arXiv:2303.03138v1 [math.NT] 6 Mar 2023

一类数域的幂基

ANUJ JAKHAR、SUMANDEEP KAUR 和 SURENDER KUMAR

Abstract. 设 $f(x) = x^n + ax^2 + bx + c \in \mathbb{Z}[x]$ 是一个不可约多项式，满足 $b^2 = 4ac$，并设 $K = \mathbb{Q}(\theta)$ 是由其复根 θ定义的代数数域。令 $\mathbb{Z}_K$ 表示 K的代数整数环。本文旨在给出仅涉及 a、c 和 n 的必要充分条件，以判定给定素数 p 是否整除子群 $\mathbb{Z}[\theta]$ 在 $\mathbb{Z}_K$中的指标。由此，我们构造出一些单生成代数数域族。此外，当 $\mathbb{Z}_K \neq \mathbb{Z}[\theta]$ 时，我们在某些情形下明确求出指标 $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$。

1. Introduction and statements of results

若次数为 n 的代数数域 K 存在形如 $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ 的整基，其中 α. 是某个代数整数，则称该域为单生成的。这样的 K 整基称为 K的幂基。判定代数数域的单生成性是代数数论中的经典问题之一。Hasse提出了刻画单生成域的问题，这一领域至今仍是活跃的研究方向。尽管尚无标准分类，但这方面已取得了一些进展。Ga´al 和 Gr´as 对单生成域这一课题进行了广泛研究。较低次数单生成扩张的相关结果可见 Ga´al 的著作 [3]。Gr´as 在 [4]中证明，对于与 6 互素的 n，次数为 n的阿贝尔单生成域只有有限多个。代数数域 $K = \mathbb{Q}(\theta)$ 的判别式 d_K 与 $\mathbb{Z}[\theta]$ 在整数环 $\mathbb{Z}_K$ 中的指标之间，由著名公式 $D_f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 d_K$紧密联系；其中 D_f 是 θ的极小多项式$f(x)$的判别式。1878年，Dedekind 给出了一条判据，为素数 p整除 $\mathbb{Z}[\theta]$ 在 $\mathbb{Z}_K$ 中的指标提供了必要充分条件（见定理 2.4）。

设 $K = \mathbb{Q}(\theta)$ 是一个代数数域，其中 θ 满足不可约四项式$f(x) = x^n + ax^2 + bx + c \in \mathbb{Z}[x]$，且 $b^2 = 4ac$。本文运用 Dedekind 判别准则，刻画所有整除群指数 $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ 的素数。这将给出仅涉及 a、c、n 的必要充分条件，以判定 $\{1, \theta, \cdots, \theta^{n-1}\}$ 是否为 K 的整基。我们还证明，若素数 $p \nmid b$ 整除 K 的判别式 d_K，则整除 d_K 的 p 的准确幂次为一次。作为这一结果的应用，在

2010年数学主题分类。11R04；11R29。关键词和短语：代数整数环；整基与判别式；单生成数域。

推论 1.6中，我们给出一个由一类四项式定义的 d_K 的显式公式。本文最后给出一些例子，它们生成了单生成代数数域族。在某些例子中，我们还确定了指标 $[\mathbf{Z}_K : \mathbf{Z}[\theta]]$ 。

具体而言，我们证明:

定理 1.1. 设 $K = \mathbb{Q}(\theta)$ 是由不可约四项式 $f(x) = x^n + ax^2 + bx + c \in \mathbf{Z}[x]$ （其中 $b^2 = 4ac$）的一个根 θ 定义的代数数域。整除 $f(x)$ 的判别式 D_f 的素数 p 不整除 $[\mathbf{Z}_K : \mathbf{Z}[\theta]]$ ，当且仅当 p 满足以下条件之一:

(1) 若 $p \mid a$ 且 $p \mid c$，则 $p^2 \nmid c$。(2) 若 $p \mid a$ 且 $p \nmid c$，其中 p 的最高次幂整除 n 为 $r \geq 1$，则或者 $p \mid b_1$ 且 $p \nmid c_1$，或者 $p \nmid b_1[(-c_1)^n + cb_1^n]$，其中 $c_1 = {}^{c+}(_{-c\ p^r})$ 且 $b_1 = \frac{b}{p}$。(3) 若 $p \nmid a$ 且 $p \mid c$，其中 p 的最高次幂整除 $n-2$ 为 $l \geq 1$，则或者$p \mid a_1$ 且 $p \nmid b_1$，或者 $p \nmid \bar{a}_1[(-\bar{a})^{2^{1-d}} \bar{a}_1{}^{\frac{n-2}{2^d}} - (-\bar{b}_1)^{\frac{n-2}{2^d}}]$，其中 $a_1 = {}^{a+}(_{-a\ p^l})$，$b_1 = \frac{b}{p}$，且 d 根据 2 是否整除 $n-2$ 分别等于 1 或 0。(4) 若 $p = 2$ 且 $p \nmid ac$，则或者 $a \equiv 1$(模 4)，或者 $c \equiv 1$(模 4)。(5) 若 $p \nmid b$，则 $p^2 \nmid D_f$.

T以下推论是上述定理的直接推论 m.

推论 1.2。 设 $K = \mathbf{Q}(\theta)$、 $f(x$如上述定理所述。那么 $\{1, \theta, \cdots, \theta^{n-1}\}$ 是 K 的整基，当且仅当每个整除 p 的素数 D_f 都满足定理 $-$ (5) 的条件之一 1.1

下述结果由 [7, 定理 1。3]证明，可由推论1.2快速推得。

推论 1.3。设 $K = \mathbf{Q}(\theta)$ 是一个代数数域，其中 θ a 是不可约多项式 $x^n - c \in \mathbf{Z}[x]$ 的一个根。那么 $\{1, \theta, \cdots, \theta^{n-1}\}$ 是 K 的整基，当且仅当 c 是一个无平方因子整数，并且当 $r \geq 1$ 是整除 n 的素数 p 的最高次幂，且 p 不整除 c 时， p^2 不整除 $c^{p^r} - c$.

推论 1.4. 设 $f(x) = x^n + ax^2 + bx + c \in \mathbf{Z}[x]$ 是一个次数为 n 的首一多项式，其中 $c \neq \pm 1$ 无平方因子。假设整除 a、 b、 c 的素数集合相同。设 $2|c$ 或 $a \equiv 1$(mod 4) 或 $c \equiv 1$(mod 4)。令 $K = \mathbf{Q}(\theta)$，其中 θ 是 $f(x)$ 的一个根。那么，$\mathbf{Z}_K = \mathbf{Z}[\theta]$ 当且仅当对于每个整除 D_f 但不整除 a 的素数 p ， p^2 不整除 D_f。

我们现在陈述以下结果，并将在定理1.1的证明之后给出证明。该结果本身也具有独立的研究价值。

命题 1.5. 设 $K = \mathbb{Q}(\theta)$ 是一个代数数域，其中 θ 满足一个不可约四项式 $f(x) = x^n + ax^2 + bx + c \in \mathbf{Z}[x]$，其次数为 $n \geq 3$，且 $b^2 = 4ac$。如果 p

是一个素数，且 $p \nmid b$ 和 p 整除 K 的判别式 d_K，那么整除 K 的判别式 d_K 的 p 的精确幂为 1。

利用 $D_f = [\mathbf{Z}_K : \mathbf{Z}[\theta]]^2 d_K$这一事实，上述命题和定理 1.1可迅速推出以下关于 d_K绝对值的显式公式。

推论 1.6。设 $K = \mathbb{Q}(\theta)$, $f(x)$ 如定理 1.1 中所述，且 $|D_f| = \prod_{i=1}^{k} p_i^{r_i} \prod_{j=1}^{l} q_j^{t_j}$是 $|D_f|$ 的素因数分解，其中各素数互不相同，满足 $p_i | b$ 且 $q_j \nmid b$。若所有素数 p_i均满足定理 1.1 的条件 (1) – (5)，则判别式 d_K 的绝对值为

$$|d_K| = \prod_{i=1}^{k} p_i^{r_i} \prod_{j=1}^{l} q_j^{\frac{1-(-1)^{t_j}}{2}}.$$

2. Preliminary Results.

对于两个多项式 $f(x)$ $g(x)$； $R(f, g)$ 表示 $f(x)$ 和 $g(x)$ 的结式。现在我们陈述一些已知的结式性质。

引理 2.1. 设 $f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0$和 $g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$是两个分别具有整数系数、次数为 m 和 n的多项式。那么

(1) $R(f, g) = (-1)^{mn} R(g, f)$。(2) 若 $f(x) = g(x)q(x) + r(x)$，则

$$R(f, g) = (b_n)^{m-k} R(r, g)$$

其中 $k = \deg r(x)$。

(3) $R(f, g) = (b_n)^m \prod_{i=1}^{n} f(\gamma_i)$

其中 γ_1、γ_2、$\cdots$、γ_n 是 $g(x)$的根。

注意，首一多项式 $f(x) \in \mathbf{Z}[x]$ 的判别式与结式由下列公式关联：

$$D_f = (-1)^{\frac{n(n-1)}{2}} R(f', f) \tag{2.1}$$

其中， f' 是 $f.$的导数。

引理 2.2. 设 $f(x) = x^n + ax^2 + bx + c \in \mathbf{Z}[x]$ 是一个次数为 $n \geq 3$ 的四项式，且 $b^2 = 4ac.$。则有：

(1) $f(x)$ 的判别式为

$$D_f = (-1)^{\frac{n(n-1)}{2}} \left[n^n (-c)^{n-1} - 4(n-2)^{n-2} \left(\frac{b}{2} \right)^n \right]. \tag{2.2}$$

(2) 如果 $p \nmid b(n-2)$, then $D_f \equiv 0 \pmod{p^2}$ if and only if $f(-\frac{nb}{2a(n-2)}) \equiv 0 \pmod{p^2}$

证明。(1) 我们可以取 $a \neq 0$，因为如果 $a = 0$，那么利用 $b^2 = 4ac$，我们有 $b = 0$。容易验证，$f(x) = x^n + c$ 的判别式为 $D_f = (-1)^{\frac{n(n-1)}{2}} n^n (-c)^{n-1}$。因此假设 $a \neq 0$。根据引理 2.1(1) 和公式 (2.1)，我们有 $D_f = (-1)^{\frac{n(n-1)}{2}} R(f, f')$。利用带余除法，可以写成

$$f(x) = f'(x)q(x) + \frac{a(n-2)}{n}x^2 + \frac{b(n-1)}{n}x + c.$$

我们将 $\frac{a(n-2)}{n} x^2 + \frac{b(n-1)}{n} x + c$ 记为 $r(x)$。牢记引理 2.1 的 (1) 和 (2)，我们有 $D_f = (-1)^{\frac{n(n-1)}{2}} n^{n-2} R(f', r)$。由于 $r(x)$ 的根为 $\gamma_1 = -\frac{b}{2a}$ 和 $\gamma_2 = -\frac{nb}{2a(n-2)}$，因此根据引理 2.1 的 (3)，我们有

$$D_f = (-1)^{\frac{n(n-1)}{2}} n^{n-2} \left(\frac{a(n-2)}{n}\right)^{n-1} f'(\gamma_1) f'(\gamma_2).$$

简单计算表明

$$D_f = (-1)^{\frac{n(n-1)}{2}} \left[n^n (-c)^{n-1} - 4(n-2)^{n-2} \left(\frac{b}{2}\right)^n \right].$$

(2) 利用假设 $b^2 = 4ac$，我们有 2 整除 b. 由于 $p \nmid b(n-2)$，可得 $f\left(-\frac{nb}{2a(n-2)}\right) \equiv 0$ (模 p^2) 当且仅当

$$\left(-\frac{nb}{2a(n-2)}\right)^n + a\left(-\frac{nb}{2a(n-2)}\right)^2 + b\left(-\frac{nb}{2a(n-2)}\right) + c \equiv 0 \pmod{p^2}.$$

利用 $b^2 = 4ac$，最后一个方程可改写为

$$(-nb)^n + n^2 c(2a)^n (n-2)^{n-2} - 2nc(2a)^n (n-2)^{n-1} + c(2a(n-2))^n \equiv 0 \pmod{p^2}.$$

两边除以 $2^n a^n c$ 并化简后，最后一个方程变为

$$\frac{1}{c}\left(\frac{-nb}{2a}\right)^n + 4(n-2)^{n-2} \equiv 0 \pmod{p^2}.$$

由于 $2a = \frac{b^2}{2c}$，我们可知 $f\left(-\frac{nb}{2a(n-2)}\right) \equiv 0$ 模 p^2 当且仅当

$$n^n (-c)^{n-1} - 4(n-2)^{n-2}\left(\frac{b}{2}\right)^n \equiv 0 \pmod{p^2},$$

结合 (1)，这就完成了该引理的证明。 □

以下结果将在定理 1.1 的证明中用到。

引理 2.3. 设 a, b, c, n 是满足 $2 \nmid ac$, $2|b$ 和 $2^2 \nmid b$ 的整数。设 $n > 2$ 为偶整数，且 $F(x) = (\frac{a+a^2}{2})x^2 + (ac + \frac{b}{2})x + (\frac{c+c^2}{2})$ 是一个多项式。那么，多项式 $F(x)$ 与 $x^{\frac{n}{2}} + ax + c$ 模2互素，当且仅当 $a \equiv 1$ (模4) 或 $c \equiv 1$(模4)。

证明。将多项式 $x^{\frac{n}{2}} + ax + c$ 记为 $h(x)$。由于 $2|n, 2|b, 2 \nmid ac, 4 \nmid b$，可写成 $n = 2m$, $a = 2A + 1, b = 2B, c = 2C + 1$，其中 $A, B, C, m \in$ 属于 $\mathbf{Z}$，且 $2 \nmid B$。因此

$$h(x) \equiv x^m + x + 1 \pmod 2,$$

而 $F(x)$ 可写为

$$F(x) = (2A^2 + 3A + 1)x^2 + ((2A + 1)(2C + 1) + B)x + (2C^2 + 3C + 1),$$

由此得到

$$F(x) \equiv (A + 1)x^2 + C + 1 \pmod 2.$$

令 $\alpha = A \pmod 2$ 且 $\gamma = C \pmod 2$。则 α 和 γ 的取值属于 $\{0, 1\}$。因此，只需在以下四种情形下证明该引理。

情形 1. $\alpha = 0, \gamma = 0$. 在此情形下

$$F(x) \equiv (x + 1)^2 \pmod 2,$$

并且很容易验证，$F(x)$与 $h(x)$模2互素。

情形 2. $\alpha = 0, \gamma = 1$. 现在我们有

$$F(x) \equiv x^2 \pmod 2.$$

因此，我们看到 $F(x)$与 $h(x)$模2互素。

情况3. $\alpha = 1, \gamma = 1$. 在这种情况下

$$F(x) \equiv 0 \pmod 2.$$

因此，$h(x)$模2整除 $F(x)$，所以在这种情形下，$F(x)$与 $h(x)$不可能模2互素。

情形 4. $\alpha = 1, \gamma = 0$. 这里我们有

$$F(x) \equiv 1 \pmod 2,$$

这表明 $F(x)$ 与 $h(x)$ 模2互素。

因此，鉴于上述四种情况，我们看到 $F(x)$ 与 $h(x)$ 模2不互素，当且仅当处于情况3，即 $\alpha = 1$ 和 $\gamma = 1$. 回到 α、γ 的定义，我们得到，这种情况发生当且仅当有 $a \equiv 3$ (模4) 和 $c \equiv 3$ (模4)，至此引理得证。□

1878年，Dedekind 提出了以下简单判别法，称为 Dedekind判别法（参见 [1, 定理 6.1。4], [2]），它给出了 $f(x)$ 必须满足的充要条件，使得 p 不整除 $[\mathbf{Z}_K : Z[\theta]]$。

定理 2.4.（Dedekind判别法）设 $K = \mathbb{Q}(\theta)$ 是一个代数数域，其中$f(x)$ 是代数整数 θ 在 $\mathbb{Q}$. 上的极小多项式。设 p 是一个素数，且$\overline{f}(x) = \overline{g}_1(x)^{e_1} \dots \overline{g}_t(x)^{e_t}$ 是 $\overline{f}(x)$ 在 $\mathbb{Z}/p\mathbb{Z}$上分解为不同不可约多项式的幂的乘积所得的因式分解，其中每个 $g_i(x) \in \mathbb{Z}[x]$ 都是首一的。令 $M(x)$ 表示多项式 $\frac{1}{p}(f(x) - g_1(x)^{e_1} \dots g_t(x)^{e_t})$，其系数取自 $\mathbb{Z}$.。那么 p不整除[Z$_K$: $\mathbb{Z}[\theta]$] 当且仅当对每个 i，均有 $e_i = 1$，或者 $\bar{g}_i(x)$ 不整除 $\overline{M}(x)$。

现在陈述如下简单引理，该引理已在（ [6, 引理 2.2]）中证明，后文将用到。利用二项式定理即可轻松证明。

引理 2.5. 设 $h(x) = x^m + ax^s + b \in$ Z$[x]$ 是一个次数为 m 的首一多项式。设 p 是一个素数，且 $k \in$N。那么，对于某个多项式 $T(x) \in$ Z$[x]$，有 $h(x^{p^k}) = h(x)^{p^k} + ph(x)T(x) + (ax^{sp^k} + b) + (-ax^s - b)$。

以下结果将在命题的证明中用到1.5 （参见 [8, 定理 4.24]）。证明从略。

定理 2.6。设 p 为一个素数，且 K/Q 是一个次数为 n的扩张。设pZ$_K = \wp_1^{e_1} \cdots \wp_t^{e_t}$，其中 $\wp_1$、$\cdots$、$\wp_t$ 是 Z$_K$ 中互不相同的素理想，且 $N_{K/\mathbf{Q}}(\wp_i) = p^{f_i}$。$_t$若对于 $1 \le i \le t$ 有 $(p, e_i) = 1$，则 d_K 被 p 整除的恰当幂次为 $\sum_{i=1} f_i(e_i - 1)$。

3. Proof of Theorem 1.1.

定理 *1.1* 的证明。考虑第一种情形，即 $p \mid a$ 且 $p \mid c$。在这种情形下$f(x) \equiv x^n$(模 p)。如定理 2.4 中所述，可以验证 $M(x) = \frac{a}{p}x^2 + \frac{b}{p}x + \frac{c}{p}$，因此可知 $p \nmid$ [Z$_K$: Z$[\theta]$] 当且仅当 x 不整除 $\overline{M}(x)$。这仅在 $p^2 \nmid c$.

现在考虑 $p \mid a$ 且 $p \nmid c$的情形。由于 $b^2 = 4ac$，我们有 $p|b$ 因此$f(x) \equiv x^n + c$ (模 p)。牢记 $p|D_f$ 以及公式（2.2），可知 $p \mid n$. 设 $n = p^r m$，其中 $r \ge 1$ 且 $p \nmid m$. 根据二项式定理，我们有

$$x^n + c \equiv (x^m + c)^{p^r} \pmod{p}. \tag{3.1}$$

$_t$设 $\prod \bar{g}_i(x)$ 是 $x^m + \bar{c}$ 在 Z$/p$Z 上的因式分解，其中 $g_1(x)$ $g_2(x)$ $\cdots$，$g_t(x)$ 属于 Z$[x]$，是模 p 下互不相同且不可约的首一多项式。将 $_t x^m + c$ 写成 $\prod \bar{g}_i(x) + pA_1(x)$ 的形式，其中某个多项式 $A_1(x)$ 属于 Z$[x]$。于是$_{i=1}$

$$f(x) = ((x^{p^r})^m + c) + ax^2 + bx = h(x^{p^r}) + ax^2 + bx$$

其中 $h(x) = x^m + c$. 现在根据 p 是否为奇素数，将这一情形分为两个子情形。

首先考虑 $p \neq 2$. 注意到 $p^2 \mid a$并将引理2.5 应用于 $h(x)$，我们得到

$$f(x) = \Big(\prod_{i=1}^{t} g_i(x) + pA_1(x)\Big)^{p^r} + pA(x)\prod_{i=1}^{t} g_i(x) + p^2B(x) + c - c^{p^r} + bx \tag{3.2}$$

对于某些多项式 $A(x)$ $B(x) \in \mathbf{Z}[x]$。分别将 $\frac{c-c^{p^r}}{p}$ 和 $\frac{b}{p}$ 记为 c_1 和 b_1。由 (3.1) 可知，$\bar{f}(x) = \Big(\prod_{i=1}^{t} \bar{g}_i(x)\Big)^{p^r}$. 将 $f(x)$ 写成 $\prod_{i=1}^{t} g_i(x)^{p^r} + pM(x)$，$M(x) \in \mathbf{Z}[x]$，$M(x) \in \mathbf{Z}[x]$。注意到 $r \geq 1$，由 (3.2) 可立即得到

$$\overline{M}(x) = \bar{A}(x)\prod_{i=1}^{t} \bar{g}_i(x) + \overline{c_1} + \overline{b_1}x.$$

应用定理 2.4，$p \nmid [\mathbf{Z}_K$ 当且仅当 $\overline{M}(x)$ 与 $\prod \bar{g}_i(x)$ 互素；根据上述等式，这当且仅当 $(\overline{c_1} + \overline{b_1}x)$ 与 $\prod \bar{g}_i(x)^{p^r} = \bar{h}(x^{p^r}) = x^n + \bar{c}$ 互素。这当且仅当 $p \mid b_1$ 和 $p \nmid c_1$，或者 $p \nmid b_1((-c_1)^n + cb_1^n)$。现在令 $p = 2$.。由于 $b^2 = 4ac$，我们得到 $4 \mid a$ 和 $4 \mid b$。因此

$$f(x) = \Big(\prod_{i=1}^{t} g_i(x) + 2A_1(x)\Big)^{2^r} + 2C(x)\prod_{i=1}^{t} g_i(x) + 4D(x) + c + c^{2^r}$$

对于某些多项式 $C(x)$ $D(x) \in \mathbf{Z}[x]$. 这里，$1 \leq i \leq t$, $\bar{g}_i(x) \nmid \overline{M}(x)$ 当且仅当$\bar{g}_i(x) \nmid (\frac{c+c^{2^r}}{2})$。这仅在 $4 \nmid (c^{2^r} + c)$ 时发生。

现在考虑 $p \nmid a$ 和 $p \mid c$. 的情形。注意，$f(x) \equiv x^2(x^{n-2} + a)$（模 p）。令 $l \geq 0$ 表示整除 $n-2$的 p的最高次幂。先考虑 $l = 0$的可能性。若 $p \neq 2$，由 $b^2 = 4ac$可知，我们有 $p^2 \mid c$.。由于 x是 $\bar{f}(x)$唯一的重因子，我们看到它整除 $\overline{M}(x) = \frac{\bar{b}}{p}x$。因此，由定理 2.4，$p$整除 $[\mathbf{Z}_K : \mathbf{Z}[\theta]]$。若 $p = 2$，则注意到 $p^2 \mid b$ 和 $p^2 \mid c$。因此，$\overline{M}(x) = \bar{0}$。所以，在 $l = 0$的情形下，p 总是整除 $[\mathbf{Z}_K : \mathbf{Z}[\theta]]$。现在假设 $l \geq 1$，即 $n - 2 = p^l s'$ 和 $p \nmid s'$。写作 $x^{s'} + a = g_1(x) \cdots g_t(x) + pH(x)$，其中 $g_1(x) \cdots$、$g_t(x)$是首一多项式，它们彼此不同，且模 p 不可约，并且 $H(x) \in \mathbf{Z}[x]$。记住 $p^2 \mid c$，并将引理 2.5 应用于 $h(x) = x^{s'} + a$，我们可以将 $f(x) = x^2(x^{n-2} + a) + bx + c$写成

$$f(x) = x^2\left[(\prod_{i=1}^{t} g_i(x) + pH(x))^{p^l} + pT(x)\prod_{i=1}^{t} g_i(x) + p^2U(x) + a + (-a)^{p^l}\right] + bx + c, \tag{3.3}$$

其中 $T(x)$ $U(x)$属于 $\mathbb{Z}[x]$。注意， x、 $\bar{g}_1(x)$ $\cdots$、 $\bar{g}_t(x)$是 $\overline{F}(x)$的互异不可约因子。分别将 $^{a+}(_{-a}{}^{p^l})$和 $\frac{b}{p}$ 记为 a_1 和 $b_{1\circ}$ 由于 $l \geq 1$，根据定理 2.4 $p \nmid [$， $\mathbb{Z}_K : \mathbb{Z}[\theta]]$ 当且仅当 $\bar{a}_1 x^{\overset{p}{2}} + \bar{b}_1$ 和 $x^{n-2} + \bar{a}$ 互素。注意，若 $p = 2$，则 $4|b$，因此在这种情况下，多项式 $\bar{a}_1 x^2 + \bar{b}_1$ 和 $x^{n-2} + \bar{a}$ 互素当且仅当 $2 \nmid \bar{a}\bar{a}_1$. 。现在假设 $p \neq 2$。在这种情况下，我们看到， $\bar{a}_1 x^2 + \bar{b}_1$和 $x^{n-2} + \bar{a}$互素当且仅当以下条件之一成立：(I) $p \mid a_1$和 $p \nmid b_1$；或 (II) $\bar{a}_1 \neq \bar{0}$和 $x^2 + \frac{\bar{b}_1}{\bar{a}_1}$、 $x^{n-2} + \bar{a}$ 互素。写作 $n - 2 = 2^d s$，其中，当 2 整除 $n - 2$ 时 d 等于 1，否则等于 0。注意，若 ξ是代数闭包 $\mathbb{Z}\,\mathbb{Z}$ 中多项式 $x^2 + \frac{\bar{b}_1}{\bar{a}_1}$、 $x^{n-2} + \bar{a}$ $/p$ $\overline{}$ $\overline{}$ $-\bar{a}$ 的公共根，则我们看到 $(\ \frac{-\bar{b}_1}{\bar{a}_1})^{\ \frac{n-2}{2^d}} = (\ )^{2^{1-d}}$。此外，简单计算可得，若 $\xi^{2^d} = (-\bar{a})^{-2^d} (-\frac{\bar{b}_1}{\bar{a}_1})^{\frac{n-1}{2^{1-d}}}$且 $(\ \frac{-\bar{b}_1}{\bar{a}_1})^{\frac{n-2}{2^d}} = (-\bar{a})^{2^{1-d}}$，则 ξ是多项式 $x^2 + \frac{\bar{b}_1}{\bar{a}_1}$、 $x^{n-2} + \bar{a}$的根。因此容易看出，(II)成立当且仅当 $p \nmid \bar{a}_1[(-\bar{a})^{2^{1-d}} \bar{a}_1{}^{\frac{n-2}{2^d}} - (-\bar{b}_1)^{\frac{n-2}{2^d}}]$。

现在考虑 $2 \nmid ac$. As $b^2 = 4ac$ 的情形，因此 $4 \nmid b$. 牢记 $2|D_f$ 和方程 (2.2)，我们看到 $2 \mid n$. 令 $n = 2m$。注意到 $\bar{f}(x) = x^n + \bar{a}x^2 + \bar{c}$。$_t$将 $x^m + ax + c$ 记为 $h(x)$，使得 $f(x) = h(x^2) + bx$. 令 $h(x) \equiv \prod g_i(x)^{r_i}$ (模2) 为 $_{i=1}$ $h(x)$ 在模2下分解为不可约多项式乘积的$_{i=1}$因式分解，其中 $g_i(x)$ 属于 $\mathbb{Z}[x]$ ，是首一的，并且 $r_i > 0$。利用引理 2.5，我们看到

$$f(x) = h(x^2) + bx = (h(x))^2 + 2h(x)N(x) + ax^2 + c + (-ax - c)^2 + bx$$

$_t$对于某个 $N(x) \in \mathbb{Z}[x]$。在上述方程中用 $H(x) \in \mathbb{Z}[x]$ 代入 $h(x) = \prod g_i(x)^{r_i} + 2H(x)$，我们看到存在 $N_1(x) \in \mathbb{Z}[x]$ 使得

$$f(x) = \Big(\prod_{i=1}^{t} g_i(x)^{r_i}\Big)^2 + 4N_1(x) + 2h(x)N(x) + ax^2 + c + (-ax - c)^2 + bx. \tag{3.4}$$

对某个 $M(x) \in \mathbb{Z}[x]$，写作 $f(x) = \Big(\prod^{t} g_i(x)^{r_i}\Big)^2 + 2M(x)$。应用定理 2.4，我们$_{i=1}$可知， $2 \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ 当且仅当 $\frac{1}{2}[ax^2 + c + (-ax - c)^2 + bx]$ 与 $h(x)$ 模2互素；根据引理 2.3，这等价于 $a \equiv 1$ (模 4) 或 $c \equiv 1$ (模 4)。

考虑最后一种情形，此时 $p \nmid b$. 鉴于 $b^2 = 4ac$ 以及 $p|D_f$这一事实，我们可知 $p \neq 2$ 且 $p \nmid n(n-2)$。容易验证， $-(\ ^{nb}_{2\ n-2()a})$ 是 $f(x)$ 唯一的重根，且重数为二。取 $d \in \mathbb{Z}$，使得

$$nbd \equiv -2(n-2)a \pmod{p^2}. \tag{3.5}$$

因此，我们有

$$\bar{f}(x) = (x - \bar{d})^2 \bar{h}(x), \tag{3.6}$$

其中 $\bar{h}(x)$ 属于 $\mathbf{Z}/p\mathbf{Z}[x]$ ，是一个可分多项式。记

$$f(x) = (x - d)q(x) + f(d) \tag{3.7}$$

对于某个首一多项式 $q(x) \in \mathbf{Z}[x]$。注意， $\bar{q}(x) = (x - d)\bar{h}(x)$，且 $(x - d)$ 不整除 $\bar{h}(x)$。设 $\bar{h}(x) = \prod_{i=1}^{t} \bar{g}_i(x)$ 是 $\bar{h}(x)$ 在 $\mathbf{Z}/p\mathbf{Z}$ 上分解为若干个互不相同的不可约多项式的因式分解，其中每个 $g_i(x) \in \mathbf{Z}[x]$ 都是首一的。记

$$q(x) = (x - d) \prod_{i=1}^{t} g_i(x) + ph_1(x)$$

对于某个 $h_1(x)$ 属于 $\mathbf{Z}[x]$。将上式代入（3.7），可得

$$f(x) = (x - d)^2 \prod_{i=1}^{t} g_i(x) + p(x - d)h_1(x) + f(d).$$

因此，应用定理 2.4，可得 $p \nmid [\mathbf{Z}_K : \mathbf{Z}[\theta]]$ 当且仅当 p^2 不整除 $f(d)$。因此，根据引理 2.2，有 $p \nmid [\mathbf{Z}_K : \mathbf{Z}[\theta]]$ 当且仅当 p^2 不整除D_f. 定理得证。 □

命题 *1.5* 的证明。牢记公式 $D_f = [\mathbf{Z}_K : \mathbf{Z}[\theta]]^2 d_K$，我们有$p|D_f$ 因为 p 整除 d_K。现在回想定理 1.1最后一种情形的证明，可知$p \neq 2$， $p \nmid n(n-2)$ 且

$$\bar{f}(x) = (x - \bar{d})^2 \prod_{i=1}^{t} \bar{g}_i(x),$$

其中 $x - d, \bar{g}_1(x) \cdots, \bar{g}_t(x)$ 是模 p 下互不相同的不可约多项式，且$g_i(x) \in \mathbf{Z}[x]$ 对每个 i 都是首一的。因此，利用亨泽尔引理可知， $f(x)$ 在 $\mathbf{Q}_p[x]$ 中有一个因式分解，使得

$$f(x) = G(x)G_1(x) \cdots G_t(x),$$

其中 $G_1(x) \cdots$、 $G_t(x)$ 是互不相同的不可约多项式。上述因式分解导出了 $p\mathbf{Z}_K$ 的素理想分解: $p\mathbf{Z}_K = \mathfrak{p}\wp_1 \cdots \wp_t$，其中 $\wp_i$ 是 $\mathbf{Z}_K$ 中互不相同的素理想，且 $N_{K/\mathbf{Q}}(\wp_i) = p^{\deg G_i(x)}$；由于 p 整除 d_K 在 $\mathbf{Z}_K$ 中分歧，我们有 $\mathfrak{p} = \wp^2$，其中某个 $\mathbf{Z}_K$ 中的素理想满足 $N_{K/\mathbf{Q}}(\wp) = p$，并且 $\gcd(\wp, \wp_i) = \mathbf{Z}_K$。由于 $p \neq 2$，利用定理 2.6，我们得到整除 d_K 的 p 的确切幂次为 1。□

4. Examples.

现在我们给出一些例子来说明我们的结果。在这些例子中， K =Q(θ)，其中 θ 是 f(x) 的一个根。

例 4.1. 设 $c \neq \pm 1$ 是一个无平方因子整数。考虑多项式$f(x) = x^7 + c(x^2 + 2x + 1)$。则 $f(x)$ 的判别式 D_f由 $D_f = c^6[2^2 \cdot 5^5 c - 7^7]$ 给出。根据定理 1.1(i)，任何整除 c 的素数 p 都不会整除 $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$。进一步，根据推论 1.2，$\mathbb{Z}_K = \mathbb{Z}[\theta]$ 当且仅当对每个整除 D_f 且不整除 c 的素数 p， p^2 都不整除 $(2^2 \cdot 5^5 c - 7^7)$。现在我们计算对应于 c 某些取值时$[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ 的确切值。

(1) 对于 $c = 2$，容易看出 $|D_f| = 2^6 \cdot 3^2 \cdot 83 \cdot 1069.$。根据定理 1.1，2、83、1069 不整除 $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$，而 3 整除 $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$。由于 $D_f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 \cdot d_K$，其中 d_K 是 K 的判别式，我们可知在这种情况下 $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ 为 3。(2) 考虑 $c = 5$。可以验证 $|D_f| = 5^6 \cdot 3 \cdot 253681$。根据定理 1.1，素数 5、3 和 253681 不整除 $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$。因此 $[\mathbb{Z}_K : \mathbb{Z}[\theta]] = 1$，所以在这种情况下 $\{1, \theta, \cdots, \theta^6\}$ 是 K 的整基。(3) 当 $c = 7$ 时，可以看到 $|D_f|$ 的素因数分解为 $7^7 \cdot 11^3 \cdot 79$。同上，7 、 79 不整除 $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$，而 11 整除$[\mathbb{Z}_K : \mathbb{Z}[\theta]]$。因此 $[\mathbb{Z}_K : \mathbb{Z}[\theta]] = 11$。

例 4.2. 假设 $c \equiv 1$(模 4)，并考虑一个不可约[1] 多项式$f(x) = x^n + c(x^2 + 2x + 1)$。那么我们有 $D_f = (-1)^{\frac{n(n-1)}{2}} c^{n-1}[(-1)^{n-1} n^n - 4(n-2)^{n-2} c]$。根据推论 1.2，$\mathbb{Z}_K = \mathbb{Z}[\theta]$ 当且仅当对于每个整除 D_f 的素数 p，当 $p \mid c$ 时 p^2 不整除 c；并且如果 $p \nmid c$，那么 $p^2 \nmid D_f$。例如，如果取 $n = 5$，且$c \neq \pm 1$ 是一个无平方因子整数，那么 $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ 是 K 的整基，当且仅当 $(3125 - 108c)$ 无平方因子。可以验证，当$c = -3$、5、13、17、21 时，$(3125 - 108c)$ 无平方因子。

References

[1]H. Cohen，《计算代数数论教程》，Springer 出版社，柏林—海德堡，1993年。.[2] R. Dedekind，关于理想理论与高次同余理论之间的联系，哥廷根科学院论丛 23（1878年），1–23。[3] I. Ga，丢番图方程与幂整基。Springer Science+Business Media, LLC，2002年。[4] M. Gr。关于整数环为单生成的循环三次域，《巴黎科学院学报》A 辑，278：59–62，1974年。

[1]假设存在 c 的一个素因子 p，使得整除 c 的 p 的最高次幂为 k，且 $\gcd(k, n) = 1$，那么根据杜马不可约性判别法 [5]， $f(x) = x^n + c(x^2 + 2x + 1) \in \mathbb{Z}[x]$ 在 Q 上不可约。

[5] A. Jakhar，关于多项式的因子，《伦敦数学会通报》52（2020年），158–160。[6] A. Jakhar、S. K. Khanduja、N. Sangwan，关于代数整数指标的素因子，《数论杂志》166（2016年），47–61。[7] B. Jhorar、S. K. Khanduja，何时是整闭的？《代数与应用杂志》15：5（2016年），1650091（7页）。[8] W. Narkiewicz，《代数数的初等与解析理论》，Springer 出版社，柏林—海德堡，2004年。

(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

电子邮箱地址，ANUJ JAKHAR：anujjakhar@iitm.ac.in, anujiisermohali@gmail.com

电子邮箱地址，SUMANDEEP KAUR：sumandhunay@gmail.com

电子邮箱地址，SURENDER KUMAR：surenderk@iitbhilai.ac.in