第五章 环和域

信息与软件学院

电子科技大学

内容安排

- 5.1 环的定义
- 5.2 整环、除环和域
- 5.3 子环、理想和商环
- 5.4 素理想、极大理想和商域

5.1 环的定义

定义 5.1.1 设 R 是一个非空集合，R 上定义有两个代数运算：加法（记为“＋”）和乘法（记为“.”），假如

（1）$(R,+)$ 是一个交换群。

（2）R 关于乘法满足结合律。即对于任意 $a,b,c\in R$，有

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

（3）乘法对加法满足左、右分配律，即对于任意 $a,b,c\in R$，有

$$a\cdot(b+c)=a\cdot b+a\cdot c,$$

$$(b+c)\cdot a=b\cdot a+c\cdot a.$$

则称 R 为环。

环的定义（续）

如果，R 还满足

（4）乘法交换，即对于任意$a,b\in R$，有 $a\cdot b=b\cdot a$ 。

则称 R 为交换环。

如果 R 中存在元素1_R，使得

（5）对于任意 $a\in R$ ，有$1_R\cdot a=a\cdot 1_R=a$。

则称 R 为有单位元环。元素1_R（或简记为 1）称为 R 中的单位元。

R 的加法群中的单位元素记为 0，称为环 R 的零元素。R 中的元素 $a\in R$ 加法逆元称为负元，记为 $-a$ 。与第三章中的群的乘法一样，R 中两个元素的乘法 $a\cdot b$ 可简记为 ab 。

例 5.1.1 （1）全体整数关于数的普通加法和乘法构成一个环，称为整数环，记为$\mathbb{Z}$。

（2）全体有理数（实数、复数）关于数的普通加法和乘法构成一个环，称为有理数域，记为$\mathbb{Q}$（$\mathbb{R}$、$\mathbb{C}$）。

例 5.1.2 R＝{所有模m的剩余类}，规定运算为

$$[a]+[b]=[a+b],[a][b]=[ab]$$

可以证明 R 关于上述运算构成一个环，称为模m的剩余类环，记为$\mathbb{Z}/m\mathbb{Z}$，或$\mathbb{Z}_m$。

例 5.1.1 中的环都是有单位元的交换环，其单位元都为整数 1。

例 5.1.2 中的$\mathbb{Z}_m$也是有单位元的交换环，其单位元为[1]。

事实上有很多环并没有单位元，也可能不满足交换律。

例 5.1.3 设 n 是偶数，$n\mathbb{Z}$对于数的普通加法和乘法来说作成一个环．但$n\mathbb{Z}$没有单位元。

例 5.1.4 数域 F 上的 n 阶方阵的全体关于矩阵的加法和乘法构成一个环，称为 F 上的 n 阶方阵环，记为$M_n(F)$。这个环的单位元为 n 阶单位矩阵。因为矩阵的乘法不满足交换律，所以$M_n(F)$不是交换环。

例 5.1.5 $R=\{0,a,b,c\}$。加法和乘法由以下两个表给定：

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$\times$	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	a	b	c
c	0	a	b	c

则 R 对于上述两种运算构成一个环.

证明：首先证明 R 对于加法构成加法交换群。根据其运算表可以看出：

（1）加法封闭。

（2)满足结合律。因为 $a+(b+c)=a+a=0,(a+b)+c=c+c=0$，所以 $a+(b+c)=(a+b)+c$。其余可一一验证。

（3）有零元为 0，0 加上任何 R 中的元素都等于该元素。

（4）有负元。任何 R 中的元素的负元为其本身。

（5）满足交换律。R 的加法运算表是对称的，所以加法满足交换律。

其次，要证明乘法封闭且满足结合律。根据乘法运算表，乘法封闭显然。又 $a(bc)=ac=0,(ab)c=0c=0$，所以 $a(bc)=(ab)c$。其余的结合律可一一验证。

最后，可验证乘法对加法满足分配律，因为，$c(a+b)=cc=c,ca+cb=a+b=c$，所以 $c(a+b)=ca+cb$。其余情形可一一验证。

综上所述，R 是环。

定理 5.1.1 设 R 是一个环， $a,b\in R$ ， m,n 是正整数， ma 表示 m 个 a 相加， a^m 表示 m 个 a 相乘，则

（1） $a\cdot 0=0\cdot a=0$;

（2） $a(-b)=(-a)b=-(ab)$;

（3） $n(a+b)=na+nb$;

（4） $m(ab)=(ma)b=a(mb)$;

（5） $a^m a^n=a^{m+n}$;

（6） $(a^m)^n=a^{mn}$ 。

定理 5.1.1 证明

证明：（1）由分配律

$$a\cdot 0=a(0+0)=a\cdot 0+a\cdot 0$$

两边同时加上$-(a\cdot 0)$，则可得$a\cdot 0=0$。同理可证$0\cdot a=0$。

（2）由$a(-b)+ab=a(-b+b)=0$，可得

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

同理可证$(-a)b=-(ab)$。

（3）由加法交换律

$$n(a+b)=\overbrace{a+b+\cdots+a+b}^{n}=\overbrace{a+\cdots+a}^{n}+\overbrace{b+\cdots+b}^{n}=na+nb$$

定理 5.1.1 证明（续）

（4）由分配律

$$m(ab) = \overbrace{ab + \cdots + ab}^{m} = (\overbrace{a + \cdots + a}^{m})b = (ma)b$$

同理可证 $m(ab) = a(mb)$ 。

（5）（6）显然成立。

定义 5.1.2 零因子

在初等数学当中，$ab=0$ 可以得出 $a=0$ 或 $b=0$。这一性质在环中不一定成立。例如，在 $\mathbb{Z}_{12}$ 中，$[3]\neq[0]$，$[4]\neq[0]$，而 $[3][4]=[12]=[0]$。

定义 5.1.2 设 $(R,+,\cdot)$ 是一个环，如果存在 $a,b\in R$，满足 $a\neq0,b\neq0$，但 $ab=0$，则称环 R 为有零因子环，称 a 为 R 的左零因子，称 b 为 R 的右零因子，否则称 R 为无零因子环。

例 5.1.6 $\mathbb{Z}$、$\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$ 均是无零因子环，而对于在一个合数 n，$\mathbb{Z}_n$ 为有零因子环。

例 5.1.7 对于环 $M_n(F)$，当 $n\geq2$ 时，这个环是有零因子环。

例 5.1.8 设 p 是一个素数，则 $\mathbb{Z}_p$ 是无零因子环。

例 5.1.8 证明

证明：根据推论 2.2.1，$\mathbb{Z}_p$中任何一个非零元均存在逆元。设$[a],[b]\in\mathbb{Z}_p$。若$[a][b]=[0]$，即$ab\equiv 0(\bmod p)$，则有当$a\not\equiv 0(\bmod p)$，

$$ab\equiv 0(\bmod p)\Rightarrow b\equiv a^{-1}\cdot 0(\bmod p)\Rightarrow b\equiv 0(\bmod p)$$

当$b\not\equiv 0(\bmod p)$，有$a\equiv 0(\bmod p)$。也就是说，由$[a][b]=[0]$，可得出$[a]=[0]$或$[b]=[0]$。因此，$\mathbb{Z}_p$是无零因子环。

定理 5.1.2 无零因子环的消去律

定理 5.1.2 设 $(R,+,\cdot)$ 是一个无零因子环， $a,b,c\in R$， $a\neq 0$， 则有

$$ab=ac\Rightarrow b=c$$
$$ba=ca\Rightarrow b=c$$

反之，若一个环里消去律成立，则这个环是无零因子环。

证明：因为 R 是无零因子环， $a\neq 0$， 所以

$$ab=ac\Rightarrow a(b-c)=0\Rightarrow b-c=0\Rightarrow b=c\text{；}$$

$$ba=ca\Rightarrow (b-c)a=0\Rightarrow b-c=0\Rightarrow b=c$$

故 R 中的乘法满足左、右消去律。

反过来，假定 R 中的乘法满足左消去律，则

$$ab=0\Rightarrow ab=a0\Rightarrow b=0$$

即 R 无零因子。

定义 5.1.3 可逆元

定义 5.1.3 设$(R,+,\cdot)$是一个有单位元环，$a\in R$。若存在元素$b\in R$，使得$ab=ba=1$，则称a是一个可逆元。

环中并不一定所有的非零元都有逆元，如在整数环$\mathbb{Z}$中，仅有± 1两个元素存在逆元。

在交换环中，左零因子、右零因子、零因子的概念是统一的。在非交换环中，左零因子不一定是右零因子，如特殊矩阵环

$$R=\left\{\begin{bmatrix}0 & a\\ 0 & b\end{bmatrix}\middle| a,b\in Z_p\right\}$$

乘法可逆元一定不是左、右零因子。

定理 5.1.3 无零因子环的特征

定理5.1.3 设 R 是一个无零因子环，则 R 中非零元的加法阶相等，这个加法阶或者是∞，或者是个素数 p。

证明：当环 R 中每个非零元的加法阶都是无穷大时，定理成立。

设 $a,b\in R$ 是非零元， a 的加法阶为 n， b 的加法阶是 m。则由

$$(na)b=a(nb)=0$$

可得 $nb=0$，所以 $n\geq m$。同理可证 $m\geq n$。因此， $m=n$。即所有非零元的加法阶相等。

定理 5.1.3 证明（续）

设 R 中所有非零元的加法阶为 n。若 n 不是素数，不妨设 $n = n_1 n_2$，$n_1 < n, n_2 < n$。

对于 $a \in R, a \neq 0$，有

$$(n_1 a)(n_2 a) = n_1 n_2 a^2 = 0$$

又 R 是无零因子环，所以有

$$n_1 a = 0 \text{或} n_2 a = 0$$

这与 n 是 a 的加法阶矛盾。因此，n 是素数。

定义 5.1.4 特征

定义 5.1.4 设 R 是一个无零因子环，称 R 中非零元的加法阶为环 R 的特征，记为 $\mathrm{Char}R$。当 R 中非零元的加法阶为无穷大时，称 R 的特征为零，记 $\mathrm{Char}R=0$；当 R 中非零元的加法阶为某个素数 p 时，称 R 的特征为 p，记 $\mathrm{Char}R=p$。

例 5.1.9 设 R 是特征为 p 的交换环，$a,b\in R$，有 $(a\pm b)^p=a^p\pm b^p$。

证明：$$(a+b)^p=a^p+\binom{p}{1}a^{p-1}b+\cdots+\binom{p}{p-1}ab^{p-1}+b^p。$$

因为，对于 $1\le k\le p-1$，$\binom{p}{k}=\dfrac{p!}{k!(p-k)!}=\dfrac{p\cdot(p-1)!}{k!(p-k)!}$。

例 5.1.9 证明（续）

由上式可知 $k!(p-k)! \mid p\cdot(p-1)!$，而 $k!(p-k)!$ 与素数 p 互素，所以

$k!(p-k)! \mid (p-1)!$，因此$\begin{pmatrix} p \\ k \end{pmatrix}$是 p 的倍数，进而有$\begin{pmatrix} p \\ k \end{pmatrix} a^{p-k} b^{k} = 0$，由此可得

$$(a+b)^p = a^p + b^p$$

$(a-b)^p = a^p - b^p$ 的证明留给读者。

5.2 整环、除环和域

定义 5.2.1 一个有单位元的无零因子的交换环叫做一个整环。

例如，$\mathbb{Z}$、$\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$都是整环，而$2\mathbb{Z}$、$\mathbb{Z}_n$ (n 是合数)、$M_n(F)$不是整环。

例 5.2.1 $\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$中任意一个非零数a都有一个逆元$\frac{1}{a}$，且

$a\left(\frac{1}{a}\right)=\left(\frac{1}{a}\right)a=1$.

5.2 整环、除环和域（续）

定义 5.2.2 一个环 R 称为**除环**，假如

（1） R 中至少包含一个不等于零的元 (即 R 中至少有两个元素);

（2） R 有单位元;

（3） R 的每一个不等于零的元有一个逆元。

注意到，除环的概念中，并没有要求它满足乘法交换律。

定义 5.2.3 交换除环称为**域**。

例如， $\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$都是域。

5.2 整环、除环和域（续）

命题 5.2.1 （1）除环是无零因子环。

（2）设 R 是一个非零环，记 $R^*=\{a\in R\,|\,a\neq 0\}=R\backslash\{0\}$，则 R 是除环当且仅当 R^* 对于 R 的乘法构成一个群，称这个群为除环 R 的乘法群。

（3）在除环 R 中，$\forall a(\neq 0)\in R, b\in R$，方程 $ax=b$ 和 $ya=b$ 都有惟一解。

证明：（1）设 R 是除环，$a,b\in R$

$$a\neq 0, ab=0 \Rightarrow a^{-1}ab=b=0$$。

（2）R^* 对于 R 的乘法构成一个群，显然 R 可满足除环定义中的三个条件。

命题 5.2.1 证明（续）

设 R 是除环。由于 R 是无零因子环，所以 R^* 对于乘法封闭；由环的定义，乘法满足结合律；由除环的定义，R^* 中有单位元，即 R 的单位元，而且 R^* 中每一个元素均有逆元。因此，R^* 是群。

（3）在除环 R 中，$\forall a(\neq 0)\in R, b\in R$，方程 $ax=b$ 和 $ya=b$ 的惟一解分别为 $a^{-1}b$ 和 ba^{-1}。注意，$a^{-1}b$ 与 ba^{-1} 未必相等。若 R 是域，则 $a^{-1}b=ba^{-1}$，统一记为 $\frac{b}{a}$，称为 b 除以 a 的商，易知商具有与普通数相似的一些性质。

5.2 整环、除环和域（续）

例 5.2.2 设$H=\{a_0+a_1i+a_2j+a_3k|a_0,a_1,a_2,a_3\in\mathbb{R}\}$是实数域$\mathbb{R}$上的四维向量空间，$1,i,j,k$ 为其一组基，规定基元素之间的乘法为：

（1）$i^2=j^2=k^2=-1$；　　　　（2）$ij=k, jk=i, ki=j$。

将其线性扩张为 H 中的元素之间的乘法。则 H 关于向量的加法和上面定义的乘法构成一个除环，称之为（Hamilton)四元数除环。

定理 5.2.1 有限除环的判定

定理5.2.1 **一个至少含有两个元素的无零因子的有限环是除环。**

证明： 设$R=\{0,a_1,\cdots,a_n\}$是一个无零因子环，n 是正整数，$a_i\neq 0, 1\leq i\leq n$。要证明R^*对于 R 的乘法构成一个群。

因为 R 无零因子，所以R^*对于 R 中的乘法封闭。任选$a(\neq 0)\in R$，考察$aa_1,aa_2,\cdots,aa_n$。若$aa_i=aa_j$，则$a(a_i-a_j)=0$，又$a\neq 0$，所以$a_i=a_j$。因此，$\{aa_1,aa_2,\cdots,aa_n\}=\{a_1,a_2,\cdots,a_n\}$。同理可得$\{a_1a,a_2a,\cdots,a_na\}=\{a_1,a_2,\cdots,a_n\}$。故对于任意$a,b\in R^*$，方程

$$ax=b \text{ 和 } xa=b$$

在R^*中有解。根据定理 4.2.1，R^*是群。 □

5.2 整环、除环和域（续）

推论5.2.1 有限整环是域。

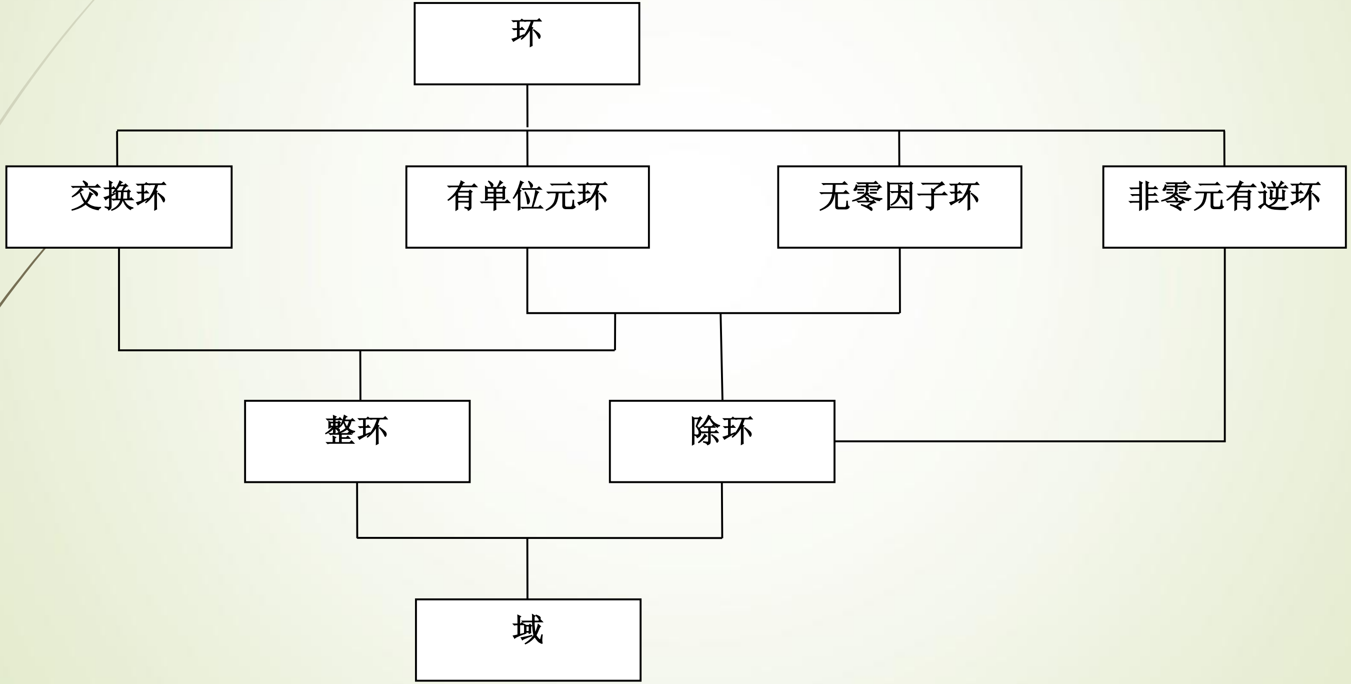
证明： 根据定理5.2.1，有限整环是除环，又整环满足乘法交换律，根据域的定义，有限整环是域。 □

例 5.2.3 模p的剩余类环$\mathbb{Z}_p$是域当且仅当p是素数。

证明： ($\Rightarrow$)：易知 $p \neq 0,1$．若p为合数，则 $p = ab, a, b \neq \pm 1$．于是$a \not\equiv 0 (mod\ p)$，$b \not\equiv 0 (mod\ p)$，但$ab \equiv 0 (mod\ p)$，即$\mathbb{Z}_p$中有零因子，此与$\mathbb{Z}_p$是域矛盾，故p是素数。

($\Leftarrow$)：设p是素数．若$ab \equiv 0 (mod\ p)$，则 $p \mid ab$，从而 $p \mid a$ 或 $p \mid b$，即有$a \equiv 0 (mod\ p)$或$b \equiv 0 (mod\ p)$，故$\mathbb{Z}_p$为一个无零因子环，于是$\mathbb{Z}_p$是一个有限整环，根据推论 5.2.1 ，$\mathbb{Z}_p$是域。

5.2 整环、除环和域（续）



5.3 子环、理想和商环

定义 5.3.1 设 S 是环 R 的一个非空子集合。如果 S 对 R 的两个运算也构成一个环，则称 S 为 R 的一个子环，称 R 为 S 的扩环。

例 5.3.1 例 5.1.1 当中，$\mathbb{Z}$是$\mathbb{Q}$的子环，$\mathbb{Q}$是$\mathbb{R}$的子环，$\mathbb{R}$是$\mathbb{C}$的子环。$n\mathbb{Z}$是$\mathbb{Z}$的子环。

类似的，可以定义子整环，子除环，子域的概念。

任意环 R 都至少有两个子环：0 和 R，称之为 R 的平凡子环。设 $S \le R$ 且 $S \ne R$，则称 S 是 R 的一个真子环。易知，子环的交仍为子环。

设 S 是环 R 的一个非空子集，则 S 对于 R 的运算一定满足结合律．于是有定理 5.3.1

5.3 子环、理想和商环（续）

定理 5.3.1（1）设 R 是环，S 是 R 的一个非空子集一个子集，S 是 R 的子环当且仅当

$$a-b\in S, ab\in S, \forall a,b\in S。$$

（2）设 R 是除环，S 是 R 的一个非空子集一个子集，S 是 R 的子除环当且仅当

$$a-b\in S, ab^{-1}\in S, \forall a,b(\neq 0)\in S。$$

证明： 根据子群的充要条件很容易验证定理中的两个充要条件。

例 5.3.2 假设 R 是环，记集合 $C(R)=\{a\in R\mid ab=ba,\forall b\in R\}$（同每一个元交换的元之集），称为环 R 的中心，则 $C(R)$ 是 R 的子环。

证明： 根据定理 5.3.1 可以直接验证。

5.3 子环、理想和商环（续）

例 5.3.3 求模 12 的剩余类环$\mathbb{Z}_{12}$的所有子环。

解： 由于$\mathbb{Z}_{12}$的加法群是一个循环群，故剩余类环$\mathbb{Z}_{12}$的子环关于加法是（$\mathbb{Z}_{12}$，＋）的子循环群，共有下面 6 个：

$$S_1 = \langle [1] \rangle = R;$$

$$S_2 = \langle [2] \rangle = \{[0], [2], [4], [6], [8], [10]\};$$

$$S_3 = \langle [3] \rangle = \{[0], [3], [6], [9]\};$$

$$S_4 = \langle [4] \rangle = \{[0], [4], [8]\};$$

$$S_5 = \langle [6] \rangle = \{[0], [6]\};$$

$$S_6 = \langle [0] \rangle = \{[0]\}。$$

经检验，它们都是$\mathbb{Z}_{12}$的子环，从而$\mathbb{Z}_{12}$有上面的 6 个子环。

5.3 子环、理想和商环（续）

设 S 是 R 的子环， S 与 R 的可以有不同的性质。

1. 对于交换律

（1）若 R 是交换环，则 S 也是交换环；

（2）若 S 是交换环，则 R 未必是交换环。

2. 对于零因子

（1）若 R 无零因子，则 S 也是无零因子；

（2）若 S 无零因子，则 R 未必无零因子。

3. 对于单位元

（1）若 R 有单位元，则 S 未必有单位元；

（2）若 S 有单位元，则 R 未必有单位元。

5.3 子环、理想和商环（续）

定义 5.3.2 设$(R,+,\cdot)$和$(R',\oplus,\circ)$是环，$f:R\to R'$为映射。若f保持运算，即对任意$a,b\in R$有

$$f(a+b)=f(a)\oplus f(b);$$
$$f(a\cdot b)=f(a)\circ f(b)$$

则称f是环 R 到 R′ 的一个**同态**。类似群中的定义，可定义环的单同态、满同态、同构的概念。

和群的情形类似，我们有定理 5.3.2

定理 5.3.2 环同态性质

定理 5.3.2 设 $f:R\to R'$为环同态.

（1） 若 0 是 R 中的零元，则 f(0)是 R′ 中的零元；

（2） $f(-a)=-f(a),\forall a\in R$；

（3） 若 R 有单位元且 1 是 R 的单位元，则 $f(1)$ 是 R' 的单位元；

（4） 若 S 是 R 的子环，则 $f(S)$ 是 R' 的子环；

（5） 若 S'是 R' 的子环，则 $f^{-1}(S')=\{a\in R\mid f(a)\in S'\}$ 是 R 的子环；

证明：（1）对于任意元素 $a\in R$，有

$$f(a)=f(a+0)=f(a)+f(0)=f(0)+f(a)$$

所以 $f(0)$是 R′ 中的零元。

定理 5.3.2 证明（续）

（2）对于任意元素 $a \in R$，有

$$f(0) = f(a-a) = f(a+(-a)) = f(a) + f(-a)$$

所以 $f(-a) = -f(a), \forall a \in R$。

（3）对于任意元素 $a \in R$，有

$$f(a) = f(a \cdot 1) = f(1 \cdot a) = f(1)f(a) = f(a)f(1)$$

所以 $f(1)$ 是 R' 的单位元。

（4）和（5）可根据同态的定义和定理 5.3.1 验证。

5.3 子环、理想和商环（续）

例5.3.4 设$f:\mathbb{Z}\to\mathbb{Z}_n$为$f(x)=x(mod\ n)$，$x\in\mathbb{Z}_n$。证明：$f:\mathbb{Z}\to\mathbb{Z}_n$为满同态。

证明：不难证明：f是$\mathbb{Z}$到$\mathbb{Z}_n$的满射。对于任意$x,y\in\mathbb{Z}$，有

$$f(x+y)=(x+y)(mod\ n)=x(mod\ n)+y(mod\ n)=f(x)+f(y)$$
$$f(xy)=(xy)(mod\ n)=x(mod\ n)y(mod\ n)=f(x)f(y)$$

所以$f:\mathbb{Z}\to\mathbb{Z}_n$为满同态。

例 5.3.5 设$R=\mathbb{Z}\times\mathbb{Z}=\{(a,b)|a,b\in\mathbb{Z}\}$，定义 R 的代数运算如下：

$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)\text{，}(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)$$

则 R 显然作成一个环，称之为$\mathbb{Z}$与$\mathbb{Z}$的直积，记为$\mathbb{Z}^{(2)}$. 易知映射

$$\pi:\mathbb{Z}\times\mathbb{Z};(a,b)\mapsto a,\forall a,b\in\mathbb{Z}$$

为满同态，但$\mathbb{Z}^{(2)}$中有零因子，而$\mathbb{Z}$无零因子。

5.3 子环、理想和商环（续）

设 $f: R \to R'$ 为环同构，记为 $R \cong R'$，则环 R 与 R′ 的代数性质完全一致。

定理 5.3.3 假定 $R \cong R'$，则 R 是整环（除环、域）当且仅当 R′ 是整环（除环、域）。

定理证明留给读者。

设 R 是一个环，A 关于 R 中的加法构成 R 的一个子加群，则有商加群

$$R/A = \{x + A \mid x \in R\}$$

其加法为 $(x+A)+(y+A)=(x+y)+A$。为了让 R/A 成为一个环，引入乘法：

$$(x+A)(y+A) = xy + A, \forall x, y \in R.$$

乘法是否有意义？

5.3 子环、理想和商环（续）

定义 5.3.3 设 R 是一个环，I 是 R 的一个非空子集，若满足

（1）$a-b\in I,\forall a,b\in I$ ；

（2）$ar\in I$，且 $ra\in I$，$\forall a\in I$，$\forall r\in R$；

则称 I 为环 R 的一个理想，记为 $I\lhd R$.

理想一定是子环，反之未必。对于任意环R，{0}和R都是理想，分别称之为零理想和单位理想。

例 5.3.6 整数 n 的所有倍数之集$(n)=\{nk|k\in\mathbb{Z}\}$构成整数环$\mathbb{Z}$的一个理想。

交换环的子环都是理想吗？

5.3 子环、理想和商环（续）

定义 5.3.4 设 R 是一个环，T 是 R 的一个非空子集，则称 R 中所以包含 T 的理想的交为由 T 生成的理想，记为$\langle T\rangle$，即$\langle T\rangle=\bigcap\limits_{T\subseteq I\lhd R} I$. 特别地，若$T=\{a\}$，则简记$\langle T\rangle$为$\langle a\rangle$，称之为由 a 生成的主理想。

显然，$\langle T\rangle$是 R 中包含 T 的最小的理想。

定理 5.3.4 设 R 是环，$\forall a\in R$。则

$$<a>=\{(x_1ay_1+\cdots+x_may_m)+sa+at+na|\forall x_i,y_i,s,t\in R,\forall m,n\in\mathbb{Z}\}。$$

证明： 利用理想的定义可以直接验证。

推论 5.3.1 主理想的元素表示

推论 5.3.1 设 R 是环， $\forall a \in R$. 则

（1） 当 R 是交换环时, $\langle a\rangle = \{sa + na | \forall s \in R, \forall n \in \mathbb{Z}\}$;

（2） 当 R 有单位元时， $\langle a\rangle = \{x_1 a y_1 + \cdots x_m a y_m | \forall x_i, y_i \in R\}$;

（3） 当 R 是有单位元的交换环时， $\langle a\rangle = Ra = \{ra | \forall r \in R\} = aR$ 。

证明：（1）当 R 是交换环时， $xay = xya = axy$ ， $sa = as$ ，所以定理 5.3.4 中

$$x_1 a y_1 + \cdots x_m a y_m + sa + at = (x_1 y_1 + \cdots x_m y_m + s + t)a = ca$$

其中 $c = x_1 y_1 + \cdots x_m y_m + s + t \in R$ 。因此 $\langle a\rangle$ 中的元素都可以表示成为 $sa + na$ （$s \in R, n \in \mathbb{Z}$）的形式。

推论 5.3.1 证明（续）

（2）当 R 有单位元时，$sa=s\cdot a\cdot 1, at=1\cdot a\cdot t$，都是形如 $x_i a y_i, x_i, y_i \in R$，所以 $\langle a\rangle$ 中的元素都可以表示成为 $x_1 a y_1+\cdots x_m a y_m, x_i, y_i \in R$ 的形式。

（3）当 R 是有单位元的交换环时，首先根据（1），理想中的元素可以表示成为 $sa+na$（$s\in R, n\in\mathbb{Z}$）的形式。又 $na=(n1)\cdot a$，所以 $\langle a\rangle$ 中的元素都可以表示成为 sa（$s\in R$）的形式。 $\square$

5.3 子环、理想和商环（续）

例 5.3.7 证明：（1）$\mathbb{Z}$的理想一定是主理想。

（2）$\langle n\rangle$是$\langle m\rangle$的子理想当且仅当$m|n$。

证明：（1）设I是$\mathbb{Z}$的理想。不妨设t是I中最小的正整数。这是一定存在的，因为I是理想，所以对于任意$l\in I$有$-l\in I$，而正整数集合的任意子集必存在最小正整数。任取$l>0\in I$，根据带余除法，有$l=qt+r, 0\le r<t$，所以$r=l-qt\in R$。由于t是I中最小的正整数，所以$r=0$，即有$t|l$。由此可得$I=\langle t\rangle$。

（2）$\mathbb{Z}$是有单位元的交换环，所以$\langle m\rangle=\{mk|k\in\mathbb{Z}\}$。当$\langle n\rangle$是$\langle m\rangle$的子理想，有$n\in\langle m\rangle$，所以$m|n$。反之，当$m|n$，设$n=lm$，对于任意$tn\in\langle n\rangle$，有$tn=tlm\in\langle m\rangle$。因此，$\langle n\rangle$是$\langle m\rangle$的子理想。

5.3 子环、理想和商环（续）

设 R 是环，I 是 R 的理想，在商群 $R/I=\{x+I \mid x\in R\}$ 中定义乘法为：

$$(x+I)(y+I)=xy+I, \forall x,y\in R。$$

由于 I 是一个理想，所以上述定义的乘法有意义。

定理 5.3.5 设 R 是环，I 是 R 的理想，则 R/I 构成一个环，称为 R 关于理想 I 的商环（或称剩余类环）．其中元素 $x+I$ 通常也记为$[x]$，称之为 x 所在的等价类或 x 模 I 的剩余类。

例 5.3.8 任意$n\in\mathbb{Z}$，$\langle n\rangle=\{nk|k\in\mathbb{Z}\}$是整数环$\mathbb{Z}$的一个理想，则有商环

$$\mathbb{Z}/\langle n\rangle=\{k+\langle n\rangle|k\in\mathbb{Z}\}=\{[0],[1],\ldots,[n-1]\},$$

其中$[i]=i+kn|k\in\mathbb{Z}\},i=0,\ldots,n-1$。称之为模 n 的剩余类环，一般记为$\mathbb{Z}/n\mathbb{Z}$或$\mathbb{Z}_n$。

5.3 子环、理想和商环（续）

定理 5.3.6 设 R 是环， $\forall I \lhd R$，则存在自然的满同态

$$\pi : R \to R/I ; a \mapsto [a], \forall a \in R。$$

证明： 利用定义可以直接验证。

定理 5.3.7（同态基本定理）设 φ 是环 R 到环 R' 的一个同态映射，则

（1） $Ker\varphi = \{x \in R \mid \varphi(x) = 0\}$ 是 R 的理想，称 $Ker\varphi$ 为同态 φ 的核；

（2） $R / Ker\varphi \cong \varphi(R)$。

证明： 类似于定理 4.4.4 的证明。

5.4 素理想、极大理想和商域

定义 5.4.1 设I是有单位元的交换环R的一个理想，$I \neq R$。$a,b \in R$，如果$ab \in I$，总有$a \in I$或$b \in I$，则称I是R的一个素理想。

定义 5.4.2 假设R是环，M是R的子环，且$M \neq R$。如果在R的所有理想中，除了M本身和R外，没有包含M的理想，则称M为R的极大理想。

例 5.4.1 整数环$\mathbb{Z}$内由素数p生成的理想$\langle p \rangle$是一个素理想，同时也是一个极大理想。

证明：$\mathbb{Z}$内由素数 p 生成的理想$\langle p \rangle = \{pk | k \in \mathbb{Z}\}$。

若$ab \in \langle p \rangle$，则$p | ab$。由p是素数，可知$p | a$或$p | b$。因此有$a \in \langle p \rangle$或$b \in \langle p \rangle$。

故$\langle p \rangle$是一个素理想。

5.4 素理想、极大理想和商域（续）

由于$1\notin\langle p\rangle$，则$\langle p\rangle\neq\mathbb{Z}$。设$I$是包含$\langle p\rangle$的一个理想．若$\langle p\rangle\neq I$，则存在$q\in N\backslash\langle p\rangle$。由$p$是素数可知，$q$与$p$互素，于是存在整数 s 和 t，使得$sp+tq=1$．又$p\in N$，而且$I$是理想，所以$1\in I$，进而有$N=\mathbb{Z}$。故$\langle p\rangle$是一个极大理想。

定理 5.4.1 设有单位元的交换环R，则

（1）M 是R的极大理想当且仅当R/M 是域。

（2）P是R的素理想当且仅当R/P是整环。

定理 5.4.1 证明

证明：（1）设 M 是 R 的极大理想。对于 $a\notin M, a\in R$，集合 $J=\{a+rm \mid m\in M, r\in R\}$ 是 R 的理想，而且 $J\supseteq M$，$J\neq M$。因此，$J=R$。特别地，存在 $m\in M, r\in R$，使得 $ar+m=1$。如果 $a+M\neq 0+M$ 是 R/M 中的非零元，则 $a+M$ 在 R/M 中存在乘法逆元。这是因为

$$(a+M)(r+M)=ar+M=1+M\text{。}$$

因此 R/M 是域。

反之，设 R/M 是域。设 J 是 R 的理想，$J\supseteq M$，$J\neq M$。则对于 $a\notin M, a\in J$，剩余类 $a+M$ 在 R/M 中有逆元，所以存在 $r\in R$，满足 $(a+M)(r+M)=1+M$。这意味着，存在 $m\in M$，使得 $ar+m=1$。又因为 J 是 R 的理想，所以 $1\in J$。因此有 $J=R$。由此可得，M 是 R 的极大理想。

定理 5.4.1 证明（续）

（2）设 P 是 R 的素理想，则 R/P 是有单位远的交换环，其单位元为 $1+P \neq 0+P$。令 $(a+P)(b+P)=0+P$，有 $ab \in P$。又 P 是 R 的素理想，所以有 $a \in P$ 或 $b \in P$，即有 $a+P=0+P$ 或 $b+P=0+P$。因此，R/P 无零因子。由此可得，R/P 是整环。 □

定理 5.4.2 分式域

定理 5.4.2 对于每一个整环 R，一定存在一个域 Q，使得 R 是 Q 的子环。

证明： 设 R 是整环。当 R 只包含零元时，定理显然成立。考虑至少含有两个元素的整环。记集合 $Q=\left\{\frac{b}{a} \mid a,b\in R, b\neq 0\right\}$。约定

（1）$a=\frac{a}{1}$，$\forall a\in R$，1 是 R 的单位元。

（2）$\frac{0}{a}=0$，$\forall a\in R$，0 是 R 的零元。

（3）$\frac{bc}{ac}=\frac{b}{a}$，$\forall a,b,c\in R, a\neq 0, c\neq 0$。

定义如下运算：

定理 5.4.2 证明（续）

（1）加法：$\frac{b}{a}+\frac{d}{c}=\frac{bc+ad}{ac}$， $a,b,c,d\in R,a\neq 0,c\neq 0$；

（2）乘法：$\frac{b}{a}\cdot\frac{d}{c}=\frac{bd}{ac}$， $a,b,c,d\in R,a\neq 0,c\neq 0$。

首先证明集合Q关于上面定义的加法构成加法交换群。由于 R 是有单位元的交换群，所以有：

（1）封闭性：显然。

（2）结合律：

$$\frac{b}{a}+\left(\frac{d}{c}+\frac{f}{e}\right)=\frac{b}{a}+\frac{ed+cf}{ce}=\frac{bce+aed+acf}{ace};$$

$$\left(\frac{b}{a}+\frac{d}{c}\right)+\frac{f}{e}=\frac{bc+ad}{ac}+\frac{f}{e}=\frac{bce+aed+acf}{ace}。$$

定理 5.4.2 证明（续）

（3）零元：为 R 中的零元。

$$\frac{b}{a}+0=\frac{b}{a}+\frac{0}{a}=\frac{b}{a};$$

$$0+\frac{b}{a}=\frac{0}{a}+\frac{b}{a}=\frac{b}{a}。$$

（4）负元：$\frac{b}{a}$的负元为$\frac{-b}{a}$

$$\frac{b}{a}+\frac{-b}{a}=\frac{0}{a}=0。$$

（5）交换律：

$$\frac{b}{a}+\frac{d}{c}=\frac{d}{c}+\frac{b}{a}。$$

因此，Q是加法交换群。

定理 5.4.2 证明（续）

对于乘法，显然满足封闭性、结合律及交换律。1 是Q的乘法单位元。对于Q中的非零元$\frac{b}{a}$，有

$$\frac{b}{a}\cdot\frac{a}{b}=1,$$

即$\frac{a}{b}$是$\frac{b}{a}$的乘法逆元。因此，Q对于乘法是乘法交换群。

乘法对加法的分配率也显然成立。

综上所述，Q是域，称为 R 的分式域。

容易验证R中的加法与乘法与Q中定义的加法和乘法一致。因此，R是Q的子环。

谢谢！