第 7 章 环

环是在群的基础上,引入另一种运算产生的代数结构．较为常见的环有整数环，多项式环等．在本章中，我们将讨论环的定义，性质，理想以及相应的商环，几种特殊类型的环，最后通过素理想和极大理想的概念，引出域的相关内容.

7.1 环

环是具有两种运算的代数结构，在继承了群的相关性质的同时，还有若干特有的结论．首先，我们简要介绍环的概念.

定义 7.1.1 设 R 是一个给定的集合，在其上定义了两种二元运算“+”和“•”，如果满足以下条件：

(1) $(R, +)$是一个交换群；

(2) $(R, \bullet)$是一个半群；

(3) 对于这两种运算有以下的分配律成立，即对任意 $a, b, c\in R$ 有，

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

则我们称$(R, +, \bullet)$为**环**．若$(R, \bullet)$是一个交换半群，则称为**交换环**

通常把运算“+”称为交换环中的“加法”，“•”称为交换环中的“乘法”．运算“+”下的单位元称为交换环的**零元**，记为 0，且元素 a 在运算“+”下的逆元称为元素 a 的**负元**；如果 R 中存在运算“•”下的单位元，我们称之为交换环的**幺元**，记为 1，且如果元素 a 在运算“•”下存在其逆元，则称该逆元为元素 a 的**逆元**，满足这样条件的元素 a 称为**可逆元素**.

例 7.1.1 $(\mathbf{Z}, +, \times)$是一个交换环，零元是 0，幺元是 1，可逆元素只有−1 和 1. $(\mathbf{Q}, +, \times)$、$(\mathbf{R}, +, \times)$和$(\mathbf{C}, +, \times)$都是交换环，零元都是 0，幺元都是 1，除了 0 以外，所有的其他元素都是可逆元素.

例 7.1.2 用 $\mathbf{Z}[i]$表示集合$\{a + bi \mid a, b\in \mathbf{Z}\}$，其中 i 为虚数单位，则 $\mathbf{Z}[i]$关于复数的加法和乘法构成交换环，称之为**高斯整数环**．零元是 0，幺元是 1，可逆元素只有−1、1、i 和 $-i$.

例 7.1.3 令 $\mathbf{Z}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b\in \mathbf{Z}\}$，则$(\mathbf{Z}(\sqrt{2}), +, \times)$是一个交换环，零元是 0，幺元是 1，都有哪些可逆元素呢？（习题）

定义 7.1.4 如果交换环 R 的一个子集 S 满足如下三个条件：

(1) $0\in S$；

(2) 如果 $a, b\in S$，则 $a-b\in S$；

(3) 如果 $a, b\in S$，则 $ab\in S$；

则我们称 S 是 R 的**子环**．并称 R 是 S 的**扩环**(或**扩张**)．如果 $S = R$ 或 $S = \{0\}$，那么显然 S 是 R 的子环，称为**平凡子环**，平凡子环以外的子环称为**真子环**.

例 7.1.4 $(\mathbf{Z}, +, \times)$、$(\mathbf{Q}, +, \times)$和$(\mathbf{R}, +, \times)$都是$(\mathbf{C}, +, \times)$的子环；$(\mathbf{Z}, +, \times)$和$(\mathbf{Q}, +, \times)$都是$(\mathbf{R}, +, \times)$的子环；$(\mathbf{Z}, +, \times)$是$(\mathbf{Q}, +, \times)$的子环.

定义 7.1.2 设$(R, +, \bullet)$是交换环，$a\in R$ 且 $a\neq 0$，如果存在 $b\in R$ 且 $b\neq 0$，使得 $a \bullet b = 0$ 成立，则称 a 是交换环 R 的**零因子**.

定义 7.1.3　$(R, +, \cdot)$是环，我们可进一步定义

(1) 若$(R, \cdot)$是一个含幺元的半群，则称为**幺环**；

(2) 若任意两个非零元的积不等于零，则称为**无零因子环**

(3) 若$(R, +, \cdot)$是无零因子的幺环，则称为**整环**；

(4) 若非零元对 • 构成群，则称为**体**；

(5) 若非零元对 • 构成 Abel 群，则称为**域**.

在后面章节中，除了特别指出外，一般考虑的环均为交换幺环.

例 7.1.5　实数域 R 上的所有 n 阶方阵构成的集合对于矩阵加法、乘法构成环，其中零元为 n 阶零方阵，幺元为 n 阶单位方阵，但该环是非交换的.

定理 7.1.1　$(R, +, \cdot)$为交换环，对任意 $a, b, c \in R$ 有，

(1) $0 \cdot a = a \cdot 0 = 0$；

(2) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$；

(3) $(-a) \cdot (-b) = a \cdot b$；

(4) $a \cdot (b - c) = a \cdot b - a \cdot c$；

(5) $(b - c) \cdot a = b \cdot a - c \cdot a$；

证明　(1) 利用分配律可知 $0 \cdot a = (0+0) \cdot a = (0 \cdot a)+(0 \cdot a)$，由加法群$(R, +)$的消去律知

$$0 \cdot a = 0.$$

同理可证 $a \cdot 0 = 0$.

(2)至(5)的证明留作读者练习.

定理 7.1.2　$(R, +, \cdot)$为交换环，$a, b \in R$，$m, n \in \mathbf{Z}$，则

(1) $m(na) = (mn)a$；

(2) $ma+na = (m+n)a$；

(3) $(na) \cdot b = a \cdot (nb) = n(a \cdot b)$；

(4) $(ma) \cdot (nb) = (mn)(a \cdot b)$；

(5) $(ma^h) \cdot (na^k) = (mn)a^{h+k}$.（其中 $h, k \in \mathbf{Z}^+$；当 a 是可逆元时，可取 $h, k \in \mathbf{Z}$.）

定理 7.1.3　即一般交换环上的二项式定理. $(R, +, \cdot)$为交换环，$a, b \in R$，则

$$(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k \cdot b^{n-k} .$$

下面我们讨论整环. 最常见的整环即为整数环 $\mathbf{Z}$，与此同时，我们还知道有理数域 $\mathbf{Q}$ 是通过扩充出来的. 最终，我们将证明所有的交换整环都能扩充成一个域.

例 7.1.6　$\mathbf{Z}$ 中没有零因子. 容易证明，$\mathbf{Z}_n$ 中没有零因子的充要条件是 n 为素数.

例 7.1.7　$(\mathbf{Z}, +, \times)$、$(\mathbf{Q}, +, \times)$、$(\mathbf{R}, +, \times)$和$(\mathbf{C}, +, \times)$都是整环. $(\mathbf{Z}_n, \oplus, \otimes)$是整环的充要条件是 n 为素数. 所以，$\mathbf{Z}_2$、$\mathbf{Z}_3$和$\mathbf{Z}_5$等等，都是整环；而$\mathbf{Z}_4$、$\mathbf{Z}_6$和$\mathbf{Z}_8$等等，都不是整环.

定义 7.1.5　若交换整环 R 和域 F 满足 $R \subset F$ 且对$\forall a \in F, \exists b, c \in R$使得

$$a = bc^{-1}$$

则称 F 为 R 的**分式域.**

例 7.1.8　整数环 $\mathbf{Z}$ 的分式域为有理数域 $\mathbf{Q}$.

定理 7.1.4　设 R 为交换整环，则存在 R 的分式域

证明　设 $R^* = R \backslash \{0\}$，定义 $R^* \times R$ 中的加法、乘法：对$\forall (a, b), (c, d) \in R^* \times R$，定义

$$(a, b) + (c, d) = (ad + bc, bd)$$

$$(a, b) \cdot (c, d) = (ac, bd)$$

容易证明, $R^*\times R$ 对上述加法、乘法构成交换幺半群，零元为(0,1)，幺元为(1,1).

在 $R^*\times R$ 中定义一个关系~：$(a,b)\sim(c,d)$ 当且仅当 $ad=bc$.

首先，~ 是等价关系：1，$ab=ab$故$(a,b)\sim(a,b)$；2,若$(a,b)\sim(c,d)$则$ad=bc$，进而$(c,d)\sim(a,b)$；3，若$(a,b)\sim(c,d)$且$(c,d)\sim(e,f)$则$adf=bcf=bde$，又因是交换整环且$d\neq 0$，所以$af=be$，进而$(a,b)\sim(e,f)$.

其次，上述乘法、加法保持~关系：1，若$(a,b)\sim(c,d),(e,f)\sim(g,h)$则有$(a,b)(e,f)=(ae,bf)$，$(c,d)(g,h)=(cg,dh)$，进而$(ae)(dh)=adeh=bcfg=(bf)(cg)$，所以$(a,b)(e,f)\sim(c,d)(g,h)$；2，若$(a,b)\sim(c,d),(e,f)\sim(g,h)$则$(a,b)+(e,f)=(af+be,bf)$和$(c,d)+(g,h)=(ch+dg,dh)$，从而$(af+be)dh=adfh+bedh=bcfh+fgbd=(ch+dg)bf$，所$(a,b)+(e,f)\sim(c,d)+(g,h)$.

最后，令 $F=R^*\times R/\sim$为 $R^*\times R$ 关于等价关系~的商集合，并设$\frac{a}{b}$ 为(a,b)所在的等价类.

易验证 F 对加法是幺半群，零元为$\frac{0}{1}$，幺元为$\frac{1}{1}$，进而 $F\backslash\{0\}$对乘法也构成幺半群，且加法与乘法之间分配律成立. 因此 F 是域，且对其中任意元素$\frac{a}{b}$有$\frac{a}{b}=\frac{a}{1}\frac{1}{b}=\frac{a}{1}(\frac{b}{1})^{-1}$，故 F 为 R 的分式域.

最后我们给出环之间同态、同构的概念. 环的同态与同构定义类似于群的同态与同构，但要求加法、乘法两种运算.

定义 7.1.5 X 与 Y 是两个环，如果存在一个映射 f:$X\to Y$，使得对$\forall x_1, x_2\in X$，都有

$$f(x_1+x_2)=f(x_1)+f(x_2),\ f(x_1\cdot x_2)=f(x_1)\cdot f(x_2)$$

则称 f 是一个从 X 到 Y 的**同态映射**或称环 X 与 Y **同态**，记作 $X\sim Y$. 其中运算+和 • 定义参照相应元素所在集合，为两个环中相应的加法与乘法.

如果 f 是单射，则称此同态为**单同态**，如果 f 是满射，则称此同态为**满同态**，如果 f 是双射，则此同态为**同构**. 记作 $X\cong Y$.

下面我们主要讨论一种称为多项式环的环，其在密码学和编码理论中有广泛的应用.

定义 7.1.6 设(R, +, •)是交换环，x 是一个变元，n 是非负整数，$a_0, a_1, \cdots, a_n\in R$，则

$$f(x)=a_0+a_1x+\cdots+a_nx^n\ ,$$

称为**交换环 R 上的一元多项式**. 其中，$a_0, a_1, \cdots, a_n$ 称为该多项式的**系数**，a_0 还称为**常数项**. 如果一个多项式的所有系数都是 0，那么该多项式称为**零多项式**. 如果 $a_n\neq 0$，那么 a_n 称为**首项系数**, n 称为一元多项式 $f(x)$的**次数**，记作

$$\deg f(x)=n.$$

对于交换幺环 R 的情形，我们将 $a_n=1$ 的多项式称为**首一多项式**. 所有交换环 R 上的一元多项式组成的集合记为 **$R[x]$**.

注意，对于零多项式，我们不定义其次数，因为零多项式就没有非零的系数.

需要注意的是，在这个定义中，符号“+”并不是 R 中的加法运算，a_nx^n 也不是 R 中的乘法运算，仅仅是一种符号.

设(R, +, •)是交换环，定义在 $R[x]$上的二元运算加法“+”和乘法“×”如下：对任意两个一元多项式，

$$f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x],$$
$$g(x)=b_0+b_1x+\cdots+b_mx^m\in R[x],$$

令

$$(f+g)(x)=(a_0+b_0)+(a_1+b_1)x+\cdots+(a_l+b_l)x^l\ ,$$

其中 $l=\max(m,n)$. 当 $n<l$ 时，$a_j=0\ (n<j\leqslant l)$，当 $m<l$ 时，$b_j=0\ (m<j\leqslant l)$.

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

其中

$$c_k=\sum_{i+j=k}a_i\cdot b_j\quad（0\leqslant i\leqslant n,\ 0\leqslant j\leqslant m,\ 0\leqslant k\leqslant n+m）.$$

定理 7.1.3 $(R,+,\bullet)$是交换环，$f(x)$和 $g(x)$是 $R[x]$中两个非零多项式，则

(1) $f\times g$ =零多项式或者 $\deg(f\times g)\leqslant\deg f+\deg g$.

(2) 如果$(R,+,\bullet)$是整环，那么 $f\times g\neq$零多项式且 $\deg f\times g=\deg f+\deg g$.

该定理的证明很容易，留作读者自行练习.

容易验证，当$(R,+,\bullet)$是交换环时，$(R[x],+,\times)$也构成一个交换环，其零元是零多项式，幺元为 $f(x)=1$，$f(x)=a_0+a_1x+\cdots+a_nx^n$ 的负元为 $f(x)=(-a_0)+(-a_1)x+\cdots+(-a_n)x^n$．进一步，由定理 7.1.3(2)可知，当$(R,+,\bullet)$是整环时，$(R[x],+,\times)$也是整环. 另外，我们注意如下的 $R[x]$的子集(只含有常数项的多项式的集合，该集合里的元素称为**常多项式**)

$$S=\{\,f(x)\mid f(x)=r,r\in R\,\},$$

很明显$(S,+,\times)$是$(R[x],+,\times)$的子环. 在 R 和 S 之间建立如下的双射，

$$r\mapsto f(x)=r\ ,$$

也很明显，该双射是一个同构映射，因此 $R\cong S$．因此，我们可以将 R 看作是$(R[x],+,\times)$的子环. 综上所述，我们有如下的定义.

定义 7.1.7 $(R,+,\bullet)$是交换环，则我们称$(R[x],+,\times)$为 ***R* 上的一元多项式环**，或 ***R* 上添加 *x* 生成的环** .

类似地，我们可以定义$(R[x_1,\cdots,x_n],+,\times)$，且容易验证其具有环的结构，

定义 7.1.8 $(R,+,\bullet)$是交换环，我们称之为 ***R* 上的 *n* 元多项式环**，或 ***R* 上添加$\boldsymbol{x_1,\cdots,x_n}$生成的环**.

定义 7.1.9 如果在交换幺环 R 中存在有限多个元素$a_1,\cdots,a_n$且$a_n\neq 0$,使得

$$a_nu^n+\ldots+a_1u+a_0=0$$

则称 u 为 R 上的**代数元**，使上述关系成立的最小的正整数 n 称为代数元的**次数**,记作 $\deg(u,R)$，而称 $f(x)=a_nx^n+\ldots+a_1x+x\in R[x]$为 ***u* 在 *R* 上的不可约多项式**，记为 $\mathrm{Irr}(u,R)$.

例 7.1.8 考虑整数环 **Z**，易知有理数域 **Q** 中的任意元素$\frac{n}{m}$为 **Z** 上代数元，因为 $m\frac{n}{m}+(-n)=0$. 容易验证$\sqrt{2}$和 $1+i$也是 **Z** 上代数元，但并非所有实数或复数都是 **Z** 上代数元.

类似地，我们给出超越元的定义.

定义 7.1.10 如果对 R 中任意不全为 0 元素$a_1,\cdots,a_n$，均有

$$a_nu^n+\ldots+a_1u+a_0\neq 0$$

则称 u 为 R 上的**超越元**.

例 7.1.9 自然常数 e ,圆周率π是 **Z** 上的超越元. 对这一命题的验证比较繁琐，此处省略.

易知当 u 为 R 上的超越元时，$R[u]$与多项式环 $R[x]$同构，所以我们将 $R[u]$视为 R 上一元的多项式环.

习题 7.1

A 组

1. 求证高斯整数环的可逆元素只有−1、1、i 和−i.
2. 令 $\mathbf{Z}(\sqrt{2})=\{a+b\sqrt{2}\mid a,\ b\in\mathbf{Z}\}$，则$(\mathbf{Z}(\sqrt{2}),+,\times)$是一个交换环，都有哪些可逆元素呢？
3. 求证$(Q(\sqrt{2}),+,\times)$是整环也是域
4. 设 C 为实数域 $\mathbf{R}$ 上的所有实函数构成的集合，定义加法与乘法为

   $(f+g)(x)=f(x)+g(x)\quad (fg)(x)=f(g(x)),\qquad \forall\ f,g\in C\quad x\in\mathbf{R}$

试问 C 对于上述加法、乘法定义是否构成环

B 组

5. 试问 $\mathbf{Z}_n$ 中的零因子和可逆元有哪些？
6. 试说明域上的线性空间具有环的结构.
7. 设$R_1,\ldots,R_n$是环，证明：$R_1\oplus\ldots\oplus R_n=\{(a_1,\ldots,a_n)|a_i\in R_i\}$具有环的结构，并给出具体定义.

7.2 理想、商环

如同群与子群的关系，环也有子环的概念. 但由于环的结构较群更为复杂，其拥有一类特殊的子环——理想. 我们在介绍理想的概念后，承接子群与商群，将介绍由环的理想生成的商环.

定义 7.2.1 I 是环 R 的子环，如果满足 $RI\subset R$，即对任意$i\in I,r\in R$有 $ri\in I$，则称 I 是 R 的**左理想**，类似地可定义**右理想**. 同时为左理想和右理想的子环称为**双边理想**或**理想**.

对于交换环 R，上述三个概念是一致的，我们统称为**理想**.

子环 0 和 R 本身都是 R 的理想，称之为**平凡理想**.

例 7.2.1 $n\mathbf{Z}$ 是交换环$(\mathbf{Z},+,\times)$的一个理想.

证明 $0=n\times 0n\in n\mathbf{Z}$；对任意 $a,b\in n\mathbf{Z}$ 存在整数 a' 和 b'，使得 $a=na'$ 和 $b=nb'$，则

$$a+b=na'+nb'=n(a'+b')\in n\mathbf{Z}\ ;$$

对任意 $a\in\mathbf{Z}$ 和任意 $r\in\mathbf{Z}$，存在整数 a' 使得 $a=na'$，则

$$ra=rna'=n(ra')\in n\mathbf{Z}\ ;$$

由理想的定义可知，$n\mathbf{Z}$ 是一个理想.

例 7.2.2 多个理想的交集仍为理想，若 A 是环 R 的子集，所有包含 A 的理想的交仍为包含 A 的理想，则该理想称为 A 生成的理想，记作$\langle A\rangle$.

定理 7.2.1 I 是环$(R,+,\cdot)$的子环，则可在中定义等价关系～

$$a\sim b\quad 若\ a+(-b)=a-b\in I$$

其中 a 所在的等价类记为 $a+I$. 若 I 是 R 的理想，则可在商集合 $R/\sim=R/I$ 中定义加法、乘法为

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

易知对 $R/\sim$ 上述定义的加法、乘法构成环，称之为 R 对 I 的**商环**.

证明 由定理 6.5.9 知$(R/I,+)$为群$(R,+)$对$(I,+)$的商群，从而由$(R,+)$是交换群易知 R/I 对上述定义的加法+为交换群. 以下只需说明$(R/I,\ \cdot\ )$构成半群以及加法乘法间的分配律成立.

对$\forall a,b,c\in R$有

$$((a+I)(b+I))(c+I)=(ab+I)(c+I)$$
$$=abc+I=a(bc)+I=(a+I)((b+I)(c+I))$$

且

$$((a+I)+(b+I))(c+I)=(a+b+I)(c+I)=(a+b)c+I$$
$$=(ac+bc)+I=(ac+I)+(bc+I)=(a+I)(c+I)+(b+I)(c+I)$$

类似有

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

即 R/I 为半群，加法乘法之间分配律成立. 故 R/I 是一个环.

类似于群同态、同构的定义，我们给出环之间同态与同构的概念.

定理 7.2.2 设 f 是交换环 S 到交换环 G 的同态映射， 则 im$f$ 是 G 的子环, ker f 是 S 的理想.

证明 由同态定义，$1=f(1)\in$im$f$；对任意 $a,b\in\in$im$f$，存在 $a',b'\in S$，使得 $a=f(a')$和 $b=f(b')$，则

$$a-b=f(a')-f(b')=f(a'-b')\in \text{im}f,$$
$$ab=f(a')f(b')=f(a'b')\in \text{im}f,$$

因此由子环定义知 im$f$ 是 G 的子环.

由 ker f 是 S 的加法群的子群可知, $0\in$ker f；对任意 $a,b\in$ker f， 必有 $a+b\in$ker f. 对任意 $a\in$ker f 和任意 $r\in S$， 必有 $f(ra)=f(r)f(a)=f(r)0=0$，即 $ra\in$ker f. 因此，由理想定义可知, ker f 是 S 的理想.

定理 7.2.3 交换环 R 的任意一族理想的交是 R 的理想.

证明 留给读者，可参考定理 6.3.6 的证明.

定义 7.2.2 $(R,+,\cdot)$是一个交换环，H 是 R 的非空子集，$(H_i\mid i\in\mathbf{N})$是 R 的所有包含集合 H 的理想， 即 $H\subseteq H_i(i\in N)$， 则$\bigcap_{i\in N}H_i$ 叫作**由子集 H 生成的理想**， 记为(H)， H 中的元素叫做理想(H)的**生成元**. 如果 $H=\{a_1,a_2,\cdots,a_n\}(n\in\mathbf{N})$， 则理想$(H)$记为$(a_1,a_2,\cdots,a_n)$, 并称为**有限生成的理想**， 由一个元素生成的理想<a>叫作**主理想**.

定理 7.2.4 $(R,+,\cdot)$是一个交换环，$a\in R$，$H=\{a_1,a_2,\cdots,a_n\}\subset R$， 则

(1) $(a)=\{x\cdot a\mid x\in R\}$,

(2) $(H)=(a_1,a_2,\cdots,a_n)=\{x_1\cdot a_1\oplus x_2\cdot a_2\oplus\cdots\oplus x_n\cdot a_n\mid x_i\in R, 1\leqslant i\leqslant n\}$.

证明 (1)很显然. (2)很明显，$a_1,a_2,\cdots,a_n$ 的所有线性组合组成的集合必然是 R 的一个理想，而且如果 $a_1,a_2,\cdots,a_n\in H$ 是 R 的理想，则该理想必然包含 $a_1,a_2,\cdots,a_n$ 的所有线性组合组成的集合，所以，根据定义 7.2.2 可知命题成立.

例 7.2.3 $(R,+,\cdot)$是任意一个交换幺环， 则 R 必然是自身的主理想，因为 $R=(1)$.

例 7.2.4 $(R,+,\cdot)$是任意一个交换幺环， 则零环$\{0\}$必然是 R 的主理想，因为$\{0\}=(0)$.

例 7.2.5 $n\mathbf{Z}$ 是交换环$(\mathbf{Z},+,\times)$的主理想， 因为 $n\mathbf{Z}=\{k\times n\mid k\in\mathbf{Z}\}=(n)$. 典型地， 偶数集合是主理想(2).

定义 7.2.3 如果交换环$(R,+,\cdot)$的所有理想都是主理想，则交换环 R 称为**主理想环**.

例 7.2.6 求证$(\mathbf{Z},+,\times)$是主理想环.

证明 设 H 是 $\mathbf{Z}$ 的非零理想， 则至少存在一个非零整数 $a\in H$， 由理想的性质， 因为 $-1\in\mathbf{Z}$, 所以有

$$-a=(-1)\times a\in H,$$

于是 H 中有正整数存在， 设 d 为 H 中的最小正整数， 则 $H=(d)=\{n\times d\mid n\in\mathbf{Z}\}$. 这是因为，对任意 $a\in H$， 由欧几里得除法定理， 一定存在整数 q,r 使得

$$a = q\times d + r,\ 0\leqslant r< d,$$

这样，由 $a\in H$ 及 $q\times d\in H$，有 $r = a - q\times d\in H$．但由于 $0\leqslant r<d$，又 d 是 H 中的最小正整数，所以

$$r = 0,$$

$$a = q\times d\in (d),$$

从而 $H\subseteq(d)$，又显然 $(d)\subseteq H$，所以 $H = (d)$．即 $\mathbf{Z}$ 的任意理想 H 都可以写成 (d) 的形式．所以 $\mathbf{Z}$ 是主理想环.

定理 7.2.5 交换环 R 的子集 H 是 R 的理想的充要条件是：

(1) $0\in H$;

(2) 对任意的 $a, b\in H$，都有 $a - b\in H$;

(3) 对任意的 $r\in R$ 和 $h\in H$，都有 $rh\in H$.

证明 与理想的定义中 3 个条件对比可知，差别只在第(2)条，因此只需证明(2)的充分性与必要性即可.

必要性．因为 $1\in R$ 且 R 是加法群，所以 $-1\in R$，因此，对任意的 $a, b\in H$，$(-1)\,b\in H$，所以 $a+(-1)\,b\in H$，即 $a - b\in H$.

充分性．因为 $1\in R$ 且 R 是加法群，所以 $-1\in R$，因此，对任意的 $a, b\in H$，$(-1)\,b\in H$，所以 $a-(-1)\,b\in H$，即 $a + b\in H$．得证.

这个定理的(1)和(2)实际上就是（加法）子群的判定定理，因此这个定理告诉我们，理想必然是 R 的加法子群.

定理 7.2.6 设 $(R, +, \cdot)$ 为交换环，H 是其理想，再设 T 是加法群 $(R, +)$ 关于其子群 $(H, +)$ 的所有不同陪集组成的集合，即商群 $T = R/H = \{a+H \mid a\in R\}$，那么 $(T, \oplus, \odot)$ 构成交换环．其中运算"$\oplus$"，"$\odot$"的定义为：对任意 $a+H\in T, b+H\in T$（$a, b\in R$），有

$$(a+H)\oplus(b+H) = (a+b)+H,$$

$$(a+H)\odot(b+H) = (a\cdot b)+H.$$

证明 由于 $(H, +)$ 是交换群 $(R, +)$ 的子群，所以也是交换子群，当然是正规子群．由商群的理论知 $(T, \oplus)$ 构成商群，所以本定理中关于加法的结论必然成立.

现在我们只须证明二元运算 $\odot$ 满足结合律、交换律和存在幺元以及两种运算满足分配律即可．首先要证明运算"$\odot$"的定义不依赖于 T 中元素的代表元的选择．即要证明：对任意 $a+H = a'+H$，$b+H = b'+H$，都有

$$(a\cdot b)+H = (a'\cdot b')+H.$$

由陪集的性质我们知

$$a - a' = h_1,\ b - b' = h_2,\ \text{其中 } h_1, h_2\in H,$$

从而

$$\begin{aligned}(a\cdot b)+H &= [(a'+h_1)\cdot(b'+h_2)]+H\\ &= [(a'\cdot b') + (a'\cdot h_2) + (h_1\cdot b') + (h_1\cdot h_2)]+H\\ &= (a'\cdot b') + [(a'\cdot h_2) + (h_1\cdot b') + (h_1\cdot h_2)]+H.\end{aligned}$$

又因为 H 是 R 的理想，所以 $(a'\cdot h_2), (h_1\cdot b'), (h_1\cdot h_2)\in H$，因此

$$(a'\cdot h_2) + (h_1\cdot b') + (h_1\cdot h_2)\ \in H$$

于是

$$[(a'\cdot h_2) + (h_1\cdot b') + (h_1\cdot h_2)]+H = H,$$

$$(a\cdot b)+H = (a'\cdot b')+H.$$

由运算"$\odot$"的定义，显然 $(a+H)\odot(b+H) = (a\cdot b)+H\in T$，即运算"$\odot$"对 T 满足封闭性，对任意 $a+H, b+H, c+H\in T$（$a, b, c\in R$），则

$$[(a+H)\odot(b+H)]\odot(c+H) = [(a\cdot b)+H]\odot(c+H) = (a\cdot b\cdot c)+H,$$

$$(a+H)\odot[(b+H)\odot(c+H)] = (a+H)\odot[(b\cdot c)+H] = (a\cdot b\cdot c)+H,$$

所以运算“⊙”满足结合律.

$$(a+H)\odot(b+H) = (a\cdot b)+H = (b\cdot a)+H = (b+H)\odot(a+H),$$

所以运算“⊙”满足交换律.

$$(a+H)\odot(1+H) = (a\cdot 1)+H = a+H,$$

$$(1+H)\odot(a+H) = (1\cdot a)+H = a+H,$$

所以运算“⊙”的幺元是 $1+H$.

$$[(a+H)+(b+H)]\odot(c+H) = [(a+b)+H]\odot(c+H) = [(a+b)\cdot c]+H = [(a\cdot c)+(b\cdot c)]+H,$$

$$(a+H)\odot(c+H)\oplus(b+H)\odot(c+H) = [(a\cdot c)+H]\oplus[(b\cdot c)+H] = [(a\cdot c)+(b\cdot c)]+H,$$

所以两种运算满足分配律.

所以，综上所述，$(T, \oplus, \odot)$构成交换环．得证.

定义 7.2.3 定理 7.2.6 中的交换环$(T, \oplus, \odot) = (R/H, \oplus, \odot)$称为 R **关于理想 H 的商环**.

例 7.2.7 当 $n\geqslant 2$ 时，$\mathbf{Z}_n$ 为 $\mathbf{Z}$ 关于理想 $n\mathbf{Z}$ 的**商环**.

例 7.2.8 考虑定义在整数交换环 $\mathbf{Z}$ 上的一元多项式环$(\mathbf{Z}[x], +, \times)$，求 $\mathbf{Z}[x]/(x)$.

解 我们在多项式中省略运算符“×”．则由多项式 x 生成的理想

$$(x) = \{xf(x) \mid f(x)\in \mathbf{Z}[x]\},$$

易知(x)是所有常数项为 0 的一元多项式.

对任意一元多项式 $z(x)\in \mathbf{Z}[x]$，设 $z(x)$的常数项为 $\boldsymbol{a}$($a\in \mathbf{Z}$)，则集合(陪集)

$$[z(x)] = z(x)+(x) = \{z(x) + xf(x) \mid xf(x)\in(x)\}$$

是商环 $\mathbf{Z}[x]/(x)$中的一个元素，显然陪集$[z(x)]$由一系列 $\mathbf{Z}[x]$中的一元多项式组成，$[z(x)]$中各个多项式的共同特点是它们的常数项都是 a，即对任意多项式 $p(x)\in[z(x)]$，都有

$$p(x)-a\in(x),$$

所以

$$[z(x)] = [a] = a+(x).$$

即陪集$[z(x)]$和陪集$[a]$中的元素一样都是一元多项式且该一元多项式与整数 a 的差是理想(x)中的元素（常数项为 0 的一元多项式）．于是我们有商环

$$\mathbf{Z}[x]/(x) = \{[a] \mid a\in \mathbf{Z}\}.$$

例 7.2.9 考虑定义在整数交换环 $\mathbf{Z}$ 上的一元多项式环$(\mathbf{Z}[x], +, \times)$，求 $\mathbf{Z}[x]/(m)$（$2\leqslant m\in\mathbf{N}$）.

解 由 m 生成的理想为

$$(m) = \{mf(x) \mid f(x)\in \mathbf{Z}[x]\},$$

它的元素是系数为 m 倍数的多项式．因此，当求得两个一元多项式 $p_1(x)$和 $p_2(x)$的差 $p(x)=p_1(x)-p_2(x)$后，如果 $p(x)$的系数为 m 的倍数，那么下面的两个陪集相等

$$[p_1(x)] = [p_2(x)],$$

所以

$$\mathbf{Z}[x]/(m) = \{[c_n x^n + \cdots + c_0] \mid 0\leqslant c_i < m, 1\leqslant i\leqslant n, n\in\mathbf{N}\},$$

它同构于整数模 m 的剩余类环 $\mathbf{Z}_m$ 上的一元多项式环，即 $\mathbf{Z}[x]/(m)\cong\mathbf{Z}_m[x]$（请读者证明该结论）.

下面给出关于环同态的这两个重要定理，它们是群理论中相应定理在环上的延伸.

定理 7.2.7 如果 H 是交换环$(R, +, \cdot)$的理想，则如下定义的映射 f: $R\to R/H$,

$$f(a) = a + H$$

是核为 H 的同态映射(该同态称为**自然同态**).

证明　定理 4.2.16 已经证明 R/H 是一个交换环，下面只需验证同态的三个条件.

$f(1) = 1 + H$, 所以同态定义中条件(1)满足；

$f(a)\oplus f(b)= (a+H)\oplus(b+H) =(a + b)+H= f(a + b)$, 所以同态定义中条件(2)满足；

$f(a)\odot f(b)= (a+H)\odot(b+H) =(a \bullet b)+H= f(a \bullet b)$, 所以同态定义中条件(3)满足；

因此, f 是同态映射.

由于 $\ker f=\{ a \mid f(a) =0+H= H,\ a\in R \}$, 所以对任意 $a\in H$, 则 $f(a) = a + H= H$, 得到 $a\in \ker f$, 从而 $H\subseteq \ker f$; 反过来，对任意 $a\in \ker f$, 则 $a + H= f(a) = H$, 得到 $a\in H$, 从而 $\ker f\subseteq H$, 所以 $\ker f=H$.

定理 7.2.8（环的同态基本定理）　设 $f:S\to G$ 是交换环 S 到交换环 G 的同态映射，则存在 $S/\ker f$ 到 $\operatorname{im} f$ 的映射

$$h: S/\ker f \to \operatorname{im} f,$$

使得 $S/\ker f \cong \operatorname{im} f$.

本定理的证明类似于群的同态基本定理，这里不再赘述，只要令 $h(a+ \ker f)= f(a)$, 读者即可自行证明.

习题 7.2

A 组

1. 证明环的同态基本定理，给出完整证明过程.
2. 试在 **Z** 内以环 n**Z** 的形式定义整除、同余、最大公倍数、最小公因子.
3. 给出商环 **Z** $[u]/<x^2+x+1>$中的加法、乘法定义.
4. 证明定理 7.2.3.

B 组

5. $u=\sqrt{2}+\sqrt{5}$, 证明：u 在 **Q** 上是代数的，并求出 **Q** $[x]$中理想 I 使得 **Q** $[u] \cong$ **Q** $[x]/I$.
6. 设 f 是环 R 到环 R'的同态映射，K=ker f, 则:

(1)建立了 R 中包含 K 的子环与 R'的子环的一一对应；

(2) f 把理想映射为理想；

(3)若 I 是的理想且 $K\subseteq I$, 则 $R/I \cong R'/f(I)$.

7.3 几类重要的环

在这一节中，我们讨论三类重要的环——唯一析因环，主理想整环与 Euclid（欧几里得）环.

1. 唯一析因环

在整数环 **Z** 中，我们通常考虑可除性、因式分解等问题. 在这部分中，我们将主要讨论交换整环上的因式分解理论.

设 R 是交换整环，U 为 $R^*=R\backslash\{0\}$中可逆元素的集合，易证明 U 是一个 Abel 群，称为 R

的**单位群**，其中的元素称为 R 的**单位**.

定义 7.3.1 设 $a,b\in R^*$，若 $\exists\ c\in R^*$ 使得 $b=ac$，则称 a **整除** b，或 a 是 b 的**因子**，记为 $a|b$. 否则称 a 不整除 b，记为 $a\nmid b$.

定理 7.3.1 (1) $\forall\ a\in R^*, a|a$.

(2) 若 $a|b$ 且 $b|c$，则 $a|c$.

(3) $\forall u\in U, a\in R$ 有 $u|a$.

(4) $u\in U$ 当且仅当 $u|1$.

证明: (1)和(2)显然. 对于(3)和(4)，我们取 $\forall u\in U$，则存在 $u^{-1}\in U$ 使得 $uu^{-1}=1$，再利用根据定义容易证明.

定义 7.3.2 设 $a,b\in R^*$ 且 $a|b, b|a$，则称与**相伴**，记作 $a\sim b$.

定理 7.3.2 (1) $a\sim b$ 当且仅当 $\exists u\in U$ 使得 $b=au$.

(2)若 $a\sim b$ 且 $c\sim d$，则 $ac\sim bd$.

(3) $u\in U$ 当且仅当 $u\sim 1$.

证明: (1)若 $a\sim b$，则存在 $c,d\in R^*$ 使得 $a=bc, b=ad$，从而 $b=b(dc)$ 进而 $dc=1$，故 $c,d\in U$. 反之，若 $b=au$ 则有 $a=auu^{-1}=bu^{-1}$，又 $a|b$，故 $a\sim b$.

(2)设 $u,v\in U$ 使得 $b=au, d=cv$，则 $bd=acuv$. 又容易验证 $uv\in U$，故 $ac\sim bd$.

(3)证明略.

例 7.3.1 整数环 $\mathbf{Z}$ 的单位群为{1, -1}，高斯整数环 $\mathbf{Z}[i]$ 的单位元为{1, -1, i, $-i$}

例 7.3.2 实数域 $\mathbf{R}$ 上的一元多项式环 $R[x]$ 的单位群为整环 $\mathbf{R}$ 的单位群，$f(x)\sim g(x)$ 当且仅当存在 $c\in \mathbf{R}^*=\mathbf{R}\setminus\{0\}$ 使得 $f(x)=cg(x)$.

例 7.3.3 考虑交换整环 $\mathbf{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}|a,b\in\mathbf{Z}\}$，对于任意 $\alpha=a+b\sqrt{-5}$，给定范数 $\mathrm{N}(\alpha)=a^2+5b^2$. 易知 $\mathrm{N}(\alpha)\geq 0$, $\mathrm{N}(\alpha\beta)=\mathrm{N}(\alpha)\mathrm{N}(\beta)$.

考虑 $\mathbf{Z}[\sqrt{-5}]$ 的单位群 U，对于 $\alpha\in U$ 存在 $\alpha^{-1}\in U$ 使得 $\alpha\alpha^{-1}=1$. 进而 $1=\mathrm{N}(1)=\mathrm{N}(\alpha\alpha^{-1})=\mathrm{N}(\alpha)\mathrm{N}(\alpha^{-1})=\mathrm{N}(\alpha)^2$，从而 $\mathrm{N}(\alpha)=1$，易知 $U=\{-1,1\}$.

定义 7.3.3 设 $a,b\in R^*$，若 $b|a$ 且 $a\nmid b$，则称 b 是 a 的**真因子**. 设 $a\in R^*\setminus U$，若 a 无非平凡的真因子，则称 a 为**不可约元素**，否则称之为**可约元素**.

定义 7.3.4 设 $p\in R^*\setminus U$ 满足：$p|ab \Rightarrow p|a$ 或 $p|b$，则称 p 为**素元素**.

定理 7.3.3 素元素是不可约元素.

证明: 若 a 是素元素 p 的一个因子即 $a|p$，则存在 $b\in R^*$ 使得 $p=ab$，因而 $p|a$ 或 $p|b$. 若 $p|a$，则 a 不是 p 的真因子. 若 $p|b$，则有 $c\in R^*$ 使得 $b=pc$，于是 $p=pac$，所以 $ac=1$，故 a 为平凡因子. 所以, p 没有非平凡的真因子，是不可约元素.

值得指出的是，不可约元素不一定是素元素.

例 7.3.4 在交换整环 $\mathbf{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}|a,b\in\mathbf{Z}\}$ 中，我们已知其单位群为 $U=\{-1,1\}$. 通过例题 7.3.3 范数的定义，易验证 3 是不可约元素. 但是, $3|9=(2+\sqrt{-5})(2-\sqrt{-5})$，但 $3\nmid 2+\sqrt{-5}$ 且 $3\nmid 2-\sqrt{-5}$，故 3 不是素元素.

定义 7.3.5 若环 R 中，不可约元素都是素元素，则称 R 满足**素性条件**.

定义 7.3.6 设 $b,c\in R^*$.若 $d\in R^*$ 满足 $d|b$ 且 $d|c$，则称 d 为 b,c 的**公因子**. 若对的任意公因子 d_1，有 $d_1|d$，则称 d 为 b,c 的**最大公因子**，记为(b,c).

若 R^* 的任意两个元素的最大公因子存在，则称 R 满足**最大公因子条件**.

定理 7.3.4 若 R 满足最大公因子条件，则有：

(1)若 d_1, d 均为 b,c 的最大公因子，则 $d_1\sim d$，即最大公因子在相伴的意义下唯一，记为(b,c).

(2) $R^*\setminus U$ 中任意有限个元素均有最大公因子 c.

(3) $((a, b),c)=(a, (b,c))$

(4) $c(a,b) = (ca,cb)$.

(5)若$(a, b)=1$(称为 a, b **互素**), $(a, c)=1$，则$(a, bc)=1$.

证明：按照最大公因子的定义即可，具体步骤留给读者.

定义 7.3.7 如果交换整环 R 满足如下条件：

(1)$\forall a \in R^*\backslash U$，可分解为有限个不可约元素的乘积，即有不可约元素 $p_i(1\le i\le r)$使得 $a = p_1p_2\cdots p_r$；

该条件称为**有限析因条件**.

(2)若$a \in R^*\backslash U$ 有两种不可约元素的分解：$a = p_1p_2\cdots p_r = q_1q_2\cdots q_s$，则有 $r=s$ 且存在置换$\pi \in S_r$使得$p_i = q_{\pi(i)}$. 那么称为**唯一析因环**或**高斯环**，记为 **UFD**.

直观地讲，唯一析因环是使唯一分解定理成立的交换整环. 整数环 **Z** 以及多项式环 **Z** $[x]$ 都是唯一析因环，但 **Z** $[\sqrt{-5}]$不是唯一析因环，因为 $9=(2+\sqrt{-5})(2-\sqrt{-5})=3 \cdot 3$ 是两种不同的分解（注意到 $2+\sqrt{-5}$, $2-\sqrt{-5}$均与 3 不相伴）.

下面给出唯一析因环的一些等价条件.

定义 7.3.8 R^*中的一个序列$a_1, a_2, \cdots, a_n, \cdots$满足$a_{i+1}|a_i$（$i=1,2,\cdots$），则称之为 R^*的一个**因子链**.

若 R^*中的任意一个因子链$a_1, a_2, \cdots, a_n, \cdots$，存在自然数 m 使得$a_n \sim a_m, \forall n \ge m$，则称 R^*满足**因子链条件**.

定理 7.3.5 若交换整环 R 满足因子链条件，则必满足有限析因条件.

证明：设$a \in R^*\backslash U$. 先说明a有不可约因子，不妨设a是可约的，则有非平凡的真因子a_1，即有$a = a_1b_1$. 此时b_1也是a的非平凡因子. 若有a_1, b_1都可约，则$a_1 = a_2b_2$，其中a_2, b_2为a_1的真因子，如此继续，可得因子链$a_1, a_2, \cdots, a_n, \cdots$且$a_{i+1}|a_i$. 由因子链条件有 m 使得 $a_{m+1} \sim a_m$，因而a_m是不可约的，即是a的不可约因子.

下面说明a可分解为有限多个不可约因子的乘积. 设p_1是a的一个不可约因子，于是 $a = p_1a'$. 若$a' \in U$，则完成证明. 若$a' \in R^*\backslash U$，则有不可约因子p_2，即$a = p_1p_2a''$. 继续上述过程，可得因子链$a, a', a'', \cdots, a^{(n)}, a^{(n+1)}\cdots$

于是有 s，使得$a^{(s)} \sim a^{(s-1)}$. 此时$a^{(s-1)} = p_s$一定是不可约的，故$a = p_1p_2\cdots p_s$ 即 R 满足有限析因条件.

定理 7.3.6 若 R 是交换整环，则下列条件等价：

(1) R 唯一析因环.

(2) R 满足因子链条件和素性条件.

(3) R 满足因子链条件和最大公因子条件.

证明：略，留给读者完成，过程可参照定理 7.3.5 证明.

2. 主理想整环

我们曾经讨论过，由一个元素生成的理想$\langle a\rangle$叫作主理想.

若是 R 交换幺环，则$\langle a\rangle= aR= Ra=\{xa|x\in R\}$

定义 7.3.9 若交换幺环的每个理想都是主理想，则称该环为**主理想环**. 若主理想环是整环，则称之为**主理想整环**.

例 7.3.4 整数环 **Z** 是主理想整环.

实际上，设 I 是 **Z** 的一个非平凡理想，存在 $m \in I$ 使得 $m= \min\{|k|| k \in I, k \neq 0\}I$. 容易验证易知 $I=\langle m\rangle$，故 **Z** 是主理想整环.

例 7.3.5 整数环上的一元多项式环 **Z** $[x]$不是主理想整环.

实际上，考虑由 2，x^2+1 生成的理想$\langle 2, x^2+1\rangle$. 若 **Z** $[x]$是主理想整环,则存在 $f(x) \in$ **Z** $[x]$

使得$<f(x)>=<2, x^2+1>$，进而$f(x)|\,2$, $f(x)|\,x^2+1$，故$f(x)=\pm 1$，从而$<f(x)>= \mathbf{Z}[x]$. 但$<2, x^2+1>$是非平凡理想，进而矛盾.

定理 7.3.7 若 R 是交换整环：

(1) $a|b$ 当且仅当$<a>\supseteq<b>$.

(2) $a\sim b$ 当且仅当$<a>=<b>$.

(3) $a\sim 1$ 当且仅当$<a>=<1>=R$.

(4) R 满足因子链条件当且仅当 R 满足**主理想的升链条件**，即任一主理想升链

$$< a_1 >\subseteq< a_2 >\subseteq \cdots \subseteq< a_n >\subseteq< a_{n+1} >\subseteq \cdots$$

一定存在m使得当$n \geq m$时，有$< a_m >=< a_n >$.

证明：按照整除、相伴的定义，略.

定理 7.3.8 主理想整环是唯一析因环.

证明：根据上一节唯一析因环等价关系，只需证明主理想整环满足主理想升链条件和最大公因子条件. 设

$$< a_1 >\subseteq< a_2 >\subseteq \cdots \subseteq< a_n >\subseteq \cdots$$

是 R 中的一个主理想升链. 令$I = \bigcup_{i=1}^{\infty} < a_i >$. 若 $a,b \in I$则存在正整数 i,j 使得 $a \in< a_i >,b \in < a_j >$. 不妨设$j \geq i$，则有 $a\text{-}b \in< a_i >\subseteq I$，故是 R 的加法子群，又易证$\forall c \in R$有$ac \in< a_i > \subseteq I$，故$I$是$R$的理想. 进而存在$d \in R$使得$I =< d >$. 因$d \in I$，存在正整数$m$使得$d \in< a_m >$，因而$n \geq m$时有

$$I =< d >\subseteq< a_m >\subseteq< a_n >\subseteq \bigcup_{i=1}^{\infty} < a_i > = I$$

即$< a_m >=< a_n >= I$，即满足主理想升链条件.

其次，设 $a,b \in R^*$. 显然$<a>+<b>$是 R 中的理想. 故存在$d \in R$使得$<a>+<b>=<d>$，因而有$<a>\subseteq<d>$，$<b>\subseteq<d>$，即 $d|a$，$d|b$，即 d 为 a,b 的公因子. 如果$c|a$，$c|b$，则有$< a >\subseteq< c >, < b >\subseteq< c >$，故$<d>=<a>+<b>$，即有$c|d$，故 d 为 a,b 的最大公因子.

综上可知 R 是唯一析因环.

定理 7.3.9 若 R 是交换整环：

(1)若 d 为 a,b 的最大公因子，则有 $u,v \in R$ 使得 $d=au+bv$.

(2) a,b 互素当且仅当$\exists u, v \in R$使得 $au+bv=1$.

证明：该定理为上一定理的直接推论，证明略.

3. 欧几里得（Euclid）环

我们比较熟悉整数环 $\mathbf{Z}$ 上的带余除法，该除法也叫作 Euclid 辗转相除法. 下面我们主要讨论交换整环中的欧几里得辗转相除法，以及具有这种性质的环.

定义 7.3.10 设 R 是交换整环. 若存在 R 到非负整数集 $\mathbf{Z}^+\cup\{0\}$上的映射δ，使得对$\forall a,b \in R$，$b \neq 0, \exists q, r \in R$，满足

$$a=qb+r, \qquad \delta(r) < \delta(b) \qquad ※$$

则称为**欧几里得（Euclid）环**.

例 7.3.6 整数环 $\mathbf{Z}$ 是欧几里得环，令$\delta(a) = |a|$即可.

例 7.3.7 高斯整数环 $\mathbf{Z}[i]=\{a + bi \mid a, b\in \mathbf{Z}\}$是 Euclid 环.

实际上，令$\delta(a + bi)=a^2+b^2$，则容易验证

$$\delta(\alpha\beta) = \delta(\alpha)\,\delta(\beta), \forall \alpha, \beta \in \mathbf{Z}[i]$$

设$\beta \neq 0$，则有$\beta^{-1} \in \mathbf{Q}[i]$，即有

$$\alpha\beta^{-1} = \mu + \nu i, \mu, \nu \in \mathbf{Q}.$$

于是$\exists c,d\in \mathbf{Z}$，使得$|c-\mu|\le\frac{1}{2}$, $|d-\nu|\le\frac{1}{2}$. 令$\varepsilon=\mu-c,\eta=\nu-d$，则有$|\varepsilon|\le\frac{1}{2}$, $|\eta|\le\frac{1}{2}$，而

$$\alpha=\beta((c+\varepsilon)+(d+\eta)i)=\beta q+r,$$

其中$q=c+di\in\mathbf{Z}[i]$，$r=\beta(\varepsilon+\eta i)=\alpha-\beta q\in\mathbf{Z}[i]$. 又

$$\delta(r)=|r|^2=\delta(\beta)(\varepsilon^2+\eta^2)|\le\delta(\beta)\left(\frac{1}{4}+\frac{1}{4}\right)<\delta(\beta),$$

故$\mathbf{Z}[i]$是欧几里得环.

定理 7.3.10 欧几里得环是主理想整环.

证明：设I是欧几里得环 R 的一个理想. 若$I=\{0\}$，显然是主理想，故假设$I\neq 0$. 取I中元素 b 使得

$$\delta(b)=\min\{\delta(c)|c\in I,c\neq 0\}$$

设 $a\in I$，则存在$q,r\in R$使得欧几里得辗转相除式※成立. 因 $a,b\in I$，故 $r=a-qb\in I$. 由 b 的取法知 $r\notin I\backslash\{0\}$. 故 $r=0$，因而 $a\in<b>$，故$I=<b>$，即 R 为主理想整环.

推论 欧几里得环是唯一析因环.

证明：由定理 7.3.8 和定理 7.3.10 可得.

值得指出的是，在欧几里得环中，可以利用※式进行辗转相除法对两个元素求最大公因子：反复利用※式，当有限步后$\delta(r)=0$ 时停止，此时的 b 即为最大公因子.

习题 7.3

A 组

1. 设 R 为主理想整环，I是 R 的非零理想，试证：
   (1) R/I 的每个理想都是主理想
   (2) R/I 中仅有有限多个理想.
2. 设 R 为交换整环，但不是域. 证明：$R[x]$不是主理想整环.
3. 在高斯整环中，对 2,3,5,7 进行素元素分解.
4. 证明 $R=\{a+\frac{b}{2}(1+3\mathrm{i})\,|\,a,b\in\mathbf{Z}\}$ 是欧几里得环.

B 组

5. 设 R 为欧几里得环且$\delta(ab)=\delta(a)\delta(b)$，证明：$a\in U$当且仅当$\delta(a)=1$.
6. 证明：任何一个域都是欧几里得环.
7. 证明定理 7.3.6.

7.4 素理想和极大理想

本节我们将主要讨论环的两类重要的理想——素理想与极大理想. 这两类理想将通过商环的概念，对应于整环与域，进而引出下一章域的相关内容.

定义 7.4.1 交换幺环 R 的理想 P 满足：

（1）$P\neq R$ ；

（2）若$ab\in P$，则$a\in P$或$b\in P$，

则 P 称为 R 的**素理想**.

定义 7.4.2 交换幺环 R 的理想 M 满足：

（1） $M\neq R$ ；

（2） 不存在理想 A 使得$M\subset A\subset R$

则 M 称为 R 的**极大理想**.

例 7.4.1 考虑整数环 $\mathbf{Z}$，易知$\langle p\rangle = p\mathbf{Z}$ 是 $\mathbf{Z}$ 的素理想，同时也是其极大理想.

设 $ab\in p\mathbf{Z}$，则有 $p|ab$. 因为是 p 素数，故 $p|a$或 $p|b$， $a\in p\mathbf{Z}$ 或 $b\in p\mathbf{Z}$，从而素理想.

此外，因为 $\mathbf{Z}$ 是主理想整环，所以若 $p\mathbf{Z}$ 不是极大理想，一定包含在一个主理想 $n\mathbf{Z}$ 中，从而 $n|p$, n=1,p，矛盾.

例 7.4.2 考虑多项式环 $\mathbf{Z}[x]$，若 $p(x)$是不可约多项式，则$\langle p(x)\rangle=\{ f(x)\in$□$[x]$ $|p(x)$整除 $f(x)\}$是 $\mathbf{Z}$ 的素理想，同时也是其极大理想. 证明类似于上题，略.

定理 7.4.1 设 R 为交换幺环

(1) R 是整环当且仅当$\{0\}$是 R 的素理想.

(2) R 是域当且仅当$\{0\}$是 R 的极大理想.

证明：(1)设 R 是整环，若$a\neq 0, b\neq 0$即$a\notin\{0\}$且$b\notin\{0\}$，则$ab\neq 0$,即$ab\notin\{0\}$，故$\{0\}$是 R 的素理想.

反义，若$\{0\}$是 R 的素理想，$a\notin\{0\}$且$b\notin\{0\}$故$ab\notin\{0\}$，即由$a\neq 0, b\neq 0$可得$ab\neq 0$，故 R 是整环.

(2)设$\{0\}$是 R 的极大理想，对$\forall a\in R$且$a\neq 0$,有$\{0\}\subset\langle a\rangle$，故$\langle a\rangle=R$. R 有含幺元 1，进而 $1\in\langle a\rangle$，故$\exists a^{-1}\in R$使得$aa^{-1}=1$，故 R 是域.

反之，若 R 是域，A 是 R 的理想且 $A\neq\{0\}$，即$\exists\, a\in A$ 且$a\neq 0$. 又因为是域，故$\exists a^{-1}\in R$使得$aa^{-1}=1\in A$. $\forall b\in R$有$b=b\cdot 1\in A$，因而 $A=R$, $\{0\}$是 R 的极大理想.

定理 7.4.2 设 R 为交换幺环，P与M为 R 的理想

(1)R/P是整环当且仅当P是素理想.

(2)R/M是域当且仅当M是极大理想.

证明：(1)设π为 R 到 R/P上的自然同态，若P是素理想，设$\pi(a)\neq 0, \pi(b)\neq 0$即$a,b\notin P$，则$ab\notin P$，即$\pi(ab)=\pi(a)\pi(b)\neq 0$，故 R/P是整环.

反之，设 R/P是整环且$ab\in P$，则有$\pi(ab)=\pi(a)\pi(b)=0$，因而$\pi(a)=0$或$\pi(b)=0$，即$a\in P$或$b\in P$，故P是素理想.

(2)设 R 的理想 A 满足$M\subset A\subset R$，可以证明A/M是R/M的理想. 当M为极大理想时，有$M=A$或$R=A$. 故 R/M仅有的理想为$\{0\}$与 R/M本身，$\{0\}$是 R/M的极大理想，由定理 7.4.1，故 R/M是域.

反义，R/M是域，由定理 7.4.1，$\{0\}$是 R/M的极大理想. 从而，若$M\neq A$，则$A/M=R/M$，故$A=R$，故M是极大理想.

此外，由于域是整环，我们有如下推论.

推论 交换幺环的极大理想是素理想.

至此，我们给出环与其理想、商环的一类性质，说明了素理想、极大理想的应用，也给出了一种由已知的环构造域的方法.

例 7.4.3 考虑整数环 $\mathbf{Z}$，$\langle p\rangle = p\mathbf{Z}$ 是 $\mathbf{Z}$ 的素理想，也是其极大理想. 故 $\mathbf{Z}_p$ 是整环，同时是域，且域的元素有限，共 p 个.

例 7.4.4 考虑多项式环 $\mathbf{Z}[x]$，$p(x)$是 $\mathbf{Z}[x]$ 中一不可约多项式，则$\langle p(x)\rangle$是素理想，同时也是极大理想，进而 $\mathbf{Z}[x]/\langle p(x)\rangle$ 是整环，同时是域.

例 7.4.5 考虑多项式环 $\mathbf{Z}_p[x]$, $p(x)$是 $\mathbf{Z}_p[x]$ 中一不可约多项式，则$\langle p(x)\rangle$是素理想，同时

也是极大理想，进而 $\mathbf{Z}_p[x]$ / <$p(x)$> 是整环，同时是域. 该域的元素有限，共 p^n 个，其中 n=deg $p(x)$，为 $p(x)$的次数.

例 7.4.6 构造由 4 个元素构成的域.

取有限域 $\mathbf{Z}_2$，构造其上的多项式环 $\mathbf{Z}_2[x]$. 易验证 x^2+x+1 是 $\mathbf{Z}_2[x]$中不可约多项式，进而< x^2+x+1>构成极大理想，从而 $\mathbf{Z}_2[x]$ /< x^2+x+1>构成域，共有四个元素：0,1, x, $x+1$. 其加法和乘法的群表如下.

加法	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

乘法	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

定理 7.4.4 设 R, R'为交换幺环，σ是 R 到 R'上的同态，且$N=\ker\sigma$. 若 H 是 R 中包含N的素理想（或极大理想），则 H'是 R'中的素理想（或极大理想）. 反之，若$\sigma(H)$是 R'素理想（或极大理想），则$\sigma^{-1}(H')=\{x\in R|\sigma(x)\in H'\}$是 R 中包含N的素理想（或极大理想）.

证明: 有环的同态基本定理知$R\backslash H\cong R'\backslash\sigma(H)$，由 7.2 节习题 5 的结论，可知 H 为包含N的素理想（或极大理想）当且仅当$\sigma(H)$是素理想（或极大理想）.

定理 7.4.5 设 R 为交换整环, $a\in R^*$, 则由 a 生成的主理想< a >为素理想当且仅当 a 为素元素.

证明: 显然，当且仅当 a 为 R 的单位，即 $a\in U$ 时, < a >=R, 故设 $a\in R^*\backslash U$. 由 $bc\in$< a >$\Leftrightarrow$ $a|bc$，因而< a >为素理想当且仅当 a 为素元素.

我们知道素元素一定是不可约元素，反之不一定成立. 但是在唯一析因环中，两个概念是等价的. 因而以上定理对于唯一析因环与其不可约元素仍旧成立.

定理 7.4.6 设 R 为主理想整环, $a\in R^*$, 则< a >为极大理想当且仅当 a 为素元素.

证明：若< a >为极大理想，则为素理想，进而由上一定理知 a 为素元素.

反之，若 a 为素元素. 若有 R 的理想 A 使得< a >$\subseteq A\subseteq R$, 由于 R 为主理想整环，固有 $n\in R$ 使得 A=< n >. 于是 $n\,|a$. 由 a 为素元素即不可约元素知 $n\sim 1$或 $n\sim a$，即 A=< n >=R 或 A=< n >=< a >. 故< a >为极大理想.

定理 7.4.7 设 F 是一个域, R 是交换整环且 $F\subseteq R$，F, R 具有相同的幺元, u 是 R 上的代数元，则存在 F 上的不可约多项式 $p(x)$=Irr(u, F)，使得

$$F[u]\cong F[x]/<p(x)>$$

且构成域。

证明：设 $I=\{f(x)\,|\,f(x)\in F[x], f(u)=0\}$，根据定理 8.1.1 知 F [x]是 Euclid 环，进而使主理想整环，从而可证明存在 $p(x)\in F[x]$ 使得 $I=<p(x)>\bigcap F=\{0\}$.

由于是整环，故可知 F [u]也是整环. 另外，由环的同态基本定理可知

$$F[u]\cong F[x]/p(x)$$

从而 $F[x]/p(x)$是整环，由定理 7.4.2 知< $p(x)$ > 为素理想，进而由定理 7.4.5 知 $p(x)$ 为素

元素，从而可进一步验证 $p(x)$ 恰为代数元 u 在 F 上的不可约多项式 $\mathrm{Irr}(u, F)$. 有定理 7.4.6 以及是主理想整环可知，$< p(x) >$ 为极大理想，从而 $F[u] \cong F[x]/p(x)$ 是一个域.

值得指出的是，上述定理给出了一个有限域的直接构造方法. 我们将在下一章介绍域扩张时，多次利用到类似的结论.

习题 7.4

A 组

1. 设试证 $\langle x \rangle$ 是 $\mathbf{Z}[x]$ 的素理想，但不是极大理想.
2. 试构造由 9 个元素构成的域.
3. 试构造由 8 个元素构成的域.
4. 证明：在无限的主理想整环中，若可逆元有限，则素理想有无穷多个.

B 组

5. 证明 $\mathbf{Z}_p[x]$ 中有无限多个不可约因式.

6. （中国剩余定理）若 R 的理想 I,J 满足 $I+J=R$，则称 I,J 互素. $I_1, \dots, I_n$ 是 R 中两两互素的理想，证明：

$$R/\bigcap_{i=1}^{n} I_i \to R/I_n \times \dots \times R/I_n$$

是同构映射.