离散数学

西安交通大学
计算机学院

离散数学

§5.环

- 环的基本概念
- 环的基本性质
- 无零因子环和含零因子环
- 整环与除环

离散数学

§5.环

定义1.环(ring)

设$(R, \oplus, \otimes)$是代数系统，$\oplus$和$\otimes$是R上的两个二元运算，若

(1) $(R, \oplus)$是交换群；

(2) $(R, \otimes)$是半群；

(3) $\otimes$对$\oplus$满足分配律：对任何$a,b,c \in R$，都有

$a\otimes(b\oplus c)=(a\otimes b)\oplus(a\otimes c)$

$(b\oplus c)\otimes a=(b\otimes a)\oplus(c\otimes a)$；

则称 $(R, \oplus, \otimes)$是环。

注：•在环中，由于$(R, \oplus)$是群，故关于$\oplus$有么元存在，将关于$\oplus$的么元记为0，称为环的零元。

•在环中，由于$(R, \oplus)$是群，故R中每个元素有逆元，设$a \in R$，将a关于$\oplus$的逆元记为-a，称为a 的负元，且将$a \oplus (-b)$简记为 a-b

(即在环中可定义减法运算)。

- 在环中，对于⊗运算，若有幺元，则记为1或e 。
- 在环中，设$a \in R$ ，若a关于⊗有逆元，则记为 a^{-1}。
- 以后谈到环，只讨论$|R| \geq 2$的情况，即不讨论一个元素的环。
- 在环的定义中，不要求⊕对⊗满足分配律，只要求 ⊗对⊕满足分配律。

例1. (I,+,×)是环。我们称此环为整数环。

这里：I是整数集合，+和×是整数的普通加法运算和普通乘法运算。由前两节知

(1)(I,+) 是交换群；

(2)(I, ×)是半群；

(3)×对+满足分配律：由算术知识知整数乘法对整数加法满足分配律。即$\forall a,b,c \in I$ 有

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

由×的交换律知×对+满足分配律；

由环的定义知(I,+, ×)是环。

离散数学

例2. $(M_{n\times n},+,\times)$是环。我们称此环为矩阵环。

这里：$M_{n\times n}$是 n × n阶实矩阵的全体，＋与×是矩阵的加法运算和乘法运算。由前两节知

(1) $(M_{n\times n},+)$是交换群；

(2) $(M_{n\times n},\times)$是半群；

(3)×对+满足分配律：由线性代数知，矩阵乘法对矩阵加法满足分配律。即 $\forall A,B,C\in M_{n\times n}$,有：

$$A\times(B+C)=(A\times B)+(A\times C)$$

$$(B+C)\times A=(B\times A)+(C\times A);$$

由环的定义知$(M_{n\times n},+,\times)$是环。

例3. $(N_m,+_m,\times_m)$是环。我们称此环为整数模环。

这里：$N_m=\{[0]_m,[1]_m,\ldots,[m-1]_m\}$，$+_m$和$\times_m$是$N_m$上的模加运算和模乘运算。由前两节知

(1) $(N_m,+_m)$是交换群；

(2) $(N_m,\times_m)$是半群；

(3)$\times_m$对$+_m$满足分配律：由于$\forall[i]_m,[j]_m,[k]_m\in N_m$,有

$$
\begin{aligned}
&[i]_m \times_m([j]_m +_m[k]_m)\\
&= [i]_m \times_m[(j+k) \bmod m]_m\\
&=[(i \times(j+k)) \bmod m]_m\\
&=[((i \times j)+(i \times k)) \bmod m]_m\\
&=[(i \times j) \bmod m]_m +_m[(i \times k) \bmod m]\\
&=([i]_m\times_m[j]_m)+_m([i]_m\times_m[k]_m)
\end{aligned}
$$

由$\times_m$的交换律知$\times_m$对$+_m$满足分配律；

由环的定义知$(N_m,+_m, \times_m)$是环。

离散数学

例4. $(2^X,\oplus,\cap)$是环。我们称此环为X的子集环

这里：X是一个非空集合， 2^X 是X的幂集， $\oplus$是集合的对称差运算, $\cap$是集合的交运算。由前两节知

(1) $(2^X,\oplus)$是交换群；

(2) $(2^X,\cap)$是半群；

(3)$\cap$对$\oplus$满足分配律：

由第一章§2定理6(8)知集合的交运算对对称差运算满足分配律。即$\forall a,b,c\in 2^X$，有

$$A\cap(B\oplus C)=(A\cap B)\oplus(A\cap C)$$

由$\cap$的交换律知$\cap$对$\oplus$满足分配律；

由环的定义知$(2^X,\oplus,\cap)$是环。

例5．$(P[x],+,\times)$是环。我们称此环为多项式环。

这里：$P[x]$ 是实系数多项式的全体，+和×是多项式的加法运算和乘法运算，由前两节知

(1) $(P[x],+)$是交换群；

(2) $(P[x],\times)$是半群；

(3)×对+满足分配律：

由于实数乘法对实数加法满足分配律，故多项式乘法对多项式加法满足分配律。即$\forall h(x),\ p(x),q(x)\in P[x]$, 有

$$h(x)\times(p(x)+q(x)) = (h(x)\times p(x))+(h(x)\times q(x))$$

由×的交换律知×对+满足分配律；

由环的定义知$(P[x],+,\times)$是环。

离散数学

定义2.交换环 含幺环 交换含幺环

设(R,⊕,⊗)是环。

(1)若⊗运算满足交换律，则我们称(R,⊕,⊗)是交换环。

(2)若关于⊗运算有幺元，则我们称(R,⊕,⊗)是含幺环。

(3)若⊗运算满足交换律又关于⊗运算有幺元，则我们称(R,⊕,⊗)是交换含幺环。

离散数学

例8. 在前面的例子中

(1)整数环$(I,+,\times)$是交换含幺环；关于$\times$运算的幺元是1；

(2)矩阵环$(M_{n\times n},+,\times)$是含幺环，但不是交换环；关于$\times$运算的幺元是单位矩阵E，矩阵乘法没有交换律；

(3)整数模环$(N_m,+_m,\times_m)$是交换含幺环；关于$\times_m$运算的幺元是$[1]_m$；

(4)X的子集环$(2^X,\oplus,\cap)$是交换含幺环；关于$\cap$运算的幺元是X；

(5)多项式环$(P[x],+,\times)$是交换含幺环；关于$\times$运算的幺元是零次多项式1；

离散数学

定理1. 环的基本性质

设 $(R,\oplus,\otimes)$是环。则$\forall a,b,c\in R$,有

(1)零元： $0\otimes a = a\otimes 0 = 0$ (加法幺元是乘法的零元)；

(2)正负、负正得负：$a\otimes(-b) = (-a)\otimes b = -(a\otimes b)$；

(3)负负得正：$(-a)\otimes(-b) = a\otimes b$；

(4)$(-1)\otimes a = -a$ (-1是乘法幺元1的负元)；

(5)$(-1)\otimes(-1)=1$ (-1的乘法逆元是其本身，即$(-1)^{-1}=-1$)；

(6)左分配律：$a\otimes(b-c)=(a\otimes b)-(a\otimes c)$ (乘法对减法的)；

右分配律：$(b-c)\otimes a=(b\otimes a)-(c\otimes a)$ (乘法对减法的)。

注：•由定理1(1)的结论知，在环$(R,\oplus,\otimes)$中，关于$\oplus$运算的幺元就是关于$\otimes$运算的零元。由于$(R,\oplus)$是交换群，故关于$\oplus$运算的幺元一定存在，因此关于$\otimes$运算的零元也一定存在。由于在一个代数系统中，零元是没有逆元的，因此在环$(R,\oplus,\otimes)$中，$(R,\otimes)$不能构成群。

离散数学

[证]. (1)只证$a\otimes 0 = 0$

$$
\begin{aligned}
a\otimes 0 &= (a\otimes 0)\oplus 0 \\
&= (a\otimes 0)\oplus((a\otimes 0)-(a\otimes 0)) \\
&= (a\otimes 0)\oplus((a\otimes 0)\oplus(-(a\otimes 0))) \\
&= ((a\otimes 0)\oplus(a\otimes 0))\oplus(-(a\otimes 0)) \quad \text{(结合律)} \\
&= (a\otimes(0\oplus 0))\oplus(-(a\otimes 0)) \quad \text{(分配律)} \\
&= (a\otimes 0)\oplus(-(a\otimes 0)) \quad (0\oplus 0 = 0) \\
&= (a\otimes 0)-(a\otimes 0) \\
&= 0 ;
\end{aligned}
$$

离散数学

(2)只证$a\otimes(-b)= -(a\otimes b)$

$a\otimes(-b)= (a\otimes(-b))\oplus 0$

$= (a\otimes(-b))\oplus((a\otimes b)-(a\otimes b))$

$= (a\otimes(-b))\oplus((a\otimes b)\oplus(-(a\otimes b)))$

$= ((a\otimes(-b))\oplus(a\otimes b))\oplus(-(a\otimes b))$ (结合律)

$= (a\otimes((-b)\oplus b))\oplus(-(a\otimes b))$ (分配律)

$= (a\otimes 0)\oplus(-(a\otimes b))$ ($(-b)\oplus b= 0$)

$= 0\oplus(-(a\otimes b))$ (根据(1) $a\otimes 0 = 0$)

$= -(a\otimes b)$;

离散数学

(3)$(-a)\otimes(-b) = -(a\otimes(-b))$ (根据(2))

$= -(-(a\otimes b))$ (根据(2))

$= a\otimes b$ (反身律)；

(4)$(-1)\otimes a = -(1\otimes a)$ (根据(2))

$= -a$ ；

(5)$(-1)\otimes(-1) = 1\otimes 1$ (根据(3))

$= 1$ ；

(6)只证$a\otimes(b-c) = (a\otimes b)-(a\otimes c)$

$a\otimes(b-c) = a\otimes(b\oplus(-c))$

$= (a\otimes b)\oplus (a\otimes(-c))$ (分配律)

$= (a\otimes b)\oplus (-(a\otimes c))$ (根据(2))

$= (a\otimes b)-(a\otimes c)$ 。

离散数学

定义3.含零因子环 无零因子环

设$(R, \oplus, \otimes)$是环。若在环$(R, \oplus, \otimes)$中

(1)$(\exists a\in R)(\exists b\in R)(a\neq 0\wedge b\neq 0\wedge a\otimes b=0)$，则称环$(R, \oplus, \otimes)$是含零因子环；称a是环中的左零因子，称b是环中的右零因子；

(2)$(\forall a\in R)(\forall b\in R)(a\neq 0\wedge b\neq 0\Rightarrow a\otimes b\neq 0)$，即环中无零因子（no nil-factor），则称环$(R, \oplus, \otimes)$是无零因子环。

注：•所谓含零因子，就是环中的两个元素，它们本身不是关于⊗运算的零元，但它们的⊗运算结果却是零元；于是就称此环为含零因子环。

•当一个环是交换环时，左零因子也就是右零因子，反之亦然；在这种情况下，左零因子、右零因子统称为零因子。

•如果在环中，不存在满足上述条件的元素，就称此环为无零因子环。

离散数学

例9. 整数环(I,+, ×)是无零因子环

已知(I,+, ×)是环，由于任意两个不为零的整数相乘,其积不为零，故由定义3知(I,+, ×)是无零因子环。

例10.矩阵环($M_{n\times n}$,+, ×)是含零因子环

已知($M_{n\times n}$,+, ×)是环(n≥2)。不妨设n=2，于是有

因为存在着$\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\neq\begin{pmatrix}0&0\\0&0\end{pmatrix}$,但$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$

即两个不为零的矩阵相乘其积为零矩阵。

由定义3知是($M_{n\times n}$,+, ×)含零因子环。

离散数学

例11. 整数模环$(N_m,+_m,\times_m)$，

当m为素数时，是无零因子环；

当m不是素数时，是含零因子环。

(1)当m为素数时，对任意的 $[i]_m$，$[j]_m \in N_m$，$[i]_m \neq [0]_m$，(即$i \neq pm$),$[j]_m \neq [0]_m$ (即$j \neq qm$),从而有$i \times j \neq km$ (否则，$i \times j = km$，由m是素数，则必有$m \mid i$或$m \mid j$，于是有 $i = pm$或 $j = qm$，矛盾)，即有

$$[i]_m \times_m [j]_m = [(i \times j) \bmod m]_m \neq [0]_m$$

即两个不为零的元素经过$\times_m$运算后不为零。

由定义3知$(N_m,+_m,\times_m)$是无零因子环。

(2)当m不是素数时，必存在着$[i]_m$，$[j]_m \in N_m$，$[i]_m \neq [0]_m$，$[j]_m \neq [0]_m$，使得 $m = i \times j$，即有

$$[i]_m \times_m [j]_m = [(i \times j) \bmod m]_m = [0]_m$$

即$[i]_m$，$[j]_m$是N_m中的零因子。

由定义3知$(N_m,+_m,\times_m)$是含零因子环。

离散数学

例12. X的子集环$(2^X,\oplus,\cap)$是含零因子环

已知$(2^X,\oplus,\cap)$是环，其零元是空集∅。

设$|X|\geq 2$,任取a，b∈X，且a ≠ b，于是有$\{a\},\{b\}\in 2^X$且$\{a\},\{b\}\neq\varnothing$，使得$\{a\}\cap\{b\}=\varnothing$。

即两个不为零的元素相交后为零元。

由定义3知$(2^X,\oplus,\cap)$是含零因子环。

例13.多项式环$(P[x],+,\times)$是无零因子环

已知$(P[x],+,\times)$是环，由于两个非零多项式相乘其积仍为一非零多项式，由定义3知$(P[x],+,\times)$是无零因子环。

离散数学

定义4.整环(integral domain)

交换含幺的无零因子环称为整环。

注：•整环又称为整区。

定义4.除环(division ring)

每个非零元都有(乘法)逆元的含幺环称为除环。即，若含幺环$(R, \oplus, \otimes)$满足：

$$(\forall a \in R)(a \neq 0 \Rightarrow a^{-1} \in R)$$

则称其为除环。

离散数学

例16. 在前面的例子中

(1)整数环(I,+,×)是整环：因为整数环(I,+,×)是交换含幺环(例8(1))，又是无零因子环(例9)。

但整数环(I,+,×)不是除环：因为在整数环(I,+,×)中，除幺元1及其负元-1外，其它非零整数$a\in I(a\neq 0)$都没有(乘法)逆元($a^{-1}=1/a\notin I$)。

(2)矩阵环($M_{n\times n,}$,+,×)不是整环：因为矩阵环($M_{n\times n,}$,+,×)不是交换环,矩阵的乘法没有交换律(例8(2))，而且还是含零因子环(例10)。

矩阵环($M_{n\times n,}$,+,×)也不是除环：因为矩阵环($M_{n\times n,}$,+,×)中一些非零矩阵(行列式是零)关于矩阵乘法没有逆元(逆矩阵)。

离散数学

(3)整数模环$(N_m,+_m,\times_m)$当m是素数时是整环：因为整数模环$(N_m,+_m,\times_m)$是交换含幺环(例8(3))，并且当m为素数时，又是无零因子环(例11)；并且也是除环（见下面注）。

整数模环$(N_m,+_m,\times_m)$当m不是素数时不是整环：因为整数模环$(N_m,+_m,\times_m)$当m不是素数时是含零因子环(例11)；并且也不是除环（见下面注）。

(4)X的子集环$(2^X,\oplus,\cap)$不是整环：因为X的子集环$(2^X,\oplus,\cap)$是含零因子环(例12)；

并且也不是除环。

离散数学

(5)多项式环(P[x],+,×)是整环：因为多项式环(P[x],+,×)是交换含幺环(例8(5))，又是无零因子环(例13)。

但多项式环(P[x],+,×)不是除环：因为有非零多项式 $ax \in P[x]$ $(a \neq 0)$，关于多项式乘法没有逆元(否则，若 $ax \times q(x)=1$，则用比较系数法，可得 $q(x)=0$，于是又有 $ax \times q(x)=0$，矛盾)。

注：•在下面定理4中，将可证：在有限含幺环中
无零因子⇔(非零元)有逆元 ；

定理2. 在环$(R,\oplus,\otimes)$中，无零因子$\Leftrightarrow$消去律，即$\forall a,b,c\in R$且$a\neq 0$，都有

$a\otimes b= a\otimes c\Rightarrow b=c$ ；

$b\otimes a= c\otimes a\Rightarrow b=c$ 。

[证]. 先证$\Rightarrow$)： $\forall a,b,c\in R$且$a\neq 0$，

$a\otimes b= a\otimes c$

$\Rightarrow (a\otimes b)-(a\otimes c)=0$ (两边同时$\oplus$上$-(a\otimes c)$)

$\Rightarrow a\otimes(b-c)=0$ (分配律)

$\Rightarrow b-c=0$ ($a\neq 0$及无零因子)

$\Rightarrow b=c$

次证$\Leftarrow$)：用反证法。假设环中有零因子，因此，必有一对元素$a,b\in R$，$a\neq 0$且$b\neq 0$，使得$a\otimes b=0$。但是$a\otimes 0 =0$，于是我们有$a\otimes b= a\otimes 0$，由$a\neq 0$及消去律可得$b= 0$，这与已知$b\neq 0$ 矛盾。

这个矛盾说明假设错误，环中无零因子。

离散数学

定理3. 除环是含幺的无零因子环。

注：•因此，除环未必是整环，整环也未必是除环；
•除环要成为整环，差乘法交换律；整环要成为除环，差(非零元)有乘法逆元 ；

[证]. 除环是含幺环，因此只须证环无零因子 即可。假设环中有零因子$a,b\in R$，$a\neq 0$且$b\neq 0$，使得$a\otimes b=0$。 则有

$a\otimes b=0=0\otimes b$

$\Rightarrow a\otimes b\otimes b^{-1}=0\otimes b\otimes b^{-1}$（两边同时乘上$b^{-1}$，因$a\neq 0$ $b\neq 0$））

$\Rightarrow a=0$

与$a\neq 0$矛盾，所以环中无零因子。

离散数学

定理4.在有限含幺环中，无零因子⇔(非零元)有逆元。

[证]. 先证⇒):

因环无零因子，故⊗运算对R\{0}是封闭的, 因此(R\{0},⊗)是代数系统。于是。在代数系统(R\{0},⊗)中，因R有限, 故对任何$r \in R\{0}$ ，必有$i, j \in N$, $j>i \geq 1 (j-i \geq 1)$,使得

$$r^i = r^j \Rightarrow r^j = r^i$$

$$\Rightarrow r^{j-i} \otimes r^i = e \otimes r^i \quad \text{(指数律、环含幺)}$$

$$\Rightarrow r^{j-i} = e \quad \text{(消去律)}$$

$$\Rightarrow r^{-1} = r^{j-i-1}$$

即，非零元有逆元。

次证⇐)：同定理3 。

离散数学

注：•关于消去律、无零因子、非零元有逆元之间的关系，见下图：

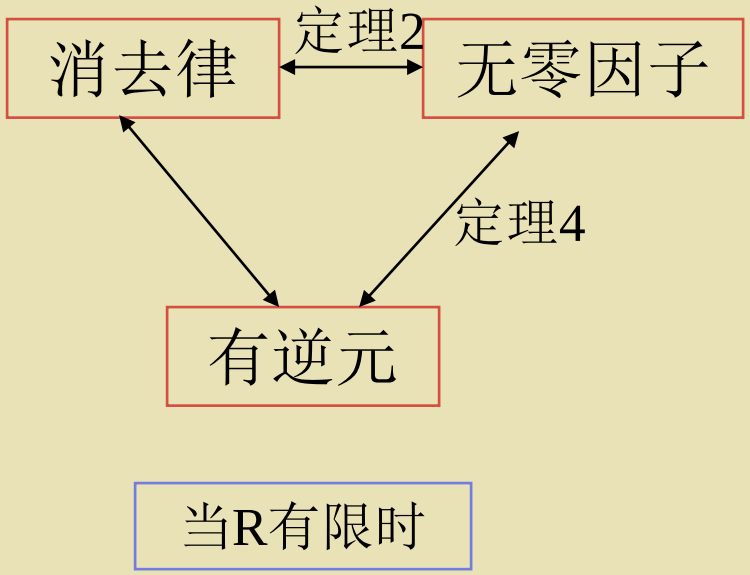

图1

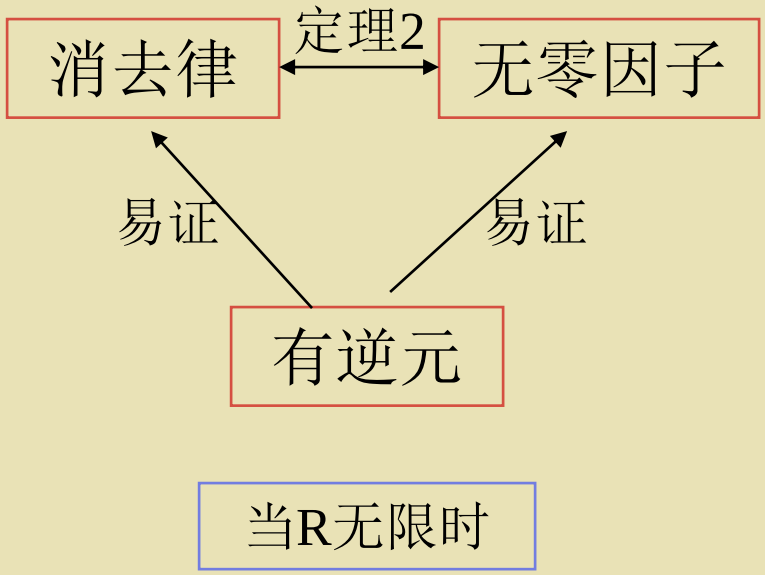

图2

离散数学

§6.域

- 域的基本概念
- 有限域

§6.域

定义1.域(field)

设$(F, \oplus, \otimes)$是代数系统，$\oplus$和$\otimes$是R上的两个二元运算，若

(1) $(F, \oplus)$是交换群；

(2) $(F\backslash\{0\}, \otimes)$是交换群；

(3) $\otimes$对$\oplus$满足分配律：对任何$a,b,c\in F$，都有

$a\otimes(b\oplus c)=(a\otimes b)\oplus(a\otimes c)$；

则称 $(F, \oplus, \otimes)$是域。

注：•在域$(F, \oplus, \otimes)$中，由于$(F\backslash\{0\}, \otimes)$是交换群，以及

$\forall a\in F, 0\otimes a=a\otimes 0=0$

因此，$\otimes$运算有交换律，所以$\otimes$对$\oplus$的分配律只写一条。

离散数学

例1.$(Q,+,\times)$是域。我们称为有理数域。
这里：Q是有理数集，$+,\times$分别是普通的有理数的加法运算和乘法运算，则$(Q,+,\times)$是域。

例2.$(R,+,\times)$是域。我们称为实数域。
这里：R是实数集，$+,\times$分别是普通的实数的加法运算和乘法运算，则$(R,+,\times)$是域。

例3.$(C,+,\times)$是域。我们称为复数域。
这里：C是复数集，$+,\times$分别是普通的复数的加法运算和乘法运算，则$(C,+,\times)$是域。

例4.$(X_1,+,\times)$是域。我们称为算术分类域。
这里：$X_1=\{a+b\sqrt{2} : a,b\in Q\}$，$+,\times$分别是普通数的加法运算和乘法运算。

包含性：$X_1\subseteq R$，$X_1\setminus\{0\}\subseteq R$；

非空性：$X_1\neq\varnothing$(因$0=0+0\sqrt{2}\in X_1$)

$X_1\setminus\{0\}\neq\varnothing$(因$1=1+0\sqrt{2}\in X_1\setminus\{0\}$)

离散数学

(1)$(X_1,+)$是交换群；只须证它是交换群$(R,+)$的子群即可

①封闭性：$\forall a+b\sqrt{2}$，$c+d\sqrt{2}\in X_1$

$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}\in X_1$；

②有逆元：$\forall a+b\sqrt{2}\in X_1$，有$-(a+b\sqrt{2})=(-a)+(-b)\sqrt{2}\in X_1$，使$(a+b\sqrt{2})+((-a)+(-b)\sqrt{2})=0$；

故根据§6定理14可知$(X_1,+)$是交换群$(R,+)$的子群。因此，$(X_1,+)$是交换群；

(2)$(X_1\backslash\{0\},\times)$是交换群；只须证它是交换群$(R\backslash\{0\},\times)$的子群即可

①封闭性：$\forall a+b\sqrt{2}$，$c+d\sqrt{2}\in X_1\backslash\{0\}$，于是a,b至少有一不为零，c,d至少有一不为零，从而

$(a+b\sqrt{2})\times(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in X_1\backslash\{0\}$

否则 $ac+2bd=0$, $ad+bc=0$,由a,b至少有一不为零可反解出c=0,d=0 (因为齐次线性方程组

离散数学

$$\begin{cases} ac+2bd=0 \\ bc+ad=0 \end{cases}$$ 的系数行列式 $$\begin{vmatrix} a & 2b \\ b & a \end{vmatrix} = a^2-2b^2 \neq 0$$

(否则a, b全为零与a, b至少有一不为零矛盾，或者全不为零且$\sqrt{2}$＝a/b是有理数，与其是无理数矛盾))，而这与c,d至少有一不为零矛盾。

②有逆元：$\forall a+b\sqrt{2}\in X_1\backslash\{0\}$，有

$$(a+b\sqrt{2})^{-1}=(a-b\sqrt{2})/(a^2-2b^2)\in X_1\backslash\{0\}$$

使 $(a+b\sqrt{2})\times(a-b\sqrt{2})/(a^2-2b^2)=1$；

故根据§6定理14可知$(X_1\backslash\{0\},\times)$是交换群$(R\backslash\{0\},\times)$的子群。因此，$(X_1\backslash\{0\},\times)$是交换群；

(3)×对+满足分配律：由代数(R,+,×)遗传；

所以按定义1知则$(X_1,+,\times)$是域。

注：•实际上易证$(X_k,+,\times)$都是域。这里$X_k=\{a+b\sqrt{p_k}: a,b\in Q\}$，其中$p_k$是第k个素数 。这正是我们为什么称此类域为算术分类域。

离散数学

定理1. 可交换的除环是域。

[证].除环是每个非零元都有(乘法)逆元的含幺环，它与域概念仅差(乘法)交换律。现在正好补齐，所以，可交换的除环是域。

定理2. 有限整环是域。

[证].整环是交换含幺的无零因子环，它与域概念仅差每个非零元都有(乘法)逆元。但在有限环的情况下，上节定理4已经证明：

无零因子⇔每个非零元都有(乘法)逆元

因此，有限整环是域。

例5. 在上节的例子中(参见上节例16)

(1)整数环(I,+,×)不是域：因为整数环(I,+,×)虽是整环，

离散数学

但不是有限环。实际上，它的非零整数$a\in I(a\neq 0)$，除幺元1及其负元-1外，都没有(乘法)逆元($a^{-1}=1/a\notin I$)；

(2)矩阵环$(M_{n\times n},+,\times)$不是域：因为它是含零因子环，它的一些非零矩阵(行列式是零)关于矩阵乘法没有逆元(逆矩阵)；

(3)整数模环$(N_m,+_m,\times_m)$当m是素数时是域：因为当m为素数时它是整环，并且又是有限的($|N_m|=m$)；

整数模环$(N_m,+_m,\times_m)$当m不是素数时不是域：因为当m不是素数时，它是含零因子环，因而并非每个非零元都有(乘法)逆元；

(4)X的子集环$(2^X,\oplus,\cap)$不是域：因为它是含零因子环，因而并非每个非零元都有(乘法)逆元；

(5)多项式环$(P[x],+,\times)$不是域：因为有非零多项式关于多项式乘法没有逆元；

离散数学

环	$(I,+,\times)$	$(M_{n\times n},+,\times)$	$(N_m,+_m,\times_m)$		$(2^X,\oplus,\cap)$	$(P[x],+,\times)$
运算	×	×	$\times_m$		∩	×
交换律	有	无	有		有	有
幺元	1	E	$[1]_m$		X	1
零因子	无	有	m是素数	m是合数	有	无
			无	有		
整环	是	不是	是	不是	不是	是
除环	不是	不是	是	不是	不是	不是
域	不是	不是	是	不是	不是	不是

表3

离散数学

第四章 代数系统

重点要求

- 掌握代数系统的概念,对几个定义:运算的封闭性、单位元、零元、逆元、等幂元及相关的结论有清晰的理解。给定集合和集合上的运算能够判断该集合对运算是否封闭;能够通过运算表确定单位元零元、逆元等(如果存在的话);对交换律、结合律、分配律、吸收律、消去律等的表示要十分清楚;给定集合和二元运算表能够判断运算是否满足结合律等等。
- 掌握代数系统的同态和同构的定义能判断两个给定代数系统间的某个映射是否为同态同构映射。
- 掌握半群及含幺半群概念。
- 掌握群的概念,并能灵活运用群的一些基本性质,理解群的同态和同构。给定一个代数系统及其运算,能够判断是否为半群、含幺半群、群等。
- 掌握群的阶和元素的阶及其性质，掌握循环群和生成元，置换群与Cayley定理。

离散数学

- **掌握子群的概念并清楚其判别方法**。掌握陪集与Lagrange定理及其推论。
- **掌握环、无零因子环、含零因子环、整环、除环的定义, 并熟悉环的基本性质。给定集合及两个二元运算能够判断其是否为环、整环、除环等**。
- **牢记消去律、无零因子、有逆元三者间的俩层关系及其运用**。
- **掌握域及有限域的定义**。

离散数学

- 第六章 代数系统
  到此已经结束！