ACTA ARITHMETICA
169.2 (2015)

Indices of subfields of cyclotomic $\mathbb{Z}_p$-extensions and higher degree Fermat quotients

by

Yoko Inoue and Kaori Ota (Tokyo)

1. Introduction. In this paper, we consider indices of subfields of cyclotomic $\mathbb{Z}_p$-extensions of number fields, and show that prime factors of the indices are only those less than the extension degree, which split completely and are closely related to higher degree Fermat quotients.

Let k be an algebraic number field and L be a finite extension of k with rings of integers O_k and O_L, respectively. We say that O_L has a power basis over O_k if there is an element θ of O_L such that $O_L = O_k[\theta]$, and if this holds for $k = \mathbb{Q}$, we simply say that O_L has a power basis. Many results have been obtained to decide whether O_L has a power basis and, if the power basis exists, to find all generators of such a basis, especially in the case $k = \mathbb{Q}$. It has been shown that there are only finitely many abelian extensions of $\mathbb{Q}$ which have power bases if the extension degree is prime to 6 (see [G, Gr1, Gr2, Gy]).

When O_L does not have a power basis over O_k, it is interesting to consider common factors of the indices $(O_L : O_k[\theta])$ for all the integral primitive elements θ of L. We denote the greatest common divisor of these indices by $I(L/k)$ and call it the index of L/k. For indices $I(L/\mathbb{Q})$, there are lots of results in the literature; here we only mention the results of Engstrom related to Ore's conjecture. Ore's conjecture states that the highest exponent χ of a prime q dividing $I(L/\mathbb{Q})$ is not in general determined by the prime ideal decomposition of qO_L (cf. [O, DD]). Engstrom has shown that if $[L : \mathbb{Q}] < 8$, then χ is completely determined by the prime ideal decomposition of qO_L, and that there are examples of two fields whose extension degrees over $\mathbb{Q}$ are 8 and have the same decomposition type of (3) with different χ's for 3 (cf. [E]). In [E, Theorem 3], he has also given a formula for χ if q splits completely in L, namely $\chi = \frac{1}{2}v_q(\prod_{1\le i\ne j\le n}(i-j))$ if $[L : \mathbb{Q}] = n$.

2010 *Mathematics Subject Classification*: Primary 11R04; Secondary 11A07, 11R99.
Key words and phrases: index of number fields, cyclotomic $\mathbb{Z}_p$-extension, Fermat quotient.

DOI: 10.4064/aa169-2-1

Here v_q is the q-adic valuation normalized by $v_q(q) = 1$. Ore's conjecture is still attracting people interested in which arithmetic invariants determine χ completely, and in what are the exact formulas for χ (cf. [Na, Sl] and [N, Problem 22]).

Now for $k = \mathbb{Q}$, the square of $(O_L : \mathbb{Z}[\theta])$ appears as the quotient of the discriminant $d_{\mathbb{Q}}(\theta)$ of θ by the discriminant $d(L/\mathbb{Q})$ of L. For a general k, there is still an analogous identity involving the ideal generated by the discriminant $d_k(\theta)$ of θ over k and the discriminant $d(L/k)$ of L/k:

$$(d_k(\theta)) = \mathfrak{m}(\theta)^2 \cdot d(L/k),$$

where $\mathfrak{m}(\theta)$ is an integral ideal of k called the inessential divisor of $d_k(\theta)$ (cf. [H, p. 452] or Proposition 2.2). Therefore it is quite natural to consider the greatest common divisor of $\mathfrak{m}(\theta)$ for all the integral primitive elements θ for L/k. We denote it by $\mathfrak{I}(L/k)$ and call it the index ideal of L/k. Any prime ideal of k dividing $\mathfrak{I}(L/k)$ has been called a common inessential discriminant divisor of L/k in [H, p. 452]. The relation between $\mathfrak{m}(\theta)$ and $(O_L : O_k[\theta])$ is

$$(O_L : O_k[\theta]) = \mathfrak{N}(\mathfrak{m}(\theta)),$$

where $\mathfrak{N}$ denotes the ideal norm, i.e., $\mathfrak{N}(\mathfrak{m}(\theta)) = (O_k : \mathfrak{m}(\theta))$ (cf. Proposition 2.5(ii)). From this, we see that if an ideal $\mathfrak{a}$ of k divides $\mathfrak{I}(L/k)$, then its norm $\mathfrak{N}(\mathfrak{a})$ divides $I(L/k)$.

It has been shown that the rings of integers of subfields of cyclotomic $\mathbb{Z}_p$-extensions of k do not have a power basis over O_k if k satisfies certain conditions, and in particular those fields over $\mathbb{Q}$ do not have power bases for $p \geq 5$ (cf. [AO, Corollary 2] or Theorem 3.5). So it is quite interesting to find the indices of these subfields, which turn out to be closely related to higher degree Fermat quotients. For a positive integer n, the nth degree Fermat quotient for an integer a with respect to an odd prime p is defined, if $a^{p-1} \equiv 1 \pmod{p^n}$, as

$$F_{p,n}(a) = \frac{a^{p-1} - 1}{p^n}$$

(cf. [Hl]). When $n = 1$, this is just the usual Fermat quotient with base a, which was studied in relation to Fermat's Last Theorem and is still of interest in various aspects (see for example [S, I-H]). If we denote the nth layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ by K_n, then we show that for a prime q smaller than the extension degree p^n, q divides $I(K_n/\mathbb{Q})$ if and only if q splits completely in K_n. So there are no other prime factors of $I(K_n/\mathbb{Q})$ than those that split completely in K_n. This means that a prime q ($< p^n$) divides $I(K_n/\mathbb{Q})$ if and only if the nth Fermat quotient satisfies $F_{p,n}(q) \equiv 0 \pmod{p}$ for p odd, which is quite interesting (Theorem 3.6). So the fact that 1093 and 3511 are the only primes p with $2 \le p < 6.7 \times 10^{15}$ satisfying $F_{p,1}(2) \equiv 0 \pmod p$ (cf. [DK]) can be restated as saying that the first layers of cyclotomic $\mathbb{Z}_p$-extensions of $\mathbb{Q}$ have odd indices for $2 \le p < 6.7 \times 10^{15}$ except for 1093 and 3511 (these are called *Wieferich primes*). We note that if $q \mid I(K_n/\mathbb{Q})$ for some n, then $F_{p,i}(q) \equiv 0 \pmod p$ for any i with $1 \le i \le n$, but this does not necessarily mean $q \mid I(K_i/\mathbb{Q})$, because for that q must satisfy $q < p^i$. It may be of some interest to see if there is any prime q satisfying $q \mid I(K_n/\mathbb{Q})$ and $q \mid I(K_{n+1}/\mathbb{Q})$ for some $n \ge 1$.

Here is the outline of the paper. In Section 2, we give the notation and recall some basic results on number fields. In Section 3, first we consider which subfields of cyclotomic $\mathbb{Z}_p$-extensions of k have relative integral bases over k by computing Steinitz classes (Proposition 3.1, Corollary 3.2). Then we determine prime factors of the indices for $K_n/\mathbb{Q}$ and kK_n/k, where k is a Galois extension of $\mathbb{Q}$ with extension degree a prime different from p (Theorems 3.6, 3.8). Since these prime factors split completely, we can use Engstrom's formula for the highest exponents (cf. [E, Theorem 3] and [DD]). In Section 4, we give examples of indices of $K_n/\mathbb{Q}$ for $n = 1, 2, 3$. As mentioned above, primes q dividing $I(K_1/\mathbb{Q})$ are those less than p whose Fermat quotients satisfy

$$F_{p,1}(q) = \frac{q^{p-1} - 1}{p} \equiv 0 \pmod p.$$

So there is already a long list of such q's in [EM], and we only list $I(K_1/\mathbb{Q})$ for small p's here.

2. Preliminaries. In this section, we give the notation and results that are needed in subsequent sections.

Let k be a finite extension of $\mathbb{Q}$, and L a finite extension of k. When the class number of k is 1, L has a relative integral basis (RIB) over k for any L, and in the general case, it is known that L has a RIB over k if and only if the Steinitz class $\mathrm{St}(L/k)$ is trivial in the ideal class group of k (cf. [N, §7.3]). Concerning $\mathrm{St}(L/k)$, we recall the following proposition.

PROPOSITION 2.1 ([A]). *Let L be an extension of k of degree m, and O_L and O_k the rings of integers of L and k, respectively. Then:*

(i) *There is a basis $\{\gamma_1, \ldots, \gamma_m\}$ for L over k and an ideal $\mathfrak{a}$ of k such that*

$$O_L = O_k\gamma_1 \oplus \cdots \oplus O_k\gamma_{m-1} \oplus \mathfrak{a}\gamma_m,$$

and the Steinitz class $\mathrm{St}(L/k)$ *is the class* $[\mathfrak{a}]$ *in the ideal class group of k.*

(ii) *Let* $\gamma_1, \ldots, \gamma_m$ *and* $\mathfrak{a}$ *be as in* (i). *For any basis* $\{\eta_1, \ldots, \eta_m\}$ *of* L *over* k*, if the matrix* A *is defined by*

$$(\gamma_1, \ldots, \gamma_m) = (\eta_1, \ldots, \eta_m)A,$$

then

$$\frac{d(L/k)}{(d_k(\eta_1, \ldots, \eta_m))} = (\mathfrak{a} \cdot \det A)^2,$$

where $d(L/k)$ *and* $d_k(\eta_1, \ldots, \eta_m)$ *denote the discriminant of* L *over* k *and the discriminant of* $\eta_1, \ldots, \eta_m$ *over* k*, respectively.*

Proof. (ii) follows from $d(L/k) = \mathfrak{a}^2(d(\gamma_1, \ldots, \gamma_m))$ (cf. [A]). ∎

Next we introduce the notion of the index ideal for L over k, which relies on the following proposition.

PROPOSITION 2.2 ([H, p. 452]). *For each integral primitive element* θ *for* L/k*, there is an ideal* $\mathfrak{m}(\theta)$ *of* k *such that*

$$(d_k(\theta)) = \mathfrak{m}(\theta)^2 \cdot d(L/k), \tag{2.1}$$

where $d_k(\theta)$ *denotes the discriminant of* θ *over* k*.*

DEFINITION 2.3. The *index ideal* $\mathfrak{I}(L/k)$ of L/k is defined by

$$\mathfrak{I}(L/k) = \gcd\{\mathfrak{m}(\theta) \mid \theta \text{ is an integral primitive element for } L/k\},$$

and the *index* $I(L/k)$ *of* L/k is defined by

$$I(L/k) = \gcd\{(O_L : O_k[\theta]) \mid \theta \text{ is an integral primitive element for } L/k\}.$$

Also, if $(O_L : O_k[\theta]) = 1$ for some integral primitive element θ for L/k, we say that O_L *has a power basis over* O_k. When $k = \mathbb{Q}$, we simply say that O_L *has a power basis*. From this definition, if O_L has a power basis over O_k, then $I(L/k) = 1$, but the opposite does not hold in general (cf. Section 4).

The next theorem is the key to finding prime divisors of $\mathfrak{I}(L/k)$.

THEOREM 2.4 ([H, p. 456]). *A prime ideal* $\mathfrak{q}$ *of* k *does not divide* $\mathfrak{I}(L/k)$ *if and only if, for every positive integer* f*, the number* $r_\mathfrak{q}(f)$ *of prime ideals* $\mathfrak{Q}$ *of* L *lying above* $\mathfrak{q}$ *of residual degree* $f_\mathfrak{Q} = f$ *satisfies the inequality*

$$r_\mathfrak{q}(f) \le \pi_\mathfrak{q}(f) := \frac{1}{f}\sum_{d|f} \mu\left(\frac{f}{d}\right)\mathfrak{N}(\mathfrak{q})^d,$$

where $\mathfrak{N}(\mathfrak{q})$ *denotes the norm of the ideal* $\mathfrak{q}$*,* $\mu(\cdot)$ *is the Möbius function and the summation is taken over all positive divisors of* f*.*

The size of prime factors of $\mathfrak{I}(L/k)$ and the relation between $\mathfrak{I}(L/k)$ and $I(L/k)$ are given by the next proposition.

Proposition 2.5. *The following hold:*

(i) *If a prime ideal* $\mathfrak{q}$ *of* k *divides* $\mathfrak{I}(L/k)$, *then* $\mathfrak{N}(\mathfrak{q}) < [L:k]$. *Moreover, if* $\mathfrak{q}$ *splits completely in* L, *then*

$$\mathfrak{q} \mid \mathfrak{I}(L/k) \quad \text{if and only if} \quad \mathfrak{N}(\mathfrak{q}) < [L:k].$$

(ii) *For an integral primitive element* θ *for* L/k, *we have* $|N_k(d_k(\theta)| = \mathfrak{N}(d(L/k))(O_L : O_k[\theta])^2$, *so*

$$(O_L : O_k[\theta]) = \mathfrak{N}(\mathfrak{m}(\theta)), \tag{2.2}$$

where N_k *denotes the norm from* k *to* $\mathbb{Q}$, *and* $\mathfrak{m}(\theta)$ *is the ideal of* k *in* (2.1). *Hence, if* $\mathfrak{a} \mid \mathfrak{I}(L/k)$ *for an ideal* $\mathfrak{a}$ *of* k, *then* $\mathfrak{N}(\mathfrak{a}) \mid I(L/k)$.

Proof. For (i), we refer to [H, p. 456], or we can derive it easily from Theorem 2.4.

For (ii), let $r = [k:\mathbb{Q}]$ and $n = [L:k]$, and let $\{\lambda_1, \ldots, \lambda_r\}$ be an integral basis of k over $\mathbb{Q}$. By calculating the discriminant $d_{\mathbb{Q}}(\{\lambda_j\theta^i \mid 1 \le j \le r,\ 0 \le i \le n-1\})$ in two ways, we can obtain the identities

$$d_{\mathbb{Q}}(\{\lambda_j\theta^i\}) = d(L/\mathbb{Q})(O_L : O_k[\theta])^2 = N_k(d_k(\theta))d(k/\mathbb{Q})^{[L:k]}. \tag{2.3}$$

For the first identity, we only need to note that

$$O_k[\theta] = \Big\{ \sum_{j=1}^{r} \sum_{i=0}^{n-1} c_{ji}\lambda_j\theta^i \;\Big|\; c_{ji} \in \mathbb{Z} \Big\}.$$

To get the second identity, let $\tilde{L}$ be the Galois closure of L over $\mathbb{Q}$, and let $G = \mathrm{Gal}(\tilde{L}/\mathbb{Q})$, $H_1 = \mathrm{Gal}(\tilde{L}/k)$ and $H_2 = \mathrm{Gal}(\tilde{L}/L)$ be the corresponding Galois groups. Then we have coset decompositions

$$G = \bigcup_{j=1}^{r} H_1\tau_j \quad \text{and} \quad H_1 = \bigcup_{i=1}^{n} H_2\sigma_i,$$

so

$$G = \bigcup_{j=1}^{r} \bigcup_{i=1}^{n} H_2\sigma_i\tau_j.$$

Here $\{\tau_1, \ldots, \tau_r\}$ are the conjugate maps of k over $\mathbb{Q}$, $\{\sigma_1, \ldots, \sigma_n\}$ are the conjugate maps of L over k, and $\{\sigma_i\tau_j \mid 1 \le j \le r,\ 1 \le i \le n\}$ are conjugate maps of L over $\mathbb{Q}$. We set

$$\gamma_1 = \lambda_1, \quad \gamma_2 = \lambda_1\theta, \quad \gamma_3 = \lambda_1\theta^2, \ \ldots, \ \gamma_n = \lambda_1\theta^{n-1},$$
$$\gamma_{n+1} = \lambda_2, \quad \gamma_{n+2} = \lambda_2\theta, \ \ldots, \ \gamma_{2n} = \lambda_2\theta^{n-1}, \ \ldots \quad \text{and} \quad \gamma_{rn} = \lambda_r\theta^{n-1}.$$

Then

$$d_{\mathbb{Q}}(\{\lambda_j\theta^i\}) = d_{\mathbb{Q}}(\gamma_1,\dots,\gamma_{rn})$$

$$= \begin{vmatrix} \lambda_1^{\sigma_1\tau_1} & (\lambda_1\theta)^{\sigma_1\tau_1} & \cdots & (\lambda_1\theta^{n-1})^{\sigma_1\tau_1} & \lambda_2^{\sigma_1\tau_1} & (\lambda_2\theta)^{\sigma_1\tau_1} & \cdots \\ \lambda_1^{\sigma_2\tau_1} & (\lambda_1\theta)^{\sigma_2\tau_1} & \cdots & (\lambda_1\theta^{n-1})^{\sigma_2\tau_1} & \lambda_2^{\sigma_2\tau_1} & (\lambda_2\theta)^{\sigma_2\tau_1} & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdots \\ \lambda_1^{\sigma_n\tau_1} & (\lambda_1\theta)^{\sigma_n\tau_1} & \cdots & (\lambda_1\theta^{n-1})^{\sigma_n\tau_1} & \lambda_2^{\sigma_n\tau_1} & (\lambda_2\theta)^{\sigma_n\tau_1} & \cdots \\ \lambda_1^{\sigma_1\tau_2} & (\lambda_1\theta)^{\sigma_1\tau_2} & \cdots & (\lambda_1\theta^{n-1})^{\sigma_1\tau_2} & \lambda_2^{\sigma_1\tau_2} & (\lambda_2\theta)^{\sigma_1\tau_2} & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdots \\ \lambda_1^{\sigma_n\tau_2} & (\lambda_1\theta)^{\sigma_n\tau_2} & \cdots & (\lambda_1\theta^{n-1})^{\sigma_n\tau_2} & \lambda_2^{\sigma_n\tau_2} & (\lambda_2\theta)^{\sigma_n\tau_2} & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdots \\ \lambda_1^{\sigma_n\tau_r} & (\lambda_1\theta)^{\sigma_n\tau_r} & \cdots & (\lambda_1\theta^{n-1})^{\sigma_n\tau_r} & \lambda_2^{\sigma_n\tau_r} & (\lambda_2\theta)^{\sigma_n\tau_r} & \cdots \end{vmatrix}^2 .$$

If we set

$$\Gamma = \begin{pmatrix} 1 & \theta^{\sigma_1} & \cdots & (\theta^{n-1})^{\sigma_1} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 1 & \theta^{\sigma_n} & \cdots & (\theta^{n-1})^{\sigma_n} \end{pmatrix} \quad \text{and} \quad \Gamma^{\tau_i} = \begin{pmatrix} 1 & \theta^{\sigma_1\tau_i} & \cdots & (\theta^{n-1})^{\sigma_1\tau_i} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 1 & \theta^{\sigma_n\tau_i} & \cdots & (\theta^{n-1})^{\sigma_n\tau_i} \end{pmatrix},$$

then

$$d_{\mathbb{Q}}(\gamma_1,\dots,\gamma_{rn}) = \begin{vmatrix} \lambda_1^{\tau_1}\Gamma^{\tau_1} & \lambda_2^{\tau_1}\Gamma^{\tau_1} & \cdots & \lambda_r^{\tau_1}\Gamma^{\tau_1} \\ \lambda_1^{\tau_2}\Gamma^{\tau_2} & \lambda_2^{\tau_2}\Gamma^{\tau_2} & \cdots & \lambda_r^{\tau_2}\Gamma^{\tau_2} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \lambda_1^{\tau_r}\Gamma^{\tau_r} & \lambda_2^{\tau_r}\Gamma^{\tau_r} & \cdots & \lambda_r^{\tau_r}\Gamma^{\tau_r} \end{vmatrix}^2$$

$$= \begin{vmatrix} \Gamma^{\tau_1} & 0 & \cdots & 0 \\ 0 & \Gamma^{\tau_2} & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & \Gamma^{\tau_r} \end{vmatrix}^2 \begin{vmatrix} \lambda_1^{\tau_1} I_n & \lambda_2^{\tau_1} I_n & \cdots & \lambda_r^{\tau_1} I_n \\ \lambda_1^{\tau_2} I_n & \lambda_2^{\tau_2} I_n & \cdots & \lambda_r^{\tau_2} I_n \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \lambda_1^{\tau_r} I_n & \lambda_2^{\tau_r} I_n & \cdots & \lambda_r^{\tau_r} I_n \end{vmatrix}^2,$$

where I_n is the identity matrix of size n. Since $|\Gamma^{\tau_i}| = |\Gamma|^{\tau_i}$ for all i, we have

$$|\Gamma^{\tau_1} \cdots \Gamma^{\tau_r}|^2 = N_k(|\Gamma|^2) = N_k(d_k(\theta)).$$

Hence

$$d_{\mathbb{Q}}(\gamma_1, \ldots, \gamma_{rn}) = N_k(d_k(\theta))d(k/\mathbb{Q})^n,$$

which gives the second identity of (2.3).

From (2.3) and the transitivity property of differents, $\mathfrak{D}(L/\mathbb{Q}) = \mathfrak{D}(L/k)\mathfrak{D}(k/\mathbb{Q})$, we get

$$|N_k(d_k(\theta)| = \mathfrak{N}(d(L/k))(O_L : O_k[\theta])^2. \tag{2.4}$$

Hence from (2.1), we obtain (2.2). ■

Note that when $k = \mathbb{Q}$, the index ideal $\mathfrak{I}(L/\mathbb{Q})$ is generated by $I(L/\mathbb{Q})$.

3. Indices of subfields of cyclotomic $\mathbb{Z}_p$-extensions. In this section, we study the indices of subfields of cyclotomic $\mathbb{Z}_p$-extensions, which turn out to be closely related to Fermat quotients.

First, we consider which subfields of cyclotomic $\mathbb{Z}_p$-extensions of number fields have relative integral bases. Let p be a prime, k an extension of $\mathbb{Q}$ of degree r, and K_n the nth layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ as in the Introduction. Then we can easily prove the following proposition about Steinitz classes.

Proposition 3.1. *Set $L_n = kK_n$. If*

$$pO_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \quad \text{with } \mathfrak{p}_i \text{ a prime ideal of } k \text{ and } e_i \geq 1 \text{ for each } i$$

is the factorization of pO_k into primes and $(e_i, p) = 1$ for each i, then the Steinitz class of L_n/k is given by

$$\mathrm{St}(L_n/k) = \Big[\prod_{i=1}^{g} \mathfrak{p}_i^{-(e_i-1)(p^n-1)/2}\Big] = \begin{cases} [(\prod_{i=1}^g \mathfrak{p}_i)^{(p^n-1)/2}] & \text{for } p \neq 2, \\ [(\prod_{i=1}^g \mathfrak{p}_i^{-(e_i-1)/2})^{2^n-1}] & \text{for } p = 2. \end{cases}$$

Proof. First we note that L_n is the nth layer of the cyclotomic $\mathbb{Z}_p$-extension of k, for $k \cap K_1 = \mathbb{Q}$ under our assumptions. Let $\{\lambda_1, \ldots, \lambda_{p^n}\}$ be an integral basis of K_n. Then $\{\lambda_1, \ldots, \lambda_{p^n}\}$ is a basis for L_n over k. So from Proposition 2.1(ii), we have

$$\frac{d(L_n/k)}{(d_k(\lambda_1, \ldots, \lambda_{p^n}))} = (\mathfrak{a} \cdot \det A)^2$$

for some ideal $\mathfrak{a}$ of k and a matrix A with entries in k. Since $d_k(\lambda_1, \ldots, \lambda_{p^n}) = d_{\mathbb{Q}}(\lambda_1, \ldots, \lambda_{p^n}) = d(K_n/\mathbb{Q})$, we get

$$\frac{d(L_n/k)}{(d(K_n/\mathbb{Q}))} = (\mathfrak{a} \cdot \det A)^2.$$

Now the Steinitz class is given by $[\mathfrak{a}]$, so we need to compute the left hand side.

Let $pO_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ be the factorization of pO_k into primes as in the statement of the proposition. Then from the assumption $(e_i, p) = 1$, $\mathfrak{p}_i$ is totally ramified in L_n and divides $d(L_n/k)$ for each i. Also $d(L_n/k)$ does not have other prime factors than $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ by the basic properties of $\mathbb{Z}_p$-extensions. From the relation between the (global) discriminant and the local ones, we have

$$d(L_n/k) = \prod_{i=1}^{g} d_{\mathfrak{p}_i}(L_n/k) \quad \text{with} \quad d_{\mathfrak{p}_i}(L_n/k) = d((L_n)_{\mathfrak{P}_i}/k_{\mathfrak{p}_i}),$$

where $\mathfrak{P}_i$ is the unique prime ideal of L_n lying above $\mathfrak{p}_i$, and $(L_n)_{\mathfrak{P}_i}$ and $k_{\mathfrak{p}_i}$ are completions of L_n and k with respect to $\mathfrak{P}_i$ and $\mathfrak{p}_i$, respectively.

To compute the local discriminant, take a prime ideal $\mathfrak{p} = \mathfrak{p}_i$ of k lying above p with ramification index e and residual degree f, and take the unique prime ideal $\mathfrak{P}$ of L_n lying above $\mathfrak{p}$ and the unique prime ideal $\mathfrak{Q}$ of K_n lying above p, respectively. We consider completions of $\mathbb{Q}$, k, K_n and L_n with respect to p, $\mathfrak{p}$, $\mathfrak{Q}$ and $\mathfrak{P}$, and denote them by $\mathbb{Q}_p$, $k_{\mathfrak{p}}$, $(K_n)_{\mathfrak{Q}}$ and $(L_n)_{\mathfrak{P}}$, respectively. If we write the valuation of each discriminant by $\tilde{d}$, then we have

$$\begin{aligned}\tilde{d}((L_n)_{\mathfrak{P}}/\mathbb{Q}_p) &= p^n \cdot \tilde{d}(k_{\mathfrak{p}}/\mathbb{Q}_p) + f \cdot \tilde{d}((L_n)_{\mathfrak{P}}/k_{\mathfrak{p}}) \\ &= ef \cdot \tilde{d}((K_n)_{\mathfrak{Q}}/\mathbb{Q}_p) + \tilde{d}((L_n)_{\mathfrak{P}}/(K_n)_{\mathfrak{Q}}),\end{aligned}$$

so

$$\tilde{d}((L_n)_{\mathfrak{P}}/k_{\mathfrak{p}}) - e \cdot \tilde{d}((K_n)_{\mathfrak{Q}}/\mathbb{Q}_p) = \frac{1}{f}\{\tilde{d}((L_n)_{\mathfrak{P}}/(K_n)_{\mathfrak{Q}}) - p^n \cdot \tilde{d}(k_{\mathfrak{p}}/\mathbb{Q}_p)\}.$$

From $(e,\ p) = 1$, we know that $\tilde{d}(k_{\mathfrak{p}}/\mathbb{Q}_p) = \tilde{d}((L_n)_{\mathfrak{P}}/(K_n)_{\mathfrak{Q}}) = f(e-1)$. So if we set $\tilde{d}((L_n)_{\mathfrak{P}}/k_{\mathfrak{p}}) = l$ and $\tilde{d}((K_n)_{\mathfrak{Q}}/\mathbb{Q}_p) = s$, then we get

$$\tilde{d}((L_n)_{\mathfrak{P}}/k_{\mathfrak{p}}) - e \cdot \tilde{d}((K_n)_{\mathfrak{Q}}/\mathbb{Q}_p) = l - es = -(e-1)(p^n-1),$$

which gives the exponent of $\mathfrak{p} = \mathfrak{p}_i$ in $d(L_n/k)/(d(K_n/\mathbb{Q}))$.

Thus if we denote e and l for each $\mathfrak{p}_i$ and $\mathfrak{P}_i$ by e_i and l_i, respectively, then we have

$$\frac{d(L_n/k)}{(d(K_n/\mathbb{Q}))} = (\mathfrak{a} \cdot \det A)^2 = \prod_{i=1}^{g} \mathfrak{p}_i^{l_i - e_i s} = \prod_{i=1}^{g} \mathfrak{p}_i^{-(e_i-1)(p^n-1)}.$$

So the Steinitz class is given by

$$\mathrm{St}(L_n/k) = [\mathfrak{a}] = \Big[\prod_{i=1}^{g} \mathfrak{p}_i^{-(e_i-1)(p^n-1)/2}\Big].$$

When $p \neq 2$, since $[\prod_{i=1}^{g} \mathfrak{p}_i^{e_i}] = 1$, we obtain the desired form. When $p = 2$, e_i is odd for each i, and we obtain the result. ∎

Corollary 3.2. *Let the notation and assumptions be as in Proposition 3.1, and further assume that $g = 1$, i.e., $pO_k = \mathfrak{p}_1^{e_1}$. Then* $\mathrm{St}(L_n/k) = 1$ *if and only if the order of* $[\mathfrak{p}_1]$ *in the ideal class group of k divides* $(p^n - 1)/2$ *for $p \neq 2$ and $2^n - 1$ for $p = 2$. So in that case, L_n has a RIB over k.*

Proof. We only note that when $p = 2$ and $\mathrm{St}(L_n/k) = 1$, the order ν of $[\mathfrak{p}_1]$ in the ideal class group of k divides both e_1 and $\frac{e_1-1}{2}(2^n - 1)$. So $\nu \mid 2^n - 1$. The rest is trivial. ■

Remark 3.3. (i) From Proposition 3.1, if p is unramified in k, then L_n has a RIB over k. This can also be seen from $O_{L_n} = O_k O_{K_n}$, which holds under our assumptions.

(ii) In Corollary 3.2, if e_1 divides $(p^n - 1)/2$ for $p \neq 2$ or $2^n - 1$ for $p = 2$, then $\mathrm{St}(L_n/k) = 1$ and L_n has a RIB over k.

Now we consider the indices of $K_n/\mathbb{Q}$ and L_n/k. For that, we need to generalize Fermat quotients to higher degree.

Definition 3.4 ([Hl]). Let n be a positive integer and a an integer coprime to p odd. If $a^{p-1} \equiv 1 \pmod{p^n}$, we set

$$F_{p,n}(a) = \frac{a^{p-1} - 1}{p^n},$$

and call it the *nth degree Fermat quotient of a with respect to p*. For $n = 1$, this is the usual Fermat quotient with base a. We note that the definition of $F_{p,n}(a)$ a priori assumes that a satisfies the congruence $a^{p-1} \equiv 1 \pmod{p^n}$. Also, notice that for an odd prime q, $F_{p,n}(q) \equiv 0 \pmod{p}$ if and only if q splits completely in K_n.

Theorem 3.5 ([AO, Corollary 2]). *Let k be an extension of $\mathbb{Q}$ of degree r such that either p is unramified in k, or k is Galois over $\mathbb{Q}$, and define $L_n = kK_n$. If $(p, r) = 1$ and $p - 1 \nmid 2r$, then O_{L_n} does not have a power basis over O_k. In particular, O_{K_n} does not have a power basis for $p \geq 5$.*

From this, it is meaningful to consider the indices $I(L_n/k)$ and $I(K_n/\mathbb{Q})$, and for $I(K_n/\mathbb{Q})$ we have the following:

Theorem 3.6. *Let q be a prime. Then for $p \geq 5$,*

$$q \mid I(K_n/\mathbb{Q}) \quad \text{if and only if} \quad 2 \leq q < p^n \text{ and } F_{p,n}(q) \equiv 0 \pmod{p}.$$

In this case, the highest exponent λ of q dividing $I(K_n/\mathbb{Q})$ is given by

$$\lambda = \sum_{i \geq 1} s_i \left\{ p^n - q^i \frac{s_i + 1}{2} \right\} \quad \text{with} \quad s_i = \left[\frac{p^n}{q^i} \right]. \tag{3.1}$$

Proof. Suppose that the prime ideal $\mathfrak{Q}$ of K_n lying above q ($\neq p$) has the residual degree $f_n(\mathfrak{Q}) = p^k$ with $k \geq 1$. Then the prime $\mathfrak{Q}'$ of K_{n-1} lying above q has $f_{n-1}(\mathfrak{Q}') = p^{k-1}$, so $q^{p^{k-1}(p-1)} \equiv 1 \pmod{p^n}$. Hence

$$q^{p^{k-1}(p-1)} > p^n,$$

which implies, with the same notation as in Theorem 2.4,

$$\begin{aligned}\pi_q(f_n(\mathfrak{Q})) \cdot f_n(\mathfrak{Q}) &= q^{p^k} - q^{p^{k-1}} \\ &> q^{p^{k-1}}(p^n - 1) \geq 2(p^n - 1) \geq p^n \\ &= r_q(f_n(\mathfrak{Q})) \cdot f_n(\mathfrak{Q}),\end{aligned}$$

so $\pi_q(f_n(\mathfrak{Q})) \geq r_q(f_n(\mathfrak{Q}))$. Hence q does not divide $I(K_n/\mathbb{Q})$. For $q = p$, $f_n(\mathfrak{Q}) = 1$ for all n and $r_p(1) = 1$ in Theorem 2.4, so p does not divide $I(K_n/\mathbb{Q})$. Hence the prime q that divides $I(K_n/\mathbb{Q})$ has to split completely in K_n, which implies $F_{p,n}(q) \equiv 0 \pmod{p}$. Hence from Proposition 2.5(i), for a prime q,

$$q \mid I(K_n/\mathbb{Q}) \quad \text{if and only if} \quad 2 \leq q < p^n \text{ and } F_{p,n}(q) \equiv 0 \pmod{p}.$$

As for the highest exponent λ of q dividing $I(K_n/\mathbb{Q})$, we refer to the result of Engstrom [E, Theorem 3], for q splits completely in K_n. ∎

Remark 3.7. In the proof of Theorem 3.6, we have shown the results without the assumption $p \geq 5$. Since $I(K_n/\mathbb{Q}) = 1$ for $p = 3$, this implies that for any positive integer n there are no primes q satisfying $q < 3^n$ and $q^2 \equiv 1 \pmod{3^{n+1}}$, but this is of course obvious from Proposition 2.5(i).

As for $I(L_n/k)$, we have the following:

Theorem 3.8. *Let $k/\mathbb{Q}$ be a Galois extension of degree r with r a prime satisfying $r \neq p$, and $L_n = kK_n$. For a prime q, we have:*

(i) *If $q \mid I(L_n/k)$, then $q \mid I(K_n/\mathbb{Q})$.*
(ii) *Suppose $q \mid I(K_n/\mathbb{Q})$. Then the following hold:*
   (a) *When q splits completely in k, we have $q \mid I(L_n/k)$. In this case, the highest exponent χ of q dividing $I(L_n/k)$ is $\chi = r\lambda'$.*
   (b) *When q is a prime in k, we have $q \mid I(L_n/k)$ only if $q^r < p^n$. In this case, $\chi = r\lambda'$.*
   (c) *When q is ramified in k, we have $q \mid I(L_n/k)$. In this case, $\chi = \lambda'$.*

   Here λ' is the highest exponent dividing $\mathfrak{I}(L_n/k)$ of a prime ideal $\mathfrak{q}$ of k lying above q, which is given by

$$\lambda' = \sum_{i \geq 1} s'_i \left\{ p^n - (\mathfrak{N}(\mathfrak{q}))^i \, \frac{s'_i + 1}{2} \right\} \quad \text{with} \quad s'_i = \left[\frac{p^n}{\mathfrak{N}(\mathfrak{q})^i} \right]. \tag{3.2}$$

Proof. Let θ be an integral primitive element of K_n over $\mathbb{Q}$, so $K_n = \mathbb{Q}(\theta)$ and $L_n = k(\theta)$. If we set $\mathfrak{N}(d(L_n/k)) = p^d$, then from (2.4) we have

$$|N_k(d_k(\theta))| = \mathfrak{N}(d(L_n/k))(O_{L_n} : O_k[\theta])^2 = p^d(O_{L_n} : O_k[\theta])^2.$$

On the other hand, if we set $d(K_n/\mathbb{Q}) = p^{d_0}$, then

$$d_k(\theta) = d_{\mathbb{Q}}(\theta) = d(K_n/\mathbb{Q})(O_{K_n} : \mathbb{Z}[\theta])^2 = p^{d_0}(O_{K_n} : \mathbb{Z}[\theta])^2,$$

so we obtain

$$(O_{L_n} : O_k[\theta])^2 = p^{rd_0-d}(O_{K_n} : \mathbb{Z}[\theta])^{2r} \tag{3.3}$$

for any integral primitive element θ of K_n over $\mathbb{Q}$.

For the proof of (i), take a prime q satisfying $q \mid I(L_n/k)$. Assume first $q \neq p$. Then from (3.3), $q \mid (O_{K_n} : \mathbb{Z}[\theta])$ for any θ, which means that $q \mid I(K_n/\mathbb{Q})$. Assume next $q = p$. If p is unramified in k, the unique prime ideal $\mathfrak{Q}$ of K_n lying above p is also unramified in L_n. From the relation $\mathfrak{D}(L_n/k)\mathfrak{D}(k/\mathbb{Q}) = \mathfrak{D}(L_n/K_n)\mathfrak{D}(K_n/\mathbb{Q})$ among differents, we have $rd_0 = d$, so $p \mid (O_{K_n} : \mathbb{Z}[\theta])$ for any θ, which means $p \mid I(K_n/\mathbb{Q})$. This contradicts Theorem 3.6. If p is ramified in k, let $\mathfrak{p}$ be the unique prime ideal of k lying above p. Then $\mathfrak{p}$ is totally ramified in L_n, so the number $r_{\mathfrak{p}}(f)$ of prime ideals in L_n lying above $\mathfrak{p}$ of residual degree f is given by

$$r_{\mathfrak{p}}(f) = \begin{cases} 1 & \text{if } f = 1, \\ 0 & \text{if } f > 1. \end{cases}$$

Hence from Theorem 2.4, $\mathfrak{p} \nmid \mathfrak{I}(L_n/k)$, which implies $p \nmid I(L_n/k)$ by (2.2). So this does not happen either, and we finish the proof of (i).

For the proof of (ii), suppose $q \mid I(K_n/\mathbb{Q})$. So $2 \le q < p^n$ and q splits completely in K_n by Theorem 3.6. Let $\mathfrak{q}$ be a prime ideal of k lying above q. Then $\mathfrak{q}$ splits completely in L_n. Hence from Proposition 2.5(i), we have

$$\mathfrak{q} \mid \mathfrak{I}(L_n/k) \quad \text{if and only if} \quad \mathfrak{N}(\mathfrak{q}) = q^{f_0} < p^n, \tag{3.4}$$

where f_0 is the residual degree of $\mathfrak{q}$ over q. For the formula (3.2) for the highest exponent λ' of $\mathfrak{q}$ dividing $\mathfrak{I}(L_n/k)$, we refer to the proof of Theorem 2 in [DD], or we can show it similarly to the case of $K_n/\mathbb{Q}$, since $\mathfrak{q}$ splits completely in L_n (cf. [Hn] and [E, Theorem 3]). In fact, λ' is equal to

$$\sum_{j=1}^{p^n-1} \sum_{l \ge 1} \left[\frac{j}{\mathfrak{N}(\mathfrak{q})^l} \right].$$

For cases (b) and (c), $\mathfrak{q}$ is the only prime ideal of k lying above q. So from (2.2) we have

$$\mathfrak{q}^{\lambda'} \parallel \mathfrak{I}(L_n/k) \quad \text{if and only if} \quad q^{f_0\lambda'} \parallel I(L_n/k),$$

where $a^\mu \parallel b$ means that $a^\mu \mid b$ and $a^{\mu+1} \nmid b$ for a prime or a prime ideal a. So from (3.4), we have

$$q \mid I(L_n/k) \quad \text{if and only if} \quad \mathfrak{N}(\mathfrak{q}) = q^{f_0} < p^n,$$

which finishes the proof of (b) and (c).

For (a), let $qO_k = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ be the factorization of qO_k into primes in k. Since $\mathfrak{N}(\mathfrak{q}_i) = q < p^n$, from (3.4) we have $\mathfrak{q}_i \mid \mathfrak{I}(L_n/k)$ for each i. Hence $q \mid I(L_n/k)$ from Proposition 2.5(ii). Let χ be the highest exponent of q dividing $I(L_n/k)$. Since $\mathfrak{q}_i^{\lambda'} \parallel \mathfrak{I}(L_n/k)$ for each i, we have $q^{\lambda'} \mid \mathfrak{I}(L_n/k)$, which implies $\mathfrak{N}((q^{\lambda'})) = q^{r\lambda'} \mid I(L_n/k)$ by Proposition 2.5(ii). Hence $r\lambda' \le \chi$. Now $\lambda' = \lambda$ in (3.1) and $q^\lambda \parallel I(K_n/\mathbb{Q})$, so there is an integral primitive element θ_0 for $K_n/\mathbb{Q}$ such that $q^\lambda \parallel (O_{K_n} : \mathbb{Z}[\theta_0])$. Then from (3.3), we have $q^{r\lambda} \parallel (O_{L_n} : O_k[\theta_0])$, which gives $\chi \le r\lambda = r\lambda'$, so $\chi = r\lambda'$. This completes the proof of (ii). ■

4. Examples. In this section, we give some examples of indices of $K_n/\mathbb{Q}$ for $n = 1, 2, 3$. From Theorem 3.6, we know that primes q dividing $I(K_n/\mathbb{Q})$ are those satisfying

$$2 \le q < p^n \quad \text{and} \quad F_{p,n}(q) \equiv 0 \pmod p.$$

For $n = 1$, there is a long list of these primes in [EM], so here we only list those p's in $5 \le p < 2700$ with $I(K_1/\mathbb{Q}) > 1$. Also we list those in $5 \le p < 2800$ and in $5 \le p < 500$ for $n = 2$ and $n = 3$, respectively.

Table 1. p and $I(K_1/\mathbb{Q})$ (> 1) for $5 \le p < 2700$

p	$I(K_1/\mathbb{Q})$	p	$I(K_1/\mathbb{Q})$	p	$I(K_1/\mathbb{Q})$	p	$I(K_1/\mathbb{Q})$
11	3^{17}	43	19^{29}	59	53^{6}	71	11^{195}
79	31^{65}	97	53^{44}	103	43^{77}	137	19^{427}
263	79^{315}	331	71^{614}	349	$223^{126}317^{32}$	359	$257^{102}331^{28}$
421	251^{170}	433	349^{84}	487	307^{180}	523	241^{323}
653	197^{777}	659	503^{156}	743	467^{276}	859	643^{216}
863	13^{29995}	907	$127^{2793}761^{146}$	919	457^{467}	983	419^{709}
1069	487^{677}	1087	617^{470}	1091	691^{400}	1093	2^{591387}
1163	241^{2242}	1223	997^{226}	1229	821^{408}	1279	683^{596}
1381	653^{803}	1483	$421^{1923}1061^{422}$	1499	941^{558}	1549	1069^{480}
1657	1481^{176}	1663	709^{1199}	1667	463^{2223}	1697	$461^{2325}857^{840}$
1747	1153^{594}	1777	1381^{396}	1787	631^{1681}	1789	449^{2673}
1877	1091^{786}	1993	$277^{6195}1747^{246}$	2011	1993^{18}	2213	367^{5571}
2221	659^{2709}	2251	151^{15659}	2281	1657^{624}	2309	$823^{2149}1453^{856}$
2371	1493^{878}	2393	431^{5500}	2473	1787^{686}	2671	2063^{608}

Table 2. p and $I(K_2/\mathbb{Q})$ (> 1) for $5 \leq p < 2800$

p	$I(K_2/\mathbb{Q})$	p	$I(K_2/\mathbb{Q})$	p	$I(K_2/\mathbb{Q})$
7	19^{41}	37	691^{678}	79	1523^{9734}
101	4943^{5573}	107	5573^{6179}	167	17987^{9902}
193	31019^{6230}	251	$33767^{29234}54973^{8028}$	293	33301^{71795}
337	24733^{206946}	383	$6619^{1552551}$	761	252709^{400115}
761	363767^{215354}	769	500413^{90948}	919	478273^{366288}
1049	$403079^{991565}668179^{432222}$	1213	864503^{606866}	1249	$238397^{4353669}$
1277	$536621^{1672461}$	1373	$192317^{8311896}$	1429	$376237^{4566650}$
1447	$416849^{4216310}$	1487	1293203^{917966}	1567	1663223^{792266}
1667	$1113401^{2217575}$	1811	2843213^{436508}	2083	$1360067^{4856265}$
2111	$351361^{26069694}$	2341	$1937557^{5147891}$	2389	$2421743^{4149413}$
2549	$4505707^{1991694}$	2593	$4316051^{2407598}$	2777	$6351629^{1360100}$

Table 3. p and $I(K_3/\mathbb{Q})$ (> 1) for $5 \leq p < 500$

p	$I(K_3/\mathbb{Q})$	p	$I(K_3/\mathbb{Q})$	p	$I(K_3/\mathbb{Q})$
13	239^{9018}	19	2819^{5261}	107	$119551^{5675125}$
137	$598987^{4295542}$	281	$5774911^{31914657}$	467	$38870627^{87083245}$
491	$69695929^{48674842}$	...	...	...	...

Acknowledgements. The authors wish to express their thanks to K. Matsuno for useful advice.

References

[AO] S. Akizuki and K. Ota, *On power bases for rings of integers of relative Galois extensions*, Bull. London Math. Soc. 45 (2013), 447–452.

[A] E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, in: Colloq. Int. CNRS 24, Paris, 1950, 19–20.

[DD] I. Del Corso and R. Dvornicich, *On Ore's conjecture and its developments*, Trans. Amer. Math. Soc. 357 (2005), 3813–3829.

[DK] F. G. Dorais and D. Klyve, *A Wieferich prime search up to* 6.6×10^{15}, J. Integer Sequences 14 (2011), art. 11.9.2.

[E] H. T. Engstrom, *On the common index divisor of an algebraic field*, Trans. Amer. Math. Soc. 32 (1930), 223–237.

[EM] R. Ernvall and T. Metsänkylä, *Tables of vanishing Fermat quotients*, users.utu.fi/taumets/fermat/fermat.htm.

[G] I. Gaál, *Diophantine Equations and Power Integral Bases. New Computational Methods*, Birkhäuser, 2002.

[Gr1] M.-N. Gras, *Non monogénéité de l'anneau des entiers de certaines extensions abéliennes de* $\mathbb{Q}$, Publ. Math. Fac. Sci. Besançon, Théor. Nombres 1983–1984, exp. 5, 25 pp.

[Gr2] M.-N. Gras, *Non monogénéité de l'anneau des entiers des extensions cycliques de* $\mathbb{Q}$ *de degré premier* $l \geq 5$, J. Number Theory 23 (1986), 347–353.

[Gy] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné, III*, Publ. Math. Debrecen 23 (1976), 141–165.

[H] H. Hasse, *Number Theory*, Grundlehren Math. Wiss. 229, Springer, 1980.

[Hl] G. Helms, *Fermat-/Euler-quotients* $(a^{p-1}-1)/p^k$ *with arbitrary* k, http://go.helms-net.de/math/expdioph/fermatquotients.pdf.

[Hn] K. Hensel, *Ueber den grössten gemeinsamen Theiler aller Zahlen, welche durch eine ganze Function von* n *Veränderlichen darstellbar sind*, J. Reine Angew. Math. 116 (1896), 350–356.

[I-H] Y. Ihara (translated and supplemented by S. Hahn), *On Fermat quotient and "differentiation of numbers"*, Univ. of Georgia Math. Preprint Series No. 9, Vol. 2 (1994), 1–16.

[N] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer Monogr. Math., Springer, 2004.

[Na] E. Nart, *On the index of a number field*, Trans. Amer. Math. Soc. 289 (1985), 171–183.

[O] Ö. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. 99 (1928), 84–117.

[S] J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory 30 (1988), 226–237.

[Sl] J. Śliwa, *On the nonessential discriminant divisor of an algebraic number field*, Acta Arith. 42 (1982), 57–72.

Yoko Inoue, Kaori Ota
Department of Mathematics
Tsuda College
2-1-1 Tsuda-cho, Kodaira-shi, Tokyo 187-8577, Japan
E-mail: ota@tsuda.ac.jp

Received on 18.3.2014
and in revised form on 14.3.2015 (7756)