Chapter 6

多项式环

这一章我们主要讨论单变元和多变元的多项式，以及多项式的根。

6.1 单变元多项式

6.1.1 一元多项式环的定义与赋值同态

我们首先来讨论单变元多项式的构造。

设 $(R,+,0,\cdot,1)$ 是一个交换环，x 是一个符号 (未定元)，我们可以形式地说 $f(x)=a_0+a_1x+\cdots+a_nx^n,\ a_i\in R,\ i=0,1,\ldots,n$ 是一个多项式。例如，$\mathbb{R}$ 上 $f(x)=x^2+2x+3$ 就是一个多项式。但这样并不严谨，因为我们没有说清楚 x 究竟是什么。为此，我们给出下面的定义。

首先，我们注意到多项式是由其“系数”决定的，而与未定元的名字是 x 还是 y 没有关系。因此，我们定义

$$\widetilde{R}=\{(a_0,a_1,a_2,\cdots)\mid a_0,a_1,a_2,\cdots\in R\text{ 且其中只有有限多个非 }0.\}$$

我们记 $(a_0,a_1,a_2,\cdots)=\widetilde{a}$，且 $\widetilde{a}$ 的第 k 个位置的元素记为 a_k(从第 0 个开始计数，下同)。特别地，$\widetilde{0}=(0,0,\cdots),\ \widetilde{1}=(1,0,\cdots)$。我们在 $\widetilde{R}$ 上定义如下的加法和乘法：

$$\begin{aligned}
&+:\widetilde{R}\times\widetilde{R}\longrightarrow\widetilde{R}\\
&\quad(\widetilde{a},\widetilde{b})\longmapsto\widetilde{c},\quad c_k=a_k+b_k,\forall k\in\mathbb{N}.\\
&\cdot:\widetilde{R}\times\widetilde{R}\longrightarrow\widetilde{R}\\
&\quad(\widetilde{a},\widetilde{b})\longmapsto\widetilde{c},\quad c_k=\sum_{i=0}^{k}a_ib_{k-i},\forall k\in\mathbb{N}.
\end{aligned}$$

容易验证上面的加法和乘法是良定义的 ($\widetilde{c}$ 中只有有限多个位置的元素非 0)，并且 $(\widetilde{R},+,\widetilde{0},\cdot,\widetilde{1})$ 是交换幺环 (验证 $\widetilde{R}$ 关于加法成交换群，于是可以定义自然的减法，乘法成交换幺半群，乘法关于加法有分配律，留作练习)。

引进符号 (未定元，indeterminate, variable)

$$x=(0,1,0,\cdots)$$

并规定单项式 (monomials)

$$x^0=\widetilde{1},\ x^i=(0,\cdots,0,1,0,\cdots)\text{ (第 }i\text{ 个位置是 }1).$$

我们看到这个规定与 $\widetilde{R}$ 上的乘法是相容的。于是我们有：

命题 6.1.1 令 $\varphi : R \to \widetilde{R},\ r \mapsto \widetilde{r} = (r, 0, 0, \cdots)$，则 φ 是单的环同态。

证明是容易的，留作练习。

于是我们可以将 $\widetilde{r} \in \widetilde{R}$ 与 $r \in R$ 等同起来，并且定义“数乘”多项式 $\widetilde{ra} = \widetilde{ra} = (ra_0, ra_1, \cdots)$。于是对任意 $\widetilde{a} \in \widetilde{R}$，不妨设 $\widetilde{a}$ 的第 n 个位置以后 (不含 n) 全为 0，则容易验证 $\widetilde{a} = a_0 + a_1 x + \cdots + a_n x^n$，即

$$\widetilde{R} = \left\{ \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N},\ a_0, \ldots, a_n \in R. \right\}$$

我们也把 $\widetilde{R}$ 记作 $R[x]$，称为 R 上的**一元多项式环** (the ring of univariate polynomials over R)，其中的元素称为一元**多项式** (univariate polynomial)。

定理 6.1.1 (1) 设 $p = p_0 + p_1 x + \cdots + p_d x^d \in R[x]$，则 $p = 0 \iff p_0 = \cdots = p_d = 0$；
(2) 设 $p = p_0 + p_1 x + \cdots + p_s x^s,\ q = q_0 + q_1 x + \cdots + q_t x^t \in R[x]$，则 $p = q \iff s = t$ 且 $\forall i = 0, 1, \ldots, s,\ p_i = q_i$。

证明: $(1) p = 0 \iff (p_0, p_1, \cdots, p_d, 0, \cdots) = (0, 0, \cdots) \iff p_0 = p_1 = \cdots = p_d = 0$；
$(2) p = q \iff (p_0, \cdots, p_s, 0, \cdots) = (q_0, \cdots, q_t, 0, \cdots) \iff p_i = q_i,\ \forall i \in \mathbb{N}$，即得结论。 □

定义 6.1.1 设 $p = p_0 + p_1 x + \cdots + p_d x^d \in R[x],\ p_i \in R, p_d \neq 0$，则我们称 d 为多项式 p 的次数 (degree)，记作 $\deg_x(p) = d$ 或 $\deg(p) = d$。我们把 p_i 称为 x^i 在 p 中的系数 (coefficient)，特别地，p_d 称为 p 的首项系数 (leading coefficient)，记作 $\mathrm{lc}_x(p) = p_d$ 或 $\mathrm{lc}(p) = p_d$。如果 $\deg(p) = 0$，则称 p 为常多项式 (constant polynomial)；如果 $\mathrm{lc}(p) = 1$，则称 p 为首一多项式 (monic polynomial)。另外，特别规定 $\deg(0) = -\infty$。

由定义立刻有

命题 6.1.2 设 $p, q \in R[x]$，则
$(1)\deg(p + q) \leqslant \max(\deg(p), \deg(q))$；
$(2)\deg(pq) \leqslant \deg(p) + \deg(q)$，当且仅当 $\mathrm{lc}(p)\mathrm{lc}(q) \neq 0$ 时 $\deg(pq) = \deg(p) + \deg(q)$ 并且 $\mathrm{lc}(pq) = \mathrm{lc}(p)\mathrm{lc}(q)$。

证明是显然的，留作练习。

例 6.1.1 在 $\mathbb{Z}_6[x]$ 中 $f = \overline{2}x^2 + \overline{3}x + \overline{1},\ g = \overline{3}x + \overline{4}$，求 $f + g$ 和 fg。

解: 计算可得

$$f + g = \overline{2}x^2 + (\overline{3} + \overline{3})x + (\overline{1} + \overline{4}) = \overline{2}x^2 + \overline{5};$$
$$fg = (\overline{2}x^2 + \overline{3}x + \overline{1})(\overline{3}x + \overline{4}) = \overline{0}x^3 + \overline{3}x^2 + \overline{3}x + \overline{2}x^2 + \overline{0}x + \overline{4} = \overline{5}x^2 + \overline{3}x + \overline{4}.$$

定理 6.1.2 设 D 是整环，则 $D[x]$ 也是整环。

证明: 只需证明 $D[x]$ 无零因子。设 $f, g \in D[x]$ 且 $f \neq 0, g \neq 0$，则 $\mathrm{lc}(f) \neq 0,\ \mathrm{lc}(g) \neq 0$。于是由 D 是整环可知 $\mathrm{lc}(f)\mathrm{lc}(g) \neq 0$，即 $fg \neq 0$。 □

注 6.1.1 当 $\mathbb{F}$ 是域时，由上面的定理知 $\mathbb{F}[x]$ 是整环，于是可以作 $\mathbb{F}[x]$ 的分式域

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

我们称 $\mathbb{F}(x)$ 为 $\mathbb{F}$ 上关于 x 的有理分式域。

在中学我们接触的多项式都是可以“代入数值”进行计算的，那么，如何严格地定义这一操作呢？这就是下面的**赋值同态** (evaluation homomorphism)。

定理 6.1.3 设 $\varphi : R \to S$ 是两个环之间的非零同态，任意固定 $a \in S$，则存在唯一的环同态 $\varphi_a : R[x] \to S$ 满足 $\varphi_a|_R = \varphi$，并且 $\varphi_a(x) = a$。

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle \mathrm{id}}\downarrow & \nearrow_{\varphi_a} & \\ R[x] & & \end{array}$$

证明: 先证存在性。构造如下的 φ_a:

$$\begin{aligned} \varphi_a : R[x] &\longrightarrow S \\ p = \sum_{i=0}^{d} p_i x^i &\longmapsto \sum_{i=0}^{d} \varphi(p_i) a^i \quad (\text{规定} a^0 = 1_S) \end{aligned}$$

首先 φ_a 是良定义的 (多项式由系数唯一确定，定理 6.1.1)。下面我们证明 φ_a 是环同态。设 $f = \sum_{i=0}^{n} f_i x^i$，$g = \sum_{i=0}^{m} g_i x^i$，$f_n, g_m \neq 0$，令 $d = \max(m, n)$，首先我们有

$$\begin{aligned} \varphi_a(f+g) &= \varphi_a(\sum_{i=0}^{d} (f_i + g_i) x^i) \\ &= \sum_{i=0}^{d} \varphi(f_i + g_i) a^i && (\varphi_a\text{的定义}) \\ &= \sum_{i=0}^{d} (\varphi(f_i) + \varphi(g_i)) a^i && (\varphi\text{是环同态}) \\ &= \sum_{i=0}^{d} \varphi(f_i) a^i + \sum_{i=0}^{d} \varphi(g_i) a^i \\ &= \varphi_a(f) + \varphi_a(g). \end{aligned}$$

同理可证 $\varphi_a(fg) = \varphi_a(f)\varphi_a(g)$，即 φ_a 是环同态。而且我们有 $\varphi(1_R) = \varphi(1_R)a^0 = 1_S \cdot 1_S = 1_S$，于是对 $\forall r \in R$，有

$$\varphi_a(r) = \varphi_a(rx^0) = \varphi(r)a^0 = \varphi(r)$$

即 $\varphi_a|_R = \varphi$，并且 $\varphi_a(x) = \varphi(1_R)a = 1_S a = a$。即我们构造的 φ_a 满足我们的所有要求。

再证唯一性。设 $\psi : R[x] \to S$ 也是满足上面要求的环同态，则

$$\begin{aligned} \psi(f) &= \psi(\sum_{i=0}^{n} f_i x^i) \\ &= \sum_{i=0}^{n} \psi(f_i)\psi(x)^i && (\psi\text{是环同态}) \\ &= \sum_{i=0}^{n} \varphi(f_i) a^i && (\psi\text{的性质}) \\ &= \varphi_a(f). \end{aligned}$$

唯一性证完。 □

定理的证明过程实际上给出了把元素“代入”多项式的具体操作。设 $f \in R[x]$，我们把 $\varphi_a(f)$ 也简记作 $f(a)$。

例 6.1.2 令 $\varphi : \mathbb{Z} \to \mathbb{Z}_5,\ a \mapsto \overline{a},\ a = \overline{3}$，取 $f(x) = x^2 - 4 \in \mathbb{Z}[x]$，求 $\varphi_a(f)$。

解: $\varphi_a(f) = \varphi(1)a^2 - \varphi(4)a^0 = \overline{1}\cdot\overline{3}^2 - \overline{4}\cdot\overline{1} = \overline{5} = \overline{0}$。

特别地，在上面的定理中取 $S = R,\ \varphi = \mathrm{id}_R$ 就得到了我们熟悉的赋值操作。在没有特别说明时的赋值我们都是指这种情形。

此外，这个定理也告诉了我们如何将矩阵代入多项式中。

命题 6.1.3 设 $\mathbb{F}$ 是域，$A \in M_n(\mathbb{F})$，则 $\mathbb{F}[A] = \{\sum_{i=0}^{m} a_i A^i \mid a_i \in \mathbb{F},\ m \in \mathbb{N}\}$（定义 $A^0 = E_n$）在矩阵加法和乘法下是一个交换环，注意到嵌入 $\rho : \mathbb{F} \to \mathbb{F}[A],\ a \mapsto aE_n$ 是环同态，于是由定理 6.1.3可以将 ρ 扩张到 $\mathbb{F}[x] \to \mathbb{F}[A]$ 上：

$$\begin{aligned} \rho_A : \mathbb{F}[x] &\longrightarrow \mathbb{F}[A] \\ f = \sum_{i=0}^{m} f_i x^i &\longmapsto \sum_{i=0}^{m} f_i A^i \end{aligned}$$

ρ_A 是环同态。

我们把 $\rho_A(f)$ 简记为 $f(A)$。

例 6.1.3 $f(x) = x^2 - 4 \in \mathbb{R}[x]$，$A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$，则 $f(A) = A^2 - 4E = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}$。

6.1.2 一元多项式的带余除法

命题 6.1.4 设 R 是交换环，$f, g \in R[x]$ 且 $g \neq 0$，如果 $\mathrm{lc}(g)$ 乘法可逆，则 $\exists!$ 一组 $q, r \in R[x]$ 满足 $f = qg + r$ 且 $\deg(r) < \deg(g)$。我们称 $q = \mathrm{quo}(f, g)$ 为商，$r = \mathrm{rem}(f, g)$ 为余式。

证明: 先证存在性。若 $\deg(f) < \deg(g)$，则取 $q = 0,\ r = f$ 即满足条件。于是我们只需考虑 $\deg(f) = \deg(g) + k,\ k \geqslant 0$ 的情形。不妨设 $\deg(g) = n$，对 k 做数学归纳法。

- $k = 0$ 时，设 $\mathrm{lc}(f) = f_n,\ \mathrm{lc}(g) = g_n$，令 $r = f - f_n g_n^{-1} g + r$，则 $\deg(r) < n$ 并且 $f = (f_n g_n^{-1})g + r$。取 $q = f_n g_n^{-1}$ 即可。
- 如果 $k \geqslant 1$ 并且存在性对次数差小于 k 的 f 和 g 成立，那么，令 $h = f - f_{n+k} g_n^{-1} x^k g$，则 $\deg(h) < n + k$，于是由归纳假设，存在 $q_1, r_1 \in R[x]$ 使得 $h = q_1 g + r_1$，满足 $\deg(r_1) < \deg(g)$，则 $f = (f_{n+k} g_n^{-1} x^k + q_1)g + r_1$，取 $q = f_{n+k} g_n^{-1} x^k + q_1$，$r = r_1$，则 $f = qg + r$ 且 $\deg(r) < \deg(g)$。

这样我们就证明了存在性。

再证唯一性。如果另有一组 $q',\ r'$ 满足 $f = q'g + r'$ 并且 $\deg(r') < \deg(g)$，则 $qg + r = q'g + r'$，即 $(q - q')g = r' - r$，注意到 $\deg(r' - r) < \deg(g)$，于是只能是 $q - q' = 0$，所以 $r' - r = 0$。这样我们就证明了唯一性。 □

特别地，如果 $\exists q(x) \in R[x]$ 使得 $f = qg$，则我们称多项式 f 能被 g 整除，记作 $g \mid f$。易证 $\mathrm{rem}(f, g) = 0 \Rightarrow g \mid f$，并且整除是 $R[x]$ 上的一个偏序关系。与整数上的竖式除法类似，我们也可以用竖式计算多项式的带余除法。我们用下面的例子展示具体的计算过程。

例 6.1.4 $f = x^3 + 2x + 1$, $g = 2x^2 + 1 \in \mathbb{R}[x]$，求 $q, r \in \mathbb{R}[x]$ 使得 $f = qg + r$ 且 $\deg(r) < \deg(g)$。

解:

$$\begin{array}{rcl|l} & & & \frac{1}{2}x \\ \hline 2x^2 & + & 1 & x^3 + 2x + 1 \\ & & & x^3 + \frac{1}{2}x \\ \hline & & & \frac{3}{2}x + 1 \end{array}$$

特别地，域上的多项式一定可以作带余除法。

定理 6.1.4 设 $\mathbb{F}$ 是域，$f, g \in \mathbb{F}[x]$，$g \neq 0$，则 $\exists!$ 一组 $q, r \in R[x]$ 满足 $f = qg + r$ 且 $\deg(r) < \deg(g)$。

证明: 由于 $g \neq 0$，$\mathbb{F}$ 是域，故 $\mathrm{lc}(g) \in \mathbb{F} \setminus \{0\}$ 可逆，再由命题 6.1.4即得结论。 □

定理 6.1.5 (**余式定理**) 设 R 是交换环，$f \in R[x]$，$\alpha \in R$，则 $f(\alpha) = \mathrm{rem}(f, x - \alpha)$。

证明: 在环 R 中 1 显然是乘法可逆元，故可以作带余除法 $f(x) = q(x)(x-\alpha) + r(x)$，由 $\deg(r(x)) < \deg(x - \alpha) = 1$ 可知 $\deg(r(x)) = 0$，即 $r(x) = r \in R$。再由赋值同态可知 $f(\alpha) = q(\alpha)(\alpha - \alpha) + r$，即 $r = f(\alpha)$。 □

于是我们可以简单地讨论一下一元多项式的根。

定义 6.1.2 设 $\mathbb{F}, \mathbb{K}$ 是域且 F 是 $\mathbb{K}$ 的子域，设 $f \in \mathbb{F}[x]$, $\alpha \in \mathbb{K}$，如果 $f(\alpha) = 0$，则称 α 是 f 在 $\mathbb{K}$ 中的一个根。

例如 $f(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$ 在 $\mathbb{Q}$ 中没有根，在 $\mathbb{R}$ 中有两个根 $\pm\sqrt{2}$，在 $\mathbb{C}$ 中有四个根 $\pm\sqrt{2}, \pm i$。

定理 6.1.6 设 $\mathbb{F}$ 是域 $\mathbb{K}$ 的子域，$\alpha \in \mathbb{K}$，$f \in \mathbb{F}[x]$ 且 $d = \deg(f) > 0$，则

(i) $f(\alpha) = 0 \iff \mathrm{rem}(f, x - \alpha) = 0$;

(ii) f 在 $\mathbb{K}$ 中至多有 d 个互不相同的根。[1]

证明: (i) 显然可以将 f 放在 $\mathbb{K}[x]$ 中，于是由余式定理立刻可证。
(ii) 不妨设 f 在 $\mathbb{K}$ 中所有互不相同的根为 $\alpha_1, \alpha_2, \ldots, \alpha_m$，则由 (i) 可知 $f(x) = q_1(x)(x - \alpha_1)$，则 $0 = f(\alpha_2) = q_1(\alpha_2)(\alpha_2 - \alpha_1)$，由 $\alpha_1 \neq \alpha_2$ 可知 $q_1(\alpha_2) = 0$ 即 $q_1(x) = q_2(x)(x - \alpha_2)$，所以 $(x-\alpha_1)(x-\alpha_2) \mid f$。重复上面的过程归纳可得 $(x-\alpha_1)\cdots(x-\alpha_m) \mid f$，即 $f = q_m(x)(x-\alpha_1)\cdots(x-\alpha_m)$，而 $(x - \alpha_1)\cdots(x - \alpha_m)$ 是一个 m 次多项式，则由命题 6.1.2易得 $m \leqslant d$。

6.1.3 一元多项式的最大公因子与辗转相除法

在介绍辗转相除法之前，我们先介绍一般的整环上的整除关系与最大公因子。

定义 6.1.3 设 D 是整环，$a, b \in D$ 且 $a \neq 0$，如果存在 $c \in D$ 使得 $b = ca$，则称 a 是 b 的因子，b 是 a 的倍式 (b 能被 a 整除)，记作 $a \mid b$。如果 b 不能被 a 整除，则记作 $a \nmid b$。如果 $a \mid b$, $b \nmid a$，则称 a 是 b 的真因子。

显然这个定义包含了 $\mathbb{Z}$ 和 $R[x]$ 上关于因子和整除的定义。注意整除关系依赖于 D 的选取。

[1] 这个命题的条件可以减弱到整环上，留作练习。

定义 6.1.4 设 D 是整环，$a,b\in D$，如果存在 $u\in D^\times$(D 中乘法可逆元）使得 $a=ub$，则称 a 与 b 相伴 (a and b are associates)，记作 $a\approx b$。

例如 $\mathbb{Z}$ 中 n 和 $-n$ 相伴。容易证明相伴是一个等价关系。

引理 6.1.1 设 D 是整环，$a,b,c\in D$，则
(1)$a\mid b,b\mid c\Longrightarrow a\mid c$;
(2)$a\mid b,a\mid c\Longrightarrow \forall f,g\in D,\ a\mid(fb+gc)$。

证明是简单的，留作练习。

引理 6.1.2 设 D 是整环，$a,b\in D^*=D\setminus\{0\}$，则 $a\approx b\iff a\mid b$ 且 $b\mid a$。

证明: $(\Longrightarrow)a\approx b\Longrightarrow\exists u\in D^\times$ 使得 $a=ub$，所以 $u^{-1}a=b$，即 $a\mid b$ 且 $b\mid a$。
$(\Longleftarrow)$ 如果 $a\mid b$ 且 $b\mid a$ 成立，即 $\exists p,q\in D$ 使得 $a=pb,\ b=qa$，则 $a=pqa$，即 $(1-pq)a=0$，由 D 是整环即有 $1-pq=0$，即 $p,q\in D^\times$，所以 $a\approx b$。 □

定义 6.1.5 设 D 是整环，$a,b\in D^*$，如果 $c\in D^*$ 同时满足 $c\mid a,\ c\mid b$，则称 c 是 a,b 的公因子 (common divisor)。设 g 是 a,b 的某个公因子，如果 g 还满足如下条件：任取 $c\in D^*$ 也是 a,b 的公因子，则 $c\mid g$，则我们称 g 是 a,b 的最大公因子 (greatest common divisor)，记作 $g=\gcd(a,b)$。

最大公因子在相伴的意义下是唯一的，即下面的命题。

命题 6.1.5 设 D 是整环，$a,b\in D^*$，g,h 都是 a,b 的最大公因子，则 $g\approx h$。

证明: 由最大公因子的定义立刻有 $g\mid h,\ h\mid g$，于是由引理 6.1.2即得结论。 □

例 6.1.5 在 $\mathbb{Z}$ 中 $\gcd(35,21)=7$或 -7。(当然习惯上我们取 7，取 -7 也不影响结果。)

下面的定理是本小节的核心结论。

定理 6.1.7 设 $\mathbb{F}$ 是域，则 $\mathbb{F}[x]$ 是整环 (定理 6.1.2)，我们有：$\forall p,q\in\mathbb{F}[x]\setminus\{0\}$，$\gcd(p,q)$ 都存在并且 $\exists u,v\in\mathbb{F}[x]$ 使得 $up+vq=\gcd(p,q)$(Bezout 关系)。

证明: 令集合 $I=\{ap+bq\mid a,b\in\mathbb{F}[x]\}$，显然 $I\setminus\{0\}$ 是非空集合，于是我们可以设 g 是 I 中次数最低的非零多项式，我们只要证明 g 是 p,q 的最大公因子即可。

首先，我们可以做带余除法 $p=hg+r$，其中 $\deg(r)<\deg(g)$。由于 $g\in I$，按 I 的定义有：$\exists u,v\in\mathbb{F}[x]$ 使得 $up+vq=g$，代入 $p=hg+r$ 并整理有：

$$p=h(up+vq)+r\Longrightarrow r=(1-hu)p+(-hv)q$$

于是按 I 的定义，$r\in I$，但由于 $\deg(r)<\deg(g)$，如果 $r\neq 0$ 就会与 g 是 I 中次数最低的非零多项式矛盾，于是 $r=0$，即 $p=hg$，$g\mid p$。同理做 $q=h'g+r'$ 即可得到 $g\mid q$。即我们证明了 g 是 p,q 的公因子。

最后我们证明 g 的最大性。另取 $c\in\mathbb{F}[x]$ 也是 p,q 的公因子，则 $c\mid p,c\mid q\Longrightarrow c\mid up+vq$，即 $c\mid g$。这样我们就完成了证明。 □

实际上，证明中出现的 I 是 p,q 生成的 $\mathbb{F}[x]$ 的理想，这个证明告诉我们 $\mathbb{F}[x]$ 是一个主理想整环 (principal ideal domain,PID)[1]。

下面我们考虑如何计算 $\mathbb{F}[x]$ 中非零多项式 f,g 的最大公因子。类似于 1.6 节中的做法，我们反复做带余除法如下：
令 $r_0=f, r_1=g$，我们有

$$\begin{aligned}
r_0 &= q_2r_1 + r_2 && \deg(r_1) > \deg(r_2)\\
r_1 &= q_3r_2 + r_3 && \deg(r_2) > \deg(r_3)\\
&\vdots && \vdots\\
r_{k-2} &= q_kr_{k-1} + r_k && \deg(r_{k-1}) > \deg(r_k)\\
r_{k-1} &= q_{k+1}r_k && r_{k+1} = 0
\end{aligned}$$

这个算法能够终止 (即必存在 $k\in\mathbb{N}$ 使得 $r_{k+1}=0$) 是因为 $\deg(r_1)>\deg(r_2)>\cdots>\deg(r_k)$，而 $\deg(r_1)$ 是有限的。结合定理 6.1.7，用类似于第 1.6 节的证明方法我们就可以证明上面的 r_k 就是我们所需要的 $\gcd(f,g)$，并且将上面的带余除法的式子从下向上回代即可得到 Bezout 关系，详细的步骤我们留给读者作为练习。这个算法仍称作辗转相除法或者 Euclidean 算法。

例 6.1.6 设 $f(x)=x^4+\overline{1}, g(x)=x^3+\overline{1}\in\mathbb{Z}_2[x]$，求 $\gcd(f,g)$。

解: 做带余除法 (利用竖式) 如下：

$$\begin{aligned}
x^4+\overline{1} &= x(x^3+\overline{1}) + x + \overline{1}\\
x^3+\overline{1} &= (x^2+x+\overline{1})(x+\overline{1})
\end{aligned}$$

即 $\gcd(f,g)=x+\overline{1}$。

定义 6.1.6 设 $\mathbb{F}$ 是域，$f,g\in\mathbb{F}[x]\setminus\{0\}$，如果 $\gcd(f,g)=1$，则我们称 f,g 互素 (relatively prime)。

定理 6.1.8 设 $\mathbb{F}$ 是域，$f,g\in\mathbb{F}[x]\setminus\{0\}$，则 f,g 互素 $\iff \exists u,v\in\mathbb{F}[x]$ 使得 $uf+vg=1$。

由定义立刻可证。

定义 6.1.7 设整环 R 满足如下条件：存在尺度函数 $\delta: R\setminus\{0\}\to\mathbb{N}$ 满足：
(1)$\forall a,b\in R^*$，$\delta(ab)\geqslant\delta(a)$；[2]
(2) 对 $\forall a\in R, b\in R^*$，$\exists q,r\in R$ 使得 $a=qb+r$，其中 $\delta(r)<\delta(b)$ 或者 $r=0$。
则我们称 R 是欧几里得环 (欧氏环,Euclidean ring)。

显然在欧氏环中我们可以做辗转相除法。类似于定理 6.1.7的证明，我们可以得到：

定理 6.1.9 欧氏环 R 中任意两个非零元素 a,b 都有最大公因子 $d=\gcd(a,b)$，并且存在 $u,v\in R$ 使得 $d=ua+vb$。

如果欧氏环 R 中 $\gcd(a,b)=1$，则我们称 a,b 互素。显然仍有 a,b 互素 $\iff\exists u,v\in R$ 使得 $ua+vb=1$。

在下一节，我们的主要任务就是证明：欧氏环一定是唯一因子分解整环。

[1]即 $\mathbb{F}[x]$ 的每个理想都可以由一个元素生成，我们会在抽象代数课程中继续学习。
[2]这个条件可以去掉，但后面证明欧氏环是唯一因子分解整环会复杂一些。

6.2 多项式的因式分解

6.2.1 唯一因子分解整环

这一节中我们统一用 D 表示整环，$\mathbb{F}$ 表示域。记 $D^* = D \setminus \{0\}$, $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$。

定义 6.2.1 设 $a \in D^* \setminus D^\times$，如果不存在 $b, c \in D^* \setminus D^\times$ 使得 $a = bc$，则称 a 是不可约元 (irreducible element)，称分解 $a = bc$ 是非平凡的；如果 $\forall b, c \in D^*$，由 $a \mid (bc)$ 都能得到 $a \mid b$ 或 $a \mid c$，则称 a 是素元 (prime element)。

例 6.2.1 在 $\mathbb{Z}$ 中不可约元和素元都是素数；在 $\mathbb{Q}[x]$ 中 $x^2 - 2$ 是不可约元，同时也是素元，但在 $\mathbb{R}[x]$ 中 $x^2 - 2$ 既不是不可约元也不是素元。

命题 6.2.1 设 $p \in D^*$ 是素元，则 p 一定是不可约元。

证明: 用反证法。假设 p 不是不可约元，即 $\exists a, b \in D^* \setminus D^\times$ 使得 $p = ab$，由 p 是素元可知 $p \mid a$ 或 $p \mid b$。不妨设 $p \mid a$，则 $\exists c \in D^*$ 使得 $cp = a$，那么我们有 $p = ab = cpb$，即 $p(1 - cb) = 0$。由于 D 是整环，$p \neq 0$，故 $bc = 1$，这与 $b \notin D^\times$ 矛盾！这样我们就证明了命题。 □

但上面命题的逆命题是不成立的，我们看下面的例子。

例 6.2.2 显然 $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ 在通常的加法和乘法下是整环，在 $\mathbb{Z}[\sqrt{-3}]$ 上定义范数 $N(a + b\sqrt{-3}) = a^2 + 3b^2$，容易验证对 $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$，有 $N(\alpha\beta) = N(\alpha)N(\beta)$ 成立。

首先我们考虑 2 在 $\mathbb{Z}[\sqrt{-3}]$ 上的分解。设 $2 = (a + b\sqrt{-3})(c + d\sqrt{-3})$, $a, b, c, d \in \mathbb{Z}$，如果 $b = 0$ 或 $d = 0$，则 $a + b\sqrt{-3}$ 或 $c + d\sqrt{-3}$ 中至少有一个是 ± 1，这样的分解显然不是非平凡的；如果 b, d 均不为 0，则取范数即得 $4 = (a^2 + 3b^2)(c^2 + 3d^2) \geqslant 3 \cdot 3 = 9$，矛盾！故 2 没有非平凡的分解，即 2 是 $\mathbb{Z}[\sqrt{-3}]$ 中的不可约元。

然而，$2 \mid (1 + \sqrt{-3})(1 - \sqrt{-3})$，但 $2 \nmid (1 + \sqrt{-3})$, $2 \nmid (1 - \sqrt{-3})$，故 2 不是素元。

上面的例子告诉我们不可约元不一定是素元。但在一些特殊的环中，不可约元和素元是等价的。

引理 6.2.1 设 $\mathbb{F}$ 是域，则 $\mathbb{F}[x]$ 中不可约元都是素元。

证明: 设 $p \in \mathbb{F}[x]$ 不可约，$f, g \in \mathbb{F}[x]$ 且 $p \mid (fg)$，我们只需证明：如果 $p \nmid f$，则必有 $p \mid g$。
由于 $p \nmid f$ 且 p 不可约，则必有 $\gcd(p, f) = 1$，于是存在 $u, v \in \mathbb{F}[x]$ 使得 $uf + vp = 1$，则 $ufg + vpg = g$，由于 $p \mid (fg)$ 且 $p \mid vp$，故 $p \mid g$。 □

定义 6.2.2 设 $a \in D^*$，如果存在 $\alpha \in D^\times$ 及不可约元 $p_1, p_2, \ldots, p_s$ 使得 $a = \alpha p_1 \cdots p_s$，则称 a 在 D 中有有限的不可约分解，称 $p_1, \ldots, p_s$ 为 a 的不可约因子。

例如，$\mathbb{Z}$ 中每个非零的整数都有有限的不可约分解 (证明是显然的，留作练习)。

命题 6.2.2 $\mathbb{F}[x]$ 中每个非零多项式都有不可约分解。

证明: 用数学归纳法。设 $f \in \mathbb{F}[x]$, $\deg(f) = d$。
(1)$d = 0, 1$ 时 f 本身不可约，这是显然的。
(2) 设 $d > 1$ 且命题对一切次数小于 d 的多项式成立。现在 $\deg(f) = d$，如果 f 本身是不可约元，则结论直接成立；否则必存在 $g, h \in \mathbb{F}[x] \setminus \{0\}$ 使得 $f = gh$，且 $g, h \notin \mathbb{F}[x]^\times$，即 $0 < \deg(g) < d$, $0 < \deg(h) < d$。由归纳假设，g, h 有有限的不可约分解，则将它们乘在一起就得到了 f 的不可约分解。 □

定义 6.2.3 如果 D^* 中的每个元素都有有限的不可约分解并且如果 $a \in D^*$ 有两个不可约分解 $a = up_1 \cdots p_m = vq_1 \cdots q_n$(其中 $u, v \in D^\times$, $p_1, \ldots, p_m, q_1, \ldots, q_n$ 都是不可约元)，则有 $m = n$ 且经过适当地调整顺序后 $\forall k \in \{1, 2, \ldots, m\}$, $p_k \approx q_k$，那么我们称 D 是唯一因子分解整环 (unique factorization domain,UFD)。

我们解释一下分解的唯一性。例如，在 $\mathbb{Z}$ 中 $24 = 2 \times 2 \times 2 \times 3 = -3 \times (-2) \times 2 \times 2$，则调整顺序后有 $3 \approx 3, 2 \approx (-2), 2 \approx 2, 2 \approx 2$。

定理 6.2.1 设 D^* 中每个元素都有有限的不可约分解，则 D 是唯一因子分解整环 $\iff$ D 中的不可约元都是素元。

证明: ($\Longrightarrow$) 设 p 是 D 中的不可约元，如果有 $a, b \in D^*$ 满足 $p \mid (ab)$ 且 $p \nmid a$，我们只需证 $p \mid b$。设

$$a = up_1 \cdots p_m,\ b = vq_1 \cdots q_n,\ u, v \in D^\times$$

分别是 a, b 的不可约分解，由 $p \mid (ab)$ 可知存在 $c \in D^*$, $ab = cp$。设 c 的不可约分解为 $c = wr_1 \cdots r_s$，其中 $w \in D^\times$，$r_1, \ldots, r_s$ 是不可约元，于是

$$w(r_1 \cdots r_s p) = uv(p_1 \cdots p_m q_1 \cdots q_n)$$

由于 D 是唯一因子分解整环，故 $s + 1 = m + n$ 并且调整顺序后每个 $r_1, \ldots, r_s, p$ 唯一地与 $p_1, \ldots, p_m, q_1, \ldots, q_n$ 中的某个元素相伴。由于 $p \nmid a$，故 p 不能与 $p_1, \ldots, p_m$ 当中的元素相伴，于是存在 $j \in \{1, \ldots, n\}$ 使得 $p \approx q_j$。不妨设 $p \approx q_1$，即 $p = \alpha q_1, \alpha \in D^\times$，则

$$b = v\alpha^{-1}(\alpha q_1)q_2 \cdots q_n = (v\alpha^{-1})pq_2 \cdots q_n.$$

即 $p \mid b$ 成立。这个方向就证完了。
($\Longleftarrow$) 任取 $a \in D^*$，设 $a = up_1 \cdots p_m = vq_1 \cdots q_n$，其中 $u, v \in D^\times$, $p_1, \ldots, p_m, q_1, \ldots, q_n$ 都是不可约元。不妨设 $m \leqslant n$，则由 $p_1 \mid q_1 \cdots q_n$(因为 $p_1 \mid v^{-1}up_1 \cdots p_m = q_1 \cdots q_n$) 及 p_1 是素元可知 $\exists j \in \{1, \ldots, n\}$ 使得 $p_1 \mid q_j$。不妨设 $j = 1$，由 q_1 不可约可知 $p_1 \approx q_1$，即 $\exists \rho_1 \in D^\times$ 使得 $q_1 = \rho_1 p_1$。那么我们有：

$$up_1 p_2 \cdots p_m = v\rho_1 p_1 q_2 \cdots q_n$$

由消去律可知 $up_2 \cdots p_m = v\rho_1 q_2 \cdots q_n$，其中 $v\rho_1 \in D^\times$。重复以上步骤可以得到 $p_1 \approx q_1, \cdots, p_m \approx q_m$ 并且

$$u = (v\rho_1 \cdots \rho_m)(q_{m+1} \cdots q_n).$$

于是如果 $m < n$，就有 $1 = (u^{-1}v\rho_1 \cdots \rho_m)(q_{m+1} \cdots q_n)$，即 $(q_{m+1} \cdots q_n)$ 是可逆元，这与 $q_{m+1}, \ldots, q_n$ 是不可约元矛盾！即必有 $m = n$ 并且 $\forall i \in \{1, \ldots, n\}$, $p_i \approx q_i$。这样我们就完成了证明。 □

我们在上一节的末尾已经定义了欧氏环。显然 $\mathbb{Z}, \mathbb{F}[x]$ 都是欧氏环，其尺度函数分别是绝对值和多项式的次数。下面我们来证明本节的主要结论。

定理 6.2.2 欧氏环是唯一因子分解整环。

证明: 设 R 是欧氏环，尺度函数为 δ. 我们首先证明：R^* 中的每一个元素都有有限的不可约分解。首先，如果 $a \in R^\times$，那么 a 本身就是不可约分解；其次，a 本身是不可约元的情形也是平凡的。于是我们只需考虑 $a \notin R^\times$ 且 a 有真因子的情形。设 $a = bc$，其中 $b, c \notin R^\times$，我们先来证明 $\delta(b) < \delta(a)$。

事实上，由尺度函数的定义，首先我们有 $\delta(b) \leqslant \delta(a)$。如果 $\delta(b) = \delta(a)$，做带余除法 $b = qa+r$，则 $\delta(r) < \delta(a)$ 且 $r \neq 0$(如果 $r = 0$，即 $a \mid b$，于是 $a \approx b$ 与 b 是 a 的真因子矛盾！)。显然 $1-qc \neq 0$(否则 $c \in R^\times$ 矛盾！)，则有

$$\delta(a) = \delta(b) \leqslant \delta(b(1-qc)) = \delta(b-qa) = \delta(r) < \delta(a)$$

这是一个矛盾！故 a 有真因子 $b \Longrightarrow \delta(b) < \delta(a)$。

现在我们可以证明不可约分解是有限的了。设 $a = a_1a_2a_3\cdots$，其中每个 $a_i, i \in \mathbb{Z}^+$ 都不可逆，则每个 $a_{i+1}a_{i+2}\cdots$ 都是 $a_ia_{i+1}a_{i+2}\cdots$ 的真因子，于是

$$\delta(a) = \delta(a_1a_2a_3\cdots) > \delta(a_2a_3\cdots) > \delta(a_3\cdots) > \cdots$$

由于 $\delta(a) \in \mathbb{N}$ 是一个有限数，故这个不等式链必然在某一步终止，即必有 $a = a_1a_2a_3\cdots a_n$ 且 $n \leqslant \delta(a)$。所以 a 的长度最长的因子链就是 a 的不可约分解 (如果其中某个元素可约，则可以分解成不可约元的乘积，这会导致因子链变长，矛盾！)。

最后我们利用定理 6.2.1来证明欧氏环是唯一因子分解整环。设 p 是 R 中的不可约元，我们只需证 p 是素元。设 $p \mid (ab)$ 且 $ab \neq 0$，不妨设 $p \nmid a$，由 p 不可约知 $\gcd(p,a) = 1$，那么由定理 6.1.9得 $\exists u, v \in R$ 使得 $up + va = 1$，于是 $upb + vab = b$，由 $p \mid upb$, $p \mid ab$ 可知 $p \mid b$，即 p 是素元。这样我们就完成了证明。 □

推论 6.2.1 $\mathbb{Z}$ 和 $\mathbb{F}[x]$ 都是唯一因子分解整环。[1]

由 $\mathbb{Z}$, $\mathbb{F}[x]$ 都是欧氏环即可证明。

然而，$\mathbb{F}[x,y]$ 就不是欧氏环，但它仍然是唯一因子分解整环。证明参见习题课讲义。

下面我们利用唯一因子分解整环的性质来更精细地讨论多项式的根。

定义 6.2.4 设 D 是唯一因子分解整环，$p \in D$ 是不可约元，$a \in D^*$。如果 $\exists m \in \mathbb{N}$ 使得 $p^m \mid a$ 但 $p^{m+1} \nmid a$，则称 m 是 p 在 a 中的重数。

例如，$\mathbb{Z}$ 上 2 在 24 中的重数为 3，$\mathbb{Q}[x]$ 中 $3x+1$ 在 $f(x) = (x-1)(3x+1)^2(x^2+1)$ 中的重数为 2。

定义 6.2.5 设 $\mathbb{F}$ 是 $\mathbb{K}$ 的子域，$\alpha \in \mathbb{K}$, $f(x) \in \mathbb{F}[x] \setminus \mathbb{F}$ 并且 $f(\alpha) = 0$，则 $\mathbb{K}[x]$ 上 $x-\alpha$ 在 f(视作 $\mathbb{K}[x]$ 中的元素) 中的重数称为根 α 的重数。特别地，当重数为 1 时，我们称 α 是 f 的单根；当重数等于 $m(>1)$ 时，称 α 是 f 的 m 重根。

例如，在 $\mathbb{C}[x]$ 中 $f(x) = (x-1)(3x+1)^2(x^2+1)$ 有单根 $x = 1, \pm i$ 和 2 重根 $x = -\frac{1}{3}$。

命题 6.2.3 设 $\mathbb{F}$ 是 $\mathbb{K}$ 的子域，$f(x) \in \mathbb{F}[x] \setminus \mathbb{F}$，并且 $f(x)$ 在 $\mathbb{K}$ 中的所有互不相同的根为 $\alpha_1, \ldots, \alpha_s$，其重数分别为 $m_1, \ldots, m_s$，则我们有 $m_1 + \cdots + m_s \leqslant \deg(f)$。

证明: 设 $d = \deg(f)$，对 d 做数学归纳法。

(1)$d = 1$ 时 f 只有一个单根，命题显然成立。

(2) 设命题对 $\mathbb{F}[x]$ 中所有次数小于 d 的多项式成立，则对 f 而言，考虑 $\alpha_s \in \mathbb{K}$ 是 f 的 m_s 重根，即存在 $g(x) \in \mathbb{K}[x]$ 使得 $f(x) = g(x)(x-\alpha_s)^{m_s}$，并且 $g(\alpha_s) \neq 0$, $\deg(g) < \deg(f)$。我们需要证明 $\alpha_1, \ldots, \alpha_{s-1}$ 是 $g(x)$ 分别是 $g(x)$ 的 $m_1, \ldots, m_{s-1}$ 重根。

[1] 前者被称为算术基本定理。

首先，由于对 $\forall i \in \{1,2,\dots,s-1\}$，有 $\alpha_i \neq \alpha_s$，则 $(x-\alpha_i)^{m_i}$ 与 $(x-\alpha_s)^{m_s}$ 在 $\mathbb{K}[x]$ 上互素 (UFD)，即存在 $u,v \in \mathbb{K}[x]$ 使得 $u(x)(x-\alpha_i)^{m_i}+v(x)(x-\alpha_s)^{m_s}=1$，于是 $u(x)(x-\alpha_i)^{m_i}g(x)+v(x)(x-\alpha_s)^{m_s}g(x)=g(x)$，也即

$$u(x)(x-\alpha_i)^{m_i}g(x)+v(x)f(x)=g(x)$$

由于 $(x-\alpha_i)^{m_i} \mid (x-\alpha_i)^{m_i}g(x)$，$(x-\alpha_i)^{m_i} \mid f(x)$，故 $(x-\alpha_i)^{m_i} \mid g(x)$。

另一方面，对 $\forall i \in \{1,2,\dots,s-1\}$，由于 α_i 是 f 的 m_i 重根，即 $(x-\alpha_i)^{m_i+1} \nmid f$，所以 $(x-\alpha_i)^{m_i+1} \nmid g$，这说明 α_i 在 g 中的重数不超过 m_i。于是由归纳假设，$\deg(g) \geqslant m_1+\cdots+m_{s-1}$，于是 $\deg(f)=\deg(g)+m_s \geqslant m_1+\cdots+m_s$。 □

于是我们立刻有：

推论 6.2.2 设 $\mathbb{F}$ 是 $\mathbb{K}$ 的子域，$f,g \in \mathbb{F}[x] \setminus \mathbb{F}$ 且 $\deg(f),\deg(g) \leqslant n$。如果 $\exists \alpha_1,\dots\alpha_{n+1} \in \mathbb{K}$ 使得 $\forall i \in \{1,\dots,n+1\}$，$f(\alpha_i)=g(\alpha_i)$，则 $f=g$。

证明：反证法，如果命题不成立，则令 $h=f-g\neq 0$，注意到 h 有 $n+1$ 个不同的根 $\alpha_1,\dots\alpha_{n+1}$，这与命题 6.2.3矛盾！ □

6.2.2 多项式函数与插值

设 D 是整环，任取多项式 $f \in D[x]$，则赋值同态给出了一个 D 到 D 的映射 (函数) $\widetilde{f}: D \to D,\ a \mapsto f(a)$。我们把所有 $\widetilde{f}$ 放在一起做成一个集合 D_{pol}，并在 D_{pol} 上定义加法和乘法运算如下：

$$\widetilde{f}+\widetilde{g}: D \to D,\ a \mapsto f(a)+g(a); \qquad \widetilde{f}\cdot\widetilde{g}: D \to D,\ a \mapsto f(a)g(a).$$

则 D_{pol} 在上述加法和乘法下构成环，称为 D 上的多项式函数环。我们显然有：$\varphi: D[x] \to D_{pol},\ f(x) \mapsto \widetilde{f}$ 是一个满同态，但这个同态不一定是同构。例如，$\mathbb{Z}_p$(p 是素数) 上 x^p-x 是一个非零多项式，但 $\varphi(x^p-x)=\widetilde{0}$，即 $\ker(\varphi)\neq\{0\}$。那么，φ 何时是同构呢？我们有下面的定理。

定理 6.2.3 如果整环 D 满足 $|D|=\infty$，则 $\varphi: D[x] \to D_{pol},\ f(x) \mapsto \widetilde{f}$ 是同构。

证明：只需证明此时 $\ker(\varphi)=\{\widetilde{0}\}$。反证法，如果存在非零多项式 $f \in D[x]$ 使得 $\widetilde{f}=\widehat{0}$，即 D 中的元素都是 f 的根，这与 f 只有有限多个不同的根 (定理 6.1.6) 矛盾！于是命题得证。 □

由上面的定理，我们可以把无限域 $\mathbb{F}$ 上的多项式 $f(x) \in \mathbb{F}[x]$ 视作 $\mathbb{F} \to \mathbb{F}$ 的函数，那么，我们自然会有这样的问题：给定这个多项式函数在一些点上的取值，如何确定这个函数的表达式 (即多项式) 呢？这就是我们下面讨论的**插值** (interpolation) 问题。

定理 6.2.4 设 $\mathbb{F}$ 是无限域，$\alpha_1,\dots,\alpha_n \in \mathbb{F}$ 两两不同，$\beta_1,\dots,\beta_n \in \mathbb{F}$，则存在唯一的 $f \in \mathbb{F}[x]$ 满足 $\deg(f)<n$ 且 $\forall i \in \{1,\dots,n\}$，$f(\alpha_i)=\beta_i$。

证明：一个自然的解决这个问题的思路是我们在中学就已经学过的待定系数法。由于我们要求 $\deg(f)<n$，故可设 $f=f_0+f_1x+\cdots+f_{n-1}x^{n-1}$，则由 $\forall i \in \{1,\dots,n\}$，$f(\alpha_i)=\beta_i$ 可以列出如下的线性方程组：

$$\begin{cases} f_0+\alpha_1 f_1+\cdots+\alpha_1^{n-1}f_{n-1}=\beta_1 \\ f_0+\alpha_2 f_1+\cdots+\alpha_2^{n-1}f_{n-1}=\beta_2 \\ \qquad\qquad\qquad\qquad\vdots \\ f_0+\alpha_n f_1+\cdots+\alpha_n^{n-1}f_{n-1}=\beta_n \end{cases}$$

即

$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}.$$

记上面方程组的系数矩阵为 A。注意到系数矩阵是 Vandermonde 矩阵，由 $\alpha_1, \ldots, \alpha_n$ 互不相同可知 $\det(A) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i) \neq 0$，于是上面的方程组存在唯一解，并且我们可以验证

$$f(x) = \sum_{i=1}^{n} \beta_i \frac{(x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_n)}{(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n)} \tag{6.2.1}$$

就是满足条件的解。这样我们就完成了证明。 □

我们把上面证明过程中出现的式 (6.2.1) 称为 Lagrange **插值公式**。Lagrange 插值公式的构造可以类比中国剩余定理的构造得到，具体细节留作思考。实际上，Lagrange 插值公式是一般交换环上中国剩余定理的特例。此外，定理也可以在有限域上使用，但需要注意的是，此时必须有限制条件 $\deg(f) < |\mathbb{F}|$ (思考之)。

我们也可以用另一种办法解决插值问题。条件同上，我们不妨设 $f(x)$ 的形式为

$$f(x) = u_0 + u_1(x-\alpha_1) + u_2(x-\alpha_1)(x-\alpha_2) + \cdots + u_{n-1}(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{n-1})$$

依次代入 $\alpha_1, \alpha_2, \ldots, \alpha_n$ 可以得到关于 $u_0, u_1, \ldots, u_{n-1}$ 的一元一次方程，这样即可确定 f。这种方法称为牛顿插值。

插值问题在理论研究和实际应用中都有重要的意义。我们在以后的学习中还会经常遇到它。

6.2.3 多项式的形式微分与无平方分解

我们在分析学中学过导数，也知道 $\mathbb{R}[x]$ 中的多项式函数是可微函数。注意到多项式函数的导数可以直接利用法则计算，而不需要依赖其分析学的意义。那么，我们是否可以在一般域的多项式环上定义代数风格的“导数”呢？这就是下面讨论的内容。

定义 6.2.6 设 $\mathbb{K}$ 是域，在 $\mathbb{K}[x]$ 上定义如下映射：

$$\frac{\mathrm{d}}{\mathrm{d}x} : \mathbb{K}[x] \to \mathbb{K}[x]$$
$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \mapsto \frac{\mathrm{d}f}{\mathrm{d}x} = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

我们把 $\dfrac{\mathrm{d}}{\mathrm{d}x}$ 称为 $\mathbb{K}[x]$ 上的形式导数或形式微分算子。显然这个定义与分析学中的定义是一致的。我们也把 $\dfrac{\mathrm{d}f}{\mathrm{d}x}$ 记作 $f'(x)$，对 f 求 n 次导数记作 $f^{(n)}(x)$ 或 $\frac{\mathrm{d}^n f}{\mathrm{d}x^n}$。

容易验证形式微分算子满足以下性质：对 $\forall f, g \in \mathbb{K}[x]$, $\lambda \in \mathbb{K}$，我们有

(1) $\dfrac{\mathrm{d}(f+g)}{\mathrm{d}x} = \dfrac{\mathrm{d}f}{\mathrm{d}x} + \dfrac{\mathrm{d}g}{\mathrm{d}x}$;

(2) $\dfrac{\mathrm{d}\lambda f}{\mathrm{d}x} = \lambda \dfrac{\mathrm{d}f}{\mathrm{d}x}$;

(3) $\dfrac{\mathrm{d}(fg)}{\mathrm{d}x} = \dfrac{\mathrm{d}f}{\mathrm{d}x} g + f \dfrac{\mathrm{d}g}{\mathrm{d}x}$(称为 Leibniz 法则).

更一般地，我们可以利用这些性质在一般的环上定义导数运算如下：

定义 6.2.7 设 A 是任意交换环，K 是 A 的子环，如果映射 $D_K : A \to A$ 满足：对 $\forall x, y \in A$ 及 $\lambda \in K$，有：

(i) $D_K(x+y) = D_K(x) + D_K(y)$;

(ii) $D_K(\lambda x) = \lambda D_K(x)$;

(iii) $D_K(xy) = D_K(x)y + xD_K(y)$.

则称 D_K 是 A 上的一个 K-导子 (或 K-导数，K-derivative)。我们把 A 上的所有 K-导子组成的集合记作 $\mathrm{Der}(A)$，称为 A 上的 K-导子代数，它是李代数 (Lie algebra) 的重要研究对象。

例 6.2.3 设 $\mathbb{K}$ 是域，令 $A = \mathbb{K}[x]$，则由上面的定义可知 A 中的所有 $\mathbb{K}$-导子必然满足 $\forall f \in \mathbb{K}[x]$, $D(f) = \dfrac{\mathrm{d}f}{\mathrm{d}x} D(x)$ (提示：利用 $D(x^n) = xD(x^{n-1}) + x^{n-1}D(x)$，归纳得到 $D(x^n) = nx^{n-1}D(x)$，再利用算子 D 的线性性质，细节留作练习)。于是 $\mathbb{K}[x]$ 中的任意 $\mathbb{K}$-导子由 $D(x)$ 的值唯一确定。特别地，当 $D(x) = 1$ 时，D 就回到了形式微分算子的情形。

此外，由定义 6.2.7的 (iii) 可知，导子 D 满足 $D^n(xy) = \sum_{k=0}^{n} \binom{n}{k} D^k(x) D^{n-k}(y)$，这个性质称为 Leibniz 公式。

下面我们考虑多项式的因子的重数和形式微分的关系。设 $\mathbb{F}$ 是域，则 $\mathbb{F}[x]$ 是唯一因子分解整环，即 $\forall f \in \mathbb{F}[x]$，存在唯一的不可约分解 $f(x) = \lambda p_1(x)^{k_1} \cdots p_r(x)^{k_r}$，$\lambda \in \mathbb{F}$，$p_1, \ldots, p_r \in \mathbb{F}[x]$ 是不可约多项式，我们把 k_i 称为素因子 p_i 的重数。

定理 6.2.5 设 $p(x)$ 是 $f(x) \in \mathbb{F}[x]$ 的 k 重不可约因子，且 $\mathrm{char}(\mathbb{F}) \nmid k$，则 p 是 f' 的 $k-1$ 重因子。特别地，设 p 是 f 的不可约因子，则 p 的重数是 $1 \iff \gcd(p, f') = 1$。

证明: 设 $f(x) = [p(x)]^k g(x)$，其中 $\gcd(p(x), g(x)) = 1$，则 $f'(x) = [p(x)]^{k-1}(kp'(x)g(x) + p(x)g'(x))$，由于 $p(x)$ 不可约，故 $p'(x) \neq 0$，又 $k \nmid \mathrm{char}(\mathbb{F})$，故 $kp'(x)g(x) \neq 0$，于是 $p(x) \nmid kp'(x)g(x)$ (注意 p 是素元)，即 $p(x) \nmid kp'(x)g(x) + p(x)g'(x)$，所以 p 是 f' 的 $k-1$ 重因子。特例可以由定理的结论直接得到。 □

推论 6.2.3 (1) 设 $\mathbb{F}$ 是域，$f(x) \in \mathbb{F}[x]$，$p(x)$ 是 f 的不可约因子，$\mathrm{char}(\mathbb{F}) \nmid k!$。则 p 在 f 中的重数是 $k \iff \forall i \in \{0, 1, \ldots, k-1\}$ 都有 $p(x) \mid f^{(i)}(x)$，但 $p(x) \nmid f^{(k)}(x)$。
(2) 设 $\mathbb{F}$ 是 $\mathbb{K}$ 的子域，$\mathrm{char}(\mathbb{F}) \nmid k!$，则 $\alpha \in \mathbb{K}$ 是 $f(x) \in \mathbb{F}[x]$ 的 k 重根 $\iff f(\alpha) = f'(\alpha) = \cdots = f^{(k-1)}(\alpha) = 0$, $f^{(k)}(\alpha) \neq 0$。
(3) 令 $f(x) = \lambda p_1(x)^{k_1} \cdots p_r(x)^{k_r}$, $\lambda \in \mathbb{F}$ 是 $f(x)$ 的不可约分解，其中 $k_i > 0$，如果对每个 $i \in \{1, \ldots, r\}$ 都有 $\mathrm{char}(\mathbb{F}) \nmid k_i$，则 $\gcd(f, f') = p_1(x)^{k_1 - 1} \cdots p_r(x)^{k_r - 1}$。

证明: (1)($\Longrightarrow$) 注意到 $\mathrm{char}(\mathbb{F}) \nmid k! \Longrightarrow \forall i \in \{0, 1, \ldots, k-1\}, \mathrm{char}(\mathbb{F}) \nmid k - i$，于是由定理 6.2.5可以归纳地得到 p 是 f' 的 $k-1$ 重因子，p 是 f'' 的 $k-2$ 重因子，……p 是 $f^{(k-1)}$ 的 1 重因子，所以 p 与 $f^{(k)}$ 互素，这样就证明了该方向。
($\Longleftarrow$) 设 p 是 f 的 l 重因子，我们只需要证明 $l = k$ 即可。由 ($\Longrightarrow$) 方向可知，p 是 f 的 l 重因子立刻有：$\forall i \in \{0, 1, \ldots, l-1\}$ 都有 $p(x) \mid f^{(i)}(x)$，但 $p(x) \nmid f^{(l)}(x)$。显然这只有当 $l = k$ 时才成立，否则与条件 “$\forall i \in \{0, 1, \ldots, k-1\}$ 都有 $p(x) \mid f^{(i)}(x)$，但 $p(x) \nmid f^{(k)}(x)$” 矛盾。
(2) 我们把 f 视作 $\mathbb{K}[x]$ 中的多项式，取 $p(x) = x - \alpha$，由 (1) 及定理 6.1.6(i) 即得结论。

(3) 由于每个 k_i 都不能被 $\mathrm{char}(\mathbb{F})$ 整除，故对每个 i，$f'(x)$ 可以写成 $[p_i(x)]^{k-1}g_i(x)$ 的形式，其中 $\gcd(p_i, g_i) = 1$。于是由 (1) 可得：对 $\forall i \in \{1, \ldots, r\}$，$p_i(x)$ 是 f' 的 $k_i - 1$ 重因子，即 $\exists g \in \mathbb{F}[x]$，$f'(x) = p_1(x)^{k_1-1} \cdots p_r(x)^{k_r-1}g(x)$，且 $\gcd(p_i, g) = 1$ 对每个 $i \in \{1, \ldots, r\}$ 成立。于是对任意一组非负整数 $l_1, \ldots, l_r$，我们有 $\gcd(p_1(x)^{l_1} \cdots p_r(x)^{l_r}, g(x)) = 1$，特别地，$\gcd(f, g) = 1$，于是 $\gcd(f, f') = p_1(x)^{k_1-1} \cdots p_r(x)^{k_r-1}$。 □

定义 6.2.8 设 $\mathbb{F}$ 是域，$f(x) = \lambda p_1(x)^{k_1} \cdots p_r(x)^{k_r}$，$\lambda \in \mathbb{F}$ 是 $f(x)$ 的不可约分解，其中 $k_i > 0$，令 $g(x) = \dfrac{f(x)}{\gcd(f, f')}$，则 $g(x)$ 与 $p_1(x) \cdots p_r(x)$ 相伴，我们称 $g(x)$ 是 f 的无平方部分。若 $f = \lambda q_1^{l_1} \cdots q_s^{l_s}$，其中 $q_1, \ldots, q_s$ 两两互素且在 $\mathbb{F}$ 上都没有重数大于 1 的因子，则称这个分解是 f 的无平方分解。

由于求 f 的无平方部分只需要求导和求最大公因子，因此我们并不需要知道 f 的素因子分解。因此，对 $\mathrm{char}(\mathbb{F}) = 0$ 的情形，我们可以通过反复地求导和辗转相除来求 f 的无平方分解。

例 6.2.4 设 $f(x) = x^5 - 3x^4 + 2x^3 + 2x^2 - 3x + 1 \in \mathbb{Q}[x]$，求 f 的无平方分解。

解：进行如下计算 (相伴意义下)：

$$
\begin{aligned}
&h_1(x) = \gcd(f, f') = x^3 - 3x^2 + 3x - 1, && g_1(x) = \frac{f}{h_1} = x^2 - 1 && \\
&h_2(x) = \gcd(h_1, h_1') = x^2 - 2x + 1, && g_2(x) = \frac{h_1}{h_2} = x - 1, && f_1 = \frac{g_1}{g_2} = x + 1 \\
&h_3(x) = \gcd(h_2, h_2') = x - 1, && g_3(x) = \frac{h_2}{h_3} = x - 1, && f_2 = \frac{g_2}{g_3} = 1 \\
&h_4(x) = \gcd(h_3, h_3') = 1, && g_4(x) = \frac{h_3}{h_4} = x - 1, && f_3 = \frac{g_3}{g_4} = 1 \\
&h_5(x) = \gcd(h_4, h_4') = 1, && g_5(x) = \frac{h_4}{h_5} = 1, && f_4 = \frac{g_4}{g_5} = x - 1.
\end{aligned}
$$

由于 $g_5 = 1$，算法停止，故 $f(x) = f_1 f_2^2 f_3^3 f_4^4 = (x + 1)(x - 1)^4$。

思考题 6.2.1 (1) 按上面例子的思路，写出一般的算法 (有余力的读者可以用计算机实现该算法)；(2) 当域的特征不为 0 时算法应该做什么样的改动 (此时会遇到 $f' = 0$ 的问题，思考之)？

6.2.4 整系数多项式的因子分解

这一小节我们来考虑整系数多项式的素因子分解。由于 $\mathbb{Z}$ 中除了 ± 1 之外的数关于乘法都不可逆，这给我们做分解带来了许多额外的困扰 (比如 $2x^2 + 3x + 1$ 就不能再写成 $2(x + 1)(x + \frac{1}{2})$ 了)。为此，我们需要新的工具来处理整系数多项式。

定义 6.2.9 设 $f(x) \in \mathbb{Z} \setminus \{0\}$，我们称 f 的所有系数的最大公因子为 f 的 **容度** (content)，记作 $\mathrm{cont}(f)$。如果 $\mathrm{cont}(f) = 1$，则称 f 是本原多项式 (primitive polynomial)。

例如，$\mathrm{cont}(2x^2+3x+1) = 1$，$\mathrm{cont}(24x^3+3x-12) = 3$。设 $a \in \mathbb{Z}$，显然我们有 $\mathrm{cont}(af) = a\mathrm{cont}(f)$。

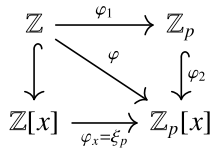
在讨论整系数多项式时，将系数模掉一个素数是一种常用的方法，这可以在使系数变小的同时保留原多项式的一些信息。

引理 6.2.2 设 p 是任意素数，则

(1) 令

$$
\begin{aligned}
\xi_p : \mathbb{Z}[x] &\longrightarrow \mathbb{Z}_p[x] \\
f = \sum_{i=0}^{d} f_i x^i &\longmapsto \overline{f} = \sum_{i=0}^{d} \overline{f}_i x^i.
\end{aligned}
$$

其中 $\overline{f_i}$ 是 f_i 模 p 的剩余类。则 ξ_p 是满的环同态。
(2) 如果 $f \in \mathbb{Z}[x]$ 是本原多项式，则 $\xi_p(f) \neq \overline{0}$。



证明: (1) 显然 $\varphi_1 : \mathbb{Z} \to \mathbb{Z}_p,\ a \mapsto \overline{a}$ 和 $\varphi_2 : \mathbb{Z}_p \to \mathbb{Z}_p[x],\ \overline{1} \mapsto \overline{1}$ 都是环同态，于是 $\varphi = \varphi_2 \circ \varphi_1 : \mathbb{Z} \to \mathbb{Z}_p[x]$ 也是环同态，由赋值同态 (定理 6.1.3) 可知 $\varphi_x = \xi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x],\ x \mapsto x$ 也是环同态。ξ_p 是满射显然。
(2) 若 $\xi_p(f) = \overline{0}$，则 $\overline{f_0} = \cdots = \overline{f_d} = \overline{0}$，即 $p \mid f_0, \ldots, p \mid f_d$，这与 $\mathrm{cont}(f) = 1$ 矛盾! □

下面我们先看一些例子。

例 6.2.5 $\mathbb{Z}_2[x]$ 中二次多项式只有 $x^2,\ x^2 + x = x(x + \overline{1}),\ x^2 + \overline{1} = (x + \overline{1})^2,\ x^2 + x + \overline{1}$，其中只有最后一个是不可约多项式。

例 6.2.6 求证 $f(x) = x^4 + x + 1 \in \mathbb{Z}[x]$ 在 $\mathbb{Z}[x]$ 上不可约。

解: 考虑 $\xi_2 : \mathbb{Z}[x] \to \mathbb{Z}_2[x]$，如果 f 在 $\mathbb{Z}[x]$ 上可约，那么 $\xi_2(f)$ 在 $\mathbb{Z}_2[x]$ 上也可约。用反证法。如果 $\xi_2(f) = \xi_2(g)\xi_2(h)$，其中 $\xi_2(g), \xi_2(h)$ 的次数都大于 1 而小于 4，那么，我们讨论两种情况：
(1)$\xi_2(g), \xi_2(h)$ 中有一个是 1 次多项式，这说明 $\xi_2(f)$ 在 $\mathbb{Z}_2$ 上有根，而 $\xi_2(f)(\overline{0}) = \xi_2(f)(\overline{1}) = \overline{1}$，矛盾！此情形不成立。
(2)$\xi_2(g), \xi_2(h)$ 都是 $\mathbb{Z}_2[x]$ 中的 2 次不可约多项式，则由上一个例子可知 $\xi_2(f)$ 只能是 $(x^2+x+\overline{1})^2 = x^4 + x^2 + \overline{1}$，这与 $\xi_2(f) = x^4 + x + \overline{1}$ 矛盾！此情形亦不成立。
综上所述，$\xi_2(f)$ 在 $\mathbb{Z}_2[x]$ 上不可约，所以 f 在 $\mathbb{Z}[x]$ 上不可约。 □

引理 6.2.3 (Gauss **引理**) 设 $f, g \in \mathbb{Z}[x]$ 是本原多项式，则 fg 也是本原多项式。

证明: 用反证法。假设 fg 不是本原多项式，则存在素数 p 使得 $p \mid \mathrm{cont}(fg)$，于是 $\xi_p(fg) = \overline{0}$。由于 ξ_p 是环同态，故 $\xi_p(f)\xi_p(g) = 0$，然而 $\mathbb{Z}_p[x]$ 是整环，故 $\xi_p(f) = \overline{0}$ 或 $\xi_p(g) = \overline{0}$，即 $p \mid \mathrm{cont}(f)$ 或 $p \mid \mathrm{cont}(g)$，这与 f, g 都是本原多项式矛盾! □

注 6.2.1 显然对 $\forall f \in \mathbb{Z}[x] \setminus \{0\}$，$f$ 可以唯一地写成 $\mathrm{cont}(f)g$ 的形式，其中 g 是本原多项式。

推论 6.2.4 设 $f, g \in \mathbb{Z}[x]$，则 $\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g)$

证明: 设 $f = \mathrm{cont}(f)u(x),\ g = \mathrm{cont}(g)v(x)$，其中 $u, v \in \mathbb{Z}[x]$ 是本原多项式。于是

$$fg = \mathrm{cont}(f)\mathrm{cont}(g) \cdot uv$$

由 Gauss 引理，uv 是本原多项式，故 $\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g)$。 □

定理 6.2.6 设 $f(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$，如果 f 不能写成 $\mathbb{Z}[x]$ 中两个正次数多项式的乘积，则 f 在 $\mathbb{Q}[x]$ 中不可约。

证明: 用反证法。如果 f 在 $\mathbb{Q}[x]$ 中可约，即 $\exists g,h\in\mathbb{Q}[x]\setminus\mathbb{Q}$ 使得 $f=gh$。设 g,h 的所有系数的分母的最小公倍数分别为 a,b，则 $ag,bh\in\mathbb{Z}[x]$，不妨设 $ag=\mathrm{cont}(ag)u(x)$，$bh=\mathrm{cont}(bh)v(x)$，其中 $u,v\in\mathbb{Z}[x]$ 是正次数的本原多项式，则由 $(ab)f=ag\cdot bh$ 可知

$$ab\mathrm{cont}(f)=\mathrm{cont}(abf)=\mathrm{cont}(ag)\mathrm{cont}(bh)$$

则 $abf=ag\cdot bh=\mathrm{cont}(ag)\mathrm{cont}(bh)uv=\mathrm{cont}(abf)=ab\mathrm{cont}(f)uv$，即 $f=\mathrm{cont}(f)uv$，这与 f 不能写成 $\mathbb{Z}[x]$ 中两个正次数多项式的乘积矛盾! □

推论 6.2.5 设 $f(x)=f_0+f_1x+\cdots+f_nx^n\in\mathbb{Z}[x]$，如果 f 有有理数根 $\frac{r}{s}$，$\gcd(r,s)=1$，则 $r\mid f_0$，$s\mid f_n$。

证明: 由命题的条件可知在 $\mathbb{Q}[x]$ 上 $x-\frac{r}{s}$ 是 f 的因子，于是 $sx-r$ 是本原多项式并且由定理6.2.6的证明过程可得 $sx-r\mid f$，于是可设 $f=(sx-r)(a_0+\cdots+a_{n-1}x^{n-1})$，其中 $a_0,\ldots,a_{n-1}\in\mathbb{Z}$，展开上式右边并对比系数可知 $a_0r=-f_0$，$a_{n-1}s=f_{n-1}$，即 $r\mid f_0$，$s\mid f_n$。 □

这个推论可以帮助我们快速判断一个整系数 (或有理系数) 多项式是否有有理数根，即试根法。

下面我们给出一个判断整系数多项式是否可约的方法。

定理 6.2.7 (Eisenstein **判别法**) 设 $n\in\mathbb{Z},n\geqslant 2$，$f=x^n+f_{n-1}x^{n-1}+\cdots+f_1x+f_0\in\mathbb{Z}[x]$。如果存在素数 $p\in\mathbb{Z}$ 使得 $p\mid f_{n-1},\ldots,p\mid f_1,p\mid f_0$ 都成立但 $p^2\nmid f_0$，则 f 在 $\mathbb{Q}[x]$ 上不可约。

证明: 用反证法。假设 f 在 $\mathbb{Q}[x]$ 中可约，则由定理 6.2.6可知，存在 $g,h\in\mathbb{Z}[x]\setminus\mathbb{Z}$ 使得 $f=gh$。不妨设 $\deg(g)=d$，$\deg(h)=e$，则 $1<d<n$，$1<e<n$，并且设

$$g=x^d+g_{d-1}x^{d-1}+\cdots+g_0,\quad h=x^e+h_{e-1}x^{e-1}+\cdots+h_0.$$

由于 $p\mid f_{n-1},\ldots,p\mid f_1,p\mid f_0$，在 $f=gh$ 两边同时取 ξ_p 可得 $\xi_p(f)=\xi_p(g)\xi_p(h)$，即

$$x^n=(x^d+\overline{g_{d-1}}x^{d-1}+\cdots+\overline{g_0})(x^e+\overline{h_{e-1}}x^{e-1}+\cdots+\overline{h_0})$$

注意到 $\mathbb{Z}_p[x]$ 是唯一因子分解整环，$\overline{g_0}\,\overline{h_0}=0$, 因此 $\overline{g_0}=0$ 或 $\overline{h_0}=0$, $p\mid g_0$ 或 $p\mid h_0$. 因为 $p^2\nmid f_0$，我们可以假设 $p|g_0$，$p\nmid h_0$. 设 i 是最小满足 $\overline{g_i}\neq 0$, 则 $x^i,i\leqslant d$ 的系数是 $\overline{g_i}\,\overline{h_0}\neq 0$ 矛盾。这样我们就完成了证明。 □

需要说明的是，Eisenstein 判别法的逆命题不成立，例如 $x^{105}-9$ 在 $\mathbb{Q}[x]$ 上不可约 (试证明之 [1])。然而我们显然找不到素数 p 满足 Eisenstein 判别法的条件。

推论 6.2.6 设 $n\in\mathbb{Z},n\geqslant 2$，$f=f_nx^n+f_{n-1}x^{n-1}+\cdots+f_1x+f_0\in\mathbb{Z}[x]$。如果存在素数 $p\in\mathbb{Z}$ 使得 $p\nmid f_n$ 但 $p\mid f_{n-1},\ldots,p\mid f_1,p\mid f_0$，而且 $p^2\nmid f_0$，则 f 在 $\mathbb{Q}[x]$ 上不可约。

证明是类似的，留作练习。

在本小节的最后，我们看几个证明多项式不可约的例题。

例 6.2.7 求证 x^5+2x+2 在 $\mathbb{Q}[x]$ 上不可约。

证明: 取 $p=2$，则 $p\mid 2$，$p^2\nmid 2$，由 Eisenstein 判别法即得结论。 □

[1] 提示：反设 $x^{105}-9=fg$，则在 $\mathbb{C}$ 上有 $f=\prod_{k=1}^{s}(x-\sqrt[105]{9}e^{2m_k\pi i})$，$m_1,\ldots,m_s\in\{0,1,\ldots,104\}$，证明 $\|f(0)\|\notin\mathbb{Z}$ 即可。

例 6.2.8 设 $p \in \mathbb{Z}^+$ 是素数，求证 $f(x) = x^{p-1} + \cdots + x + 1$ 在 $\mathbb{Q}[x]$ 上不可约。

证明: 作变量替换 $x \mapsto x+1$(注意 $\mathbb{Q}[x] \to \mathbb{Q}[x]$, $x \mapsto x+1$ 是环同构)，则

$$\begin{aligned} h(x) = f(x+1) &= (x+1)^{p-1} + \cdots + (x+1) + 1 \\ &= \frac{(x+1)^p - 1}{(x+1) - 1} \quad \text{(形式计算，可省略)} \\ &= x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-2} x + \binom{p}{p-1} \end{aligned}$$

显然 f 不可约 $\iff$ h 不可约。由于 $p \mid \binom{p}{k}$ 对每个 $k \in \{1, 2, \ldots, p-1\}$ 都成立，但 $p^2 \nmid \binom{p}{p-1}$，故由 Eisenstein 判别法可知 h 不可约。这样我们就完成了证明。 □

6.2.5 有理函数的准素分解

最后我们简单讨论一下形如多项式的“比值”的表达式的化简。

在 §4.4 节中，我们已经讨论了如何从一个整环出发，通过局部化的方法得到其分式域。特别地，我们知道域 $\mathbb{F}$ 上的多项式环 $\mathbb{F}[x]$ 是整环，则可以构造 $\mathbb{F}[x]$ 的分式域

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

注意 $\mathbb{F}(x)$ 中的元素是等价类，并且可以将 $\mathbb{F}[x]$ 自然地嵌入到 $\mathbb{F}(x)$ 中。$\mathbb{F}(x)$ 上的加法和乘法的定义与性质已经在 §4.4 中讨论过了。我们把 $\mathbb{F}(x)$ 称为**有理函数域** (rational function field)，其中的元素称为 $\mathbb{F}$ 上的**有理函数**或有理分式。

定义 6.2.10 设 $\mathbb{F}$ 是域，$\frac{f}{g} \in \mathbb{F}[x]$，我们称 f 为分子，g 为分母，定义有理函数的次数 $\deg(\frac{f}{g}) = \deg(f) - \deg(g)$。这个定义是良定义的，因为如果 $\frac{f}{g} = \frac{f'}{g'}$，即 $fg' = f'g$，于是 $\deg(f) + \deg(g') = \deg(fg') = \deg(f'g) = \deg(f') + \deg(g)$，即 $\deg(f) - \deg(g) = \deg f' - \deg(g')$。如果 $\deg(\frac{f}{g}) < 0$，则称 $\frac{f}{g}$ 是真分式；如果 $\frac{f}{g}$ 中 $\gcd(f, g) = 1$，则称 $\frac{f}{g}$ 是既约分式。显然每个有理分式都会等价于一个既约分式，因此，下面我们提到的有理分式默认都是既约的。

对有理分式 $\frac{f}{g}$ 来说，如果 $\deg(f) \geqslant \deg(g)$，那么我们可以做带余除法 $f(x) = q(x)g(x) + r(x)$, $\deg(r) < \deg(g)$ 或 $r(x) = 0$，则

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

其中 $\frac{r(x)}{g(x)}$ 是真分式。由带余除法的唯一性可得该分解的唯一性。此外，我们称形如 $\frac{f(x)}{p(x)^n}$ (其中 $p(x) \in \mathbb{F}[x]$ 是不可约多项式，$\deg(f) < \deg(p)$) 的有理分式为最简分式。下面我们讨论如何将真分式写成最简分式的和。

引理 6.2.4 设 $p(x) \in \mathbb{F}[x]$ 是不可约多项式，则对 $\forall f(x) \in \mathbb{F}[x]$，存在唯一一组 $q_0(x), q_1(x), \ldots, q_k(x)$ 使得 $\forall i \in \{0, \ldots, k\}$, $\deg(q_i) < \deg(p)$ 并且

$$f(x) = \sum_{i=0}^{k} q_i(x)(p(x))^i.$$

证明: 如果 $\deg(f) < \deg(p)$，则直接取 $q_0 = f$ 即得结论；否则，我们可以反复做带余除法

$$\begin{aligned}
&f = h_1 p + q_0, && \deg(q_0) < \deg(p);\\
&h_1 = h_2 p + q_1, && \deg(q_1) < \deg(p);\\
&\cdots && \cdots\\
&h_{k-1}(x) = h_k p + q_{k-1}, && \deg(q_{k-1}) < \deg(p);\\
&h_k = q_k, && \deg(h_k) < \deg(p).
\end{aligned}$$

算法终止是因为 $\deg(f) \geqslant \deg(h_1) + \deg(p)$，$\deg(h_1) \geqslant \deg(h_2) + \deg(p), \cdots\cdots$，于是进行到某一步必然有 $\deg(h_k) < \deg(p)$，即算法终止。

将上面的式子从下向上依次代入即得 $f(x) = \sum_{i=0}^{k} q_i(x)(p(x))^i$。 □

现在我们可以对真分式进行分解了。

定理 6.2.8 *有理函数域 $\mathbb{F}(x)$ 中的每个真分式都可以分解成一些分母不同的最简分式的和，而且和式中的最简分式由原来的真分式唯一确定 (即不计加法次序下该分解唯一)。*

证明: 设 $\dfrac{f}{g} \in \mathbb{F}(x)$，$\deg(f) < \deg(g)$。显然我们可以将 $\mathrm{lc}(g)$ 放到分子上，即将 g 简化为首一多项式。下面我们分以下三步证明原命题。

(1) 如果 g 本身是不可约多项式的方幂，则直接进行第 (3) 步。反之，如果 $g(x) = g_1(x)g_2(x)$，其中 g_1, g_2 首一，互素且 $1 \leqslant \deg(g_i) < \deg(g)$，$\forall i = 1, 2$，则存在 $u_1(x), v_1(x) \in \mathbb{F}[x]$ 使得 $u_1 g_1 + v_1 g_2 = 1$，于是 $f(x) = u_1(x)g_1(x)f(x) + v_1(x)g_2(x)f(x)$，做带余除法

$$v_1(x)f(x) = u_2(x)g_1(x) + f_1(x), \quad \deg(f_1) < \deg(g_1)$$

再令 $f_2(x) = u_1(x)f(x) + u_2(x)g_2(x)$，则

$$\begin{aligned}
f(x) &= u_1(x)g_1(x)f(x) + v_1(x)g_2(x)f(x)\\
&= (u_1(x)f(x) + u_2(x)g_2(x))g_1(x) + f_1(x)g_2(x)\\
&= f_2(x)g_1(x) + f_1(x)g_2(x)
\end{aligned}$$

于是

$$\frac{f(x)}{g(x)} = \frac{f(x)}{g_1(x)g_2(x)} = \frac{f_2(x)}{g_2(x)} + \frac{f_1(x)}{g_1(x)}$$

此时，由于 $\deg(f) < \deg(g) = \deg(g_1) + \deg(g_2)$，利用 $f(x) = f_2(x)g_1(x) + f_1(x)g_2(x)$ 可得

$$\deg(f_2) + \deg(g_1) \leqslant \max\{\deg(f_2 g_1), \deg(f_1 g_2)\} = \deg(f) < \deg(g_1) + \deg(g_2)$$

即 $\deg(f_2) < \deg(g_2)$。这样我们就把 $\dfrac{f(x)}{g(x)}$ 分解成了两个真分式的和。

我们还需要证明 f_1, f_2 由 g_1, g_2 唯一确定。设另有 f_1', f_2' 也满足

$$\frac{f(x)}{g(x)} = \frac{f_2'(x)}{g_2(x)} + \frac{f_1'(x)}{g_1(x)}, \quad \deg(f_1') < \deg(g_1),\ \deg(f_2') < \deg(g_2)$$

则

$$\frac{f_2'(x)}{g_2(x)} + \frac{f_1'(x)}{g_1(x)} = \frac{f(x)}{g_1(x)g_2(x)} = \frac{f_2(x)}{g_2(x)} + \frac{f_1(x)}{g_1(x)}$$

通分整理即有

$$(f_2'(x) - f_2(x))g_1(x) = (f_1(x) - f_1'(x))g_2(x)$$

又因为 $\gcd(g_1, g_2) = 1$，所以 $g_1(x) \mid (f_1(x) - f_1'(x))$，然而由于

$$\deg(f_1 - f_1') \leqslant \max(\deg(f_1), \deg(f_1')) < \deg(g_1)$$

所以只能是 $f_1 - f_1' = 0$，即 $f_1(x) = f_1'(x)$。同理 $f_2(x) = f_2'(x)$，即 f_1, f_2 由 g_1, g_2 唯一确定。

(2) 设 $g(x)$ 有素因子分解 $g(x) = (p_1(x))^{n_1}(p_2(x))^{n_2}\cdots(p_s(x))^{n_s}$，其中 $p_i(x),\ i = 1, \ldots, s$ 是两两不同的首一的不可约多项式。则由 (1)，对 s 归纳即可得到

$$\begin{aligned}
\frac{f(x)}{g(x)} &= \frac{f_1(x)}{(p_1(x))^{n_1}} + \frac{h_1(x)}{(p_2(x))^{n_2}\cdots(p_s(x))^{n_s}} \\
&= \frac{f_1(x)}{(p_1(x))^{n_1}} + \frac{f_2(x)}{(p_2(x))^{n_2}} + \frac{h_2(x)}{(p_3(x))^{n_3}\cdots(p_s(x))^{n_s}} \\
&= \cdots \\
&= \frac{f_1(x)}{(p_1(x))^{n_1}} + \frac{f_2(x)}{(p_2(x))^{n_2}} + \cdots + \frac{f_s(x)}{(p_s(x))^{n_s}}
\end{aligned}$$

其中 $\deg(f_i) < \deg(p_i^{n_i})$。下面我们只需把形如 $\dfrac{f_i(x)}{(p_i(x))^{n_i}}$ 的分式分解成最简分式之和即可。

(3) 由引理 6.2.4，对 (2) 中的每个 $f_i(x)$，存在唯一一组 $q_{0i}(x), q_{1i}(x), \ldots, q_{n_i-1,i}(x)$ 使得 $f_i(x) = \sum_{j=0}^{n_i-1} q_{ji}(x)(p_i(x))^j$，其中 $\deg(q_{ji}) < \deg(p_i),\ j = 1, \ldots, n_i - 1$，于是

$$\frac{f_i(x)}{(p_i(x))^{n_i}} = \sum_{j=0}^{n_i-1} \frac{q_{ji}(x)}{(p_i(x))^{n_i-j}}.$$

所以

$$\frac{f(x)}{g(x)} = \sum_{i=1}^{s}\sum_{j=0}^{n_i-1} \frac{q_{ji}(x)}{(p_i(x))^{n_i-j}}.$$

上式右边的每一项都是最简分式，而且由 (1)(3) 两步的唯一性可知整个分解是唯一的。这样我们就完成了证明。 □

这个定理的证明过程实际上也给出了将真有理分式分解成最简分式的算法。此外，我们也可以用待定系数法来计算该分解，细节留给读者思考。准素分解在分析学中有很大的作用，它是计算有理函数的不定积分的重要工具。另外，由此出发我们可以建立起一套判定一个函数的积分是否是初等函数的理论 (类比 Galois 理论)，并由此得到 Γ 函数不是初等函数等有意义的结果。

6.3 多元多项式简介

6.3.1 定义与对称多项式

定义 6.3.1 设 R 是交换环，$x_1,\dots,x_n$ 是未定元，则我们称 $R[x_1][x_2]\cdots[x_n]$ 是 R 上的 n 元多项式环，记作 $R[x_1,\dots,x_n]$。

注 6.3.1 显然 $R[x_1,\dots,x_n]$ 是交换环。注意到 $R[x_1][x_2]$ 与 $R[x_2][x_1]$ 是同构的，因此 R 上的 n 元多项式环在同构意义下是唯一的。

定理 6.3.1 (1) 若 R 是整环，则 $R[x_1,\dots,x_n]$ 也是整环。
(2) 若 R 是唯一因子分解整环，则 $R[x_1,\dots,x_n]$ 也是唯一因子分解整环。

(1) 的证明是显然的，(2) 的证明我们放在习题课讲义中。

一个多元多项式可以整理成不同的形式。例如在 $\mathbb{Q}[x,y]$ 中

$$\begin{aligned} f &= (x^2+1)y^2+(x+1)y+x^5+2x \\ &= x^2y^2+y^2+xy+y+x^5+2x \\ &= x^5+y^2x^2+(y+2)x+y^2+y \end{aligned}$$

定义 6.3.2 设 $R[x_1,\dots,x_n]$ 是交换环 R 上的 n 元多项式环，令

$$X_n=\left\{x_1^{i_1}\cdots x_n^{i_n}\mid i_1,\dots,i_n\in\mathbb{N}\right\}\subset R[x_1,\dots,x_n]$$

则我们称 X_n 中的元素为单项式 (monomial)。

与单变元多项式相比，定义多元多项式的次数更复杂一些。

定义 6.3.3 设 $M=x_1^{i_1}\cdots x_n^{i_n}\in X_n$，我们称 $i_1+\cdots+i_n$ 为单项式 M 的全次数，记为 $\deg(M)$；相对应地我们称 i_k 为 M 关于变元 x_k 的次数，记作 $\deg_{x_k}(M)=i_k$。特别地，我们同样规定 $M\in R^*$ 的次数是 0，0_R 的次数是 $-\infty$。

显然，若 $M=x_1^{i_1}\cdots x_n^{i_n}$，$N=x_1^{j_1}\cdots x_n^{j_n}\in X_n$，则两个单项式的乘积 $MN=x_1^{i_1+j_1}\cdots x_n^{i_n+j_n}$，于是 $\deg(MN)=\deg(M)+\deg(N)$。

我们可以将多项式写成单项式的线性组合，即下面的命题。

命题 6.3.1 设 $f\in R[x_1,\dots,x_n]\setminus\{0\}$，则存在唯一一组两两不同的 $\alpha_1,\dots,\alpha_k\in R$ 及 $M_1,\dots,M_k\in X_n$ 使得 $f=\sum_{i=1}^k\alpha_iM_i$。此时我们称 α_i，$i\in\{1,\dots,k\}$ 是 M_i 的系数，称 f 的这个形式为分布式 (distributive form)。

利用多元多项式的定义即可证明。

定义 6.3.4 设 $f=\sum_{i=1}^k\alpha_iM_i$ 是分布式，则我们称 f 的全次数为 $\max\{\deg(M_1),\dots,\deg(M_k)\}$，记作 $\deg(f)$；称 f 关于变元 x_i 的次数为 $\max\{\deg_{x_i}(M_1),\dots,\deg_{x_i}(M_k)\}$。显然后者与将 f 视作关于 x_i 的单变元多项式时 x_i 的次数是一致的。

例如，设 $f=x^2y^2+y^2+xy+y+x^5+2x\in\mathbb{Q}[x,y]$，则 $\deg(f)=\deg_x(f)=5$，$\deg_y(f)=2$。

利用组合中的挡板法容易证明，X_n 中次数不超过 d 的单项式有 $\binom{n+d}{n}$ 个。

定义 6.3.5 设 $h=\sum_{i=1}^{k}\alpha_i M_i\in R[x_1,\dots,x_n]$ 是分布式，如果 $\forall i\in\{1,\dots,k\}$，$\deg(M_1)=\deg(M_2)=\cdots=\deg(M_k)=d$，则我们称 h 是 d 次的齐次多项式 (homogeneous polynomial)。特别地，0 是任意次的齐次多项式。

于是，若 $f\in R[x_1,\dots,x_n]$，$\deg(f)=d$，则 f 可以唯一的写成 $f=h_d+\cdots+h_0$，其中 h_i 是 i 次的齐次多项式。

定理 6.3.2 设 $p,q\in R[x_1,\dots,x_n]$，$\deg(p)=d$，$\deg(q)=e$，则 $\deg(p+q)\leqslant\max\{\deg(p),\deg(q)\}$，$\deg(pq)\leqslant\deg(p)+\deg(q)$。当 R 是整环时后者的等号成立。

类比于单变元多项式的赋值同态，我们有下面的定理。

定理 6.3.3 设 R,S 是交换环，$\varphi:R\to S$ 是环同态，则对任意的 $s_1,\dots s_n\in S$，存在唯一的环同态 $\varphi_{s_1,\dots,s_n}:R[x_1,\dots,x_n]\to S$ 使得 $\varphi_{s_1,\dots,s_n}\big|_R=\varphi$ 并且 $\forall i\in\{1,\dots,n\}$，有 $\varphi_{s_1,\dots,s_n}(x_i)=s_i$。

利用单变元情形时的赋值同态定理及数学归纳法即可证明，细节留作练习，或者参考 Algebra, Thomas W. Hungerford, GTM73 的 Chapter III, Theorem5.5。

特别地，如果 $\mathbb{F}$ 是域，则恒等映射 $\mathrm{id}:\mathbb{F}\to\mathbb{F}$ 诱导了 $\mathbb{F}[x_1,\dots,x_n]\to\mathbb{F}$ 上的通常的赋值 (“代入” 操作)。于是，设 $f\in\mathbb{F}[x_1,\dots,x_n]$，$a_1,\dots,a_n\in\mathbb{F}$，如果 $f(a_1,\dots,a_n)=0$，则我们称 $(a_1,\dots,a_n)$ 是 f 在 $\mathbb{F}$ 上的一个零点。

下面我们讨论在变元的置换下多元多项式的变化。

例 6.3.1 我们可以考虑嵌入 $\varphi:R\to R[x_1,\dots,x_n]$ 诱导的赋值同态。设 $\sigma\in S_n$，则由上面的定理可知，存在唯一的环同态 φ_σ 使得

$$\varphi_\sigma(x_i)=x_{\sigma(i)},\ \text{且}\varphi_\sigma\big|_R=\varphi$$

并且，容易证明 φ_σ 有逆映射 $\varphi_{\sigma^{-1}}$，且逆映射也是环同态。于是 φ_σ 是 $R[x_1,\dots,x_n]$ 上的自同构。

例如，在 $\mathbb{Q}[x_1,x_2,x_3]$ 上，取 $\sigma=(12)$，$f=x_1+2x_2^2-x_3$，则 $\varphi_\sigma(f)=x_2+2x_1^2-x_3$。

下面我们就可以定义对称多项式 (symmertric polynomial) 了。

定义 6.3.6 设 $p\in R[x_1,\dots,x_n]$，如果对任意 $\sigma\in S_n$，都有 $\varphi_\sigma(p)=p$，则称 p 是关于 $x_1,\dots,x_n$ 的 n 元对称多项式。容易证明所有的 n 元对称多项式构成 $R[x_1,\dots,x_n]$ 的子环。

下面我们考虑一类特殊的对称多项式，它们被称为初等对称多项式。设 $p=(x_{n+1}-x_1)(x_{n+1}-x_2)\cdots(x_{n+1}-x_n)\in R[x_1,\dots,x_n,x_{n+1}]$，我们也可以将 p 视作关于 x_{n+1} 的单变元多项式，这样 p 的系数就落在 $R[x_1,\dots,x_n]$ 中，即

$$p=x_{n+1}^n-s_1x_{n+1}^{n-1}+\cdots+(-1)^{n-1}s_{n-1}x_{n+1}+(-1)^n s_n,\ \text{其中}s_1,\dots,s_n\in R[x_1,\dots,x_n].$$

直接展开计算可得

$$\begin{aligned}
s_1&=x_1+x_2+\cdots+x_n\\
s_2&=x_1x_2+x_1x_3+\cdots\cdots+x_{n-1}x_n\\
&\cdots\cdots\\
s_k&=\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}x_{i_1}x_{i_2}\cdots x_{i_k}\\
&\cdots\cdots\\
s_n&=x_1x_2\cdots x_n.
\end{aligned}\tag{6.3.1}$$

容易验证上面的 s_k, $k = 1, \ldots, n$ 是 k 次的齐次对称多项式，称为 n 元 k 次初等对称多项式或基本对称多项式 (elementary symmertric polynomial)。利用上面的计算过程我们也可以得到单变元多项式根与系数的关系。

定理 6.3.4 (Vieta, **韦达定理**) 设 $\mathbb{F}$ 是域，$f(x) = a_0 + \cdots + a_n x^n \in \mathbb{F}[x]$，并且 f 在域 $\mathbb{K} \supset \mathbb{F}$ 上有 n 个根 (计重数)$\alpha_1, \ldots, \alpha_n$(允许重复)，则

$$\frac{a_i}{a_n} = (-1)^{n-i} s_{n-i}(\alpha_1, \ldots, \alpha_n)$$

其中 $s_{n-i} \in \mathbb{F}[y_1, \ldots, y_n]$ 是 $n-i$ 次的 n 元 $n-i$ 次初等对称多项式。

在 $p = (x_{n+1} - x_1)(x_{n+1} - x_2) \cdots (x_{n+1} - x_n)$ 中取 $x_{n+1} = x$, $\forall i = 1, \ldots, n$, $x_i = \alpha_i$，展开 p 并与 f 对比系数即可。细节留作练习。

特别地，当 $\deg(f) = 2$ 时，上面的定理就回到了我们中学学过的情形。

设 $p \in \mathbb{Z}^+$ 是素数，我们考虑 $\mathbb{Z}_p[x]$ 中的多项式 $f = x^{p-1} - \overline{1}$。显然 $\deg f = p - 1$ 并且 f 在 $\mathbb{Z}_p$ 上有 $p-1$ 个根 $\overline{1}, \overline{2}, \ldots, \overline{p-1}$，于是由韦达定理，$-\overline{1} = (-1)^{p-1} s_{p-1}(\overline{1}, \ldots, \overline{p-1})$，即 $\mathbb{Z}_p$ 中 $\overline{(p-1)!} = -\overline{1}$(分 $p = 2$ 和 $p \neq 2$ 讨论一下)，即 $(p-1)! + 1 \equiv 0 \mod p$。反之，如果 $p = p_1 p_2$, $1 < p_1, p_2 < p$，那么 $(p-1)! \equiv 0 \mod p_1$，于是 $(p-1)! + 1 \not\equiv 0 \mod p_1$，即 $(p-1)! + 1 \not\equiv 0 \mod p$。综上所述，我们有

定理 6.3.5 (Wilson) $p \in \mathbb{Z}^+$ 是素数 $\iff (p-1)! + 1 \equiv 0 \mod p$。

证明如前所述。

之所以我们把式 (6.3.1) 中的 s_k 称作“基本”对称多项式，是因为我们有下面的定理。

定理 6.3.6 (**对称多项式基本定理**) 设 R 是整环，$f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ 是对称多项式，则存在唯一的多项式 $g(y_1, \ldots, y_n) \in R[y_1, \ldots, y_n]$ 使得 $f(x_1, \ldots, x_n) = g(s_1, \ldots, s_n)$，其中 $s_1, \ldots, s_n$ 是 $R[x_1, \ldots, x_n]$ 上的初等对称多项式。而且，g 的系数是 f 系数的整数线性组合。

证明思路是将 f 按照 $x_1 > \cdots > x_n$ 的字典序排列，之后用 $s_1, \ldots, s_n$ 消去 f 的首项，归纳地做下去，利用字典序是良序保证有限步内算法停止。唯一性只需证明 $g(y_1, \ldots, y_n) \neq g'(y_1, \ldots, y_n) \Longrightarrow g(s_1, \ldots, s_n) \neq g'(s_1, \ldots, s_n)$，取 $g - g'$ 在字典序 $y_1 > \cdots > y_n$ 下的首项，利用反证法即可。细节参见代数学引论，以后补充。

对称多项式基本定理说明，对称多项式一定是初等对称多项式的多项式。在实际计算中，我们也常用待定系数法计算如何用初等对称多项式表出一般的对称多项式。

下面我们考虑一类特殊的对称多项式：幂和。我们称 $p_k(x_1, \ldots, x_n) = x_1^k + \cdots + x_n^k \in \mathbb{R}[x_1, \ldots, x_n]$ 为 k 次幂和，由对称多项式基本定理，p_k 一定可以用初等对称多项式 $s_1, \ldots, s_n$ 表出，那么，具体的表出形式是什么呢?

命题 6.3.2 (Newton **公式**) p_k, s_k 记号的意义如上，则

(1) 如果 $1 \leqslant k \leqslant n$，则 $p_k - p_{k-1} s_1 + \cdots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k = 0$;

(2) 如果 $k > n$，则 $p_k - p_{k-1} s_1 + \cdots + (-1)^{n-1} p_{k-n+1} s_{n-1} + (-1)^n p_{k-n} s_n = 0$。

证明: 用数学归纳法可以直接证明该定理。这里我们给出一个更巧妙的方法。

令 $\lambda(t) = (1 + x_1 t)(1 + x_2 t) \cdots (1 + x_n t)$，对 $\lambda(t)$ 按 t 展开，则由初等对称多项式的定义 (或韦达定理) 可知 $\lambda(t) = 1 + s_1 t + \cdots + s_n t^n$，那么

$$\frac{\mathrm{d} \ln(\lambda(t))}{\mathrm{d}t} = \frac{s_1 + 2 s_2 t + \cdots + n s_n t^{n-1}}{1 + s_1 t + \cdots + s_n t^n}. \tag{6.3.2}$$

另一方面，对 $\ln(\lambda(t))$ 不展开直接求导可得

$$\frac{\mathrm{d}\ln(\lambda(t))}{\mathrm{d}t} = \frac{x_1}{1+x_1t} + \frac{x_2}{1+x_2t} + \cdots + \frac{x_n}{1+x_nt}.$$

利用习题课关于形式幂级数的结论 $(1+x)^{-1} = 1 - x + x^2 - \cdots + (-1)^k x^k + \cdots$ 可知

$$\begin{aligned}\frac{\mathrm{d}\ln(\lambda(t))}{\mathrm{d}t} &= x_1(1 - x_1t + x_1^2t^2 - \cdots) + x_2(1 - x_2t + x_2^2t^2 - \cdots) + \cdots + x_n(1 - x_nt + x_n^2t^2 - \cdots) \\ &= p_1 - p_2t + p_3t^2 - \cdots + (-1)^k p_{k+1}t^k + \cdots\end{aligned} \tag{6.3.3}$$

对比式 (6.3.2) 和 (6.3.3) 可知

$$s_1 + 2s_2t + \cdots + ns_nt^{n-1} = (1 + s_1t + \cdots + s_nt^n)(p_1 - p_2t + p_3t^2 - \cdots + (-1)^k p_{k+1}t^k + \cdots)$$

展开上式右边并依次与左边对比 $t^i, i = 0, 1, \cdots, n-1, \cdots$ 的系数即可得到定理的结论。 □

6.3.2 判别式与结式

我们看到韦达定理是用对称多项式表示单变元多项式的根与系数的关系。那么，单变元多项式是否有重根这一问题应该如何判定呢？这就需要我们下面讨论的判别式 (discriminant)。

定义 6.3.7 设 $\mathbb{F}$ 是域并且 $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x]$ 在 $\mathbb{F}$ 上有 n 个根 $x_1, \cdots, x_n$(计重数)，我们定义

$$D(f) = a_n^{2n-2} \prod_{1 \leqslant j < i \leqslant n} (x_i - x_j)^2$$

称 $D(f)$ 为多项式 f 的判别式。

之所以我们要这样定义判别式，首先基于这样的观察：f 有重根 $\iff D(f) = 0$。注意到 $D(f)$ 是关于 $x_1, \cdots, x_n$ 的对称多项式，因此它一定可以用初等对称多项式表出。$D(f)$ 前面的系数 a_n^{2n-2} 不是本质的，取这个系数的目的是和后面的结式对应起来。下面我们讨论如何将 $D(f)$ 用根的初等对称多项式表出，进而由韦达定理，将 $D(f)$ 用 f 的系数表出。

首先，注意到

$$\prod_{1 \leqslant j < i \leqslant n} (x_i - x_j) = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1} \end{vmatrix},$$

于是

$$
\begin{aligned}
D(f) &= a_n^{2n-2}\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}^2 \\
&= a_n^{2n-2}\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} \\
&= a_n^{2n-2}\begin{vmatrix} n & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ p_2 & p_3 & p_4 & \cdots & p_{n+1} \\ \vdots & \vdots & \vdots & & \vdots \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{vmatrix}
\end{aligned}
$$

由 Newton 公式，p_i 可以用 s_i(即 $(-1)^i\dfrac{a_{n-i}}{a_n}$) 表示出来，这样我们就可以用 f 的系数表示 $D(f)$ 了。当然在 $\deg(f)$ 比较小时，我们也可以直接用待定系数法计算。后面学完结式以后我们会有更简单的计算方法。

特别地，如果 $f = x^2 - bx + c \in \mathbb{C}[x]$ 在 $\mathbb{C}$ 上有根 x_1, x_2，则 $s_1(x_1, x_2) = b$，$s_2(x_1, x_2) = c$，而

$$
D(f) = \begin{vmatrix} 2 & p_1 \\ p_1 & p_2 \end{vmatrix} = \begin{vmatrix} 2 & s_1 \\ s_1 & s_1^2 - 2s_2 \end{vmatrix} = s_1^2 - 4s_2.
$$

即 $D(f) = b^2 - 4c$。这与我们中学时学过的一元二次方程的判别式是一致的。

下面我们来定义两个多项式的 Sylvester 结式，结式也是通过研究多项式的最大公因子得到的。

定义 6.3.8 设 $\mathbb{F}$ 是域，$f = a_0 + a_1x + \cdots + a_nx^n$，$g = b_0 + b_1x + \cdots + b_mx^m \in \mathbb{F}[x]$，$a_n, b_m \neq 0$，我们称下面的行列式

$$
\begin{vmatrix}
a_n & a_{n-1} & \cdots & a_0 & & & \\
 & a_n & \cdots & a_1 & a_0 & & \\
 & & \ddots & & \ddots & \ddots & \\
 & & & a_n & \cdots & a_1 & a_0 \\
b_m & \cdots & b_0 & & & & \\
 & b_m & \cdots & b_0 & & & \\
 & & b_m & \cdots & b_0 & & \\
 & & & \ddots & & \ddots & \\
 & & & & b_m & \cdots & b_0
\end{vmatrix}
\begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}\text{m 行} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}\text{n 行} \end{matrix}
\qquad (\text{空白部分为 } 0)
$$

为 f 和 g 的 Sylvester 结式 (Sylvester Resultant)，记作 $\mathrm{Res}_x(f, g)$ 或简记为 $\mathrm{Res}(f, g)$ (称对应

的矩阵为 Sylvester 矩阵)。特别地，如果 $f = a_0 \in \mathbb{F}$，则 $\mathrm{Res}(f,g) = a_0^m$；如果 $g = b_0 \in \mathbb{F}$，则 $\mathrm{Res}(f,g) = b_0^n$；如果 f,g 都在 $\mathbb{F}\setminus\{0\}$ 中，则 $\mathrm{Res}(f,g) = 1$，如果 $f = g = 0$，则 $\mathrm{Res}(f,g) = 0$。

引理 6.3.1 设 $\mathbb{F}$ 是域，$f,g \in \mathbb{F}[x]\setminus\mathbb{F}$，则存在非零多项式 $u(x),v(x) \in \mathbb{F}[x]$ 使得 $uf+vg = \mathrm{Res}(f,g)$，并且 $\deg(u) < \deg(g)$，$\deg(v) < \deg(f)$。

证明: 对 f,g 的 Sylvester 矩阵 S 作如下的初等列变换：对 $i \in \{1,2,\ldots,m+n-1\}$，将 S 的第 i 列乘以 x^{m+n-i} 后加到最后一列，得到矩阵 S'：

$$S' = \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & & & x^{m-1}f \\ & a_n & \cdots & a_1 & a_0 & & x^{m-2}f \\ & & \ddots & & \ddots & \ddots & \vdots \\ & & & a_n & \cdots & a_1 & f \\ b_m & \cdots & b_0 & & & & x^{n-1}g \\ & b_m & \cdots & b_0 & & & x^{n-2}g \\ & & b_m & \cdots & b_0 & & x^{n-3}g \\ & & & \ddots & & \ddots & \vdots \\ & & & & b_m & \cdots & g \end{pmatrix}$$

则 $\det(S') = \det(S)$。将 $\det(S')$ 按最后一列展开，再分别按含有 f 和 g 合并同类项，即得存在 $u,v \in \mathbb{F}[x]$ 使得 $\mathrm{Res}(f,g) = \det(S') = u(x)f(x) + v(x)g(x)$。而次数关系可以直接由行列式展开时最后一列关于 x 的次数得到。

下面我们证明 u,v 均不是 0。当 $\mathrm{Res}(f,g) \neq 0$ 时结论显然。如果 $\mathrm{Res}(f,g) = 0$，则我们不妨设 $u(x) = u_{m-1}x^{m-1} + \cdots + u_0$，$v(x) = v_{n-1}x^{n-1} + \cdots + v_0$，则将 $\mathrm{Res}(f,g) = \det(S') = u(x)f(x)+v(x)g(x)$ 的右边展开并对比系数可知 $u_{m-1},\ldots,u_0,v_{m-1},\ldots,v_0$ 满足

$$(u_{m-1},\ldots,u_0,v_{m-1},\ldots,v_0)\begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & & & \\ & a_n & \cdots & a_1 & a_0 & & \\ & & \ddots & & \ddots & \ddots & \\ & & & a_n & \cdots & a_1 & a_0 \\ b_m & \cdots & b_0 & & & & \\ & b_m & \cdots & b_0 & & & \\ & & b_m & \cdots & b_0 & & \\ & & & \ddots & & \ddots & \\ & & & & b_m & \cdots & b_0 \end{pmatrix} = (0,\ldots,0,0,\ldots,0)$$

由 $\mathrm{Res}(f,g) = 0$ 可知这个关于 $u_{m-1},\ldots,u_0,v_{m-1},\ldots,v_0$ 的方程组有非零解，即 u,v 均不为 0(注意此时 u,v 有一个是 0 即可得到 $u = v = 0$)。这样我们就完成了证明。 □

定理 6.3.7 设 $\mathbb{F}$ 是域，$f,g \in \mathbb{F}[x]$，则 $\mathrm{Res}(f,g) = 0 \iff f = g = 0$ 或者 $\deg(\gcd(f,g)) > 0$。

证明: ($\Longleftarrow$) 用反证法。如果 $\mathrm{Res}(f,g) \neq 0$，由上面的引理，必有 $\gcd(f,g) \mid \mathrm{Res}(f,g)$，而 $\mathrm{Res}(f,g) \in \mathbb{F}$ 是常数，故 $\gcd(f,g)$ 与 1 相伴，即 $\deg(\gcd(f,g)) = 0$，矛盾!

($\Longrightarrow$) 如果 $\mathrm{Res}(f,g) = 0$，则 $f = g = 0$ 的情形显然，下设 f,g 不同时为 0。不妨设 $f \neq 0$，则由上面的引理，$\exists u(x),v(x) \in \mathbb{F}[x]$ 使得 $u(x)f(x) = -v(x)g(x)$，如果 $\deg(\gcd(f,g)) = 0$，即 f 和 g 互素，那么 $f(x) \mid v(x)$，这与 $\deg(v) < \deg(f)$ 矛盾! □

下面我们考虑结式和判别式之间的联系。为此我们需要下面的命题。

命题 6.3.3 设 $\mathbb{F}$ 是域，$f,g\in\mathbb{F}[x]$ 并且在 $\mathbb{F}[x]$ 中可以分解成一次因子的乘积：

$$f(x)=a_n(x-\alpha_1)\cdots(x-\alpha_n)$$
$$g(x)=b_m(x-\beta_1)\cdots(x-\beta_m)$$

那么

$$\mathrm{Res}(f,g)=a_n^m\prod_{i=1}^n g(\alpha_i)=b_m^n\prod_{j=1}^m f(\beta_j)=a_n^m b_m^n\prod_{i=1}^n\prod_{j=1}^m(\alpha_i-\beta_j).$$

证明: 首先，由结式的定义容易验证 $\mathrm{Res}(f,g)=(-1)^{mn}\mathrm{Res}(g,f)$，因此我们只需证明 $\mathrm{Res}(f,g)=a_n^m\prod_{i=1}^n g(\alpha_i)$ 即可。引入一个新的参变元 y，考虑 $\mathrm{Res}_x(f,g-y)$ (即将 g 的常数项 b_0 换成 b_0-y)。由结式的定义可知 $\mathrm{Res}_x(f,g-y)$ 是一个关于 y 的 n 次多项式，并且其关于 y 的常数项恰为 $\mathrm{Res}(f,g)$。注意到 $\mathrm{Res}_x(f,g-y)$ 关于 y^n 的系数为 $(-1)^n a_n^m$，即

$$\mathrm{Res}_x(f,g-y)=(-1)^n a_n^m y^n+\cdots+\mathrm{Res}(f,g)$$

由于 $\forall i\in\{1,\ldots,n\}$, $f(\alpha_i)=g(\alpha_i)-g(\alpha_i)=0$，即 $x-\alpha_i\mid f$, $x-\alpha_i\mid g(x)-g(\alpha_i)$，所以

$$\mathrm{Res}_x(f(x),g(x)-g(\alpha_i))=0.$$

那么反过来，关于 y 的多项式 $\mathrm{Res}_x(f,g-y)$ 有根 $y=g(\alpha_i)$，即 $\forall i\in\{1,\ldots,n\}$, $g(\alpha_i)-y\mid\mathrm{Res}_x(f,g-y)$。于是取遍 $i=1,\ldots,n$ 并对比首项系数和次数就有

$$\mathrm{Res}_x(f,g-y)=a_n^m\prod_{i=1}^n(g(\alpha_i)-y)$$

在上式中令 $y=0$，即得 $\mathrm{Res}(f,g)=a_n^m\prod_{i=1}^n g(\alpha_i)$。这样我们就完成了证明。 □

命题 6.3.4 设 $f\in\mathbb{F}[x]$, $\deg(f)=n$, $\mathrm{lc}(f)=a_n$，则

$$D(f)=(-1)^{\frac{n(n-1)}{2}}a_n^{-1}\mathrm{Res}(f,f').$$

证明: 不妨设 f 在 $\mathbb{F}$ 上恰有 n 个根 $\alpha_1,\ldots,\alpha_n$(计重数) [1]，由上面的命题立刻有

$$\mathrm{Res}(f,f')=a_n^{n-1}\prod_{i=1}^n f'(\alpha_i).$$

对 $f=a_n(x-\alpha_1)\cdots(x-\alpha_n)$ 求导数得

$$f'(x)=a_n\sum_{i=1}^n\prod_{j\neq i}(x-\alpha_j).$$

以 $x=\alpha_i$ 代入上式得

$$f'(\alpha_i)=a_n\prod_{j\neq i}(\alpha_i-\alpha_j).$$

于是

$$\begin{aligned}\mathrm{Res}(f,f')&=a_n^{2n-1}\prod_{i=1}^n\prod_{j\neq i}(\alpha_i-\alpha_j)\\&=a_n^{-1}(-1)^{\frac{n(n-1)}{2}}a_n^{2n-2}\prod_{j<i}(\alpha_i-\alpha_j)^2\\&=a_n^{-1}(-1)^{\frac{n(n-1)}{2}}D(f).\end{aligned}$$

这样我们就完成了证明。 □

[1] 任何一个域的代数闭包都存在，我们会在抽象代数课程中证明这一点。

例 6.3.2 分别计算 $\mathbb{Q}[x]$ 中多项式 $f(x)=x^2+bx+c$ 和 $g(x)=x^3+px+q$ 的判别式。

解: $(1)D(f)=-\mathrm{Res}(f,f')=\begin{vmatrix}1&b&c\\2&b&0\\0&2&b\end{vmatrix}=b^2-4c;$

$$(2)D(g)=-\mathrm{Res}(g,g')=\begin{vmatrix}1&0&p&q&\\&1&0&p&q\\3&0&p&&\\&3&0&p&\\&&3&0&p\end{vmatrix}=-4p^3-27q^2.$$

最后我们证明下面的结论。

命题 6.3.5 f,g 的条件同定义 6.3.8，则 $\mathrm{Res}(f,g)$ 是关于 $a_n,\ldots,a_0,b_m,\ldots,b_0$ 的不可约多项式 (将系数视作符号)。

证明: 用反证法。容易验证 $\mathrm{Res}(f,g)$ 分别是关于 f,g 的根 $\alpha_1,\ldots,\alpha_n$ 和 $\beta_1,\ldots,\beta_m$ 的对称多项式，若其可约，则可设 $\mathrm{Res}(f,g)=AB$，其中 A,B 都是关于 $\alpha_1,\ldots,\alpha_n$ 和 $\beta_1,\ldots,\beta_m$ 的正次数对称多项式 (思考之)。由命题 6.3.3，$\alpha_1-\beta_1\mid\mathrm{Res}(f,g)$，则 $\alpha_1-\beta_1\mid AB$，不妨设 $\alpha_1-\beta_1\mid A$，则由 A 是对称多项式，可知 $\forall i,j$，有 $\alpha_i-\beta_j\mid A$，于是 $\prod_{i,j}(\alpha_i-\beta_j)\mid A$。这说明 $B\mid a_n^m b_m^n$，于是 $B=\lambda a_n^p b_m^q$，$0\leqslant p\leqslant m$，$0\leqslant q\leqslant n$，$\lambda\neq 0$。但容易验证 $a_n\nmid\mathrm{Res}(f,g)$，$b_m\nmid\mathrm{Res}(f,g)$，于是 $p=q=0$，这与 B 是正次数的相矛盾! □

有关结式的更多内容，可以参考 Using Algebraic Geometry, David A.Cox, e.t.c., GTM185 的 Chapter 3。

6.4 实根隔离与近似求根简介

6.4.1 实根隔离

这一小节我们简单地讨论一下实系数多项式 $f(x)$ 在闭区间 $[a,b]$ 内有多少个根的问题。

我们首先需要有限实数序列的变号数这一概念。设一个有限的实数序列为 $S=\{c_1,\ldots,c_m\}$，记 V_S 为使 $c_ic_{i+1}<0$, $i\in 1,\ldots,m-1$ 的 i 的个数，并称 V_S 为序列 S 的变号数。如果序列 S 中含有 0，则 S 的变号数等于将 S 中的 0 都去掉后所得序列的变号数。例如，序列 $\{1,0,-1,1,-1\}$ 的变号数为 3。

下面我们回到本节一开始的问题。不失一般性，我们可以设 $f\in\mathbb{R}[x]$ 是无平方的 (否则取 f 的无平方部分即可)。我们直接给出以下定义。

定义 6.4.1 给定非零实系数多项式 $f(x)$ 和闭区间 $[a,b]$，称多项式序列

$$f_0(x)=f(x),f_1(x),\cdots,f_s(x)$$

是多项式 $f(x)$ 在闭区间 $[a,b]$ 上的 Sturm 序列，如果这些多项式都是实系数多项式且以下条件成立:

(1) 最后一个多项式 $f_s(x)$ 在 $[a,b]$ 上没有根;

(2) $f(a)f(b)\neq 0$;

(3) 对 $c\in[a,b]$ 和 $1\leqslant k\leqslant s-1$，若 $f_k(c)=0$，则 $f_{k-1}(c)f_{k+1}(c)<0$;

(4) 对 $c\in[a,b]$，若 $f(c)=0$，则 $(f_0(x)f_1(x))'\big|_{x=c}>0$。

由条件 (3) 知 Sturm 序列中相邻的多项式在 $[a,b]$ 上没有公共根。对 $c\in[a,b]$，序列 $f_0(c),f_1(c),\cdots,f_s(c)$ 的变号数记作 V_c 或 $V_c(f)$，即

$$V_c=V_c(f)=V(\{f_0(c),f_1(c),\cdots,f_s(c)\}).$$

我们有以下定理。

定理 6.4.1 (Sturm) 设 $f_0=f,f_1,\ldots,f_s$ 是正次数多项式 $f(x)\in\mathbb{R}[x]$ 在闭区间 $[a,b]$ 上的一个 Sturm 序列，则 f 在开区间 (a,b) 内的不同实根的个数 (不计重数) 为 Sturm 序列在 a,b 两点处的变号数之差，即 V_a-V_b。

证明从略。

那么,Sturm 序列具体应该如何构造呢?可以证明 (过程从略) 以下的序列 $f_0(x)=f(x),f_1(x),\cdots,f_s(x)$ 是 Sturm 序列:

$$\begin{aligned}
f_0(x)&=f(x)\\
f_1(x)&=f'(x)\\
f_2(x)&=-\mathrm{rem}(f_0,f_1)\\
f_3(x)&=-\mathrm{rem}(f_1,f_2)\\
&\cdots\cdots\\
f_s(x)&=-\mathrm{rem}(f_{s-2},f_{s-1})\neq 0\\
&\quad(\mathrm{rem}(f_{s-1},f_s)=0)
\end{aligned}$$

以上的序列称为标准 Sturm 序列。

例 6.4.1 设 $f(x)=x^4-2x^2-3x+3$，求 f 的实根个数。

解: f 在闭区间 $[-M,M](M>0$ 充分大) 上的标准 Sturm 序列为

$$\begin{aligned} f_0 &= f \\ f_1 &= 4x^3-4x-3 \\ f_2 &= x^2+\frac{9}{4}x-3 \\ f_3 &= -\frac{113}{4}x+30 \\ f_4 &= -\frac{6603}{113^2} \end{aligned}$$

于是 Sturm 序列在 $x=-M,\ x=M$ 处的符号如下表:

	f_0	f_1	f_2	f_3	f_4
$x=-M$	+	-	+	+	-
$x=M$	+	+	+	-	-

从而 $V_{-M}=3,\ V_M=1$，于是 f 只有两个不同的实根。

我们还有以下的结论。

定理 6.4.2 (Descartes) 设 $f\in\mathbb{R}[x]$，则 f 的正根个数 (计重数) 不超过其系数序列的变号数，且两者有相同的奇偶性。如果 f 没有虚根，则两者相等。

证明从略。

6.4.2 根的近似求解

我们中学时就已经接触过用二分法近似地求解一个多项式的根，在数学分析课程中又证明了其收敛性。那么，是否有更快速的近似解算法呢？本小节介绍的牛顿法就是一个更快的算法。

如果我们已知多项式 f 在 $x=c$ 附近有根，那么，我们令

$$c_0=c,\ c_{k+1}=c_k-\frac{f(c_k)}{f'(c_k)},\ k=0,1,2,\ldots$$

如果序列 $\{c_k\}$ 收敛到 a，则 $f(a)=0$。因此我们可以通过以上的迭代公式，计算某个 $c_n(n$ 足够大) 使得 $|c_n-a|$ 满足我们所需要的精度要求，即我们把 c_n 当作 $f(x)=0$ 的近似解。这种做法称为牛顿迭代法，其几何意义是不断作函数的切线与 x 轴的交点会越来越接近函数的零点。需要注意的是牛顿迭代并不总是收敛的，关于牛顿法的收敛性判别与收敛速度的分析，读者可以在一般的数值分析教材中找到。

6.5 代数基本定理

定义 6.5.1 (**代数基本定理**) 任何正次数的复系数多项式都至少有一个复数根。

证明从略。代数基本定理至今尚没有纯代数的证明，最简单的证明是利用复分析中的刘维尔定理 (有界整函数必为常数) 给出的，《代数学引论》给出的则是一个常见的应用代数知识稍多的证明。

推论 6.5.1 设 $f \in \mathbb{C}[x]$，$\deg(f) = n > 0$，则 f 在 $\mathbb{C}$ 上有且只有 n 个根 (计重数)。

对 n 归纳即可证明。

下面我们列举一些关于实系数多项式的结论，利用代数基本定理可以很快证明它们。

定理 6.5.1 设 $f \in \mathbb{R}[x]$，$c \in \mathbb{C}$ 是 f 的根，则 $\overline{c}$ 也是 f 的根，并且 $\overline{c}$ 的重数与 c 的重数相同。

推论 6.5.2 (1) 实系数不可约多项式的次数不超过 2；
(2) 设 $f \in \mathbb{R}[x]$，$\deg(f) = 2$，则 f 在 $\mathbb{R}[x]$ 中不可约 $\iff D(f) < 0$。
(3)$\mathbb{R}[x]$ 中的每个正次数多项式都可以分解成一些一次和二次实系数多项式的乘积。

证明留作练习。

讲义上册到此完成。