加群、环的定义

交换律、单位元、零因子、整环

除环、域

无零因子环的特征

子环、环的同态

多项式环

理想

剩余类环、同态与理想

执一而万物治

——庄子

第三章　环与域

January 10, 2007

wujunanhuiwuhu@gmail.com

§1 加群、环的定义

本节主要包括以下内容:

1 环的概念;

2 两个重要的环;

3 环的简单性质.

一、环的定义与例子

定义

设$(R,+,\cdot)$是具有两个代数运算的代数体系,如果这个代数体系满足:

(1) $(R,+)$是一个加法交换群;

一、环的定义与例子

定义

设$(R,+,\cdot)$是具有两个代数运算的代数体系,如果这个代数体系满足:

(1) $(R,+)$是一个加法交换群;

(2) $(R,\cdot)$是一个半群;

一、环的定义与例子

定义

设$(R,+,\cdot)$是具有两个代数运算的代数体系,如果这个代数体系满足:

(1) *$(R,+)$是一个加法交换群;*

(2) *$(R,\cdot)$是一个半群;*

(3) *R的乘法"$\cdot$"对加法"$+$"满足左右分配律,即对$\forall a,b,c\in R$有*

$$a(b+c)=ab+ac \quad 且 \quad (b+c)a=ba+ca$$

一、环的定义与例子

定义

设$(R,+,\cdot)$是具有两个代数运算的代数体系,如果这个代数体系满足:

(1) $(R,+)$是一个加法交换群;

(2) $(R,\cdot)$是一个半群;

(3) R的乘法“$\cdot$”对加法“$+$”满足左右分配律,即对$\forall a,b,c\in R$有

$$a(b+c)=ab+ac \quad \text{且} \quad (b+c)a=ba+ca$$

则称$(R,+,\cdot)$是一个环,简记为R.

环的几个例子

例

$(\mathbb{Z}, +, \cdot)$是一个环,习惯上称之为整数环,记为$\mathbb{Z}$.

环的几个例子

例

$(\mathbb{Z},+,\cdot)$是一个环,习惯上称之为整数环,记为$\mathbb{Z}$. 同样有有理数环$\mathbb{Q}$,实数环$\mathbb{R}$,复数环$\mathbb{C}$.这几个环都由数组成,称为数环.

环的几个例子

例

$(\mathbb{Z},+,\cdot)$ 是一个环，习惯上称之为整数环，记为 $\mathbb{Z}$. 同样有有理数环 $\mathbb{Q}$，实数环 $\mathbb{R}$，复数环 $\mathbb{C}$. 这几个环都由数组成，称为**数环**.

例

偶数集 $2\mathbb{Z}=\{\cdots,-4,-2,0,2,4,\cdots\}$ 对于通常的加法和乘法是一个环.

环的几个例子

例

$(\mathbb{Z}, +, \cdot)$是一个环,习惯上称之为整数环,记为$\mathbb{Z}$. 同样有有理数环$\mathbb{Q}$,实数环$\mathbb{R}$,复数环$\mathbb{C}$.这几个环都由数组成,称为**数环**.

例

偶数集$2\mathbb{Z} = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$对于通常的加法和乘法是一个环.

例

设$\mathbb{Z}[i] = \{a + bi \mid \forall a, b \in \mathbb{Z}\}$,则$\mathbb{Z}[i]$按复数的通常的加法和乘法构成一个环,这个环叫做**高斯整数环**.

例

设F是一个数域,由F上一切多项式组成的集合$F[x]=\{a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\mid a_i\in F,n\in\mathbb{N}\}$关于多项式通常的加法与乘法构成一个环,这个环$(F[x],+\cdot)$称为关于$x$的一元多项式环,或一元多项式环.

例

设F是一个数域,由F上一切多项式组成的集合$F[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in F, n \in \mathbb{N}\}$关于多项式通常的加法与乘法构成一个环,这个环$(F[x], +.\cdot)$称为关于$x$的一元多项式环,或一元多项式环.

[注]　**将本例中的数域F换成任一个数环,也能构成多项式环,如$\mathbb{Z}[x]$ 叫做整系数多项式环.**

例

设F是一个数域,由F上一切多项式组成的集合$F[x]=\{a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\mid a_i\in F,n\in\mathbb{N}\}$关于多项式通常的加法与乘法构成一个环,这个环$(F[x],+.\cdot)$称为关于$x$的一元多项式环,或一元多项式环.

[注] 将本例中的数域F换成任一个数环,也能构成多项式环,如$\mathbb{Z}[x]$ 叫做整系数多项式环.

环的几个例子

例

数域F上的全部n阶方阵组成的集合$M_n(F) = \{A = (a_{ij}) \mid a_{ij} \in F, 1 \leq i, j \leq n\}$关于矩阵的加法和乘法构成一个环,这个环$(M_n(F), +, \cdot)$叫做$n$阶**矩阵环**.

例

数域F上的全部n阶方阵组成的集合$M_n(F) = \{A = (a_{ij}) \mid a_{ij} \in F, 1 \leq i, j \leq n\}$关于矩阵的加法和乘法构成一个环,这个环$(M_n(F), +, \cdot)$叫做$n$阶矩阵环.

[注] **将本例中的数域F换成任一个数环,也能构成多项式环,如用偶数环$2\mathbb{Z}[x]$替换F得环**

$$M_n(2\mathbb{Z}) = \{A = (a_{ij}|a_{ij} \in 2\mathbb{Z}, 1 \leq i, j \leq n\}.$$

二、两个重要的环

例

模n的剩余类环$(\mathbb{Z}_n, +, \cdot)$.

二、两个重要的环

例

模n的剩余类环$(\mathbb{Z}_n, +, \cdot)$.

例

加群G的自同态环$(End(G), +, \cdot)$.

三、环的简单性质

设R**是一个环,则对**$\forall a,b,c\in R,n,m\in\mathbb{N}^*$,**有如下性质:**

1 $c(a-b)=ca-cb \quad \& \quad (a-b)c=ac-ab;$

2 $0a=a0=0;$

3 $(-a)b=a(-b)=-ab;$

4 $(-a)(-b)=ab;$

5 **若**$a_1,a_2,\cdots,a_m\in R$,**则**$\sum\limits_{i=1}^{m}=a_1+a_2+\cdots+a_m;$

6 $(\sum\limits_{i=1}^{m}a_i)(\sum\limits_{j=1}^{n}b_j)=\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n}a_ib_j;$

环的简单性质

7 $(na)b = a(nb) = n(ab) \overset{def}{=} nab;$

8 $a^m = \underbrace{aa\cdots a}_{m}, a^m a^n = a^{m+n}, (a^m)^n = a^{mn};$

9 $(-n)a = \underbrace{(-a)+(-a)+\cdots+(-a)}_{n}, n(a+b) = na+nb, (n+m)a = na+ma, (nm)a = n(ma).$

§2 交换律、单位元、零因子、整环

本节主要包括以下内容:

1 **交换环的概念与简单性质;**

2 **无零因子环;**

3 **有单位元的环,整环.**

一、交换环

定义

如果环$(R,+,\cdot)$*关于乘法满足交换律,即*$\forall a,b \in R, ab=ba$, *则称*R*为***交换环**.

一、交换环

定义

如果环$(R,+,\cdot)$关于乘法满足交换律,即$\forall a,b \in R$, $ab=ba$, 则称R为**交换环**.

例

数环、偶数环、高斯整数环、一元多项式环都是交换环.

当$n>1$时,$M_n(F)$不是交换环.

一、交换环

定义

如果环$(R,+,\cdot)$关于乘法满足交换律,即$\forall a,b\in R, ab=ba$, 则称R为**交换环**.

例

数环、偶数环、高斯整数环、一元多项式环都是交换环.

当$n>1$时,$M_n(F)$不是交换环.

例

如果环$(R,+,\cdot)$的加法群是循环群,则R是交换环.

设R是交换环,$\forall a, b \in R$,**有**

1 $\forall n \in \mathbb{N}, (ab)^n = a^n b^n;$

设R是交换环,$\forall a, b \in R$,有

1 $\forall n \in \mathbb{N}, (ab)^n = a^n b^n$;

2 $(a \pm b)^2 = a^2 \pm 2ab + b^2,\ \ a^2 - b^2 = (a+b)(a-b), a^3 \pm b^3 = (a \pm b)(a^2 \mp ab + b^2)$;

设R**是交换环,**$\forall a, b \in R$,**有**

1. $\forall n \in \mathbb{N}, (ab)^n = a^n b^n$;
2. $(a \pm b)^2 = a^2 \pm 2ab + b^2$, $a^2 - b^2 = (a+b)(a-b)$, $a^3 \pm b^3 = (a \pm b)(a^2 \mp ab + b^2)$;
3. $(a+b)^n = a^n + C_n^1 a^{n-1} b + C_n^2 a^{n-2} b^2 + \cdots + C_n^{n-1} a b^{n-1} + b^n$.

二、无零因子环

定义

设R是环,如果R中元$a \neq 0, b \neq 0$,但$ab = 0$,则称a是R的一个**左零因子**, b是R的一个**右零因子**.

二、无零因子环

定义

设R是环,如果R中元$a \neq 0, b \neq 0$,但$ab = 0$,则称a是R的一个*左零因子*, b是R的一个*右零因子*.

注

1 R有左零因子$\Leftrightarrow$ R有右零因子;

二、无零因子环

定义

设R是环,如果R中元$a \neq 0, b \neq 0$,但$ab = 0$,则称a是R的一个左零因子, b是R的一个右零因子.

注

1 R有左零因子$\Leftrightarrow$ R有右零因子;

2 R的左零因子未必是右零因子,例如,取$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$, 则$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$是$R$的 右零因子, 但不是左零因子;

二、无零因子环

定义

设R是环,如果R中元$a \neq 0, b \neq 0$,但$ab = 0$,则称a是R的一个*左零因子*, b是R的一个*右零因子*.

注

1. R有左零因子$\Leftrightarrow$ R有右零因子;
2. R的左零因子未必是右零因子,例如,取$R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$, 则$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$是$R$的右零因子, 但不是左零因子;
3. 若R为交换环,则R的每个左(右)零因子都是右(左)零因子;

4 若环R中的元素a既是左零因子又是右零因子,则称a为R的**零因子**.

4 **若环R中的元素a既是左零因子又是右零因子,则称a为R的零因子.**

定义

若环R中没有左零因子,则称R为无零因子环.

4 **若环R中的元素a既是左零因子又是右零因子,则称a为R的零因子.**

定义

若环R中没有左零因子,则称R为无零因子环.

定理

设R是一个环,则

(1) *R中没有左零因子$\Leftrightarrow$ R中有左消去律;*

4 **若环R中的元素a既是左零因子又是右零因子,则称a为R的零因子.**

定义

若环R中没有左零因子,则称R为无零因子环.

定理

设R是一个环,则

(1) *R中没有左零因子$\Leftrightarrow$ R中有左消去律;*

(2) *R中没有右零因子$\Leftrightarrow$ R中有右消去律.*

推论

设R是一个环,则下列叙述等价:

(1) R中无左零因子;

(2) R中无右零因子;

(3) R中满足左消去律;

(4) R中满足右消去律.

推论

设R是一个环,则下列叙述等价:

(1) *R中无左零因子;*

(2) *R中无右零因子;*

(3) *R中满足左消去律;*

(4) *R中满足右消去律.*

由于R是无零因子环$\Leftrightarrow \forall a(\neq 0), b(\neq 0) \in R^*, ab \neq 0$**(即$R^*$是封闭的)** $\Leftrightarrow R^*$ **是封闭的**$\Leftrightarrow R^*$**是乘法半群.故有**

几个例子

推论

设R是一个环,则下列叙述等价:

(1) R中无左零因子;

(2) R中无右零因子;

(3) R中满足左消去律;

(4) R中满足右消去律.

由于R是无零因子环$\Leftrightarrow \forall a(\neq 0), b(\neq 0) \in R^*, ab \neq 0$(即$R^*$是封闭的) $\Leftrightarrow$ R^* 是封闭的$\Leftrightarrow$ R^*是乘法半群.故有

推论

R是无零因子环$\Leftrightarrow$ $(R^*, \cdot)$是半群.

例

设$A \in M_n(F)(n \geq 2)$,则A是左(右)零因子$\Leftrightarrow |A| = 0$.

无零因子环的特征性质

例

设$A \in M_n(F)(n \geq 2)$,则A是左(右)零因子$\Leftrightarrow |A| = 0$.

例

$\mathbb{Z}_n$是无零因子环$\Leftrightarrow n$为素数.

无零因子环的特征性质

例

设 $A \in M_n(F)(n \geq 2)$,*则* A *是左(右)零因子* $\Leftrightarrow |A| = 0$.

例

$\mathbb{Z}_n$ *是无零因子环* $\Leftrightarrow n$ *为素数*.

定理

设 $(R, +, \cdot)$ *是一个无零因子环,则加群* $(R, +)$ *中每个非零元素的阶彼此相同.并且,当这个阶有限时必为素数*.

三、有单位元的环

定义

若环$(R,+,\cdot)$中有元素e,使$\forall a\in R$都有$ea=ae=a$,则称这个元素为R的**单位元**.记为1_R.

三、有单位元的环

定义

若环$(R,+,\cdot)$中有元素e,使$\forall a \in R$都有$ea = ae = a$,则称这个元素为R的**单位元**.记为1_R.

注

(1) **环中的单位元未必是整数1;**

三、有单位元的环

定义

若环$(R,+,\cdot)$中有元素e,使$\forall a\in R$都有$ea=ae=a$,则称这个元素为R的**单位元**.记为1_R.

注

(1) **环中的单位元未必是整数1;**

(2) **并不是每个环都有单位元;**

三、有单位元的环

定义

若环$(R,+,\cdot)$中有元素e,使$\forall a \in R$都有$ea = ae = a$,则称这个元素为R的单位元.记为1_R.

注

(1) 环中的单位元未必是整数1;

(2) 并不是每个环都有单位元;

(3) 若环中有单位元,则这个单位元是惟一的.

有单位元的环

定义

设R是有单位元1_R的环,$a \in R$.若有$b \in R$使$ab = ba = 1_R$,则称a是R中的**可逆元**, 并称b为a的**逆元**.

定义

设R是有单位元1_R的环,$a \in R$.若有$b \in R$使$ab = ba = 1_R$,则称a是R中的**可逆元**, 并称b为a的**逆元**.

注

(1) **只有在有单位元的环中才能谈论逆元的问题;**

有单位元的环

定义

设R是有单位元1_R的环,$a \in R$.若有$b \in R$使$ab = ba = 1_R$,则称a是R中的**可逆元**,并称b为a的**逆元**.

注

(1) 只有在有单位元的环中才能谈论逆元的问题;

(2) 即使在有单位元的环中,也不保证每个元素都有逆元;

定义

设R是有单位元1_R的环,$a \in R$.若有$b \in R$使$ab = ba = 1_R$,则称a是R中的**可逆元**,并称b为a的**逆元**.

注

(1) 只有在有单位元的环中才能谈论逆元的问题;

(2) 即使在有单位元的环中,也不保证每个元素都有逆元;

(3) 若元a可逆,则a的逆元素是惟一的,记为a^{-1}.

有单位元的环

定义

设R是有单位元1_R的环,$a \in R$.若有$b \in R$使$ab = ba = 1_R$,则称a是R中的**可逆元**, 并称b为a的**逆元**.

注

(1) **只有在有单位元的环中才能谈论逆元的问题;**

(2) **即使在有单位元的环中,也不保证每个元素都有逆元;**

(3) **若元a可逆,则a的逆元素是惟一的,记为a^{-1}.**

性质

设R是有单位元的环,R中所有可逆元构成的集合

整环的概念

定义

设R是环,若满足

(1) R是交换环;

定义

设R是环,若满足

(1) R是交换环;

(2) R有单位元;

整环的概念

定义

设R是环,若满足

(1) R是交换环;

(2) R有单位元;

(3) R是无零因子环,

则称R为**整环**.

整环的概念

定义

设R是环,若满足

(1) R是交换环;

(2) R有单位元;

(3) R是无零因子环,

则称R为**整环**.

例

整数环、多项式环、模p(p为素数)的剩余类环都是整环.

整环的概念

定义

设R是环,若满足

(1) R是交换环;

(2) R有单位元;

(3) R是无零因子环,

则称R为**整环**.

例

整数环、多项式环、模p(p为素数)的剩余类环都是整环.

偶数环、矩阵环、模n(n为合数)的剩余类环都不是整环.

§3 除环、域

本节主要介绍除环与域的概念

一、除环

定义

设R是环,若满足

(1) R中有非零元;

除环的定义

一、除环

定义

设R是环,若满足

(1) R中有非零元;

(2) R有单位元;

一、除环

定义

设R是环,若满足

(1) R中有非零元;

(2) R有单位元;

(3) R^*中每个元素都可逆(于是$R^* = R^\cdot$),

则称R为除环.

除环的几个性质

性质

(1) *除环是无零因子环,反之不然;*

除环的几个性质

性质

(1) *除环是无零因子环,反之不然;*

(2) *若R是除环,则R^*是一个乘法群;*

除环的几个性质

性质

(1) *除环是无零因子环,反之不然;*

(2) *若R是除环,则R^*是一个乘法群;*

(3) *非零环R是除环$\Leftrightarrow$ R^*是乘法群;*

除环的几个性质

性质

(1) *除环是无零因子环,反之不然;*

(2) *若R是除环,则R^*是一个乘法群;*

(3) *非零环R是除环$\Leftrightarrow$ R^*是乘法群;*

(4) *有限的非零环R是除环$\Leftrightarrow$ R是无零因子环.*

二、域

定义

*若环R是交换除环,则称R为**域**,记为F.*

二、域

定义

若环R是交换除环,则称R为域,记为F.

由于域F为除环,所以$(F^*,+,\cdot)$是乘法群,因而对$\forall a,b\in F^*$方程:

$$ax=b \qquad \text{与} \qquad ya=b$$

在F^*中有惟一解$x=a^{-1}b,y=ba^{-1}$.但F为域,所以$a^{-1}b=ba^{-1}\overset{def}{=}\dfrac{b}{a}$,并称$\dfrac{b}{a}$为"$b$除以$a$所得的商"(或"$a$除$b$的商").

在域F中，$\dfrac{b}{a}(a(\neq 0), b \in F)$有下列性质

(1) 若$a \neq 0, c \neq 0$,则$\dfrac{b}{a} = \dfrac{d}{c} \Leftrightarrow ad = bc;$

在域F中，$\frac{b}{a}(a(\neq 0), b \in F)$有下列性质

(1) **若**$a \neq 0, c \neq 0$,**则**$\frac{b}{a} = \frac{d}{c} \Leftrightarrow ad = bc$;

(2) $\frac{b}{a} \pm \frac{d}{c} = \frac{bc \pm ad}{ac}$;

在域F中，$\frac{b}{a}(a(\neq 0), b \in F)$有下列性质

(1) 若$a \neq 0, c \neq 0$，则$\frac{b}{a} = \frac{d}{c} \Leftrightarrow ad = bc$;

(2) $\frac{b}{a} \pm \frac{d}{c} = \frac{bc \pm ad}{ac}$;

(3) $\frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac}$;

在域F中，$\frac{b}{a}(a(\neq 0), b \in F)$有下列性质

(1) **若**$a \neq 0, c \neq 0$,**则**$\frac{b}{a} = \frac{d}{c} \Leftrightarrow ad = bc$;

(2) $\frac{b}{a} \pm \frac{d}{c} = \frac{bc \pm ad}{ac}$;

(3) $\frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac}$;

(4) $\frac{b}{a} / \frac{d}{c} = \frac{bc}{ad}$.

在域F中,$\frac{b}{a}(a(\neq 0), b \in F)$有下列性质

(1) **若**$a \neq 0, c \neq 0$,**则**$\frac{b}{a} = \frac{d}{c} \Leftrightarrow ad = bc$;

(2) $\frac{b}{a} \pm \frac{d}{c} = \frac{bc \pm ad}{ac}$;

(3) $\frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac}$;

(4) $\frac{b}{a} / \frac{d}{c} = \frac{bc}{ad}$.

定理

设R是一个有限的非零环,则R是域$\Leftrightarrow$ R是整环.

作业

$$\mathbf{p.\ 89\ \ 1,2,5\quad p.\ 93\ \ 1,2,5}$$

§4 无零因子环的特征

本节主要介绍环的特征的概念

一般环的特征的概念

定义

设R为任意环,如果存在正整数n,使对$\forall a \in R$,都有$na = 0$,则称这样的最小正整数n为环R的**特征**,记为$char(R)$.如果不存在这样的正整数,则称R的特征为无穷大,记为$char(R) = \infty$.

一般环的特征的概念

定义

设R为任意环,如果存在正整数n,使对$\forall a \in R$,都有$na = 0$,则称这样的最小正整数n为环R的**特征**,记为$char(R)$.如果不存在这样的正整数,则称R的特征为无穷大,记为$char(R) =\infty$.

例

$char(\mathbb{Z}) = \infty$, $char(F(x)) = \infty$,
$char(M_n(F)) = \infty$.
$char(\mathbb{Z}_n) = n$.

注

(1) **若环R的加群中有一个元素的阶为∞,则$\text{char}(R)=\infty$;**

环的特征的几个性质

注

(1) **若环R的加群中有一个元素的阶为∞,则char$(R)=\infty$;**

(2) **若环R的加群中每个元素都是有限阶的且最大的阶为n,则char$(R)=n$;**

注

(1) 若环R的加群中有一个元素的阶为∞,则$\mathrm{char}(R) = \infty$;

(2) 若环R的加群中每个元素都是有限阶的且最大的阶为n,则$\mathrm{char}(R) = n$;

(3) 存在环R,使得加群$(R, +)$中既有无穷阶的元素又有有限阶的元素(如$R = \mathbb{Z}_n \times \mathbb{Z}, (a, b) + (c, d) = (a + c, b + d), (a, b)(c, d) = (0, 0)$);

注

(1) 若环R的加群中有一个元素的阶为∞,则$\mathrm{char}(R)=\infty$;

(2) 若环R的加群中每个元素都是有限阶的且最大的阶为n,则$\mathrm{char}(R)=n$;

(3) 存在环R,使得加群$(R,+)$中既有无穷阶的元素又有有限阶的元素(如$R=\mathbb{Z}_n\times\mathbb{Z},(a,b)+(c,d)=(a+c,b+d),(a,b)(c,d)=(0,0)$);

(4) 存在环R,使得加群$(R,+)$中每个元素都是有限阶的,但不存在最大的阶(如$R=\{x\in\mathbb{C}|\exists n\in\mathbb{N}\ni x^n=1)\},x\oplus y=xy,x\otimes y=1)$.

例

若R中每个元素都是幂等元(即$\forall a \in R, a^2 = a$)且$R \neq \{0\}$, 则R是特征为2的交换环.

例

若R中每个元素都是幂等元(即$\forall a \in R, a^2 = a$)且$R \neq \{0\}$, 则R是特征为2的交换环.

证

$\forall a \in R$,由$2a = (2a)^2 = 4a^2 = 4a = 2a + 2a$得$2a = 0$, 再由$R \neq \{0\}$得char$R$=2,于是对$\forall a, b \in R$, $a + b = (a+b)^2 = a^2 + b^2 + ab + ba$,即$ab = -ba$,但$a = -a$,所以$ab = ba$.

在第二节,我们已经证明了

定理

设$(R,+,\cdot)$是一个无零因子环,则加群$(R,+)$中每个非零元素的阶彼此相同.并且,当这个阶有限时必为素数.

在第二节,我们已经证明了

定理

设$(R,+,\cdot)$是一个无零因子环,则加群$(R,+)$中每个非零元素的阶彼此相同.并且,当这个阶有限时必为素数.

所以有

推论

整环,除环和域的特征或是无限大,或是一个素数.

练习

练习

1. 设$a(\neq 0)\in R$,若a不是零因子,则$\mathrm{char}(R)=|a|$;
2. 若域F的阶为偶数,则$\mathrm{char}(F)=2$.

§5 子环、环的同态

本节主要包含以下内容:

1 子环的定义,尤其是子整环,子除环和子域的定义.

2 环同态映射的定义与基本性质.

3 环同构的应用–挖补定理.

子环的定义

定义

设S是环R的非空子集,如果S关于R中的加法和乘法作成一个环,则称S为R的一个**子环**,同时称R为S的**扩环**.

定义

设S是环R的非空子集,如果S关于R中的加法和乘法作成一个环,则称S为R的一个子环,同时称R为S的扩环.

等价地,有

定义

设$S(\neq \emptyset) \subseteq (R, +, \cdot)$.若$S$满足

(1) $(S, +)$是$(R, +)$的子群(即$\forall a, b \in S, a - b \in S$);

子环的定义

定义

设S是环R的非空子集,如果S关于R中的加法和乘法作成一个环,则称S为R的一个子环,同时称R为S的扩环.

等价地,有

定义

设$S(\neq \emptyset) \subseteq (R, +, \cdot)$.若$S$满足

(1) $(S, +)$是$(R, +)$的子群(即$\forall a, b \in S, a - b \in S$);

(2) $(S, \cdot)$对乘法封闭(即$\forall a, b \in S, ab \in S$)

则称S是R的子环.

子环的定义

类似地,可以定义子整环,子除环和子域:

类似地,可以定义子整环,子除环和子域:

定义

设R是整环,$S(\neq \emptyset) \subseteq R$,若$\forall a, b \in S, a-b \in S, ab \in S$, 且$S$中有单位元, 则称$S$是$R$的子整环.

子环的定义

类似地,可以定义子整环,子除环和子域:

定义

设R是整环,$S(\neq\emptyset)\subseteq R$,若$\forall a,b\in S, a-b\in S, ab\in S$, 且$S$中有单位元, 则称$S$是$R$的子整环.

定义

设R是除环,$S(\neq\emptyset)\subseteq R$,若

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

(2) $S\neq\{0\}$,且S中有单位元(即$(S^*,\cdot)$是一个乘法群),

则称S是R的子除环.

几个例子

定义

若S既是R的子整环也是R的子除环,则称S是R的子域.

几个例子

定义

若S既是R的子整环也是R的子除环,则称S是R的子域.

例

1 *对任意环R,零环$\{0\}$和R是R的子环,这两个环称为R的平凡子环.*

几个例子

定义

若S既是R的子整环也是R的子除环,则称S是R的子域.

例

1. 对任意环R,零环$\{0\}$和R是R的子环,这两个环称为R的平凡子环.
2. 偶数环$2\mathbb{Z}$是整数环的子环,但不是子整环.

几个例子

定义

若S既是R的子整环也是R的子除环,则称S是R的子域.

例

1. *对任意环R,零环$\{0\}$和R是R的子环,这两个环称为R的平凡子环.*
2. *偶数环$2\mathbb{Z}$是整数环的子环,但不是子整环.*
3. *$\mathbb{Z}[x]$是$F[x]$的子环,其中F是数域.*

几个例子

定义

若S既是R的子整环也是R的子除环,则称S是R的子域.

例

1. 对任意环R,零环$\{0\}$和R是R的子环,这两个环称为R的平凡子环.
2. 偶数环$2\mathbb{Z}$是整数环的子环,但不是子整环.
3. $\mathbb{Z}[x]$是$F[x]$的子环,其中F是数域.
4. $S = \{[0], [2], [4]\}$是$\mathbb{Z}_6$的子域,但$\mathbb{Z}_6$不是整环,并且S与$\mathbb{Z}_6$的单位元不相等.

5 **设** $S_1=\left\{\begin{pmatrix} n & 0\\ 0 & n\end{pmatrix}, n\in\mathbb{Z}\right\}$,

$S_2=\left\{\begin{pmatrix} \alpha & 0\\ 0 & \alpha\end{pmatrix}, \alpha\in\mathbb{C}\right\}$,

$S_3=\left\{\begin{pmatrix} \alpha & \beta\\ -\bar\beta & \bar\alpha\end{pmatrix}, \alpha,\beta\in\mathbb{Z}\right\}$.

则S_1是$M_2(\mathbb{C})$的子整环,S_2是$M_2(\mathbb{C})$的子域, S_3是子除环,但$M_2(\mathbb{C})$不是整环,不是除环,更不是域.

由此可以看出,子环具有很多奇怪的性质,总之有

子环的奇怪性质

性质

设S是R的子环,则

(1) R有单位元,S未必有单位元;

子环的奇怪性质

性质

设S是R的子环,则

(1) R有单位元,S未必有单位元;

(2) R没有单位元,S可能有单位元;

性质

设S是R的子环,则

(1) R有单位元,S未必有单位元;

(2) R没有单位元,S可能有单位元;

(3) R不是交换环,S可能是交换环;

性质

设S是R的子环,则

(1) *R有单位元,S未必有单位元;*

(2) *R没有单位元,S可能有单位元;*

(3) *R不是交换环,S可能是交换环;*

(4) *R和S都有单位元,但它们的单位元可能不一致;*

性质

设S是R的子环,则

(1) R有单位元,S未必有单位元;

(2) R没有单位元,S可能有单位元;

(3) R不是交换环,S可能是交换环;

(4) R和S都有单位元,但它们的单位元可能不一致;

(5) R不是整环(除环、域),S可能是整环(除环、域);

子环的奇怪性质

性质

设S是R的子环,则

(1) R有单位元,S未必有单位元;

(2) R没有单位元,S可能有单位元;

(3) R不是交换环,S可能是交换环;

(4) R和S都有单位元,但它们的单位元可能不一致;

(5) R不是整环(除环、域),S可能是整环(除环、域);

(6) R是整环(除环、域),S未必是整环(除环、域).

子环的几个性质

性质

设R为环,记$C(R) = \{a \in R | \forall x \in R, ax = xa\}$,则$C(R)$是$R$的子环,这个子环叫做$R$的**中心**,并且若$R$是交换环,则$C(R) = R$.

子环的几个性质

性质

设R为环,记$C(R) = \{a \in R | \forall x \in R, ax = xa\}$,则$C(R)$是$R$的子环,这个子环叫做$R$的中心,并且若$R$是交换环,则$C(R) = R$.

性质

设R_1和R_2都是环,则$R_1 \cap R_2$是R_1和R_2的子环.

环同态的定义

定义

设φ是环$(R,+,\cdot)$到环$(\bar{R},\bar{+},\bar{\cdot})$的映射.若有

$$\varphi(a+b)=\varphi(a)\bar{+}\varphi(b),\varphi(a\cdot b)=\varphi(a)\bar{\cdot}\varphi(b),\forall a,b\in R$$

则称φ是一个**环同态**映射,如果φ 满射(单射、双射),则称φ为**环满同态(环单同态、环同构)**.当φ是环同态满射时,称R与$\bar{R}$**同态**,记为$R\sim\bar{R}$.

由定义即得

定理

设$(A,+,\cdot),(\bar{A},\bar{+},\bar{\cdot})$是两个代数系统,如果$\varphi$是$A$到$\bar{A}$的满射,且对$\forall a,b\in A,\varphi(a+b)=\varphi(a)\bar{+}\varphi(b),\varphi(a\cdot b)=\varphi(a)\bar{\cdot}\varphi(b)$, 则当$(A,+,\cdot)$是环时,$(\bar{A},\bar{+},\bar{\cdot})$也是环.

环同态的几个性质

定理

设$R \overset{\varphi}{\sim} \bar{R}$是环同态满射,则

(1) $\varphi(0_R) = 0_{\bar{R}}$;

(2) $\varphi(1_R) = 1_{\bar{R}}$;

(3) $\varphi(-a) = -\varphi(a)$;

(4) 若R是交换环,则$\bar{R}$也是交换环.

两个例子

例

1 $\varphi : \mathbb{Z} \to \mathbb{Z}_6; n \mapsto [n]$为环满同态，$\mathbb{Z}$是整环,但$\varphi(2)$是$\mathbb{Z}_6$中的零因子.这说明:非零因子的象可能是零因子.

例

1. $\varphi : \mathbb{Z} \to \mathbb{Z}_6; n \mapsto [n]$为环满同态, $\mathbb{Z}$是整环,但$\varphi(2)$是$\mathbb{Z}_6$中的零因子.这说明:非零因子的象可能是零因子.
2. 设$R = \mathbb{Z} \times \mathbb{Z} = \{(a, b)|a, b \in \mathbb{Z}\}, R$ 中的加法和乘法均为分量的加法和乘法,则R是一个环,R到$\mathbb{Z}$的投射$\pi_1 : R \to \mathbb{Z}; (a, b) \mapsto a$是环同态满射,这个同态满射使$R$ 中零因子的象不是零因子.

环同构的性质

定理

若$R \overset{\varphi}{\cong} \bar{R}$是环同构,则$R$是整环(除环,域)当且仅当$\bar{R}$是整环(除环,域).

环同构的性质

定理

若$R \overset{\varphi}{\cong} \bar{R}$是环同构,则$R$是整环(除环,域)当且仅当$\bar{R}$是整环(除环,域).

由此可以得到

引理

设$(R,+,\cdot)$是一个环,$\varphi: R \to A$是一个双射(A为集合),则可以给集合A定义加法和乘法,使得φ成为R到A的同构.

定理 (挖补定理)

设S是环$(R,+,\cdot)$的一个子环,$B=R-S$.$\bar{S}$也是环且$S\overset{\varphi}{\cong}\bar{S}$, $B\cap S=\emptyset$.则存在环$\bar{R}$,满足:(1) $R\cong\bar{R}$; (2) $\bar{S}$是$\bar{R}$的子环.

定理 (挖补定理)

设S是环$(R,+,\cdot)$的一个子环,$B=R-S$.$\bar{S}$也是环且$S\overset{\varphi}{\cong}\bar{S}$, $B\cap S=\emptyset$.则存在环$\bar{R}$,满足:(1) $R\cong\bar{R}$; (2) $\bar{S}$是$\bar{R}$的子环.

证

设$S=\{a_S,b_S,c_S,\cdots\}\xrightarrow{\varphi}\bar{S}=\{\bar{a_S},\bar{b_S},\bar{c_S},\cdots\}$; $x_S\mapsto\bar{x_S}$.记$B=\{a,b,c,\cdots\}$.

作$f:R\to\bar{R}$; $x\mapsto\begin{cases}\bar{x_S}, & 若x\in S;\\ x & 若x\in B.\end{cases}$ 则f为双射.

由引理,可为$\bar{R}$定义加法$\bar{+}$和乘法$\bar{\cdot}$,使$\bar{R}$为环且$R\overset{f}{\cong}\bar{R}$.

挖补定理

设S与$\bar{S}$中的加法和乘法分别记为$+,\cdot$,下证:在$\bar{S}$内,$+$与$\bar{+}$是一致的,$\cdot$与$\bar{\cdot}$是一致的.

$\forall \bar{x}_S, \bar{y}_S \in \bar{S}, \bar{x}_S + \bar{y}_S = \bar{z}_S \in \bar{S}$, 则有$x_S, y_S, z_S \in S$使$\varphi(x_S) = \bar{x}_S, \varphi(y_S) = \bar{y}_S, \varphi(z_S) = \bar{z}_S$,于是$\bar{x}_S \bar{+} \bar{y}_S = \varphi(x_S) \bar{+} \varphi(y_S) = f(x_S) \bar{+} f(y_S) = f(x_S + y_S) = f(z_S) = \varphi(z_S) = \bar{z}_S$, 这说明在$\bar{S}$中$\bar{+}$与$+$是一致的.

同理可证,在$\bar{S}$中$\bar{\cdot}$与$\cdot$也是一致的.所以,$\bar{S}$ 是$\bar{R}$的子环. $\square$

§6 多项式环

本节主要包含以下内容:

1 多项式环的定义.

2 未定元存在定理.

设R_0是有单位元1_{R_0}的交换环,R是R_0的子环且$1_{R_0} \in R$.任取定$\alpha \in R_0$,考察R_0中含R与α的最小子环:

$$R[\alpha] = \{f(\alpha) = \sum_{i=0}^{n} a_i\alpha^i \mid a_i \in R, n \in \mathbb{N}\},$$

显然有

$$f(\alpha) = \sum_{i=0}^{n} a_i\alpha^i = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in R_0.$$

多项式的定义

设R_0是有单位元1_{R_0}的交换环,R是R_0的子环且$1_{R_0} \in R$.任取定$\alpha \in R_0$,考察R_0中含R与α的最小子环:

$$R[\alpha] = \{f(\alpha) = \sum_{i=0}^{n} a_i\alpha^i \mid a_i \in R, n \in \mathbb{N}\},$$

显然有

$$f(\alpha) = \sum_{i=0}^{n} a_i\alpha^i = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in R_0.$$

定义

如上形式的$f(\alpha)$叫做R上关于α的一个多项式,a_i叫做多项式$f(\alpha)$的系数.

$R[\alpha]$作成一个环(R_0的子环),还需指出$R[\alpha]$中的运算:

$\forall f(\alpha)=\sum_{i=0}^{n} a_i\alpha^i, g(\alpha)=\sum_{j=0}^{m} b_j\alpha^j$,不妨设$m\leq n, b_{m+1}$ $b_{m+2}=\cdots=b_n=0$, 运算为

$$f(\alpha)+g(\alpha)=\sum_{i=0}^{n}(a_i+b_i)\alpha^i,$$

$$f(\alpha)\cdot g(\alpha)=(\sum_{i=0}^{n} a_i\alpha^i)(\sum_{j=0}^{m} b_j\alpha^j)=\sum_{k=0}^{n+m} c_k\alpha^k$$

其中$c_k=\sum_{i+j=k} a_ib_j$.

多项式环的定义

定义

环$R[\alpha]$叫做R上的α的**多项式环**.

多项式环的定义

定义

环$R[\alpha]$叫做R上的α的多项式环.

由于$R[\alpha]$中多项式$f(\alpha)$的表达形式未必惟一(例如,$R=\mathbb{Z},\alpha=\sqrt{2}\in R_0=\mathbb{R}$,则在$\mathbb{Z}[\sqrt{2}]$中有$0=0+0(\sqrt{2})^2=-2+(\sqrt{2})^2$,即0的表达式不惟一),就是说:上述定义的多项式环中会出现一种现象:$f(\alpha)$ $a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n=0$,但系数$a_0,a_1,a_2,\ldots,a_n$ 全为零.这与高等代数中的零多项式的定义相矛盾.因此,我们有必要对α作进一步讨论.

定义

R_0中的一个元素α叫做R上的一个未定元(超越元),如果在R中找不到不全为零的元素$a_0, a_1, a_2, \ldots, a_n$使$\sum\limits_{i=0}^{n} a_i\alpha^i = 0$.否则,称$\alpha$为$R$上的代数元.习惯上,记$R$上的未定元为$x$.

定义

R_0中的一个元素α叫做R上的一个未定元(超越元),如果在R中找不到不全为零的元素$a_0, a_1, a_2, \ldots, a_n$使$\sum_{i=0}^{n} a_i\alpha^i = 0$.否则,称$\alpha$为$R$上的代数元.习惯上,记$R$上的未定元为$x$.

定义

设$f(\alpha) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n (a_n \neq 0)$为环$R$上的一元多项式，则非负整数$n$叫做这个多项式的次数，多项式0没有次数.

R上未定元的多项式才可定义次数,但对给定的环,未定元未必存在.例如,设$R_0 = \mathbb{Q}, R = \mathbb{Z}$的未定元不存在.

未定元存在定理

R上未定元的多项式才可定义次数,但对给定的环,未定元未必存在.例如,设$R_0=\mathbb{Q}, R=\mathbb{Z}$的未定元不存在.

定理 (未定元存在定理)

设R是有单位元的交换环,则存在R的扩环R_0,使得R_0中含有R的未定元.

未定元存在定理

R上未定元的多项式才可定义次数,但对给定的环,未定元未必存在.例如,设$R_0=\mathbb{Q}$, $R=\mathbb{Z}$的未定元不存在.

定理 (未定元存在定理)

设R是有单位元的交换环,则存在R的扩环R_0,使得R_0中含有R的未定元.

证明思路

(1) **记**$P=\{(a_0,a_1,a_2,\cdots)\mid a_i\in R$, **只有有限个**$a_i\neq 0\}$, **其运算为:**$(a_0,a_1,a_2,\cdots)+(b_0,b_1,b_2,\cdots)=(a_0+b_0,a_1+b_1,a_2+b_2,\cdots)$, $(a_0,a_1,a_2,\cdots)\cdot(b_0,b_1,b_2,\cdots)=(c_0,c_1,c_2,\cdots)$,

未定元存在定理

其中$c_k = \sum_{i+j=k} a_i b_j$.则$P$是有单位元$(1, 0, 0, \cdots)$的交换环.

其中$c_k=\sum\limits_{i+j=k}a_ib_j$.则$P$是有单位元$(1,0,0,\cdots)$的交换环.

(2) P中全体形为$(a,0,0,\cdots)$的元素作成与R同构的子环$\bar{R}$,且$(P-\bar{R})\cap R=\emptyset$,由挖补定理得到一个新的环$R_0$,使得$R$是$R_0$的子环且$R_0\cong P$, R_0的单位元就是R中单位元1_R.

其中$c_k = \sum\limits_{i+j=k} a_i b_j$.则$P$是有单位元$(1,0,0,\cdots)$的交换环.

(2) P中全体形为$(a,0,0,\cdots)$的元素作成与R同构的子环$\bar{R}$,且$(P-\bar{R})\cap R=\emptyset$,由挖补定理得到一个新的环$R_0$,使得$R$是$R_0$的子环且$R_0 \cong P$, R_0的单位元就是R中单位元1_R.

(3) 记$x=(0,1,0,0,\cdots)$,则x是R上的未定元.

其中$c_k = \sum\limits_{i+j=k} a_i b_j$.则$P$是有单位元$(1,0,0,\cdots)$的交换环.

(2) P中全体形为$(a,0,0,\cdots)$的元素作成与R同构的子环$\bar{R}$,且$(P-\bar{R})\cap R=\emptyset$,由挖补定理得到一个新的环$R_0$,使得$R$是$R_0$的子环且$R_0 \cong P$, R_0的单位元就是R中单位元1_R.

(3) 记$x=(0,1,0,0,\cdots)$,则x是R上的未定元.

例

设F为整环,R为F的子环,如果F中的每个元素都是R上的代数元, 则F是一个域.

多元多项式环

设R_0是有单位元的交换环,R是R_0的子环且$1_{R_0} \in R$.任取R_0中n个元素$\alpha_1, \alpha_2, \cdots, \alpha_n$,首先作$R$上$\alpha_1$的多项式环$R[\alpha_1]$,再作$R[\alpha_1]$上$\alpha_2$的多项式环$R[\alpha_1][\alpha_2]$,后作$R[\alpha_1][\alpha_2]\cdots[\alpha_{n-1}]$上$\alpha_n$的多项式$R[\alpha_1]\cdots[\alpha_n]$. $\forall f(\alpha_1, \ldots, \alpha_n) \in R[\alpha_1]\cdots[\alpha_n]$,有$f(\alpha_1, \ldots, \alpha_n) = \sum a_{i_1 i_2 \cdots i_n} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}$,其中系数$a_{i_1 i_2 \cdots i_n} \in R$ 只有有限个$\neq 0$.

设R_0是有单位元的交换环,R是R_0的子环且$1_{R_0}\in R$.任取R_0中n个元素$\alpha_1,\alpha_2,\cdots,\alpha_n$,首先作$R$上$\alpha_1$的多项式环$R[\alpha_1]$,再作$R[\alpha_1]$上$\alpha_2$的多项式环$R[\alpha_1][\alpha_2]$,后作$R[\alpha_1][\alpha_2]\cdots[\alpha_{n-1}]$上$\alpha_n$的多项式$R[\alpha_1]\cdots[\alpha_n]$. $\forall f(\alpha_1,\ldots,\alpha_n)\in R[\alpha_1]\cdots[\alpha_n]$,有$f(\alpha_1,\ldots,\alpha_n)=\sum a_{i_1i_2\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}$,其中系数$a_{i_1i_2\cdots i_n}\in R$只有有限个$\neq 0$.

定义

*上述描述的每个$f(\alpha_1,\ldots,\alpha_n)$称为$R$上的$\alpha_1,\ldots,\alpha_n$**多元多项式**,而每个$a_{i_1i_2\cdots i_n}$叫作$f(\alpha_1,\ldots,\alpha_n)$的**系数**.习惯上,$R$上$\alpha_1,\ldots,\alpha_n$的多元多项式环$R[\alpha_1]\cdots[\alpha_n]$记作$R[\alpha_1,\ldots,\alpha_n]$.*

多元多项式环中的加法和乘法运算为

$$\Big(\sum_{i_1 i_2\cdots i_n} a_{i_1 i_2\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}\Big)+$$

$$+\Big(\sum_{j_1 j_2\cdots j_n} b_{j_1 j_2\cdots j_n}\alpha_1^{j_1}\alpha_2^{j_2}\cdots\alpha_n^{j_n}\Big)$$

$$=\Big(\sum_{i_1 i_2\cdots i_n}(a_{i_1 i_2\cdots i_n}+b_{i_1 i_2\cdots i_n})\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}\Big)$$

$$\Big(\sum_{i_1 i_2\cdots i_n} a_{i_1 i_2\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}\Big)$$

$$\Big(\sum_{j_1 j_2\cdots j_n} b_{j_1 j_2\cdots j_n}\alpha_1^{j_1}\alpha_2^{j_2}\cdots\alpha_n^{j_n}\Big)$$

$$=\Big(\sum_{k_1 k_2\cdots k_n} c_{k_1 k_2\cdots k_n}\alpha_1^{k_1}\alpha_2^{k_2}\cdots\alpha_n^{k_n}\Big)$$

其中 $c_{k_1 k_2\cdots k_n}=\sum_{i_m+j_m=k_m} a_{i_1 i_2\cdots i_n} b_{j_1 j_2\cdots j_n}$

多元多项式环中也存在着表示不惟一的问题,因此要定义无关未定元.

定义

R_0中n个元$x_1, x_2, \cdots, x_n$叫做R上的**无关未定元**,如果它们满足:R上的任一个关于$x_1, x_2, \cdots, x_n$的多项式为零$\Leftrightarrow$该多项式的系数全为零.

容易证明

定理

设R是一个有单位元的交换环,对任意正整数n,存在R上的无关未定元$x_1, x_2, \cdots, x_n$,使多项式环$R[x_1, x_2, \cdots, x_n]$存在.

未定元的重要性质

定理

设$\alpha, x \in R_0$, R是R_0的子环,x为R上的未定元,则$R[x] \sim R[\alpha]$.

一般地,有

定理

设$R[x_1, x_2, \ldots, x_n]$和$R[\alpha_1, \alpha_2, \ldots, \alpha_n]$都是有单位元的交换环$R$上的多项式环,且$x_1, x_2, \ldots, x_n$是$R$上的无关未定元,而$\alpha_1, \alpha_2, \ldots, \alpha_n$是$R_0$中的任意元,则$R[x_1, x_2, \ldots, x_n] \sim R[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

推论

在$R[x]$中,设$u(x) = f(x) + g(x), v(x) = f(x) \cdot g(x)$,则在$R[\alpha]$中有$u(\alpha) = f(\alpha) + g(\alpha), v(\alpha) = f(\alpha) \cdot g(\alpha)$.

作业

p. 97 1 p. 101 2,3,4
p. 109 2

§7 理想

本节主要包括以下内容:

1 理想的定义;

2 单环的概念;

3 生成理想的概念及其中元素的表示形式;

4 主理想和特殊情况下主理想的结构.

设N**是环**R**的子环,则**$(N,+)\leq(R,+)$,**且由**$(R,+)$**是可换群可知**$N\lhd R$, **于是有商群**$R/N=\{a+N\mid\forall a\in R\}$,**商群中的加法为**$(a+N)+(b+N)=(a+b)+N$.

问题的提出

设N是环R的子环,则$(N,+)\leq(R,+)$,
且由$(R,+)$是可换群可知$N\lhd R$, 于是有商群$R/N=\{a+N\mid\forall a\in R\}$,商群中的加法为$(a+N)+(b+N)=(a+b)+N$.

对于R/N,是否可以再定义一个乘法使R/N成为环?

设N是环R的子环,则$(N,+)\leq(R,+)$,且由$(R,+)$是可换群可知$N\lhd R$, 于是有商群$R/N=\{a+N\mid\forall a\in R\}$,商群中的加法为$(a+N)+(b+N)=(a+b)+N$.

对于R/N,是否可以再定义一个乘法使R/N成为环?

如果R/N成为环,必有

$$(a+N)(b+N)=ab+N. \qquad (*)$$

要使$(*)$式成立,N该满足什么条件呢?

设N是环R的子环,则$(N,+) \leq (R,+)$,且由$(R,+)$是可换群可知$N \lhd R$, 于是有商群$R/N = \{a+N \mid \forall a \in R\}$,商群中的加法为$(a+N)+(b+N)=(a+b)+N$.

对于R/N,是否可以再定义一个乘法使R/N成为环?

如果R/N成为环,必有

$$(a+N)(b+N)=ab+N. \qquad (*)$$

要使$(*)$式成立,N该满足什么条件呢?

由于$ab+N \subseteq ab+N+aN+bN=(a+N)(b+N)$,所以,$(*)$成立的关键是$(a+N)(b+N) \subseteq ab+N$.由此可以得到

问题的提出

性质

对$\forall a,b\in R$,

$$(a+N)(b+N)=ab+N\Leftrightarrow aN\subseteq B\text{且}Nb\subseteq N.$$

问题的提出

性质

对$\forall a,b\in R$,

$$(a+N)(b+N)=ab+N \Leftrightarrow aN\subseteq B \text{且} Nb\subseteq N.$$

所以,R的子环N满足$\forall a,b\in R, aN, Nb\subseteq N$是很重要的.因为，由此可以在商群$(R/N,+)$中定义乘法,使$\forall a,b\in R,(a+N)(b+N)=ab+N$.

定义

设N是R的子环.

(1) 如果$\forall a \in R$,有$aN \subseteq N$,则称N是R的一个**左理想**;

理想的定义

定义

设N是R的子环.

(1) 如果$\forall a \in R$,有$aN \subseteq N$,则称N是R的一个左理想;

(2) 如果$\forall a \in R$,有$Na \subseteq N$,则称N是R的一个右理想;

理想的定义

定义

设N是R的子环.

(1) 如果$\forall a \in R$,有$aN \subseteq N$,则称N是R的一个左理想;

(2) 如果$\forall a \in R$,有$Na \subseteq N$,则称N是R的一个右理想;

(3) 如果$\forall a, b \in R$,有$aN \subseteq N, Nb \subseteq N$,则称$N$是$R$的一个理想.

定义

设N是R的子环.

(1) 如果$\forall a \in R$,有$aN \subseteq N$,则称N是R的一个**左理想**;

(2) 如果$\forall a \in R$,有$Na \subseteq N$,则称N是R的一个**右理想**;

(3) 如果$\forall a, b \in R$,有$aN \subseteq N, Nb \subseteq N$, 则称$N$是$R$的一个**理想**.

本节主要讨论理想.N是R的理想是指:N首先是R的子环;其次,$\forall a, b \in R, aN \subseteq N, Nb \subseteq N$.于是有

理想的定义

定义

设N是R的非空子集,如果

(1) $\forall a, b \in N, a - b \in N, ab \in N;$

理想的定义

定义

设N是R的非空子集,如果

(1) $\forall a, b \in N, a - b \in N, ab \in N;$

(2) $\forall r \in R, rN \subseteq N, Nr \subseteq N,$

定义

设N是R的非空子集,如果

(1) $\forall a, b \in N, a-b \in N, ab \in N;$

(2) $\forall r \in R, rN \subseteq N, Nr \subseteq N,$

则称N为R的一个**理想**.

定义

设N是R的非空子集,如果

(1) $\forall a, b \in N, a - b \in N, ab \in N;$

(2) $\forall r \in R, rN \subseteq N, Nr \subseteq N,$

则称N为R的一个理想.

等价地,有

定义

设$N(\neq \emptyset) \subseteq R$,如果

(1) $\forall a, b \in N, a - b \in N;$

定义

设N是R的非空子集,如果

(1) $\forall a, b \in N, a-b \in N, ab \in N;$

(2) $\forall r \in R, rN \subseteq N, Nr \subseteq N,$

则称N为R的一个理想.

等价地,有

定义

设$N(\neq \emptyset) \subseteq R$,如果

(1) $\forall a, b \in N, a-b \in N;$

(2) $\forall r \in R, \forall n \in N, rn, nr \in N,$

则称N为R的一个理想,记为$N \lhd R$.

理想的例子

例

对任意环R,有0(零理想)$\lhd$, R(单位理想) $\lhd R$.这两个理想统称为R的平凡理想.而R的其它理想(如果存在的话),叫做R的真理想.

理想的例子

例

对任意环R,有0(零理想)$\lhd$, R(单位理想) $\lhd R$.这两个理想统称为R的平凡理想.而R的其它理想(如果存在的话),叫做R的真理想.

例

$2\mathbb{Z} \lhd \mathbb{Z}.$

理想的例子

例

对任意环R,有0(零理想)$\lhd$, R(单位理想) $\lhd R$.这两个理想统称为R的平凡理想.而R的其它理想(如果存在的话),叫做R的真理想.

例

$2\mathbb{Z} \lhd \mathbb{Z}$.

例

设R是 数 环,则$N = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid \forall a \in R \right\}$是$M_2(R)$的子环,但$N \ntriangleleft M_2(R)$.

有关理想的重要性质

定理

除环(或域)R只有平凡理想.

有关理想的重要性质

定理

除环(或域)R只有平凡理想.

定义

*只有平凡理想的环称为**单环**.*

定理

除环(或域)R只有平凡理想.

定义

*只有平凡理想的环称为**单环**.*

显然,除环和域都是单环.

有关理想的重要性质

性质

- 若N是有单位元的环R的理想,且$1_R \in N$,则$N = R$;

有关理想的重要性质

性质

- 若N是有单位元的环R的理想,且$1_R \in N$,则$N = R$;
- 若$N_1, N_2 \lhd R$,则$N_1 + N_2 \overset{def}{=} \{a + b | a \in N_1, b \in N_2\} \lhd R$,这个理想通常称为理想$N_1$与$N_2$的和理想;

有关理想的重要性质

性质

- *若N是有单位元的环R的理想,且$1_R \in N$,则$N = R$;*
- *若$N_1, N_2 \lhd R$,则$N_1 + N_2 \overset{def}{=} \{a + b | a \in N_1, b \in N_2\} \lhd R$,这个理想通常称为理想$N_1$与$N_2$的和理想;*
- *若$N_1, N_2 \lhd R$,则$N_1N_2 = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n | a_i \in N_1, b_i \in N_2\} \lhd R$,这个理想通常称为理想$N_1$与$N_2$的积理想;*

性质

- 若N是有单位元的环R的理想,且$1_R \in N$,则$N = R$;
- 若$N_1, N_2 \lhd R$,则$N_1 + N_2 \overset{def}{=} \{a + b | a \in N_1, b \in N_2\} \lhd R$,这个理想通常称为理想$N_1$与$N_2$的和理想;
- 若$N_1, N_2 \lhd R$,则$N_1 N_2 = \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n | a_i \in N_1, b_i \in N_2\} \lhd R$,这个理想通常称为理想$N_1$与$N_2$的积理想;
- 若$N_i \lhd R, i \in I$,则$\cap_{i \in I} N_i \lhd R$.

设R**为环,**$S(\neq\emptyset)\subseteq R, \Omega=\{A|A\lhd R$ **且**$S\subseteq A\}$. **则**$\cap_{A\in\Omega}A\lhd R$, **这个理想叫做由子集**S**生成的理想,记为**(S), S**叫做**(S)**的生成子集.显然,**(S)**是**R**中包含**S**的理想中最小的一个.当**$S=\{a_1,a_2,\cdots,a_n\}$**是有限集时,记**$(S)=(a_1,a_2,\cdots,a_n)(=\sum_{i=1}^{n}(m_ia_i+x_ia_iy_i+r_ia_i+a_is_i)$**,其中**$m_i\in\mathbb{Z},\forall x_i,y_i,r_i,s_i\in R)$.**特别地,**

设R为环,$S(\neq \emptyset) \subseteq R, \Omega = \{A | A \lhd R$ 且$S \subseteq A\}$. 则$\cap_{A\in\Omega} A \lhd R$, 这个理想叫做由子集$S$生成的理想,记为$(S)$, S叫做(S)的生成子集.显然,(S)是R中包含S的理想中最小的一个.当$S = \{a_1, a_2, \cdots, a_n\}$是有限集时,记$(S) = (a_1, a_2, \cdots, a_n)(= \sum\limits_{i=1}^{n}(m_i a_i + x_i a_i y_i + r_i a_i + a_i s_i))$,其中$m_i \in \mathbb{Z}, \forall x_i, y_i, r_i, s_i \in R)$.特别地,

定义

由环R中一个元素a生成的理想(a)叫做R的主理想.

当R是有单位元的交换环时,$(a) = \{ra | r \in R\}$.

非主理想的一个例子

例

已知$\mathbb{Z}[x]$是整环,$(2,x)=\{2f(x)+xg(x)|f(x),g(x)\in R[x]\}=\{a_nx^n+\cdots+a_1x+2a_0|a_i\in\mathbb{Z}\}\lhd\mathbb{Z}[x]$. 但$(2,x)$不是$\mathbb{Z}[x]$的主理想.

例

已知$\mathbb{Z}[x]$是整环,$(2,x)=\{2f(x)+xg(x)|f(x),g(x)\in R[x]\}=\{a_nx^n+\cdots+a_1x+2a_0|a_i\in\mathbb{Z}\}\lhd\mathbb{Z}[x]$. 但$(2,x)$不是$\mathbb{Z}[x]$的主理想.

事实上,若$\exists f(x)\in\mathbb{Z}[x]$ 使$(2,x)=(f(x))$, 则有$2=g(x)f(x),x=h(x)f(x)$, 于是$f(x),g(x)$都是非零常数,$x=h(x)a$,故$|a|=1$, 所以$1\in(2,x)$,这是不可能的.

§8 剩余类环、同态与理想

本节的主要内容是环的同态基本定理与对应定理.

设I是环R的理想,则对于加法来说,I是R的正规子群,于是I的陪集$a+I, b+I, c+I, \cdots$作成R的一个分类,这个分类叫做模I的**剩余类**.这个分类也相当于给出了R的元素间的一个等价关系:$a \sim b \Leftrightarrow a-n \in I$, 这个等价关系也记为$a \equiv b \pmod{I}$(或$a \equiv b(I)$).

第三章 环与域

加群、环的定义

交换律、单位元、零因子、整环

除环、域

无零因子环的特征

子环、环的同态

多项式环

理想

剩余类环、同态与理

设I是环R的理想,则对于加法来说,I是R的正规子群,于是I的陪集$a+I, b+I, c+I, \cdots$作成R的一个分类,这个分类叫做模I的**剩余类**.这个分类也相当于给出了R的元素间的一个等价关系:$a \sim b \Leftrightarrow a-n \in I$, 这个等价关系也记为$a \equiv b \pmod{I}$(或$a \equiv b(I)$).

R模I的剩余类的集合记为R/I,这是一个加法群.对$\forall a+I, b+I \in R/I$, 定义

$$(a+I)\cdot(b+I) = ab+I,$$

则这个定义是有意义的,并且$(R/I, \cdot)$作成一个半群, R/I中的乘法对加法满足左右分配律,所以,$(R/I, +, \cdot)$是一个环.

定义

设R为环,$I \lhd R$.称$(R/I,+,\cdot)$为R关于理想I的**剩余类环 (商环)**,R/I中的元素叫做模I的剩余类.

定义

设R为环,$I \lhd R$.称$(R/I,+,\cdot)$为R关于理想I的**剩余类环**(**商环**),R/I中的元素叫做模I的剩余类.

例

设$R=\mathbb{Z}, I=(6)=6\mathbb{Z}$,则$R/I=\mathbb{Z}_6$.

剩余类环的定义

定义

设R为环,$I \lhd R$.称$(R/I, +, \cdot)$为R关于理想I的*剩余类环*(*商环*),R/I中的元素叫做模I的剩余类.

例

设$R = \mathbb{Z}, I = (6) = 6\mathbb{Z}$,则$R/I = \mathbb{Z}_6$.

例

设$R = \mathbb{Z}_6[x], I = (1+x)$,则$R/I \cong \mathbb{Z}_6$.

剩余类环的定义

定义

设R为环,$I\lhd R$.称$(R/I,+,\cdot)$为R关于理想I的剩余类环(商环),R/I中的元素叫做模I的剩余类.

例

设$R=\mathbb{Z}, I=(6)=6\mathbb{Z}$,则$R/I=\mathbb{Z}_6$.

例

设$R=\mathbb{Z}_6[x], I=(1+x)$,则$R/I\cong\mathbb{Z}_6$.

例

设$R=\mathbb{Z}_6[x], I=(x)$,则$R/I\cong\mathbb{Z}_6$.

定义

设$\varphi: R_1 \to R_2$为环同态,称R_2中零元的完全原象$\varphi^{-1}(0)=\{a\in R_1|\varphi(a)=0\}$为$\varphi$的核,记为$ker\varphi$.

定义

设$\varphi : R_1 \rightarrow R_2$为环同态,称$R_2$中零元的完全原象$\varphi^{-1}(0) = \{a \in R_1 | \varphi(a) = 0\}$为$\varphi$的核,记为$ker\varphi$.

定理

设$\varphi : R \rightarrow \bar{R}$为环同态满射,$I = ker\varphi$.则

(1) $I \lhd R$;

(2) $R/I \cong \bar{R}$.

定义

设$\varphi: R_1 \to R_2$为环同态,称R_2中零元的完全原象$\varphi^{-1}(0)=\{a\in R_1|\varphi(a)=0\}$为$\varphi$的核,记为$ker\varphi$.

定理

设$\varphi: R\to \bar{R}$为环同态满射,$I=ker\varphi$.则

(1) $I \lhd R$;

(2) $R/I \cong \bar{R}$.

定理

设R是环,$I\lhd R$.则有环同态$\varphi: R\to R/I$使φ是环满同态且$ker\ \varphi = I$.称这样的φ为环的自然同态.

上面的两个定理合称为环的同态基本定理.

定理

设$\varphi : R \to \bar{R}$为是环同态映射,则

(1) 若S是R的子环,则$\varphi(S)$是$\bar{R}$的子环;

上面的两个定理合称为环的同态基本定理.

定理

设$\varphi: R \to \bar{R}$为是环同态映射,则

(1) 若S是R的子环,则$\varphi(S)$是$\bar{R}$的子环;

(2) 若I是R的理想且φ为满射,则$\varphi(I)$是$\bar{R}$的理想;

上面的两个定理合称为环的同态基本定理.

定理

设$\varphi: R \to \bar{R}$为是环同态映射,则

(1) 若S是R的子环,则$\varphi(S)$是$\bar{R}$的子环;

(2) 若I是R的理想且φ为满射,则$\varphi(I)$是$\bar{R}$的理想;

(3) 若$\bar{S}$是$\bar{R}$的子环,则$\varphi^{-1}(\bar{S})$是R的子环;

上面的两个定理合称为环的同态基本定理.

定理

设$\varphi: R \to \bar{R}$为是环同态映射,则

(1) 若S是R的子环,则$\varphi(S)$是$\bar{R}$的子环;

(2) 若I是R的理想且φ为满射,则$\varphi(I)$是$\bar{R}$的理想;

(3) 若$\bar{S}$是$\bar{R}$的子环,则$\varphi^{-1}(\bar{S})$是R的子环;

(4) 若$\bar{S}$是$\bar{R}$的理想,则$\varphi^{-1}(\bar{S})$是R的理想.

作业

p. 113 2,5 p. 116 3

§9 最大理想

本节主要包括以下内容:

1 最大理想的概念和判断最大理想的方法;

2 通过最大理想获得域的方法;

3 素理想的概念和基本性质.

§9 最大理想

本节主要包括以下内容:

1 最大理想的概念和判断最大理想的方法;

2 通过最大理想获得域的方法;

3 素理想的概念和基本性质.

注

本教材中的“最大理想”在很多书中被称为“极大理想”.为了与教材一致,我们仍用“最大理想”这个名词.

§9 最大理想

本节主要包括以下内容:

1 最大理想的概念和判断最大理想的方法;
2 通过最大理想获得域的方法;
3 素理想的概念和基本性质.

注

本教材中的"最大理想"在很多书中被称为"极大理想".为了与教材一致,我们仍用"最大理想"这个名词.

事实上,本教材中的"最大" 是"极大"的意思,就是没有谁比它大(而"最大"应该是比谁都大的意思,这是本教材的一个缺陷).

最大理想的概念

整数12有因数1,2,3,4,6,4和6是12的“最大”(极大)因数.一般地,a是n的“最大”因数当且仅当n/a是素数.本节主要是将这种思想应用到环上来.

整数12有因数1,2,3,4,6,4和6是12的“最大”(极大)因数.一般地,a是n的“最大” 因数当且仅当n/a是素数.本节主要是将这种思想应用到环上来.

定义

设I是环R的一个理想,且$I \neq R$,如果R除了R和I外,没有能包含I的其他理想,则称I是R的一个**最大理想**.

验证R的理想I是最大理想一般有两步:

整数12有因数1,2,3,4,6,4和6是12的“最大”(极大)因数.一般地,a是n的“最大”因数当且仅当n/a是素数.本节主要是将这种思想应用到环上来.

定义

*设I是环R的一个理想,且$I \neq R$,如果R除了R和I外,没有能包含I的其他理想,则称I是R的一个**最大理想**.*

验证R的理想I是最大理想一般有两步:

(1) $I \neq R$(当$1_R \in R$时,通常证明$1_R \notin I$);

整数12有因数1,2,3,4,6,4和6是12的“最大”(极大)因数.一般地,a是n的“最大”因数当且仅当n/a是素数.本节主要是将这种思想应用到环上来.

定义

设I是环R的一个理想,且$I \neq R$,如果R除了R和I外,没有能包含I的其他理想,则称I是R的一个最大理想.

验证R的理想I是最大理想一般有两步:

(1) $I \neq R$(当$1_R \in R$时,通常证明$1_R \notin I$);

(2) 若$(I \subsetneqq) J \lhd R$,则$J = R$.

几个例子

例

1 设$R=\mathbb{Z}$,p是素数,则由p生成的理想$I=(p)$是R的最大理想.

几个例子

例

1. 设$R = \mathbb{Z}$, p是素数,则由p生成的理想$I = (p)$是R的最大理想.
2. 设$R = \mathbb{Q}$, p是素数,则由p生成的理想$I = (p)$不是R的最大理想.

几个例子

例

1. 设$R=\mathbb{Z}$, p是素数,则由p生成的理想$I=(p)$是R的最大理想.
2. 设$R=\mathbb{Q}$, p是素数,则由p生成的理想$I=(p)$不是R的最大理想.
3. 设R是非零环,则R为单环当且仅当零理想$\{0\}$是最大理想.

几个例子

例

1 设$R = \mathbb{Z}$, p是素数,则由p生成的理想$I = (p)$是R的最大理想.

2 设$R = \mathbb{Q}$, p是素数,则由p生成的理想$I = (p)$不是R的最大理想.

3 设R是非零环,则R为单环当且仅当零理想$\{0\}$是最大理想.

4 设R是偶数环,$I = 4\mathbb{Z} \lhd R$,则I是R的最大理想.

引理

设$I(\neq R) \lhd R$,则剩余类环R/I为单环$\Leftrightarrow$ I是R的最大理想.

引理

设$I(\neq R) \lhd R$,则剩余类环R/I为单环$\Leftrightarrow$ I是R的最大理想.

引理

设R是有单位元$1_R(\neq 0)$的交换环,则R为域$\Leftrightarrow$ R为单环.

主要定理

加群、环的定义
交换律、单位元、零因子、整环
除环、域
无零因子环的特征
子环、环的同态
多项式环
理想
剩余类环、同态与理

引理

设$I(\neq R) \lhd R$,则剩余类环R/I为单环$\Leftrightarrow$ I是R的最大理想.

引理

设R是有单位元$1_R(\neq 0)$的交换环,则R为域$\Leftrightarrow$ R为单环.

定理

设R是有单位元$1_R(\neq 0)$的交换环,$I \lhd R$,则R/I为域$\Leftrightarrow$ I是R的一个极大理想.

素理想

定义

设$I \lhd R$,若$\forall a,b \in R$,由$ab \in R$必有$a \in R$或$b \in R$,则称I为R的一个**素理想**.

素理想

定义

设$I \lhd R$,若$\forall a,b \in R$,由$ab \in R$必有$a \in R$或$b \in R$,则称I为R的一个素理想.

例

设p是素数,则(p)与$\{0\}$都是$\mathbb{Z}$的素理想.

素理想

定义

设$I \lhd R$,若$\forall a, b \in R$,由$ab \in R$必有$a \in R$或$b \in R$,则称I为R的一个**素理想**.

例

设p是素数,则(p)与$\{0\}$都是$\mathbb{Z}$的素理想.

性质

设R是环,则

(1) R是素理想;

素理想

定义

设$I \lhd R$,若$\forall a,b \in R$,由$ab \in R$必有$a \in R$或$b \in R$,则称I为R的一个素理想.

例

设p是素数,则(p)与$\{0\}$都是$\mathbb{Z}$的素理想.

性质

设R是环,则

(1) R是素理想;

(2) 零理想是素理想$\Leftrightarrow$ R是无零因子环.

§10 商域

本节主要介绍由无零因子交换环来构造商域的方法.

主要定理

定理

设R是无零因子交换环,则存在一个域Q,使R成为Q的一个子环,且$Q = \left\{ \frac{a}{b} \mid a, b(\neq 0) \in R \right\}$.

主要定理

定理

设R是无零因子交换环,则存在一个域Q,使R成为Q的一个子环,且$Q = \left\{\frac{a}{b} \mid a, b(\neq 0) \in R\right\}$.

定义

设R是环而Q是包含R的一个域,如果$Q = \left\{\left[\frac{a}{b}\right] \mid a, b(\neq 0) \in R\right\}$,则称$Q$为$R$的**商域**.

辅助定理

定理

设$R \neq 0$,且F为包含R的域,则F必包含R的商域.

辅助定理

定理

设$R \neq 0$,且F为包含R的域,则F必包含R的商域.

定理

若环R与环$\bar{R}$同构,则它们各自的商域也同构.

辅助定理

定理

设$R \neq 0$,且F为包含R的域,则F必包含R的商域.

定理

若环R与环$\bar{R}$同构,则它们各自的商域也同构.

注

这两个定理是说,环R可能会有两个“不同”的商域,但在同构的意义下,每个环最多只有一个商域.

作业

p. 119 1　p. 124 1,2