第6章 环和域

具有两种运算的代数结构

6.1 环和域的基本概念

定义 **6.1.1**（环） 设R为某种元素组成的一个非空集合，若在R内定义两种运算（通常表示为加法“$+$”和乘法“$\cdot$”），R中所有元素满足以下条件：

则称R关于“$+$”和“$\cdot$”形成一个环**(Ring)**，记作$(R, +, \cdot)$，通常在不混淆的情况下省略“$+$”和“$\cdot$”，用R来表示一个环。

关于环的概念我们需要注意以下几点：

（一）环的定义中的运算“$+$”与“$\cdot$”是抽象运算，不一定是我们通常在整数中定义的加法和乘法。

（二）当环R中的运算“$\cdot$”满足交换律时，我们称环R为交换环。

（三）当环R中存在元素e，使得对环R中任意一个元素a都有$e\cdot a=a\cdot e=a$时，我们称e为环R的单位元，并且称环R为含单位元的环。

（四）通常在不会混淆时，$a\cdot b$简记为ab；
加法单位元一般记作 **0**，称为零元；乘法单位元一般记作 **1**。
同样这里 **0** 和 **1** 也是抽象元，不同于整数 **0** 和整数 **1**。

（五）由环的定义及群的幂运算，易得环的如下性质：

$$\begin{cases} a^n \cdot a^m = a^{n+m} \\ (a^n)^m = a^{nm} \\ (ab)^n = a^n b^n \text{(仅交换环成立)} \end{cases}, \quad \begin{cases} na + ma = (n+m)a \\ n \cdot ma = nm \cdot a \\ n(a+b) = na + nb \end{cases} 。$$

（六）设a是有单位元 **1** 的环R中的任意一个元素，如果存在$b \in R$，使$ab = 1$（$ba = 1$），则称b为a的一个右逆元（左逆元），记为a_r^{-1}（a_l^{-1}）；

如果a既有右逆元a_r^{-1}，又有左逆元a_l^{-1}，则它们一定相等，因为

$$a_r^{-1} = 1 \cdot a_r^{-1} = (a_l^{-1}a)a_r^{-1} = a_l^{-1}(aa_r^{-1}) = a_l^{-1}e = a_l^{-1},$$

此时称a有逆元，记为a^{-1}。

（七）设R是一个具有单位元 1 的交换环，我们来定义其中的素元或不可约元：

$a,b\in R,b\neq 0$，如果存在$c\in R$，使得$a=bc$，则称b整除a，记作$b\mid a$。b叫做a的因子，a叫做b的倍元。

对$a,b\in R$，如果存在可逆元$c\in R$，使$a=bc$，则称a和b为相伴的。

若b是a的因子，但和a不是相伴的，则b称为a的真因子。

若a不是可逆元、零元，且除可逆元外没有其它真因子，则称a为素元或不可约元。

（八）环R中的零元与其它元素之间的乘法已由环中的分配律给出：

$$ab = a(b-c+c) = a(b-c)+ac \Rightarrow a(b-c) = ab-ac$$

$$ba+(-b)a = (b+(-b))a = (b-b)a = ba-ba \Rightarrow b(-a) = -ba$$

同理 $b(-a) = -ba$，$(-b)(-a) = ba$

$$0\cdot a = (b+(-b))\cdot a = ba+(-b)a = ba+(-ba) = 0$$

$$a\cdot 0 = a\cdot(b+(-b)) = ab+a(-b) = ab+(-ab) = 0$$

$$0\cdot a = (0+0)\cdot a = 0\cdot a+0\cdot a \Rightarrow 0\cdot a = 0$$

例 1 在通常意义的加法、乘法运算下，Z, Q, R, C 均构成环，且是交换环，加法单位元 **0** 即为数 **0**，乘法单位元 **1** 即为数 **1**。

例 **2** 对任意正整数 n，在模 n 加法和模 n 乘法运算下，Z_n 是一个交换环，其加法单位元 **0** 为数 **0**，乘法单位元 **1** 为数 **1**。

在整数环中，任意非零元的乘积都不会为 **0**，这一性质对一般的环不一定成立：事实上，当 n 是合数时，设

$$n = ab$$

为 n 的一个非平凡分解，则环 Z_n 中，

$$a \neq 0, b \neq 0，而 a \cdot b = n \bmod n = 0。$$

定义 **6.1.2** a,b为环R中两个非零元，如果$ab=0$，则称a,b为零因子。

定义 **6.1.3** 含有单位元的交换环，若没有零因子，则称之为整环。

例 **3** Z,Q,R,C均为整环。

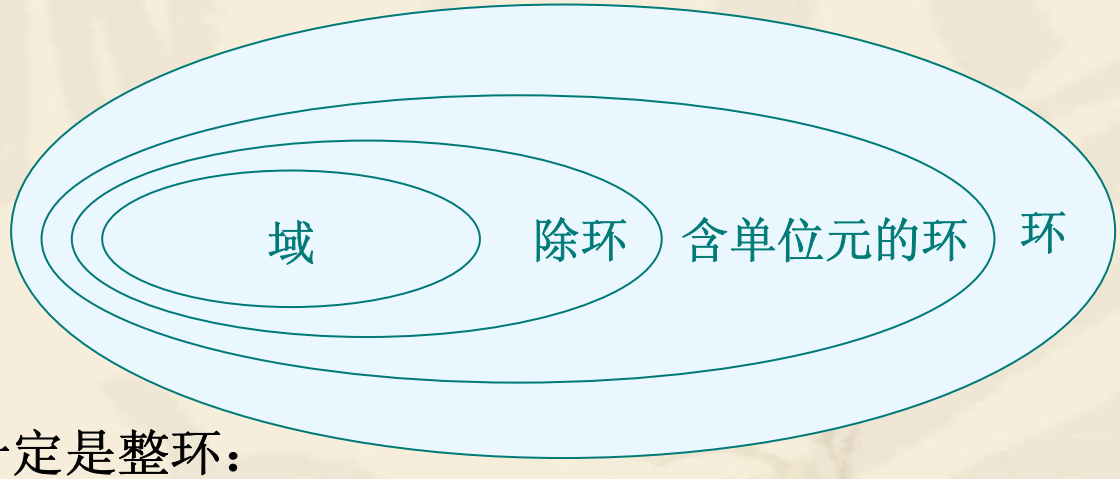
定义 **6.1.4** 如果一个环中的非零元全体在乘法运算“$\cdot$”下构成群，则称该环为除环（或斜域）。

定义 **6.1.5**（域）可交换的除环称为域。

例 **4** Q,R,C均为域，而Z不是域。

例 **5** 任一整环至少含有两个元素：**0**，**1**。$F_2=\{0,1\}$关于模 **2** 加法及乘法运算即构成二元域。

由环，除环，域的定义易知，它们具有如下的包含关系：



域一定是整环：

若 $ab=0$且$a\neq 0$，

则a一定存在逆元a^{-1}，从而$a^{-1}ab=a^{-1}0=0$，

即 $b=0$。

反过来，整环却不一定是域，对于有限整环我们有以下结论。

定理 6.1.1 有限整环一定是域。

证明：利用有限性证明R中的每个非零元都有逆元。

有限群，子群以及群的阶的概念均可以直接推广到环和域。

定义 6.1.6 一个环（域）如果包含有限个元素，则称其为有限环（有限域）。元素的个数称为该环（域）的阶。

定义 6.1.7 设R（F）为一个环（域），R'（F'）为R（F）的一个非空子集，若R'（F'）关于R（F）的运算“$+$”“$\cdot$”构成一个环（域），则称R'（F'）为R（F）的一个子环（子域），也记作$R' \leq R$（$F' \leq F$）。

对于环R及其子环R'而言，它们的零元是同一个元素 **0**，而乘法单位元则不同，它们的乘法单位元不一定是同一个，甚至还可以没有。

例 **6** 环$R=\{(a,b)\,|\,a,b\in Z\}$，其加法和乘法定义如下：

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

$$(a,b)*(a',b')=(a\cdot a',b\cdot b'),$$

其中“＋”与“·”为 **Z** 中的加法与乘法。该环的乘法单位元为$(1,1)$

考虑其子集$R'=\{(a,0)\,|\,a\in Z\}$，事实上该子集是环R的一个子环，该子环的乘法单位元为$(1,0)$。

例 7 (1) 整数环Z具有乘法单位元 1，而其子环$\{nk \mid k \in Z, n > 1\}$没有乘法单位元。

(2) 易知实数域上的所有方阵$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$关于矩阵加法和乘法构成环，该环无单位元，但是由所有$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$构成的子环有单位元$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$。

对于域F及其子域F'而言，它们具有相同的加法单位元 0 和乘法单位元 1

定义 6.1.8 设R是一个环，对R中任意元a，如果存在一个最小的正整数n使得$na=0$，则称环R的特征为n，记为$char(R)=n$。如果这样的正整数不存在，则称环R的特征为**0**，记为$char(R)=0$。

定理 6.1.2 设R为一整环，则$char(R)=0$或$char(R)=p$，其中p为一素数。

证明：R为一整环，则$1\in R$，$<1>$为$(R,+)$的循环子群。

对$<1>$或为无限子群或为有限子群分别进行讨论。

注：(1) 整环R的加法群中每一非零元的阶或都为无穷，或都为一素数；

(2) 整环R的特征即为单位元“1”在R的加法群中的阶。

推论 6.1.2 域的特征不为零，则为素数。

推论 6.1.2′ 有限域的特征必为一素数。

定理 6.1.3 在特征为素数 p 的含有单位元的交换环 R 中，对任意 $a,b\in R$ 及任意自然数 m，有

$$(a+b)^{p^m}=a^{p^m}+b^{p^m}，\ (a-b)^{p^m}=a^{p^m}-b^{p^m}。$$

6.2 理想和商环

定义 6.2.1 设I为环R的一个子环，如果对任意$a \in I$，$r \in R$，有$ar \in I, ra \in I$，则称I为环R的一个理想，也记作$I \lhd R$。

例 1 $\{0\}$和R本身显然是环R的理想，$\{0\}$称为零理想，

R本身称为单位理想，它们通称为平凡理想。

例 2 由交换环R元素a生成的理想为

$$I=(a)=\{ra+na\,|\,r\in R,n\in Z\}。$$

因为包含a的理想一定包含所有倍元ra和$\sum\pm a=na$，

从而包含所有的和$ra+na$。

又易验证$\{ra+na\,|\,r\in R,n\in Z\}$构成$R$的一个理想，所以$(a)$是包含$a$的最小理想。

当环R有单位元“1”时，由元素a生成的理想为

$$(a)=\{ra\,|\,r\in R\}。$$

因为此时有$ra+na=ra+(n\cdot 1)a=(r+n\cdot 1)a=r'a$。

例如整数环Z，它有单位元“1”，其理想(n)就是由所有n的倍数组成。

定义 6.2.2 由一个元素生成的理想称为主理想。

环R的理想I也将环R分成不相交的陪集，我们称之为模I的同余类。

环R中的元素a模I的同余类记为 $[a]=a+I=\{a+i \mid i\in I\}$。

若$b\in[a]$，我们形式上记为 $a\equiv b \bmod I$。

可以验证环R模I的同余类的集合关于下面定义的运算构成环：

$$[a]+[b]=[a+_R b]$$

$$[a]\cdot[b]=[a\cdot_R b]$$

“0” [0]=*I*, -[*a*]=[-*a*]

易知上述“$+$”和“$\cdot$”的定义和代表元的选取无关：

事实上，若$a\equiv s \bmod I$，$b\equiv t \bmod I$，则存在$i,j\in I$，使

$$s=a+_R i,\quad t=b+_R j,$$

从而有

$$s+_R t=a+_R b+_R (i+_R j)\in[a+_R b]$$

$$s\cdot_R t=a\cdot_R b+_R a\cdot_R j+_R b\cdot_R i+_R i\cdot_R j\in[a\cdot_R b]$$

定义 6.2.3 环R模I的同余类的全体关于上述定义的运算“$+$”“$\cdot$”构成环，称之为环R关于理想I的商环，记为R/I。

例 **3** 整数环Z关于理想(n)的同余类的全体$Z/(n)$为Z关于(n)的商环。

$Z/(n)$的元素为

$$[0]=0+(n),$$
$$[1]=1+(n),$$
$$\vdots$$
$$[n-1]=n-1+(n)。$$

若p为素数，则商环$Z/(p)$形成一个域。

定义 6.2.4 设R, R'是两个环，$f: R \to R'$为一个映射，如果f满足

(1) $\forall a, b \in R$，有$f(a+b) = f(a) + f(b)$,

(2) $\forall a, b \in R$，有$f(ab) = f(a)f(b)$,

则称f为环同态。如果f是单射，则称f为单同态；如果f是满射，则称f为满同态；如果f是一一映射，则称f为同构。

定理 6.2.1 (环的同态基本定理) 设 $f: R \to R'$ 是一个满同态，则同态核 $\ker(f) = \{r \in R \mid f(r) = 0\}$ 为环 R 的一个理想，且 $R/\ker(f) \cong R'$。设 φ 为 R 到 $R/Ker(f)$ 的自然同态，即 $\varphi(r) = r + \ker(f)$，则存在 $R/\ker(f)$ 到 R' 的同构 σ，使 $f = \sigma\varphi$。

环的同态也是它们的加法群之间的同态。这里定义的核与作为加法群的同态而定义的核是一致的。

因此，$\ker(f)$ 是 R 的加法群的一个子群，且 f 是单射当且仅当 $\ker(f) = \{0\}$。

映射可将一个代数结构所具有的结构传递给一个原本没有代数结构的集合。

例：R为环，f为R到集合S上的一个一一映射，则我们可以利用f在S上导出一个环结构，使得S成为一个环结构。

令$s_1, s_2 \in S$，r_1, r_2为由f唯一决定的R中的元，即

$$f(r_1) = s_1, \quad f(r_2) = s_2,$$

由此可以定义

$$s_1 + s_2 \text{为} f(r_1 + r_2),$$
$$s_1 \cdot s_2 \text{为} f(r_1 r_2)。$$

可以验证S关于以上定义的“+”“·”构成一个环，称为f导出的环。

定义 6.2.5 设p为素数，$F_p = \{0,1,\cdots,p-1\}$，f为$Z/(p)$到F_p的映射，定义为$f([a]) = a$，$a = 0,1,\cdots,p-1$。则F_p嵌入到由f导出的域结构，成为一个有限域，称为p阶 **Galois** 域，也记为 **GF(p)**。

群同态的同态像是群，群同态将单位元映射为单位元，逆元映射为逆元。

环同态的同态像是环，环同态将零元素 $\mathbf{0}$ 与任意元素 a 的负元映射到零元素及负元，若环有单位元，则环同态将单位元也映射到单位元。

环 R 的一些性质，有些可以传给它的商环，有一些则不能。

例如，环 R 有单位元，则其商环也有单位元，如整数环 Z 有单位元 $\mathbf{1}$，

而其商环 $Z/(n)$ 有单位元 $\overline{1}$；

整数环 Z 是整环，但是其商环 $Z/(n)$ 不一定是整环。

定义 6.2.6 环R中的一个理想P称为环R的一个素理想，是指对任意$a,b\in R$，若$ab\in P$，则$a\in P$或$b\in P$。

定义 6.2.7 环R中的一个理想M称为环R的一个极大理想，是指若有R的理想I，$M\subset I\subseteq R$，则$I=R$，即R中没有包含理想M的真理想。

定理 6.2.2 设R为含有单位元的交换环，则

(1) R的理想M为极大理想当且仅当R/M为域。

(2) R的理想P为素理想当且仅当R/P为整环。

推论 6.2.2 R为含有单位元的交换环，则R的每一个极大理想都是素理想。

证明：注意到域一定是整环，因此由定理 **6.2.2** 直接可得命题结论。

$$M \text{ 为 } R \text{ 的极大理想} \Leftrightarrow R/M \text{ 为域}$$

$$\Downarrow$$

$$R/M \text{ 为整环} \Leftrightarrow M \text{ 为 } R \text{ 的素理想}$$

例 **4** 我们知道当p为素数时，$Z/(p)$为域。

事实上，(p)是Z的极大理想，也是Z的素理想。

若$(p) \subseteq I = (a)$，则$a \mid p$，　由p为素数知　$a = 1$或$a = p$，

即$I = Z$或$I = (p)$，因此，(p)是Z的极大理想。

若$ab \in (p)$，则$p \mid ab$，　由p为素数知　$p \mid a$或$p \mid b$，

即$a \in (p)$或$b \in (p)$，因此，(p)是Z的素理想。

定义 6.2.8 若环R的所有理想都是主理想，则称环R为主理想环。

定理 6.2.3 R为主理想整环，则$R/(a)$为域当且仅当a为R的一个素元

6.3 多项式环

设R是一个环，x是不属于环R的一个符号，n是任意非负整数，形如

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0，\ a_i \in R$$

的形式和，叫作系数属于环R的x的多项式，或叫作环R上的x的多项式。

其中x称为环R上的不定元，

$a_i x^i$叫作该多项式的i次项，

a_i叫作i次项的系数。

$$R[x]=\{f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\mid a_i\in R,n\in N\}$$

$$f(x)=\sum_{i=0}^{n}a_ix^i,g(x)=\sum_{i=0}^{n}b_ix^i$$

$$f(x)=g(x)\ \Leftrightarrow\ a_i=b_i,0\le i\le n。$$

定义$R[x]$中的加法“$+$”和乘法“$\cdot$”如下：

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

为定义乘法，记$f(x)=\sum_{i=0}^{n}a_ix^i,g(x)=\sum_{j=0}^{m}b_jx^j$，定义

$$f(x)\cdot g(x)=\sum_{k=0}^{n+m}c_kx^k,$$

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

定义 6.3.1 $R[x]$关于上述加法运算“$+$”和乘法运算“$\cdot$”构成的环称为环R上的多项式环。

$R[x]$中所有系数均为零的元素称为零多项式，记为 **0**（**0** 表示零多项式或环R中零元视情况而定），它是$R[x]$中的加法零元，$f(x)$的加法逆元为

$$-f(x)=\sum_{i=0}^{n}(-a_i)x^i.$$

定义 6.3.2 设 $f(x)=\sum_{i=0}^{n} a_i x^i$，$a_n \neq 0$，则称多项式 $f(x)$的次数为n，记为$\deg(f)=\deg(f(x))=n$。a_n称为 $f(x)$的首系数。若环R含有单位元 **1**，则将首系数为 **1** 的多项式称为首一多项式。约定$\deg(0)=-\infty$。

定理 6.3.1 设 $f, g \in R[x]$，则

$$\deg(f+g) \le \max\{\deg(f), \deg(g)\},$$

$$\deg(fg) \le \deg(f) + \deg(g)。$$

当 R 为整环时，有 $\deg(fg) = \deg(f) + \deg(g)$。

例 2 多项式环$Z[x]$中，$f_1(x)=x^3+5x+2$，$f_2(x)=x^2-5x+1$，

我们有$\deg(f_1)=3$，$\deg(f_2)=2$，易知

$$f_1(x)+f_2(x)=x^3+x^2+3,$$

$$f_1(x)f_2(x)=x^5-5x^4+6x^3-23x^2-5x+2,$$

$$\deg(f_1+f_2)=3=\max\{\deg(f_1),\deg(f_2)\},$$

$$\deg(f_1f_2)=5=\deg(f_1)+\deg(f_2)。$$

再考虑多项式环$Z_6[x]$中，$g_1(x)=3x^3+2x+1$，$g_2(x)=2x^2+5$，

我们有$\deg(g_1)=3$，$\deg(g_2)=2$，易知

$$g_1(x)+g_2(x)=3x^3+2x^2+2x,$$

$$g_1(x)g_2(x)=x^3+2x^2+4x+5,$$

$$\deg(g_1+g_2)=3=\max\{\deg(g_1),\deg(g_2)\},$$

$$\deg(g_1g_2)=3<\deg(g_1)+\deg(g_2)=5。$$

定理 6.3.2 设R为一整环，则多项式环$R[x]$也是一个整环。

定理 6.3.3 设R为一整环，则多项式环$R[x]$中的可逆元就是R中的可逆元。

例 **3** 整数环Z是一整环，其中的可逆元仅有整数 **1** 和-1，
则多项式环$Z[x]$中的可逆元仅有零次多项式± 1。

整数环Z上的多项式环$Z[x]$就是我们通常说的整系数多项式，在实际当中用到较多的还有域上的多项式环，以下我们就考虑域F上的多项式环。

定义 6.3.4 设$f(x), g(x) \in F[x]$，$g(x) \neq 0$。若存在$q[x] \in F[x]$，使$f(x) = g(x)q(x)$，则称$g(x)$整除$f(x)$，记作$g(x) \mid f(x)$。$g(x)$叫作$f(x)$的因式，$f(x)$叫作$g(x)$的倍式。否则称$g(x)$不能整除$f(x)$，记作$g(x) \nmid f(x)$。

定义 6.3.5 设 $f(x)\in F[x]$，$f(x)$非常数。若有$g_1(x),g_2(x)\in F[x]$使得 $f(x)=g_1(x)g_2(x)$，则$g_1(x)$或$g_2(x)$为常数（**0** 次多项式），那么称 $f(x)$为多项式环$F[x]$中的不可约多项式，或$F[x]$中的素元。

注：多项式是否可约与所在的代数结构有密切关系。

例 **5** $x^2+2\in Q[x]$是不可约的，

但$x^2+2\in C[x]$是可约的，因为在复数域C上的多项式环$C[x]$中我们有

$$x^2+2=(x-i\sqrt{2})(x+i\sqrt{2})。$$

定理 6.3.4 设 $f(x), g(x) \in F[x]$， $g(x) \neq 0$，则存在多项式 $q(x), r(x) \in F[x]$，使

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

其中 $\deg(r) < \deg(g)$.

定理 6.3.5 （唯一因式分解定理）设 $f \in F[x]$，$\deg(f) > 0$，则必有

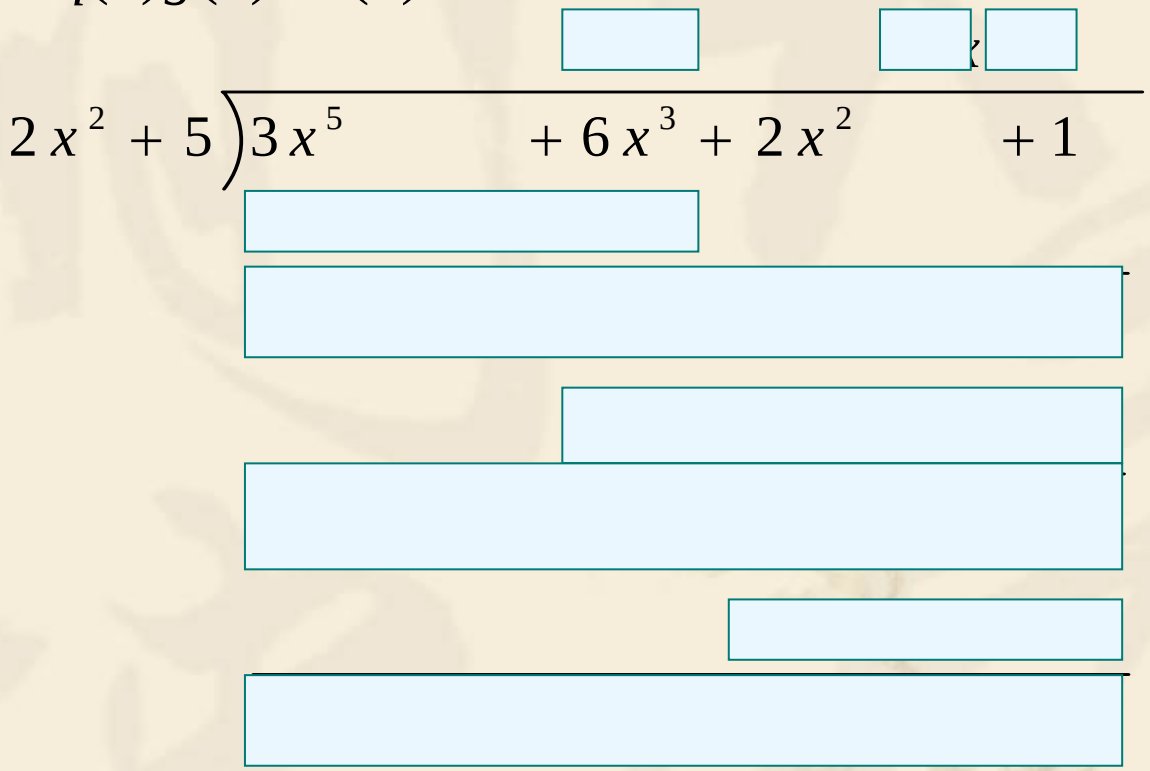
$$f = cp_1^{e_1} p_2^{e_2} \cdots p_s^{e_s},$$

其中 $c \in F$， $p_1, \cdots, p_s$ 为 $F[x]$ 中互不相同的首一不可约多项式，$e_i (1 \leq i \leq s)$ 均为正整数，并且若不计不可约因式的次序，这个分解式是唯一的。

例 **6** $f(x)=3x^5+6x^3+2x^2+1\in F_7[x]$，$g(x)=2x^2+5\in F_7[x]$，

下面我们利用多项式的长除法来求$q(x),r(x)\in F_7[x]$，使

$f(x)=q(x)g(x)+r(x)$：



从而$q(x)=5x^3+x+1$，$r(x)=2x+3$，

$\deg(r)=1<\deg(g)=2$。

定理 6.3.6 域F上的多项式环$F[x]$为主理想整环。

定理 6.3.7 设 $f(x)\in F[x]$，则 $F[x]/(f(x))$ 为域当且仅当 $f(x)$ 为域 F 上的不可约多项式。

同 $Z/(n)$ 类似，$F[x]/(f(x))$ 中的元即为次数小于 $f(x)$ 的次数的所有 F 上的多项式，其中的加法、乘法运算分别为模多项式 $f(x)$ 的加法和乘法运算。

若 $F=F_p$，$deg(f)=n$，则 $|F_p[x]/(f)|=p^n$。

例 7 设 $f(x)=x^2+x+1\in F_2[x]$，则 $f(x)$在F_2上是不可约的，由定理 **6.3.7** 知$F_2[x]/(f)$构成一个具有$|F_2[x]/(f)|=2^2=4$个元素的域，其元素及元素间的运算表如下：

$F_2[x]/(f)=\{[0],[1],[x],[x+1]\}$

+	**[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]**

[0]是零元，

·	**[0]**	**[1]**	**[x]**	[x+1]
[0]	**[0]**	**[0]**	**[0]**	**[0]**
[1]	**[0]**	**[1]**	**[x]**	**[x+1]**
[x]	**[0]**	**[x]**	**[x+1]**	**[1]**
[x+1]	**[0]**	**[x+1]**	**[1]**	**[x]**

[1]是单位元

定义 6.3.6 设 $f(x)\in F[x]$，$\alpha\in F$，若 $f(\alpha)=0$，则称α是 $f(x)$的一个根。

定理 6.3.8 设 $f(x)\in F[x]$，$\alpha\in F$，则α是 $f(x)$的一个根当且仅当$(x-\alpha)\mid f(x)$。

若 $f(x)\in F[x]$在域F 上有根，则 $f(x)$在F 上一定可约，反过来则不一定成立，但对于F 上的 **2** 次和 **3** 次多项式，我们有以下结论。

定理 6.3.9 设 $f(x)\in F[x]$，$f(x)$的次数等于 **2** 或 **3**，则 $f(x)$为域 F 上的不可约多项式当且仅当 $f(x)$在 F 上没有根。

例 **8** 例 **7** 中 $f(x)=x^2+x+1\in F_2[x]$为F_2上的不可约多项式，因为

$$f(0)=f(1)=1\neq 0,$$

即 $f(x)$在F_2上没有根。

$f(x)=x^2+1\in F_3[x]$为F_3上的不可约多项式，因为

$$f(0)=1\neq 0,\quad f(1)=f(2)=2\neq 0$$

即 $f(x)$在F_3上没有根。

$f(x)=x^4+x^2+1\in F_2[x]$

$$f(0)=f(1)=1\neq 0,$$

但是 $f(x)=x^4+x^2+1=(x^2+x+1)^2$

利用定理 **6.3.8**，我们可以将定理 **2.4.6** 作一推广，得到关于域上多项式的根的个数的一个重要结论：

定理 6.3.10 设 $f(x)\in F[x]$，$\deg(f)=n$，则 $f(x)$在F 上最多有n个不同的根。

定义 6.3.7 设 $f(x)\in F[x]$，$\alpha\in F$，正整数$k\geq 2$，若$(x-\alpha)^k \mid f(x)$，而$(x-\alpha)^{k+1} \nmid f(x)$，则称$\alpha$为 $f(x)$的k 重根，简称重根。

定义 6.3.8 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$，称

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1\in F[x]$$

为 $f(x)$的一阶导数。

定理 6.3.11 设 $f(x)\in F[x]$，则 $\alpha\in F$ 为 $f(x)$ 的重根当且仅当 α 既是 $f(x)$ 的根又是 $f'(x)$ 的根。

推论 6.3.11 设 $f(x)\in F[x]$，若 $\alpha\in F$ 为 $f(x)$ 的 k 重根，则 α 为 $f'(x)$ 的 $k-1$ 重根。

推论 6.3.11′ 设 $f(x)\in F[x]$，若 $(f(x), f'(x))=1$，则 $f(x)$ 没有重根。

定义 6.3.9 设 $f_1, f_2, \cdots, f_n$ 为域 F 上 n 个不全为零的多项式，首一多项式 $d(x) \in F[x]$ 称为 $f_1, f_2, \cdots, f_n$ 的最大公因式，是指 $d(x)$ 满足：

(1) $d(x) \mid f_i(x)$，$1 \le i \le n$；

(2) 若有 $h(x) \in F[x]$，$h(x) \mid f_i(x)$，$1 \le i \le n$，则 $h(x) \mid d(x)$。

记 $d(x) = \gcd(f_1, f_2, \cdots, f_n)$。

定理 6.3.12 设 $f_1, f_2, \cdots, f_n$ 为域 F 上 n 个不全为零的多项式，则存在 $b_1, b_2, \cdots, b_n \in F[x]$，使得

$$\gcd(f_1, f_2, \cdots, f_n) = b_1 f_1 + b_2 f_2 + \cdots + b_n f_n。$$

利用带余除法，我们同样可以得到以下求$\gcd(f,g), f,g\in F[x]$的**Euclid** 算法。不失一般性，设$g\neq 0$，$g\nmid f$，我们如下不断使用带余除法：

$$\begin{aligned}
f &= q_1 g + r_1 && 0\le \deg(r_1) < \deg(g)\\
g &= q_2 r_1 + r_2 && 0\le \deg(r_2) < \deg(r_1)\\
r_1 &= q_3 r_2 + r_3 && 0\le \deg(r_3) < \deg(r_2)\\
&\vdots && \vdots\\
r_{n-2} &= q_n r_{n-1} + r_n && 0\le \deg(r_n) < \deg(r_{n-1})\\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

其中$q_1,\cdots,q_{n+1},r_1,\cdots,r_n\in F[x]$，由于$\deg(g)$是有限的，故经有限步后，必有整数$n$使$\deg(r_{n+1})=-\infty$。若最后一个非零余式$r_n$的首系数为$a$，则

$$\gcd(f,g)=a^{-1}r_n。$$

为求$\gcd(f_1, f_2, \cdots, f_n)$，可先求$\gcd(f_1, f_2)$，再求$\gcd(\gcd(f_1, f_2), f_3)$，如此继续下去直到求得$\gcd(f_1, f_2, \cdots, f_n)$。

由定理 **6.3.12** 知，一定存在$s,t \in F[x]$使得$\gcd(f, g) = sf + tg$。为求s和t，同样可以利用 **Euclid** 算法的逆过程。

例 **9** $f(x)=x^7+x^5+x^2+1\in F_2[x]$，$g(x)=x^4+x^2+x\in F_2[x]$，

求$\gcd(f,g)$，并且求$s,t\in F[x]$使得$\gcd(f,g)=sf+tg$。

解：利用 Euclid 算法及其逆过程，可得

$$x^7+x^5+x^2+1=(x^3+1)(x^4+x^2+x)+x+1$$

$$x^4+x^2+x=(x^3+x^2+1)(x+1)+1$$

$$x+1=(x+1)\cdot 1$$

$\downarrow\uparrow$

$$1=(x^4+x^2+x)+$$

$$(x^3+x^2+1)(f+(x^3+1)g)$$

$$1=(x^4+x^2+x)+(x^3+x^2+1)(x+1)$$

于是

$$\gcd(f,g)=1=(x^3+x^2+1)f+(x^6+x^5+x^2)g,$$

即

$$s=x^3+x^2+1，\ t=x^6+x^5+x^2。$$

定义 6.3.10 当$\gcd(f,g)=1$时，称f和g互素。

定义 6.3.11 设$f_1, f_2, \cdots, f_n$为域F上n个非零多项式，首一多项式$m(x)\in F[x]$称为$f_1, f_2, \cdots, f_n$的最小公倍式，是指$m(x)$满足：

(1) $f_i(x)\mid m(x)$，$1\le i\le n$；

(2) 若有$h(x)\in F[x]$，$f_i(x)\mid h(x)$，$1\le i\le n$，则$m(x)\mid h(x)$。

记$m(x)=\mathrm{lcm}(f_1, f_2, \cdots, f_n)$。

定理 6.3.13 设 $f(x), g(x)$ 为域 F 上两个非零多项式，则

$$a^{-1}fg = \gcd(f,g)\mathrm{lcm}(f,g),$$

其中 a 为多项式 fg 的首系数。

根据定理 **6.3.13**，我们可以由 $\gcd(f,g)$ 来求解 $\mathrm{lcm}(f,g)$。

对于多个元的最小公倍式，同样利用

$$\mathrm{lcm}(f_1, f_2, \cdots, f_n) = \mathrm{lcm}(\mathrm{lcm}(f_1, f_2, \cdots, f_{n-1}), f_n)$$

来求。