数论讲义

SHU LUN JIANG YI

柯召 孙琦 编著

下

高等教育出版社

数 论 讲 义

下 册

柯召 孙琦 编著

高等教育出版社

本书是根据作者多年教学经验和科研成果写成的。内容除通常的初等数论教材中所包括的基本内容外，还包括高次剩余，三次、四次互反律，代数数论初步，有限域上某些不定方程的基础知识等。作者在介绍熟知的经典结果时，也注意介绍新的证明方法和近代进展，并尽可能介绍它们的应用。

本书共分上、下两册。上册前五章可作为初等数论课教学内容，上册第六章及下册可作为选修课教学内容。

本书可供数学专业、计算机科学专业及数字信号处理、组合数学方面的学生和研究生用作教材或参考书。也可供从事上面这些方面的教学、科研人员参考。

数论讲义

下　册

柯召　孙琦　编著

*

高等教育出版社出版
新华书店北京发行所发行
河北省香河县印刷厂印装

*

开本 850×1168 1/32　印张 7.875 字数 189 000
1987 年 4 月第 1 版　1988 年 2 月第 2 次印刷
印数 5,121—13,130
ISBN 7-04-001250-2/O·400
定　价 1.30 元

目　录

第七章　多　项　式

有理系数多项式，整系数多项式，以及系数在有限域 F_p 上的多项式，都是数论所研究的重要内容．本章着重讨论有理数域和有限域 F_p 上多项式的不可约问题，以及分圆多项式，x^n-y^n 的本原因式，F_p 上本原多项式等重要多项式的基本性质．本章还将介绍有限域的构造和有限域上多项式的一些问题．这些内容在某些应用学科中也很有用．

§1　有理数域上的多项式

设 Q 代表有理数域，Q 上的 n 次多项式 $f(x)$ 是指

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

$$n>0, a_i\in Q, i=0,1,\cdots,n, a_n\neq 0.$$

选取适当的整数 c 乘 $f(x)$，总可以使 $cf(x)$ 是一个整系数多项式．很明显，$f(x)$ 和 $cf(x)$ 在 Q 上同为可约或同为不可约．那么，整系数多项式在 Q 上可约，是否在整数环 Z 上可约呢？也就是说，如果整系数多项式可分解为较低次的有理系数因式的乘积，是否一定可分解为较低次的整系数因式的乘积？回答是肯定的．在代数中已证明：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，那么它一定能够分解成两个次数较低的整系数多项式的乘积．这就告诉了我们，在 Z 上不可约的整系数多项式，在 Q 上也不可约．因此，关于有理数域上多项式的可约性问题，可以简化为讨论整系数多项式在整数环上的可约性问题，下一节我们将主要讨论这个问题．

在代数中还证明了：域 F 上每一个 n 次($n>0$)多项式，如果不计零次因式，因式分解是唯一的．对于有理数域 Q，下面我们将证明存在一个有限步的分解方法，把 Q 上的一个 n 次多项式分解成不可约因式的乘积．

定理　有理数域 Q 上的任一 n 次多项式 $f(x)$，存在一个有限步的分解方法．

证　不失一般，可设 $f(x)$ 是整系数多项式．并设 $f(x)$ 的因式为形如

$$\varphi(x)=b_sx^s+\cdots+b_1x+b_0$$

的 $s,1\leqslant s\leqslant\left[\frac{n}{2}\right]$ 次整系数多项式．取 $a_1,a_2,\cdots,a_{s+1}$ 是 $s+1$ 个不同的整数，使得

$$f(a_j)\neq0,\ j=1,\cdots,s+1.$$

设 $k_j\mid f(a_j),\ j=1,\cdots,s+1,\ k_1,\cdots,k_{s+1}$ 是一组分别为 $f(a_1),\cdots,f(a_{s+1})$ 的因数的整数．如果 $\varphi(x)$ 是 $f(x)$ 的因式，则 $\varphi(a_i)\mid f(a_i)$，故令

$$\begin{aligned}
\varphi(a_1)&=b_sa_1^s+b_{s-1}a_1^{s-1}+\cdots+b_1a_1+b_0=k_1,\\
\varphi(a_2)&=b_sa_2^s+b_{s-1}a_2^{s-1}+\cdots+b_1a_2+b_0=k_2,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \qquad (1)\\
\varphi(a_{s+1})&=b_sa_{s+1}^s+b_{s-1}a_{s+1}^{s-1}+\cdots+b_1a_{s+1}+b_0=k_{s+1}.
\end{aligned}$$

由于

$$\begin{vmatrix}
a_1^s & a_1^{s-1} & \cdots & a_1 & 1\\
a_2^s & a_2^{s-1} & \cdots & a_2 & 1\\
\vdots & \vdots & & \vdots & \vdots\\
a_{s+1}^s & a_{s+1}^{s-1} & \cdots & a_{s+1} & 1
\end{vmatrix}\neq0,$$

故由(1)可唯一决定一组 $\varphi(x)$ 的系数 $b_s,b_{s-1},\cdots,b_1,b_0$，如果它们都是整数，就决定了一个 $\varphi(x)$，它可能是 $f(x)$ 的因式．因为

$k_1,\cdots,k_{s+1}$ 只有有限组值，故对每一个 s，$s\leqslant\left[\frac{n}{2}\right]$，只有有限个 s 次多项式可能是 $f(x)$的因式. 故存在一个有限步的分解方法.

证完

§2 整系数多项式不可约的判别条件

当 n 大时，判别一个整系数多项式是否可约，常常是困难的. 关于这方面有许多研究工作，其中较为著名的是下面的定理.

定理 1 (Eisenstein 判别法) 设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

是一个 n 次整系数多项式，如果至少有一个方法可以选出素数 p，适合 $p\nmid a_n$，$p\mid a_i\ (0\leqslant i<n)$，且 $p^2\nmid a_0$，那么多项式在有理数域 Q 上不可约.

证 假定 $f(x)$在 Q 上可约，由 §1的定理可设

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

$$g(x)=b_lx^l+b_{l-1}x^{l-1}+\cdots+b_1x+b_0,$$

$$h(x)=h_mx^m+\cdots+h_1x+h_0,$$

$$l+m=n,\ l>0,\ m>0,\ b_lh_m\neq0,$$

式中 $b_j(j=0,1,\cdots,l)$和 $h_j(j=0,1,\cdots,m)$均为整数，$a_t=\sum_{i+j=t}b_ih_j$，$t=0,1,\cdots,n$. 由 $a_0=b_0h_0$，$p\mid a_0$，可知 $p\mid b_0$ 或 $p\mid h_0$，不妨设 $p\mid b_0$，则由 $p^2\nmid a_0$ 知 $p\nmid h_0$. 因为 $a_1=b_0h_1+b_1h_0$，故 $p\mid b_1$. 又因 $a_2=b_0h_2+b_1h_1+b_2h_0$，故 $p\mid b_2$. 依此类推，最后可得 $p\mid b_l$，而 $a_n=b_lh_m$，此与 $p\nmid a_n$ 矛盾.

证完

我们知道，在复数域，每一个次数大于 1 的多项式都是可约的. 而在实数域上，每一个次数大于 2 的实系数多项式也是可约的，定理 1 告诉我们，对于有理数域 Q 的情形则完全不同，对任给的整数 $n>0$，都存在 Q 上的 n 次不可约多项式. 例如，p 是任给

的素数，由定理 1 知多项式 x^n+p 在 Q 上不可约.

另一个著名的判别法则是 Perron 于 1907 年给出的，他首次通过比较多项式系数的大小，来判别多项式的不可约性.

定理 2 (Perron 判别法) 设

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\quad a_0\neq 0 \tag{1}$$

是一个整系数多项式，如果

$$|a_{n-1}|>1+|a_{n-2}|+|a_{n-3}|+\cdots+|a_1|+|a_0|, \tag{2}$$

则 $f(x)$在有理数域 Q 上不可约.

证明定理 2 之前先证明一个引理.

引理 1 如果(1)中的多项式 $f(x)$ 在复数域上仅有一个零点 α 满足 $|\alpha|\geqslant 1$，则 $f(x)$在 Q 上不可约.

证 若 $f(x)$在 Q 上可约，可设 $f(x)=f_1(x)f_2(x)$，此处 $f_i(x)$ $(i=1,2)$ 均为次数低于 n 的整系数多项式，如果 $f_1(\alpha)=0$，不妨设 $f_2(x)=x^l+b_{l-1}x^{l-1}+\cdots+b_1x+b_0$，$b_0\neq 0$，$f_2(x)=0$ 的全部根设为 $\beta_1,\cdots,\beta_l$，它们的模均小于 1，故有

$$|b_0|=|f_2(0)|=|\beta_1|\cdots|\beta_l|<1.$$

这与 b_0 是非零整数矛盾. 证完

定理 2 的证明 由复变函数论中的 Rouché 定理知，条件(2)给出 $f(x)$在单位圆 $|x|<1$ 内的零点恰有 $n-1$ 个，故 $f(x)$在复数域上仅有一个零点 α，其模满足 $|\alpha|\geqslant 1$，由引理知 $f(x)$在 Q 上不可约. 证完

1933 年，Berwald 把条件 (2) 改进为 $|a_{n-1}|>|1+a_{n-2}|+|a_{n-3}|+\cdots+|a_1|+|a_0|$.

1948 年，Brauer 证明了，整系数多项式 $f(x)=x^n+a_{n-2}x^{n-2}+a_{n-3}x^{n-3}+\cdots+a_1x+a_0$，$a_0\neq 0$，在 $|a_{n-2}|>|1+a_{n-4}|+|a_{n-3}|+|a_{n-5}|+\cdots+|a_1|+|a_0|$ 时，在 Q 上不可约.

设 n 次整系数多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，易

知，$f(x)$在Q上不可约的充分必要条件是$y^n f\left(\frac{1}{y}\right)$在$Q$上不可约(留作习题)．由此，由 Perron 判别法立刻推出以下的推论．

推论 设整数k满足$|k|\geqslant 3$，则多项式$f(x)=x^n+kx\pm 1$在Q上不可约．

1956 年，Selmer 证明了：多项式x^n-x-1在Q上不可约，当$n\not\equiv 2(\mathrm{mod}3)$时，多项式$x^n+x+1$在$Q$上不可约．

整系数多项式$f(x)$的不可约性与$f(x)$在Z上的取值是有密切关系的．1969 年，Brown 和 Graham 证明了下面一个结果：设$f(x)$是n次整系数多项式，$S(f)=\{\cdots,|f(-1)|,|f(0)|,|f(1)|,\cdots\}$，$N_1$表示$S(f)$中的 1 的个数，$N_p$表示$S(f)$中素数的个数，如果$N_p+2N_1-4>n$，则$f(x)$在$Q$上不可约．

例 $f(x)=2x^3-x^2+x-1$，由于$f(0)=-1, f(1)=1, f(2)=13, f(-2)=-23, f(3)=47, f(-1)=-5$，$N_p\geqslant 4, N_1\geqslant 2$，故$N_p+2N_1-4\geqslant 4>3$，故$f(x)$在$Q$上不可约．

本世纪初，Schur 对于多项式的不可约性提出了许多有趣的问题，有的已经解决了，有的迄今尚未解决．下面的定理解决了 Schur 提出的两个简单问题．

定理 3 设$a_1,\cdots,a_n$是彼此不相同的整数，则

① $f(x)=(x-a_1)\cdots(x-a_n)-1$在有理数域$Q$上不可约．

② $f(x)=(x-a_1)^2\cdots(x-a_n)^2+1$在有理数域$Q$上不可约．

证 ① 如果$f(x)$在Q上可约，可设$f(x)=f_1(x)f_2(x)$，$f_i(x)$是整系数多项式，$1\leqslant\partial^\circ(f_i(x))<n(i=1,2)$，其中$\partial^\circ(f(x))$表示$f(x)$的次数．由于$f(a_i)=-1, i=1,\cdots,n$，故$f_1(a_i)=\pm 1, f_2(a_i)=\mp 1, i=1\cdots,n$，即

$$f_1(a_i)+f_2(a_i)=0,\quad i=1,\cdots,n.$$

因为$f_1(x)+f_2(x)$的次数小于n，故$f_1(x)+f_2(x)=0$，即得$f_1(x)$

$=-f_2(x)$, $f(x)=-f_1^2(x)$, 因为 $f(x)$的最高项系数是 1，此不可能.

② 显然, $f(x)$没有实根, 如果 $f(x)$在 Q 上可约，类似①可设 $f(x)=f_1(x)f_2(x)$, 此处 $1\leqslant\partial^\circ(f_i(x))<2n(i=1,2)$, 因为对所有实数, $f(x)>0$, 不妨设对于所有实数 $f_1(x)>0$, $f_2(x)>0$, 故有

$$f_1(a_i)=f_2(a_i)=1, \quad i=1,\cdots,n, \tag{3}$$

如果 $f_1(x)$(或 $f_2(x)$)的次数小于 n, 则由(3), $f_1(x)$(或 $f_2(x)$)恒等于 1, 和所设不合, 故 $\partial^\circ(f_i(x))=n(i=1,2)$, 于是

$$f_1(x)=1+a(x-a_1)\cdots(x-a_n),$$

$$f_2(x)=1+b(x-a_1)\cdots(x-a_n),$$

此处 a, b 是整数, 因此

$$(x-a_1)^2\cdots(x-a_n)^2+1=f_1(x)f_2(x)$$

$$=1+(a+b)(x-a_1)\cdots(x-a_n)+ab(x-a_1)^2\cdots(x-a_n)^2,$$

比较两端系数得 $ab=1$, $a+b=0$, 此不可能. 证完

在定理 3 中, 把 $f(x)$分别换成 $f(x)=k\prod_{i=1}^{n}(x-a_i)-1$, $f(x)=k\prod_{i=1}^{n}(x-a_i)^2+1$, $k>0$, 显然定理仍然成立. 但 Schur 猜想 $m>1$ 时, $f(x)=\prod_{i=1}^{n}(x-a_i)^{2^m}+1$ 在 Q 上不可约, 迄今只证明了一些特殊情形(如$n=2$).

最后, 我们介绍一个有关多项式不可约性的结果. 1981 年, Newman 利用这个结果, 曾给出了一类根式不定方程的全部正整数解.

定理 4 设 a 是一个有理数, $a>0$, $a\neq1$, 把 a 写成 $a=\prod_{i=1}^{s}p_i^{\alpha_i}$, 这里$\alpha_i\neq0$, p_i 是不同的素数$(i=1,\cdots,s)$, 设 $v(a)$

$=(\alpha_1,\cdots,\alpha_s)$. 则多项式

$$f(x)=x^n-a$$

在Q上不可约的充分必要条件是$(n,v(a))=1$.

证明 如果$f(x)$不可约，则有$(n,v(a))=1$，否则设$d=(n,v(a))>1$,则

$$f(x)=x^{\frac{n}{d}\cdot d}-a^{\frac{1}{d}\cdot d},$$

$(x^{\frac{n}{d}}-a^{\frac{1}{d}})\mid f(x)$，由于$1\leqslant\frac{n}{d}<n$, $a^{\frac{1}{d}}$是有理数，故与所设矛盾.

反之，设$d=1$,如果$f(x)$可约，则可设

$$f(x)=f_1(x)f_2(x),$$

$f_1(x)$为首项系数为1的k次有理系数多项式，$1\leqslant k<n$. 设η是n次单位原根，故

$$x^n-a=\prod_{i=1}^{n}(x-\eta^i a^{\frac{1}{n}}).$$

不妨设

$$f_1(x)=\prod_{j=1}^{k}(x-\eta^{i_j}a^{\frac{1}{n}}),\quad 1\leqslant i_1<i_2<\cdots<i_k\leqslant n,$$

因为$\prod_{j=1}^{k}(\eta^{i_j}a^{\frac{1}{n}})$是有理数，故$\pm a^{\frac{k}{n}}$为有理数，即

$$a^{\frac{k}{n}}=\prod_{i=1}^{s}p_i^{\alpha_i\cdot k/n}\in Q,$$

故得

$$\frac{\alpha_i k}{n}\equiv 0\pmod 1,\quad i=1,\cdots,s. \tag{4}$$

因为存在整数t_i, $i=1,\cdots,s$, 使$v(a)=\sum_{i=1}^{s}t_i\alpha_i$,故由(4)推出

$$\frac{v(a)k}{n}\equiv 0 \pmod 1. \tag{5}$$

因为$(v(a),n)=1$,(5)推出$n|k$,与所设$1\leqslant k<n$矛盾. 证完

用这个定理,Newman 证明了:

设m,n,r是正整数,不定方程

$$x^{\frac{1}{m}}+y^{\frac{1}{n}}=z^{\frac{1}{r}}$$

的全部正整数解由

$$x=t^{m/d}a^m,\ y=t^{n/d}b^n,\ z=t^{r/d}(a+b)^r$$

给出,这里$(m,n,r)=d,a,b,t$是任意的正整数,且满足$(a,b)=1$.

§3 有理数域上的分圆多项式

熟知,设$n>0$,全体n次单位根为

$$\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n},\quad k=0,1,\cdots,n-1,$$

设$\eta_1,\eta_2,\cdots,\eta_{\varphi(n)}$是$\varphi(n)$个$n$次单位原根.

定义 多项式

$$F_n(x)=\prod_{i=1}^{\varphi(n)}(x-\eta_i)$$

叫做**分圆多项式**.

设η是一个n次单位原根,则

$$\eta,\eta^2,\cdots,\eta^n \tag{1}$$

给出全体n次单位根. 设$1\leqslant a\leqslant n$, $(a,n)=d$, 则η^a是$\frac{n}{d}$次单位原根,(1)中给出$\varphi\left(\frac{n}{d}\right)$个$\frac{n}{d}$次单位原根, 即(1)中包含了全体$\frac{n}{d}$$(d|n)$次单位原根,于是当$d$通过$n$的全部正因数时,就有

$$x^n-1=\prod_{d|n}F_d(x). \tag{2}$$

由第三章§5麦比乌斯反演公式得

$$F_n(x)=\prod_{d\mid n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}. \tag{3}$$

定理1 $F_n(x)$是首项系数为1的整系数多项式，而且在有理数域Q上不可约.

下面我们给出一个初等的证明. 为此，先证明几个引理.

引理1 设$f(x)$和$g(x)$是两个有理系数的多项式. 如果$g(x)$不可约，且$f(x)$和$g(x)$有一个公共零点，则有$g(x)\mid f(x)$.

证 设α是它们的公共零点，$(f(x),g(x))=d(x)$，故$(x-\alpha)\mid d(x)$. 因为$g(x)$是不可约的，故$d(x)=ag(x)$，这里$a\neq 0$是一个有理数，由此推出$g(x)\mid f(x)$. 证完

引理1告诉我们，一个有理系数不可约多项式不能和比它次数低的有理系数多项式有公共零点.

引理2 设$f(x)$是一个首项系数为1的整系数多项式，$g(x)$是一个首项系数为1的有理系数多项式，如果$g(x)\mid f(x)$，则$g(x)$的系数必定是整数.

证 可以假设

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

这里$h(x)$的系数是有理数. 设M是最小的正整数使得$Mg(x)$是一个整系数多项式，N是最小的正整数使得$Nh(x)$是一个整系数多项式. 因$g(x),h(x)$的首项系数均为1，故$Mg(x)$和$Nh(x)$均为本原多项式. 于是，$MNg(x)h(x)$也是一个本原多项式，但是，由$MNg(x)h(x)=MNf(x)$，$f(x)$是一个本原多项式，故$MN=1$，$M=N=1$，这就证明了$g(x)$的系数必定是整数. 证完

引理3 设

$$g(x)=x^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0$$

是一个整系数多项式，具有零点$x_1,\cdots,x_m$，再设

$$G(x)=x^m+A_{m-1}x^{m-1}+\cdots+A_1x+A_0$$

具有零点 $x_1^p, x_2^p, \cdots, x_m^p$，这里 p 是一个素数. 则系数 $A_0, A_1, \cdots, A_{m-1}$ 是整数，且

$$p \mid A_i-a_i, \quad i=0,1,\cdots,m-1. \tag{4}$$

证 因为

$$(-1)^u a_{m-u}=\sum_{1\leqslant i_1<i_2<\cdots<i_u\leqslant m} x_{i_1}x_{i_2}\cdots x_{i_u},$$
$$u=1,\cdots,m-1,m, \tag{5}$$

$$(-1)^u A_{m-u}=\sum_{1\leqslant i_1<i_2<\cdots<i_u\leqslant m} (x_{i_1}x_{i_2}\cdots x_{i_u})^p,$$
$$u=1,\cdots,m-1,m, \tag{6}$$

易知(6)的右端是$x_1,\cdots,x_m$的对称整系数多项式，由对称多项式的基本定理知，它可以表成 $x_1,\cdots,x_m$ 的初等对称多项式的整系数多项式，故由(5)得知 $A_i(i=0,1,\cdots,m-1)$均为整数. 再由

$$((-1)^u a_{m-u})^p=(\sum_{1\leqslant i_1<\cdots<i_u\leqslant m} x_{i_1}x_{i_2}\cdots x_{i_u})^p \tag{7}$$

知道，(7)的右端的每一个大于 1 的系数均能被 p 整除. 于是得到

$$((-1)^u a_{m-u})^p=(-1)^u A_{m-u}+pS(x_1,\cdots,x_m) \tag{8}$$

$S(x_1,\cdots,x_m)$是一个整系数对称多项式，故由对称多项式基本定理及(5)知 $S(x_1,\cdots,x_m)$是一个整数，对(8)式取模 p 得

$$a_{m-u}\equiv A_{m-u}(\mathrm{mod}p), \quad u=1,\cdots,m.$$

故引理成立. 证完

定理 1 的证明：

首先，我们来证明 $F_n(x)$是一个整系数多项式. 使用归纳法，当 $n=1$ 时，$F_1(x)=x-1$，是一个整系数多项式. 现设对于所有 $k<n(n\geqslant 2)$，$F_k(x)$均为整系数多项式，由(2)式得

$$x^n-1=F_n(x)\cdot\prod_{\substack{d\mid n\\ d<n}}F_d(x)=F_n(x)G_n(x).$$

由归纳法假设 $G_n(x)$ 是一个首项系数为 1 的整系数多项式，由多项式的除法，易知 $F_n(x)$是一个首项系数为 1 的有理系数多项式，由引理 2 知 $F_n(x)$ 是整系数多项式. 现在我们来证明 $F_n(x)$在 Q 上不可约. 否则，可设

$$F_n(x)=f_1(x)f_2(x)\cdots f_t(x),\quad t>1,$$

这里 $f_j(x)(j=1,\cdots,t)$ 是有理系数不可约多项式. 又因为 $F_n(x)$ 在 Q 上无重因式，故 $f_1(x),\cdots,f_t(x)$是互不相同的. 再由引理 2，$f_1(x),\cdots,f_t(x)$ 都是首项系数为 1 的整系数多项式. 现在我们指出 $f_1(x),\cdots,f_t(x)$的次数是相同的. 不失一般，我们来证明 $f_1(x)$ 的次数等于 $f_2(x)$的次数. 设 η 是 $f_1(x)=0$ 的一个根，因为 η 是 n 次单位原根，故存在一个正整数 k，$(k,n)=1$，使得 η^k 是 $f_2(x)=0$ 的根. 构造多项式 $g(x)$，它们全体根分别是 $f_1(x)$的全体根的 k 次方幂，显然 $g(x)$是整系数多项式，因为 $f_2(x)=0$ 与 $g(x)=0$ 有公共根，$f_2(x)$是 Q 上不可约多项式，由引理 1 知 $f_2(x)\mid g(x)$，所以 $f_2(x)$的次数不大于 $f_1(x)$的次数. 类似可证 $f_1(x)$ 的次数不大于 $f_2(x)$的次数，故 $f_1(x)$的次数等于 $f_2(x)$的次数，且 $f_2(x)=0$ 的全体根分别是 $f_1(x)=0$ 的全体根的 k 次方幂.

设 A_{ij} 代表 $f_i(x)-f_j(x)(i\neq j)$ 的系数的绝对值的最大值，取

$$M>\max\{n, A_{ij}(\text{对所有 } i\neq j)\},$$

再设

$$T=\prod_{\substack{p\leqslant M\\ p\nmid k}} p, \tag{9}$$

$$H=Tn+k. \tag{10}$$

显然 $\eta^H=\eta^k$. 设 $H=q_1\cdot q_2\cdots q_s$，这里 $q_1,\cdots,q_s$ 是素数，由(9)、(10)和 $(n,k)=1$ 知，$q_j>M$，$j=1,\cdots,s$. 构造首项系数为 1 的多项式 $h_1(x)$使得它每一个零点正好是 $f_1(x)$的每一个零点的 q_1 次方幂，

再作首项系数为1的多项式$h_2(x)$使得它每一个零点正好是$h_1(x)$的每一个零点的q_2次方幂. 依此继续做下去,可得一多项式序列

$$h_1(x),h_2(x),\cdots,h_s(x), \tag{11}$$

其中诸多项式为首项系数为1的整系数多项式,且$h_s(x)=f_2(x)$,诸多项式的次数皆相同. 因为对任一正整数l,如果多项式$(x-\xi_1)(x-\xi_2)\cdots(x-\xi_f)$是整系数多项式,那么多项式$(x-\xi_1^l)(x-\xi_2^l)\cdots(x-\xi_f^l)$也是整系数多项式,故知$f_2(x)$在$Q$上不可约时,$h_1(x),h_2(x),\cdots,h_{s-1}(x)$在$Q$上也不可约. 因为$(H,n)=1$,故(11)中的任一多项式$h_i(x)$与某一个多项式$f_j(x)$有公共零点,故$h_i(x)=f_j(x)$,因为$f_1(x)\neq f_2(x)$,故(11)中的多项式不能都等于$f_1(x)$,设$h_r(x)=f_j(x)$是(11)中第一个不等于$f_1(x)$的多项式. 由于$h_{r-1}(x)=f_1(x)$,于是,$f_j(x)$的全体零点正好是$f_1(x)$的全体零点的$q_r$次方幂. 由引理3,$f_1(x)-f_2(x)$的所有系数均能被$q_r$整除,但是因为$q_r>M$,这是矛盾的. 这就证明了$F_n(x)$在$Q$上不可约. 证完.

下面我们给出分圆多项式的一些简单性质.

定理2 设$F_n(x)$表示一个分圆多项式,则

① p是素数,$p\nmid m$,$F_{mp^k}(x)=F_{mp}(x^{p^{k-1}})$;

② p是素数,$p\nmid m$,$F_{mp}(x)=\dfrac{F_m(x^p)}{F_m(x)}$;

③ $n\geqslant 3$,$2\nmid n$,$F_{2n}(x)=F_n(-x)$;

④ $n\geqslant 2$,$x^{\varphi(n)}F_n\left(\dfrac{1}{x}\right)=F_n(x)$.

证

① $$F_{mp^k}(x)=\prod_{d\mid mp^k}(x^{\frac{mp^k}{d}}-1)^{\mu(d)}=\prod_{d\mid mp}((x^{p^{k-1}})^{\frac{mp}{d}}-1)^{\mu(d)}$$

$$=F_{mp}(x^{p^{k-1}}).$$