第 7 章　环

在群只有一种运算的基础上，本章将再添加一种运算，同时两种运算间存在特定的规律将其联系起来，从而构成新的代数系统——环. 从群到环的扩展是一个重要的里程碑，使得代数结构更加丰富和复杂.

本章从环的概念入手，介绍各类具有不同属性的环，并着重考虑新加运算所蕴含的新性质，特别是类似于整数间除法给出环元素间的整除关系等. 同时，类比于群论中子群、正规子群、群同态与同构，给出子环、理想、环同态与同构的定义，并得到相应的环同态基本定理等结果. 最后，着重介绍多项式整环，包括多项式除法、不可约多项式、多项式同余等基础性框架，尝试为更复杂的代数结构的学习与研究提供有力的工具和方法.

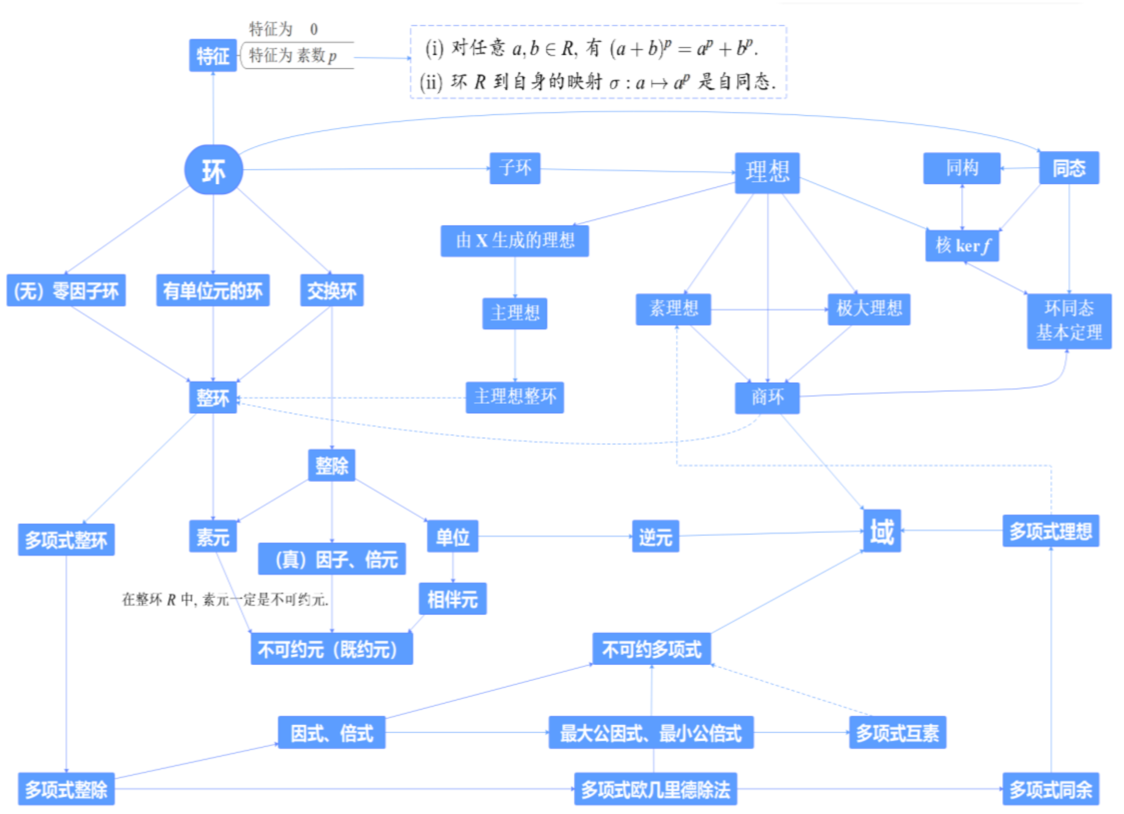

图 7-1 环知识点图谱

7.1 环的定义

定义 7.1.1 设 R 是具有两种运算（通常表示为加法和乘法）的非空集合. 如果下面的条件成立：

(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

$$\left(a+b\right)c=ac+bc \text{ 和 } a\left(b+c\right)=ab+ac,$$

则 R 叫做**环**.

例 7.1.1 整数环$(Z,+,\bullet)$

(i) $(Z,+)$构成交换群. 即满足：①封闭性；②结合律；③单位元（零元）0；④a的逆为$-a$,负元；⑤交换律$a+b=b+a$.

(ii) $(Z,\bullet)$ 构成半群. 即满足：①封闭性，$a\bullet b\in Z(\forall a,b\in Z)$ ②结合律，$(ab)c=a(bc)$.

(iii) 满足分配律:

$$\forall a,b,c\in Z$$
$$\begin{cases} a(b+c)=ab+ac \\ (b+c)a=ba+ca \end{cases}$$

$\therefore(Z,+,\bullet)$是环.

定义 7.1.2 如果环 R 还满足对任意的$a,b\in R$，有 $ab=ba$，则 R 叫做**交换环**.

定义 7.1.3 如果 R 中有一个元素$e=1_R$使得 对任意的$a\in R$，有$a1_R=1_Ra=a$，则 R 叫做**有单位元环**.

例 7.1.2 实数环$\left(R,+,\bullet\right)$有单位元，则 R 叫做有单位元的环.

定理 7.1.1 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$\left(-a\right)b=a\left(-b\right)=-ab$；

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

(iv) 对任意$n\in Z$，任意$a,b\in R$，有$\left(na\right)b=a\left(nb\right)=nab$；

(v) 对任意$a_i,b_j\in R$，有

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

定理 7.1.2 设 R 是有单位元的环，设 n 是正整数，$a,b,a_1,\cdots a_r \in R$.

(i) 如果 $ab=ba$，则

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

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

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

定义 7.1.4 设 a 时环 R 中的一个非零元. 如果存在非零元 $b\in R$(对应地，$c\in R$)使得 $ab=0$(对应地，$ca=0$)，则称 a 为**左零因子**（对应地，**右零因子**）. 如果同时为左零因子和右零因子，则称 a 为**零因子**.

例 7.1.3 针对 $\left(Z_6,+,\bullet\right)$，其中

$Z_6=Z/6Z=\left\{[0],[1],[2],[3],[4],[5]\right\}=\left\{0,1,2,3,4,5\right\}=\left\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\right\}$，

"+"是 $\oplus_6$,"$\bullet$"是 $\otimes_6$.

$\because$ [2][3] = [0] = [3][2].

$\therefore[2]$是零因子,$[3]$是零因子.

综述：Z_6 是一个交换环，$[a][b]=[b][a]$；有单位元 $[1]$；有零因子环.

$\therefore\left(Z_6,+,\bullet\right)$是一个有零因子，单位元的交换环.

例 7.1.4 针对 $\left(Z_5,+,\bullet\right)$，其中

$Z_5=Z/5Z=\left\{[0],[1],[2],[3],[4]\right\}=\left\{0,1,2,3,4\right\}=\left\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\right\}$,

"+"是 $\oplus_5$,"$\bullet$"是 $\otimes_5$.

Z_5 是一个交换环，$[a][b]=[b][a]$；有单位元 $[1]$；无零因子环.

定义 7.1.5 设 a 是有单位元 1_R 的环 R 中的一个元. 如果存在 b, 使得 $ab=1_R$，则称 a 为**左逆元**，这时 b 叫做 a 的**右逆元**. 如果同时为左逆元和右逆元，则称 a 为**逆元**.

例 7.1.5 有理数 Q，$\left(Q,+,\bullet\right)$满足

1) $\left(Q,+\right)$交换加群.

2) $(Q,\bullet)$ 半群.

3) 满足分配律.

$\therefore (Q,+,\bullet)$ 是环，有单位元 1，无零因子，$\forall a \in Q$，逆元存在 $a^{-1}=\dfrac{1}{a}$.

希望一些环具有整数环 Z 的一些性质.

定义 7.1.6 设 R 是一个交换环，如果 R 中有单位元，但没有零因子，则称 R 为**整环**.

例 7.1.6 整数 Z，$(Z,+,\bullet)$；有理数 Q，$(Q,+,\bullet)$ 均为整环.

我们也希望整数环的整除性也可以应用到环上.

定义 7.1.7 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 $a = bc$，就称 b **整除** a 或者 a 被 b 整除，记作 $b \mid a$.

(i) 当 b 整除 a 时，把 b 叫做 a 的**因子**，把 a 叫做 b 的**倍元**. 而且如果此时 b, c 都不是单位元，就称 b 为 a 的**真因子**.

(ii) 对于 R 中的元素 p，如果 p 不是单位元，且没有真因子，则称 p 为**不可约元**或**既约元**. 也就是说，此时如果有元素 $b,c \in R$ 使得 $p = bc$，则 b 或 c 一定是单位元.

(iii) 设 p 是环 R 中的非零元, 如果 p 不是单位, 且当 $p \mid ab$ 时, 有 $p \mid a$ 或 $p \mid b$, 则称 p 为**素元**.

(iv) 两个元素 $a,b \in R$，如果存在可逆元 $u \in R$ 使得 $a = bu$，称 a 和 b 为**相伴**的.

定义 7.1.8 设 R 为交换环. 如果 R 中有单位元，且每个非零元都有可逆元，即 R 对于加法构成一个交换群，$R^{*} = R \setminus \{0\}$ 对于乘法构成一个交换群. 同时，R 中的加法和乘法运算满足分配律：$\forall a,b \in R, a(b+c) = ab + ac$. 则称 R 是一个**域**.

例 7.1.7 有理数 Q，$(Q,+,\bullet)$ 是域，称为有理数域.

实数 R，$(R,+,\bullet)$ 是域，称为实数域.

复数 C，$(C,+,\bullet)$ 是域，称为复数域.

例 7.1.8 设 p 是素数，$Z_p = \{[0],[1],[2],\cdots,[p-1]\}$，对 $(Z_p,+,\bullet)$，有

(i) $(Z_p,+)$ 是交换加群.

(ii) $\left(Z_p^{\,*},\bullet\right)$是交换乘群.

(iii) $\forall a,b,c\in Z_p, a\bullet(b+c)=a\bullet b+a\bullet c$.

$\therefore\left(Z_p,+,\bullet\right)$构成域.

例 7.1.9 $GF(2)=\{[0],[1]\}$称为二元域.

在$\left(GF(2),+,\bullet\right)$中,

$+$即"$\oplus_2$"，“模 2 加”，可由数字信号的“异或”实现;

$\bullet$即"$\otimes_2$"，“模 2 乘”，可由数字信号的“与”实现.

所以，二元域$GF(2)$是信息科学技术领域及信息安全领域应用最多的域之一.

7.2 环同态与同构

本节讨论两个环之间的关系.

定义 7.2.1 设R,R'是两个环，如果映射$f:R\to R'$满足如下条件：

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

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

则称映射$f:R\to R'$为**环同态**. 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 7.2.2 设R,R'是两个环，如果存在一个R到R'的同构，则称R,R'为**环同构**.

定义 7.2.3 设R是一个环. 如果存在一个最小正整数n使得对任意$a\in R$,都有$na=0$，则称环R的**特征**为n. 如果不存在这样的正整数，则称环R的特征为 0.

例 7.2.1 $Z_5=\{[0],[1],[2],[3],[4]\}, n=5$.

5[1]=[1]+[1]+[1]+[1]+[1]=[0]且对于任意 $0<m\le 4$, $m[1]\ne[0]$.

另有 5[0]=[0], 5[2]=[0], 5[3]=[0], 5[4]=[0].

$\therefore\left(Z_5,+,\bullet\right)$的特征为$n=5$.

注：①无零因子环R的特征是有限整数n，那么n是一个素数.

②在没有零因子的环 R 里，所有不等于零的元，对于加法来说，阶都是一样的.

定理 7.2.1 设 R 是有单位元的交换环，如果环 R 的特征是素数 p，则对任意 $(a,b)\in R$，有

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

证 我们有

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

对于 $1 \le k \le p-1$，有 $\left(p, k!(p-k)!\right) = 1$，

从而 $p \mid p\dfrac{(p-1)!}{k!(p-k)!}$，

这样，由 R 得特征是素数 p 得到 $\dfrac{p!}{k!(p-k)!} a^k b^{p-k} = 0$.

因此，结论成立.

定理 7.2.2 如果域 K 的特征不为零，则其特征为素数.

证 设域 K 的特征为 n. 如果 n 不是素数，则存在整数 $1 < n_1, n_2 < n$，使得 $n = n_1 n_2$.

$\therefore$ 对不等于零的元 a, $n_1 a \ne 0$，$n_2 a \ne 0, (n_1 a)(n_2 a) = (n_1 n_2) a^2 = n a^2 = 0$.

因为域中没有零因子，所以与 $(n_1 a)(n_2 a) = 0$ 矛盾.

所以 n 是素数.

7.3 子环

7.3.1 子环的定义

定义 7.3.1 一个环 $(R,+,\bullet)$ 的非空子集 $S(S \subset R)$，假如 S 对于 R 的代数运算做成一个环，称 S 为 $(R,+,\bullet)$ 的**子环**. 相应地，一个域 $(F, +, \bullet)$ 的子集 $S(S \subset F)$，假如 S 对于域 F 的代数运算做成一个域，称 S 为 $(F, +, \bullet)$ 的**子域**.

例 7.3.1 整数环 $(Z,+,\bullet)$ 是 $(Q,+,\bullet)$ 的子环.

例 7.3.2 证明：$Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in Q\}$ 是 $(R,+,\bullet)$ 的子环.

证　显然$Q\left(\sqrt{2}\right)$非空，是实数集合 R 的子集.

$\forall x=\left(a_1+b_1\sqrt{2}\right),\quad y=\left(a_2+b_2\sqrt{2}\right)\in Q\sqrt{2}$，

$x\text{-}y=\left(a_1+b_1\sqrt{2}\right)\text{-}\left(a_2+b_2\sqrt{2}\right)=\left(a_1\text{-}a_2\right)+\left(b_1\text{-}b_2\right)\sqrt{2}\in Q\sqrt{2}$，

$x\cdot y=\left(a_1+b_1\sqrt{2}\right)\cdot\left(a_2+b_2\sqrt{2}\right)=\left(a_1a_2+2b_1b_2\right)+\left(a_1b_2+a_2b_1\right)\sqrt{2}\in Q\sqrt{2}$，

所以$\left(Q\sqrt{2},+,\bullet\right)$是$\left(R,+,\bullet\right)$的子环.

7.3.2 理想与商环

接下来讨论一种特别重要的子环，就是理想. 理想在环论里的地位与正规子群在群论里的地位类似.

定义 7.3.2　设 R 是一个环，I 是 R 的子环.

如果对任意$r\in R$和对任意的$a\in I$，都有$ra\in I$，则称 I 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$ar\in I$，则称 I 为 R 的**右理想**.

如果 I 同时为左理想和右理想，则称 I 为 R 的**理想**.

例 7.3.3 找出模 6 的剩余类环 R 的所有理想.

解　设模 6 的剩余类环为$R=\{[0],[1],[2],[3],[4],[5]\}$.

若 I 是 R 的理想，

则$(I,+)$是$(R,+)$的子群.

因为$(R,+)$是循环群，所以$(I,+)$一定是循环群，有生成元.

又因为$(R,+,\bullet)$是一个有单位元的交换群，所以生成的理想都是主理想.

即$(a)=\{ra\mid\forall r\in R\}$.

$([0])$生成的理想为$\{[0]\}$，

$([1])$生成的理想为$\{[0],[1],[2],[3],[4],[5]\}=R$，

$([2])$生成的理想为$\{[0],[2],[4]\}$，

$([3])$生成的理想为$\{[0],[3]\}$，

$([4])=([2]),([5])=([1])$.

所以所有理想共有 4 个，分别为$\{[0]\}$，$\{[0],[3]\}$，$\{[0],[2],[4]\}$，R.

定理 7.3.1 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，$ar\in I$）.

注：(1)“理想$\leftrightarrow$子环”的关系如下：

A. 理想一定是子环：由(i)可知理想 I 是一个加群，由(ii)可知 I 对于乘法是封闭的.

B. 由(ii), 不仅要求 I 的两个元的乘积必须在 I 里，而且进一步要求 I 的一个任意元与 R 的一个任意元的乘积都必须在 I 里.

所以一个理想所适合的条件比一般子环要强些.

(2) 设$(R,+,\bullet)$是一个环，I 是 R 的理想，则 I 是$(R,+)$的正规子群.

注：一个环是不是一定有理想？ 是！

至少有 2 个理想：

(i) **零理想**：$I=\{0\}$ 只含有零元的集合.

(ii) **单位理想**：$I=R$ R 本身.

例 7.3.3 $\{0\}$和 R 都是 R 的理想，叫做 R 的**平凡理想**.

例 7.3.4 两个理想的交集还是理想.

证 设H_1与H_2是环R的两个理想. 要证$H_1\bigcap H_2$是理想，只需证明：

① $\forall a,b\in H_1\bigcap H_2, a-b\in H_1\bigcap H_2$.

② $\forall r\in R, a\in H_1\bigcap H_2, ar\in H_1\bigcap H_2, ra\in H_1\bigcap H_2$.

事实上,

① 对于$\forall a,b\in H_1\bigcap H_2$有$a\in H_1, a\in H_2, b\in H_1, b\in H_2$.

$\because H_1$ 是理想，$\therefore a\text{-}b\in H_1$.

又$\because H_2$ 是理想，$\therefore a\text{-}b\in H_2$.

$\therefore a-b\in H_1\bigcap H_2$.

② 设$\forall r\in R,\forall a\in H_1\bigcap H_2$，

$\therefore a\in H_1, a\in H_2$，$\because H_1$是理想,$\therefore ar\in H_1, ra\in H_1$.

$\because H_2$是理想，$\therefore ar \in H_2, ra \in H_2$.

$\therefore ar \in H_1 \bigcap H_2, ra \in H_1 \bigcap H_2$.

综上，$H_1 \bigcap H_2$是环R的两个理想.

例 7.3.5 设$\{A_i\}_{i\in I}$是环R中的一族理想，则$\bigcap_{i\in I} A_i$也是一个理想.

与此相关的，还有以下结论：

① 两个子群的交，是子群.

② 两个正规子群的交，是正规子群.

③ 两个子环的交，是子环.

④ 两个子整环的交，是子整环.

⑤ 两个子域的交，是子域.

⑥ 两个理想的交，是理想.

定义 7.3.3 设X是环R的一个子集，设$\{A_i\}_{i\in I}$是环R中包含X的所有（左）理想，则$\cap_{i\in I} A_i$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$X=\{a_1,\cdots a_n\}$，则理想(X)记为$(a_1,\cdots a_n)$，称为**有限生成的**. 特别地，由一个元素生成的理想(a)叫做**主理想**.

定理 7.3.2 环$(R,+,\bullet)$，$\forall a\in R$，由a生成的主理想可表示为如下形式的元素：

$$(a)=\left\{\sum_{i=1}^{m} x_i a y_i + sa + at + na \mid x_i, y_i, s, t \in R, n \in Z\right\}.$$

注：（i）两个这种形式的元相减，显然还是一个这种形式的元.

（ii）对$r\in R$，左乘(a)的一个元，也得到一个这种形式的元，即

$$\left[(rx_1)ay_1+(rx_2)ay_2+\cdots+(rx_m)ay_m+rat\right]+(rs+nr)a.$$

（iii）同理，$\forall r\in R$，用r右乘上面的任意一元，情形一样.

所以，包含a的理想为(a)，或者由a生成的理想为(a).

一个主理想(a)的元的形式，并不是永远像上面那样复杂.

① 当 R 是交换环时，(a) 的元显然都可以写成

$$ra+na,(r\in R,n\in Z).$$

② 当 R 有单位元的时候，(a) 的元都可以写成

$$\sum x_i a y_i,(x_i,y_i\in R).$$

因为此时 $sa=sa\cdot I_R,\quad at=I_R\cdot at,\quad na=(nI_R)aI_R$.

③ 当 R 既是交换环，又有单位元时，(a) 的元形式特别简单，可以写成

$$ra\quad (r\in R).$$

定义 7.3.5 如果环 R 的所有理想都是主理想，则称 R 为**主理想环**.

例 7.3.6 整数环 $(Z,+,\bullet)$ 有单位元，交换环，元素 $1\in Z$，则

(*i*) $(1)=\{r\cdot 1\mid r\in Z\}=Z$，单位理想.

(*ii*) $(0)=\{r\cdot 0\mid r\in Z\}=\{0\}$，零理想.

(*iii*) $(2)=\{r\cdot 2\mid r\in Z\}=\{\text{偶数}\}$，偶数环.

(*iv*) $(3)=\{r\cdot 3\mid r\in Z\}=\{\cdots,-3,0,3,\cdots\}$.

现在，设 $(R,+,\bullet)$ 是一个环，I 是 R 的理想，则 I 是 $(R,+)$ 的正规子群.

我们考虑陪集集合 $\{a+I,b+I,c+I,\cdots\}=R/I$，组成的商集，定义以下

运算：$+:(a+I)+(b+I)=(a+b)+I$.

$\bullet:(a+I)\bullet(b+I)=(a\bullet b)+I.$

可知，$(R/I,+,\bullet)$满足：

（*i*）$(R/I,+)$ 构成商群，可交换；

（*ii*）$(R/I,\bullet)$ 构成半群：

i) 封闭性：$\forall a+I,b+I,(a+I)\bullet(b+I)=(a\bullet b)+I\in R/I.$

ii) 结合律：$[(a+I)\bullet(b+I)]\bullet(c+I)=[(ab)\bullet c]+I=[a\bullet(bc)]+I$

$$=(a+I)\bullet[(b+I)\bullet(c+I)].$$

iii）分配律：

$$(a+I)[(b+I)+(c+I)]=(a+I)\cdot[(b+c)+I]=[a\cdot(b+c)]+I=[ab+ac]+I$$
$$=(ab+I)+(ac+I)=(a+I)\cdot(b+I)+(a+I)\cdot(c+I).$$

同理，$[(b+I)+(c+I)]\bullet(a+I)=(b+I)\bullet(a+I)+(c+I)\bullet(a+I)$.

$\therefore (R/I,+,\bullet)$构成环，称其为**商环**.

定理 7.3.3 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：

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

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.

例 7.3.7 做出环 Z_6 关于主理想 $(3)=\{0,3\}$ 的商环 $Z_6/(3)$ 的运算表.

解：$\because (3)=\{0,3\}, Z_6=\{0,1,2,3,4,5\}$.

$\therefore Z_6$ 关于 (3) 的陪集有 3 个，

即 $(3)=(3)+0=\{0,3\}$，$1+(3)=\{1,4\}$，　$2+(3)=\{2,5\}$.

故 $Z_6/(3)=\{(3),1+(3),2+(3)\}$.

而由 $(a+H)+(b+H)=(a+b)+H,(a+H)\cdot(b+H)=ab+H$，得到

+	(3)	1+(3)	2+(3)
(3)	(3)	1+(3)	2+(3)
1+(3)	1+(3)	2+(3)	(3)
2+(3)	2+(3)	(3)	1+(3)

•	(3)	1+(3)	2+(3)
(3)	(3)	(3)	(3)
1+(3)	(3)	1+(3)	2+(3)
2+(3)	(3)	2+(3)	1+(3)

现在，给出环同态基本定理

定理 7.3.4 设 f 是环 R 到 R' 的同态，则 $\ker f$ 是 R 的理想. 设 I 是环 R 的理想，规定

$$\begin{aligned} S: R &\to R/I \\ r &\mapsto I+r \end{aligned},$$

则 S 是 $R\to R/I$ 的满同态映射（称为 $R\to R/I$ 的自然同态）且 $\ker f=I$.

证 $i)$ $\because$ 对$\forall a,b\in\ker f, f(a)=f(b)=0$.

$\therefore f(a-b)=f(a)-f(b)=0-0=0$.

$\therefore a-b\in\ker f$.

$ii)$ $\because$ 对$\forall r\in R, a\in\ker f$，$\therefore f(a)=0$.

$$f(ra)=f(r)f(a)=f(r)\cdot 0=0,\quad \therefore ra\in\ker f.$$

$$f(ar)=f(a)f(r)=0\cdot f(r)=0,\quad \therefore ar\in\ker f.$$

综上，$\ker f$ 是 R 的理想.

定理 7.3.5（环同态基本定理） 设 f 是环 R 到 R' 的同态，则存在唯一的 $R/\ker f$ 的像子环 $f(R)$ 的同构 $\overline{f}: r+I\mapsto f(r)$ 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，$i:c\mapsto c$是$f(R)$到R'的恒等同态. 即有如下的交换图：

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

定义 7.3.6 设 P 是环 R 的理想. 如果$P\neq R$，且对任意的理想$A,B,\ AB\subset P$，有$A\subset P$或$B\subset P$，则称 P 为 R 的**素理想**.

定理 7.3.6 设 P 是环 R 的理想. 如果$P\neq R$，且对任意的$a,b\in R$，当$ab\in P$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，则对于任意 a, b∈P, ab∈P, 有$a\in P$或$b\in P$.

证 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$ab\in AB\subset P$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，且 R 是交换环，则对任意的$a,b\in R$，满足$ab\in P$，有$(a)(b)=(ab)\subset P$. 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$b\in P$.

例 7.3.8 设 R 是整环，零理想$\{0\}$是素理想.

事实上，$\forall a,b\in R,$若$ab\in\{0\},$即$ab=0$.

$\because R$是整环，无零因子. $\therefore a=0$或$b=0$，即$a\in\{0\}$或$b\in\{0\}$.

$\therefore\{0\}$是素理想.

例 7.3.9 设 p 是素数，则 $P=(p)=pZ$ 是 Z 的素理想.

证 $(p)=\{rp \mid r\in Z, p是素数\}$.

对任意的整数 a, b,

若 $ab\in P=(p)$，则 $p\mid ab$.

因为 p 是素数，所以有 $p\mid a$ 或 $p\mid b$.

由此得到 $a\in P$ 或 $b\in P$.

根据定理 7.3.6，$P=(p)=pZ$ 是 Z 的素理想.

定理 7.3.7 在有单位元 $1_R\neq 0$ 的交换环 R 中，理想 P 是素理想的充要条件是商环 R/P 是整环.

证 $\Rightarrow$（i）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 $1_R+P\neq P$.

（ii）现在说明 R/P 无零因子.

事实上. 若 $(a+P)(b+P)=ab+P=P$，则 $ab+P=P$.

因此，$ab\in P$.

但 P 是交换环 R 的素理想，根据定理 7.3.6，得到 $a\in P$ 或 $b\in P$，即 $a+P=P$ 或 $b+P=P$ 是 R/P 的零元.

（iii）R/P 是交换环.

事实上，因为 $(a+P)(b+p)=ab+P$，而 R 是交换环，即 $ab=ba$，

所以，$(a+P)(b+p)=ab+P=ba+p=(b+p)(a+P)$.

故商环 R/P 是整环.

$\Leftarrow$ 反过来，对任意的 $a,b\in R$，满足 $ab\in P$，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 7.3.6，理想 P 是素理想.

定义 7.3.7 设 M 是环 R 的(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 $N=R$，则称 M 为 R 的**最大（左）理想**.

定理 7.3.8 在有单位元的非零环 R 中，最大（左）理想总是存在的. 事实上，R 的每个

（左）理想（$\neq R$）都包含在一个最大（左）理想中.

定理 7.3.9 设 R 是一个理想，如果 $R^2=R$（特别地，如果 R 有单位元），则 R 的每个最大理想是素理想.

7.4 多项式整环

本节考虑多项式环. 因为多项式理论和方法对于研究后续域的结构起到关键性作用，在信息安全和密码领域也有着重要的应用，所以需进一步介绍其更多的性质.

7.4.1 多项式整环与不可约多项式

定义 7.4.1 设 $(R,+,\bullet)$ 是整环，x 为变量，

$f(x)=a_nx^n+\cdots+a_1x+a_0$，其中 $a_i\in R$，

则称 $f(x)$ 为**环 R 上的**（一元）**多项式**. 此时，

(i) a_i 称为多项式 $f(x)$ 的**系数**，$a_i\in R$.

(ii) 若 $a_n\neq 0$，则称多项式 $f(x)$ 的**次数**为 n，记为 $\deg f=n$.

我们考虑整环 R 上的全体多项式组成的集合 $R[X]$.

首先，定义 $R[X]$ 上的加法. 设

$$f(x)=a_nx^n+\cdots a_1x+a_0,$$
$$g(x)=b_nx^n+\cdots b_1x+b_0$$

定义 $f(x)$ 和 $g(x)$ 的加法为

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

则 $R[X]$ 中的零元为 0，

$$f(x)\text{ 的负元为}(-f)(x)=(-a_n)x^n+\cdots+(-a_1)x+(-a_0).$$

其次，定义 $R[X]$ 上的乘法. 设

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

定义 $f(x)$ 和 $g(x)$ 的乘法为

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

其中 $c_k=\sum_{i+j=k}a_ib_j, 0\le k\le n+m$，即

$$\begin{aligned}&c_{n+m}=a_nb_m,\\&c_{n+m-1}=a_nb_{m-1}+a_{n-1}b_m,\\&\cdots,\\&c_0=a_0b_0\end{aligned}$$

则 $R[X]$ 中的单位元为 1.

综上，$R[X]$ 对于上述加法运算和乘法运算构成一个整环，称其为**多项式整环**.

例 7.4.1 设 $f(x)=x^6+x^4+x^2+x+1, g(x)=x^7+x+1\in F_2[x]$，则

$$f(x)+g(x)=x^7+x^6+x^4+x^2,$$

$$f(x)g(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1.$$

事实上，

$$\begin{aligned}&f(x)g(x)=\left(x^6+x^4+x^2+x+1\right)\cdot\left(x^7+x+1\right)\\&=x^{13}+x^{11}+x^8+x^7\\&\quad+x^7+x^5+x^3+x^2+x\\&\quad+x^6+x^4+x^2+x+1\\&=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1\end{aligned}.$$

例 7.4.2 设 R 是模 7 的剩余类环，计算 $R[x]$ 中乘积 $([3]x^3+[5]x-[4])([4]x^2-x+[3])$.

解：模 7 的剩余类环 $R=\{[0],[1],[2],[3],[4],[5],[6]\}$.

首先把负号变成正号，然后有

原式 $=([3]x^3+[5]x+[3])([4]x^2+[6]x+[3])$

$=[3][4]x^5+[3][6]x^4+\left([3][3]+[5][4]\right)x^3+\left([3][4]+[5][6]\right)x^2+\left([5][3]+[3][6]\right)x+[3][3]$

$=[5]x^5+[4]x^4+x^3+[5]x+[2].$

定义 7.4.2 设 $f(x)$，$g(x)$ 是整环 R 上的任意两个多项式，其中 $g(x)\neq 0$. 如果存在一个多项式 $q(x)$ 使得整式 $f(x)=g(x)q(x)$ 成立，就称 $g(x)$ **整除** $f(x)$ 或者 $f(x)$ 被 $g(x)$ 整除，记作 $g(x)\mid f(x)$.

这时，把 $g(x)$ 叫做 $f(x)$ 的**因式**，把 $f(x)$ 叫做 $g(x)$ 的**倍式**. 否则，就称 $g(x)$ **不能整除** $f(x)$ 或者 $f(x)$ 不能被 $g(x)$ 整除，记作 $g(x)\nmid f(x)$.

定义 7.4.3 设 $f(x)$ 是整环 R 上的非常数多项式. 如果除了因式 1 和 $f(x)$ 外，$f(x)$ 没有其他因式，那么 $f(x)$ 叫做**不可约多项式**，否则，$f(x)$ 叫做**合式**.

例 7.4.3 在 $Z[x]$ 中，多项式 x^2+1 不可约.

7.4.2 多项式的欧几里德除法

定理 7.4.1 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, a_n\neq 0$，$g(x)=x^m+\cdots b_1x+b_0$ $m\geq 1$ 是整环 R 上的两个多项式，则一定存在多项式 $q(x)$ 和 $r(x)$ 使得

$$f(x)=g(x)q(x)+r(x),\quad \deg r<\deg g.$$

注：此过程称为**多项式欧几里德除法**. 上式中的 $q(x)$ 叫做 $f(x)$ 被 $g(x)$ 除所得的**不完全商**，$r(x)$ 叫做 $f(x)$ 被 $g(x)$ 除所得的**余式**.

例 7.4.4 设 $f(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$,

$g(x)=x^8+x^4+x^3+x+1\in F_2[x]$,

求 $q_1(x)$ 和 $r_1(x)$ 使得 $f(x)=g(x)q_1(x)+r_1(x)$，$\deg r_1<\deg g$.

解 逐次消除最高次项，

$$\begin{aligned}&x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1-x^5\left(x^8+x^4+x^3+x+1\right)\\&=x^{11}+x^4+x^3+1\end{aligned}$$

$$\begin{aligned}&x^{11}+x^4+x^3+1-x^3\left(x^8+x^4+x^3+x+1\right)\\&=x^7+x^6+1\end{aligned}$$

因此 $q_1(x)=x^5+x^3$，$r_1(x)=x^7+x^6+1$.

类似于整数中的最大公因数和最小公倍数，我们可以给出多项式环 $R[X]$ 中的最大公因式和最小公倍式.

定义 7.4.4 设 $f(x),g(x)\in R[X]$, 如果 $d(x)\in R[X]$ 满足

(1) $d(x)\mid f(x)$, $d(x)\mid g(x)$.

(2) 若 $h(x)\mid f(x)$, $h(x)\mid g(x)$，则 $h(x)\mid d(x)$.

则称 $d(x)$ 为 $f(x),g(x)$ 的**最大公因式**，记作 $(f(x),g(x))$.

定义 7.4.5 设 $f(x),g(x)\in R[X]$, 如果 $D(x)\in R[X]$ 满足

(1) $f(x)|D(x),g(x)|D(x)$.

(2) 若 $f(x)\mid h(x),g(x)\mid h(x)$，则 $D(x)\mid h(x)$.

则称 $D(x)$ 为 $f(x)$，$g(x)$ 的**最小公倍式**，记作 $[f(x),g(x)]$.

如何求 $(f(x),g(x))$？ 重复使用多项式广义欧几里德除法即得**.**

设 $f(x)$，$g(x)$ 是域 K 上的多项式，$\deg g\ge 1$. 记 $r_0(x)=f(x),r_1(x)=g(x)$. 反复运用多项式欧几里德除法，我们有

$$
\begin{aligned}
&r_0(x)=r_1(x)q_1(x)+r_2(x), \quad 0\le \deg r_2<\deg r_1\\
&r_1(x)=r_2(x)q_2(x)+r_3(x), \quad 0\le \deg r_3<\deg r_2\\
&\qquad\cdots\cdots\\
&r_{k-2}(x)=r_{k-1}(x)q_{k-1}(x)+r_k(x), \quad 0\le \deg r_k<\deg r_{k-1}\\
&r_{k-1}(x)=r_k(x)q_k(x)+r_{k+1}(x), \quad \deg r_{k+1}=0
\end{aligned}
$$

经过有限步骤，必然存在 k 使得 $r_{k+1}(x)=0$.

这是因为

$$0=\deg r_{k+1}<\deg r_k<\deg r_{k-1}<\cdots<\deg r_2<\deg r_1=\deg g,$$

且 $\deg g$ 是有限正整数.

定理 7.4.2 设 $f(x)$, $g(x)$ 是域 K 上的多项式, $\deg g\ge 1$ ，则 $(f(x),g(x))=r_k(x)$，其中 $r_k(x)$ 是多项式广义欧几里德除法中最后一个非零余式.

从多项式广义欧几里德除法中逐次消去 $r_{k-1}(x),r_{k-2}(x),\cdots,r_3(x),r_2(x)$，我们可找到多项式 $s(x),t(x)$ 使得

$$s(x)f(x)+t(x)g(x)=(f(x),g(x)).$$

定理 7.4.3 设 $f(x)$，$g(x)$是域 K 上的多项式，则存在多项式$s(x),t(x)$使得

$$s(x)f(x)+t(x)g(x)=(f(x),g(x)).$$

注：如果 $f(x)$ 与 $g(x)$ 的最大公因式$(f(x),g(x))=1$，则称它们是**互素**（或**互质**）的.

例 7.4.5 设 $f(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1\in F_2[x]$，

$g(x)=x^8+x^4+x^3+x+1\in F_2[x]$，

求多项式$s(x),t(x)$使得 $s(x)f(x)+t(x)g(x)=(f(x),g(x))$.

解：

$x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1-x^5\left(x^8+x^4+x^3+x+1\right)$

$=x^{11}+x^4+x^3+1$.

$x^{11}+x^4+x^3+1-x^3\left(x^8+x^4+x^3+x+1\right)$

$=x^7+x^6+1$.

$\therefore q_1(x)=x^5+x^3, r_1(x)=x^7+x^6+1$.

反复运用广义多项式欧几里德除法，我们有

$$\begin{aligned}
f(x)&=g(x)q_1(x)+r_1(x), & q_1(x)&=x^5+x^3, & r_1(x)&=x^7+x^6+1,\\
g(x)&=r_1(x)q_2(x)+r_2(x), & q_2(x)&=x+1, & r_2(x)&=x^6+x^4+x^3,\\
r_1(x)&=r_2(x)q_3(x)+r_3(x), & q_3(x)&=x+1, & r_3(x)&=x^5+x^3+1,\\
r_2(x)&=r_3(x)q_4(x)+r_4(x), & q_4(x)&=x, & r_4(x)&=x^3+x,\\
r_3(x)&=r_4(x)q_5(x)+r_5(x), & q_5(x)&=x^2, & r_5(x)&=1,\\
r_4(x)&=r_5(x)q_6(x)+r_6(x), & q_6(x)&=x^3+x, & r_6(x)&=0,
\end{aligned}$$

从而，

$$
\begin{aligned}
r_5(x) &= r_3(x)+q_5(x)\big(r_2(x)+r_3(x)q_4(x)\big)\\
&= -q_5(x)q_5(x)+\left(x^3+1\right)\big(r_1(x)+r_1(x)q_2(x)\big)\\
&= \left(x^3+1\right)r_1(x)+\left(x^4+x^3+x^2+x+1\right)\big(g(x)+r_1(x)q_2(x)\big)\\
&= \left(x^4+x^3+x^2+x+1\right)g(x)+\left(x^5+x^3\right)\big(f(x)+g(x)q_1(x)\big)\\
&= \left(x^5+x^3\right)f(x)+\left(x^{10}+x^6+x^4+x^3+x^2+x+1\right)g(x)
\end{aligned}
$$

因此，$s(x)=x^5+x^3, t(x)=x^{10}+x^6+x^4+x^3+x^2+x+1$.

对应的，也可以给出多项式同余的概念.

定义 7.4.6 给定 $R[X]$ 中一个首一多项式 $m(x)$. 如果 $R[X]$ 中的两个多项式 $f(x)$，$g(x)$ 满足 $m(x)\mid f(x)-g(x)$，则称 $f(x)$ 与 $g(x)$ 模 $m(x)$ **同余**，记作

$f(x)\equiv g(x)\big(\bmod m(x)\big)$.

否则，称 $f(x)$ 与 $g(x)$ 模 $m(x)$ **不同余**，记作 $f(x)\not\equiv g(x)\big(\bmod m(x)\big)$.

定义 7.4.7 设 $p(x)$ 是 $R[x]$ 中的多项式,则称 $\big(p(x)\big)=\{f(x)\mid\ p(x)\mid f(x)\}$ 为 $R[x]$ 中的**多项式理想**.

注: 设 $R[x]$ 是整环, 由此可得到商环 $R/(p(x))$. 其中商环 $R/(p(x))$ 上的运算法则是:

$$f(x)+g(x)=(f+g)(x)\ \ \big(\bmod p(x)\big).$$

$$f(x)\cdot g(x)=(f\cdot g)(x)\ \ \big(\bmod p(x)\big).$$

进一步，可以得到:

定理 7.4.4 设 K 是一个域. $p(x)$ 是 $K[X]$ 中的不可约多项式，则商环 $K[X]/(p(x))$ 对于上述运算法则构成一个域.

证 只需要证明 $K[X]/(p(x))$ 中的非零元 $f(x)\big(\bmod p(x)\big)$ 为可逆元.

事实上，对于满足 $f(x)\not\equiv 0\big(\bmod p(x)\big)$ 的多项式 $f(x)$，有 $\big(f(x),p(x)\big)=1$，根据多项式广义欧几里德除法，存在多项式 $s(x),t(x)$，使得

$$s(x)f(x)+t(x)p(x)=1.$$

从而，

$$s(x)f(x)\equiv 1(\bmod p(x)).$$

这说明 $f(x)(\bmod p(x))$为可逆元，$s(x)(\bmod p(x))$为其逆元.

习题

1. 集合$\{a+b\sqrt{5}|a,b\in Z\}$关于实数中通常的加法与乘法是否构成环，说明理由.
2. 证明所有元素为实数的n阶方阵的集合$M(n\times n;R)$，对于矩阵的加法、乘法构成环$(M(n\times n;R),+,\times)$.
3. 设R是有单位元e的环，证明R中的可逆元不是零因子.
4. 找出模 12 剩余类环中的全部零因子.
5. 判别下列集合 S 关于所给运算是否构成环:

   (1) $r\oplus s=2(r+s), r*s=rs, S=\mathbf{R}$;

   (2) $r\oplus s=2rs, r*s=rs, S=\mathbf{R}-\{0\}$;

   (3) $r\oplus s=rs, r*s=rs, S=\mathbf{R}^+$.
6. 证明：集合$Z[\sqrt{3}]=\{a+b\sqrt{3}\mid a,b\in Z\}$.
7. 设$(R,+)$是一个加群. 定义R上的乘法运算为

$$a\cdot b=0,\forall a,b\in R.$$

   证明：R 关于加法和乘法构成一个环.
8. 设$(R,+,\cdot)$为一个环，r为 R 中一个固定元素，$\forall a,b\in R$，定义新的运算：

$$a\oplus b=a+b-r$$
$$a^\circ b=ab-ar-rb+r^2+r$$

   1) 证明：$(R,\oplus,\circ)$也是环.

   2) 证明：$(R,+,\cdot)$与$(R,\oplus,\circ)$同构.
9. 设$\phi: Z_6\longrightarrow Z_2$ 使$\phi(x+\langle 6\rangle)=x+\langle 2\rangle$. 证明: ϕ为Z_6到Z_2的环同态.并求同态的核Ker ϕ.
10. 集合 $S=\left\{\begin{pmatrix}x & y\\ 0 & z\end{pmatrix}|x,y,z\in\mathbf{Z}\right\}$ 按通常矩阵的加法与乘法构成一个环. 令

$$\psi:\quad S\quad\longrightarrow\quad\mathbf{Z}$$
$$\begin{pmatrix}x & y\\ 0 & z\end{pmatrix}\quad\longmapsto\quad z.$$

   (1) 证明：ψ为S 到Z 的满同态;

   (2) 求ψ的核K，并给出S/K 到Z 的一个同构映射.
11. 试求环$Q[\sqrt{2}]$的所有自同构.
12. 设ϕ为环R到环R'的同态. 证明ϕ是单同态的充分必要条件是$Ker\phi=\{0\}$.
13. 环$2\boldsymbol{Z}$与$4\boldsymbol{Z}$是否同构?

14. 设R为一可交换环，$M=\{a\in R|\exists n\in N^{+},a^{n}=0\}$，求证：$M$为$R$的子环。

15. 指出下列集合中哪些是$M_2(\mathbf{R})$ 的子环?

(1) $S=\left\{\begin{pmatrix}0 & b\\ c & d\end{pmatrix}|b,c,d\in\mathbf{R}\right\}$;

(2) $S=\left\{\begin{pmatrix}a & 0\\ c & d\end{pmatrix}|a,c,d\in\mathbf{R}\right\}$;

(3) $S=GL_2(\mathbf{R})$;

(4) $S=\left\{\begin{pmatrix}a & b\\ b & a\end{pmatrix}|a,b\in\mathbf{R}\right\}$.

16. 设$\mathcal{F}(\mathbf{R})$为全体实函数关于函数的加法与乘法所构成的环. 问下列子集中哪些是$\mathcal{F}(\mathbf{R})$的子环?

(1) $S=\{f\in\mathcal{F}(\mathbf{R})\mid f(1)=0\}$;

(2) $S=\{f\in\mathcal{F}(\mathbf{R})\mid f(1)=0$ 或 $f(0)=0\}$;

(3) $S=\{f\in\mathcal{F}(\mathbf{R})\mid f(2)\neq 0\}$;

(4) $S=\{f\in\mathcal{F}(\mathbf{R})\mid f(3)=f(4)\}$.

17. 设$H=\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}|a,b,c,d\in Z\},I$是元素为偶数的所有二阶矩阵的集合。证明：$I$是$(H,+,\cdot)$的理想。

18. 设R为加法群，定义R的乘法为 $a\cdot b=0,\forall a,b\in R$. 证明：$(R,+,\cdot)$为环，并求出$R$的所有理想.

19. 设环$S=\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}|a,b,d\in\mathbf{R}\}$.求$S$的所有理想.

20. 设R 是交换环，I 是R 的理想. 令$\sqrt{I}=\{r\in R|$存在$n\in\mathbb{N}$,使$r^{n}\in I\}$，证明：$\sqrt{I}$是R的理想.

21. 设$a(x)$，$b(x)$是如下所示的多项式，试计算$a(x)+b(x)$和$a(x)\cdot b(x)$在数域F_5上的结果。

$$a(x)=x^{6}+5x^{5}+4x^{4}+3x^{3}+x+3,b(x)=x^{6}+3x^{5}+5x^{4}+6x^{3}+2x+1$$

22. 设R是整环. 证明：对R上的任何非零多项式$f(x),g(x)$，有

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

如果R不是整环，这一结论还成立吗?

23. 设D是欧几里得整环，σ为D的欧几里得映射，满足

$$\sigma(a)\leqslant\sigma(ab),\quad 对任意a,b\in D,a,b\neq 0.$$

证明:

(1) $d\in D$ 是单位当且仅当$\sigma(d)=\sigma(1)$;

(2) 如果$a,b\neq 0,a\sim b$，则$\sigma(a)=\sigma(b)$.