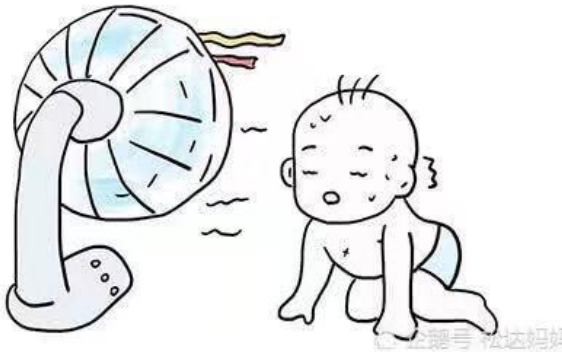
离散数学

Discrete Mathematics

<G,*>：半群，含幺半群，子群，元素周期，循环群，对称群与置换群，有限群中拉格朗日定理，陪集，正规子群与商群。

<A,+,*>： Ring（环）与（域）Fields
整环，除环，域，素域与域的特称理想与商环

<L,≤>格 与 布尔代数<B,⊕,*>



§6.1 定义及基本性质 (1)

6.1.1 环

假设 <A,+,*> 是一个代数系统，其中，+和 * 都是集合 A 上的二元运算，如果满足：

（1）<A,+> 是交换群（Abel群）；

（2）<A,*> 是半群；

（3） * 对+ 是可分配的；

则称 <A,+,*> 是一个环**(Ring)**。

§6.1 定义及基本性质 (1)

6.1.1 环

例 $<Z,+,\times>$ 是一个环。

$<Z,+>$ 是Abel群。 $<Z,\times>$是半群。 $\times$对+是可分配的; 整数环

例 $<Q,+,\times>$ 是一个环。

例 $<R,+,\times>$ 是一个环。

例$<Z_m,+_m,\times_m>$是一个环。 模**m**剩余环。

§6.1　定义及基本性质

例 **n**阶整数矩阵所成集合 $(\mathbf{Z})_n$,关于矩阵的加法与乘法作成一个环.

n阶有理数矩阵集合$(\mathbf{Q})_n$，**n**阶实数矩阵集合 $(\mathbf{R})_n$, 在矩阵加法与乘法运算下也均构成环。

例 **x**的一切整（有理、实）系数多项式所成集合**Z[x]**（**Q[x]**，**R[x]**）在多项式加法与乘法运算下构成环.

§6.1　定义及基本性质

例　设i是虚数单位，即$i^2=-1$，令

$$Z(i)=\{a+bi \mid a, b\in Z\}$$

则$<Z(i),+,\cdot>$是一个环。

通常称作高斯环.

§6.1　定义及基本性质

6.1.2 环的性质

假设 <A,+,*> 是一个环。

（1）因为<A,+>是Abel群，所以+满足结合性、交换性、消去律，<A,+>中有单位元。

§6.1 定义及基本性质 (3)

6.1.2 环的性质

约定：$a^n = a+a+\ldots+a = na$;

对$\forall a,b\in A$, $(a+b)^n = na+nb$;

$a^{m+n} = a^m+a^n = (m+n)a$;

$a^{mn} = (a^m)^n = n(ma)$。

§6.1 定义及基本性质 (4)

6.1.2 环的性质

（2）假设 e 是<A,+>的单位元，对∀a,b,c∈A有：

① a * e = e * a = e （θ *a=a* θ = θ)

对∀a,b,c∈A有：a*(b+c)=a*b+a*c

∵e+e=e ∴ a*(e+e)=a*e a*e+a*e=a*e=a*e+e

∴ a * e =e 同理 e * a = e

所以 在环中加法单位元一定是乘法零元。 e (θ)

例如 <Z,+, × > , +单位元e=0，是 × 的零元θ=0

§6.1 定义及基本性质 (4)

6.1.2 环的性质

（2）假设 e 是<A,+>的单位元，对∀a,b,c∈A有：

② $a * b^{-1} = a^{-1} * b = (a*b)^{-1}$

例：<Z,+, · >，+单位元0，是 · 的零元

$2 \cdot 3^{-1} = 2^{-1} \cdot 3 = (2 \cdot 3)^{-1} = -6$

§6.1 定义及基本性质 (4)

6.1.2 环的性质

（2）假设 e 是<A,+>的单位元，对∀a,b,c∈A有：

③ $a^{-1} * b^{-1} = a * b$ $(a*b)^{-1}=a*b^{-1}=a^{-1}*b$

$(a*b)+(a^{-1}*b)=(a+a^{-1})*b=e*b=e$

$(a^{-1}*b)+(a*b)=(a^{-1}+a)*b=e*b=e$

$(a*b)^{-1}=a^{-1}*b$ 同理 $(a*b)^{-1}=a*b^{-1}$

$a^{-1}*b=a*b^{-1}$ （1） $a * b = (a^{-1})^{-1} * b = a^{-1} * b^{-1}$

例如： $<Z,+,\cdot>, 2^{-1}\cdot 3^{-1} = 2\cdot 3 = 6$

§6.1 定义及基本性质 (4)

6.1.2 环的性质

（2）假设 e 是<A,+>的单位元，对$\forall a,b,c\in A$有：

④ $a*(b+c^{-1}) = (a*b)+(a*c)^{-1}$

$a*(b+c^{-1}) = a*b+a*c^{-1} = (a*b)+(a*c)^{-1}$

⑤ $(b+c^{-1})*a = (b*a)+(c*a)^{-1}$

§6.1 定义及基本性质 (4)

6.1.2 环的性质

（2）假设 e 是<A,+>的单位元，对∀a,b,c∈A有：

① $a * e = e * a = e$

② $a * b^{-1} = a^{-1} * b = (a*b)^{-1}$

③ $a^{-1} * b^{-1} = a * b$;

④ $a*(b+c^{-1}) = (a*b)+(a*c)^{-1}$

⑤ $(b+ c^{-1}) * a = (b*a)+(c*a)^{-11}$

$0a = a0 = 0$

$a(-b) = (-a)b = -(ab)$

$(-a)(-b) = ab$

$a(b-c) = ab-ac$

$(b-c)a = ba-ca$

例 1： 假设 <G,*> 是一个二阶群，则 <G×G,*>是一个Klein群。

*	<e,e>	<e,a>	<a,e>	<a,a>
<e,e>	<e,e>	<e,a>	<a,e>	<a,a>
<e,a>	<e,a>	<e,e>	<a,a>	<a,e>
<a,e>	<a,e>	<a,a>	<e,e>	<e,a>
<a,a>	<a,a>	<a,e>	<e,a>	<e,e>

<e,e>记为e, <e,a>记为a, <a,e>记为b, <a,a>记为c,

<K,*>是Klein四元群。K={e,a,b,c};

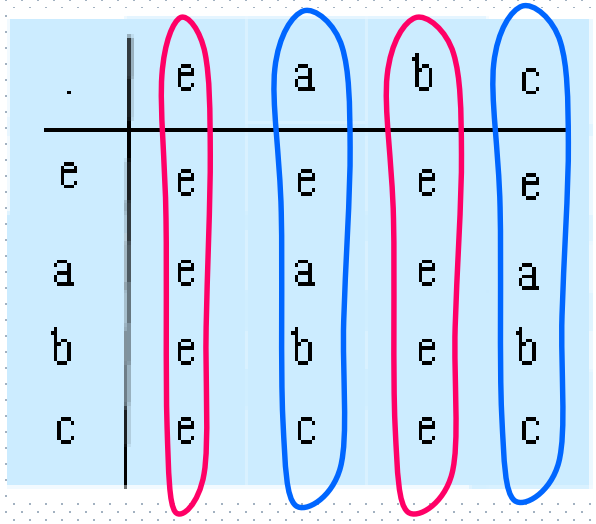
“.”运算定义如下，则<K,*，.>是环。

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

.	e	a	b	c
e	e	e	e	e
a	e	a	e	a
b	e	b	e	b
c	e	c	e	c

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

（1）<K,*>是Abel群



（2）<K，.>是半群（封闭、可结合）

∀x，y，z∈K 有(x . y) . z=x .(y . z)

若z=e或z=b 则(x . y) . z=e=x .(y . z)

若z=a或z=c 则(x . y) . z=x . y=x .(y . z)

所以 <K，.>是半群

*对.可分配

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

.	e	a	b	c
e	e	e	e	e
a	e	a	e	a
b	e	b	e	b
c	e	c	e	c

.对* 是可分配

(y * z) . x=(y *x).(z*x) ; x .(y * z) =(x* y).(x*z)

若x=e或x=b 则(y * z) .x=e=e.e=(y *x).(z*x)

若x=a或x=c 则(y * z) .x=y*z=(y *x).(z*x)

同理：x.(y * z) =(x* y).(x*z)

所以<K,*，.>是环

例2：s是非空集合，**P(s)**是幂集，在**P(s)**上定义二元运算+和*，则**< P(s),+，· >**是环。

$\forall A，B \in \mathbf{P(s)}$

$A+B = \{ x \mid x \in S \wedge (x \in A \vee x \in B) \wedge x \notin A \cap B \}$

$A \cdot B = A \cap B$

S={a，b，c}，

P(s)={∅，{a},{b},{c},{a,b},{a,c},{b,c},{a,b,c}},

∀A，B∈P(s)

（1）封闭，{a}+{a,b}={b}，…

可结合，({a}+{a,b})+{c}={a}+({a,b}+{c})，…

可交换，{a}+{a,b}={a,b}+{a}，…

单位元，∅

逆元，{a}+{a}= ∅,{a}自身为逆元，…

< P(s), +>是abel群

（2）< P(s),·>是半群，

·可结合 ({a} · {a,b}) ·{a,b,c}={a} ·({a,b} ·{a,b,c})

(3)·对+可分配

{a} ·({b}+{a,b})={a} ·{b}+{a} ·{a,b}

例3：证明 任一环的同态象也是一环。

证明：设 <A,+, · >是一环,且<f(A), ⊕, ⊗ > 是关于同态映射f的同态象。

由f(A)的定义， f(A)为 f 的值域，所以 f一定是满同态。

由 <A,+>是Abel群，易证 <f(A), ⊕>也是Abel群。

是<A,*>半群，易证 <f(A), ⊗ >也是半群。

现只需证： ⊗对 ⊕是可分配的。

$\forall b_1, b_2, b_3 \in f(A)$，则必有相应的$a_1, a_2, a_3$使得：$f(a_i) = b_i, i = 1,2,3$

$$b_1 \otimes (b_2 \oplus b_3) = f(a_1) \otimes (f(a_2) \oplus f(a_3)) = f(a_1) \otimes (f(a_2 + a_3))$$
$$= f(a_1 \cdot (a_2 + a_3)) = f((a_1 \cdot a_2) + (a_1 \cdot a_3)) = f(a_1 \cdot a_2) \oplus f(a_1 \cdot a_3)$$
$$= (f(a_1) \otimes f(a_2)) \oplus (f(a_1) \otimes f(a_3))$$
$$= (b_1 \otimes b_2) \oplus (b_1 \otimes b_3)$$

同理可证 $(b_2 \oplus b_3) \otimes b_1 = (b_2 \otimes b_1) \oplus (b_3 \otimes b_1)$

因此$< f(A), \oplus, \otimes >$也是环。

§6.1　定义及基本性质

6.1.3 由 * 运算确定的几种环

（1）在环 <A,+,*> 中，如果 <A,*> 是含幺半群，并且 e′ 是单位元，则称 e′ 为环的单位元。这时称 A 为有**单位元的环**（**有/含幺环**）。如果元素 a 在 <A,*> 中有逆元，则在含有单位元的环中，该元素的逆也称为环中元素的逆。

§6.1　定义及基本性质　　(6)

6.1.3 由 * 运算确定的几种环

（2）如果环中只含有一个元素，此时该元素应该是 <A,+> 中的单位元，当然也是 <A,*> 中的零元，所以这种环称为零环。

环 A = { θ(e) } 称为零环.

定理 1　设**A**为有单位元的环，且不只含一个元素，
则 $1 \neq 0$。(0 加法单位元，　1 乘法单位元)

证明　若 $1 = 0$，则　$\forall\, \mathbf{a} \in \mathbf{A}$,

$$\mathbf{a} = \mathbf{a} \cdot 1 = \mathbf{a} \cdot 0 = 0$$

故**A**只含一个元素 0，矛盾。

以后提到有单位元的环时，总指非零环。

因此 $1 \neq 0$ 总成立。

（3）设 <A,+,*> 是环，当 <A,*> 是可交换半群时，称 <A,+,*> 是可交换环。

例3：

全体整数按普通加法和普通乘法构成有单位元（1）可交换（*）的环。

摸m的全体剩余类构成什么环？

有单位元（$\times_4$ 的单位元1），可交换环（$\times_4$）

多选题 2分

设置

全体偶数按普通加法和普通乘法构成环，环的类型是：。

A 有单位元

B 无单位元

C 可交换

D 不可交换

提交

多选题 2分

设置

$<Z_4,+_4,\times_4>$是一个环，可以构成的环的类型为：

A 有单位元

B 可交换

C 无单位元

D 不可交换

提交

多选题 2分

设置

$<Z_5,+_5,\times_5>$是一个环，可以构成的环的类型为：

A 有单位元

B 可交换

C 无单位元

D 不可交换

提交

多选题 2分

设置

实系数多项式的全体按普通加法和普通乘法可以构成的环的类型为：

A 有单位元

B 可交换

C 无单位元

D 不可交换

提交

多选题 2分

设置

全体n阶方阵按矩阵的加法和乘法可以构成的环的类型为：

A 有单位元

B 可交换

C 无单位元

D 不可交换

提交

§6.2　整环、除环和域

6.2.1 零因子

设 $<A,\star,*>$ 是环，如果存在 $a,b\in A$，这里 $a\neq\theta$，$b\neq\theta$，但 $a*b=\theta$，则称 a 为 A 中的左零因子，b 为 A 中的右零因子，左、右零因子统称为零因子。

§6.2 整环、除环和域 (2)

6.2.1 零因子

例如：$<Z_4,+_4,\times_4>$是一个环。其中,$+_4,\times_4$ 的运算表如下：

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\times_4$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

$\times_4$是否有零因子？

$[2]\times_4[2]=[0]$

在$<Z_6,+_6,\times_6>$中有零因子？ $[2]\times_6[3]=[0]$

§6.2 整环、除环和域 (2)

6.2.1 零因子

例如 $<Z_5,+_5,\times_5>$是一个环。其中$\times_5$的运算表如下：

$\times_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[2]	[2]	[1]

无零因子。

§6.2 整环、除环和域 (2)

6.2.1 零因子

例如 $<Z_6,+_6,\times_6>$是一个环。其中$\times_6$的运算表如下：

$\times_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[2]
[4]	[0]	[4]	[2]	[0]	[2]	[2]
[5]	[0]	[5]	[4]	[2]	[2]	[1]

$[2]\times_6[3]=[0]$

$[3]\times_6[4]=[0]$

两对零因子。

[2]与[3]

[3]与[4]

§6.2　整环、除环和域

例　用 **(R)2**表示 2 阶实数矩阵集合，＋，·表示矩阵的加法与乘法，则〈**(R)2**，＋，·〉是一个环。

存在一对零因子。 $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$

还有其它零因子吗？ 有！

例　对于剩余环$\langle \mathbf{Z}_m, +_m, \times_m \rangle$，证明 若**m**不是素数，则$\mathbf{Z}_m$中必存在零因子.

证明：$\mathbf{Z}_m$中的零元为$[0]$．因为**m**不是素数，故存在整数n_1，n_2，使　$m=n_1n_2$　，　$1<n_1\leq n_2<m$

因此　$[n_1]\neq[0]$，　$[n_2]\neq[0]$，

但　$[n_1]\times \mathrm{m}\ [n_2]=[0]$.

即$[n_1]$，　$[n_2]$是$\mathbf{Z}_m$的一对零因子.

§6.2 整环、除环和域

6.2.1 零因子

当一个环中不含有零因子时，称它为无零因子环。即在无零因子环中，对任意的 $a,b\in A$，若 $a * b = \theta$，则必有 $a = \theta$ 或 $b = \theta$。

定理1：

设 $<A,+,*>$ 是无零因子的环，则 * 在 A 上消去律成立。**a***c=b*c 或c***a**=c*b 得 **a**=b ;反之亦然。

$<A,+,*>$ 是无零因子的环 $\Leftrightarrow$ * 在 A 上消去律成立

§6.2 整环、除环和域

证明 无零因子的环中消去律成立

设**R**中无零因子，$\forall c\neq 0$，如果 $ac=bc$，

则 $ac-bc=0$，$(a-b)c=0$.

由于$c\neq 0$，**R**中无零因子，故 $a-b=0$，即$a=b$.

同理$ca=cb \Rightarrow a=b$;

反之，设环**R**中乘法消去律成立，

反证法 若**R**中有零因子$a\neq 0$，$b\neq 0$，使得 $ab=0$

又因为 $a0=0$ 所以，$ab=a0$

由消去律得 $b=0$，矛盾.

故**R**中必无零因子.

§6.2 整环、除环和域

6.2.2 整环

设 **<A,+,*>** 是无零因子环，并且是可交换的含幺环，则称它为整环。

即 **<A,+,*>** 是环，并且 **<A,*>** 有单位元，* 运算可交换，对 $\forall a,b\in A$，若 $a*b=\theta$，则必有 $a=\theta$ 或 $b=\theta$。

e(θ)* e′=e(θ) 应该如何理解？ **x* e′=x**

§6.2 整环、除环和域

例**4**：全体有理数按普通加法和普通乘法构成无零因子的交换环，所以是整环。

全体实数、复数？（可以构成 整环）

§6.2 整环、除环和域

例：整数环〈**Z**，＋，·〉是一个整环，

高斯环〈**Z[i]**，＋，·〉是一个整环.

例：若**m**是一个素数，则〈$\mathbf{Z}_m$，$+_m$，$\times_m$〉是一个整环.

（若 $[i]\times_m[j]=[0]$，则
$[ij]=[0]$，因而 **m | ij** 故**m | i** 或 **m | j**，［**i**］
$=[0]$ 或 ［**j**］$=[0]$）

〈$\mathbf{Z}_m$，$+_m$，$\times_m$〉是整环 $\Leftrightarrow$ m为素数

野人与传教士

图论

环、整环、除环和域

（1）环〈A，＋，·〉环，加法单位元是乘法零元。

（2）零环，可交换环，含幺环。

（3）零因子，无零因子的环 ⇔ 乘法消去律成立。

（4）整环:无零因子，可交换，含幺元。

〈Z_m，$+_m$，$\times_m$〉是整环 ⇔ m为素数

多选题 4分

设置

s是集合，P(s)是幂集，在P(s)上定义二元运算+和·，
则< P(s),+，· >构成的环的类型是：

$\forall A，B \in P(s)\ A \cdot B = A \cap B$

$A+B = \{ x \mid x \in S \wedge (x \in A \vee x \in B) \wedge x \notin A \cap B \}$

- A 有单位元
- B 无单位元
- C 可交换
- D 不可交换
- E 有零因子
- F 无零因子

提交

例4：s是集合，P(s)是幂集，在P(s)上定义二元运算+和*，则< P(s),+，· >不是整环。

$\forall A，B \in P(s)$

$A+B = \{ x \mid x \in S \wedge (x \in A \vee x \in B) \wedge x \notin A \cap B \}$

$A \cdot B = A \cap B$

<P(S), + > 中的单位元是∅，同时也是<P(S), · > 中的零元

<P(S), · > 中的单位元是S，并且S≠∅，

若 S1是S的任意真子集（$S1 \subseteq S$ ），并且$S_1 \neq \varnothing$，

取$S_2 = S - S1 \neq \varnothing$

但是$S_1 \cdot S_2 = S1 \cap S2 = \varnothing$

所以<P(S), +，· >中含有一对零因子S1,S2。

故 <P(S), +，· >不是整环。（可交换，有单位元）

例5：证明 <{0,1},⊕,⊗>是一个整环，其中运算 ⊕和 ⊗定义如下图。

⊕	0	1
0	0	1
1	1	0

二进制1位数加

⊗	0	1
0	0	0
1	0	1

二进制1位数乘

整环：有单位元，无零因子的交换环为整环.

一、 **<{0,1},⊕>**是交换群

<{0,1},⊕>是交换群：首先运算是封闭的，是一个代数系统，

(1)结合律：

(0⊕0)⊕0＝0⊕(0⊕0)=0

(0⊕0)⊕1= 0⊕(0⊕1)=1

(0⊕1)⊕0 = 0⊕(1⊕0)=1

(0⊕1)⊕1= 0⊕(1⊕1)=0

(1⊕0)⊕0= 1⊕(0⊕0)=1

(1⊕0)⊕1= 1⊕(0⊕1)=0

(1⊕1)⊕0= 1⊕(1⊕0)=0

(1⊕1)⊕1= 1⊕(1⊕1)=1

(2)单位元：0 0⊕0＝0 0⊕1＝1

(3)逆元：0⊕0＝0，1⊕1＝0，0的逆元是0，1的逆元是1

(4)交换律：0⊕0＝0⊕0＝0;0⊕1＝1⊕0＝1;1⊕1＝1⊕1＝1

所以 <{0,1},⊕>是交换群

二、<{0,1},⊗>可交换的半群：首先运算是封闭的，是一个代数系统，

结合律： (0⊗0) ⊗0＝0⊗ (0⊗0)=0

(0⊗0) ⊗1= 0⊗ (0⊗1) =0

(0⊗1) ⊗0 = 0⊗ (1⊗0) =0

(0⊗1) ⊗1= 0⊗ (1⊗1) =0

(1⊗0) ⊗0= 1⊗ (0⊗0) =0

(1⊗0) ⊗1= 1⊗ (0⊗1) =0

(1⊗1) ⊗0= 1⊗ (1⊗0) =0

(1⊗1) ⊗1= 1⊗ (1⊗1) =1

交换　　交换律：0⊗0=0⊗0=0；0⊗1=1⊗0=0；1⊗1=1⊗1=1

单位元　　单位元：1⊗0＝0，1⊗1＝1，单位元1

三、⊗对⊕满足分配律：　0⊗(0⊕0) = (0⊗0)⊕(0⊗0)=0

0⊗(0⊕1) = (0⊗0)⊕(0⊗1)=0

0⊗(1⊕0) = (0⊗1)⊕(0⊗0)=0

0⊗(1⊕1) = (0⊗1)⊕(0⊗1)=0

1⊗(0⊕0) = (1⊗0)⊕(1⊗0)=0

1⊗(0⊕1) = (1⊗0)⊕(1⊗1)=1

1⊗(1⊕0) = (1⊗1)⊕(1⊗0)=1

1⊗(1⊕1) = (1⊗1)⊕(1⊗1)=0

(0⊕0) ⊗0= (0⊗0)⊕(0⊗0)=0

(0⊕1) ⊗0= (0⊗0)⊕(1⊗0)=0

(1⊕0) ⊗0 = (1⊗0)⊕(0⊗0)=0

(1⊕1) ⊗0= (1⊗0)⊕(1⊗0)=0

(0⊕0) ⊗1= (0⊗1)⊕(0⊗1)=0

(0⊕1) ⊗1= (0⊗1)⊕(1⊗1)=1

(1⊕0) ⊗1= (1⊗1)⊕(0⊗1)=1

(1⊕1) ⊗1= (1⊗1)⊕(1⊗1)=0

无零因子：**<{0,1},⊕,⊗>**中，不等于**0**的元素只有**1**，因为**1*1=1,**所以，不存在非零元素**b**，使得**1*b=0,** 或**b*1=0**

一、**<{0,1},⊕>**是交换群;

二、**<{0,1},⊗>**可交换的半群;

三、 ⊗对⊕满足分配律，无零因子，有单位元，可交换

所以，**<{0,1},⊕,⊗>**是整环。

例6：设 $<A_1,\bigstar,*>$,$<A_2,\bigstar,*>$都是环，$A_1\times A_2$ 是环的直积定义为：$A_1\times A_2=\{<a,b>|a\in A_1,b\in A_2\}$。

在 $A_1\times A_2$ 上定义运算 $\oplus$ 和 $\otimes$ 如下：

对任意的$<a_1,b_1>,<a_2,b_2>\in A_1\times A_2$，则

$$<a_1,b_1>\oplus<a_2,b_2>=<a_1\bigstar a_2,b_1\bigstar b_2>$$

$$<a_1,b_1>\otimes<a_2,b_2>=<a_1 * a_2, b_1 * b_2>$$

证明：

（1）$<A_1\times A_2,\oplus,\otimes>$构成环；

（2）若 A_1,A_2 都是有单位元的环，则 $A_1\times A_2$也是吗？

（3）若 A_1,A_2 都是无零因子的环，则 $A_1\times A_2$也是吗？

<A1×A2,⊕>交换群

首先运算是封闭的，是一个代数系统：

对任意的<a1,b1>,<a2,b2>∈ A1×A2，　<a1,b1>⊕<a2,b2>=<a1★a2,b1★b2>

因为<A1, ★,*> ,<A2, ★,*>都是环，所以★运算在A1，A2上封闭，

a1∈A1，a2∈A1, 所以，a1★a2∈A1,

b1∈A2，b2∈A2,所以，b1★b2∈A2，

所以<a1★a2,b1★b2>∈A1×A2

所以封闭

结合律：

对任意的<a1,b1>,<a2,b2><a3,b3>∈ A1×A2，

(<a1,b1>⊕<a2,b2>)⊕<a3,b3>＝< (a1★a2)★a3, (b1★b2)★b3>

<a1,b1>⊕(<a2,b2>⊕<a3,b3>)＝< a1★(a2★a3), b1★(b2★b3)>

因为<A1, ★,*> ,<A2, ★,*>都是环，所以<A1, ★> ,<A2, ★>满足结合律

所以(a1★a2)★a3＝a1★(a2★a3)，(b1★b2)★b3＝b1★(b2★b3)

所以< (a1★a2)★a3, (b1★b2)★b3>＝< a1★(a2★a3), b1★(b2★b3)>

所以(<a1,b1>⊕<a2,b2>)⊕<a3,b3>＝<a1,b1>⊕(<a2,b2>⊕<a3,b3>)

所以满足结合律

单位元：
设<A1, ★> ,<A2, ★>上单位元分别是e1,e2
则，任取<a1,b1>∈ A1×A2， <a1,b1>⊕<e1,e2>=<a1★e1,b1★e2>=<a1,b1>
<e1,e2>⊕<a1,b1>=<e1★a1,e2★b1>=<a1,b1>
所以存在单位元<e1,e2>
逆元：
任取<a1,b1>∈ A1×A2，因为<A1,★,*> ,<A2,★,*>都是环，所以在<A1,★>上存在a1的逆元

单位元：
设<A1, ★> ,<A2, ★>上单位元分别是e1,e2
则，任取<a1,b1>∈ A1×A2， <a1,b1>⊕<e1,e2>=<a1★e1,b1★e2>=<a1,b1>
<e1,e2>⊕<a1,b1>=<e1★a1,e2★b1>=<a1,b1>
所以存在单位元<e1,e2>

逆元：

任取<a1,b1>∈ A1×A2，因为<A1, ★,*> ,<A2, ★,*>都是环，所以在<A1, ★>上存在 a1 的逆元 $a1^{-1}$，在<A2, ★>上存在 b1 的逆元 $b1^{-1}$，

<a1,b1>⊕<$a1^{-1}$, $b1^{-1}$>=<a1★ $a1^{-1}$, b1★ $b1^{-1}$>=<e1,e2>，所以<$a1^{-1}$, $b1^{-1}$>是<a1,b1>的逆元，所以，存在逆元

交换律：

对任意的<a1,b1>,<a2,b2>∈ A1×A2，<a1,b1>⊕<a2,b2>=<a1★a2,b1★b2>

<a2,b2>⊕<a1,b1>=<a2★a1, b2★b1>

因为<A1, ★,*> ,<A2, ★,*>都是环，所以<A1, ★>满足交换律，<A2, ★>满足交换律，所以，a1★a2＝a2★a1，b1★b2＝b2★b1，所以<a1★a2,b1★b2>＝<a2★a1, b2★b1>

所以，<a1,b1>⊕<a2,b2>＝<a2,b2>⊕<a1,b1>

所以，满足交换律

<A1×A2, ⊗>半群

首先运算是封闭的，是一个代数系统

对任意的<a1,b1>,<a2,b2>∈ A1×A2，　　<a1,b1>⊗<a2,b2>=<a1*a2,b1*b2>

因为<A1, ★,*> ,<A2, ★,*>都是环，所以*运算在 A1，A2 上封闭，

a1∈A1，a2∈A1,所以，a1*a2∈A1,

b1∈A2，b2∈A2,所以，b1*b2∈A2，

所以<a1*a2,b1*b2>∈A1×A2 所以封闭

结合律：

对任意的<a1,b1>,<a2,b2><a3,b3>∈ A1×A2，

(<a1,b1>⊗<a2,b2>)⊗<a3,b3>＝＜(a1*a2)*a3，(b1*b2)*b3>

<a1,b1>⊗ (<a2,b2>⊗<a3,b3>)＝＜a1*(a2*a3)，b1*(b2*b3)>

因为<A1, ★,*> ,<A2, ★,*>都是环，所以<A1, *> ,<A2, *>是半群，满足结合律

所以(a1*a2)*a3＝a1*(a2*a3)，(b1*b2)*b3＝b1*(b2*b3)

所以＜(a1*a2)*a3，(b1*b2)*b3>＝＜a1*(a2*a3)，b1*(b2*b3)>

所以(<a1,b1>⊗<a2,b2>)⊗<a3,b3>＝<a1,b1>⊗ (<a2,b2>⊗<a3,b3>)

所以满足结合律

⊗ 对 ⊕ 满足分配律

对任意的<a1,b1>,<a2,b2><a3,b3>∈ A1×A2，

<a1,b1>⊗ (<a2,b2>⊕<a3,b3>)＝＜a1*(a2★a3)，b1*(b2★b3)>

(<a1,b1>⊗ <a2,b2>)⊕(<a1,b1>⊗<a3,b3>)=<(a1*a2) ★(a1*a3),(b1*b2) ★(b1*b3)>

因为<A1, ★,*> ,<A2, ★,*>都是环,

所以，a1*(a2★a3)＝(a1*a2) ★(a1*a3)，b1*(b2★b3)＝(b1*b2) ★(b1*b3)

所以，＜a1*(a2★a3)，b1*(b2★b3)>＝<(a1*a2) ★(a1*a3),(b1*b2) ★(b1*b3)>

所以，<a1,b1>⊗ (<a2,b2>⊕<a3,b3>)＝(<a1,b1>⊗ <a2,b2>)⊕(<a1,b1>⊗<a3,b3>)

（<a1,b1>⊕<a2,b2>）⊗<a3,b3>＝＜（a1★a2）*a3,（b1★b2)*b3>

(<a1,b1>⊗ <a3,b3>)⊕(<a2,b2>⊗<a3,b3>)=<(a1*a3) ★(a2*a3),(b1*b3) ★(b2*b3)>

因为<A1, ★,*> ,<A2, ★,*>都是环,

所以，(a1★a2）*a3＝(a1*a3) ★(a2*a3)，（b1★b2)*b3＝,(b1*b3) ★(b2*b3)

所以，<（a1★a2）*a3,（b1★b2)*b3>=<(a1*a3) ★(a2*a3),(b1*b3) ★(b2*b3)>

所以，（<a1,b1>⊕<a2,b2>）⊗<a3,b3>=(<a1,b1>⊗ <a3,b3>)⊕(<a2,b2>⊗<a3,b3>)

所以满足分配律

（2）

A1,A2 都是有单位元的环，设其单位元分别为 E1，E2

任取<a1,b1>∈ A1×A2， <a1,b1>⊗<E1,E2>=<a1*E1,b1*E2>=<a1,b1>

<E1,E2>⊗<a1,b1>=<E1*a1,E2*b1>=<a1,b1>

所以存在单位元<E1,E2>

(3)<A1×A2,⊕,⊗>的零元是<e1,e2>

设<A1, ★> ,<A2, ★>上单位元分别是 e1,e2

则，任取<a1,b1>∈ A1×A2， <a1,b1>⊕<e1,e2>=<a1★e1,b1★e2>=<a1,b1>

<e1,e2>⊕<a1,b1>=<e1★a1,e2★b1>=<a1,b1>

所以存在单位元<e1,e2>

假设存在零因子<c1,c2><d1,d2>, <c1,c2>⊗<d1,d2>=<c1*d1,c2*d2>=<e1,e2>

即，c1*d1=e1，c2*d2=e2,

A1,A2 都是无零因子的环

因为 A1 无零因子，所以 c1，d1 中有至少一个等于 e1，

因为 A2 无零因子，所以 c2，d2 中有至少一个等于 e2，

（1）若 d1=e1, c2=e2

即取<c1,e2><e1,d2>,且 c1 不等于 e1, d2 不等于 e2

<c1,e2>⊗<e1,d2>=<c1*e1,e2*d2>

因为 c1*e1=e1,且 e2*d2=e2

则存在零因子<c1,e2><e1,d2>

（2）同理取 c1=e1，d2=e2，则存在零因子<e1,c2><d1,e2>

（3）若取 c1=d1= e1，c2,d2 中有一个为 e2,则<c1,c2><d1,d2>,中有一个等于<e1,e2>，矛盾，无零因子

（4）若取 c1=d1= e1，c2=d2=e2,则<c1,c2><d1,d2>,两个都等于<e1,e2>，矛盾，无零因子

所以，虽然 A1,A2 中都无零因子，A1×A2 中不一定无零因子

§6.2 整环、除环和域

6.2.3 除环、域

除环

假设 <A,+,*> 是一个代数系统，其中，+ 和 * 都是集合 A 上的二元运算，如果满足：

（1）<A,+> 是交换群（Abel群）；

（2）<A-{e}, * >是群；

（3） * 对+ 是可分配的；

则称 <A,+,*> 是一个除环。

§6.2 整环、除环和域

域

假设 <A,+,*> 是一个代数系统，其中，+和 * 都是集合 A 上的二元运算，如果满足：

（1）<A,+> 是交换群（Abel群）；

（2）<A-{e}, *>也是交换群（Abel群）；

（3） * 对+ 是可分配的；

则称 <A,+,*> 是一个域。

除环, 域的另一表示

设**R**是一个有 1 的环，$\hat{R}=R-\{0\}$ ，
如果〈$\hat{R}$，·〉是一个群，则称**R**为除环，
如果〈$\hat{R}$，·〉是一个可交换群，则称**R**为域.

（1）有单位元的环**R**是除环 ⇔ **R**中非零元的逆元都存在
⇔ $\hat{R}$ 构成乘法群 $\hat{R}=R-\{0\}$.

（2）有单位元的环**R**是域 ⇔ **R**是交换环,且**R**中非零元素均可逆.

§6.2 整环、除环和域

例 〈**Q**，＋，·〉，〈**R**，＋，·〉均是域，分别称为有理数域和实数域.

分析：〈**Q**，＋〉是交换群；〈**Q-{0}**，·〉是交换群

·对＋可分配，所以是域.

分析：〈**R**，＋〉是交换群；〈**R -{0}**，·〉是交换群

·对＋可分配，所以是域.

例 令 $\mathbf{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$；＋，·为通常数的加法和乘法，则〈$\mathrm{Q}[\sqrt{2}]$，＋，·〉是域.

§6.2 整环、除环和域

定理2：

设**R**是一个无零因子的有限环，且 | **R** | ≥ 2，则**R**必为除环。

证明　需要证明〈**R-{0}**，·〉为群.

由于 | **R** | ≥ 2，故**R-{0}**非空，

又，**R**中不含零因子，故**R-{0}**对 · 封闭，

从而〈 **R-{0}** ，·〉必构成半群，

且由定理 1 知，在该半群中消去律成立，从而〈 **R-{0}** ，·〉是一个满足消去律的有限半群，故必为群.

§6.2 整环、除环和域

定理2的推论。

推论： 有限整环必为域. （可交换，含幺，无零因子）

为什么？

（1）无零因子的有限环为除环（2）可交换的除环为域

无零因子⇔乘法削去律必成立

有限集，削去律成立⇔群

例如由于$\mathbf{Z}_p$是一个有限整环，知$\mathbf{Z}_p$为域（这个域称为素域）.

推论 若p为素数，则$\langle \mathbf{Z}_p, +_p, \times_p \rangle$为域.

$\langle \mathbf{Z}_p, +_p, \times_p \rangle$为有限整环。

$|\mathbf{Z}_p|=p$,无零因子，含幺，可交换

设P为素数，则代数系统 $<Z_p,+_p,\times_p>$为域

证明:因为对任意的 $[a],[b],[c]\in Z_p$

有 $[a]+_p([b]+_p[c])=[a]+_p[b+c]=[a+(b+c)]=[(a+b)+c]$

$=[a+b]+_p[c]=([a]+_p[b])+_p[c]$

$[a]\times_p([b]\times_p[c])=[a]\times_p[b\times c]=[a\times(b\times c)]=[(a\times b)\times c]$

$=[a\times b]\times_p[c]=([a]\times_p[b])\times_p[c]$

所以 $+_p,\times_p$ 满足结合律。

又有 $[a]+_p[b]=[a+b]=[b+a]=[b]+_p[a]$ $[a]\times_p[b]=[a\times b]=[b\times a]=[b]\times_p[a]$

所以 $+_p,\times_p$ 满足交换律。

又有 $[a]\times_p([b]+_p[c])=[a]\times_p[b+c]=[a\times(b+c)]=[a\times b+a\times c]$

$=[a\times b]+_p[a\times c]=([a]\times_p[b])+_p([a]\times_p[c])$

$\times_p$对$+_p$满足分配率

又因为对**[0]**是关于 $+_p$ 的幺元；对任意的 $[a]\in Z_p$ ，$[p-a]\in Z_p$ 是其逆元。

所以 $<Z_p,+_p>$ 是**abel**群，$<Z_p,+_p,\times_p>$ 是交换环。

由 $\times_p$ 运算的定义可知**[1]**是关于 $\times_p$ 的幺元。

而且对于 $[a],[b]\in Z_p$

若 $[a]\times_p[a]=[ab]=0$ 则**p|ab,**因为**P**是素数，所以必有**p|a** 或**p|b**

即**[a]=0**或**[b]=0,**那么 $<Z_p,+_p,\times_p>$ 中没有零因子，

所以，$<Z_p,+_p,\times_p>$ 是整环（无零因子，含幺，可交换）。而且为有限整环。

所以，$<Z_p,+_p,\times_p>$ 是域。

§6.2 整环、除环和域

设**F**是一个域，若**b**≠ 0 (**e**)，可将**b**$^{-1}$写成 $\frac{1}{b}$ ，**b**$^{-1}$**a**（或**ab**$^{-1}$）写成 $\frac{a}{b}$，在这种记号下，有以下性质成立.

（1） 设**b**≠ 0，**d**≠ 0，则

$$\mathbf{ad} = \mathbf{bc} \Leftrightarrow \frac{a}{b} = \frac{c}{d}$$

（2） 设**b**≠ 0，**d**≠ 0，则 .

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$$

§6.2 整环、除环和域

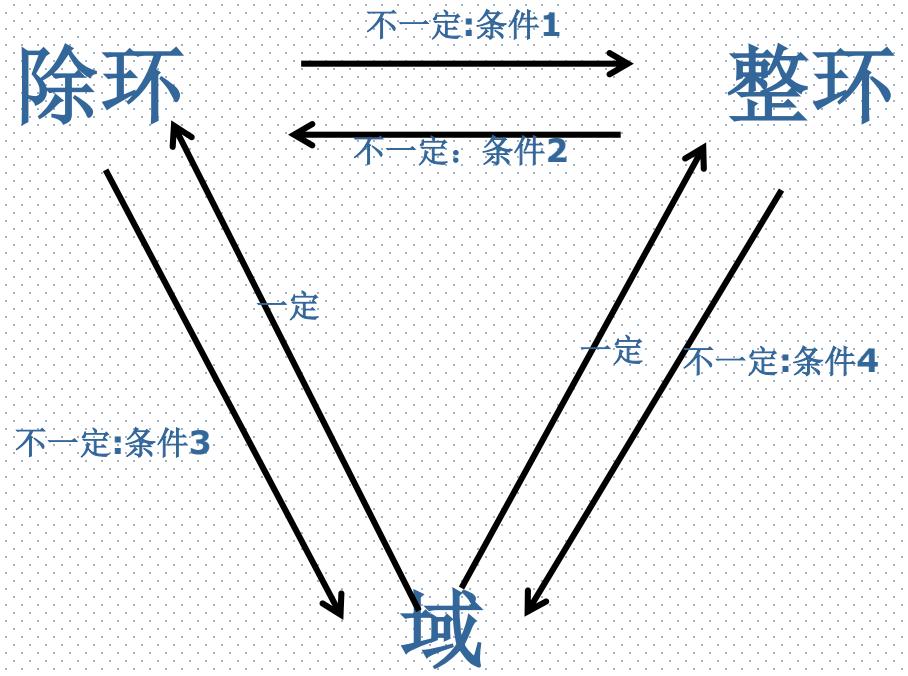
（3） 设$b\neq 0$，$d\neq 0$，则.

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

（4） 设$b\neq 0$，$c\neq 0$，$d\neq 0$，则.

$$\frac{a}{b}/\frac{c}{d}=\frac{ad}{bc}$$

整环、除环和域



条件1：除环如可交换则是整环。

<A,+,*>是除环，则<A-{e},*>是群

所以 *有单位元，*削去律成立，则无零因子

又可交换，是整环

条件2：如A-{e}每个元素都有逆元，则是除环。

条件3：可交换的除环是域。

条件4：A-{e}每个元素都有逆元的整环，是域。或有限整环也是域。

§6.2 整环、除环和域

6.2.3整环、域

例 证明：域一定是整环，并且域一定也是除环。

<A, +, *>是域。
则(1)<A, +>是Abel群；(2)<A-{e}, *>也是Abel群；(3)*对+可分配

是否满足构成整环的条件：
(1)<A, +>是Abel群；
(2)<A, *>是半群（封闭、可结合），且含幺元、无零因子、可交换。
<A-{e}, *>是Abel群，所以<A, *> 封闭、可结合，含幺元；且*可交换
<A, *>无零因子。
若存在零因子即a≠e, b≠e 但a*b=e,
则有a*b=e=a*e 由消去率得 b=e(矛盾)

证明：域一定是整环，但整环不一定是域。

整环不一定是域。因为<A-{e},*>中不一定保证任意元素的逆元存在
也就是说<A-{e},*>不一定构成Abel群。

满足什么条件的整环是域?

（1）A-{e}中任意元素的逆元都存在的**整环是域**

或者**(条件4 ?)**（2）可交换的除环**是域(条件3)　条件4 ？ 有限整环必是域。**

单选题 2分

设置

零环就是没有零因子的环。

A 正确

B 错误

提交

单选题 2分

设置

有幺元、可交换、无零因子的环一定是整环。

A 正确

B 错误

提交

单选题 2分

设置

可交换的除环一定是整环。

A 正确

B 错误

提交

单选题 2分

设置

可交换的除环一定是域。

A 正确

B 错误

提交

单选题 2分

设置

有限整环（有限集上的加、乘运算构成的环）一定是域。

A 正确

B 错误

提交

单选题 2分

设置

整环既然没有零因子，可交换，并且乘法单位元存在，因此整环中乘法削去律一定成立。

A 正确

B 错误

提交

单选题 2分

设 | A | ≥ 2 ， A是一个无零因子的有限环，则R必为除环。

A 正确

B 错误

提交

单选题 2分

设 <A,+, · >是环,<f(A), ⊕, ⊗ > 是环的同态象，则f是A→f(A)的满同态。

A 正确

B 错误

提交

作业

习题一 2，7

习题二 1，2，4，5

∀∃∅∩∪⊆⊂⊄∉∀∈≤≥…ℵ∑{ }≡±°∞

αβσρυωζψηδεφλμπΔ θ ±∏∧∨∀ }∴

√⊃

≌≈∽∞⊇∩∪℃‰≥≤∶·∏∈∑〈〉½¼ §

¥{}?± ↔∨∧¬→←⇒⇔

↓↑Λ⊕≠⊙— 〈〉

☆★▽〈〉⌒∴∵∪∩≠—— 〃

// ∴ ∵ ∶∶ ⊥ ↘ ↗ ↙ ↖ × √

〔 「– 」 ÷·º·‹2, b› ‿ Φ