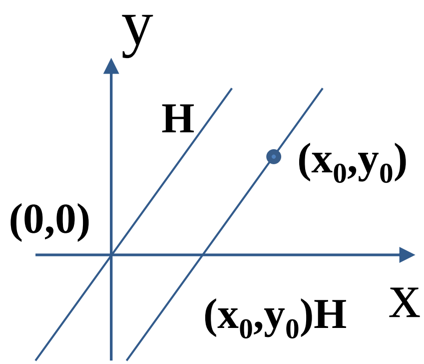
$+_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

例1. 求出$<N_6,+_6>$关于子群$<\{0,3\},+_6>$的所有左陪集和右陪集，其中$N_6=\{0,1,2,3,4,5\}$。

解: 令$H=\{0,3\}$,则

左陪集:	右陪集:
$0H=\{0,3\}=3H=\cdots$	$H0=\{0,3\}=H3=\cdots$
$1H=\{1,4\}=4H=\cdots$	$H1=\{1,4\}=H4=\cdots$
$2H=\{2,5\}=5H=\cdots$	$H2=\{2,5\}=H5=\cdots$

从中可以看出：$\{0H,1H,2H\}$是G的一个划分。



例2

代数系统<G,+>，其中G=R*R,+定义为

$<x_1,y_1>+<x_2,y_2>=<x_1+x_2,y_1+y_2>$， 显然<G,+>是一个群。G的几何意义？二维平面

- H={<x,y>|y=2x}，容易验证<H,+>是<G,+>的一个子群。H的几何意义是？

一条经过(0,0)的直线y=2x

- 对于$\langle x_0y_0\rangle\in G$，左陪集$<x_0,y_0>H$

$=\{<x+x_0,y+y_0>|y=2x\}$的几何意义？

一条经过（x_0,y_0）且平行于y=2x的直线

关于陪集

性质1: 设$<H,*>$是$<G,*>$的子群,$\forall a,b\in G$,

则 $aH=bH$ 或 $aH\cap bH=\Phi$。

证: 设$aH\cap bH\neq\Phi$,即$\exists f\in aH\cap bH$。

$\therefore \exists h_1, h_2\in H$,使$f=a*h_1=b*h_2$,

$\therefore a=b*h_2*h_1^{-1}\in bH$。

对于任意的$a*h\in aH$,
有(将$a=b*h_2*h_1^{-1}$代入)
$a*h=b*h_2*h_1^{-1}*h=b*h_3\in bH$

$\forall x\in aH$,则$\exists h_3\in H, x=a*h_3=b*h_2*h_1^{-1}*h_3\in bH$

$\therefore aH\subseteq bH$,同理$bH\subseteq aH$。

$\therefore aH=bH$。 #

(注:所得结论对右陪集也平行成立)

性质2：设<H,*>是<G,*>的子群，则子群<H,*>的任意左陪集的大小(即基数)相等。

证：$\forall a \in G, a*h_1, a*h_2 \in aH$，$h_1 \neq h_2$，

$\therefore a*h_1 \neq a*h_2$，

$\therefore |aH| = |H|$。

$\therefore$ H的任意陪集大小相同。

注：可以证明：

1）设<H,*>是<G,*>的子群，$\forall a \in G$，则aH非空。

2）设<H,*>是<G,*>的子群，$G = \cup_{a \in G} aH$。

由左陪集性质可见：｛aH｝是G的一个划分。

拉格朗日定理

定理5-7.1 设$<H,*>$是群$<G,*>$的子群,那么$R=\{<a,b>|a\in G,\ b\in G,\ a^{-1}*b\in H\}$是一个等价关系，称为H的左陪集等价关系。

(a)对于$a\in G$，若记$[a]_R=\{x|x\in G$,且$<a,x>\in R\}$则$[a]_R=aH$。

(b)如果G是有限群，$|G|=n$, $|H|=m$,则 $m|n$

即：一个有限群<G, *>的子群<H, *>的阶|H|只可能是G的阶|G|的因子。

等价关系：自反、对称且传递。

拉格朗日定理之一

- 定理5-7.1　　设 $<H,*>$ 是群 $<G,*>$ 的子群，那么 $R=\{<a,b>|a\in G, b\in G, a^{-1}*b\in H\}$ 是一个等价关系，称为H的左陪集等价关系。

(1)$a\in G$，$a^{-1}\in G$，有 $a^{-1}*a=e\in H$，所以 $<a,a>\in R$，因此 R 是自反的。

(2)若 $<a,b>\in R$，有 $a^{-1}*b\in H$，$(a^{-1}*b)^{-1}= b^{-1}*a$，因为 H 是 G 的子群，所以 $(a^{-1}*b)^{-1}\in H$，即 $b^{-1}*a\in R$，所以 $<b,a>\in R$，因此 R 是对称的。

(3)若 $<a,b>,<b,c>\in R$，则有 $a^{-1}*b\in H$ 和 $b^{-1}*c\in H$，所以 $(a^{-1}*b)*(b^{-1}*c)\in H$，而 $(a^{-1}*b)*(b^{-1}*c)=a^{-1}*c\in H$，所以 $<a,c>\in H$，因此 R 是传递的。

所以 R 是一个等价关系。

拉格朗日定理之一

- 定理5-7.1　设$<H,*>$是群$<G,*>$的子群,那么$R=\{<a,b>|a\in G, b\in G, a^{-1}*b\in H\}$是一个等价关系，称为H的左陪集等价关系,。
- 对于$a\in G$，若记$[a]_R=\{x|x\in G,$且$<a,x>\in R\}$则$[a]_R=aH$。

$x\in [a]_R$

$$\Leftrightarrow <a,x> \in R$$

$$\Leftrightarrow a^{-1}*x \in H$$

$$\Leftrightarrow x\in aH。$$

拉格朗日定理之二

要证明: $[a]_R = aH$, $m \mid n$

- 证明 设*R*是*G*中的等价关系，将*G*分成不同等价类，由以上讨论知

$$G = \bigcup_{i=1}^{k} [a_i]_R = \bigcup_{i=1}^{k} a_i H$$

- 由于这*k*个左陪集是两两不相交的基数相同的集合，所以有 $|G|=|a_1H|+|a_2H|+\ldots+|a_kH|$ **(5.7.1)**
- 可知$|a_iH|=|H|$(i=1,2,…,k), 将这些代入式(5.7.1)得

$$n=|G|=k|H| = km$$

其中*k*为不同左(右)陪集的数目。定理得证。

拉格朗日定理之二（同上）

定理5-7.1:有限群$<G,*>$的任意子群$<H,*>$的阶数可以整除群G的阶数。

证:$\forall a\in G \Rightarrow a\in aH$,

$\therefore G=\cup_{a\in G}aH$。

由左陪集的性质知：H的左陪集集合是G的一个划分。

又$\forall a,b\in G, |aH|=|bH|=|H|$。

$\therefore |G|/|H|$是G的划分的块数（即划分的秩）是个整数。

$\therefore |H|$可整除$|G|$ 。

推论

1. 质数阶的群没有非平凡子群 (<{e},*>,<G,*> 称为 <G,*> 的平凡子群)。

2. 有限群<G,*>中的任何元素a的阶可整除|G|。

证: 若 $a\in G$ 的阶是r（即 $a^r=e$）, 则 $\{e,a,a^2,a^3,\ldots,a^{r-1}\}$ 是G的子群。

3. 质数阶的群,一定是循环群。

证: 设<G,*>为质数阶群,

$\forall a\in G, a\neq e$，由推论2知:

a的阶数可整除|G|,但是|G|为质数,所以a的阶数等于群的阶数,

$\therefore \{a,a^2,\ldots,a^r\}=G$，（r为a的阶数）

$\therefore$ <G,*>是循环群。

例3.设K= {e,a,b,c} ,在K上定义二元运算 * 如下表所示：证明〈K，＊〉是一个群，但不是循环群。

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

证：由运算表可知，运算＊是封闭的和可结合的。幺元是e，每个元素的逆是自身，所以〈K，＊〉是群。又因为a, b, c都是二阶元素，故〈K，＊〉不是循环群。

称〈K，＊〉为Klein四元群。

例4.四阶群只有二个,一个是四阶循环群,另一个是Klein四元群。

证:1) 设四阶群为< {e,a,b,c} , * >。其中e是幺元。当四阶群含有一个四阶元素时，这个群就是循环群。

2) 当四阶群不含有四阶元素时，则由推论2可知，除幺元e外，a,b,c的阶数一定都是2。

假设a * b等于a,b或e，则b=e,a=e或a=b矛盾。所以a * b=c。

类似可证：b * a=c

a * c=c * a=b

b * c=c * b=a。

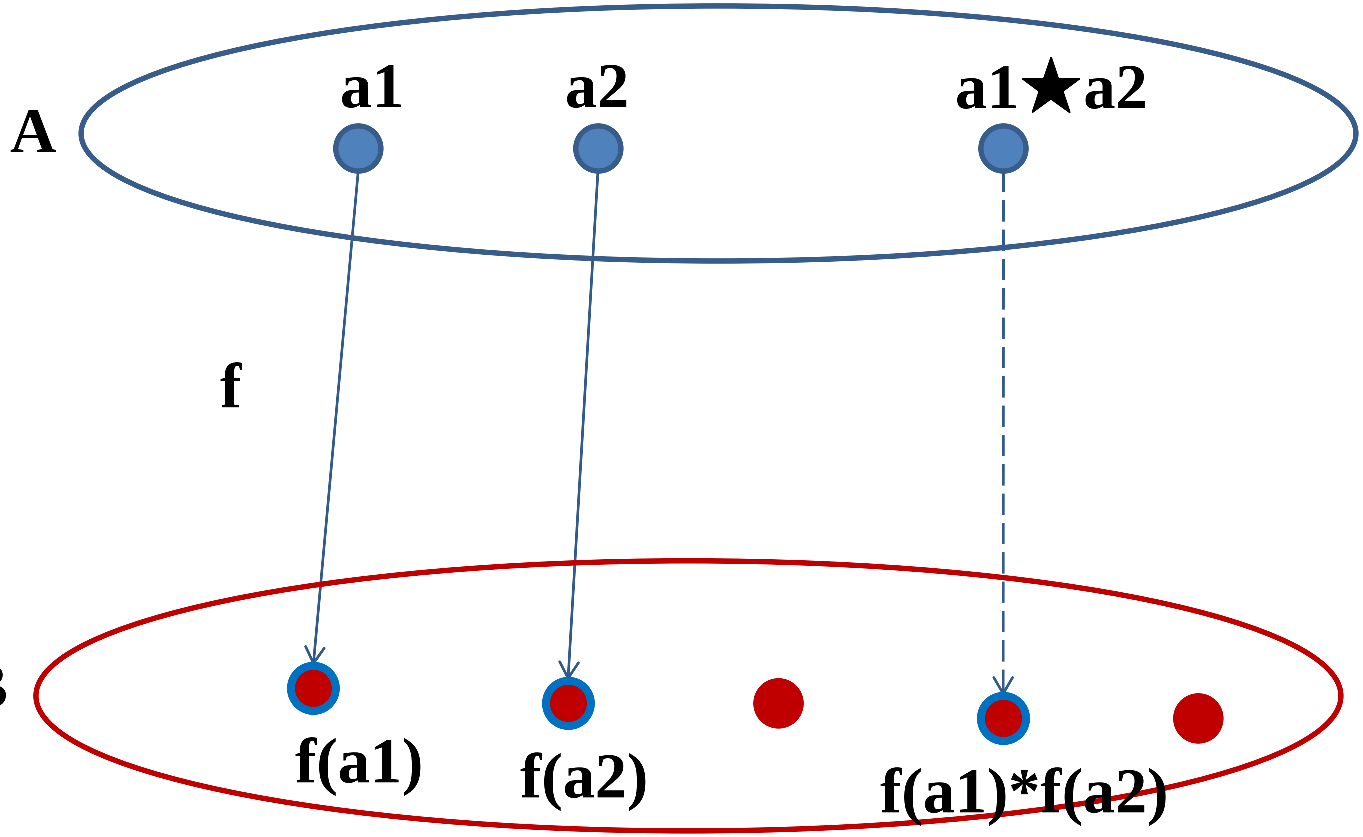
因此，这是一个Klein四元群。

5.8 同态与同构

定义5-8.1 设$<A,★>$和$<B,*>$是两个代数系统，f是从A到B的映射，$\forall a,b \in A$，有$f(a_1 ★ a_2)=f(a_1)*f(a_2)$ 则称 f 是从 $<A,★>$ 到 $<B,*>$的一个同态映射，称$<A,★>$ **同态**于$<B,*>$，记作$<A,★> \sim <B,*>$。

把$<f(A),*>$称为$<A,★>$的一个同态象，其中$f(A)=\{x \mid x=f(a), a \in A\}$，包含于B。

示意图



例1 <I, × >是一个代数系统，

另一个代数系统<B, ⊙ >，其中B={正，负，零}，

⊙运算表如下，

作映射f：I →B如下，

$$f(n)=\begin{cases} 正 & n>0 \\ 负 & n<0 \\ 零 & n=0 \end{cases}$$

⊙	正	负	零
正	正	负	零
负	负	正	零
零	零	零	零

显然，对于任意a，b属于I，有

f(a×b)=f(a) ⊙f(b)，所以**<I, × >同态于<B, ⊙ >**

同态像的性质

定理5-8.2 设f是代数系统$\langle A,* \rangle$到代数系统$\langle B, \star \rangle$的同态,则

1)若$\langle A,* \rangle$是半群,则$\langle f(A), \star \rangle$也是半群。

证:$\forall a,b,c \in f(A), \exists x,y,z \in A$,有$a=f(x), b=f(y), c=f(z)$,

则$a \star b=f(x) \star f(y)=f(x*y) \in f(A)$,

封闭性

又$a \star (b \star c)=f(x) \star (f(y) \star f(z))$

$=f(x) \star f(y*z)$

$=f(x*(y*z))$

$=f((x*y)*z)=f(x*y) \star f(z)$

$=(f(x) \star f(y)) \star f(z)=(a \star b) \star c$ 。

结合律

$\therefore \langle f(A), \star \rangle$是半群。

同态像的性质

2)若<A,*>是独异点,则<f(A), ★ >也是独异点.

证:$\forall a \in f(A)$,则$\exists x$,有$a=f(x)$,$e \in A$,$f(e) \in f(A)$,

右幺元

$\therefore a ★ f(e)=f(x) ★ f(e)=f(x*e)=f(x)=a$,

左幺元

$f(e) ★ a=f(e) ★ f(x)=f(e*x)=f(x)=a$。

$\therefore$ f(e)是<f(A), ★ >的幺元, $\therefore$ <f(A), ★ >是独异点。

3)若<A,*>是一个群,则<f(A), ★ >也是一个群.

证:$\forall f(x) \in f(A)$,

右逆元 左逆元

$f(x) ★ f(x^{-1})=f(x*x^{-1})=f(e)$, $f(x^{-1}) ★ f(x)=f(x^{-1}*x)=f(e)$,

$\therefore f(x)^{-1}=f(x^{-1})$, 即<f(A), ★ >也是一个群。

同态像的性质

4)若$\langle A,*\rangle$是阿贝尔群,则$\langle f(A),\bigstar\rangle$也是阿贝尔群.

证：$\forall a,b\in f(A)$

$\exists x,y\in A$,使得：$a=f(x),b=f(y)$

由$\langle A,*\rangle$是阿贝尔群可知：

$x*y=y*x$

交换律

故$a\bigstar b=f(x)\bigstar f(y)=f(x*y)=f(y*x)=f(y)\bigstar f(x)=b\bigstar a$

即$\langle f(A),\bigstar\rangle$也是阿贝尔群。

总结:

1)同态像f（A）将继承原象代数系统A的所有性质。

2)若h是$\langle A,*\rangle\to\langle B,\bigstar\rangle$的同态映射，$\langle B,\bigstar\rangle$不一定满足$\langle A,*\rangle$中的所有性质。

同构

定义5-8.2 设f是从代数系统<A,★>到<B,*>的同态，

如果f是满射，则称f为满同态；

如果f是入射，则称f为单一同态；

如果f是双射，则称f同构映射，此时代数系统A与B是**同构**的,记作<A, ★ >≌<B,*>。

例1.a) f是$<N,+>$到$<N_k,+_k>$的满同态，

证：$f:N\to N_k(k>0)$， $f(x)=x \bmod k$，

设$x_1=lk+h_1, x_2=mk+h_2$ $(h_1,h_2<k)$，

则$\because f(x_1+x_2)=(x_1+x_2) \bmod k$

$=(h_1+h_2) \bmod k = h_1+_k h_2 = f(x_1)+_k f(x_2)$。

$\therefore f(x_1+x_2)=f(x_1)+_k f(x_2)$。

又$\because f$是满射 $\therefore f$是$<N,+>$到$<N_k,+_k>$的满同态。

b）设f：$R\to R$定义为对任意$x\in R$，$f(x)=5^x$，那么f是从$<R,+>$到$<R,*>$的单一同态。

c）设$H=\{7n，n \in I\}$，定义f：$I \to H$为对于任意$n \in I$，有$f(n)=7n$，那么f是从$<I,+>$到$<H,+>$的一个同构。

例2.证$<R_+,\cdot>$同构于$<R,+>$。

证:i)令h: $R_+\rightarrow R$, $h(x)=\lg x$

则因为对数函数单调增,

$\therefore h$是单射。

$\forall y\in R,\exists x=10^y$, 使$y=\lg 10^y=h(x)$,

$\therefore h$是满射。

$\therefore h$是从R_+到R的双射。

ii)$h(a\cdot b)=\lg(a\cdot b)=\lg a+\lg b=h(a)+h(b)$

$\therefore <R_+,\cdot>$同构于$<R,+>$。

定理5-8.1 代数系统之间的同构关系是等价关系。

证明：1）（**自反性**）设 $\langle A, *\rangle$ 为任何代数系统。$\langle A, *\rangle \cong \langle A, *\rangle$

作恒等映射 $f:A\to A$，则 f 是双射。并且 $\forall a,b\in A$ 有：

$f(a*b)=a*b=f(a)*f(b)$。所以 $\langle A, *\rangle \cong \langle A, *\rangle$。

2）（**对称性**）设 $\langle A, *\rangle \cong \langle B, ☆\rangle$。

则存在双射 $f:A\to B$，并且 $\forall a,b\in A$ 有：$f(a*b)=f(a) ☆ f(b)$。

所以 $f^{-1}:B\to A$ 也是双射。$\forall y_1,y_2\in B$，存在 $x_1,x_2\in A$，使得 $f(x_1)=y_1, f(x_2)=y_2$。

故有：
$$\begin{aligned} f^{-1}(y_1 ☆ y_2) &= f^{-1}(f(x_1) ☆ f(x_2)) \\ &= f^{-1}(f(x_1 * x_2)) \\ &= x_1 * x_2 \\ &= f^{-1}(y_1) * f^{-1}(y_2)\text{。} \end{aligned}$$

因此 $\langle B, ☆\rangle \cong \langle A, *\rangle$。

3）（**传递性**）设 $\langle A, *\rangle \cong \langle B, ☆\rangle$，$\langle B, ☆\rangle \cong \langle C, \triangle\rangle$。

则存在双射 $f:A\to B$ 和 $g:B\to C$，故 $g\circ f$ 也为双射。

$\forall a,b\in A$ 有：
$$\begin{aligned} g\circ f(a*b) &= g(f(a) ☆ f(b)) \\ &= g(f(a)) \triangle g(f(b)) \\ &= g\circ f(a) \triangle g\circ f(b) \end{aligned}$$

所以，$\langle A, *\rangle \cong \langle C, \triangle\rangle$。 #

同态核

定义5-8.3 设代数系统<A,*>，如果f是<A,*>到<A,*>的同态，则称f**自同态**；

如果f是<A,*>到<A,*>的同构，则称f**自同构**。

定义5-8.4: 设f是由群<G,*>到群<G',*>的同态，e'是G'的幺元，称$ker(f)=\{x \mid x\in G \wedge f(x)=e'\}$为f的**同态核**。

把<f(A),*>称为<A,★>的一个**同态象**，其中$f(A)=\{x \mid x=f(a), a\in A\}$，包含于B。

例 :$f:\langle I,+\rangle \to \langle N_5,+_5\rangle, \forall x \in N, f(x)=x \bmod 5$,

则f是同态吗?

$\forall x,y \in I, f(x+y)=(x+y) \bmod 5$

$=x \bmod 5 +_5 y \bmod 5 = f(x) +_5 f(y)$,

$\therefore$ f是从$\langle I,+\rangle$到$\langle N_5,+_5\rangle$的同态。

f的同态核?

$\ker(f)=\{x \mid x \in I \land f(x)=0\}=\{\ldots -10,-5,0,5,10,\ldots\}$。

定理5-8.3：f是群$<G,*>$到$<G',*'>$的同态，则$<\ker(f),*>$必定是$<G,*>$的子群；若令$K=\ker(f)$，则$aK=Ka$。

证： 1)$\forall x,y\in\ker(f)$，则$f(x)=e'$，$f(y)=e'$， 幺元

$\therefore f(x*y)=f(x)*'f(y)=e'*e'=e'$，

$\therefore x*y\in\ker(f)$。 封闭性

2)$\forall x\in\ker(f)$，则因$f(x^{-1})=f(x)^{-1}=(e')^{-1}=e'$， 逆元

$\therefore x^{-1}\in\ker(f)$ $\therefore$ $<\ker(f),*>$是群$<G,*>$的子群。

3)令$k=\ker(f)$，$\forall a\in G$，设$f(a)=a'$，$\forall k_1\in K$

则$f(a\cdot k_1\cdot a^{-1})=f(a)*'f(k_1)*'f(a^{-1})=f(a)*'f(a^{-1})=f(e)=e'$

即：$\exists k_2\in K$，有$a\cdot k_1\cdot a^{-1}=k_2$ 两边乘a

$\therefore a\cdot k_1=k_2\cdot a$ $\therefore aK=Ka$ 即左陪集等于右陪集。

注意： 左陪集等于右陪集的子群称为不变子群（不作要求）。

同余关系

定义5-8.5: $<A,*>$是一个代数系统，R是A上的等价关系，若$\forall <a,b>,<c,d>\in R$都有$<a*c，b*d>\in R$，称R是A上关于$*$的**同余关系**，R将A划分的等价类称为**同余类**。

例1 代数系统<A,*>，其中A={a，b，c，d}，*运算表如下，定义在A上的等价关系R={<a,a>,<a,b>,<b,a>,<b,b>,<c,c>,<c,d>,<d,c>,<d,d>}，

试验证R是A上的同余关系，并求R划分的同余类。

*	a	b	c	d
a	a	a	d	c
b	b	a	c	d
c	c	d	a	b
d	d	d	b	a

答：{a,b},{c,d}

例2：$<I,+>$，在I上定义R: $<x,y>\in R \Leftrightarrow |x|=|y|$，

问R是$<I,+>$的同余关系否?

解:1) 自反性：$\forall x\in I, |x|=|x| \therefore <x,x>\in R$。

2) 对称性：$\forall x,y\in I$，若$<x,y>\in R$则$|x|=|y| \therefore <y,x>\in R$。

3) 传递性：$\forall x,y,z\in I$，若

$<x,y>\in R, <y,z>\in R \therefore |x|=|y|=|z| \therefore <x,z>\in R$。

$\therefore$R是一等价关系。

$\forall x_1,y_1,x_2,y_2\in I$，若$<x_1,y_1>\in R, <x_2,y_2>\in R$,

$<x_1+x_2,y_1+y_2>\in R$ 成不成立?

不一定成立

举一个反例：如$<1,-1>\in R, <2,2>\in R$但$<1+2,-1+2>\notin R$,

$\therefore$R不是同余关系。

由此可见，等价关系未必都是同余关系。

定理5-8.4: 设$\langle A,* \rangle$是一个代数系统，R是A上的一个同余关系，$B=\{A_1,A_2,\cdots,A_r\}$是由R诱导的划分，则**必存在同态映射f，使$\langle B,★ \rangle$是$\langle A,* \rangle$的同态象**。

是否存在这个等价类

证:1)构造在B上运算★

定义：$\forall[a],[b]\in B$， 有 $[a]_R ★ [b]_R=[a*b]_R$

先证明此定义是合理的,即它确实是一个运算。

若$[a_1]_R=[a_2]_R,[b_1]_R=[b_2]_R$则$\langle a_1,a_2\rangle\in R,\langle b_1,b_2\rangle\in R$。

因为R是同余关系$\therefore \langle a_1*b_1,a_2*b_2\rangle \in R$即$[a_1*b_1]_R=[a_2*b_2]_R$。

$\therefore$ ★确实是一个运算。

2)构造映射$f: A\to B$，$\forall a\in A,f(a)=[a]_R$，再证f是一个同态映射，

$\forall x,y\in A,f(x*y)=[x*y]_R=[x]_R ★ [y]_R=f(x) ★ f(y)$，

$\therefore$ f是从$A\to B$的同态， 又$\forall[a]_R\in B,\exists a\in A$有$f(a)=[a]_R$。

$\therefore$ f是满同态 ， 证毕 。

可见，任一同余关系诱导一种同态的存在。

定理5-8.5: 设f是代数系统$<A,*>$到$<B,\bigstar>$的同态，定义A上的关系R: $<a,b>\in R \Leftrightarrow f(a)=f(b)$，那么，R是A上的一个同余关系。

证:1) 易证R是一个等价关系。

2) $<a,b>\in R, <c,d>\in R$,

$\therefore f(a)=f(b), f(c)=f(d)$,

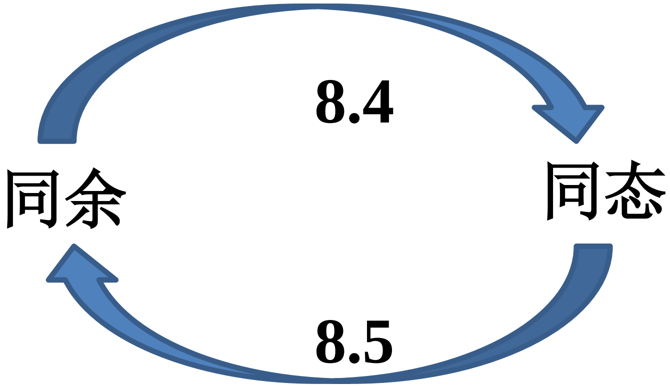
则$f(a*c)=f(a)*' f(c)=f(b)*' f(d)=f(b*d)$,

$\therefore <a*c,b*d>\in R$。

$\therefore$ R是A上的同余关系。

也即，任一同态映射可诱导一个同余关系

- 理解同态与同余之间的“诱导”



- 这是因为，其实 (教科书220页)
  - 同态象，可以看作是抽掉次要元素的情况下，对该系统的粗糙描述。
  - 同余类，也可以描述简要描述原系统的性态。

5.9 环与域

定义5-9.1 代数系统$<R,+,\cdot>$，若具有如下性质:

1) $<R,+>$是个阿贝尔群,
2) $<R,\cdot>$是个半群,
3) 乘法$\cdot$对加法$+$可分配，即

$$\forall a,b,c\in R,\ a\cdot(b+c)=a\cdot b+a\cdot c,\ 且\ (b+c)\cdot a=b\cdot a+c\cdot a,$$

称$<R,+,\cdot>$是一个环。

我们约定: a的加法逆元记为-a，a+(-b)可简写为a-b。

重要约定（参考）

环内有两个运算，每个运算都可能有单位元、逆元等特殊元素。

为方便起见，做如下约定：

- 设$< A, +, \cdot >$是一个环，加群$< A, + >$中的单位元通常记做0，称为零元（这个叫法是针对乘法的）。元素a在加群中的逆元记做$-a$，称为a的负元。如果乘法半群$< A, \cdot >$中有单位元，则称其为环A的单位元，记做1。如果乘法半群$< A, \cdot >$中某元素a有逆元，则称其为环A中元素a的逆元，记做a^{-1}。
- 可见，环中的单位元和逆元是针对乘法运算的，而加法运算中的单位元和逆元则称为零元和负元。
- 元素的倍数和幂定义为： $na = \underbrace{a + a + \cdots + a}_{n个a}$，$a^n = \underbrace{aa \ldots a}_{n个a}$

且满足$(na)b = a(nb) = nab$，$a^n a^m = a^{n+m}$, $(a^n)^m = a^{nm}$

例1.

1) $<I,+,\times>$ 是个环。

2) $<N_k,+_k,\times_k>$ 是个环。

证： ① $<N_k,+_k>$ 是个阿贝尔群， 0是加法幺元，

② $<N_k,\times_k>$ 是个半群。

③ $\forall a,b,c \in N_k \quad a\times_k(b+_k c)=a\times_k((b+c) \bmod k)$

$=(a\times(b+c)) \bmod k=(a\times b+a\times c) \bmod k$

$=(a\times b) \bmod k+_k(a\times c) \bmod k \;=(a\times_k b)+_k(a\times_k c)$

关于环

定理5-9.1: 设$\langle A,+,\cdot\rangle$是个环，$\forall a,b,c\in A$，

1)环的加法幺元必为环的乘法零元， 即 $\theta\cdot a=a\cdot\theta=\theta$。

证： $a\cdot\theta=a\cdot(\theta+\theta)=a\cdot\theta+a\cdot\theta$，由消去律可得： $a\cdot\theta=\theta$。

类似可证$\theta=\theta\cdot a$。

2)$(-a)\cdot b=a\cdot(-b)=-(a\cdot b)$

证:$(-a)\cdot b+a\cdot b=((-a)+a)\cdot b=\theta\cdot a=\theta$，

$\therefore(-a)\cdot b=-(a\cdot b)$。类似可证$a\cdot(-b)=-(a\cdot b)$。

3) $(-a)\cdot(-b)=a\cdot b$ (教科书 pp.224)

证:$(-a)\cdot(-b)=-a\cdot(-b)=a\cdot b$（利用2）的结果）

4) $a\cdot(b-c)=a\cdot b-a\cdot c$

证:$a\cdot(b-c)=a\cdot(b+(-c))=a\cdot b+a\cdot(-c)=a\cdot b+(-(a\cdot c))=a\cdot b-a\cdot c$

5) $(b-c)a=ba-ca$（类似4）的证明）

三种特殊的环

定义5-9.2: 设<R,+,·>是环,

若<R,·>是可交换的，称<R,+,·>为**交换环**。

若<R,·>含么元，称<R,+,·>为**含么环**。

若$\exists a,b \in A$，$a \neq \theta$，$b \neq \theta$，使$a \cdot b = \theta$，称<A,+,·>是含零因子环，其中a,b称为零因子；否则称为**无零因子环**。

注：无零因子：$\forall a,b \in A$，$a \neq \theta, b \neq \theta$，则必有$a \cdot b \neq \theta$

例如，<I, +, · >就是无零因子环。

※教科书中没有零因子的定义

关于无零因子环的判定

定理5-9.2 环<A,+,·>是无零因子环当且仅当乘法消去律成立，也即对于$c\neq\theta$且$c\cdot a=c\cdot b$，必有$a=b$。

证明：

1：若无零因子，设$c\neq\theta$且$c\cdot a=c\cdot b$，则

$c\cdot(a-b)=\theta$，则$a-b=\theta$，则$a=b$，即

消去律成立；

2：若消去律成立，即$c\neq\theta$且$c\cdot a=c\cdot b$，必有$a=b$，

即 $c\neq\theta$ 且$a\neq b$，必有$c\cdot a\neq c\cdot b$，

即 $c\neq\theta$ 且$a\neq b$，必有$c\cdot(a-b)\neq\theta$，则无零因子

一个更特殊的环

定义5-9.3: 设$<A,+,\cdot>$是环，如果满足：

① $<A,+,\cdot>$既是交换环；

② $<A,+,\cdot>$还是含幺环；

③ $<A,+,\cdot>$且是无零因子环；

则称$<A,+,\cdot>$为**整环**。

例2. 1) $<I,+,\times>$是整环。

2) $<N_4,+_4,\times_4>$不是整环。

域

定义5-9.4: 设代数系统$<A,+,\cdot>$满足

1)$<A,+>$是阿贝尔群；

2)$<A-\{\theta\},\cdot>$是阿贝尔群；

3)运算$\cdot$对$+$可分配，

则称$<A,+,\cdot>$是**域**。

例

1) Q为有理数集合，$<Q,+,\times>$是一个域。

R为实数集合，$<R,+,\times>$是一个域。

C为复数集合，$<C,+,\times>$是一个域。

2) I为整数集，$<I,+,\times>$不是域。

关于域

定理5-9.3：域一定是整环。

证明：（判断消去律是否成立）

证明无零因子环

设$<A,+,\cdot>$是任一域。

对于$\forall a,b,c \in A$且$a \neq \theta$,

如果有$a \cdot b = a \cdot c$,（1是乘法幺元）则

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$$

$$= (a^{-1} \cdot a) \cdot c = 1 \cdot c = c$$

因此，$<A,+,\cdot>$是一个整环。

定理5-9.4　有限整环必是域。

证：（判断是否有逆元）

整环有幺元，交换

设$<A,+,\cdot>$是有限整环，$\forall a,b,c \in A$且$c \neq \theta$(证明c逆存在).

若$a \neq b$，由无零因子推出的可约律，则$a \cdot c \neq b \cdot c$，

因为A为有限集，由运算封闭性

$\therefore$设$A-\{\theta\}=\{a_1,\ldots,a_n\}$，则$A-\{\theta\}=\{ca_1,\ldots,ca_n\}=c(A-\{\theta\})$。

$\therefore \forall c \in A, \exists d$有$c \cdot d=e$　$\therefore$ c逆元存在为d 。

$\therefore <A-\{\theta\},\cdot>$是阿贝尔群。

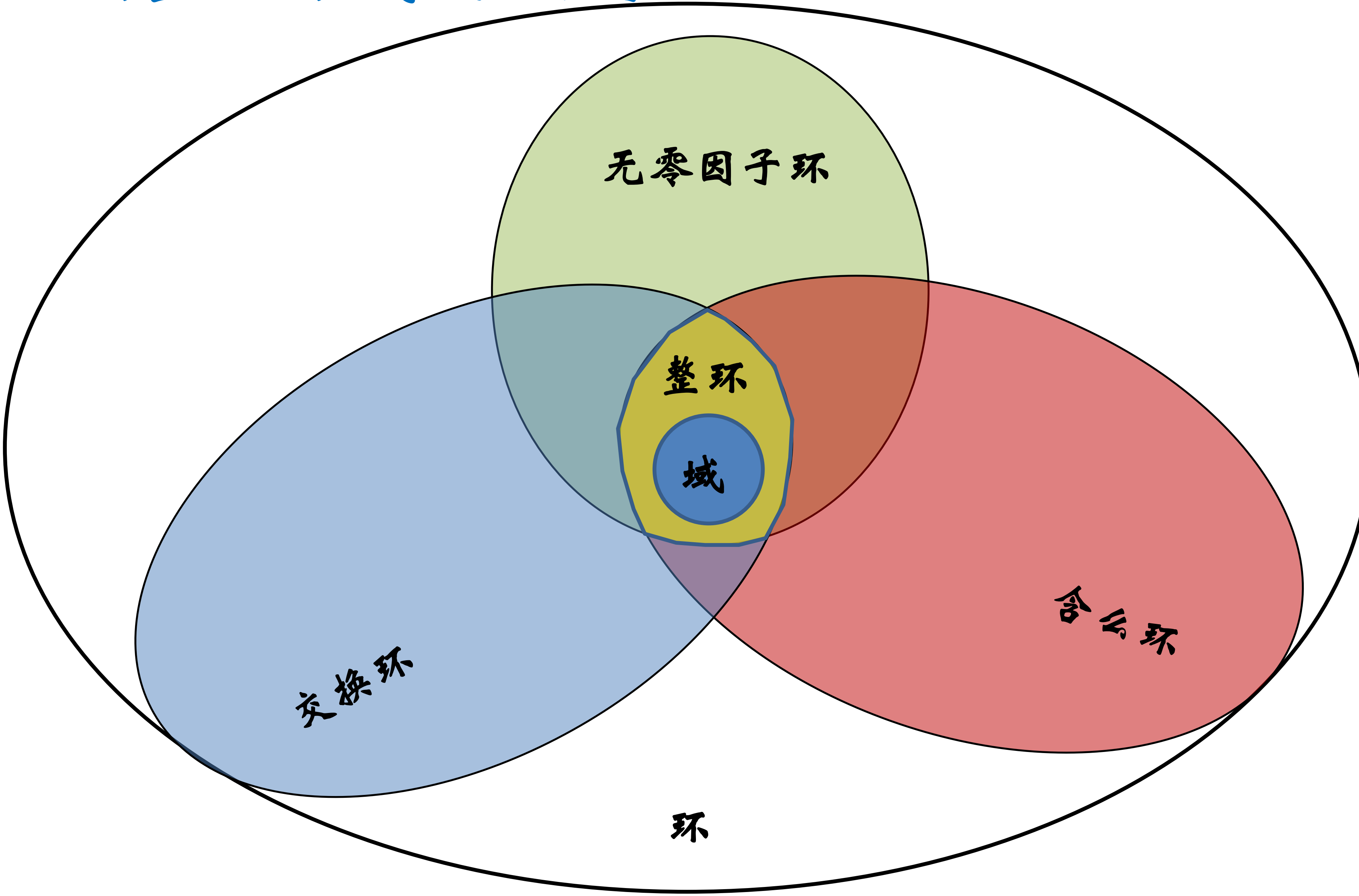
因为有限整环满足分配律，$\therefore <A,+,\cdot>$是域。

- 无限整环未必是域。

例如，$<I,+,\times>$是整环，却不是域！

可见，域是一种特殊的整环。

环，整环，域的关系



环的同态

定义5-9.5: 设$<A,+,\cdot>$，$<B,\oplus,\odot>$是环，若$\exists f: A\to B$，$\forall a,b\in A$有$f(a+b)=f(a)\oplus f(b)$，$f(a\cdot b)=f(a)\odot f(b)$，称 f 是 $<A,+,\cdot>$ 到 $<B,\oplus,\odot>$的**环同态**。

定理5-9.5: 环的同态象必定是一个环。

证:由群同态,半群同态知:是$<f(A),\oplus>$是阿贝尔群,$<f(A),\odot>$是半群，又因为 $f(a)\odot(f(b)\oplus f(c))$

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

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

$$=f(a)\odot f(b)\oplus f(a)\odot f(c)$$

分配律

所以 $<f(A),\oplus,\odot>$是一个环。

对于域来说，该结论不成立。