arXiv:2301.00365v1 [math.NT] 1 Jan 2023

关于由 x^7+ax+b 定义的数域的公共指数因子

ANUJ JAKHAR、SUMANDEEP KAUR 和 SURENDER KUMAR

Abstract. 设 $f(x)=x^7+ax+b$ 是一个系数为整数的不可约多项式，$K=\mathbb{Q}(\theta)$ 是由 $f(x)$ 的一个根 θ 生成的代数数域。在本文中，对于每个有理素数 p，我们的目标是确定仅涉及 a、b 的充要条件，使得 p 是域 K 的指数的一个除数。特别地，我们给出关于 a 和 b 的充分条件，在这些条件下，K 是非单生成的。在一个特殊情形下，我们证明，若 8 同时整除 $a\pm1$ 和 b，或 32 同时整除 $a+4$ 和 b，则 K 是非单生成的。我们通过例子说明所得结果。

1. Introduction and statements of results

设 $K=\mathbb{Q}(\theta)$ 是一个代数数域，其中 θ 属于 K 的代数整数环 $\mathbb{O}_K$。设 $f(x)\in\mathbb{Z}[x]$ 是 θ 在有理数域 $\mathbb{Q}$ 上的次数为 n 的最小多项式。代数数论中的一个基本结论是，$\mathbb{O}_K$ 是秩为 n 的自由阿贝尔群。若存在某个 $\alpha\in\mathbb{O}_K$，使得 $\{1,\alpha,\cdots,\alpha^{n-1}\}$ 是 K 的整数基，则称代数数域 K 为单生成的。在这种情况下，$\mathbb{O}_K=\mathbb{Z}[\alpha]$，即 $[\mathbb{O}_K:\mathbb{Z}[\alpha]]=1$。若 K 不存在这样的 α，则称域 K 为非单生成的。众所周知，每个二次域和分圆域都是单生成的。了解一个数域是否单生成十分重要。Dedekind 首先给出了一个非单生成数域 $K=\mathbb{Q}(\xi)$，其中 ξ 是多项式 x^3-x^2-2x-8 的一个根（参见 [15, , 第 64] 页）。数域单生成性的判定问题以及幂整数基的构造问题已得到深入研究（参见 [1], [2], [6], [9], [10], [11], [14], [18]）。1984 年，Funakura [5] 给出了使四次域 $\mathbb{Q}(m^{1/4})$ 为单生成域的整数 m 的充要条件。Ahmad、Nakahara 和 Husnine 在 [1], [2] 中证明，对于一个与 ±1 模 9 不同余的无平方因子整数 m，六次纯域 $\mathbb{Q}(m^{1/6})$ 在 $\mathbb{Q}$ 上的次数为六；当 $m\equiv2$ 或模 4 同余于 3 时，该域是单生成的；当 $m\equiv1$ 模 4 时，该域是非单生成的。

2010年数学主题分类：11R04，11R21。关键词和短语：单生成性，Ore 定理，素理想分解。第一作者感谢 SERB 资助项目 SRG/2021/000393 以及印度理工学院马德拉斯分校提供的 NFIG RF/22-23/1035/MA/NFIG/009034 资助。第二作者感谢位于新德里的科学与工业研究委员会通过资助编号 09/135(0878)/2019-EMR-1，以高级研究奖学金的形式提供经费支持。第三作者感谢位于新德里的大学拨款委员会通过参考编号 1129/(CSIR-NET 2019年6月)，以初级研究奖学金的形式提供经费支持。

2017 年，Ga´al 和 Remete [6] 研究了如下形式的代数数域的单生成性：$\mathbb{Q}(m^{1/n})$，其中 $3 \leq n \leq 9$ 且 m 为无平方因子整数。在 [9], A. Jakhar 和 S. Kumar 给出了一些充分条件，使数域 K （由六次三项式定义）$x^6 + ax + b \in \mathbb{Z}[x]$，为非单生成域。在 [7], Ga´al 研究了由若干六次不可约三项式定义的数域的单生成性。

回顾一下，对于代数数域 $L = \mathbb{Q}(\xi)$，若 ξ 是满足关于 $\mathbb{Q}$ 的首一不可约多项式 $g(x)$ 的代数整数，则 $g(x)$ 的判别式 D 与 L 的判别式 d_L 之间的关系由下式给出

$$D = (\operatorname{ind} \xi)^2 \cdot d_L. \tag{1.1}$$

在本文中，$\operatorname{ind} \theta$ 表示子群 $\mathbb{Z}[\theta]$ 在 $\mathbb{O}_K$ 中的指数，而 $i(K)$ 表示由下式定义的域 K 的指数

$$i(K) = \gcd\{\operatorname{ind} \alpha \mid K = \mathbb{Q}(\alpha) \text{ and } \alpha \in \mathbb{O}_K\}.$$

$i(K)$ 的一个素因子称为 K 的公共指数因子。注意，对于每个单生成数域 K，都有 $i(K) = 1$。然而，也存在满足 $i(K) = 1$ 的非单生成数域，例如，$K = \mathbb{Q}(\sqrt[3]{175})$ 是非单生成的，且 $i(K) = 1$。

以下设 $K = \mathbb{Q}(\theta)$ 是代数数域，θ 是不可约三项式 $f(x) = x^7 + ax + b \in \mathbb{Z}[x]$ 的一个根。那么对于每个有理素数 p，我们给出关于 a、b 的充要条件，使得 p 是 K 的公共指数因子。特别地，在这些条件下，K 是非单生成的。我们的方法基于牛顿多边形理论和 Ore 定理。1878 年，Dedekind（见 [[4], 定理 6.1.4]）给出了判定 p 是否整除指数 $[\mathbb{O}_K$ 的准则：$\mathbb{Z}[\theta]]$。当 p 整除指数 $[\mathbb{O}_K$: $\mathbb{Z}[\theta]]$ 时，可以使用 Ore 于 1928 年提出的方法计算 $p\mathbb{O}_K$ 的素理想分解（见 [19], [20]）。如果 Ore 的方法不适用，则可使用 Guardia、Montes 和 Nart 基于高阶牛顿多边形提出的算法 [21], ，来确定 $p\mathbb{O}_K$ 的素理想分解。

对于素数 p，以及属于 p 进整数环 $\mathbb{Z}_p$ 的非零元素 m ， $v_p(m)$ 表示整除 m 的 p 的最高次幂。对于非零整数 l，令 l_p 表示 $\frac{l}{p^{v_p(l)}}$。若有理素数 p 满足 p^6 整除 a 且 p^7 整除 b，则 θ/p 是具有整数系数的多项式 $x^7 + (a/p^6)x + (b/p^7)$ 的一个根。因此，我们可以假设对每个素数 p

$$\text{either } v_p(a) \leq 5 \text{ or } v_p(b) \leq 6. \tag{1.2}$$

此外， D 表示 $f(x)$ 的判别式。容易验证

$$D = -7^7 b^6 - 6^6 a^7. \tag{1.3}$$

在上述记号和假设（1.2）下，我们证明

定理 1.1. 设 $K = \mathbb{Q}(\theta)$ 是一个代数数域，其中 θ 是不可约多项式 $f(x) = x^7 + ax + b$ 的一个根。若 $u = {}^{v_2(D)_2}{}^{-6}$ 且 $\rho = 2^u + \frac{7b}{6a}$，则 $2 \mid i(K)$ 当且仅当以下条件之一成立：

(1) $a\equiv 3$ 模 4 且 $b\equiv 0$ 模 8。(2) $a\equiv 3$ 模 8 且 $b\equiv 4$ 模 8。(3) $a\equiv 1$ 模 4 且 $b\equiv 0$ 模 4。(4) $a\equiv 1$ 模 4, $b\equiv 2$ 模 4, 且 $v_2(D)$ 为奇数。(5) $a\equiv 1$ 模 4, $b\equiv 2$ 模 4, $v_2(D)$ 为偶数, 且 $v_2(f(\rho))=2u+1$。(6) $a\equiv 1$ 模 4, $b\equiv 2$ 模 4, $v_2(D)$ 为偶数, 且 $v_2(f(\rho))\geq 2u+3$。(7) $a\equiv 28$ 模 32 且 $b\equiv 0$ 模 32。(8) $a\equiv 48$ 模 64 且 $b\equiv 0$ 模 128。

以下三个推论可由上述定理立即得出。

推论 1.2. 设 $K=\mathbb{Q}(\theta)$ 是一个代数数域, 其中 θ 满足不可约多项式 $x^7+ax+b\in\mathbb{Z}[x]$。若 8 整除 $a\pm 1$ 和 b, 则 K 是非单生成的。

推论 1.3. 设 $K=\mathbb{Q}(\theta)$ 是由不可约多项式 x^7+ax+b 的一个根 θ 生成的代数数域, 其中该多项式属于 $\mathbb{Z}[x]$。若 $a+4$ 和 b 均被 32 整除, 则 K 是非单生成的。

推论 1.4. 设 $K=\mathbb{Q}(\theta)$ 是由不可约多项式 x^7+ax+b 的一个根 θ 生成的代数数域, 其中该多项式属于 $\mathbb{Z}[x]$。若 $a+16$ 和 b 均被 128 整除, 则 K 是非单生成的。

定理 1.5. 设 $K=\mathbb{Q}(\theta)$ 是一个代数数域, θ 是不可约多项式 $f(x)=x^7+ax+b$ 的一个根。那么, 当且仅当以下条件之一成立时, $3\mid i(K)$:

(1) $a\equiv 2$ 模 9, $v_3(b)=1$, $b_3\equiv 1$ 模 3, $v_3(a+7)=2$ 且 $v_3(b-a-1)\geq 3$。(2) $a\equiv 2$ 模 9, $v_3(b)=1$, $b_3\equiv 1$ 模 3, $v_3(a+7)\geq 3$, $v_3(b-a-1)\geq 3$, $2v_3(a+7)>v_3(b-a-1)+1$ 且 $(b-a-1)_3\equiv -1$ 模 3。(3) $a\equiv 2$ 模 9, $v_3(b)=1$, $b_3\equiv 1$ 模 3, $v_3(a+7)\geq 3$, $v_3(b-a-1)\geq 3$ 且$2v_3(a+7)<v_3(b-a-1)+1$。(4) $a\equiv 2$ 模 9, $v_3(b)=1$, $b_3\equiv -1$ 模 3, $v_3(a+7)=2$ 且 $v_3(b+a+1)\geq 3$。(5) $a\equiv 2$ 模 9, $v_3(b)=1$, $b_3\equiv -1$ 模 3, $v_3(a+7)\geq 3$, $v_3(b+a+1)\geq 3$, $2v_3(a+7)>v_3(a+b+1)+1$ 且 $(b+a+1)_3\equiv -1$ 模 3。(6) $a\equiv 2$ 模 9, $v_3(b)=1$, $b_3\equiv -1$ 模 3, $v_3(a+7)\geq 3$, $v_3(b+a+1)\geq 3$ 且$2v_3(a+7)=v_3(a+b+1)+1$。(7) $a\equiv 5$ 模 9 且 $v_3(b)=1$。(8) $v_3(a+1)>1$, $v_3(b)>1$ 且 $((a+1)3, b_3)\in\{(-1,1),(1,-1)\}$ 模 3。(9) $v_3(a+1)>1$, $v_3(b)>1$ 且 $((a+1)3, b_3)\in\{(-1,-1),(1,1)\}$ 模 3。

以下推论可由上述定理直接得出。

推论 1.6. 设 $K=\mathbb{Q}(\theta)$, 其中 θ 满足不可约多项式 x^7+ax+b。那么, 如果满足以下条件之一, K 就是非单生成的:

(1) $a\equiv 5$ 模 9, $b\equiv 3$ 模 9。

(2) $a \equiv 5$ 模 9， $b \equiv 6$ 模 9。

定理 1.7. 设 $K = \mathbb{Q}(\theta)$ 是一个代数数域，其中 θ 是不可约多项式 $f(x) = x^7 + ax + b \in \mathbb{Z}[x]$ 的一个根。设 $p \geq 5$ 是有理素数，则 $p \nmid i(K)$。

注记 1.8. 注意，当 $a = 0$ 且 b 是非零奇整数时， K 的指数为 1。

推论 1.9. 设 $K = \mathbb{Q}(\theta)$ 是由一个根生成的代数数域 θ ，该根属于不可约多项式 $f(x) = x^7 + ax + b \in \mathbb{Z}[x]$. 若 $a \equiv 15$ 模 72，且 $b \equiv 12$ 模 72，则根据定理 1.1、1.5 和 1.7，我们有 $i(K) = 1$

现在给出一些非单生成数域的例子。

例 1.10。 设 $K = \mathbb{Q}(\theta)$，其中 θ是 $f(x) = x^7 + 17x + 51$的一个根。注意， $f(x)$ 关于 17 满足艾森斯坦判别法，因此它在 $\mathbb{Q}$上不可约。所以，根据推论 1.6 K 是非单生成的。

例 1.11。 设 $K = \mathbb{Q}(\theta)$，其中 θ 满足 $f(x) = x^7 + 7x + 56$。容易看出， $f(x)$ 是 7-艾森斯坦多项式。因此，根据推论 1.4 K 是非单生成的。

2. Preliminary Results

设 $K = \mathbb{Q}(\theta)$ 是一个代数数域，其中 θ 是属于 $f(x)$ 的首一不可约多项式的一个根 $\mathbb{Z}[x]$。下文中， $\mathbb{O}_K$ 表示 K的代数整数环。对于有理素数 p，令 $\mathbb{F}_p$ 表示含有 p 个元素的有限域。以下引理（参见 [17, 定理 2。2]）将在定理 1.1、1.5 和 1.7的证明中发挥重要作用。

引理 2.1. 设 K 是一个代数数域， p 是一个有理素数。那么， p 是 K 的公共指数因子，当且仅当存在某个正整数 h，使得 $\mathbb{O}_K$ 中位于 p 之上且剩余次数为 h的不同素理想的个数，大于 $\mathbb{F}_p[x]$中次数为 h 的首一不可约多项式的个数。

我们先介绍高斯赋值、 ϕ-牛顿多边形和二阶牛顿多边形的概念，其中 $\phi(x)$ 是一个属于 $\mathbb{Z}_p[x]$ 且在 $\mathbb{F}_p$上不可约的首一多项式，具有 $\overline{\phi}(x)$。

定义 2.2. 有理函数域 $\mathbb{Q}_p(x)$ 关于不定元 x 的高斯赋值，它扩张了 $\mathbb{Q}_p$ 上的赋值 v_p ，并定义在 $\mathbb{Q}_p[x]$ 上如下：

$$v_{p,x}(\ a_0 + a_1x + a_2x^2 + ... + a_sx^s) = \min\{v_p(a_i), 1 \leq i \leq s\}, a_i \in \mathbb{Q}_p.$$

定义 2.3. 设 p 为有理素数。设 $\phi(x) \in \mathbb{Z}_p[x]$为模 p 不可约的首一多项式，且 $f(x) \in \mathbb{Z}_p[x]$ 为不能被 $_n\phi(x)$ 整除的首一多项式。设 $\sum_{i=0} a_i(x)\phi(x)^i$ ，其中 deg $a_i(x) <$ deg $\phi(x)$， $a_n(x) \neq 0$ 为 $\phi(x)$-展开式，将其除以

$f(x)$ 后得到，该过程依次除以 $\phi(x)$ 的各次幂。设 P_i 表示平面上坐标为 $(i,v_{p,x}(a_{n-i}(x)))$ 的点，其中 $a_{n-i}(x)\neq 0, 0\leq i\leq n$。若 $a_{n-i}(x)a_{n-j}(x)\neq 0$，则设 μ_{ij} 为连接点 P_i 与 P_j 的直线的斜率。设 i_1 为不超过 n 的最大正指数，使得

$$\mu_{0i_1}=\min\{\ \mu_{0j}\mid 0<j\leq n,\ a_{n-j}(x)\neq 0\}.$$

若 $i_1<n$，令 i_2 为满足 $i_1<i_2\leq n$ 的最大指数，其中

$$\mu_{i_1i_2}=\min\{\ \mu_{i_1j}\mid i_1<j\leq n,\ a_{n-j}(x)\neq 0\}$$

依此类推。关于 p 的 ϕ-牛顿多边形 $\mathbb{N}(x)$ 是由线段 $P_0P_{i_1}$、$P_{i_1}P_{i_2}$、.....、$P_{i_{k-1}}P_{i_k}$ 组成的折线路径，其中 $i_k=n$。这些线段称为 ϕ-牛顿多边形的边，其斜率构成严格递增的序列；由于 $f(x)$ 是一个系数属于 $\mathbb{Z}_p$的首一多项式，这些斜率均为非负数。

定义 2.4。设 $\phi(x)\in\mathbb{Z}_p[x]$ 是一个模有理素数 p 不可约的首一多项式，并且在 $\mathbb{Q}_p$的代数闭包 $\mathbb{Q}_p$ 中有一个根 α。设 $f(x)\in\mathbb{Z}_p[x]$ 是一个不被 $\phi(x)$ 整除的首一多项式，其 $\phi(x)$-展开为 $\phi(x)^n+a_{n-1}(x)\phi(x)^{n-1}+\cdots+a_0(x)$，使得 $\overline{f}(x)$ 是 $\overline{\phi}(x)$ 的幂。假设 $f(x)$ 的 ϕ-牛顿多边形仅由一条边组成，记为 S，其正斜率记作 $\frac{l}{e}$，其中 l、e 互素，即

$$\min\left\{\frac{v_{p,x}(a_{n-i}(x))}{i}\ \mid\ 1\leq i\leq n\right\}=\frac{v_{p,x}(a_0(x))}{n}=\frac{l}{e}$$

因此 n 可被 e 整除，记作 $n=et$ 和 $v_{p,\,x}(a_{n-ej}(x))\geq lj$，其中 $1\leq j\leq t$。于是，多项式 $b_j(x):=\frac{a_{n-ej}(x)}{\phi(x)^{n-lj}}$ 的系数属于 $\mathbb{Z}_p$，因此 $b_j(\alpha)\in\mathbb{Z}_p[\alpha]$，其中 $1\leq j\leq t$。$_t$以不定元 Y 定义的多项式 $T(Y)$ 为 $f(x)$ 关于 (ϕ,S) 的剩余多项式，其$_{j=1}$系数属于 $\mathbb{F}_p[\overline{\alpha}]\cong\frac{\mathbb{F}_p[x]}{\langle\phi\ x\ \rangle}$()。

下述定义给出了当 $f(x)$ 更一般时剩余多项式的概念。

定义 2.5. 设 $\phi(x)$ α 如定义 2.4 所述。设 $g(x)\in\mathbb{Z}_p[x]$ 为一个不能被 $\phi(x)$ 整除的首一多项式，且 $\overline{g}(x)$ 是 $\overline{\phi}(x)$ 的幂。设 $\lambda_1<\cdots<\lambda_k$ 为 $g(x)$ 的 ϕ-牛顿多边形各边的斜率，并令 S_i 表示斜率为 λ_i的边。根据 Ore 证明的一个经典结果（参见 [3, 定理 1.5], [13, 定理 1.1]），可将 $g(x)$ 写为 $=g_1(x)\cdots g_k(x)$，其中 $g_i(x)\in\mathbb{Z}_p[x]$的 ϕ-牛顿多边形只有一条边，记为 S_i'，它是 S_i的平移。令属于 $\mathbb{F}_p[\overline{\alpha}][Y]$的 $T_i(Y)$ 表示 $g_i(x)$ 关于 $(\phi,\ S_i')$ 的剩余多项式，其定义如定义 2.4 所述。为方便起见，将多项式 $T_i(Y)$ 称为 $g(x)$ 关于 (ϕ,S_i) 的剩余多项式。若多项式 $g(x)$ 的所有多项式 $T_i(Y)$ 在 $\mathbb{F}_p$, $1\leq i\leq k$的代数闭包中均无重根，则称其关于 ϕ 是 p-正则的。一般而言，若属于 $\mathbb{Z}_p[x]$ 的 $F(x)$ 是首一多项式，且 $\overline{f}(x)=\overline{\phi}_1(x)^{e_1}\cdots\overline{\phi}_r(x)^{e_r}$ 是其模 p 分解为不可约多项式所得的因式分解，其中

每个属于 $\mathbb{Z}_p[x]$ 的 $\phi_i(x)$ 都是首一的，且 $e_i > 0$，则根据亨泽尔引理，存在属于 $\mathbb{Z}_p[x]$ 的首一多项式 $f_1(x) \cdots, f_r(x)$，使得 $f(x) = f_1(x) \cdots f_r(x)$，并且对每个 i，都有 $\overline{f}_i(x) = \overline{\phi}_i(x)^{e_i}$。若多项式 $f(x)$ 的每个 $f_i(x)$ 都关于 ϕ_i是 p-正则的，则称该多项式关于 $\phi_1, \cdots, \phi_r$是 p-正则的。

为了确定位于有理素数 $\mathbb{O}_K$ 之上的不同素理想p的个数，我们将使用二阶牛顿多边形以及以下定理；该定理是 [13]中的定理 1.2 的一个较弱版本。

定理 2.6. 设 $L = \mathbb{Q}(\xi)$ 是一个代数数域，其 ξ 满足不可约多项式 $g(x) \in \mathbb{Z}[x]$，且 p 是一个有理素数。设 $\overline{\phi}_1(x)^{e_1} \cdots \overline{\phi}_r(x)^{e_r}$ 是 $g(x)$ 模 p 的分解，分解为 $\mathbb{F}_p$上的互异不可约多项式的幂，其中每个 $\phi_i(x) \neq g(x)$ 属于 $\mathbb{Z}[x]$ 首一多项式。假设 ϕ_i-牛顿多边形 $g(x)$ 有 k_i 条边，记为 S_{ij}，其斜率为 $\lambda_{ij} = \frac{l_{ij}}{e_{ij}}$，且对 $1 \leq j \leq k_i$，$\gcd(l_{ij}, e_{ij}) = 1$。若 $T_{ij}(Y) = \prod U_{ijs}(Y)$ 是剩余多项式 $T_{ij}(Y)$ 关于 (ϕ_i, S_{ij}) 的分解，分解为 $\mathbb{F}_p$ 上的互异$_{s=1}$不可约因子，其中 $1 \leq j \leq k_i$，则

$$p\mathbb{O}_L = \prod_{i=1}^{r} \prod_{j=1}^{k_i} \prod_{s=1}^{s_{ij}} \mathfrak{p}_{ijs}^{e_{ij}},$$

其中 $\mathfrak{p}_{ijs}$ 是 $\mathbb{O}_L$ 中剩余次数为 $\deg \phi_i(x) \times \deg U_{ijs}(Y)$ 的不同素理想。

设 $L = \mathbb{Q}(\gamma)$，其中 γ 是首一多项式 $g(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$，$a_0 \neq 0$ 的一个根。设 p 是满足 $g(x) \equiv x^n (p)$ 的素数。假设 $g(x)$ 的 p-牛顿多边形由一条斜率为正的边组成，其斜率为 $\lambda = \frac{l}{e}$，其中 $\gcd(l, e) = 1$。设 $g(x)$ 的剩余多项式 $T_g(Y) \in \mathbb{F}_p[Y]$ 是域 $\mathbb{F}_p$ 上首一不可约多项式 $\psi(Y)$ 的幂，即 $T_g(Y) = \psi(Y)^s$ 属于 $\mathbb{F}_p[Y]$，其中 $s \geq 2$。在这种情形下，我们构造一个与斜率 λ 相对应的关键多项式 $\Phi(x)$，使其满足以下条件：

(i) $\Phi(x)$ 同余于 x 的一个幂模 p。(ii) $\Phi(x)$ 的一阶 p-牛顿多边形是斜率为 λ 的单边形。(iii) 关于 p 的 $\Phi(x)$ 的剩余多项式是 $\mathbb{F}_p[Y]$ 中的 $\psi(Y)$。(iv) $\deg \Phi(x) = e \deg \psi(Y)$。

如[8, 第 2 节2], 所述，数据（x； λ， ψ（Y））确定了域 $\mathbb{Q}_p$（x）的一个 p-进赋值 V，该赋值满足以下性质：

（i） V（x）$= l$，其中 $\lambda = \frac{l}{e}$，且 $\gcd$（l， e）$= 1$。

(ii) 如果 $p(x) = \sum b_i x^i \in \mathbb{Z}_p[x]$ 是任意多项式，那么$_{0 \leq i}$

$$V(p(x)) = e \min_{0 \leq i} \{v_p(b_i) + i\lambda\} \tag{2.1}$$

我们将上述赋值 V 定义为二阶赋值。

若 $g(x)=\sum_{i=0}^{u} a_i(x)\Phi(x)^i \in \mathbb{Z}_p[x]$ 是 Φ-进展开式，表示 $g(x)$，则牛顿多边形相对于 V 的 $g(x)$（也称为 $g(x)$的二阶 V-牛顿多边形）是欧几里得平面上点集 $(i, V(a_{u-i}(x)\Phi(x)^i))$ 的下凸包。

设 $g(x)$的二阶 V-牛顿多边形有 k条边 E_1、$\cdots$、E_k，其正斜率分别为 λ_1、$\cdots$、λ_k。设 $\lambda_t=\frac{l_t}{e_t}$满足 $\gcd(l_t, e_t)=1$，并令 $[a_t, b_t]$ 表示斜率为 λ_t 的边在水平轴上的投影，其中 $1\le t\le k.$。那么，每条边 E_t都自然对应一个二阶剩余多项式 $\psi_t(Y)$，其次数与该边的次数一致（即$\frac{b_t-a_t}{e_t}$）[8, 第2节。只有位于边上的 $g(x)$的 V-牛顿多边形的整点，才会决定该二阶剩余多项式的非零系数。若附属于 $g(x)$的二阶 V-牛顿多边形中边 E_t 所对应的二阶剩余多项式 $\psi_t(Y)$在 $\frac{\mathbb{F}_p[Y]}{\langle\psi\ Y\rangle}$( )中可分，则称 $g(x)$为 ψ_t-正则。若对每个 t、$1\le t\le k$，$g(x)$均为 ψ_t-正则，则称 $g(x)$为 V-正则。此外，若每个剩余多项式 $\psi_t(Y)$、$t\in\{1,\ 2,\cdots,k\}$在 $\frac{\mathbb{F}_p[Y]}{\langle\psi\ Y}$( )$\rangle$ 中均不可约，则每个 $\psi_t(Y)$都给出一个素理想，其剩余次数为 $\deg\ \psi\cdot\deg\psi_t$，分歧指数为 $e\cdot e_t$。

3. Proof of Theorems 1.1, 1.5 and 1.7.

定理 1.1 的证明。若 2 是 K 的公共指数因子，则 $2\mid D$，即 $2\mid b$。情形 A1：$a\equiv 1$ 模 2，$b\equiv 0$ 模 2。在这种情形下，$f(x)\equiv x(1+x+x^2)^2(x+1)^2$模 2。令 $\phi_1(x)=x$、$\phi_2(x)=1+x+x^2$，且 $\phi_3(x)=x+1$。$f(x)$ 的 ϕ_1-牛顿多边形只有一条边，连接点 (0, 0) 与 (7, $v_2(b)$)。与这条边对应的剩余多项式是线性的。因此，ϕ 给出一个剩余次数为 1 的素理想，记为 $\mathfrak{p}_1$。所以

$$2\mathbb{O}_K=\mathfrak{p}_1\mathfrak{P},\ \text{where } \mathfrak{P} \text{ is an ideal of } \mathbb{O}_K \tag{3.1}$$

利用定理 2.6，可知 ϕ_2 给出剩余次数为 2 的倍数的素理想。因此，考虑到引理 2.1，$2\mid i(K)$ 当且仅当 ϕ_2 且 ϕ_3 至少给出两个剩余次数为 t 的素理想，其中 $t\in\{1,2\}$。对于 ϕ_i，当 $i=2$ 时，对$f(x)$ 作 3 进展开为

$$(x-3)\phi_2^3+(3x+5)\phi_2^2-(4x+2)\phi_2+b+x(a+1) \tag{3.2}$$

$$\phi_3^7-7\phi_3^6+21\phi_3^5-35\phi_3^4+35\phi_3^3-21\phi_3^2+(a+7)\phi_3+(b-a-1) \tag{3.3}$$

ϕ_2-牛顿多边形 $f(x)$ 是由点 (0, 0)、(1, 0)、(2, 1) 和 (3, $\min\{v_2(b)\ v_2(a+1)\}$) 构成的下凸包，而 ϕ_3-牛顿多边形 $f(x)$ 是由点 (0, 0)、(1, 0)、(2, 0)、(3, 0)、(4, 0)、(5, 0)、(6, $v_2(a+7)$) 和 (7, $v_2(b-a-1)$) 构成的下凸包。

设 $a\equiv 3$ 模 4，且 $b\equiv 2$ 模 4，则 $v_2(a+1)\ge 2$。对于每个 $i=2$，3，ϕ_i-牛顿多边形 $f(x)$ 只有一条斜率为 $_{1\,2}$ 的边。与这条边相关联的剩余多项式是线性的。因此 ϕ_2 给出一个素理想，记作 $\mathfrak{p}_2$，其剩余次数为 2；而 ϕ_3 给出一个素理想，记作 $\mathfrak{p}_3$，其剩余次数为 1。因此根据定理 2.6，$\mathfrak{P}=\mathfrak{p}_2^2\mathfrak{p}_3^2$。因此 $2\nmid i(K)$。

设 $a \equiv 3$ 模 8，且 $b \equiv 0$ 模 8，则对于每个 $i = 2$，3，ϕ_i-牛顿多边形 $f(x)$ 只有一条正斜率边。$f(x)$ 的与这条边相关联的剩余多项式，关于 ϕ_2，是在 $\frac{\mathbb{F}_2[x]}{\langle \phi_2\ x \rangle}()\rangle$ 上的 $(Y-(x+1))(Y-1)$；关于 ϕ_3，则是$Y^2+Y+\bar{1} \in F_2[Y].$。因此 $\mathfrak{P} = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$，其中对于每个 $\mathfrak{p}_i$，$i = 2$ 为 3、4 时，其剩余次数均为 2。因此 $2 \mid i(K)$。

设 $a \equiv 7$ 模 8 且 $b \equiv 0$ 模 8。那么对于每个 $i = 2$，3，$f(x)$ 的 ϕ_i-牛顿多边形有两条正斜率边。与每条边对应的 $f(x)$ 的剩余多项式都是线性的。因此 $\mathfrak{P} = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5$，其中每个 $\mathfrak{p}_2$、$\mathfrak{p}_3$ 的剩余次数为 2，而 $\mathfrak{p}_4$、$\mathfrak{p}_5$ 的剩余次数为 1。于是 $2 \mid i(K)$。

设 $a \equiv 3$ 模 8 且 $b \equiv 4$ 模 8。那么 $f(x)$ 的 ϕ_2-牛顿多边形只有一条正斜率边。相对于 ϕ_2，与这条边对应的 $f(x)$ 的剩余多项式在 $\frac{\mathbb{F}_2[x]}{\langle \phi_2\ x \rangle}()\rangle$ 上为 $Y^2 + xY + 1$。$f(x)$ 的 ϕ_3-牛顿多边形有两条正斜率边。与每条边对应的 $f(x)$ 的剩余多项式都是线性的。因此 $\mathfrak{P} = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$，其中 $\mathfrak{p}_2$ 的剩余次数为 4，而 $\mathfrak{p}_3$、$\mathfrak{p}_4$ 的剩余次数为 1。因此 $2 \mid i(K)$。

设 $a \equiv 7$ 模 8，且 $b \equiv 4$ 模 8。则 ϕ_2- $f(x)$ 的牛顿多边形只有一条正斜率的边。相对于 ϕ_2，与这条边相关联的 $f(x)$ 的剩余多项式为 Y^2+xY+x，其在 $\frac{\mathbb{F}_2[x]}{\langle \phi_2\ x \rangle}()\rangle$ 上。$f(x)$ 的 ϕ_3- 牛顿多边形只有一条正斜率的边。与这条边相关联的 $f(x)$ 的剩余多项式为 $Y^2 + Y + \bar{1}$。因此 $\mathfrak{P} = \mathfrak{p}_2\mathfrak{p}_3$，其中 $\mathfrak{p}_2$ 和 $\mathfrak{p}_3$ 的剩余次数分别为 4 和 2。故 $2 \nmid i(K)$。

设 $a \equiv 1$ 模 4，且 $b \equiv 0$ 模 2。则 ϕ_2-牛顿多边形 $f(x)$ 只有一条斜率为 $_1\ _2$ 的边。因此 ϕ_2 给出一个素理想，例如 $\mathfrak{p}_2$，其剩余次数为 1。因此利用 (3.1)，可得

$$2\mathbb{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{I}, \qquad \text{where } \mathfrak{I} \text{ is an ideal of } \mathbb{O}_K. \tag{3.4}$$

显然，$2 \mid i(K)$成立，当且仅当 ϕ_3 给出两个剩余次数各为 2 的素理想，或至少给出一个剩余次数为 1 的素理想。

若 $a \equiv 1$ 模 4 且 $b \equiv 0$ 模 4，则 ϕ_3 给出一个剩余次数为 1 的素理想，记为 $\mathfrak{p}_3$。因此，$\mathfrak{I} = \mathfrak{p}_3^2$。所以，$2 \mid i(K)$。

可以观察到，若 $a \equiv 1$ 模 4，$b \equiv 2$ 模 4，$v_2(b-a-1) < 2v_2(a+7)$ 且$v_2(b-a-1)$为偶数，则 ϕ_3-牛顿多边形只有一条正斜率边，其剩余多项式不含平方因子，因此我们可以找到某个有理数 μ，使得 $f(x)$是 $x-\mu$ 正则的。

设 $a \equiv 1$ 模 4 且 $b \equiv 2$ 模 4，并取$\mu = \frac{-7b}{6a}$，则 $v_2(\mu) = 0$。设 $\phi_3(x) = x-\mu$，则 $f(x)$的 ϕ_3 展开式为

$$\phi_3^7 + 7\mu\phi_3^6 + 21\mu^2\phi_3^5 + 35\mu^3\phi_3^4 + 35\mu^4\phi_3^3 + 21\mu^5\phi_3^2 + f'(\mu)\phi_3 + f(\mu) \tag{3.5}$$

简单计算可得，$f(\mu) = \frac{-Db}{6^7a^7}$且 $f'(\mu) = \frac{D}{6^6a^6}$。显然，$v_2(f(\mu)) = v_2(f'(\mu)) = v_2(D) - 6$。容易验证，$v_2(D) - 6 \geq 1$。若 $v_2(D)$ 为奇数，则ϕ_3- $f(x)$ 的牛顿多边形有一条正斜率边，连接点 (5, 0) 和 (7, $v_2(D) - 6$)。因此，ϕ_3 给出一个剩余次数为 1 的素理想，记作 $\mathfrak{p}_3$。所以$\mathfrak{I} = \mathfrak{p}_3^2$，从而 $2 \mid i(K)$。

如果 $v_2(D)$ 是偶数，那么 $f(x)$ 不是 $x-\mu$ 正则的。因此我们选择另一个有理数。

这里有 $a\equiv 1$ 模 4、$b\equiv 2$ 模 4，且 $v_2(D)$ 为偶数。取 $u=\frac{v_2(D)}{2}-6$ 并定义 $\rho=2^u-\mu$，则 $v_2(\rho)=0$。令 $\phi_3(x)=x-\rho$。$f(x)$ 的 ϕ_3 展开式为

$$\phi_3^7+7\rho\phi_3^6+21\rho^2\phi_3^5+35\rho^3\phi_3^4+35\rho^4\phi_3^3+21\rho^5\phi_3^2+f'(\rho)\phi_3+f(\rho) \tag{3.6}$$

可以验证，$v_2(f(\rho))\geq 2u+1$ 和 $v_2(f'(\rho))=u+1$。如果 $v_2(f(\rho))=2u+1$，那么 ϕ_3 给出一个剩余次数为 1 的素理想，例如 $\mathfrak{p}_3$。因此 $\mathfrak{I}=\mathfrak{p}_3^2$。所以 $2\mid i(K)$。如果 $v_2(f(\rho))=2u+2$，那么 ϕ_3 给出一个剩余次数为 2 的素理想，例如 $\mathfrak{p}_3$。因此 $\mathfrak{I}=\mathfrak{p}_3$。所以 $2\nmid i(K)$。如果 $v_2(f(\rho))\geq 2u+3$，那么 ϕ_3 给出两个剩余次数各为 1 的素理想，例如 $\mathfrak{p}_3$ 和 $\mathfrak{p}_4$。因此 $\mathfrak{I}=\mathfrak{p}_3\mathfrak{p}_4$。所以 $2\mid i(K)$

情形 A2：$a\equiv 0$ 模 2，$b\equiv 0$ 模 2。此处 $f(x)\equiv x^7$ 模 2。$f(x)$ 的 x-牛顿多边形是由点 (0, 0)、(6, $v_2(a)$) 和 (7, $v_2(b)$) 构成的下凸包。

令 $7v_2(a)>6v_2(b)$，则由 (1.2)，$v_2(b)<7$。$f(x)$ 的 x-牛顿多边形只有一条斜率为正的边 $\frac{v_2(b)}{7}$。与这条边对应的剩余多项式是线性的。因此 $2\mathbb{O}_K=\mathfrak{p}^7$。于是 $2\nmid i(K)$。

对于剩余情形，令 $7v_2(a)<6v_2(b)$。则由 (1.2)，我们有 $1\leq v_2(a)\leq 5$。$f(x)$ 的 x-牛顿多边形有两条斜率为正的边。第一条边，记作 S_1，是连接点 (0, 0) 与 (6, $v_2(a)$) 的线段，斜率为 $\frac{v_2(a)}{6}$。第二条边，记作 S_2，是连接点 ($\overline{6,\ v_2(a)}$) 与 (7, $v_2(b)$) 的线段。与边 S_2 对应的剩余多项式是线性的。因此 S_2 给出一个剩余次数为 1 的素理想，记作 $\mathfrak{q}$。于是

$$2\mathbb{O}_K=\mathfrak{R}\mathfrak{q},\ \text{where } \mathfrak{R} \text{ is an ideal of } \mathbb{O}_K \tag{3.7}$$

若 $v_2(a)\in\{1,5\}$，则 S_1 给出一个素理想，例如 $\mathfrak{p}_1$，其剩余次数为 1。因此 $\mathfrak{R}=\mathfrak{p}_1^6$。于是 $2\nmid i(K)$。

若 $v_2(a)=3$，则与 S_1 相关联的剩余多项式为 $(Y+\bar{1})(Y^2+Y+\bar{1})$。因此 $\mathfrak{R}=\mathfrak{p}_1^2\mathfrak{p}_2^3$，其中 $\mathfrak{p}_1$ 和 $\mathfrak{p}_2$ 的剩余次数分别为 1 和 2。于是$2\nmid i(K)$。

若 $v_2(a)=2$，则 $\lambda=\frac{1}{3}$，且与 S_1 相关联的剩余多项式为 $(Y+\bar{1})^2$，，即剩余多项式不是无平方因子的。令 $\psi(Y)=Y+\bar{1}$, $h=1$ 和 $e=3$。由于 $e>1$，对于 $2\mathbb{O}_K$的素理想分解，我们将使用高阶牛顿多边形。取$\Phi(x)=x^3+2$，则 $\Phi(x)$ 是附属于数据 (x, $\lambda,\psi(Y)$) 的关键多项式。如 (2.1) 中所示，我们可以定义二阶赋值 V，使得 $V(\Phi)=3$, $V(x)=1$ 且$V(2)=3$。$\Phi(x)$ 对 $f(x)$ 的展开为

$$f(x)=x\Phi^2(x)-4x\Phi(x)+(a+4)x+b \tag{3.8}$$

Φ-牛顿多边形的二阶 $f(x)$是点 (0, 7)、(1, 10) 和 (2, v) 的下凸包，其中 $v=\min\{3v_2(b),\ 3v_2(a+4)+1\}$。由于 $v_2(a)=2$，我们有 $v_2(b)\geq 3$。

若 $a\equiv 4$ 模 16 且 $b\equiv 0$ 模 16，则 $v=10$。$f(x)$ 的 Φ-牛顿多边形二阶情形只有一条边，且与该边对应的剩余多项式是线性的。

因此， $\mathfrak{R}=\mathfrak{p}_1^6$，其中 $\mathfrak{p}_1$ 的剩余次数为 1。于是 $2\nmid i(K)$。
如果 $a\equiv 12$ 模 16 且 $b\equiv 16$ 模 32，则 $v=12$。$f(x)$ 的二阶 Φ-牛顿多边形只有一条边，其剩余多项式是线性的。因此， $\mathfrak{R}=\mathfrak{p}_1^6$，其中 $\mathfrak{p}_1$ 的剩余次数为 1。于是 $2\nmid i(K)$

如果 $a\equiv 12$ 模 32 且 $b\equiv 0$ 模 32，则 $v=13$，那么 $f(x)$ 的二阶 Φ-牛顿多边形只有一条边，且附属于这条边的剩余多项式为 $Y^2+Y+\bar{1}$。因此， $\mathfrak{R}=\mathfrak{p}_2^3$，其中 $\mathfrak{p}_2$ 的剩余次数为 2。于是 $2\nmid i(K)$。

如果 $a\equiv 28$ 模 32 且 $b\equiv 0$ 模 32，则 $v>13$，那么 $f(x)$ 的二阶 Φ-牛顿多边形有两条正斜率的边。附属于每条边的剩余多项式都是线性的。因此， Φ 给出两个素理想，记为 $\mathfrak{p}_1$ 和 $\mathfrak{p}_2$，其剩余次数均为 1。因此 $\mathfrak{R}=\mathfrak{p}_1^3\mathfrak{p}_2^3$。于是 $2\mid i(K)$。

注意，若 $v_2(b)=3$，则 $f(x)$ 的二阶 Φ-牛顿多边形只有一条边。与这条边对应的剩余多项式没有无平方因子。因此我们将使用另一个关键多项式。

令 $v_2(b)=3$ 并取 $\Phi(x)=x^3+2x+2$。则 $\Phi(x)$ 是与 $(x,{}_{13},\psi(Y))$ 对应的关键多项式。令 V与上文给出的一致。 $f(x)$ 的 $\Phi(x)$ 展开为

$$f(x)=x\Phi^2(x)+(4-4x-4x^2)\Phi(x)+(b-8+(a-4)x+8x^2) \tag{3.9}$$

$f(x)$ 的二阶 Φ-牛顿多边形是由点 (0, 7)、(1, 9) 和 (2, w) 构成的下凸包，其中 $w=V(b-8+(a-4)x+8x^2)$。
若 $a\equiv 12$ 模 16 且 $b\equiv 8$ 模 16，则 $w=10$。 Φ 给出一个素理想，记作$\mathfrak{p}_1$，其剩余次数为 1。因此，$\mathfrak{R}=\mathfrak{p}_1^6$。于是 $2\nmid i(K)$。
如果 $a\equiv 4$ 模 16 且 $b\equiv 8$ 模 16，那么 $w=11$，于是 Φ 给出一个剩余次数为 2 的素理想，记作$\mathfrak{p}_1$。因此， $\mathfrak{R}=\mathfrak{p}_1^3$。从而 $2\nmid i(K)$。

设 $v_2(a)=4$，则 $v_2(b)\geq 5$、$\lambda=\frac{2}{3}$、$h=2$ 以及 $e=3$。取 $\Phi(x)=x^3+4$。在 (2.1) 中定义的二阶赋值 V满足 $V(\Phi)=6$、$V(x)=2$ 以及$V(2)=3$。 $f(x)$ 的 $\Phi(x)$ 展开式为

$$x\Phi^2(x)-8x\Phi(x)+(a+16)x+b \tag{3.10}$$

设 $w'=\min\{3v_2(b)\ 3v_2(a+16)\ +2\})$，则 $w'\geq 15$。 $f(x)$ 的 Φ-牛顿多边形（二阶）是点 (0, 14)、(1, 17) 和 (2, w') 的下凸包。
若 $a\equiv 16$ 模 32 且 $b\equiv 32$ 模 64，则 $w'=15$。 Φ 给出一个剩余次数为 1 的素理想，记作$\mathfrak{p}_1$。因此，$\mathfrak{R}=\mathfrak{p}_1^6$。故 $2\nmid i(K)$。
若 $a\equiv 16$ 模 64 且 $b\equiv 0$ 模 128，则 $w'=17$。因此， $f(x)$ 的二阶 Φ-牛顿多边形只有一条正斜率的边。与这条边对应的剩余多项式是线性的。因此 $\mathfrak{R}=\mathfrak{p}_1^6$。故 $2\nmid i(K)$。

若 $a\equiv 48$ 模 64 且 $b\equiv 0$ 模 128，则 $w'=20$。因此， $f(x)$ 的二阶 Φ-牛顿多边形只有一条正斜率的边。与这条边对应的剩余多项式是 $Y^2+Y+\bar{1}$。因此 $\mathfrak{R}=\mathfrak{p}_1^3$。故 $2\nmid i(K)$。

若 $a\equiv 16$ 除以 64 的余数为 $b\equiv 64$，且 $w'=17$ 除以 128 的余数为 $\mathfrak{R}=\mathfrak{p}_1^6$，则 $2\nmid i$。因此 K。故 $a\equiv 48($ $b\equiv 64)$。若 $w'=18$ 除以 64 的余数为 Φ，且 x 除以 128 的余数为 $=x^3+4x+4$，则 。因此，取 () 。Th e

Φ (f) 的展开式为

$$x\Phi^2(x)-(8x+4x^2)\Phi(x)+b-64+x(a-48)+32x^2 \tag{3.11}$$

$f(x)$ 的二阶 Φ-牛顿多边形是由点 (0, 14)、(1, 16) 和 (2, 19) 构成的下凸包。因此， Φ 提供两个素理想，分别记为 $\mathfrak{p}_1$ 和 $\mathfrak{p}_2$ ，它们的剩余次数均为 1。因此 $\mathfrak{R}=\mathfrak{p}_1^3\mathfrak{p}_2^3$。于是 $2\mid i(K)$。定理得证。□

定理*1.5*的证明若 $3\mid i(K)$，则利用 (1.1) 和 (1.3)，可得 $3\mid b$。
情形B1：设 $a\equiv 0$ 模 3 且 $b\equiv 0$ 模 3，则 $f(x)\equiv x^7$ 模 3。 $f(x)$ 的 x-牛顿多边形是由点 (0, 0)、(6, $v_3(a)$) 和 (7, $v_3(b)$) 构成的下凸包。若 $7v_3(a)>6v_3(b)$，则 x 提供一个剩余次数为 1 的素理想。因此 $3\mathbb{O}_K=\mathfrak{p}^6$。

设 $7v_3(a)<6v_3(b)$。则 x-牛顿多边形是点 (0, 0)、(6, $v_3(a)$) 和 (7, $v_3(b)$) 的下凸包，它有两条斜率为正的边。第一条边 S_1 是连接点 (0, 0) 和 (6, $v_3(a)$) 的线段。第二条边 S_2是连接点 (6, $v_3(a)$) 和 (7, $v_3(b)$) 的线段。与边 S_2 对应的剩余多项式是线性的。因此，对于某个 $\mathbb{O}_K$ 的理想 $\mathfrak{L}$ ，有 $3\mathbb{O}_K=\mathfrak{L}\mathfrak{q}$。利用 (1.2) 和 $7v_3(a)>6v_3(b)$，我们有 $v_3(b)\in\{1,2,3,4,5\}$.

如果 $v_3(a)\in\{1,5\}$，那么 S_1 给出一个剩余次数为 1 的素理想，记为 $\mathfrak{p}_1$ 。因此 $\mathfrak{L}=\mathfrak{p}_1^6$。
如果 $v_3(a)\in\{2,4\}$，那么与 S_1 对应的剩余多项式为 $(Y-\bar{1})(Y+\bar{1})$。因此$\mathfrak{L}=\mathfrak{p}_1^3\mathfrak{p}_2^3$。

令 $v_2(a)=3$，则与 S_1 相关联的剩余多项式为 $(Y+\delta)^2$, ，其中 $\delta\in\{1,-1\}$。令 $\psi(Y)=Y+\delta$, $\lambda=\frac{1}{2}$。取 $\phi(x)=x^2+3\delta$, $h=1$ 和 $e=2$，则 $\Phi(x)$ 是附属于数据 $(x,\lambda,\psi(Y))$ 的关键多项式。式 (2.1) 中给出的 $\mathbb{Q}_2[x]$ 上的赋值 V 满足 $V(\Phi)=2, V(x)=1$ 且 $V(3)=2$。 $f(x)$ 的 $\Phi(x)$ 展开式为

$$x\Phi^3(x)-9\delta\Phi^2(x)+27x\Phi(x)+b+x(a-27\delta) \tag{3.12}$$

该 $\Phi(x)$-二阶牛顿多边形是由以下各点构成的下凸包：(0, 7)、(1, 9)、(2, 9) 和 (3, 最小值$\{2v_3(b)\ 2v_3(a-27\delta)\ +1\}$)。由于 $v_3(a)=3$，因此利用 (1.2)，可得 $v_3(b)\geq 4$.

如果 $v_3(b)=4$，那么 $f(x)$ 的 Φ-牛顿多边形有一条斜率为$_{1\,3}$的边。与这条边对应的剩余多项式是线性的。因此 $\mathfrak{L}=\mathfrak{p}_1^6$，其中 $\mathfrak{p}_1$ 的次数为 1。
如果 $v_3(b)>4$ 且 $v_3(a-27\delta)=4$，那么 $f(x)$ 的 Φ-牛顿多边形有一条斜率为$_{2\ 3}$的边。与这条边对应的剩余多项式是线性的。因此 $\mathfrak{L}=\mathfrak{p}_1^6$，其中 $\mathfrak{p}_1$ 的次数为 1。

如果 $v_3(b)=5$且 $v_3(a-27\delta)>4$，那么 $f(x)$ 的 Φ-牛顿多边形有一条边连接点 (0, 7) 和 (3, 10)，且边上有一个格点 (2, 9)。与这条边对应的剩余多项式是 $Y^3\pm Y\pm\bar{1}$，它是可分的。因此 $\mathfrak{L}=\mathfrak{p}_1^2$，其中 $\mathfrak{p}_1$ 的次数为 3。

若 $v_3(b)>5$且 $v_3(a-27\delta)>4$，则 Φ- $f(x)$ 的牛顿多边形有两条正斜率的边。与第一条边相关联的剩余多项式为 $Y^2+\bar{1}$。因此 $\mathfrak{L}=\mathfrak{p}_1^2\mathfrak{p}_2^2$。由此我们得出，当 $a\equiv 0$ 模 3 且 $b\equiv 0$ 模 3 时， $3\nmid i(K)$。

情形 B2： $a \equiv -1$ 模 3 且 $b \equiv 0$ 模 3。在此情形下， $f(x) \equiv x(x-1)^3(x+1)^3$模 3。显然， $f(x)$ 的 x-牛顿多边形给出一个剩余次数为 1 的素理想，记作 $\mathfrak{q}$ 。因此

$$3\mathbb{O}_K = \mathfrak{q}\mathfrak{J}, \text{ where } \mathfrak{J} \text{ is an ideal of } \mathbb{O}_K \tag{3.13}$$

记住引理 2.1， $3 \mid i(K)$ 当且仅当 $x-1$ 且 $x+1$ 分别提供至少三个剩余次数为 1 的素理想。令 $\phi_\delta(x) = (x+\delta)$，其中 $\delta \in \{-1, 1\}$，那么$\phi_\delta(x$展开式为 $f(x)$ 为

$$\phi_\delta^7(x) - 7\delta\phi_\delta^6(x) + 21\phi_\delta^5(x) - 35\delta\phi_\delta^4(x) + 35\delta\phi_\delta^3(x) - 21\delta\phi_\delta^2(x) + (a+7)\phi_\delta(x) + (b - \delta(a+1)) \tag{3.14}$$

$\phi_\delta(x)$- $f(x)$ 牛顿多边形是点 (0, 0)、(1, 0)、(2, 0)、(3, 0)、(4, 0)、(5, 1)、(6, $v_3(a+7)$) 和 (7, $v_3(b - \delta(a+1))$ 的下凸包。如果 $v_3(a+1) = 1$ 且 $v_3(b) > 1$，那么对于每个 $\delta \in \{-1, 1\}$， ϕ_δ 提供一个剩余次数为 1 的素理想。因此 $\mathfrak{J} = \mathfrak{p}_1^3\mathfrak{p}_2^3$。所以 $3 \nmid i(K)$。

注意，当 $v_3(a+1) = 1$ 且 $v_3(b) = 1$时，要么 $a \equiv 2 \bmod 9$，要么 $a \equiv 5 \bmod 9$。

设 $a \equiv 2 \bmod 9$， $b_3 \equiv 1 \bmod 3$ 且 $v_3(b-a-1) = 2$，则对每个 $\delta \in \{1, -1\}$， ϕ_δ-牛顿多边形 $f(x)$ 都只有一条正斜率的边，且附属于这条边的剩余多项式是线性的。因此 $\mathfrak{J} = \mathfrak{p}_1^3\mathfrak{p}_2^3$，其中 $\mathfrak{p}_1$ 和 $\mathfrak{p}_2$ 的剩余次数为 1。故 $3 \nmid i(K)$。

设 $a \equiv 2 \bmod 9$， $b_3 \equiv 1 \bmod 3$， $v_3(a+7) = 2$ 且 $v_3(b-a-1) \geq 3$。那么 ϕ_{-1} 提供一个次数为 1 的素理想。 $f(x)$ 的 ϕ_1-牛顿多边形有两条正斜率的边。第一条边是连接点 (4, 0) 和 (6, 2) 的线段。第二条边是连接点 (6, 2) 和 (7, $v_3(b-a-1)$) 的线段。附属于每条边的剩余多项式都是线性的。因此 $\mathfrak{J} = \mathfrak{p}_1^3\mathfrak{p}_2^2\mathfrak{p}_3$，其中对每个 $i = 1$， 2， 3， $\mathfrak{p}_i$ 的剩余次数为 1。故 $3 \mid i(K)$。

设 $a \equiv 2 \bmod 9$、 $b_3 \equiv 1 \bmod 3$、 $v_3(a+7) \geq 3$、 $v_3(b-a-1) \geq 3$ 和 $2v_3(a+7) > v_3(b-a-1) + 1$。那么， ϕ_{-1} 给出一个剩余次数为 1 的素理想，并且 ϕ_1- $f(x)$ 的牛顿多边形有两条正斜率边。第一条边是连接点 (4, 0) 和 (5, 1) 的线段，第二条边连接点 (5, 1) 与 (7, $v_3(b-a-1)$)。第一条边对应的剩余多项式是线性的，第二条边对应的剩余多项式是 $(Y-\bar{1})(Y+\bar{1})$ 或 $Y^2 + \bar{1}$ （分别当 $(b-a-1)_3 \equiv -1 \bmod 3$ 或 $(b-a-1)_3 \equiv 1 \bmod 3$ 时）。因此，要么 $\mathfrak{J} = \mathfrak{p}_1^3\mathfrak{p}_2^2\mathfrak{p}_3$，其中 $\mathfrak{p}_i = 1$ 的剩余次数对每个 $i = 1$ 都是 2、3 或 $\mathfrak{J} = \mathfrak{p}_1^3\mathfrak{p}_2^2\mathfrak{p}_3$，其中 $\mathfrak{p}_1$、 $\mathfrak{p}_2$ 的剩余次数为 1，而 $\mathfrak{p}_3$ 的剩余次数为 2。

设 $a \equiv 2$ 模 9、 $b_3 \equiv 1$ 模 3、 $v_3(a+7) \geq 3$、 $v_3(b-a-1) \geq 3$ 和 $2v_3(a+7) = v_3(b-a-1) + 1$。那么， ϕ_{-1} 给出一个剩余次数为 1 的素理想，而 ϕ_1 有两条正斜率边。附着于第一条边的剩余多项式是线性的，附着于第二条边的剩余多项式是 $Y^2 - Y - 1$ 或 $Y^2 + Y - 1$。因此， $\mathfrak{J} = \mathfrak{p}_1^3\mathfrak{p}_2^2\mathfrak{p}_3$，其中 $\mathfrak{p}_1$、 $\mathfrak{p}_2$ 的剩余次数为 1，而 $\mathfrak{p}_3$ 的剩余次数为 2。所以， $3 \nmid i(K)$。

设 $a \equiv 2$ 模 9， $b_3 \equiv 1$ 模 3， $v_3(a+7) \geq 3$， $v_3(b-a-1) \geq 3$ ，以及 $2v_3(a+7) < v_3(b-a-1) + 1$。则 ϕ_{-1} 给出一个剩余次数为 1 的素理想，而 ϕ_1- $f(x)$ 的牛顿多边形有三条正斜率边。第一条边是连接

点 (4, 0) 和 (5, 1) 的线段，第二条边连接点 (5, 1) 和 (6, $v_3(a+7)$)，第三条边连接点 (6, $v_3(a+7)$) 和 (7, $v_3(b-a-1)$)。每条边对应的剩余多项式都是线性的。因此，对于每个$i=1$，2，3，4，$\mathfrak{p}_i=1$的剩余次数均为 1。于是 $3\mid i(K)$。

设 $a\equiv 2$ 模 9，$b_3\equiv -1$ 模 3，且 $v_3(b+a+1)=2$，则对每个 $\delta\in\{1,-1\}$，$f(x)$ 的 ϕ_δ-牛顿多边形只有一条正斜率的边，且附属于这条边的剩余多项式是线性的。因此 $\mathfrak{J}=\mathfrak{p}_1^3\mathfrak{p}_2^3$，其中 $\mathfrak{p}_1$ 和 $\mathfrak{p}_2$ 的剩余次数为 1。故 $3\nmid i(K)$。

设 $a\equiv 2$ 模 9，$b_3\equiv -1$ 模 3，$v_3(a+7)=2$，且 $v_3(b+a+1)\geq 3$。那么 ϕ_1 给出一个次数为 1 的素理想。$f(x)$ 的 ϕ_{-1}-牛顿多边形有两条正斜率的边。第一条边是连接点 (4, 0) 和 (6, 2) 的线段。第二条边是连接点 (6, 2) 和 (7, $v_3(b-a-1)$) 的线段。附属于每条边的剩余多项式都是线性的。因此 $\mathfrak{J}=\mathfrak{p}_1^3\mathfrak{p}_2^2\mathfrak{p}_3$，其中对每个 $i=1$、2、3，$\mathfrak{p}_i$ 的剩余次数为 1。故 $3\mid i(K)$。

设 $a\equiv 2 \bmod 9$, $b_3\equiv -1 \bmod 3$, $v_3(a+7)\geq 3$, $v_3(b+a+1)\geq 3$ 和 $2v_3(a+7)>v_3(a+b+1)+1$。那么，ϕ_1 给出一个剩余次数为 1 的素理想，并且 ϕ_{-1}- $f(x)$ 的牛顿多边形有两条正斜率的边。第一条边是连接点 (4, 0) 和 (5, 1) 的线段，第二条边连接点 (5, 1) 与 (7, $v_3(b-a-1)$)。第一条边对应的剩余多项式是线性的，第二条边对应的剩余多项式是 $(Y-\bar{1})(Y+\bar{1})$ 或 $Y^2+\bar{1}$（分别对应 $(b+a+1)_3\equiv -1 \bmod 3$ 或 $(b+a+1)_3\equiv 1 \bmod 3$）。因此，要么是 $\mathfrak{J}=\mathfrak{p}_1^3\mathfrak{p}_2^2\mathfrak{p}_3$，其中 $\mathfrak{p}_i=1$ 的剩余次数对每个 $i=1$ 都为 2、3 或 $\mathfrak{J}=\mathfrak{p}_1^3\mathfrak{p}_2^2\mathfrak{p}_3$，要么是 $\mathfrak{p}_1$，其中 $\mathfrak{p}_2$ 的剩余次数为 1，而 $\mathfrak{p}_3$ 的剩余次数为 2。

设 $a\equiv 2 \bmod 9$、$b_3\equiv -1 \bmod 3$、$v_3(a+7)\geq 3$、$v_3(b+a+1)\geq 3$，以及 $2v_3(a+7)=v_3(a+b+1)+1$。则 ϕ_1 给出一个剩余次数为 1 的素理想，而 ϕ_{-1} 有两条正斜率的边。与第一条边对应的剩余多项式是线性的，与第二条边对应的剩余多项式是 Y^2-Y-1 或 Y^2+Y-1。因此 $\mathfrak{J}=\mathfrak{p}_1^3\mathfrak{p}_2^2\mathfrak{p}_3$，其中 $\mathfrak{p}_1,\mathfrak{p}_2$ 的剩余次数为 1，而 $\mathfrak{p}_3$ 的剩余次数为 2。所以，$3\nmid i(K)$。

设 $a\equiv 2 \bmod 9$、$b_3\equiv -1 \bmod 3$、$v_3(a+7)\geq 3$、$v_3(b+a+1)$，以及 $2v_3(a+7)<v_3(a+b+1)+1$。则 ϕ_{-1} 给出一个剩余次数为 1 的素理想，而 ϕ_1- $f(x)$的牛顿多边形有三条正斜率的边。第一条边是连接点 (4, 0) 和 (5, 1) 的线段，第二条边连接 (5, 1) 和 (6, $v_3(a+7)$)，第三条边连接 (6, $v_3(a+7)$) 和 (7, $v_3(b+a+1)$)。与每条边对应的剩余多项式都是线性的。因此 $\mathfrak{J}=\mathfrak{p}_1^3\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$，其中对于每个$i=1$，$\mathfrak{p}_i=1$的剩余次数均为 1，2，3，4。故 $3\mid i(K)$。

设 $a\equiv 5$ 模 9 且 $v_3(b)=1$，则 $v_3(a+7)=1$。其中，要么 ϕ_1 给出一个剩余次数为 1 的素理想，而 ϕ_{-1} 各给出两个剩余次数为 1 的素理想；要么 ϕ_1 各给出两个剩余次数为 1 的素理想，而 ϕ_{-1} 给出一个剩余次数为 1 的素理想（分别对应于 $b_3\equiv -1$ 模 3 或 $b_3\equiv 1$ 模 3）。因此 $\mathfrak{J}=\mathfrak{p}_1^3\mathfrak{p}_2^2\mathfrak{p}_3$，其中对于每个 $i=1$，2，3，$\mathfrak{p}_i$的剩余次数均为 1。因此 $3\mid i(K)$。

设 $v_3(a+1)>1$ 且 $v_3(b)=1$，则 $v_3(a+7)=1$ 且 $v_3(b-\delta(a+1))=1$。因此，对于每个 δ，ϕ_δ 给出一个剩余次数为 1 的素理想。所以 $\mathfrak{J}=\mathfrak{p}_1^3\mathfrak{p}_2^3$。

令 $v_3(a+1)>1$，$v_3(b)>1$ 且 $((a+1)_3,b_3)\in\{(-1,1),(1,-1)\}$ 模 3，于是

$v_3(b-a-1) > 1$ 且 $v_3(b+a+1) = 1$。因此， $f(x)$ 的 ϕ_{-1}-牛顿多边形有两条正斜率边，且附着于每条边的剩余多项式都是线性的。并且， ϕ_1给出了一个次数为 1 的素理想。因此 $\mathfrak{J} = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3^3$。于是 $3 \mid i(K)$。

设 $v_3(a+1) > 1$, $v_3(b) > 1$ 且 $((a+1)_3, b_3) \in \{(-1,-1), (1,1)\}$ 模 3，则$v_3(b+a+1) > 1$ 且 $v_3(b-a-1) = 1$。因此， $f(x)$ 的 ϕ_1-牛顿多边形有两条正斜率边，且每条边对应的剩余多项式都是线性的。 ϕ_{-1}给出一个次数为 1 的素理想。因此 $\mathfrak{J} = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3^3$。于是 $3 \mid i(K)$。

情形 B3： $a \equiv 1$ 模 3 且 $b \equiv 0$ 模 3。在这种情形下， $f(x) \equiv x(x^2+1)^3$ 模 3。在这种情形下， x- 给出一个剩余次数为 1 的素理想。若记 $R(\mathfrak{p})$ 为素理想 $\mathfrak{p}$ 的剩余次数，则对于 $3\mathbb{O}_K$ ，有以下几种可能。

Case	$3\mathbb{O}_K$的因式分解	剩余次数
(1)	$3\mathbb{O}_K = \mathfrak{p}_1\mathfrak{p}_2^3$	$R(\mathfrak{p}_1) = 1$ 和 $R(\mathfrak{p}_1) = 2$
(2)	$3\mathbb{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$R(\mathfrak{p}_1) = 1$, $R(\mathfrak{p}_1) = 2$ 和 $R(\mathfrak{p}_1) = 4$
(3)	$3\mathbb{O}_K = \mathfrak{p}_1\mathfrak{p}_2$	$R(\mathfrak{p}_1) = 1$ 和 $R(\mathfrak{p}_2) = 6$
(4)	$3\mathbb{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3$	$R(\mathfrak{p}_1) = 1$, $R(\mathfrak{p}_1) = 2$ 和 $R(\mathfrak{p}_1) = 2$
(5)	$3\mathbb{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$R(\mathfrak{p}_1) = 1$和 $R(\mathfrak{p}_i) = 2, i = 2, 3, 4$

表

显然，在每种情形下，剩余次数为 2 的素理想至多有 3 个。但在 $\mathbb{F}_3$. 上有 5 个次数为 2 的首一不可约多项式。因此，鉴于引理 2.13 $\nmid i(K)$，证明完成。□

定理 *1.7* 的证明。在此情形下， $5 \mid i(K$ 当且仅当 $a^7 \equiv 2b^6$ 模 5。
即 $(a, b) \in \{(0,0), (2,2), (2,-2), (3,1), (3,-1)\}$。
设 $(a, b) = (0,0)$，则 $f(x) \equiv x^7$ 模 7。若 $7v_5(a) > 6v_5(b)$，则 x- $f(x)$ 的牛顿多边形有一条正斜率的边。与这条边对应的剩余多项式是线性的。因此 $5\mathbb{O}_K = \mathfrak{p}^7$。若 $7v_5(a) < 6v_5(b)$ 且 $v_5(a) \in \{1,5\}$，则 x- $f(x)$ 的牛顿多边形有两条正斜率的边。与每条边对应的剩余多项式都是线性的。因此 $5\mathbb{O}_K = \mathfrak{p}_1^6\mathfrak{p}_2$。若 $7v_5(a) < 6v_5(b)$ 且 $v_5(a) \in \{2,4\}$，则 x- $f(x)$ 的牛顿多边形有两条正斜率的边。与第一条边对应的剩余多项式为 $(Y+\bar{1})(Y-\bar{1})$ 或 $(Y+\bar{3})(Y-\bar{2})$，与第二条边对应的剩余多项式是线性的。因此 $\mathfrak{p}_1^3\mathfrak{p}_2^3\mathfrak{p}_3$。若 $7v_5(a) < 6v_5(b)$ 且 $v_5(a) \in \{2,4\}$，则 x- $f(x)$ 的牛顿多边形有两条正斜率的边。与第一条边对应的剩余多项式为 $(Y+\bar{1})(Y^2-Y+\bar{1})$ 或 $(Y-\bar{1})(Y^2+Y+\bar{1})$，与第二条边对应的剩余多项式是线性的。因此$5\mathbb{O}_K = \mathfrak{p}_1^3\mathfrak{p}_2^3\mathfrak{p}_3$。由此 $5 \nmid i(K)$。
设 $(a, b) = (2,2)$，则 $f(x) \equiv (x+2)^2(x-1)(x^4+2x^3+4x^2+2x+2) \bmod 5$，因此$5\mathbb{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ 或 $5\mathbb{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$。于是 $5 \nmid i(K)$。
Let $(a, b) = (2\ \ -2)$，则 $f(x) \equiv (x+1)(x+3)^2(x^4+3x^2+4x^2+3x+2)$ 模 5，因此

$5\mathbb{O}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ 或 $5\mathbb{O}_K=\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$ 或 $5\mathbb{O}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$。因此 $5\nmid i(K)$。令 $(a,\ b)\ =(2,\ -2)$，则 $f(x)\ \equiv(x+1)(x+3)^2(x^4+3x^3+4x^2+3x+2)$ 模 5，因此$5\mathbb{O}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ 或 $\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3$ $5\mathbb{O}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$。因此 $5\nmid i(K)$。令 $(a,\ b)\ =(3,1)$，则 $f(x)\ \equiv(x+4)(x+3)^2(x^4+4x^3+x^2+x+2)$ 模 5，因此$5\mathbb{O}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ 或 $\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3$ $5\mathbb{O}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$。因此 $5\nmid i(K)$。令 $(a,\ b)\ =(3,\ -1)$，则 $f(x)\ \equiv(x+1)(x+2)^2(x^4+x^2+x^2+4x+2)$ 模 5，因此 $5\mathbb{O}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ 或 $\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3$ $5\mathbb{O}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$。因此 $5\nmid i(K)$。接下来我们证明 $7\nmid i(K)$。假设存在 $\mathbb{O}_K$ 的互不相同的非零素理想 $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$，使得 $7\mathbb{O}_K=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$，其中 $e_i\geq1$，则由基本等式，$e_1f_1+\cdots+e_rf_r=7$，其中 f_i 是 $i=1$ 对应的 $\mathfrak{p}_i$ 的剩余次数，2，$\cdots,r$。由于对所有 $i=1$，2，$\cdots,r$，都有 $e_i\geq1$，因此位于 7 上方的素理想至多有 7 个；但对于每个正整数 h，$\mathbb{F}_7[x]$ 中次数为 h 的首一不可约多项式的数量大于或等于 7。因此由引理 2.1，$7\nmid i(K)$。证毕。□

References

[1] S. Ahmad、T. Nakahara、A. Hameed，关于与 Hasse 问题相关的某些纯六次域，《国际代数与计算杂志》26(3)（2016），577-583。[2] S. Ahmad、T. Nakahara、S. M. Husnine，某些纯六次域的幂积分基，《国际数论杂志》10(8)（2014），2257-2265。[3] S. D. Cohen、A. Movahhedi、A. Salinier，局部域上的因式分解与广义差分多项式的不可约性，《Mathematika》47（2000），173-196。[4] H. Cohen，《计算代数数论教程》，GTM 138，Springer-Verlag Berlin Heidelberg（1993）。[5] T. Funakura，关于纯四次域的整数基，《冈山大学数学杂志》26（1984），27-41。[6] I. Ga´al、L. Remete，纯域的幂积分基与单生成性，《数论杂志》173（2017），129-146。[7] I. Ga´al，关于一族三项式单生成性的实验，《JP代数数论及其应用杂志》51(1)（2021），97-111。[8] J. Gu´ardia、J. Montes、E. Nart，代数数论中的高阶牛顿多边形，《美国数学会汇刊》364 (1)（2012），361–416。[9] A. Jakhar、S. Kumar，关于由 x^6+ax+b 定义的非单生成数域，《加拿大数学通报》（2021），即将出版。DOI:10.4153/S0008439521000825。[10] A. Jakhar、Sumandeep Kaur 和 S. Kumar，由三项式定义的某些八次数域的非单生成性，《数学讨论会》（2022），DOI: $10.4064/$cm8799-3-2022。[11] A. Jakhar、S. Kaur，关于由六次三项式导出的数域非单生成性的一则注记，（2022），DOI:10.2989/16073606.2022.2043948。[12]S. K. Khanduja，《代数数论教程》，Unitext 丛书第135卷，Springer（2022）ISBN:978-981-16-9149-2[13] S. K. Khanduja、S. Kumar，关于通过牛顿多边形的赋值延拓与多项式提升，《纯粹与应用代数杂志》216（2012），2648-2656。[14]R. MacKenzie、J. Scheuneman，一个没有相对整数基的数域，《美国数学月刊》78（1971），882-823。

[15] W. Narkiewicz，代数数初等与解析理论（第三版），施普林格数学专著，施普林格出版社，柏林，2004。[16] J. Neukirch，《代数数论》，柏林-海德堡，施普林格出版社，1999。[17] H·史密斯，根式扩张的单生成性，《算术学报》198(3)，313-327。[18] A·苏拉米、M·萨穆迪，利用相对二次扩张求六次整基，《巴拉那数学学会通报》38(4)（2020），175-180。[19] J. Montes 和 E. Nart，关于 Ore 定理，《代数杂志》146(2)（1992），318–334。[20] O·奥雷，代数数域理论中的牛顿多边形，《数学年刊》99（1928），84–117。[21] J·瓜迪亚、J. Montes 和 E. Nart，代数数论中的高阶牛顿多边形，《美国数学学会会刊》364 (1)（2012），361–416。

（ANUJ JAKHAR）Department of Mathematics, Indian Institute of Technology (IIT) Madras

（SUMANDEEP KAUR）Department of Mathematics, Panjab University Chandigarh

（SURENDER KUMAR）Department of Mathematics, Indian Institute of Technology (IIT)Bhilai