LOGO

§9 有理系数多项式

定义 1.11 如果非零的整系数多项式 $g(x)=b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ 的系数 $b_n, b_{n-1}, \cdots, b_0$ 是互素的，则称 $g(x)$ 为一个本原多项式。

引理（Gauss 引理） 两个本原多项式的乘积还是本原多项式。

证明 设

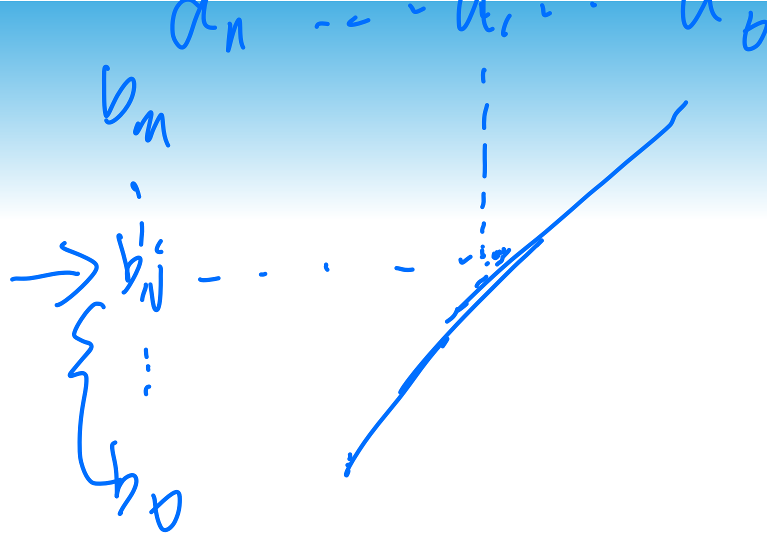
$$f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_0,\quad g(x)=b_m x^m+b_{m-1}x^{m-1}+\cdots+b_0$$

是两个本原多项式，而

$$h(x)=f(x)g(x)=d_{n+m}x^{n+m}+d_{n+m-1}x^{n+m-1}+\cdots+d_0$$

是它们的乘积。用反证法。如果 $h(x)$ 不是本原多项式，那么就有一个素数 p 能整除 $h(x)$ 的每一个系数 $d_{n+m},d_{n+m-1},\cdots,d_0$。因为 $f(x)$ 是本原多项式，所以 p 不能同时整除 $f(x)$ 的每一个系数。设 $p\mid a_0$，$\cdots$ ，$p\mid a_{i-1}$，但 $p\nmid a_i$，同样地，可设 $p\mid b_0$，$\cdots$ ，$p\mid b_{j-1}$，但 $p\nmid b_j$。

比较 $h(x)=f(x)g(x)$ 两边 x^{i+j} 的系数得



$$d_{i+j}=a_ib_j+a_{i+1}b_{j-1}+a_{i+2}b_{j-2}+\cdots+a_{i-1}b_{j+1}+a_{i-2}b_{j+2}+\cdots$$

根据 a_i 和 b_j 的取法，p 整除等式左端的 d_{i+j} 和右端除 a_ib_j 外所有的项，因此，p 整除右端的 a_ib_j，这与 $p\nmid a_i$ 且 $p\nmid b_j$ 矛盾。这就证明了，$h(x)$ 一定是本原多项式。证毕。

注　任何一个非零的有理系数多项式 $f(x)$ 都可以表示成一个有理数 r 与一个本原多项式 $g(x)$ 的乘积，且这种表示法是唯一的（不计 ± 1），即如果

$$f(x)=rg(x)=r_1 g_1(x),$$

其中 r,r_1 是有理数，$g(x),g_1(x)$ 都是本原多项式，那么必有

$$r=\pm r_1,\quad g(x)=\pm g_1(x).$$

这里只证表示法是唯一的。设 $\dfrac{r}{r_1}=\dfrac{k}{s}$，其中 k,s 是互素的整数，设

$$g(x)=b_n x^n+b_{n-1}x^{n-1}+\cdots+b_0,\quad g_1(x)=c_n x^n+c_{n-1}x^{n-1}+\cdots+c_0,$$

由 $rg(x)=r_1 g_1(x)$ 得：

$$k(b_n x^n+b_{n-1}x^{n-1}+\cdots+b_0)=s(c_n x^n+c_{n-1}x^{n-1}+\cdots+c_0),$$

比较对应项系数得：$kb_i=sc_i$，$i=0,1,\cdots,n$，由于 $(k,s)=1$，所以 $s\mid b_i$，$i=0,1,\cdots,n$，

又因为 $b_n,b_{n-1},\cdots,b_0$ 没有异于 ±1 的公因子，所以 $s=\pm1$，同理 $k=\pm1$，于是 $k=\pm s$，

$r=\pm r_1$，从而有 $g(x)=\pm g_1(x)$。这就证明了表示法是唯一的。

定理 1.10 如果一非零的整系数多项式能够分解成两个次数较低的有理系数多项式的乘积，那么它一定可以分解成两个次数较低的整系数多项式的乘积。

证明 设整系数多项式 $f(x)$ 有分解式

$$f(x)=g(x)h(x),$$

其中 $g(x),h(x)$ 是有理系数多项式，且

$$\partial(g(x))<\partial(f(x)), \quad \partial(h(x))<\partial(f(x)),$$

令 $f(x)=af_1(x)$，$g(x)=rg_1(x)$，$h(x)=sh_1(x)$，这里 $f_1(x),g_1(x),h_1(x)$ 都是本原多项式，a 是整数，r,s 是有理数，于是

$$af_1(x)=rsg_1(x)h_1(x)。$$

因为 $g_1(x)h_1(x)$ 是本原多项式，所以 $rs=\pm a$ ，这就是说，rs 是一整数。因此，我们有

$$f(x)=(rsg_1(x))h_1(x) ,$$

这里 $rsg_1(x)$ 与 $h_1(x)$ 都是整系数多项式，且次数都低于 $f(x)$ 的次数。证毕。

例 设$a_1,a_2,\cdots,a_n$是互不相同的整数，证明：

$$f(x)=(x-a_1)(x-a_2)\cdots(x-a_n)-1$$

在有理数域上不可约。

证明 用反证法。若$f(x)$可分解为两个次数都大于零的有理系数多项式的乘积，则$f(x)$可分解为两个次数都大于零的整系数多项式的乘积，即$f(x)=g(x)h(x)$，其中$g(x)$，$h(x)$是整系数多项式，由此得$f(a_i)=g(a_i)h(a_i)=-1$，因为$g(a_i),h(a_i)$都是整数，所以$g(a_i)=-h(a_i)=\pm 1$，$i=1,\cdots,n$。令$F(x)=g(x)+h(x)$，则$F(a_i)=0$，$i=1,\cdots,n$，而$g(x)$，$h(x)$的次数都小于n，所以$F(x)=0$，即$g(x)=-h(x)$，从而$f(x)=-g^2(x)$，但是$f(x)$的首项系数为1，矛盾。这就证明了$f(x)$在有理数域上不可约。

整 有理

$a f_0 = b g h_0$

定理 1.11 设 $f(x)$ 是整系数多项式，$g(x)$ 是本原多项式，如果 $f(x)=g(x)h(x)$，其中 $h(x)$ 是有理系数多项式，那么 $h(x)$ 一定是整系数多项式。

证明 设 $f(x)=af_1(x)$，$h(x)=sh_1(x)$，这里 $f_1(x)$ 和 $h_1(x)$ 都是本原多项式，a 是整数，s 是有理数，于是 $af_1(x)=sg(x)h_1(x)$。由于 $g(x)h_1(x)$ 是本原多项式，所以 $s=\pm a$，这就是说，s 是一整数。因此，$h(x)=sh_1(x)$ 是整系数多项式。

定理 1.12 设

$$f(x)=\underbrace{a_n}_{s}x^n+a_{n-1}x^{n-1}+\cdots+\underbrace{a_0}_{r}$$

是一个整系数多项式，而 $\dfrac{r}{s}$ 是它的一个有理根，其中 r,s 互素，那么必有 $s\mid a_n, r\mid a_0$。特别地，如果 $f(x)$ 的首项系数 $a_n=1$，那么 $f(x)$ 的有理根都是整数根，而且是 a_0 的因子。

证明 因为 $\dfrac{r}{s}$ 是 $f(x)$ 的一个有理根，由根与一次因式的关系有

$$f(x)=(x-\frac{r}{s})\varphi(x)=(sx-r)g(x),$$

其中 $g(x)$ 是有理系数多项式。由于 $sx-r$ 是本原多项式，所以 $g(x)$ 是整系数多项式。设

$$g(x)=b_{n-1}x^{n-1}+\cdots+b_0,$$

其中 $b_{n-1},\cdots,b_0$ 都是整数，从而有

$$f(x)=(sx-r)(b_{n-1}x^{n-1}+\cdots+b_0)\text{，}$$

比较两边系数得 $a_n=sb_{n-1}$， $a_0=-rb_0$，因此， $s\mid a_n, r\mid a_0$。证毕。

定理 1.13（Eisenstein 判别法） 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

是一个整系数多项式，若有一个素数 p，满足

（1） $p \nmid a_n$；

（2） $p \mid a_{n-1}, a_{n-2}, \cdots, a_0$；

（3） $p^2 \nmid a_0$，

则多项式 $f(x)$ 在有理数域上不可约。

$$\overset{p\,\nmid}{a_n} \quad \underline{a_{n-1} \cdots\cdots \overset{p^2\,\nmid}{a_0}}$$

证明 用反证法。假设 $f(x)$ 在有理数域上可约，那么 $f(x)$ 可以分解成两个次数较低的整系数多项式的乘积

$$f(x)=(b_l x^l+b_{l-1}x^{l-1}+\cdots+b_0)(c_m x^m+c_{m-1}x^{m-1}+\cdots+c_0)\ ,$$

其中 $l,m<n$，$l+m=n$。 $\Rightarrow l<n \Rightarrow k<n$

（1）因为 $p\mid a_0=b_0c_0$，所以 $p\mid b_0$ 或 $p\mid c_0$，不妨设 $p\mid b_0$，而 $p^2\nmid a_0$，因此 $p\nmid c_0$。

（2）因为 $p\nmid a_n=b_lc_m$，所以 $p\nmid b_l$。设 $p\mid b_0,b_1,\cdots,b_{k-1}$，而 $p\nmid b_k$。

（3）由于 $a_k=b_kc_0+\boxed{b_{k-1}c_1+\cdots}$，所以 $p\mid b_kc_0$，又由于 p 是素数，所以 $p\mid c_0$ 或 $p\mid b_k$，

但两者都不成立。因此，$f(x)$ 在有理数域上不可约。证毕。

注 若r是素数，那么对任意正整数n，$f(x)=x^n \pm r$在有理数域上都是不可约的。

作业：27 1），28 2）。

LOGO

谢谢观赏