第十章 环与理想
2015年10月26日

信息安全数学基础

陈恭亮　教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

10.1 环与理想

本章考虑具有两种运算(加法"+" 及乘法"·")的集合, 如同整数集合$\mathbf{Z}$. 该集合对于加法构成交换群, 对于乘法构成代数系.

对集合运算的思考

1. 一个有两种运算的集合应该具有什么样的性质? 举例说明.
2. 从有效性的角度而言, 一个有运算的集合应该具有什么样的性质? 举例说明.
3. 从安全性的角度而言， 一个有运算的集合应该具有什么样的性质? 举例说明.
4. 同构的环具有相同的计算复杂性吗? 举例说明.
5. 如何借助同构的环来提高运算效率. 编程实现$\mathbf{F}_p$ 中的乘法运算, 并举例说明.
6. 如何借助同构的环来提高运算效率. 研究和实现加密算法AES 中的乘法运算, 并举例说明.
7. 如何得到同构的环.

1. 环的定义和基本性质.
2. 子环及其判断.
3. 理想和商环.
4. 素理想和整环
5. 极大理想和域
6. 同态和同构.
7. 同态分解定理.

10.1.1 基本定义

定义10.1.1 设R 是具有两种结合法(通常表示为加法(+)和乘法)的非空集合. 如果如下条件成立:

(i) R 对于加法构成一个交换群.

(ii) (结合律) 对任意的$a,\ b,\ c \in R$, 有$(ab)c = a(bc)$.

(iii) (分配律) 对任意的$a,\ b,\ c \in R$, 有

$$(a+b)c = ac + bc \quad \text{和} \quad a(b+c) = ab + ac.$$

则R 叫做**环**.

如果还满足 (iv) 对任意的$a, b \in R$, 有$ab = ba$,

则R 叫做**交换环**.

如果R 中有一个元素$e = 1_R$ 使得 (v) 对任意的$a \in R$, 有$a1_R = 1_R a = a$,

则R 叫做**有单位元环**.

下面考虑环R 中元素的运算性质.

定理10.1.1 设R 是一个环. 则

(i) 对任意$a \in R$, 有$0a = a0 = 0$.

(ii) 对任意$a, b \in R$, 有$(-a)b = a(-b) = -ab$.

(iii) 对任意$a, b \in R$, 有$(-a)(-b) = ab$.

(iv) 对任意$n \in \mathbf{Z}$, 任意$a, b \in R$, 有$(na)b = a(nb) = nab$.

(v) 对任意$a_i, b_j \in R$, 有

$$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j.$$

证 (i) 因为$0a = (0+0)a = 0a + 0a$, 所以$0a = 0$. 同样, $a0 = 0$.

(ii) 因为$(-a)b + ab = ((-a) + a)b = 0a = 0$,

$a(-b) + ab = a((-b) + b) = a0 = 0$,

所以$(-a)b = a(-b) = -ab$.

(iii), (iv) 和(v) 可有(i) 和(ii) 得到.

定理10.1.2 设R 是有单位元的环. 设n 是正整数, $a,\ b,\ a_1,\ \ldots,\ a_r \in R$.

(i) 如果$ab = ba$, 则 $(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k}$.

(ii) 如果$a_i a_j = a_j a_i,\ 1 \le i, j \le r$, 则

$$(a_1 + \cdots + a_r)^n = \sum_{i_1+\cdots+i_r=n} \frac{n!}{i_1! \cdots i_r!} a_1^{i_1} \cdots a_r^{i_r}.$$

证 (i) 对n 用数学归纳法. 当$n = 1$时, 结论显然.

假设对$n = s$时成立, 即有 $(a+b)^s = \sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k}$.

则当$n = s+1$时有(注意到$ab = ba$)

$$\begin{aligned}
(a+b)^{s+1} &= (a+b)^s (a+b) = \left(\sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k} \right) (a+b) \\
&= \sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k} a + \sum_{k=0}^{s} \frac{s!}{k!(s-k)!} a^k b^{s-k+1} \\
&= \sum_{k=0}^{s-1} \left(\frac{s!}{k!(s-k)!} a^{k+1} b^{s-k} + \frac{s!}{(k+1)!(s-k)!} a^{k+1} b^{s-k} \right) + a^{s+1} + b^{s+1} \\
&= \sum_{k=0}^{s+1} \frac{(s+1)!}{k!(s+1-k)!} a^k b^{s+1-k}
\end{aligned}$$

即对$n = s+1$结论也成立, 故定理成立.

(ii) 对r用归纳法. 当$r=2$时即为(i)的结论, 显然成立.

假设$r \le m$时结论成立.

当$r=m+1$时,由(i) 及归纳假设可得

$$(a_1+\cdots+a_m+a_{m+1})^n=((a_1+\cdots+a_m)+a_{m+1})^n$$

$$=\sum_{i_{m+1}=0}^{n}\frac{n!}{i_{m+1}!(n-i_{m+1})!}(a_1+\cdots+a_m)^{n-i_{m+1}}a_{m+1}^{i_{m+1}}$$

$$=\sum_{i_{m+1}=0}^{n}\frac{n!}{i_{m+1}!(n-i_{m+1})!}\sum_{i_1+\cdots+i_m=n-i_{m+1}}\frac{(n-i_{m+1})!}{i_1!\cdots i_m!}a_1^{i_1}\cdots a_m^{i_m}a_{m+1}^{i_{m+1}}$$

$$=\sum_{i_1+\cdots+i_m+i_{m+1}=n}\frac{n!}{i_1!\cdots i_m!\cdot i_{m+1}!}a_1^{i_1}\cdots a_m^{i_m}a_{m+1}^{i_{m+1}}$$

即得当$r=m+1$时结论也成立.

证毕

例10.1.1 整数集**Z** 是有单位元的交换环.

1) **Z** 对于加法$a+b$ 构成一个交换加群. 零元为0, a 的负元为$-a$.

2) **Z** 对于乘法$a \cdot b$, 满足结合律和分配律, 还满足交换律, 有单位元1.

因此, **Z** 是有单位元的交换环.

例10.1.2 多项式集$\mathbf{R}[X]$ 是有单位元的交换环.

设$f(x)=a_nx^n+\cdots+a_1x+a_0,\ g(x)=b_nx^n+\cdots+b_1x+b_0\in\mathbf{R}[X]$.

1) 在$\mathbf{R}[X]$ 上定义加法:

$$(f+g)(x)=(a_n+b_n)x^n+\cdots+(a_1+b_1)x+(a_0+b_0),$$

则$\mathbf{R}[X]$ 对于该加法构成一个交换加群.

零元为0, $f(x)$ 的负元为$(-f)(x)=(-a_n)x^n+\cdots+(-a_1)x+(-a_0)$.

设$f(x)=a_nx^n+\cdots+a_1x+a_0,\ a_n\neq 0,\quad g(x)=b_mx^m+\cdots+b_1x+b_0,\ b_m\neq 0$,

2) 在$\mathbf{R}[X]$ 上定义乘法:

$$(f\cdot g)(x)=c_{n+m}x^{n+m}+c_{n+m-1}x^{n+m-1}+\cdots+c_1x+c_0,$$

其中$c_k=\sum\limits_{i+j=k}a_ib_j,\ 0\leq k\leq n+m$, 即

$$c_{n+m}=a_nb_m,\ c_{n+m-1}=a_nb_{m-1}+a_{n-1}b_m,\ldots,\ c_0=a_0b_0.$$

$\mathbf{R}[X]$ 对于该乘法, 满足结合律和分配律, 还满足交换律, 有单位元1.

因此, $\mathbf{R}[X]$ 是有单位元的交换环.

例10.1.3 $\mathbf{Z}/6\mathbf{Z} = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}\}$ 是一个有单位元的交换环.

1) $\mathbf{Z}/6\mathbf{Z}$ 对于加法$a + b$ 构成一个交换加群. 零元为0, a 的负元为$6 - a$.

2) $\mathbf{Z}/6\mathbf{Z}$ 对于乘法$a \cdot b$, 满足结合律和交换律, 有单位元$\overline{1}$.

$\mathbf{Z}/6\mathbf{Z}$ 还有分配律, 是一个有单位元的交换环. 但有两个非零元的乘积为零, 如

$$\overline{2} \cdot \overline{3} = 0.$$

10.1.2 零因子环

我们给出如下定义.

定义10.1.2 设R 是环. R 中非零元a 称为**左零因子**(对应地. **右零因子**) , 如果存在非零元$b \in R$ (对应地. $c \in R$) 使得$ab = 0$ (对应地. $ca = 0$), a 称为**零因子**, 如果它同时为左零因子和右零因子. 这时, 称R 为有零因子环.

$\overline{2}$ 和$\overline{3}$ 是环$\mathbf{Z}/6\mathbf{Z}$ 中的零因子.

定义10.1.3 设R 是有单位元1_R 的环. R 中元a 称为**左逆元**(对应地. **右逆元**) , 如果存在元$b \in R$ (对应地. $c \in R$) 使得$ab = 1_R$ (对应地. $ca = 1_R$). 这时, b (对应地. c) 叫做a 的**右逆**(对应地. **左逆**). a 称为**逆元**, 如果它同时为左逆元和右逆元.

$\overline{1}$ 和$\overline{5}$ 是环$\mathbf{Z}/6\mathbf{Z}$ 中的逆元.

例10.1.4 $M_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z} \right\}$ 对于矩阵的加法和乘法是一个有单位元和零因子的非交换环.

1) $M_2(\mathbf{Z})$ 对于矩阵加法

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}$$

构成一个交换加群.

有结合律, 零元为 $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 的负元为 $-\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$.

2) $M_2(\mathbf{Z})$ 对于矩阵乘法

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$$

满足结合律和分配律, 有单位元 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

3) 有零因子和非交换

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0\cdot 0+0\cdot 1 & 0\cdot 0+0\cdot 0 \\ 1\cdot 0+0\cdot 1 & 1\cdot 0+0\cdot 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}.$$

因此, $M_2(\mathbf{Z})$ 是一个有单位元和零因子的非交换环.

10.1.3 整环及域

我们希望一些环具有整数环Z 的一些性质, 即整环. 后面会对整环作进一步的讨论.

定义10.1.4 设R 是一个交换环. 称R 为**整环**, 如果R 中有单位元, 但没有零因子.

整数环Z 是一个整环.

性质10.1.1 设R 是整环. 则R 中有消去律成立. 即当$c \neq 0$, $c \cdot a = c \cdot b$ 时, 有$a = b$. **证** 当$c \cdot a = c \cdot b$ 时, 有

$$c(a - b) = 0.$$

因为R 是整环, 无零因子, 所以$a - b = 0$. 结论成立. 证毕

例10.1.5 多项式环$\mathbf{Z}[X]$是一个整环.

易知$\mathbf{Z}[X]$是一个有单位元的交换环(例??). 现在只需说明$\mathbf{Z}[X]$中无零因子.

设$f(x)=a_nx^n+\cdots+a_1x+a_0,\ a_n\neq 0,\quad g(x)=b_mx^m+\cdots+b_1x+b_0,\ b_m\neq 0,$

假设

$$(f\cdot g)(x)=c_{n+m}x^{n+m}+c_{n+m-1}x^{n+m-1}+\cdots+c_1x+c_0=0,$$

其中$c_k=\sum\limits_{i+j=k}a_ib_j,\ 0\leq k\leq n+m$, 即

$$c_{n+m}=a_nb_m,\ c_{n+m-1}=a_nb_{m-1}+a_{n-1}b_m,\ldots,\ c_0=a_0b_0.$$

则$c_{n+m}=a_nb_m=0$. 因为$\mathbf{Z}$是整环, 所以有$a_n=0$或$b_m=0$, 矛盾.

进一步, 我们希望一些环具有有理数集$\mathbf{Q}$ 的一些性质(如非零元集是交换乘群), 即域. 后面会对域作进一步的讨论.

定义10.1.5 们称交换环K 为一个域, 如果K 中有单位元, 且每个非零元都是可逆元. 即K 对于加法构成一个交换群, $K^* = K \setminus \{0\}$ 对于乘法构成一个交换群.

例如, 有理数域$\mathbf{Q}$, 实数域$\mathbf{R}$, 复数域$\mathbf{C}$, 二元域$\mathbf{F}_2$, 有限数域$\mathbf{F}_p$.

10.1.4 交换环上的整除

最后, 我们希望整数环的整除性也可以应用到环上.

定义10.1.6 设R 是一个交换环, $a,\ b \in R,\ b \neq 0$. 如果一个元素$c \in R$ 使得$a = c\,b$, 就称b **整除** a 或者a 被b 整除, 记作$b \mid a$. 这时, 把b叫做a 的**因子**, 把a 叫做b 的**倍元**.

如果$b,\ c$ 都不是单位元, 就b 称为a 的**真因子**.

R 中的元素p 称为**不可约**元或**素元**, 如果p 不是单位元, 且没有真因子. 也就是说, 如果有元素$b,\ c \in R$ 使得$p = c\,b$, 则b 或c 一定是单位元.

两个元素$a,\ b \in R$ 称为**相伴的**, 如果存在可逆元$u \in R$ 使得$a = u\,b$. 相伴元$a,\ b$ 具有相同的不可约性.

整数环$\mathbf{Z}$ 中的不可约元就是素数.

多项式环$\mathbf{Q}$ 中的不可约元就是不可约多项式.

环$\mathbf{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,\ b \in \mathbf{Z}\}$ 的元素$2,\ 3,\ \sqrt{-5},\ 1+\sqrt{-5},\ 6+\sqrt{-5}$ 都是不可约元, 但$5,\ 41,\ 7+\sqrt{-5}$ 都是可约元. 事实上,

$$5 = \sqrt{-5}\cdot(-\sqrt{-5}),\ 41 = (6+\sqrt{-5})(6-\sqrt{-5}),\ 7+\sqrt{-5} = (1+\sqrt{-5})(2-\sqrt{-5}).$$

例10.1.6 高斯环$\mathbf{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a,\ b \in \mathbf{Z}\}$ 是一个整环.

1) $\mathbf{Z}[\sqrt{-1}]$ 对于加法

$$(a + b\sqrt{-1}) \oplus (c + d\sqrt{-1}) = (a + c) + (b + d)\sqrt{-1}$$

构成一个交换加群.

零元为0, $a + b\sqrt{-1}$ 的负元为$-(a + b\sqrt{-1}) = (-a) + (-b)\sqrt{-1}$.

2) $\mathbf{Z}[\sqrt{-1}]$ 对于乘法

$$(a + b\sqrt{-1}) \otimes (c + d\sqrt{-1}) = (ac - bd) + (ad + bc)\sqrt{-1}$$

满足结合律和分配律, 还满足交换律, 有单位元1.

3) $2,\ 2 + \sqrt{-1}$ 是不可约元, $3 = (2 + \sqrt{-1})(2 - \sqrt{-1})$ 是可约元.

4) 无零因子. 事实上, 若$a+b\sqrt{-1}\neq 0$ 为零因子, 则存在非零元$c+d\sqrt{-1}$ 使得

$$(a+b\sqrt{-1})\otimes(c+d\sqrt{-1})=(ac-bd)+(ad+bc)\sqrt{-1}=0$$

从而$ac-bd=0,\ ad+bc=0$, 进而$ac^2=c(bd)=d(-ad),\ a(c^2+d^2)=0$. 故$a=0,\ b=0$. 矛盾.

因此, $\mathbf{Z}[\sqrt{-1}]$ 是一个整环.

5) 可逆元$a+b\sqrt{-1}$ 为$1,\ -1,\ \sqrt{-1},\ -\sqrt{-1}$.

进一步, 可在$\mathbf{Z}[\sqrt{-1}]$ 中讨论$\alpha=a+b\sqrt{-1}$ (其共轭元$\overline{\alpha}=a-b\sqrt{-1}$) 的模:

$$|\alpha|=(\alpha\cdot\overline{\alpha})^{1/2}=\sqrt{a^2+b^2}.$$

则有三角不等式: $|\alpha+\beta|\leq|\alpha|+|\beta|$ 以及$\alpha=0$ 的充要条件是$|\alpha|=0$.

10.2 同态

本节讨论两个环之间的关系.

定义12.2.1 设R, R' 是两个环. 称映射$f : R \longrightarrow R'$ 为**环同态**, 如果f 满足如下条件:

(i) 对任意的a, $b \in R$, 有$f(a+b) = f(a) + f(b)$;

(ii) 对任意的a, $b \in R$, 有$f(ab) = f(a)f(b)$.

如果f 是一对一的, 则称f 为**单同态**; 如果f 是满的, 则称f 为**满同态**; 如果f 是一一对应的, 则称f 为**同构**.

定义12.2.1 设R, R' 是两个环. 我们称R 与R' **同构**, 如果存在一个R到R' 的同构.

10.3 特征及素域

本节给出最小的域的表述.

先给出特征的表述.

定义10.3.1 设R 是一个环. 如果存在一个最小正整数p 使得对任意$a \in R$, 都有

$$p\,a = \underbrace{a + \cdots + a}_{p\text{个}\ a} = 0,$$

则称环R 的**特征**为p. 如果不存在这样的正整数, 则称环R 的特征为0.

定理10.3.1 如果域K 的特征不为零, 则其特征必为素数.

证 设域K 的特征为p. 如果p 不是素数, 则存在整数$1 < p_1,\ p_2 < p$, 使得$p = p_1 \cdot p_2$. 从而,

$$(p_1 1_{\mathbf{K}})\,(p_2 1_{\mathbf{K}}) = (p_1 \cdot p_2) 1_{\mathbf{K}} = 0.$$

因为域$\mathbf{K}$ 无零因子, 所以$p_1\,1_{\mathbf{K}} = 0$ 或$p_2\,1_{\mathbf{K}} = 0$. 这与特征p 的最小性矛盾. 证毕

定理10.3.2 设R是有单位元的交换环. 如果环R的特征是p, 则

(i) 对任意$a,\ b \in R$, 有 $(a+b)^p = a^p + b^p$.

(ii) 环R到自身的映射$\sigma:\ a \longmapsto a^p$是自同态.

证 (i) 根据定理10.1.2, 我们有

$$(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k b^{p-k}.$$

对于$1 \le k \le p-1$, 有$(p,\ k!(p-k)!) = 1$, 从而$p \mid p \cdot \dfrac{(p-1)!}{k!(p-k)!}$. 这样, 由$R$的特征$p$为素数, 得到$\dfrac{p!}{k!(p-k)!} a^k b^{p-k} = 0$. 因此, (i) 成立.

(ii) 根据(i), 有

$$\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a)\sigma(b),$$

$$\sigma(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = \sigma(a)\,\sigma(b).$$

因此, $\sigma:\ a \longmapsto a^p$是自同态. 证毕

定理10.3.3 设p 是一个素数. 设$f(x) = a_n x^n + \cdots + a_1 x + a_0$ 是整系数多项式. 则

$$f(x)^p \equiv f(x^p) \pmod{p}.$$

证 在域$\mathbf{F}_p$ 上的多项式环$\mathbf{F}_p[x]$ 上, 应用定理10.3.2 及Fermat 小定理(定理2.4.2), 有

$$\begin{aligned} f(x)^p &= (a_n)^p (x^n)^p + \cdots + (a_1)^p (x)^p + (a_0)^p \\ &\equiv a_n (x^p)^n + \cdots + a_1 (x^p) + a_0 \\ &= f(x^p) \pmod{p}. \end{aligned}$$

证毕

定义10.3.2 设R_1 ($\mathbf{K}_1$) 是环R (域$\mathbf{K}$) 的非空子集. 如果对于环R (域$\mathbf{K}$) 的运算, R_1 ($\mathbf{K}_1$) 也构成一个环(域), 则R_1 ($\mathbf{K}_1$) 叫做R 的**子环** ($\mathbf{K}$ 的**子域**) .

定义10.3.3 一个域叫做**素域**, 如果它不含真子域.

例10.3.1 有理数域$\mathbf{Q}$ 是素域. $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ 是素域.

定理10.3.4 设$\mathbf{F}$ 是一个域. 如果$\mathbf{F}$ 的特征为0, 则$\mathbf{F}$ 有一个与$\mathbf{Q}$ 同构的素域. 如果$\mathbf{F}$ 的特征为p, 则$\mathbf{F}$ 有一个与$\mathbf{F}_p$ 同构的素域.
考虑由单位元$1_{\mathbf{K}}$ 所生成的域.

10.4 分式域

从整数集Z 构造出分式域有理数集Q 是经典和重要的方法. 我们运用该方法从整环构造出对应的分式域.

域的构造方式之一

定理10.4.1 设A 是一个整环. 令$E = A \times A^*$. 在E 上定义关系R:

$$(a,b)R(c,d) \text{ 如果 } ad = bc.$$

则R 是E 上的等价关系, 即有

(i) 自反性: 对任意$(a,b) \in E$, 有$(a,b)R(a,b)$.

(ii) 对称性: 如果$(a,b)R(c,d)$, 则$(c,d)R(a,b)$.

(iii) 传递性: 如果$(a,b)R(c,d)$ 和$(c,d)R(e,f)$, 则$(a,b)R(e,f)$.

证 (i) 对任意$(a,b) \in E$, 有$ab = ba$,所以$(a,b)R(a,b)$.

(ii) 设$(a,b)R(c,d)$, 由定义, 有$ad = bc$, 进而由交换性, 有$cb = da$. 因此, $(c,d)R(a,b)$.

(iii) 设$(a,b)R(c,d)$, $(c,d)R(e,f)$, 由定义, 有$ad = bc$, $cf = de$, 进而

$$adf = (bc)f = b(de) \quad \text{及} \quad d(af - be) = 0.$$

因为d 是整环A 中的非零元, 所以$af = be$. 因此, $(a,b)R(e,f)$. 证毕

设$(a,b)\in E$, 记$\frac{a}{b}=C_{(a,b)}=\{(c,d)\mid \in E,(c,d)R(a,b)\}$ 为(a,b) 的等价类.
易知,

$$\frac{0}{1}=C_{(0,1)}=\{(0,d)\mid \in E,(0,d)R(0,1)\},$$

$$\frac{1}{1}=C_{(1,1)}=\{(d,d)\mid \in E,(d,d)R(1,1)\},$$

以及对任意$d\in A^*$, 有 $\frac{ad}{bd}=C_{(ad,bd)}=C_{(a,b)}=\frac{a}{b}$.
现在以$\frac{a}{b}$ 为元素构造新的集合

$$E/R=\{\frac{a}{b}\mid (a,b)\in E.\}$$

定理10.4.2 设A 是整环, $E=A\times A^*$. 假设E 上有关系R: $(a,b)R(c,d)$ 如果$ad=bc$. 再设商集E/R 是由(a,b) 的等价类组成的集合.
则对于E/R 上定义加法和乘法如下:

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

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

E/R 构成一个域.

证 首先证明E/R是一个交换加群.

1) E/R结合律. 对任意$\frac{a}{b},\ \frac{c}{d},\ \frac{e}{f} \in E/R$, 有

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{(ad+bc)f+(bd)e}{(bd)f}=\frac{a(df)+b(cf+de)}{b(df)}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)$$

2) E/R有零元. $\frac{0}{1}$.

$$\frac{a}{b}+\frac{0}{1}=\frac{a\cdot 1+b\cdot 0}{b\cdot 1}=\frac{a}{b},\quad \frac{0}{1}+\frac{a}{b}=\frac{0\cdot b+1\cdot a}{1\cdot b}=\frac{a}{b}.$$

3) $\frac{a}{b} \in E/R$的负元为$-\frac{a}{b}=\frac{-a}{b}$.

$$\frac{a}{b}+\frac{-a}{b}=\frac{a\cdot b+b\cdot(-a)}{b\cdot b}=\frac{0}{1},\quad \frac{-a}{b}+\frac{a}{b}=\frac{(-a)\cdot b+b\cdot a}{b\cdot b}=\frac{0}{1}.$$

4) E/R交换律. 对任意$\frac{a}{b},\ \frac{c}{d} \in E/R$, 有

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{cb+da}{db}=\frac{c}{d}+\frac{a}{b}.$$

其次证明$(E/R)^* = (E/R) \setminus \{\frac{0}{1}\}$ 是一个交换乘群.

5) $(E/R)^*$ 结合律. 对任意$\frac{a}{b},\ \frac{c}{d},\ \frac{e}{f} \in (E/R)^*$, 有

$$\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f} = \frac{ac}{bd}\cdot\frac{e}{f} = \frac{(ac)e}{(bd)f} = \frac{a(ce)}{b(df)} = \frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right).$$

6) $(E/R)^*$ 有单位元. $\frac{1}{1}$.

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

7) $\frac{a}{b} \in (E/R)^*$ 的逆元为$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

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

8) $(E/R)^*$ 交换律. 对任意$\frac{a}{b},\ \frac{c}{d} \in (E/R)^*$, 有

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

因此, E/R 构成一个域. 证毕

定理10.4.2 中的域E/R 叫做整环A 的**分式域**.

bf 例10.4.1 取$A = \mathbf{Z}$, 则$\mathbf{Z}$ 是一个整环, 从而有分式域, 叫做$\mathbf{Z}$ 的**有理数域** , 记为$\mathbf{Q}$.

加法和乘法运算为:

$$\frac{a}{b}+\frac{c}{d}=\frac{a\,d+b\,c}{b\,d},\quad \frac{a}{b}\cdot\frac{c}{d}=\frac{a\,c}{b\,d}.$$

$$\frac{1}{3}+\frac{2}{5}=\frac{1\cdot 5+3\cdot 2}{3\cdot 5}=\frac{11}{15},\quad \frac{1}{3}\cdot\frac{2}{5}=\frac{1\cdot 2}{3\cdot 5}=\frac{2}{15}.$$

例10.4.2 取$A = \mathbf{Z}/p\mathbf{Z}$, 其中$p$ 为素数. 则A 是一个整环, 从而有分式域, 叫做$\mathbf{Z}/p\mathbf{Z}$ 的 $p-$ **元域**, 记为$\mathbf{F}_p$ 或$GF(p)$.

实际上, 我们有$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. 事实上, 对于$\frac{a}{b} \in \mathbf{F}_p$, 有$b \notin p\mathbf{Z}$, 从而$p \nmid b$. 根据广义欧几里得除法, 存在整数$s,\ t$ 使得$s \cdot b + t \cdot p = 1$, $s \cdot b \equiv 1 \pmod{p}$. 因此,

$$\frac{a}{b} = \frac{s \cdot a}{s \cdot b} = s \cdot a \in \mathbf{Z}/p\mathbf{Z}.$$

$p = 7.\ a = 4,\ b = 5.\ \ 3 \cdot 5 + (-2) \cdot 7 = 1$

$$\frac{4}{5} = \frac{3 \cdot 4}{3 \cdot 5} = 3 \cdot 4 = 5 \in \mathbf{Z}/7\mathbf{Z}.$$

例10.4.3 设K 是一个域. 则$A = \mathbf{K}[x]$ 是一个整环, 从而有分式域, 叫做$\mathbf{K}[x]$ 的**多项式分式域**, 记为$\mathbf{K}(x)$. 即

$$\mathbf{K}(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x),\ g(x) \in \mathbf{K}[x],\ g(x) \neq 0 \right\}.$$

加法和乘法运算为:

$$\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)\, g_2(x) + g_1(x)\, f_2(x)}{g_1(x)\, g_2(x)}, \quad \frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)\, f_2(x)}{g_1(x)\, g_2(x)}.$$

10.5 理想和商环

10.5.1 理想

设R 是一个环, I 是R 的子环. 则I 是R 的正规子群, 从而有商群$R/I = \{a + I \mid a \in R\}$. 人们自然希望$R/I$ 构成一个环. 为此, 要对子环I 作进一步的要求, 即要求I 为理想.

定义10.5.1 设R 是一个环, I 是R 的子环. I 称为R 的**左理想**, 如果对任意的$r \in R$ 和对任意的$a \in I$, 都有$r\,a \in I$. I 称为R 的**右理想**, 如果对任意的$r \in R$ 和对任意的$a \in I$, 都有$a\,r \in I$. I 称为R 的**理想**, 如果R 同时为左理想和右理想.

例10.5.1 $\{0\}$ 和R 都是R 的理想, 叫做R 的**平凡理想**.

定理10.5.1 环R的非空子集I是左(对应地. 右)理想的充要条件是:

(i) 对任意的$a, b \in I$, 都有$a - b \in I$.

(ii) 对任意的$r \in R$和对任意的$a \in I$, 都有$ra \in I$. (对应地. $ar \in I$.)

证 必要性是显然的. 我们证明充分性.

由(i) 知, I是R的子群.

再由(ii) 立即知道I对乘法封闭, 且作为环R的子集满足环的条件, 因而I是子环. 同时, I也满足理想的条件, 故I是R的理想. 证毕

我们考虑多个理想的交集.

定理10.5.2 设$\{A_j\}_{j\in J}$ 是环R 中的一族(左)理想. 则$\bigcap_{j\in J} A_j$ 也是一个(左)理想.

证 (i) 对任意的$a,\ b \in \bigcap_{j\in J} A_j$, 有$a,\ b \in A_j,\ j \in J$. 因为$A_j$ 是R 的理想, 根据定理10.5.1, 我们有$a-b \in A_j,\ j \in J$. 进而, $a-b \in \bigcap_{j\in J} A_j$.

(ii) 对任意的$r \in R$ 和对任意的$a \in \bigcap_{j\in J} A_j$, 有$a \in A_j,\ j \in J$. 因为$A_j$ 是R 的理想, 根据定理10.5.1, 我们有$r\,a \in A_j,\ j \in J$. 进而, $r\,a \in \bigcap_{j\in J} A_j$.

根据定理10.5.1, $\bigcap_{j\in J} A_j$ 是R 的一个理想. 证毕

根据定理10.5.2, 人们可给出一个非空子集X 生成一个理想的表述, 即包含X 的最小理想.

定义10.5.2 设X 是环R 的一个子集. 设$\{A_j\}_{j\in J}$ 是环R 中包含X 的所有(左)理想. 则$\bigcap\limits_{j\in J} A_j$ 称为由X**生成的(左)理想**. 记为(X).

X 中的元素叫做理想(X) 的**生成元**. 如果$X = \{a_1, \ldots, a_n\}$, 则理想(X) 记为$(a_1, \ldots, a_n)$, 称为**有限生成的**. 由一个元素生成的理想(a) 叫做**主理想**.

下面给出$< X >$中元素的显示表示.

定理10.5.2 设R是交换环, $a \in R,\ X \subset R$. 则

(i) 主理想(a)为

$$(a) = \{r\,a + a\,r' + n\,a + \sum_{i=1}^{m} r_i\,a\,s_i \mid r,\ s,\ r_i,\ s_i \in R,\ m \in \mathbf{N},\ n \in \mathbf{Z}\}.$$

(ii) 如果R有单位元1_R时, 则

$$(a) = \{\sum_{i=1}^{m} r_i\,a\,s_i \mid r_i,\ s_i \in R,\ m \in \mathbf{N},\}.$$

(iii) 如果a在R的中心(即对任意$r \in R$, 有$r\,a = a\,r$), 则

$$(a) = \{r\,a + n\,a \mid r \in R,\ n \in \mathbf{Z}\}.$$

(iv) $Ra = \{r\,a \mid r \in R\}$ (对应地. $aR = \{a\,r \mid r \in R\}$) 是R中的的左(对应地. 右)理想. 如果R有单位元, 则$a \in Ra,\ a \in aR$.

证 (i) 令

$$I = \{r\,a + a\,r' + n\,a + \sum_{i=1}^{m} r_i\,a\,s_i \mid r,\ s,\ r_i,\ s_i \in R,\ m \in \mathbf{N},\ n \in \mathbf{Z}\}$$

则I 是一个包含a 的理想. 事实上, 对任意

$$a_1 = r_1\,a + a\,r_1' + n_1\,a + \sum_{i=1}^{m_1} r_{1,i}\,a\,s_{1,i},\ \ a_2 = r_2\,a + a\,r_2' + n_2\,a + \sum_{i=1}^{m_2} r_{2,i}\,a\,s_{2,i} \in I,$$

以及$r \in R$, 有

$$a_1 - a_2 = (r_1 - r_2)\,a + a\,(r_1' - r_2') + (n_1 - n_2)\,a + \sum_{i=1}^{m_1} r_{1,i}\,a\,s_{1,i} + \sum_{i=1}^{m_2} (-r_{2,i})\,a\,s_{2,i} \in I,$$

$$r\,a_1 = (r\,r_1)a + r\,a\,r_1' + (n_1\,r)a + \sum_{i=1}^{m_1} (r\,r_{1,i})a\,s_{1,i} \in I,$$

$$a_1\,r = r_1\,a\,r + a(r_1'\,r) + n_1(a\,r) + \sum_{i=1}^{m_1} r_{1,i}\,a\,(s_{1,i}\,r) \in I,$$

因此, I 是包含a 的理想.

再设A_j 是包含a 的任意理想. 则对任意

$$a_i = r\,a + a\,r' + n\,a + \sum_{i=1}^{m} r_i\,a\,s_i \in I, \quad r,\ s,\ r_i,\ s_i \in R,\ m \in \mathbf{N},\ n \in \mathbf{Z},$$

因为A_j 是理想, 所以$r\,a, a\,r', r_i\,a\,s_i, n\,a \in H_j$, 从而

$$a_i = r\,a + a\,r' + n\,a + \sum_{i=1}^{m} r_i\,a\,s_i \in A_j.$$

即$I \subset A_j,\ I \subset \bigcap_j A_j$. 因此, I 是由a 生成的理想.

(ii) 如果R 有单位元1_R , 则有

$$r\,a = r\,a\,1_R, \quad a\,r' = 1_R\,a\,r', \quad n\,a = (n1_R)\,a.$$

因此, (ii) 成立.

(iii) 如果a 在R 的中心, 则有

$$a\,r' = r'\,a, \quad \sum_{i=1}^{m} r_i\,a\,s_i = (\sum_{i=1}^{m} r_i\,s_i)\,a.$$

因此, (iii) 成立.

由(ii) 和(iii) 即可得到(iv). 证毕

环R叫做**主理想环**, 如果R的所有理想都是主理想.

注 主理想环中的因式分解是唯一的.

10.5.3 整环**Z** 是主理想环, 且理想$I=(a)$的表达式为

$$I=(a)=\{s\,a \mid s\in \mathbf{Z}\}$$

证 设I是**Z** 中的一个非零理想. 当$b\in I$时, 有$0=0\,b\in I$及$-b=(-1)b\in I$. 因此, I中有正整数存在. 设a是I中的最小正整数, 则$I=(a)=\{s\,a \mid s\in \mathbf{Z}\}$. 事实上, 对任意$b\in I$, 存在整数$s,\ r$使得

$$b=s\,a+r,\quad 0\le r<a.$$

这样, 由$b\in I$及$(-s)\,a\in I$, 得到$r=a+(-s)\,a\in I$. 但$r<a$以及a是I中的最小正整数. 所以, $r=0,\ b=s\,a\in(a)$. 从而$I\subset(a)$. 又显然有$(a)\subset I$. 故$I=(a)$, **Z** 是主理想环. 证毕

推论 设$I=(a)$ 是整环**Z** 中的理想. 则整数$b\in I$ 的充要条件是$a\mid b$.

证 必要性. 设$b\in I=(a)$, 则存在整数s 使得$b=s\,a$, 因此, $a\mid b$.

充分性. 设$a\mid b$, 则存在整数s 使得$b=s\,a$, 因此, $b\in I=(a)$. 证毕

例10.5.2 $\mathbf{R}[X]$ 是主理想环.

证明参见定理11.6.1.

例10.5.3 $\mathbf{Z}[\sqrt{-5}]$ 不是主理想环.

下面考虑理想的运算.

设R 是一个环. $A,\ B$ 是R 的(左)理想. 则

由$X=\{a+b \mid a\in A,\ b\in B\}$ 生成的(左)理想,称为(左)理想$A,\ B$ 的**和理想**, 记作$A+B$.

由$X=\{a\,b \mid a\in A,\ b\in B\}$ 生成的(左)理想, 称为理想A, B 的**积理想**, 记作$A\cdot B$. 简记为AB.

进一步, 设R 是一个环. $A_1,\ A_2,\ \ldots,\ A_{n-1},\ A_n$ 是环R 的(左)理想. 则可递归定义:

由$A_1+A_2+\cdots+A_{n-1}$, A_n 生成的理想, 称为$A_1,\ A_2,\ \ldots,\ A_{n-1},\ A_n$ 的和理想, 记作$A_1+A_2+\cdots+A_{n-1}+A_n$.

由$A_1\cdot A_2\cdots A_{n-1}$, A_n 生成的理想, 称为$A_1,\ A_2,\ \ldots,\ A_{n-1},\ A_n$ 的积理想, 记作$A_1\cdot A_2\cdots A_{n-1}\cdot A_n$.

10.5.5 设$A,\ B,\ C$ 是环R 的(左)理想. 则

(i) $A+B=\{a+b \mid a\in A,\ b\in B\}$.

(ii) $AB=\{\sum\limits_{j=1}^{s} a_j\, b_j \mid a_j\in A,\ b_j\in B,\ s\in \mathbf{N}\}$.

(iii) $(A+B)+C=A+(B+C)$

(iv) $(AB)C=ABC=A(BC)$.

证 (i) 设$I=\{a+b \mid a\in A,\ b\in B\}$. 先证明$I$ 是(左)理想. 对任意$u,\ v\in I$ 以及$r\in R$, 存在$a_1,\ a_2\in A,\ b_1,\ b_2\in B$ 使得$u=a_1+b_1,\ v=a_2+b_2$. 因为$A,\ B$ 是(左)理想, 所以$a_1-a_2,\ r\,a_1\in A$ 及$b_1-b_2,\ r\,b_1\in B$, 从而

$$u-v=(a_1-a_2)+(b_1-b_2)\in I,\qquad r\,u=(r\,a_1)+(r\,b_1)\in I.$$

故I 是R 的(左)理想. 显然, I 是包含$\{a+b \mid a\in A,\ b\in B\}$ 的最小理想. 故$A+B=I$.

(ii) 设$J=\{\sum_{j=1}^{s} a_j\,b_j \mid a_j\in A,\ b_j\in B,\ s\in \mathbf{N}\}$. 先证明$J$ 是(左)理想. 对任意$u,\ v\in J$ 以及$r\in R$, 存在$a_i\in A,\ b_i\in B,\ 1\le i\le s+t$ 使得$u=\sum_{j=1}^{s} a_j\,b_j,\ v=\sum_{j=s+1}^{s+t} a_j\,b_j$, 因为$A,\ B$ 是(左)理想, 所以$(-a_j),\ r\,a_j\in A,\ 1\le j\le s+t$, 从而

$$u-v=\sum_{j=1}^{s} a_j\,b_j+\sum_{j=s+1}^{s+t}(-a_j)\,b_j\in J,$$

及

$$r\,u=\sum_{j=1}^{s}(r\,a_j)\,b_j\in J.$$

故J 是R 的(左)理想.

进一步, 对于包含$\{a\,b \mid a\in A,\ b\in B\}$ 的任一理想A_k , 由$a_j\in A,\ b_j\in B$, 得到$a_j\,b_j\in J$, 又A_k 是理想, 所以$u=\sum_{j=1}^{s} a_j\,b_j\in A_k$, $J\subset A_k$. 这说明, $AB=J$.

(iii) 对于任意的$u \in A+B,\ c \in C$, 存在$a \in A,\ b \in B$, 使得$u = a+b$, 从而

$$u + c = (a + b) + c = a + (b + c) \in A + (B + C).$$

因此, $(A + B) + C \subset A + (B + C)$.

同样可得, $A+(B+C) \subset (A+B)+C$. 故$(A+B)+C = A+(B+C)$.

(iv) 对于任意的$u \in AB,\ c \in C$, 存在$a_j \in A,\ b_j \in B,\ \ 1 \le j \le s$, 使得$u = \sum_{j=1}^{s} a_j\, b_j$, 从而

$$uc = (\sum_{j=1}^{s} a_j\, b_j)c = \sum_{j=1}^{s} a_j\, (b_j\, c) \in A(BC).$$

因此, $(AB)C \subset A(BC)$.

同样可得, $A(BC) \subset (AB)C$. 故$(AB)C = A(BC)$. 证毕

例10.5.4 设$A=(a),\ B=(b)$ 是整环$\mathbf{Z}$ 的两个理想. 证明:

$$A+B=((a,b)),\qquad AB=(a\,b),$$

其中(a,b) 是整数$a,\ b$ 的最大公因数.

证 1) 根据定理10.5.5 和定理10.5.4, 有

$$A+B=\{s\,a+t\,b\mid s,\ t\in\mathbf{Z}\}.$$

根据广义欧几里得除法, 可找到整数$s_0,\ t_0$ 使得$s_0\,a+t_0\,b=(a,b)$, 因此, $(a,b)\in A+B$.

又根据整数的性质, 由$(a,b)\mid a,\ (a,b)\mid b$ 可推得: 对任意整数$s,\ t$, 有$(a,b)\mid s\,a+t\,b$, 因此, (a,b) 是$A+B$ 中最小正整数.

故$A+B=((a,b))$.

2) 根据定理10.5.5 和定理10.5.4, 有

$$AB=\{\sum_{j=1}^{s}a_j\,b_j\mid a_j\in A,\ b_j\in B,\ s\in\mathbf{N}\}=\{k\,a\,b\mid k\in\mathbf{Z}\}.$$

证毕

定理10.5.6 设$A_1,\ A_2,\ \ldots,\ A_n,\ B,\ C$ 是环R 的(左)理想. 则

(i) $A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n \mid a_i \in A_i,\ 1 \le i \le n\}$ 是(左)理想.

(ii) $A_1A_2 \cdots A_n = \{\sum_{j=1}^{s} a_{1,j}\, a_{2,j} \cdots a_{n,j} \mid a_{i,j} \in A_i,\ 1 \le i \le n,\ 1 \le j \le s,\ s \in \mathbf{N}\}$ 是(左)理想.

(iii) $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$,

$(A_1 + A_2 + \cdots + A_n)C = A_1C + A_2C + \cdots + A_nC$.

证 对n 用数学归纳法. 当$n = 2$ 时, 由定理10.5.5, 定理成立.

假设$n - 1$ 时, 定理成立.

对于n, 有

(i) $A_1 + A_2 + \cdots + A_{n-1} + A_n = (A_1 + A_2 + \cdots + A_{n-1}) + A_n$ 是(左)理想.

(ii) $A_1A_2 \cdots A_{n-1}A_n = (A_1A_2 \cdots A_{n-1})A_n$ 是(左)理想.

(iii)
$$\begin{aligned} B(A_1 + A_2 + \cdots + A_{n-1} + A_n) &= B(A_1 + A_2 + \cdots + A_{n-1}) + BA_n \\ &= BA_1 + BA_2 + \cdots + BA_{n-1} + BA_n, \end{aligned}$$

$$\begin{aligned} (A_1 + A_2 + \cdots + A_{n-1} + A_n)C &= A_1C + (A_2 + \cdots + A_{n-1} + A_n)C \\ &= A_1C + A_2C + \cdots + A_{n-1}C + A_nC. \end{aligned}$$

证毕

10.5.2 商环

下面考虑商环R/I 的构造.

定理10.5.7 设R 是一个环. I 是R 的一个理想. 则R/I 对于加法运算

$$(a+I)+(b+I)=(a+b)+I,$$

和乘法运算 $\quad (a+I)(b+I)=ab+I,$

构成一个环. 当R 是交换环或有单位元时, R/I 也是交换环或有单位元.

证 首先说明加法和乘法的定义是合理的, 即运算的定义不依赖于代表元的选择.

因为I 是环R 的一个理想, 所以I 是$(R,+)$ 的一个正规子群. 因此, 所定义的加法运算是合理的.

再考虑乘法运算定义的合理性. 设$a_1+I=a_2+I,\ b_1+I=b_2+I$, 则有

$$a_1=a_2+r_1,\quad b_1=b_2+r_2,\qquad r_1,\ r_2\in I.$$

因为I 是理想, 所以$r_1b_2,\ a_2r_2,\ r_1r_2\in I$. 从而,

$$a_1b_1+I=(a_2+r_1)(b_2+r_2)+I=a_2b_2+r_1b_2+a_2r_2+r_1r_2+I=a_2b_2+I.$$

因此, 所定义的乘法运算是合理的.

其次, R/I中有结合律. 事实上, 对任意$a+I, b+I, c+I \in R/I$, 有

$$\begin{aligned}(a+I)((b+I)(c+I)) &= (a+I)((bc)+I) = a(bc)+I \\ &= (ab)c+I \\ &= ((a+I)(b+I))(c+I)\end{aligned}.$$

再其次, R/I 有分配律. 事实上, 对任意$a+I, b+I, c+I \in R/I$, 有

$$\begin{aligned}(a+I)((b+I)(c+I)) &= (a+I)((bc)+I) = a(bc)+I \\ &= (ab)c+I \\ &= ((a+I)(b+I))(c+I)\end{aligned}.$$

最后, 当R 为交换环, 且有单位元1_R 时, 对任意$a+I, b+I \in R/I$, 有

$$(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I),$$

$$(a+I)(1_R+I) = a1_R+I = a, \quad (1_R+I)(a+I) = 1_Ra+I = a+I.$$

故R/I 构成环. 且当R 是交换环或有单位元时, R/I 也是交换环或有单位元. 证毕

定理10.5.7 中的环R/I 叫做R 关于I 的**商环**.

10.5.3 环同态分解定理

下面给出同态分解定理.

定理10.5.8 设f 是环R 到环R' 的同态, 则f 的核$\ker(f)$ 是R 的理想.

反过来, 如果I 是环R 的理想, 则映射

$$\begin{aligned} s : R &\longrightarrow R/I \\ a &\longmapsto a+I \end{aligned}$$

是核为I 的同态.

证 设f 是环R 到环R' 的同态, 则对任意$a,\ b \in \ker(f),\ r \in R$, 有

$$f(a-b) = f(a) - f(b) = 0,$$

以及

$$f(r\,a) = f(r)f(a) = f(r)\cdot 0 = 0, \quad f(a\,r) = f(a)f(r) = 0 \cdot f(r) = 0,$$

从而$a-b,\ r\,a, a\,r \in \ker(f)$. 因此, $\ker(f)$是R 的理想.

反过来, 作映射

$$\begin{aligned} s : R &\longrightarrow R/I \\ a &\longmapsto a+I \end{aligned}$$

则s 是同态. 事实上, 对任意$a,\ b \in R$, 有

$$s(a+b) = (a+b)+I = (a+I)+(b+I) = s(a)+s(b),$$

$$s(a\,b) = a\,b+I = (a+I)(b+I) = s(a)s(b).$$

此外, 对任意$(a+I) \in R/I$, 有原像为a, 故s为R到R/I的满同态. 进一步,

$$\ker(s) = \{a \mid a+I = I,\ a \in R\} = \{a \mid a \in I\} = I.$$

证毕

映射$s : R \longrightarrow R/I$ 称为R 到R/I **自然同态**.

定理10.5.9(同态分解) 设f 是环R 到环R' 的同态, 则存在惟一的$R/\ker(f)$ 到像子环$f(R)$ 的同构$\overline{f} : a+\ker(f) \longmapsto f(a)$ 使得$f = i \circ \overline{f} \circ s$, 其中$s$ 是环R 到商环$R/\ker(f)$ 的自然同态, $i : c \longmapsto c$ 是$f(R)$ 到R' 的恒等同态. 即有如下的交换图:

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \mathrm{s}\downarrow & & \uparrow \mathrm{i} \\ R/\ker(f) & \xrightarrow{\overline{f}} & f(R) \end{array}$$

证 根据定理??, $\ker(f)$ 是环R 的理想, 所以存在商环$R/\ker(f)$. 现在要证明:

$$\overline{f} : a+\ker(f) \longmapsto f(a)$$

是$R/\ker(f)$ 到像子环$f(R)$ 的同构.

首先, $\overline{f}$ 是$R/\ker(f)$ 到$f(R)$ 的同态. 事实上, 对任意的$a+\ker(f)$, $b+\ker(f) \in R/\ker(f)$,

$$\begin{aligned} \overline{f}((a+\ker(f))(b+\ker(f))&=\overline{f}((a\,b)+\ker(f)) = f(a\,b) = f(a)f(b) \\ &=\overline{f}(a+\ker(f))\overline{f}(b+\ker(f)). \end{aligned}$$

其次, $\overline{f}$ 是一对一. 事实上, 若$a+\ker(f)\in\ker(\overline{f})$, 使得

$$\overline{f}(a+\ker(f))=f(a)=0'.$$

则有$a\in\ker(f)$ 以及$a+\ker(f)=\ker(f)$.
最后, $\overline{f}$ 是满同态. 事实上, 对任意$c\in f(R)$, 存在$a\in R$ 使得$f(a)=c$. 从而, $\overline{f}(a+\ker(f))=f(a)=c$. 即$a+\ker(f)$ 是c 的像源.
因此, $\overline{f}$ 是同构, 并且有$f=i\circ\overline{f}\circ s$. 事实上, 对任意$a\in R$, 有

$$(i\circ\overline{f}\circ s)(a)=i(\overline{f}(s(a)))=i(\overline{f}(a+\ker(f)))=i(f(a))=f(a).$$

此外, $\overline{f}$ 是惟一的.事实上, 假如还有同构$g:R/\ker(f)\longrightarrow f(R)$ 使得$f=i\circ g\circ s$, 则对任意$a+\ker(f)\in R/\ker(f)$, 我们有

$$g(a+\ker(f))=i(g(s(a)))=(i\circ g\circ s)(a)=f(a)=\overline{f}(a+\ker(f)).$$

因此, $g=\overline{f}$. 证毕

10.6 素理想

本节将讨论素理想.

我们先研究整环$\mathbf{Z}$ 中由素数生成的理想及其具有的性质.

假设p 是素数. 则当整数$a,\ b$ 满足$p \mid a\,b$ 时, 一定有$p \mid a$ 或$p \mid b$.

根据定理**??**及其推论, 上述表述可用理想表述为:

$$\boxed{\text{若}(a\,b) \subset (p), \text{则}(a) \subset (p) \text{ 或}(b) \subset (p).}$$

或

$$\boxed{\text{若}a\,b \in (p), \text{则}a \in (p) \text{ 或}b \in (p).}$$

我们将此表述抽象为:

定义10.6.1 设P 是环R 的理想. P 称为R 的**素理想**, 如果$P \neq R$, 且对任意理想$A, B,\ AB \subset P$, 有$A \subset P$ 或$B \subset P$.

定理10.6.1 设P 是环R 的理想. 如果$P \neq R$, 且对任意的$a, b \in R$, 当$a\,b \in P$时, 有$a \in P$ 或$b \in P$, 则P 是素理想. 反过来, 如果P 是素理想, 且R 是交换环, 则上述结论也成立.

证 必要性. 如果理想A, B 使得$AB \subset P$, $A \not\subset P$, 则存在元素$a \in A$, $a \notin P$. 对任意元素$b \in B$, 根据假设, 从$a\,b \in AB \subset P$ 及$a \notin P$ 可得到$b \in P$. 这说明, $B \subset P$. 因此, P 是素理想.

反过来, 设P 是素理想, 则对任意的$a, b \in R$, 满足$a\,b \in P$, 有$(a)(b) = (a\,b) \subset P$. 根据素理想的定义, 我们有$(a) \subset P$ 或$(b) \subset P$. 由此得到, $a \in P$ 或$b \in P$. 证毕

例10.6.1 任意整环的零理想是素理想.

例10.6.2 设p 是素数. 则$P = (p) = p\mathbf{Z}$ 是$\mathbf{Z}$ 的素理想.

证 对任意的整数$a,\ b$, 若$a\,b \in P = (p)$, 则$p \mid a\,b$. 根据定理1.4.2, 有$p \mid a$ 或$p \mid b$. 由此得到, $a \in P$ 或$b \in P$. 根据定理10.6.1, $P = (p) = p\mathbf{Z}$ 是$\mathbf{Z}$ 的素理想. 证毕

定理10.6.2 设R是有单位元$1_R \neq 0$的交换环. 则理想P是素理想的充要条件是商环R/P是整环.

证 因为环R有单位元$1_R \neq 0$, 所以R/P有单位元$1_R + P$和零元$0_R + P = P$. 又因为P是素理想, 所以$1_R + P \neq P$.

现在说明R/P无零因子. 事实上, 若$(a+P)(b+P) = P$, 则$ab+P = P$. 因此, $ab \in P$. 但P是交换环R的素理想, 根据定理10.6.1, 得到$a \in P$或$b \in P$, 即$a + P = P$或$b + P = P$是R/P的零元. 故商环R/P是整环.

反过来, 对任意的$a, b \in R$, 满足$ab \in P$, 则有$(a + P)(b + P) = ab + P = P$. 因为商环$R/P$是整环, 没有零因子, 所以$a + P = P$或$b + P = P$. 由此得到, $a \in P$或$b \in P$. 根据定理10.6.1, 理想P是素理想. 证毕

定义10.6.2 设M是环R的(左)理想. M称为R的**极大(左)理想**, 如果$M \neq R$, 且对任意的理想N, 使得$M \subset N \subset R$, 有$N = M$或$N = R$.

定理10.6.3 设R是有单位元$1_R \neq 0$的非零环. 则极大(左)理想总是存在的. 事实上, R的每个(左)理想($\neq R$)都包含在一个极大(左)理想中.

证 设A是R的任一理想, 并且$A \neq R$, 令

$$S = \{B \mid B \text{ 是 } R \text{ 的理想, 且 } A \subset B \neq R\}.$$

S显然是非空的, 依包含关系作成一个偏序集, 取S的任一非空有序子集, $L = \{H_i \mid i \in I\}$, 令$H = \bigcup_{i\in I} H_i$, 则H是R的理想.又有$A \subset H_i \subset H$, 同时对任意$H_i \neq R$, 即$1 \notin H_i$, 有$1 \notin H$. 所以$H \neq R, H \in S$. 显然H是L的上界, 即S的任一非空有序子集均有上界, 由Zorn引理知, S有极大元H', 这一极大元即为R的一个极大理想, 且$A \subset H'$. 证毕

定理10.6.4 整环**Z** 中的每个素理想都是极大理想.

证 设P 是**Z** 中的素理想, 则$P = (p)$, 其中p 是素数.

若M 是真包含P 的理想, 则存在元素$a \in M \setminus P$.

因此, 有$p \nmid a$, 从而$(a, p) = 1$. 根据广义欧几里得除法, 可找到整数$s,\ t$ 使得$s\,a + t\,p = 1$. 由此得到$1 \in M$ 以及$M = \mathbf{Z}$. 因此, P 是极大理想. 证毕

定理10.6.5 设R 是一个有单位元$1_R \neq 0$ 的环. 则R 的每个极大理想是素理想.

证 设$a\,b \in M$, 但$a \notin M$. 因为$(a) + M$ 是严格包含M 的理想, 所以$(a) + M = R$. 又因为$1_R \in R$, 所以存在$s \in R$, $m \in M$, 使得$1_R = s\,a + m$. 进而, $b = 1_R \cdot b = s\,a\,b + m\,b \in M$. 因此, M 是素理想. 证毕

定理10.6.6 设R是一个有单位元$1_R \neq 0$的交换环, M是R的一个理想. 则M是极大理想的充要条件是商环R/M是一个域.

证 必要性. 设M是极大理想, 则对任意$a \in R \setminus M$, 由$(a)+M$是R中的理想, 推得$(a)+M=R$. 因为$1 \in R$, 所以存在$r \in R$, $m \in M$, 使得$1 = a \cdot r + m$, 从而有$(a+M)(r+M) = 1+M$, 即R/M中任一非零元都有逆, 故R/M是域.

充分性. 对于元$a \in R \setminus M$, 有$a+M$是R/M中的非零元, 而R/M是一个域, 所以存在$r+M$, 使得$(a+M)(r+M)=1$. 由此, $(a)+M=R$. 故M是R的一个极大理想. 证毕

定理10.6.7 设R 是一个有单位元$1_R \neq 0$ 的交换环, 则如下条件等价:

(i) R 是的一个域.

(ii) R 没有真理想.

(iii) 0 是R 的最大理想.

(iv) 每个非零环同态$R \to R'$ 是单同态.

证 (i) $\Rightarrow$ (ii) . 设I 是R 的理想. 若$I \neq 0$, 则有$a \in I,\ a \neq 0$. 因为R 是域, 所以a 是可逆元, 存在$r \in R$, 使得$r\,a = 1$. 因此, $1 = r\,a \in I$, $I = R$. 这说明R 中没有真理想.

(ii) $\Rightarrow$ (iii) . 由(ii), 真包含0 的理想只有R, 这说明0 是极大理想.

(iii) $\Rightarrow$ (iv) . 设$f : R \to R'$ 是非零的环同态. 则$\ker(f) \neq R$ 是包含0 的理想, 0 是极大理想, 所以$\ker(f) = 0$, 即f 是单同态.

(iv) $\Rightarrow$ (i). 若R 不是域, 则存在非零的不可逆元a, 因此, 理想$I = (a)$ 是真理想, 从而R 到R/I 的自然同态$s : R \to R/I$ 不是单同态. 矛盾. 因此R 是域. 证毕