§2 多项式II:因式分解

2.1 互素

定义：设$f(x),g(x)\in\mathbb{F}[x]$满足$(f(x),g(x))=1$, 则称$f(x)$与$g(x)$互素。

判别法：

定理 设$f(x),g(x)\in\mathbb{F}[x]$, 则$f(x)$与$g(x)$互素当且仅当存在$u(x),v(x)\in\mathbb{F}[x]$, 使得

$$u(x)f(x)+v(x)g(x)=1.$$

证明：若$f(x)$与$g(x)$互素,即它们的首项系数为1的最大公因式=1，则应用最大公因式的Bezout等式即可。反之，若以上等式成立，则$f(x)$与$g(x)$的任意公因式整除1，即公因式是非零常数，因此$(f(x),g(x))=1$.

注：设$f(x),g(x)\in\mathbb{F}[x]$满足$(f(x),g(x))=1$，设$\mathbb{K}$是包含$\mathbb{F}$的数域，则$f(x),g(x)\in\mathbb{K}[x]$且$f(x)$与$g(x)$在$\mathbb{K}$上互素。因此，互素是和数域无关的。

2.1 互素

推论1：若$f_1(x) \mid g(x)$，$f_2(x) \mid g(x)$且 $(f_1(x), f_2(x)) = 1$，则$f_1(x)f_2(x) \mid g(x)$.

推论2：设$(f(x), g(x)) = 1$，且$f(x) \mid g(x)h(x)$，则$f(x) \mid h(x)$.

推论3：设$(f(x), g(x)) = d(x)$，$f(x) = f_1(x)d(x), g(x) = g_1(x)d(x)$,则$(f_1(x), g_1(x)) = 1$.

推论4：设$(f(x), g(x)) = d(x)$，则$(t(x)f(x), t(x)g_1(x)) = t(x)d(x)$.

推论5：设$(f_1(x), g(x)) = 1$，$(f_2(x), g(x)) = 1$,则$(f_1(x)f_2(x), g(x)) = 1$.

2.1 互素

例题 设$f(x), g(x) \in \mathbb{F}[x]$互素. 证明：对任意$h(x) \in \mathbb{F}[x]$, 都有 $(f(x)h(x), g(x)) = (h(x), g(x))$.

证明：应用推论4， $(f(x)h(x), g(x)) \mid (f(x)h(x), g(x)h(x)) = h(x)$. 由定义$(f(x)h(x), g(x)) \mid g(x)$. 因此， $(f(x)h(x), g(x)) \mid (h(x), g(x))$. 反之， 显然有$(h(x), g(x)) \mid (f(x)h(x), g(x))$.

2.2 因式分解

定义：设$f(x)\in\mathbb{F}[x]$，$\deg f(x)\geq 1$. 若$f(x)$不能写成$\mathbb{F}[x]$中两个次数小于$f(x)$的多项式乘积，则称$f(x)$在数域$\mathbb{F}$上不可约或$f(x)$是$\mathbb{F}[x]$中的不可约多项式.

例如： x^4+2在$\mathbb{Q}$上不可约，在$\mathbb{R}$上可约.

注：不可约多项式的地位正如素数在整数中的地位.

性质：1.设$f(x)\in\mathbb{F}[x]$不可约，则$cf(x)$也不可约，其中$c\in\mathbb{F}$.

2.设$\mathbb{F}_1\subseteq\mathbb{F}_2$是两个数域， $f(x)\in\mathbb{F}_1[x]$， 若$f(x)$在$\mathbb{F}_2$上不可约，则它在$\mathbb{F}_1$上不可约.

3.设$f(x)\in\mathbb{F}[x]$不可约,$g(x),h(x)\in\mathbb{F}[x]$且$f(x)\mid g(x)h(x)$，则$f(x)\mid g(x)$或$f(x)\mid h(x)$.

4.设$f(x)\in\mathbb{F}[x]$不可约, $g(x)\in\mathbb{F}[x]$, 则$(f(x),g(x))=1$或$f(x)\mid g(x)$.

2.2 因式分解

定理：设$f(x)\in\mathbb{F}[x]$,次数≥ 1, 则

(1)$f(x)$可以分解为$\mathbb{F}[x]$上有限个不可约多项式的乘积；（因式分解的存在性）

(2)若$f(x)=p_1(x)p_2(x)\cdots p_s(x)=q_1(x)q_2(x)\cdots q_t(x)$是$f(x)$的两个不可约分解，即$p_i(x),q_j(x)$是$\mathbb{F}$上不可约多项式，其中$i=1,\cdots,s,j=1,\cdots,t$, 则$s=t$, 且经过调换因式次序，有$p_i(x)=c_iq_i(x)$, $c_i\neq 0\in\mathbb{F}$.（因式分解的唯一性）

推论：设$f(x)\in\mathbb{F}[x]$，则$f(x)=cp_1^{e_1}(x)\cdots p_s^{e_s}(x)$, 其中$c\in\mathbb{F}$,$s\geq 1,e_1,\cdots,e_s\geq 1$，$p_i(x)$是$\mathbb{F}$上不可约多项式.

应用：设$f(x)=c_1p_1^{e_1}(x)\cdots p_t^{e_t}(x),g(x)=c_2p_1^{f_1}(x)\cdots p_t^{f_t}(x)$, 其中$e_i\geq 0,f_i\geq 0,i=1,\cdots,t$. 则$f(x),g(x)$的最大公因式 是$cp_1^{k_1}(x)\cdots p_t^{k_t}(x)$, 其中$k_i=\min\{e_i,f_i\}$, $i=1,\cdots,t$.

问题：求$\mathbb{F}[x]$上的全部不可约多项式？

2.3 复系数多项式的因式分解

目标：刻画$\mathbb{C}[x]$上的不可约多项式。

定理（代数基本定理）：每个次数大于等于1的复系数多项式在复数域中至少有一个零点.

推论：每个次数等于n（$n \geq 1$）的复系数多项式在复数域中有n个零点（包括重根）.
因为若$f(x) \in \mathbb{C}[x]$, $\deg f(x) = n \geq 1$, 则存在$a_1 \in \mathbb{C}$, $f(a_1) = 0$. 由上一节零点定理$f(x) = (x - a_1)f_1(x)$. 对$f_1(x)$重复使用代数基本定理.

推论：$\mathbb{C}[x]$中的不可约多项式是一次多项式.

推论（$\mathbb{C}[x]$中的因式分解）：设$f(x) \in \mathbb{C}[x]$, $\deg f(x) = n \geq 1$, 则

$$f(x) = c(x - a_1)^{n_1}(x - a_2)^{n_2} \cdots (x - a_s)^{n_s},$$

其中$c \in \mathbb{C}$, $a_1, a_2, \cdots, a_s \in \mathbb{C}$互不相同，$n_1, \cdots, n_s$均大于等于1,且$n_1 + \cdots + n_s = n$. .

2.4 实系数多项式的因式分解

目标：刻画$\mathbb{R}[x]$上的不可约多项式。

定理：设$f(x)\in\mathbb{R}[x]$, 若$a+bi(b\neq 0)$是它的根，则$a-bi$也是它的根.

因为$f(a-bi)=\overline{f(a+bi)}=0.$

推论：$\mathbb{R}[x]$中的不可约多项式是一次多项式或二次多项式.

原因：设$f(x)\in\mathbb{R}[x]$是次数大于1的不可约多项式，则由代数基本定理, $f(x)$有一个复根$z=a+bi(b\neq 0)$, 因此，$a-bi$也是它的根。从而$(x-z)(x-\overline{z})=x^2-2ax+(a^2+b^2)\mid f(x)$. 但是$f(x)$不可约，所以$f(x)=cx^2-2ax+(a^2+b^2), c\in\mathbb{R}$.

推论（$\mathbb{R}[x]$中的因式分解）：设$f(x)\in\mathbb{R}[x]$, $\deg f(x)=n\geq 1$, 则 $f(x)$是有限个一次多项式或二次不可约多项式的乘积.

例题：1.奇数次实系数多项式必有一个实根.

2. x^4+2在实数域上是可约多项式.

2.5 有理系数多项式的有理根

目标：刻画$\mathbb{Q}[x]$上的多项式的有理根。

设$f(x) \in \mathbb{Q}[x]$, 则存在$m \in \mathbb{Z}$, $mf(x) \in \mathbb{Z}[x]$.

定理：设$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$,若$f(\frac{q}{p}) = 0$, 其中$p, q$是互素的整数，则$p \mid a_n, q \mid a_0$.

例题：证明$f(x) = x^5 - 12x^3 + 36x + 12$无有理根.

注：$f(x) = 0$无有理根并不说明$f(x)$在$\mathbb{Q}$上不可约，例如$f(x) = (x^2+1)^2$.

2.6 Vieta定理

定理：若数域$\mathbb{F}$上的一元多项式$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$在$\mathbb{F}$中有$n$个零点$x_1, \cdots, x_n$(可能有重复)，则

$$\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n = -\frac{a_{n-1}}{a_n},$$

$$\sum_{1\le i<j\le n} x_i x_j = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \frac{a_{n-2}}{a_n}$$

$$\sum_{1\le i<j<k\le n} x_i x_j x_k = x_1x_2x_3 + \cdots + x_{n-2}x_{n-1}x_n = -\frac{a_{n-3}}{a_n}$$

$$\cdots\cdots\cdots$$

$$x_1x_2\cdots x_n = (-1)^n\frac{a_0}{a_n}.$$

2.6 Vieta定理

例题：设n阶方阵A的特征多项式是$f(\lambda) = \lambda^n + a_1\lambda^{n-1} + a_2\lambda^{n-2} + \cdots + a_n$. 且由行列式性质知 a_r等于$(-1)^r$乘以A的所有r阶主子式之和。因此，由Vieta定理，$\sum_{1\le i_1<i_2<\cdots<i_r\le n}\lambda_{i_1}\lambda_{i_2}\cdots\lambda_{i_r}$等于$A$的所有$r$阶主子式之和.

例题：$x^n-1=0$在复数域上有n个根，它们是$x_1=1, x_2=e^{\frac{2\pi i}{n}},\cdots,x_n=e^{\frac{2(n-1)\pi i}{n}}$，则

1. $x_1^k+x_2^k+\cdots+x_n^k=0, 1\le k\le n-1$. 因为$x_1^k,\cdots,x_n^k$恰好是$x^n-1=0$在复数域上的$n$个根（以上$n$个根的重排.）
2. $\overline{x_i}=x_{n-i+2}$(假设$x_{n+1}=x_1$)
3. 令$F_n=(f_{st})_{n\times n}$，$f_{st}=w^{(s-1)(t-1)}$,其中$w=e^{\frac{2\pi i}{n}}$. F_n被称为n阶Fourier矩阵，满足$F_n\overline{F}_n=nI_n$.