第 7 章 环和域

实数或复数系统包含两个基本的二元运算：加法和乘法。群论仅仅处理一个二元运算，更没有涉及两个二元运算之间的关系——乘法对加法的分配律。本章将介绍一种新的代数结构——环和域。

7.1 环的定义

定义 7.1. 在具有两个二元运算加法$+$和乘法$\bullet$的集合R中，如果

(1) $\langle R, +\rangle$是交换群;

(2) $\langle R, \bullet\rangle$是含幺半群；

(3) 乘法对加法有左、右分配律，即对任意的三个元素$a, b, c \in R$，都有

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

则称$\langle R, +, \bullet\rangle$为**环**。

如果在环$\langle R, +, \bullet\rangle$中，对任意的两个元素$a, b \in R$，都有$a \bullet b = b \bullet a$，则称该环是交换环。

从环的定义中可以看出，环中的两个运算$+$和$\bullet$的地位是不同的。集合R对$+$构成交换群，而对$\bullet$只构成含幺半群。加法运算的单位元称为零元，记为0；乘法运算的单位元称为乘法单位元，记为1。R中的任意元素$a \in R$都有加法逆元，称为负元，记为$-a$；但不一定都有乘法逆元。有乘法逆元的元素称为环中的可逆元。

下面是环的几个例子。

例 7.1. $\langle \mathbb{R}, +, \bullet\rangle$，$\langle \mathbb{C}, +, \bullet\rangle$和$\langle \mathbb{Q}, +, \bullet\rangle$分别是实数环、复数环和有理数环，其中$+$和$\bullet$运算是普通的加法和乘法运算。这些环统称为数环。

例 7.2. 全体n阶整数方阵$M_n(\mathbb{Z})$对矩阵加法和矩阵乘法构成n阶矩阵环$\langle M_n(\mathbb{Z}), +, \bullet\rangle$。全部元素都为*0*的$n$阶方阵为零元，$n$阶单位矩阵为乘法单位元，该环是非交换环。

例 7.3. $\langle G, +\rangle$是交换群，$E = \{f | f : G \to G$ 是同态映射$\}$。在E上定义二元运算$+$和$\cdot$如下：对E中的任意两个映射f, g，以及任意的$x \in G$，

$$(f + g)(x) = f(x) + g(x),$$
$$(f \cdot g)(x) = f(g(x)).$$

证明$\langle E, +, \cdot\rangle$是环，被称为交换群$G$上的自同态环。

证明： 对于任意的$f, g \in E$，以及$x \in G$，定义$(f+g)(x) = f(x)+g(x)$。显然，$f + g$是G上的映射。由于f和g都是G上的自同态映射，所以有

$$\begin{aligned}(f + g)(x + y) &= f(x + y) + g(x + y)\\ &= (f(x) + f(y)) + (g(x) + g(y))\\ &= (f(x) + g(x)) + (f(y) + g(y))\\ &= (f + g)(x) + (f + g)(y).\end{aligned}$$

可见，$f + g$保持加法运算，因此$f + g$是G上的自同态映射，即$f + g \in E$。由于$\langle G, +\rangle$是交换群，所以E中的$+$运算满足结合律和交换律。令$f_0 : G \to G$，对任意的$x \in G$，$f_0(x) = 0_G$，其中0_G是交换群$\langle G, +\rangle$的零元。显然，f_0是E的零元。对于E中的任意元素$f : G \to G$，定义$f_- : G \to G$，对任意的$x \in G$，$f_-(x) = -f(x)$。易见f_-是f的负元。综上所述可知，$\langle E, +\rangle$是交换群。

对于任意的$f, g \in E$，以及$x \in G$，定义$(f \cdot g)(x) = f(g(x))$。显然，$f \cdot g$是G上的映射。由于f和g都是G上的自同态映射，所以有

$$\begin{aligned}(f \cdot g)(x + y) &= f(g(x + y)) = f(g(x) + g(y))\\ &= f(g(x)) + f(g(y)) = (f \cdot g)(x) + (f \cdot g)(y).\end{aligned}$$

可见，$f \cdot g$保持加法运算，因此$f \cdot g$是G上的自同态映射，即$f \cdot g \in E$。映射的复合运算满足结合律。令$f_1 : G \to G$，对任意的$x \in G$，$f_1(x) = x$。显然，f_1是E的乘法单位元。综上可知，$\langle E, \cdot\rangle$是含幺半群。

对任意的$f, g, h \in E$和$x \in G$，有

$$\begin{aligned}(f \cdot (g + h))(x) &= f((g + h)(x)) = f(g(x) + h(x))\\ &= f(g(x)) + f(h(x)) = (f \cdot g + f \cdot h)(x).\end{aligned}$$

$$((g+h)\cdot f)(x) = (g+h)(f(x)) = g(f(x) + h(f(x))$$
$$= (g\cdot f + h\cdot f)(x),$$

即$f\cdot(g+h) = f\cdot g + f\cdot h$，$(g+h)\cdot f = g\cdot f + h\cdot f$，$\cdot$对$+$满足左、右分配律。因此，$\langle E, +, \cdot\rangle$是环，并且是非交换环。证毕。

例 7.4. 在$\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$上定义

$$[i] + [j] = [i+j],$$
$$[i]\cdot[j] = [i\cdot j].$$

易证如此定义的同余类加法和乘法与代表元的选取无关，即当$[i_1] = [i_2]$，$[j_1] = [j_2]$，则$[i_1 + j_1] = [i_2 + j_2]$，$[i_1 \cdot j_1] = [i_2 \cdot j_2]$。显然，$\langle \mathbb{Z}_n, +\rangle$是交换群，其中$[0]$为零元，$[-i]$是$[i]$的负元；$\langle \mathbb{Z}_n, \cdot\rangle$是含幺半群，其中$[1]$为乘法单位元。此外，$\cdot$ 对$+$ 满足左、右分配律。注意到$\mathbb{Z}_n$中的$\cdot$满足交换律，因此，$\langle \mathbb{Z}_n, +, \cdot\rangle$是环，而且是交换环，被称为模$n$同余类环。

从环的定义知，$\langle R, +\rangle$是交换群，满足左、右消去律。因此，

$$x + a = a \Rightarrow x = 0,$$
$$a + x = 0 \Rightarrow x = -a,$$
$$a + b = a + c \Rightarrow b = c.$$

对环的两个运算$+$和$\cdot$，有以下结论。

定理 7.1. 在环$\langle R, +, \cdot\rangle$中，0和1分别是零元和乘法单位元。对于$R$中的任意元素$a$和$b$，有

(1) $a\cdot 0 = 0\cdot a = 0$；

(2) $a\cdot(-b) = (-a)\cdot b = -(a\cdot b)$，特别地，$(-1)\cdot a = -a$；

(3) $(-a)\cdot(-b) = a\cdot b$，特别地，$(-1)\cdot(-1) = 1$。

证明： (1) $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$，由消去律得到$a\cdot 0 = 0$。同理可证，$0\cdot a = 0$。

(2) $a \cdot (-b) + a \cdot b = a \cdot ((-b) + b) = a \cdot 0 = 0$，因此$a \cdot (-b) = -(a \cdot b)$。同理可证，$(-a) \cdot b = -(a \cdot b)$。特别地，取$b = 1$，即得$(-1) \cdot a = -a$。

(3) $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$。特别地，取$a = b$，即有$(-1) \cdot (-1) = 1$。证毕。

在环$\langle R, +, \cdot \rangle$中，如果零元$0_R$等于乘法单位元$1_R$，即$0_R = 1_R$，任取$r \in R$，

$$r = r \cdot 1_R = r \cdot 0_R = 0_R,$$

即$R = \{0_R\}$。

定义 7.2. 在环$\langle R, +, \cdot \rangle$中，如果$|R| = 1$，则$R = \{0_R\}$，称该环为**平凡环**。如果$|R| > 1$，那么必有$0_R \neq 1_R$，称这样的环为**非平凡环**。

例 7.5. 环$\langle R, +, \cdot \rangle$中所有可逆元关于$\cdot$构成群。

证明： 令$H = \{r | r \in R, \exists r' \in R, r \cdot r' = r' \cdot r = 1_R\}$。任取$r_1, r_2 \in H$，存在$r_1', r_2' \in R$，使得$r_1 \cdot r_1' = r_1' \cdot r_1 = 1_R$，$r_2 \cdot r_2' = r_2' \cdot r_2 = 1_R$。由于$(r_1 \cdot r_2) \cdot (r_2' \cdot r_1') = (r_2' \cdot r_1') \cdot (r_1 \cdot r_2) = 1_R$，因此，$r_2' \cdot r_1' \in R$是$r_1 \cdot r_2$的乘法逆元，故$r_1 \cdot r_2 \in H$，即$H$对$\cdot$运算是封闭的。因为$\langle R, \cdot \rangle$是含幺半群，而$H \subseteq R$，显然，$\cdot$运算在$H$中也满足结合律。因为$1_R$的乘法逆元就是自身，即$1_R' = 1_R$，所以$1_R \in H$。任取$r \in H$，$r$是$r'$的乘法逆元，故$r' \in H$。综上所述，$\langle H, \cdot \rangle$是群。证毕。

7.2 整环和域

本节介绍两类特殊的环——整环和域。先观察下面的两个例子。

例 7.6. 在整数环$\langle \mathbb{Z}, +, \cdot \rangle$中，$0$是零元。对任何$m, n \in \mathbb{Z}$，如果$m \cdot n = 0$，则必有$m = 0$或$n = 0$。换句话说，如果$m \neq 0$，$m \cdot n = 0$，则必有$n = 0$。这个性质允许我们在等号两边消去非零元素。这是因为如果$a \cdot b = a \cdot c$且$a \neq 0$，那么$a \cdot (b - c) = 0$。由此推出$b - c = 0$，即$b = c$。

例 7.7. 在模4同余类环中，$[0]$是零元。$[2] \neq [0]$，但是$[2] \cdot [2] = [0]$，从$[2] \cdot [1] = [2] \cdot [3]$ 推不出$[1] = [3]$。

定义 7.3. 在环$\langle R,+,\bullet\rangle$中，对于非零元素$a\in R$，如果存在一个非零元素$b\in R$，使得$a\bullet b=0$，则称$a$为**左零因子**。如果存在一个非零元素$c\in R$，使得$c\bullet a=0$，则称$a$为**右零因子**。若$a$既是左零因子又是右零因子，则称$a$为**零因子**。

定理 7.2. 环$\langle R,+,\bullet\rangle$中没有左零因子当且仅当环中的乘法有左、右消去律。

证明： 如果环$\langle R,+,\bullet\rangle$中没有左零因子，对于$R$中的非零元素$a$，如果$a\bullet b=a\bullet c$，即$a\bullet(b-c)=0$，可得$b-c=0$，即$b=c$，故左消去律成立。

假如环$\langle R,+,\bullet\rangle$中存在右零因子$b\in R$且$b\neq 0$，那么必然存在非零元素$c$使得$c\bullet b=0$。则$c$是$R$的左零因子，与环$R$中无左零因子矛盾。换句话说，在环$R$中无左零因子，那么也一定没有右零因子。用与上面相同的方法同理可证右消去律成立。

反之，环R中的乘法存在左、右消去律。任取环R中的非零元素a，如果$a\bullet b=0$，由于$a\bullet b=0=a\bullet 0$，根据左消去律可得$b=0$，所以a不是左零因子。由a 的任意性可知，环R中没有左零因子。证毕。

定义 7.4. 非平凡交换环$\langle R,+,\bullet\rangle$中，如果没有零因子，则称之为**整环**。

显然在整环中，对于任意元素$a,b\in R$，若$a\bullet b=0$，则必有$a=0$或$b=0$。由定理7.2知，整环中有左、右消去律。

定理 7.3. 在整环中，每个非零元素关于加法运算的阶(简称加阶)或者是无限的，或者是素数。

证明： 整环$\langle R,+,\bullet\rangle$乘法单位元$1_R$的加阶有两种情况。

(1) 1_R的加阶是无限的。假设R的某个非零元素a的加阶为m，即$ma=0_R$。

$$ma=\underbrace{a+a+\cdots+a}_{m}=(\underbrace{1_R+1_R+\cdots+1_R}_{m})\bullet a=0_R.$$

因为$a\neq 0_R$，所以$m1_R=\underbrace{1_R+1_R+\cdots+1_R}_{m}=0_R$，这与$1_R$的加阶是无限的矛盾，故$R$中所有非零元素的加阶都是无限的。

(2) 1_R的加阶是有限数k。假设k不是素数，设$k = mn$，即$(mn)1_R = 0_R$。而

$$
\begin{aligned}
(mn)1_R &= \underbrace{1_R + 1_R + \cdots + 1_R}_{mn} \\
&= \underbrace{(\underbrace{1_R + 1_R + \cdots + 1_R}_{m}) + (\underbrace{1_R + 1_R + \cdots + 1_R}_{m}) + \cdots (\underbrace{1_R + 1_R + \cdots + 1_R}_{m})}_{n} \\
&= \underbrace{(m1_R) + (m1_R) + \cdots + (m1_R)}_{n} \\
&= (\underbrace{1_R + 1_R \cdots + 1_R}_{n}) \cdot (m1_R) = (n1_R) \cdot (m1_R),
\end{aligned}
$$

且R 是整环，因此有$m1_R = 0_R$或者$n1_R = 0_R$。这与1_R的加阶为$k = mn$矛盾，因此1_R的加阶必为素数。令1_R的加阶为素数p，任取R中的非零元素a，

$$pa = \underbrace{a + a + \cdots + a}_{p} = (\underbrace{1_R + 1_R + \cdots + 1_R}_{p}) \cdot a = 0_R \cdot a = 0_R.$$

因此元素a的加阶是p的因子，而$a \neq 0_R$，所以a的加阶不是1，只能是素数p。证毕。

定义 7.5. 在整环中，如果每个非零元素的加阶为素数p，则称该整环的**特征**为p。如果每个非零元素的加阶是无限的，则称该整环的特征为0。

在特征为p的整环中，

$$(a + b)^p = a^p + C_p^1 a^{p-1} b + \cdots + C_p^{p-1} a b^{p-1} + b^p,$$

由于$p | C_p^i$，$1 \leq i \leq p - 1$，所以$(a + b)^p = a^p + b^b$。

定义 7.6. 在非平凡交换环R中，如果每个非零元素a都存在乘法逆元$a' \in R$，则称环R为**域**。即，非平凡交换环中，如果所有非零元素关于乘法运算构成交换群，则该环是域。

定理 7.4. 域是整环。

证明： 在域F中，若$a \cdot b = 0_F$且$a \neq 0_F$，那么非零元素a有乘法逆元$a' \in F$，

$$b = 1 \cdot b = (a' \cdot a) \cdot b = a' \cdot (a \cdot b) = a' \cdot 0_F = 0_F.$$

即F中没有零因子，所以域F是整环。证毕。

由定理7.4和定理7.3知，有限域的特征为素数p。

定理 7.5. 有限整环是域。

证明： 设$\langle R, +, \cdot \rangle$是有限整环。令$R = \{r_0, r_1, \cdots, r_n\}$。不妨假设$r_0 = 0_R$，$r_1 = 1_R$。任取$r_i \in R$，$1 \leq i \leq n$，

$$r_i R = \{r_i \cdot r_0, r_i \cdot r_1, \cdots, r_i \cdot r_n\} \subseteq R.$$

由于整环中有左、右消去律，当$k \neq l$时，$r_i \cdot r_k \neq r_i \cdot r_l$，所以$|r_i R| = |R|$，从而有$r_i R = R$。存在$j$使得$r_i \cdot r_j = r_1 = 1_R$，即$r_j$是$r_i$的乘法逆元。这说明$R$中所有非零元素都有乘法逆元，所以$R$是域。证毕。

例 7.8. 设p为素数，则$\langle \mathbb{Z}_p, +, \cdot \rangle$是域。

证明： $\mathbb{Z}_p = \{[0], [1], \cdots, [p-1]\}$。易知，$\langle \mathbb{Z}_p, +, \cdot \rangle$是非平凡交换环，$[0]$是零元，$[1]$是乘法单位元。如果$[a] \neq [0]$ 且$[a] \cdot [b] = [0]$，那么$[a \cdot b] = [0]$，即$p | a \cdot b$。而$p \nmid a$，因此$p | b$，即$[b] = [0]$。这说明$\langle \mathbb{Z}_p, +, \cdot \rangle$是有限整环，所以它是域。证毕。

例 7.9. $\langle \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}, +, \cdot \rangle$是域。

证明： 令$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$。容易验证，$\langle \mathbb{Q}(\sqrt{2}), + \rangle$是交换群，$\langle \mathbb{Q}(\sqrt{2}), \cdot \rangle$ 是含幺半群。0是零元，$-a - b\sqrt{2}$是$a + b\sqrt{2}$的负元，1是乘法单位元。乘法运算是可交换的，并且乘法对加法有左、右分配律。当$a + b\sqrt{2} \neq 0$ 时，$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$是$a + b\sqrt{2}$的乘法逆元。故$\langle \mathbb{Q}(\sqrt{2}), +, \cdot \rangle$是域。证毕。

7.3 子环和环同态

定义 7.7. 在环$\langle R,+,\cdot\rangle$中，S是R的非空子集。如果

(1) $\langle S,+\rangle$是$\langle R,+\rangle$的子群；

(2) S对乘法运算$\cdot$封闭；

(3) 环R的乘法单位元$1_R\in S$。

则称$\langle S,+,\cdot\rangle$是$\langle R,+,\cdot\rangle$的**子环**。

显然如此定义的子环$\langle S,+,\cdot\rangle$本身是环。

例 7.10. $\langle\mathbb{Z},+,\cdot\rangle$是$\langle\mathbb{Q},+,\cdot\rangle$的子环。

例 7.11. $\langle R,+,\cdot\rangle$是环，令

$$Z(R)=\{x|x\in R,\forall a\in R,a\cdot x=x\cdot a\},$$

则$\langle Z(R),+,\cdot\rangle$是$\langle R,+,\cdot\rangle$的子环。

证明： $Z(R)$是环R中与所有元素可交换的元素集合。显然，R的乘法单位元$1_R\in Z(R)$，所以$Z(R)$是R的非空子集。任取$x,y\in Z(R)$，$\forall a\in R$，

$$\begin{aligned}(x+y)\cdot a=x\cdot a+y\cdot a=a\cdot x+a\cdot y&=a\cdot(x+y),\\(-x)\cdot a=-(x\cdot a)=-(a\cdot x)&=a\cdot(-x),\end{aligned}$$

即$x+y,-x\in Z(R)$，故$\langle Z(R),+\rangle$是$\langle R,+\rangle$的子群。

$$\begin{aligned}(x\cdot y)\cdot a&=x\cdot(y\cdot a)=x\cdot(a\cdot y)=(x\cdot a)\cdot y\\&=(a\cdot x)\cdot y=a\cdot(x\cdot y),\end{aligned}$$

即$x\cdot y\in Z(R)$，因此，$Z(R)$对$\cdot$是封闭的。

综上所述，$\langle Z(R),+,\cdot\rangle$是$\langle R,+,\cdot\rangle$的子环。证毕。

定义 7.8. R_1, R_2是环，f是从R_1到R_2的映射，1_{R_1}和1_{R_2}分别是R_1和R_2的乘法单位元。如果对任意$a, b \in R_1$，有

$$f(a+b) = f(a) + f(b),$$
$$f(a \cdot b) = f(a) \cdot f(b),$$
$$f(1_{R_1}) = 1_{R_2},$$

则称f是从R_1到R_2的**环同态映射**。

如果f是满射(单射、双射)，则称f为满环同态映射(单一环同态映射，环同构映射)。

例 7.12. 从$\mathbb{R}^n$到其自身的线性变换全体对加法和乘法运算构成环$\langle L(\mathbb{R}^n, \mathbb{R}^n), +, \cdot \rangle$。$n$阶实数矩阵环记为$\langle M_n(\mathbb{R}), +, \cdot \rangle$。证明这两个环是同构的。

证明： 从$\mathbb{R}^n$到其自身的线性变换α对于$\mathbb{R}^n$的一组基$\mathbf{x_1}, \mathbf{x_2}, \cdots, \mathbf{x_n}$有

$$\alpha \begin{pmatrix} \mathbf{x_1} \\ \mathbf{x_2} \\ \vdots \\ \mathbf{x_n} \end{pmatrix} = \begin{pmatrix} a_{11}\mathbf{x_1} + a_{12}\mathbf{x_2} + \cdots + a_{1n}\mathbf{x_n} \\ a_{21}\mathbf{x_1} + a_{22}\mathbf{x_2} + \cdots + a_{2n}\mathbf{x_n} \\ \vdots \\ a_{n1}\mathbf{x_1} + a_{n2}\mathbf{x_2} + \cdots + a_{nn}\mathbf{x_n} \end{pmatrix}.$$

定义映射$f : L(\mathbb{R}^n, \mathbb{R}^n) \to M_n(\mathbb{R})$为

$$f(\alpha) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

在线性代数中已经学习过：给定n维空间的一组基，每个线性变换对应一个n阶方阵，并且线性变换的和对应于矩阵的和，线性变换的积对应于矩阵的乘积。所以，对于任意两个线性变换$\alpha, \beta \in L(\mathbb{R}^n, \mathbb{R}^n)$，

$$f(\alpha + \beta) = f(\alpha) + f(\beta),$$
$$f(\alpha \cdot \beta) = f(\alpha) \cdot f(\beta).$$

若γ是单位线性变换，则$f(\gamma)$是单位矩阵。

反之，对任意n阶实数矩阵都可以定义相应的线性变换。不同的线性变换对应不同的矩阵，所以f是满射和单射，因此f是环同构映射。故环$\langle L(\mathbb{R}^n, \mathbb{R}^n), +, \cdot\rangle$与环$\langle M_n(\mathbb{R}), +, \cdot\rangle$是同构的。证毕。

例 7.13. $\langle \mathbb{Z}_{24}, +, \cdot\rangle$与$\langle \mathbb{Z}_4, +, \cdot\rangle$是两个环。令$f : \mathbb{Z}_{24} \to \mathbb{Z}_4$，$f([x]_{24}) = [x]_4$。首先指出映射$f$的定义与代表元的选取无关。这是因为若$[x]_{24} = [y]_{24}$，则$24|(x-y)$。而$4|24$，故$4|(x-y)$，即$[x]_4 = [y]_4$。容易验证，

$$
\begin{aligned}
f([x]_{24} + [y]_{24}) &= f([x+y]_{24}) = [x+y]_4 \\
&= [x]_4 + [y]_4 = f([x]_{24}) + f([y]_{24}), \\
f([x]_{24} \cdot [y]_{24}) &= f([x \cdot y]_{24}) = [x \cdot y]_4 \\
&= [x]_4 \cdot [y]_4 = f([x]_{24}) \cdot f([y]_{24}), \\
f([1]_{24}) &= [1]_4.
\end{aligned}
$$

所以f是环同态映射。

环同态映射也有类似于群同态映射的一些性质。

定理 7.6. 设f是从环R_1到环R_2的同态映射，0_{R_1}和0_{R_2}分别是环R_1和R_2的零元。则f有以下性质：

(1) $f(0_{R_1}) = 0_{R_2}$；

(2) $f(-a) = -f(a)$；

(3) 若a是R_1的可逆元，则$f(a)$是R_2的可逆元并且$f(a') = (f(a))'$。

证明: f是从环R_1到环R_2的同态映射，那么f也是从交换群$\langle R_1, +\rangle$到交换群$\langle R_2, +\rangle$群同态映射，所以(1)和(2)显然成立。对于(3)，若a是R_1 的可逆元，即存在$a' \in R_1$，使得$a \cdot a' = a' \cdot a = 1_{R_1}$，那么

$$
\begin{aligned}
f(a) \cdot f(a') = f(a \cdot a') = f(1_{R_1}) = 1_{R_2}, \\
f(a') \cdot f(a) = f(a' \cdot a) = f(1_{R_1}) = 1_{R_2}.
\end{aligned}
$$

因此，$f(a')$是$f(a) \in R_2$的乘法逆元，即$f(a') = (f(a))'$。证毕。

例 7.14. $\langle\mathbb{Z},+,\cdot\rangle$与$\langle\mathbb{Z}_n,+,\cdot\rangle$是环。令$f:\mathbb{Z}\to\mathbb{Z}_n$，$f(m)=[m]$。易证，$f$是满同态映射。$\langle\mathbb{Z},+,\cdot\rangle$是整环，但$\langle\mathbb{Z}_n,+,\cdot\rangle$不一定是整环。事实上，当$n$是合数时，$\langle\mathbb{Z}_n,+,\cdot\rangle$不是整环。这是因为当$n=k\cdot l$时，$[k]\cdot[l]=[0]$且$[k],[l]\neq[0]$，环$\langle\mathbb{Z}_n,+,\cdot\rangle$ 中有零因子，所以不是整环。

例 7.15. $\langle\mathbb{Z}\times\mathbb{Z},+,\cdot\rangle$与$\langle\mathbb{Z},+,\cdot\rangle$是环。令$f:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$，$f((a,b))=a$。易证，$f$ 是满同态映射。$\mathbb{Z}\times\mathbb{Z}$中的非零元素$(2,0)$和$(0,1)$是零因子，所以$\langle\mathbb{Z}\times\mathbb{Z},+,\cdot\rangle$不是整环，但$\langle\mathbb{Z},+,\cdot\rangle$是整环。

以上两个例子说明环同态映射并不保持环的全部代数结构。但环同构映射对整环和域则不然。

定理 7.7. *f是从环R_1到环R_2的同构映射，如果R_1是整环(域)，则R_2也是整环(域)。*

证明： 如果R_1是整环，则它是非平凡交换环且没有零因子。令$f:R_1\to R_2$是环同构映射。因为R_1是非平凡环，所以$0_{R_1}\neq 1_{R_1}$，故$0_{R_2}=f(0_{R_1})\neq f(1_{R_1})=1_{R_2}$，于是$R_2$是非平凡环。

任取$x_2,y_2\in R_2$，必存在$x_1,y_1\in R_1$，使$f(x_1)=x_2$，$f(y_1)=y_2$。

$$\begin{aligned}x_2\cdot y_2&=f(x_1)\cdot f(y_1)=f(x_1\cdot y_1)=f(y_1\cdot x_1)\\&=f(y_1)\cdot f(x_1)=y_2\cdot x_2.\end{aligned}$$

所以，R_2是交换环。

如果$x_2,y_2\in R_2$且$x_2\cdot y_2=0_{R_2}$，由于存在$x_1,y_1\in R_1$，使$f(x_1)=x_2$，$f(y_1)=y_2$，故有

$$0_{R_2}=x_2\cdot y_2=f(x_1)\cdot f(y_1)=f(x_1\cdot y_1).$$

而f是单射，所以$x_1\cdot y_1=0_{R_1}$。因为R_1中没有零因子，故有$x_1=0_{R_1}$或$y_1=0_{R_1}$，进而得出$x_2=f(x_1)=0_{R_2}$或$y_2=f(y_1)=0_{R_2}$，即R_2中无零因子，故R_2是整环。

设R_1是域。任取R_2的非零元素x_2，因为f是满射，所以必存在$x_1\in R_1$使$f(x_1)=x_2$。f又是单射，所以x_1是R_1中的非零元素，在R_1中有乘法逆元x_1'。

$$f(x_1)\cdot f(x_1')=f(x_1\cdot x_1')=f(1_{R_1})=1_{R_2}$$

所以$f(x_1')\in R_2$是x_2的乘法逆元。由x_2的任意性知R_2是域。证毕。

定理 7.8. 设$\langle R,+,\bullet\rangle$是环。在非空集合$R_1$上定义两个运算$+$和$\bullet$。如果存在满射$f:R\to R_1$，对于任意$a,b\in R$有

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

则$\langle R_1,+,\bullet\rangle$是环。

证明： $f:R\to R_1$是满射，所以R_1中的元素都可以表示成$f(a)$形式，$a\in R$。由于$\langle R,+\rangle$是交换群，易证，R_1中$+$运算是封闭的且满足交换律和结合律，$f(0_R)\in R_1$是R_1的零元，$f(-a)$是$f(a)$在R_1中的负元，故$\langle R_1,+\rangle$是交换群。由于$\langle R,\bullet\rangle$是含幺半群，所以，R_1 中$\bullet$运算是封闭的且满足结合律，$f(1_R)\in R_1$是R_1的乘法单位元，故$\langle R_1,\bullet\rangle$是含幺半群。因为$R$中$\bullet$对$+$有左、右分配律，所以$R_1$中$\bullet$ 对$+$也有左、右分配律。故$\langle R_1,+,\bullet\rangle$是环。证毕。

7.4 理想与商环

本节将用类似商群的方法定义商环，其中与正规子群对应的概念是理想。商环是基于对一个理想的所有陪集组成的集合而定义的。

定义 7.9. 设I是环$\langle R,+,\bullet\rangle$的非空子集。如果$\forall x,y\in I$，$r\in R$，有$x-y\in I$，$x\bullet r\in I$ 并且$r\bullet x\in I$，则称I是环R 的一个**理想**。

根据定义7.9，由于$\forall x,y\in I$，有$x-y\in I$，易得$\langle I,+\rangle$是$\langle R,+\rangle$的子群。

每个环R都有两个理想：R和$\{0_R\}$，称这两个理想为**平凡理想**。非平凡理想称为**真理想**。

设I_1,I_2是环R的理想，定义

$$I_1\bullet I_2=\{\sum_{k=1}^{n}r_{1k}\bullet r_{2k}|r_{1k}\in I_1,r_{2k}\in I_2,1\le k\le n,n=1,2,\cdots\},$$

$$I_1+I_2=\{r_1+r_2|r_1\in I_1,r_2\in I_2\},$$

那么$I_1\bullet I_2$与I_1+I_2都是R的理想。证明留作习题。

例 7.16. 在模6同余类环$\langle \mathbb{Z}_6, +, \cdot\rangle$中，$I_1 = \{[0], [3]\}$是理想。在环$\langle \mathbb{Z} \times \mathbb{Z}, +, \cdot\rangle$中，$I_2 = \{(0, n) | n \in \mathbb{Z}\}$ 是理想。

在环R中，利用R的理想I建立了一个关系：对环R中任意两个元素x与y，

$$x\text{与}y\text{模}I\text{同余} \quad \text{当且仅当}x - y \in I.$$

不难证明环R中的模I同余关系是等价关系。元素x所在的等价类

$$[x] = \{y | y \in R, x - y \in I\} = \{x + i | i \in I\} = x + I.$$

在商集R/I中定义

$$[x] + [y] = [x + y],$$
$$[x] \cdot [y] = [x \cdot y].$$

首先指出，如此定义的等价类加法和乘法是与代表元选取无关的。这是因为，如果$[x_1] = [x_2]$，$[y_1] = [y_2]$，那么由$x_1 - x_2 \in I$，$y_1 - y_2 \in I$知

$$(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) \in I,$$
$$(x_1 \cdot y_1) - (x_2 \cdot y_2) = x_1 \cdot (y_1 - y_2) + (x_1 - x_2) \cdot y_2 \in I.$$

故$(x_1+y_1)+I = (x_2+y_2)+I$，$(x_1 \cdot y_1)+I = (x_2 \cdot y_2)+I$，即$[x_1+y_1] = [x_2+y_2]$，$[x_1 \cdot y_1] = [x_2 \cdot y_2]$。

定理 7.9. 设I是环R的理想。$R/I = \{x + I | x \in R\}$中的加法$+$和乘法$\cdot$如上定义。则$\langle R/I, +, \cdot\rangle$是环，被称为$R$模$I$的**商环**。

证明： R/I中的$+$和$\cdot$运算是由等价类代表元的$+$与$\cdot$运算实现的，因此，R/I的$+$运算满足结合律和交换律，$0_R + I$是R/I的零元，$(-x) + I$ 是$x + I$的负元，故$\langle R/I, +\rangle$是交换群。R/I的$\cdot$运算满足结合律，$1_R + I$是R/I的乘法单位元，故$\langle R/I, \cdot\rangle$是含幺半群。$\cdot$ 对$+$ 显然有左、右分配律。综上所述，$\langle R/I, +, \cdot\rangle$是环。证毕。

例 7.17. 在例*7.16*中，

$$\mathbb{Z}_6/I_1 = \{[0] + I_1, [1] + I_1, [2] + I_1\},$$
$$\mathbb{Z} \times \mathbb{Z}/I_2 = \{(m, 0) + I_2 | m \in \mathbb{Z}\}.$$

定理 7.10. 如果环R的理想I中有可逆元，则$I = R$。

证明： 设环R的理想I中有R的可逆元r，即其乘法逆元$r' \in R$。由理想的定义知$1_R = r \cdot r' \in I$。任取$\widetilde{r} \in R$，$\widetilde{r} = \widetilde{r} \cdot 1_R \in I$，于是$R \subseteq I$。又知理想$I$是$R$的非空子集，即$I \subseteq R$，因此$I = R$，即该理想是平凡理想。证毕。

在域F中，若I是F的理想且$I \neq \{0_F\}$，则必存在一个非零元素$a \in I$。而域的所有非零元素都有乘法逆元，由定理7.10知，$I = F$。也就是说，域F只有两个平凡理想$\{0_F\}$ 和F，没有真理想。因此，域F的商域或是$F/\{0_F\} = \{r + \{0_F\} | r \in F\} \cong F$，或是$F/F = \{F\} \cong \{0_F\}$。它们的结构很简单，不必深入讨论。

本节最后讨论一种特殊的理想。

定理 7.11. 设R是交换环。$\forall a \in R$，$(a) = \{a \cdot r | r \in R\}$是$R$的理想，称之为由$a$生成的理想。这类特殊的理想叫做**主理想**。

证明： 对于$a \in R, a = a \cdot 1_R \in (a)$。所以$(a)$是$R$的非空子集。$\forall a_1, a_2 \in (a)$，存在$r_1, r_2 \in R$使得$a_1 = a \cdot r_1$，$a_2 = a \cdot r_2$。$a_1 - a_2 = a \cdot (r_1 - r_2) \in (a)$。对任意$r \in R$和$a_1 \in (a)$，$r \cdot a_1 = r \cdot (a \cdot r_1) = a \cdot (r \cdot r_1) \in (a)$，$a_1 \cdot r = a \cdot (r_1 \cdot r) \in (a)$。所以$(a)$是$R$的理想。证毕。

这个概念可以推广到交换环R的子集上。令$S = \{a_1, a_2, \cdots, a_k\} \subseteq R$，

$$(a_1, a_2, \cdots, a_k) = \{a_1 \cdot r_1 + a_2 \cdot r_2 + \cdots + a_k \cdot r_k | r_1, r_2, \cdots r_k \in R\},$$

是R的理想，被称为S生成的理想，也是主理想。

定义 7.10. 如果环R的所有理想都是主理想，则称R是**主理想环**。

例 7.18. 整数环$\langle \mathbb{Z}, +, \cdot \rangle$是主理想环。

证明： 设I是整数环$\langle \mathbb{Z}, +, \cdot \rangle$的理想。如果$I$中没有非零元素，即$I = \{0\}$，则$I$是由$0$生成的理想。

如果I中有非零元素，那么必有正整数$a \in I$ (如果$b < 0$且$b \in I$，由于I是理想，$-1 \in \mathbb{Z}$，$-b = (-1) \cdot b \in I$，并且$-b > 0$)。这样就可以在I 中找到最小的正整数k。对于I中任意元素n，$n = m \cdot k + q$，$0 \leq q \leq k - 1$。由于I是理想，所以$q = n - m \cdot k \in I$。而k是I中最小的正整数，必有$q = 0$，即$n = m \cdot k \in (k)$。因此$I \subseteq (k)$。又由于$k \in I$，显然$m \cdot k \in I$，故$(k) \subseteq I$。因此，$I = (k)$。即整数环是主理想环。证毕。

7.5 多项式环

7.5.1 环上的多项式

环$\langle R,+,\cdot\rangle$上的多项式定义为

$$p(x)=a_0+a_1x+\cdots+a_nx^n,\quad a_n\neq 0_R, n\geq 0,$$

其中$a_0,a_1,\cdots,a_n\in R$称为系数，x为未定元，n为$p(x)$的次数，即$deg(p(x))=n$。环R上的非零元素称为零次多项式(或常数多项式)，零元素0_R称为零多项式。

环R上的全体多项式组成的集合记为$R[x]$，在其上定义运算$+$和$\cdot$。对任意的$f(x),g(x)\in R[x]$，其中$f(x)=\sum_{i=0}^n a_ix^i$，$g(x)=\sum_{j=0}^m b_jx^j$，

$$f(x)+g(x)=\sum_{k=0}^{\max\{m,n\}}(a_k+b_k)x^k,$$

$$f(x)\cdot g(x)=\sum_{k=0}^{m+n}c_kx^k,\quad c_k=\sum_{i+j=k}a_i\cdot b_j, 0\leq k\leq m+n,$$

其中$m<n$时$a_k=0$，$n<k\leq m$；$m<n$时$b_k=0$，$m<k\leq n$。不难验证$\langle R[x],+,\cdot\rangle$是环。零多项式是零元，$-f(x)$ 是$f(x)$ 的负元，常数多项式1_R是乘法单位元。

设R是整环，即R是非平凡交换环并且没有零因子。设$f(x)$与$g(x)$是$R[x]$中的非零多项式，它们的次数分别是$n,m(\geq 0)$，即$f(x)=a_nx^n+\cdots$，$g(x)=b_mx^m+\cdots$，$a_n,b_m\neq 0_R$。由于R是整环，所以$a_n\cdot b_m\neq 0_R$。故

$$f(x)\cdot g(x)=a_nb_mx^{n+m}+\cdots$$

是非零多项式，因此$R[x]$中没有零因子。又$R[x]$是非平凡交换环，故$R[x]$是整环。

7.5.2 域上的多项式

定理 7.12. 设F是域，$f(x),g(x)$是多项式环$F[x]$的元素。如果$g(x)$不是零多项式，则存在唯一的$q(x),r(x)\in F[x]$，使得

$$f(x)=q(x)\cdot g(x)+r(x),$$

其中$r(x)$或是零多项式，或是次数小于$deg(g(x))$的多项式。

证明： 令$g(x) = b_0 + b_1 x + \cdots + b_m x^m$，$b_m \neq 0_F$，$m \geq 0$。考虑集合

$$S' = \{f(x) - s(x) \cdot g(x) | s(x) \in F[x]\}.$$

有两种可能的情况：

(1) 零多项式$0_F \in S'$。此时存在$q(x) \in F[x]$，使得$f(x) = q(x) \cdot g(x)$。

(2) 零多项式$0_F \notin S'$。记S'中次数最小的多项式为$r(x)$，则存在$q(x) \in F[x]$，使得$r(x) = f(x) - q(x) \cdot g(x)$，即$f(x) = q(x) \cdot g(x) + r(x)$。设$r(x) = c_t x^t + \cdots + c_0$，$c_t \neq 0_F$。假设$deg(r(x)) = t \geq deg(g(x)) = m$。现构造一个新的多项式，

$$r_1(x) = f(x) - q(x) \cdot g(x) - c_t \cdot b'_m x^{t-m} \cdot g(x) = r(x) - c_t x^t + \cdots,$$

于是$deg(r_1(x)) < deg(r(x))$，而

$$r_1(x) = f(x) - [q(x) + c_t \cdot b'_m x^{t-m}] \cdot g(x)] \in S'.$$

这与$r(x)$是S'中次数最低的多项式矛盾，所以必有$deg(r(x)) < deg(g(x))$。

下面证明$q(x)$和$r(x)$是唯一的。假设$q_1(x), r_1(x)$及$q_2(x), r_2(x)$均满足：

$$f(x) = q_1(x) \cdot g(x) + r_1(x),$$
$$f(x) = q_2(x) \cdot g(x) + r_2(x),$$

并且$r_1(x)$，$r_2(x)$的次数均小于$g(x)$的次数(即m)。将上面两式相减，可得

$$(q_1(x) - q_2(x)) \cdot g(x) = r_2(x) - r_1(x).$$

如果$q_1(x) - q_2(x)$不是零多项式，那么上式左边多项式的次数大于等于m，而右边多项式的次数小于m，矛盾。故必有$q_1(x) = q_2(x)$，由此又可得出$r_1(x) = r_2(x)$。证毕。

定理7.12说明域上的多项式可以做除法，商和余式是唯一确定的。如果$f(x) = q(x) \cdot g(x)$，则称$g(x)$是$f(x)$的因式。特别地，取$g(x) = x - a$，$f(x)$除以$x - a$的余氏是域F的元素，即

$$f(x) = q(x) \cdot (x - a) + r_0, \quad r_0 \in F.$$

令$x=a$，则$r_0=f(a)$。由此可知，在$F[x]$中，多项式$x-a$是$f(x)$的因式当且仅当$f(a)=0_F$，这时称a是多项式$f(x)$的根。

定理 7.13. 域F上的多项式环$F[x]$是主理想环。

证明： 设I是$F[x]$的一个理想。若I中没有非零多项式，则$I=\{0_F\}$，它是由0_F生成的理想。若I中有非零多项式，其中次数最低的非零多项式记为$g(x)$。根据$g(x)$的次数可以分为两种情况：

(1) $deg(g(x))=0$。即$g(x)=a\in F$且$a\neq 0_F$。a在F中有乘法逆元a'，$a'\in F[x]$。$a'\cdot a=1_F\in I$，与定理7.10 的证明类似，可得$I=F[x]$。I是由1_F生成的理想。

(2) $deg(g(x))\neq 0$。任取$f(x)\in I$，由定理7.12知，存在$q(x),r(x)\in F[x]$使$f(x)=q(x)\cdot g(x)+r(x)$。因为$g(x)\in I$且I是$F[x]$ 的理想，所以$r(x)=f(x)-q(x)\cdot g(x)\in I$。由于$g(x)$是$I$中次数最低的多项式，故必有$r(x)=0_F$，即$f(x)=q(x)\cdot g(x)\in(g(x))$。由$f(x)$的任意性知$I\subseteq(g(x))$。反之，$g(x)\in I$，对任何$q(x)\in F[x]$，$q(x)\cdot g(x)\in I$，所以$(g(x))\subseteq I$。综上，$I=(g(x))$。

所以域F上的多项式环$F[x]$是主理想环。证毕。

7.5.3 域上的多项式商环

域F的多项式环$F[x]$是主理想环。$F[x]$的理想都是$P=(p(x))$形式，其中$p(x)=a_0+a_1x+\cdots+a_nx^n$，$a_n\neq 0_F$，则

$$F[x]/P=\{f(x)+P|f(x)\in F[x]\}.$$

而$f(x)=q(x)\cdot p(x)+r(x)$，$f(x)-r(x)\in(p(x))$，即$f(x)+P=r(x)+P$。所以

$$F[x]/P=\{b_0+b_1x+\cdots+b_{n-1}x^{n-1}+P|b_0,b_1,\cdots,b_{n-1}\in F\}.$$

例 7.19. 写出$\mathbb{Z}_2[x]/(x^2+x+1)$的加法表和乘法表。

解： $\mathbb{Z}_2=\{[0],[1]\}$，简记为$\mathbb{Z}_2=\{0,1\}$。(x^2+x+1)是$\mathbb{Z}_2[x]$的主理想。令$P=(x^2+x+1)$，则有

$$\begin{aligned}\mathbb{Z}_2[x]/P&=\{(ax+b)+P|a,b\in\mathbb{Z}_2\}\\&=\{P,1+P,x+P,1+x+P\}.\end{aligned}$$

表 7.1: $\mathbb{Z}_2[x]/(x^2+x+1)$的加法表和乘法表

$+$	P	$1+P$	$x+P$	$1+x+P$
P	P	$1+P$	$x+P$	$1+x+P$
$1+P$	$1+P$	P	$1+x+P$	$x+P$
$x+P$	$x+P$	$1+x+P$	P	$1+P$
$1+x+P$	$1+x+P$	$x+P$	$1+P$	P

$\cdot$	P	$1+P$	$x+P$	$1+x+P$
P	P	P	P	P
$1+P$	P	$1+P$	$x+P$	$1+x+P$
$x+P$	P	$x+P$	$1+x+P$	$1+P$
$1+x+P$	P	$1+x+P$	$1+P$	$x+P$

它的加法表和乘法表如表7.1所示。

7.6 环同态定理

定义 7.11. 设φ是从环R_1到环R_2的同态映射。0_{R_2}是R_2的零元。$Ker\varphi = \{r | r \in R_1, \varphi(r) = 0_{R_2}\}$称为$\varphi$的**同态核**。

定理 7.14. 设φ是从环R_1到环R_2的同态映射，则$Ker\varphi$是R_1的理想。

证明： φ是从R_1到R_2的环同态映射，所以也是从交换群$\langle R_1, +\rangle$到$\langle R_2, +\rangle$的群同态映射。由定理6.6知，$\mathrm{Ker}\varphi$是$\langle R_1, +\rangle$的正规子群。任取$x_1, x_2 \in \mathrm{Ker}\varphi$，$x_1 - x_2 \in \mathrm{Ker}\varphi$。又若$x \in \mathrm{Ker}\varphi$，$r \in R_1$，

$$\varphi(x \cdot r) = \varphi(x) \cdot \varphi(r) = 0_{R_2} \cdot \varphi(r) = 0_{R_2},$$

故$x \cdot r \in \mathrm{Ker}\varphi$。同理可证$r \cdot x \in \mathrm{Ker}\varphi$。所以，$\mathrm{Ker}\varphi$是$R_1$的理想。证毕。

定理 7.15. **（环同态基本定理）** 环R_1的任意商环都是环R_1的同态像。若φ是从环R_1到环R_2的满同态映射，则

$$R_1/Ker\varphi \cong R_2.$$

证明： 设I_1是环R_1的理想。令$\widetilde{\varphi}: R_1 \to R_1/I_1$，$\widetilde{\varphi} = r + I_1$。显然，$\widetilde{\varphi}$是满射。对任意$r_1, r_2 \in R_1$，

$$\begin{aligned}
\widetilde{\varphi}(r_1 + r_2) &= (r_1 + r_2) + I = (r_1 + I) + (r_2 + I) = \widetilde{\varphi}(r_1) + \widetilde{\varphi}(r_2),\\
\widetilde{\varphi}(r_1 \cdot r_2) &= (r_1 \cdot r_2) + I = (r_1 + I) \cdot (r_2 + I) = \widetilde{\varphi}(r_1) \cdot \widetilde{\varphi}(r_2),\\
\widetilde{\varphi}(1_{R_1}) &= 1_{R_1} + I,
\end{aligned}$$

因此，$\widetilde{\varphi}$是满同态映射，$\widetilde{\varphi}(R_1) = R_1/I_1$。因此，环$R_1$的任意商环都是环$R_1$的同态像。

若φ是从环R_1到环R_2的满同态映射，那么φ也是从$\langle R_1, +\rangle$到$\langle R_2, +\rangle$的群同态映射。由群同态基本定理知$\widetilde{\varphi}: R_1/\mathrm{Ker}\varphi \to R_2$，$\widetilde{\varphi}(r + \mathrm{Ker}\varphi) = \varphi(r)$是群同构映射。另有

$$\begin{aligned}
&\widetilde{\varphi}((r_1 + \mathrm{Ker}\varphi) \cdot (r_2 + \mathrm{Ker}\varphi)) = \widetilde{\varphi}(r_1 \cdot r_2 + \mathrm{Ker}\varphi) = \varphi(r_1 \cdot r_2)\\
&\quad = \varphi(r_1) \cdot \varphi(r_2) = \widetilde{\varphi}((r_1 + \mathrm{Ker}\varphi)) \cdot \widetilde{\varphi}((r_2 + \mathrm{Ker}\varphi)),\\
&\widetilde{\varphi}((1_{R_1} + \mathrm{Ker}\varphi)) = \varphi(1_{R_1}) = 1_{R_2},
\end{aligned}$$

故$\widetilde{\varphi}$是环同构映射，从而$R_1/\mathrm{Ker}\varphi \cong R_2$。证毕。

例 7.20. $\mathbb{Q}[x]$是有理数域$\mathbb{Q}$上的多项式集合。令$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$。证明

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2}).$$

证明： 令$\psi: \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$，$\psi(f(x)) = f(\sqrt{2})$。易证，$\psi$是从$\mathbb{Q}[x]$到$\mathbb{Q}(\sqrt{2})$的环同态映射。任取$a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$，存在$a + bx \in \mathbb{Q}[x]$，使$\psi(a + bx) = a + b\sqrt{2}$，所以$\psi$是满同态映射。

下面求$\mathrm{Ker}\psi$。若$p(x) \in \mathrm{Ker}\psi$，即$p(\sqrt{2}) = 0$。取$g(x) = x^2 - 2$，由定理7.12知，

$$p(x) = q(x)(x^2 - 2) + a_0 + a_1 x,\ a_0, a_1 \in \mathbb{Q}.$$

由$p(\sqrt{2})=0$可得$a_0+a_1\sqrt{2}=0$，因此$a_0=a_1=0$。由此得到$p(-\sqrt{2})=a_0-a_1\sqrt{2}=0$。故，$x^2-2$是$p(x)$的因式。于是，$\mathrm{Ker}\psi=\{p(x)|x^2-2$是$p(x)$的因式$\}=(x^2-2)$，是$x^2-2$生成的理想。根据环同态基本定理知，$\mathbb{Q}[x]/(x^2-2)\cong\mathbb{Q}(\sqrt{2})$。证毕。

例 7.21. 证明$\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$。

证明： 令$\psi:\mathbb{R}[x]\to\mathbb{C}$，$\psi(f(x))=f(\mathrm{i})$，其中$\mathrm{i}=\sqrt{-1}$。易证，$\psi$是从$\mathbb{R}[x]$到$\mathbb{C}$ 的环同态映射。任取$a+b\mathrm{i}\in\mathbb{C}$，存在$a+bx\in\mathbb{R}[x]$，使得$\psi(a+bx)=a+b\mathrm{i}$，所以$\psi$是满同态映射。

下面求$\mathrm{Ker}\psi$。任取$p(x)\in\mathrm{Ker}\psi$，即$p(\mathrm{i})=0$。取$g(x)=x^2+1$，由定理7.12知，

$$p(x)=q(x)(x^2+1)+a_0+a_1x,\ a_0,a_1\in\mathbb{R}.$$

由$p(\mathrm{i})=0$可得$a_0+a_1\mathrm{i}=0$，因此$a_0=a_1=0$。由此得到$p(-\mathrm{i})=a_0-a_1\mathrm{i}=0$。故，$x^2+1$是$p(x)$的因式。于是，$\mathrm{Ker}\psi=\{p(x)|x^2+1$是$p(x)$的因式$\}=(x^2+1)$，是$x^2+1$生成的理想。根据环同态基本定理知，$\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$。证毕。

定理 7.16. f是从环R_1到环R_2的同态映射，则

(1) 若S_1是R_1的子环，则$f(S_1)$是R_2的子环。特别地，$f(R_1)$是R_2的子环。

(2) 若S_1是R_1的理想，则$f(S_1)$是$f(R_1)$的理想。

(3) 若S_2是$f(R_1)$的子环，则$f^{-1}(S_2)$是R_1的子环。

(4) 若S_2是$f(R_1)$的理想，则$f^{-1}(S_2)$是R_1的理想，且$R_1/f^{-1}(S_2)\cong f(R_1)/S_2$。

证明： 这里只证明(1)和(4)，(2)和(3)的证明方法类似，留作习题。

(1) f是从R_1到R_2的环同态映射，那么f是从$\langle R_1,+\rangle$到$\langle R_2,+\rangle$的群同态映射。S_1是R_1的子环，故$\langle S_1,+\rangle$到$\langle R_1,+\rangle$的子群。由定理6.7知$\langle f(S_1),+\rangle$是$\langle R_2,+\rangle$的子群。任取$x_2,y_2\in f(S_1)$，存在$x_1,y_1\in S_1$，使得$f(x_1)=x_2$，$f(y_1)=y_2$。因为$x_1\bullet y_1\in S_1$，所以

$$x_2\bullet y_2=f(x_1)\bullet f(y_1)=f(x_1\bullet y_1)\in f(S_1).$$

$f(S_1)$对乘法$\cdot$是封闭的。$1_{R_1} \in S_1$，$f(1_{R_1}) = 1_{R_2}$，即$1_{R_2} \in f(S_1)$。由此可知，$\langle f(S_1), +, \cdot\rangle$是$\langle R_2, +, \cdot\rangle$的子环。特别地，取$S_1 = R_1$，可得$f(R_1)$是$R_2$的子环。

(4) 因为S_2是$f(R_1)$的理想，所以$f(R_1)/S_2$是环。令$\psi : f(R_1) \to f(R_1)/S_2$，$\psi(f(r_1)) = f(r_1) + S_2$。显然，$\psi$是满射。又因为$f$是从$R_1$ 到$f(R_1)$的满射，所以$\psi \circ f$是从R_1到$f(R_1)/S_2$的满射。对于$r_1, r_2 \in R_1$，

$$\begin{aligned}(\psi \circ f)(r_1 + r_2) &= \psi(f(r_1 + r_2)) = f(r_1 + r_2) + S_2 = (f(r_1) + f(r_2)) + S_2 \\ &= (f(r_1) + S_2) + (f(r_2) + S_2) = (\psi \circ f)(r_1) + (\psi \circ f)(r_2), \\ (\psi \circ f)(r_1 \cdot r_2) &= \psi(f(r_1 \cdot r_2)) = f(r_1 \cdot r_2) + S_2 = (f(r_1) \cdot f(r_2)) + S_2 \\ &= (f(r_1) + S_2) \cdot (f(r_2) + S_2) = (\psi \circ f)(r_1) \cdot (\psi \circ f)(r_2), \\ (\psi \circ f)(1_{R_1}) &= \psi(f(1_{R_1})) = f(1_{R_1}) + S_2 = 1_{R_2} + S_2,\end{aligned}$$

因此，$\psi \circ f$是从环R_1到环$f(R_1)/S_2$的满同态映射。

$$\begin{aligned}\operatorname{Ker}(\psi \circ f) &= \{r | r \in R_1, (\psi \circ f)(r) = S_2\} \\ &= \{r | r \in R_1, f(r) \in S_2\} = f^{-1}(S_2).\end{aligned}$$

由环同态基本定理可得，$R_1/f^{-1}(S_2) \cong f(R_1)/S_2$。证毕。

定理 7.17. I_1, I_2是环R的两个理想，$I_2 \subseteq I_1$，则I_1/I_2是R/I_2的理想，且

$$\frac{R/I_2}{I_2/I_1} \cong R/I_1.$$

证明： I_1, I_2是环R的理想，所以R/I_2和R/I_1是两个商环。因为$I_2 \subseteq I_1 \subseteq R$，商集$I_1/I_2 = \{i + I_2 | i \in I_1\} \subseteq R/I_2$。定义$f : R/I_2 \to R/I_1$，$f(r + I_2) = r + I_1$。当$r_1 + I_2 = r_2 + I_2$时，$r_1 - r_2 \in I_2$，而$I_2 \subseteq I_1$，所以$r_1 - r_2 \in I_1$，从而$r_1 + I_1 = r_2 + I_1$。所以映射$f$与代表元选取无关。显然，$f$是满射。对于$r_1, r_2 \in R$，

$$\begin{aligned}f((r_1 + I_2) + (r_2 + I_2)) &= f((r_1 + r_2) + I_2) = (r_1 + r_2) + I_1 \\ &= (r_1 + I_1) + (r_2 + I_1) = f((r_1 + I_2)) + f((r_2 + I_2)), \\ f((r_1 + I_2) \cdot (r_2 + I_2)) &= f((r_1 \cdot r_2) + I_2) = (r_1 \cdot r_2) + I_1 \\ &= (r_1 + I_1) \cdot (r_2 + I_1) = f((r_1 + I_2)) \cdot f((r_2 + I_2)), \\ f(1_{R_1} + I_2) &= 1_{R_1} + I_1,\end{aligned}$$

所以，f是从环R/I_2到环R/I_1的满同态映射。

$$\mathrm{Ker} f = \{r + I_2 | r + I_1 = I_1\} = \{r + I_2 | r \in I_1\} = I_1/I_2.$$

由环同态基本定理知，$\frac{R/I_2}{I_1/I_2} \cong R/I_1$。证毕。

7.7 素理想和极大理想

I是环R的理想，则R/I是环。那么什么样的理想能使R/I为整环或者为域呢？以整数环$\langle \mathbb{Z}, +, \cdot \rangle$为例。整数环$\mathbb{Z}$的所有理想都是主理想。设$p$为素数，$(p) = \{k \cdot p | k \in \mathbb{Z}\}$是$\mathbb{Z}$的理想。

$$\mathbb{Z}/(p) = \{(p), 1 + (p), \cdots, p - 1 + (p)\} \cong \mathbb{Z}_p.$$

如果$(i + (p)) \cdot (j + (p)) = (p)$，即$i \cdot j \in (p)$，$p | i \cdot j$，由素数的性质知$p | i$或$p | j$。因此，$i + (p) = (p)$或$j + (p) = (p)$。所以，$\mathbb{Z}/(p)$ 是整环。由此引出素理想的概念。

定义 7.12. I是非平凡交换环R的理想，$I \neq R$。对于R的任意元素a, b，如果$a \cdot b \in I$，必有$a \in I$ 或$b \in I$，那么称I为环R的**素理想**。

定理 7.18. I是非平凡交换环R的理想。R/I是整环当且仅当I是素理想。

证明： 假设R/I是整环。对R中的任意元素a, b，如果$a \cdot b \in I$，则$(a + I) \cdot (b + I) = a \cdot b + I = I$。由于$R/I$中没有零因子，所以必有$a + I = I$或者$b + I = I$ (I是R/I的零元)。于是，$a \in I$ 或者$b \in I$。所以I是素理想。

反之，如果I是环R的素理想。在环R/I中，若$(a+I) \cdot (b+I) = a \cdot b + I = I$，则必有$a \cdot b \in I$。因为$I$是素理想，所以$a \in I$或者$b \in I$，即$a + I = I$ 或者$b + I = I$。这说明R/I中没有零因子。所以R/I是整环。证毕。

例 7.22. 证明主理想环$F[x]$的任意理想(x)都是素理想，其中F是域。

证明： 设(x)是$F[x]$的一个理想，商环

$$F[x]/(x) = \{f(x) + (x) | f(x) \in F[x]\} = \{a + (x) | a \in F[x]\}.$$

定义$\varphi : F[x]/(x) \to F$，$\varphi(a+(x)) = a$，易证φ是环同构映射。因此，$F[x]/(x) \cong F$，$F[x]/(x)$是整环，由定理7.18知，(x)是素理想。证毕。

定义 7.13. I是环R的理想，$I \neq R$。若$I \subset M$，M是R的理想，则必有$M = R$。称这样的理想I是R的**极大理想**。

例 7.23. 整数环$\mathbb{Z}$中，p是素数，(p)是$\mathbb{Z}$的素理想，也是$\mathbb{Z}$的极大理想。这是因为，若M是$\mathbb{Z}$的理想并且$(p) \subset M$，则M中必有元素$m \notin (p)$，即$m = kp + l$，$0 < l < p$。因为$m, p \in M$，所以$l = m - kp \in M$。若$l \neq p$，则l与p互素，存在$a, b \in \mathbb{Z}$使$la + pb = 1$，因此$1 \in M$，与定理*7.10*的证明类似，可得$M = \mathbb{Z}$。

例 7.24. 域F上的多项式环$F[x]$中，(x)是$F[x]$的素理想，也是$F[x]$的极大理想。这是因为如果M是$F[x]$的理想且$(x) \subset M$，则M中存在$f(x) \notin (x)$，即$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in M$，$a_0 \neq 0$ *(*因为$f(x) \notin (x)$*)*。令$f(x) = f_1(x) + a_0$，$f_1(x) \in (x) \subset M$，由此可得$a_0 \in M$。而a_0是域F的非零元素，所以是F的可逆元，也是$F[x]$的可逆元。也就是说，$F[x]$的理想M包含可逆元a_0，由定理*7.10*知，$M = F[x]$。

定理 7.19. I是非平凡交换环R的理想。R/I是域当且仅当I是极大理想。

证明: 已知R/I是域，$I \neq R$。若$I \subset M$，M是R的理想，那么存在$a \in M$且$a \notin I$。显然，$a + I$是域R/I的非零元素，它的乘法逆元是$x + I$，即$(a+I)\cdot(x+I) = 1_R + I$。因为$a \in M$，$x \in R$，$M$是$R$的理想，所以$a \cdot x \in M$。又$I \subset M$，故$1_R + I = (a+I)\cdot(x+I) = a\cdot x + I \subseteq M$，故有$1_R \in M$，从而$M = R$。即$I$是极大理想。

反之，I是极大理想，任取$a \notin I$，$a + I$是R/I的非零元素。如果$x + I$是$a + I$的乘法逆元，那么x应该满足

$$(a+I)\cdot(x+I) = a\cdot x + I = 1_R + I,$$

即$a \cdot x - 1_R \in I$。考虑集合

$$A = \{-i + a\cdot x | i \in I, x \in R\}.$$

显然，$I \subset A$，A是R的非空子集。任取$-i_1+a\bullet x_1, -i_2+a\bullet x_2 \in A$，$y \in R$，

$$(-i_1 + a\bullet x_1) - (-i_2 + a\bullet x_2) = -(i_1 - i_2) + a(x_1 - x_2) \in A,$$
$$(-i_1 + a\bullet x_1)\bullet y = -i_1\bullet y + a\bullet(x_1\bullet y) \in A,$$

因此，A是R的理想，且$I \subset A$。由于I是极大理想，所以$A = R$，于是R的乘法单位元$1_R \in A$。因此存在$i_0 \in I, x_0 \in R$使得$1_R = -i_0 + a\bullet x_0$，即$a\bullet x_0 - 1_R = i_0 \in I$。因此，$x_0 + I$是$a + I$的乘法逆元。有$a + I$的任意性可知，$R/I$是域。证毕。

如果I是非平凡交换环R的极大理想，那么R/I是域；而域又是整环，所以R/I是整环，进而得出I是R的素理想。故有下面的推论：

推论 7.1. 非平凡交换环的极大理想一定是素理想。

此推论的逆命题不一定成立。例如整数环$\mathbb{Z}$上的多项式环$\mathbb{Z}[x]$，(x)是$\mathbb{Z}[x]$的素理想。$\mathbb{Z}[x]/(x) \cong \mathbb{Z}$，而$\mathbb{Z}$不是域，故$(x)$不是$\mathbb{Z}[x]$的极大理想。

习题

1. 下列代数系统哪些是环?

(1) $\langle \mathbb{Z}\times\mathbb{Z}, +, \bullet\rangle$，其中$+$与$\bullet$均是对分量的运算；

(2) $\langle 2\mathbb{Z}\times\mathbb{Z}, +, \bullet\rangle$，其中$+$与$\bullet$同上；

(3) $\langle \mathbb{R}, +, *\rangle$，其中$+$是实数加法，$a * b = |a|\bullet b$。

2. 写出下列各环的全部可逆元。

(1) $\langle \mathbb{Z}, +, \bullet\rangle$； (2) $\langle \mathbb{Z}, +, \bullet\rangle$；

(3) $\langle \mathbb{Z}_4, +, \bullet\rangle$； (4) $\langle \mathbb{Z}_6, +, \bullet\rangle$。

3. 在环$\langle R, +, \bullet\rangle$中，如果$\langle R, +\rangle$是循环群，则$\langle R, +, \bullet\rangle$是交换环。

4. 在环R中，如果对于任意$a \in R$均有$a^2 = a$，则称该环是布尔环。证明：

(1) $\forall a \in R$，$2a = 0_R$；

(2) R是交换环。

5. 下列环中哪些是整环，哪些是域? 说明理由。

(1) $\langle\mathbb{Z}\times\mathbb{Z},+,\bullet\rangle$;

(2) $\langle\{a+b\sqrt{2}|a,b\in\mathbb{Z}\},+,\bullet\rangle$;

(3) $\langle\{a+b\sqrt{3}|a,b\in\mathbb{Q}\},+,\bullet\rangle$。

6. 若a是环R的可逆元，则

(1) $-a$也是可逆元;

(2) a不是零因子。

7. 在交换环中，若$a\bullet b$是零因子，则a是零因子或b是零因子。

8. E加群$\langle G,+\rangle$的自同态环，如果H是G的子群，那么

$$E_H=\{f|f\in E,f(H)\subseteq H\}$$

是E的子环。

9. 一个环的任意两个子环的交仍是子环。

10. 令$f:\mathbb{Z}\times\mathbb{Z}\to Z$，$f(a,b)=a$。证明$f$是从环$\langle\mathbb{Z}\times\mathbb{Z},+,\bullet\rangle$到环$\langle\mathbb{Z},+,\bullet\rangle$的同态映射，并求$\mathrm{Ker}f$。

11. 求出环$\mathbb{Z}_6$的所有理想。

12. 若I_1和I_2是环R的理想，则$I_1\cap I_2$，$I_1\bullet I_2$，I_1+I_2都是R的理想，并且$I_1\bullet I_2\subseteq I_1\cap I_2$。

13. 证明$I=\left\{\begin{pmatrix}0&2x\\0&0\end{pmatrix}\middle|x\in\mathbb{Z}\right\}$是$R=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix}\middle|a,b,c\in\mathbb{Z}\right\}$的理想。商环$R/I$是由哪些元素构成的?

14. 在高斯整数环$\mathbb{Z}[\mathrm{i}]=\{a+b\mathrm{i}|a,b\in\mathbb{Z}\}$中，$I=(2+\mathrm{i})$含有哪些元素? $\mathbb{Z}[\mathrm{i}]/(2+\mathrm{i})$含有哪些元素?

15. 令$R=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|a,b,c,d\in\mathbb{Z}\right\}$，$I=\left\{\begin{pmatrix}2m&2n\\2k&2l\end{pmatrix}\middle|m,n,k,l\in\mathbb{Z}\right\}$。

(1) 证明I是R的理想;

(2) R/I是由哪些元素组成的?

16. $\mathbb{Q}[x]$是有理数域$\mathbb{Q}$上的多项式环，证明$(2,x)$是$\mathbb{Q}[x]$的主理想。

17. $F[x]$是数域F上的多项式环。在$F[x]$上定义运算$f(x)\bullet g(x)=f(g(x))$。则$\langle F[x],+,\bullet\rangle$是否是环? 为什么?

18. $\langle\mathbb{Z}_7,+,\bullet\rangle$上的多项式$f(x)=-4+5x+3x^3$，$g(x)=3-x+4x^3$，试计算$f(x)+g(x)$，$f(x)\bullet g(x)$。

19. 域$\langle \mathbb{Z}_2, +, \cdot \rangle$上的多项式$1+x+x^2+\cdots+x^n$有因式$1+x$当且仅当$n$为奇数。

20. 找出从$\mathbb{Z}$到$\mathbb{Z}$的所有同态映射，并写出其同态核。

21. 找出从$\mathbb{Z}$到$\mathbb{Z}_2$的所有同态映射。

22. 证明：$(3)/(6)$是$\mathbb{Z}/(6)$的理想，并且

$$\frac{\mathbb{Z}/(6)}{(3)/(6)} \cong \mathbb{Z}/(3).$$

23. 给定正整数m和r，且$r|m$。用$\overline{a}$表示$\mathbb{Z}_m$中a所在的同余类，$[a]$表示$\mathbb{Z}_r$中a所在的同余类。令$f: \mathbb{Z}_m \to \mathbb{Z}_r$，$f(\overline{a}) = [a]$。

(1) 证明f是环同态映射；

(2) 求$\mathrm{Ker}f$，并找出与$\mathbb{Z}_m/\mathrm{Ker}f$同构的环。

24. 令$\varphi: \mathbb{R}[x] \to \mathbb{R}$，$\varphi(f(x)) = \varphi(a_0 + a_1x + \cdots + a_nx^n) = a_0$。

(1) 证明φ是从环$\mathbb{R}[x]$到环$\mathbb{R}$的满同态映射；

(2) 求$\mathrm{Ker}\varphi$，并找出与$\mathbb{R}[x]/\mathrm{Ker}\varphi$同构的环。

25. 若φ是从环R_1到环R_2的满同态映射，I_1是R_1的理想。证明：

(1) $\varphi^{-1}(\varphi(I)) = I + \mathrm{Ker}\varphi$；

(2) $\varphi(I) = R_2$ 当且仅当$I + \mathrm{Ker}\varphi = R_1$。

26. 整数环$\mathbb{Z}$中，(n)是$\mathbb{Z}$的素理想当且仅当$|n| = 0$或p，其中p是素数。

27. 证明：在环$\mathbb{Z}[x]$中，(x, n)是极大理想当且仅当n为素数。