

ON ORE'S CONJECTURE AND ITS DEVELOPMENTS

ILARIA DEL CORSO AND ROBERTO DVORNICICH

ABSTRACT. The p -component of the index of a number field K , $\text{ind}_p(K)$, depends only on the completions of K at the primes over p . More precisely, $\text{ind}_p(K)$ equals the index of the \mathbb{Q}_p -algebra $K \otimes \mathbb{Q}_p$. If K is normal, then $K \otimes \mathbb{Q}_p \cong L^n$ for some L normal over \mathbb{Q}_p and some n , and we write $I_p(nL)$ for its index. In this paper we describe an effective procedure to compute $I_p(nL)$ for all n and all normal and tamely ramified extensions L of \mathbb{Q}_p , hence to determine $\text{ind}_p(K)$ for all Galois number fields that are tamely ramified at p . Using our procedure, we are able to exhibit a counterexample to a conjecture of Nart (1985) on the behaviour of $I_p(nL)$.

1. INTRODUCTION

Let K be a number field and let R_K be its ring of integers. The index of a number field K is defined as

$$\text{ind}(K) = \gcd\{\text{ind}(\theta) \mid \theta \in R_K, K = \mathbb{Q}(\theta)\},$$

where $\text{ind}(\theta) = [R_K : \mathbb{Z}[\theta]]$ denotes the index of the element θ .

Let $\text{ind}(K) = \prod_p p^{s_p(K)}$ be the factorization of $\text{ind}(K)$ into primes, and let $\text{ind}_p(K) = s_p(K)$. The problem of finding formulas giving $\text{ind}_p(K)$ for all primes p and all number fields K is still open, and appears as Problem 22 in the list of unsolved problems in Narkiewicz' book [3].

Dedekind [1] characterized when a rational prime p divides $\text{ind}(K)$ in terms of the form of the factorization of the ideal (p) in R_K , thus settling completely the question of deciding whether $\text{ind}_p(K) = 0$ or not, but leaving open the problem of determining $\text{ind}_p(K)$ exactly when it is positive.

Contrary to the characterization given by Dedekind, Ore conjectured in 1928 [5] that the factorization type of (p) in R_K is not sufficient, in general, for deciding what is the actual value of $\text{ind}_p(K)$. Soon after, in 1930, Engstrom [2] proved Ore's conjecture by exhibiting two number fields K_1, K_2 , of degree 8 over \mathbb{Q} , with the same factorization type of (3) , but such that $\text{ind}_3(K_1) \neq \text{ind}_3(K_2)$.

In the same paper, however, Engstrom gave an explicit formula for $\text{ind}_p(K)$ when p splits completely in K , and showed that in this particular case $\text{ind}_p(K)$ *does* depend only on the factorization type of pR_K or, equivalently, only on the degree $[K : \mathbb{Q}]$.

Also, in 1982 Śliwa [6] proved that, when p is unramified in K , $\text{ind}_p(K)$ is again completely determined by the factorization type of (p) in R_K .

Received by the editors July 31, 2000 and, in revised form, April 20, 2004.
2000 *Mathematics Subject Classification*. Primary 11R04; Secondary 11R99.

In 1985, Nart [4] gave a significant contribution to the understanding of the problem. He associated to each number field K an invariant, $e_p(K)$, which can be interpreted as the isomorphism class of the \mathbb{Q}_p -algebra $K \otimes \mathbb{Q}_p$. To see how $e_p(K)$ relates to the factorization type of (p) in K , decompose $K \otimes \mathbb{Q}_p$ as a direct sum of fields, $K \otimes \mathbb{Q}_p \cong L_1 \oplus \cdots \oplus L_r$, where the L_i 's are the completions of K at the primes lying over p . This decomposition clearly determines the factorization type of (p) in R_K , while two number fields with the same factorization type of (p) can have different completions at some primes over p . This is exactly what happens in Engstrom's example.

In [4, Theorem 1] Nart showed that the invariant $e_p(K)$ completely determines the value of $\text{ind}_p(K)$. More precisely, he proved that $\text{ind}_p(K) = I_p(e_p(K))$, where $I_p(e_p(K))$ is the index of $e_p(K)$, *i.e.* is the minimum power of p which divides $\text{ind}(f)$ when f runs over all polynomials of $\mathbb{Z}_p[X]$ such that $\mathbb{Q}_p[X]/(f(X)) \cong K \otimes \mathbb{Q}_p$ (see Section 2 for details).

From this characterization it follows that the problem of the explicit computation of the index of a number field can be reduced to a problem in local fields. Using local techniques, Nart also obtained a generalization of Engstrom's formula to splittings that have an unrestricted number of primes of degree 1 and a limited number of totally ramified primes. In this case the index depends only on the factorization type of (p) and on the multiplicities n_i of the isomorphism classes $[L]$ in the decomposition of $K \otimes \mathbb{Q}_p$ as a sum of finite extensions of \mathbb{Q}_p , but not on the particular classes $[L_i]$ (see [4, Theorem 2]). Although this is not true in general, one may ask if there is a larger class of number fields for which this property holds. In view of these considerations, Nart suggested the following modified version of Ore's conjecture.

Nart's conjecture. *Let L, L' be two Galois extensions of \mathbb{Q}_p with the same ramification numbers (*i.e.* $[L : \mathbb{Q}_p] = [L' : \mathbb{Q}_p]$) and the i -th ramification groups of $\text{Gal}(L/\mathbb{Q}_p)$ and $\text{Gal}(L'/\mathbb{Q}_p)$ have the same order for all i). Then*

$$(1) \quad I_p(nL) = I_p(nL') \quad \text{for all } n \in \mathbb{N}.$$

In this paper we start by proving Nart's conjecture in the case where L is a totally and tamely ramified extension of \mathbb{Q}_p . We can remove the assumption that L/\mathbb{Q}_p be normal and we can rather easily prove that in fact $I_p(n[L]) = I_p(n[L'])$ for all n and all pairs (L, L') of tamely and totally ramified extension of \mathbb{Q}_p of the same degree (see Theorem 1).

On the other hand, in Section 6 we give a counterexample to Nart's conjecture. We let L_1 and L_2 be the two normal and tamely ramified extensions of degree 4 over \mathbb{Q}_3 that have ramification index equal to 2, and show that $I_3(13L_1) \neq I_3(13L_2)$.

The main achievement of the paper, however, is the description of an effective procedure to compute $I_p(nL)$ for all n and all normal and tamely ramified extensions L of \mathbb{Q}_p . Observe that, if K/\mathbb{Q} is Galois, then $e_p(K) = rL$ for some r and some Galois extension L of \mathbb{Q}_p . Thus our procedure allows us to determine $\text{ind}_p(K)$ for all Galois number fields that are tamely ramified at p .

To approach the problem, we have found it much more convenient to look for *elements* in $K \otimes \mathbb{Q}_p$ of minimal index instead of minimal polynomials as in [4]. In fact, all integral elements of $K \otimes \mathbb{Q}_p \cong L_1 \oplus \cdots \oplus L_r$ can be easily expressed as r -tuples of power series in the uniformizing elements of the L_i , while it seems

much harder to obtain an equally satisfactory description of the monic polynomials generating $K \otimes \mathbb{Q}_p$.

For an n -tuple $(x^{(1)}, \dots, x^{(n)})$ of integers of L , we have the formula

$$(2) \quad I_p(x^{(1)}, \dots, x^{(n)}) = \sum_{i=1}^n \text{ind}_p(x^{(i)}) + \sum_{1 \leq i < j \leq n} \text{Res}_p(x^{(i)}, x^{(j)}),$$

where we denote by $\text{Res}_p(x^{(i)}, x^{(j)})$ the largest power of p that divides the resultant between the minimal polynomials of $x^{(i)}$ and $x^{(j)}$. Since (2) is clearly symmetric in $x^{(1)}, \dots, x^{(n)}$, in order to compute $I_p(nL)$ we have to explicitly find, for each n , a set $\{x^{(1)}, \dots, x^{(n)}\}$ that minimizes (2). For the small values of n considered by Nart, the problem is fairly easy; in fact, there is a natural choice of $x^{(1)}, \dots, x^{(n)}$ that *simultaneously* minimizes $\text{ind}_p(x^{(i)})$ and $\text{Res}_p(x^{(i)}, x^{(j)})$ for all i, j .

For general n , however, the problem of minimizing (2) is far from being obvious. For instance, let L be a quadratic ramified extension of \mathbb{Q}_3 ; in [4, Example 3.4] it is shown that, for $n \geq 7$, the minimum cannot be reached by choosing the $x^{(i)}$'s of minimal possible index, since this choice would increase the sum $\sum \text{Res}_p(x^{(i)}, x^{(j)})$ too much.

As in many problems of minimizing a sum of terms that are not independent of each other, it turns out that, for large values of n , the minimum does not correspond to a simultaneous minimum of all terms, but rather to a balance among all terms.

A great advantage in studying such problems can come from an inductive argument. This can be used, for instance, if one can prove that a minimizing set with $n+1$ elements can be obtained by just *adjoining* one new element to a minimizing set with n elements.

Assuming that L is a normal and tamely ramified extension of \mathbb{Q}_p , we shall show that this is actually the case. At the same time, we shall describe a recursive effective procedure for finding an infinite sequence $\omega_0, \omega_1, \dots$ of integers of L such that, for all n , the set $\{\omega_0, \omega_1, \dots, \omega_{n-1}\}$ minimizes (2) (Theorem 2).

An important feature of this procedure is that it allows us to compute $I_p(nL)$ in an effective way, and in particular to show that it is a convex function of n .

A detailed analysis of our construction has led us to check that, already in the tamely ramified case, $I_p(nL)$ cannot be determined in terms of f and e only.

In fact, the fields L_1 and L_2 in the example of Section 6 are both Galois extensions of \mathbb{Q}_3 with $e = f = 2$, but their Galois groups are not isomorphic. It would be interesting to establish whether, restricting to the case of tamely ramified extensions L, L' with $\text{Gal}(L/\mathbb{Q}_p) \cong \text{Gal}(L'/\mathbb{Q}_p)$, conclusion (1) holds true.

2. PRELIMINARIES AND CONJECTURES

In this section we introduce some notation and briefly recall the principal results of [4].

By the letter p we shall always denote a fixed prime number.

For a number field K we let R_K be its ring of integers. As usual, \mathbb{Q}_p and \mathbb{Z}_p are the field and the ring of p -adic numbers, respectively, and $\overline{\mathbb{Q}_p}$ is an algebraic closure of \mathbb{Q}_p . We denote by $|x|$ the p -adic valuation of $\overline{\mathbb{Q}_p}$, normalized so that $|p| = 1$. If m is a non-zero integer, we shall also use the notation $\nu_p(m)$ for $|m|$, *i.e.* the largest power of p dividing m .

If L is a finitely generated extension of \mathbb{Q}_p , we let \mathcal{O}_L be the integral closure of \mathbb{Z}_p in L . If $x, y \in \mathcal{O}_L$ are such that $\mathbb{Q}_p(x) = \mathbb{Q}_p(y) = L$, we denote by f_x and f_y the minimal polynomials over $\mathbb{Z}_p[X]$ of x and y , respectively. We let $\text{disc}(x)$ be the discriminant of x , $\text{ind}(x) = [\mathcal{O}_L : \mathbb{Z}_p[x]]$ and $\text{Res}(f_x, f_y)$ be the resultant of f_x and f_y . Finally, we put $\text{disc}_p(x) = |\text{disc}(x)|$, $\text{ind}_p(x) = |\text{ind}(x)|$ and $\text{Res}_p(x, y) = |\text{Res}(f_x, f_y)|$.

Definition 1. For $\mathbf{x} = (x^{(1)}, \dots, x^{(r)}) \in \mathcal{O}_{L_1} \oplus \dots \oplus \mathcal{O}_{L_r}$ we define

$$I_p(\mathbf{x}) = \left\{ \sum_{1 \leq i < j \leq r} \text{Res}_p(x^{(i)}, x^{(j)}) + \sum_{i=1}^r \text{ind}_p(x^{(i)}) \right\}.$$

Since both $\text{ind}_p(x^{(i)})$ and $\text{Res}_p(x^{(i)}, x^{(j)})$ are symmetric in the conjugates of the $x^{(i)}$, it is clear that the set of values of $I_p(\mathbf{x})$ depends only on the isomorphism class of the fields L_i .

To put it into a more invariant way, consider the set \mathcal{E} of isomorphism classes $[L]$ of finite extension of \mathbb{Q}_p in $\overline{\mathbb{Q}_p}$. For each $[L] \in \mathcal{E}$, denote by \mathcal{O}_L the ring of integers of any field in $[L]$. Let $\bar{\mathcal{E}}$ be the free abelian monoid generated by \mathcal{E} . For $\Gamma = [L_1] + \dots + [L_r] \in \bar{\mathcal{E}}$ we define

$$I_p(\Gamma) = \min_{\mathbf{x} \in \mathcal{O}_{L_1} \oplus \dots \oplus \mathcal{O}_{L_r}} I_p(\mathbf{x}).$$

Moreover, we associate to each field K a unique element of $\bar{\mathcal{E}}$,

$$e_p(K) = n_1[L_1] + \dots + n_s[L_s],$$

where n_i is the multiplicity of the isomorphism class $[L_i]$ in the decomposition of $K \otimes \mathbb{Q}_p$.

With this notation we have

Proposition 1 (Nart). *For every number field K ,*

$$\text{ind}_p(K) = I_p(e_p(K)).$$

Proof. See [4, Thm. 1]. □

If p is unramified in K , then $e_p(K)$ is completely determined by the factorization type of pR_K . Hence, in particular, Proposition 1 implies the result of Śliwa [6].

Concerning the actual value of $I_p(e_p(K))$, Nart gave explicit formulas under the following restriction on $e_p(K)$:

$$e_p(K) = m\mathbb{Q}_p + n_1[L_1] + \dots + n_s[L_s],$$

where m is any natural number, L_i are totally ramified extensions of \mathbb{Q}_p of degree $e_i = e_{i,0}p^{\alpha_i}$ ($(e_{i,0}, p) = 1$) and $n_i \leq \frac{p(p-1)}{(e_{i,0}, p-1)}$. In the particular case when p splits completely in K , *i.e.* when $n_i = 0$ for all i , he reobtained Engstrom's formula

$$(3) \quad I_p(m\mathbb{Q}_p) = \sum_{j=1}^{m-1} \nu_p(j!).$$

3. TOTALLY AND TAMELY RAMIFIED EXTENSIONS

Let $L = \mathbb{Q}_p(\pi)$ be a tamely and totally ramified extension of \mathbb{Q}_p , where π is a root of the polynomial $X^e - pa$ for some unit $a \in \mathbb{Q}_p$ and $(e, p) = 1$. Also, let X be the set of Teichmüller representatives in $\mathcal{O}_L = \mathbb{Z}_p[\pi]$ of the residue field $\mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{F}_p$ (we shall assume that $0 \in X$). Note that actually $X \subset \mathbb{Z}_p$ and in particular is independent of L . With this notation, every element $x \in \mathcal{O}_L$ can be written as $x = \sum_{k=0}^{\infty} x_k \pi^k$, where $x_k \in X$ for all k .

We shall denote by $\zeta = \zeta_e$ a primitive e -th root of unity in $\bar{\mathbb{Q}}_p$. For $i = 0, \dots, e-1$, we shall let $\sigma_i : L \rightarrow \bar{\mathbb{Q}}_p$ be the embedding of L over \mathbb{Q}_p defined by $\sigma_i(\pi) = \zeta^i \pi$.

Lemma 1. *Let $x, y \in \mathbb{Z}_p[\pi]$, $x = \sum_{k=0}^{\infty} x_k \pi^k$, $y = \sum_{k=0}^{\infty} y_k \pi^k$. Then $\text{ind}_p(x)$ and $\text{Res}_p(x, y)$ depend only on the sets $\{x_k\}$, $\{y_k\}$ and are independent of a and π .*

Proof. We have

$$(4) \quad \text{ind}_p(x) = \frac{\text{disc}_p(x) - (e-1)}{2} = \frac{1}{2} \left(e \sum_{i=1}^{e-1} |\sigma_i(x) - x| - (e-1) \right),$$

$$(5) \quad \text{Res}_p(x, y) = \sum_{i,j=0}^{e-1} |\sigma_i(x) - \sigma_j(y)|,$$

and

$$(6) \quad |\sigma_i(x) - \sigma_j(y)| = \left| \sum_{k=0}^{\infty} (\zeta^{ik} x_k - \zeta^{jk} y_k) \pi^k \right|.$$

Since the expression in (6) is clearly independent of a and π , the lemma follows. \square

Theorem 1. *If L, L' are two totally and tamely ramified extensions of the same degree e , then $I_p(n[L]) = I_p(n[L'])$ for all $n \in \mathbb{N}$.*

Proof. Let $L = \mathbb{Q}(\pi)$, $L' = \mathbb{Q}(\pi')$, with $\pi^e = ap$, $\pi'^e = a'p$, and let $S = \{x_1, \dots, x_n\} \subset \mathcal{O}_L$, $S' = \{x'_1, \dots, x'_n\} \subset \mathcal{O}_{L'}$, where $x_j = \sum_k x_{jk} \pi^k$ and $x'_j = \sum_k x'_{jk} \pi'^k$. Then, by Lemma 1, we have $I_p(S) = I_p(S')$. It follows that the set of indexes of the n -subsets of \mathcal{O}_L and $\mathcal{O}_{L'}$ are the same, hence their minima are the same. \square

Corollary 1. *Let K, K' be Galois extensions of \mathbb{Q} of degree en , where $(e, p) = 1$. If pR_K and $pR_{K'}$ have the same factorization type $(P_1 \cdots P_n)^e$, then*

$$\text{ind}_p(K) = \text{ind}_p(K').$$

Proof. Under our hypotheses, we have $e_p(K) = n[L]$, where L is totally and tamely ramified over \mathbb{Q}_p . Hence Theorem 1 applies. \square

4. COMPUTATION OF THE INDEX: PRELIMINARY STEPS

From now on L will denote a tamely ramified extension of \mathbb{Q}_p . We let F be the maximal unramified subextension of L , and let $[F : \mathbb{Q}_p] = f$ and $[L : F] = e$ (with $(e, p) = 1$) be the inertial degree and the ramification index of the extension L/\mathbb{Q}_p , respectively.

Let $q = p^f$ and $\zeta = \zeta_{q-1}$ be a primitive $(q-1)$ -th root of unity. We shall write $L = F(\pi)$, where π is a root of the polynomial $X^e - \zeta^a p$, for some integer

with $0 \leq a < q - 1$. As in Section 3, $X \subset \mathcal{O}_F$ will be the set of Teichmüller representatives in \mathcal{O}_L of the residue field $\mathcal{O}_L/\pi\mathcal{O}_L \cong \mathbb{F}_q$ and we shall write every element $x \in \mathcal{O}_L$ as $x = \sum_{k=0}^\infty x_k \pi^k$, where $x_k \in X$ for all k .

In the sequel we shall deal with the problem of the explicit computation of $I_p(nL)$. Recalling Definition 1 we can write

$$I_p(nL) = \min_{\substack{Y \subset \mathcal{O}_L \\ |Y|=n}} I_p(Y);$$

in fact, in this case an n -tuple of \mathcal{O}_L is an ordered subset of cardinality n of \mathcal{O}_L and

$$(7) \quad I_p(\{x^{(1)}, \dots, x^{(n)}\}) = \sum_{i=1}^n \text{ind}_p(x^{(i)}) + \sum_{1 \leq i < j \leq n} \text{Res}_p(x^{(i)}, x^{(j)})$$

is clearly symmetric on the $x^{(i)}$.

To compute $I_p(nL)$ we have to explicitly find, for each n , a set which minimizes (7).

We start by subdividing the elements of \mathcal{O}_L according to their valuation.

Definition 2. For $h \geq 0$, let $A_h = \{x \in \mathcal{O}_L \mid |x|_p = \frac{h}{e}\}$ and $B_h = \{x \in \mathcal{O}_L \mid |x|_p \geq \frac{h}{e}\}$.

We observe that the following hold:

- $B_h = A_h \cup B_{h+1}$ for all $h \geq 0$;
- $\mathcal{O}_L = A_0 \cup A_1 \cup \dots \cup A_{e-1} \cup B_e$.

We denote by x_k and y_k the coefficients of the π -adic expansion of generic elements x and y of \mathcal{O}_L . A first rough bound for (7) can be given in terms of the valuation of the $x^{(i)}$.

Lemma 2. Let $x \in A_h$ and $y \in A_l$. Then, for all embeddings $\sigma, \tau : L \rightarrow \bar{\mathbb{Q}}_p$,

$$(8) \quad |\sigma(x) - \tau(y)| \geq \frac{\min\{h, l\}}{e}$$

and strict inequality holds if and only if $h = l$ and $\sigma(x_h \pi^h) = \tau(y_h \pi^h)$. In particular

$$(9) \quad \text{Res}_p(x, y) \geq ef^2 \min\{h, l\}$$

and strict inequality holds if and only if $h = l$ and $x_h \pi^h, y_h \pi^h$ are conjugate.

Proof. From the properties of the p -adic valuation we have

$$|\sigma(x) - \tau(y)| \geq \min\{|\sigma(x)|, |\tau(y)|\} = \frac{\min\{h, l\}}{e},$$

hence

$$(10) \quad \text{Res}_p(x, y) = \sum_{\sigma, \tau} |\sigma(x) - \tau(y)| \geq ef^2 \min\{h, l\}.$$

Clearly in both equations equality holds whenever $h \neq l$. Now let $h = l$. Observe that, for each embedding σ , we have that $(\frac{\sigma(\pi)}{\pi})^e = \frac{\sigma(\pi^e)}{\pi^e}$ is a $(q - 1)$ -th root of unity and therefore we may write $\sigma(\pi) = \xi_\sigma \pi$, where ξ_σ is an $e(q - 1)$ -th root of unity. We have inequality in (8) if and only if $|\sigma(x_h) \xi_\sigma^h - \tau(y_h) \xi_\tau^h| > 0$; since both $\sigma(x_h) \xi_\sigma^h$ and $\tau(y_h) \xi_\tau^h$ are roots of unity of order coprime to p , this happens if and only if they coincide. \square

The previous lemma characterizes when $|\sigma(x) - x| > |x|$ and when $|\sigma(x) - \tau(y)| > \min\{|x|, |y|\}$. We now show how to evaluate these terms by using an inductive argument. We start with some more definitions.

Definition 3. For any field E such that $\mathbb{Q}_p \subseteq E \subseteq L$, denote by e_E the ramification index of the extension L/E and by Σ_E the set of embeddings $\sigma : L \rightarrow \bar{\mathbb{Q}}_p$ over E (we shall simply write Σ when $E = \mathbb{Q}_p$). In analogy with the case of the ground field, we define the normalized relative p -discriminant $\text{disc}_p^E(x)$ of an element $x \in \mathcal{O}_L$ as the norm of the usual relative discriminant, namely

$$(11) \quad \text{disc}_p^E(x) = ef \sum_{\sigma \in \Sigma_E \setminus \{1\}} |\sigma(x) - x|,$$

and the relative index $\text{ind}_p^E(x)$ as

$$(12) \quad \text{ind}_p^E(x) = \frac{1}{2} \left(ef \sum_{\sigma \in \Sigma_E \setminus \{1\}} |\sigma(x) - x| - f(e_E - 1) \right).$$

Observe that $\text{ind}_p^E(x)$ coincides with the p -adic exponent of the usual index of subgroups $[\mathcal{O}_L : \mathcal{O}_E[x]]$.

Similarly, for $x, y \in \mathcal{O}_L$, we define the normalized relative resultant $\text{Res}_p^E(x, y)$ as the norm of the usual relative resultant, namely

$$(13) \quad \text{Res}_p^E(x, y) = [E : \mathbb{Q}_p] \sum_{\sigma, \tau \in \Sigma_E} |\sigma(x) - \tau(y)| = ef \sum_{\sigma \in \Sigma_E} |\sigma(x) - y|.$$

Finally, we define the relative index of a set $\{x^{(1)}, \dots, x^{(n)}\} \in L$ as

$$(14) \quad I_p^E(\{x^{(1)}, \dots, x^{(n)}\}) = \sum_{i=1}^n \text{ind}_p^E(x^{(i)}) + \sum_{1 \leq i < j \leq n} \text{Res}_p^E(x^{(i)}, x^{(j)}).$$

We point out that in the case when $E = \mathbb{Q}_p$ the relative discriminant, index and resultant coincide with the usual one.

Proposition 2. Let $x \in A_h$, $x = x_h \pi^h (1 + x')$ and let $E = \mathbb{Q}_p(x_h \pi^h)$. Then

$$\text{ind}_p(x) = \frac{f(h ef - h - e + e_E)}{2} + \text{ind}_p^E(x').$$

Proof. We have $|\sigma(x) - x| = |\sigma(x_h \pi^h)(1 + \sigma(x')) - x_h \pi^h(1 + x')| = \frac{h}{e}$ if and only if $\sigma(x_h \pi^h) \neq x_h \pi^h$. Therefore

$$(15) \quad \text{disc}_p(x) = ef \frac{h}{e} (ef - 1) + ef \sum_{\sigma \in \Sigma_E \setminus \{1\}} |\sigma(x') - x'|.$$

From (12) we get

$$(16) \quad ef \sum_{\sigma \in \Sigma_E \setminus \{1\}} |\sigma(x') - x'| = 2 \text{ind}_p^E(x') + f(e_E - 1)$$

and the lemma then follows recalling that

$$(17) \quad \text{ind}_p(x) = \frac{\text{disc}_p(x) - f(e - 1)}{2}.$$

□

Proposition 3. *Let $x, y \in A_h$ such that $x \equiv y \pmod{\pi^{h+1}}$. Let $x = x_h\pi^h(1 + x')$, $y = x_h\pi^h(1 + y')$ and $E = \mathbb{Q}_p(x_h\pi^h)$. Then*

$$\text{Res}_p(x, y) = hef^2 + \text{Res}_p^E(x', y').$$

Proof. We have

$$\text{Res}_p(x, y) = \sum_{\sigma, \tau \in \Sigma} |\sigma(x) - \tau(y)| = ef \sum_{\sigma \in \Sigma} |\sigma(x) - y|.$$

For all $\sigma \in \Sigma$ we have $|\sigma(x) - y| \geq \frac{h}{e}$ and, if $\sigma \notin \Sigma_E$, then $|\sigma(x) - y| = \frac{h}{e}$. If $\sigma \in \Sigma_E$, then observe that $|\sigma(x) - y| = \frac{h}{e} + |\sigma(x') - y'|$ and the sum of $|\sigma(x') - y'|$ relative to these σ is exactly the definition of $\text{Res}_p^E(x', y')$. \square

Definition 4. Let $h \geq 0$ and let x_h be a non-zero element of X . We define the congruence class $C(h, x_h)$ as

$$C(h, x_h) = \{x \in \mathcal{O}_L \mid x \equiv x_h\pi^h \pmod{\pi^{h+1}}\}.$$

Corollary 2. *Let $h \geq 0$ and let A be a subset of m elements of $C(h, x_h)$. Set $A = x_h\pi^h(1 + A')$ and $E = \mathbb{Q}_p(x_h\pi^h)$. Then*

$$(18) \quad I_p(A) = \frac{1}{2}hef^2m^2 - \frac{fm}{2}(e + h - e_E) + I_p^E(A').$$

Proof. By Propositions 2 and 3 we have

$$(19) \quad I_p(A) = \frac{mf}{2}(hef - h - e + e_E) + \binom{m}{2}hef^2 + I_p^E(A').$$

A simple calculation gives (18). \square

We have prepared the ground for our construction of an infinite sequence $\omega_0, \omega_1, \dots$ of elements of \mathcal{O}_L such that $I_p(nL) = I_p(\{\omega_0, \dots, \omega_{n-1}\})$ for all n . Before stating our main theorem, we need some more notation.

Definition 5. Let E be any field such that $\mathbb{Q}_p \subseteq E \subseteq L$. Let \mathcal{Y} be a subset of \mathcal{O}_L and let Y be a subset of \mathcal{Y} with m elements ($m > 0$). We say that Y is *E-optimal* in \mathcal{Y} (or simply optimal if $E = \mathbb{Q}_p$) if

$$I_p^E(Y) = \min_{\substack{Y' \subset \mathcal{Y} \\ |Y'|=m}} I_p^E(Y').$$

We shall omit the reference to \mathcal{Y} when this is clear from the context. We shall denote by $I_{\mathcal{Y}}^E(m)$ the *E-index* of an optimal subset of \mathcal{Y} with m elements.

We call a sequence $\mathcal{S} = \{s_0, s_1, \dots\}$ of \mathcal{Y} an *E-optimal sequence* if, for each m , its first m -segment, *i.e.* $\mathcal{S}(m) = \{s_0, \dots, s_{m-1}\}$, is *E-optimal*.

- Lemma 3.**
- (i) *Let $h \geq 0$, $T \subset B_h$ be a finite set and let E be any field such that $\mathbb{Q}_p \subseteq E \subseteq L$. If T is *E-optimal*, then $A = T \cap A_h$ and $B = T \cap B_{h+1}$ are *E-optimal*.*
 - (ii) *Let $h \geq 0$. If $\mathcal{T} \subset B_h$ is an *E-optimal sequence*, then $\mathcal{T} \cap A_h$ and $\mathcal{T} \cap B_{h+1}$ are *E-optimal sequences* of A_h and B_{h+1} .*

Proof. Suppose that an optimal T has $|A| = a$ and $|B| = b$. By Lemma 2 we have

$$I_p^E(T) = I_p^E(A) + I_p^E(B) + [L : E] \cdot hfab,$$

and both statements follow. \square

Definition 6. For $h \geq 0$, we define an equivalence relation on the congruence classes $C(h, x_h)$ contained in A_h . We say that $C(h, x_h)$ and $C(h, y_h)$ are equivalent if there exists $\sigma \in \Sigma$ such that $\sigma(x_h \pi^h) = y_h \pi^h$.

We shall write $A_h = \Gamma_1 \cup \dots \cup \Gamma_{r_h}$ where $\Gamma_1, \dots, \Gamma_{r_h}$ are the equivalence classes. Also, for $i = 1, \dots, r_h$, we shall denote by $C(h, x_{\Gamma_i})$ a representative of the conjugacy class Γ_i .

Lemma 4. (i) *Let $S \subset A_h$ be a optimal set in A_h . Then $S_i = S \cap \Gamma_i$ is optimal for all i .*

(ii) *Let $S \subset A_h$ be an optimal sequence in A_h . Then $S \cap \Gamma_i$ is an optimal sequence for Γ_i for all i .*

Proof. For $i = 1, \dots, r_h$, $s_i = |S_i|$. We have

$$I_p(S) = \sum_{i=1}^{r_h} I_p(S_i) + hef^2 \sum_{1 \leq i < i' \leq r_h} s_i s_{i'}$$

and the statement follows as in Lemma 3. □

5. MAIN THEOREM

Theorem 2. *Let L be a normal and tamely ramified extension of \mathbb{Q}_p . Then there exists an effectively computable optimal sequence $\Omega = \{\omega_0, \omega_1, \dots\}$ of elements of \mathcal{O}_L .*

Proof. We prove that for any intermediate field E , $\mathbb{Q}_p \subset E \subset L$, there exists an effectively computable E -optimal sequence Ω^E . (Here and in the following, we denote by a superscript E whatever is related to the extension E .) The proof will be by induction, considering $E = L$ as the initial case, and then assuming that the assertion is true for all fields F strictly containing E and proving it for E .

However, in the course of the proof we shall also need that the sequence $\mathcal{B}_1^E = \Omega^E \cap B_1$ (which is an E -optimal sequence of B_1 by Lemma 3) has the property that $I_{B_1}^E(n)$ is a convex function of n (or, equivalently, that the difference function $\Delta_{B_1}^E(n) = I_{B_1}^E(n+1) - I_{B_1}^E(n)$ is an increasing function of n). We shall prove this property by induction as well.

The initial case $E = L$ corresponds to the trivial extension. Arguing as in Engstrom [2], one can construct an L -optimal sequence $\Omega^L = \{\omega_0^L, \omega_1^L, \dots\}$ as follows. Choose a basis $\{1, u_1, \dots, u_{f-1}\}$ of the residue field $\mathcal{O}_L/\pi\mathcal{O}_L \cong \mathbb{F}_q$, considered as a vector space over \mathbb{F}_p , and consider the bijection $\bar{\eta} : \{0, 1, \dots, q-1\} \rightarrow \mathbb{F}_q$ given by

$$\bar{\eta}(a_0 + a_1p + \dots + a_{f-1}p^{f-1}) = \bar{a}_0 + \bar{a}_1u_1 + \dots + \bar{a}_{f-1}u_{f-1},$$

where $0 \leq a_j < p$ and \bar{a}_j denotes the reduction of $a_j \pmod p$. Fix a bijection $\theta : \mathbb{F}_q \rightarrow X \cup \{0\}$ such that $\theta(0) = 0$ and lift $\bar{\eta}$ to a bijection $\eta : \{0, 1, \dots, q-1\} \rightarrow X \cup \{0\}$ by putting $\eta = \theta \circ \bar{\eta}$. Next write all natural numbers n in their q -adic expansion, $n = b_0 + b_1q + \dots$ and denote again by η its extension $\eta : \mathbb{N} \rightarrow \mathcal{O}_L$ defined by

$$\eta(b_0 + b_1q + \dots) = \eta(b_0) + \eta(b_1)\pi + \dots$$

It is fairly easy to check that $\Omega^L = \{\eta(1), \eta(2), \dots\}$ is an L -optimal sequence. A simple computation gives

$$I_p^L(nL) = f \sum_{j=0}^{n-1} \sum_{r \geq 1} \lfloor \frac{j}{q^r} \rfloor.$$

Finally, the subsequence $\{\eta(q), \eta(2q), \dots\}$ is exactly $\Omega^L \cap B_1 = \mathcal{B}_1^L$ and this gives

$$I_{B_1}^L(n) = f\binom{n}{2} + I_p^L(nL),$$

whence $\Delta_{B_1}^L(n) = f(n + \sum_{r \geq 1} \lfloor \frac{n}{q^r} \rfloor)$ is an increasing function of n .

As remarked at the beginning, the inductive step consists of assuming our statements true for all fields E strictly containing E , and proving the same statements for E . Since however the argument is identical for general E and for $E = \mathbb{Q}_p$, we prefer not to use the heavier notation that would be required for general E and to give the argument only in the case $E = \mathbb{Q}_p$.

In the rest of the proof we shall hence suppose that, for all subextensions of $E \neq \mathbb{Q}_p$ (for which clearly L/E is normal, tamely ramified of degree less than $[L : \mathbb{Q}_p]$), we are given an E -optimal sequence Ω^E such that $\Delta_{B_1}^E(n)$ is an increasing function of n . □

5.1. Auxiliary optimal sequences. To construct the sequence Ω , we split \mathcal{O}_L as $\mathcal{O}_L = A_0 \cup A_1 \cup \dots \cup A_{e-1} \cup B_e$. In this subsection we shall only consider the subsets A_h : we shall construct auxiliary optimal sequences for each A_h for $h > 0$, and an auxiliary optimal sequence for a suitable subset of A_0 .

To construct an optimal sequence for A_h (or for a subset of A_0), we split A_h as the union of its equivalence classes, $A_h = \Gamma_1 \cup \dots \cup \Gamma_{r_h}$; we first construct an optimal sequence for each Γ_i and then we prove that the union of these sequences in a suitable order is in fact an optimal sequence for A_h . The reason why the case $h = 0$ is exceptional is that our construction works only when the field $E = \mathbb{Q}_p(x_\Gamma \pi^h)$ strictly contains \mathbb{Q}_p , because only under this assumption the inductive hypothesis allows us to take advantage of the results of Section 4. Now, if $0 < h < e$, then E is certainly ramified over \mathbb{Q}_p , and hence cannot be equal to \mathbb{Q}_p , whereas, if $h = 0$, it may well happen that $\mathbb{Q}_p(x_\Gamma) = \mathbb{Q}_p$.

The next proposition is the only step of the proof where we use the hypothesis that L is a normal extension of \mathbb{Q}_p .

Proposition 4. *Let $\Gamma = \Gamma_i$ be an equivalence class of A_h , let $C(h, x_\Gamma)$ be a representative of the class and assume $E = \mathbb{Q}_p(x_\Gamma \pi^h) \neq \mathbb{Q}_p$. Then there exists an effectively computable optimal sequence $\mathcal{A}_\Gamma = \{\alpha_{\Gamma,0}, \alpha_{\Gamma,1}, \dots\}$ for Γ .*

Proof. Since L is a normal extension of \mathbb{Q}_p , if two classes $C(h, x_h)$ and $C(h, y_h)$ of A_h are equivalent, then they are also conjugate over \mathbb{Q}_p . In fact, let $\sigma \in \Sigma = \text{Gal}(L/\mathbb{Q}_p)$ be such that $\sigma(x_h \pi^h) = y_h \pi^h$; then $\sigma(C(h, x_h)) = \sigma(x_h \pi^h(1 + \pi \mathcal{O}_L)) = y_h \pi^h(1 + \sigma(\pi \mathcal{O}_L)) = y_h \pi^h(1 + \pi \mathcal{O}_L) = C(h, y_h)$. On the other hand, we have trivially that $\text{ind}_p(x) = \text{ind}_p(\sigma(x))$ and $\text{Res}_p(x, y) = \text{Res}_p(\sigma(x), \tau(y))$ for all $x, y \in \mathcal{O}_L$ and all embeddings σ, τ of L in \mathbb{Q}_p . Hence, in order to compute the index, we may suppose that every element $x \in A_h$ belongs to the representative class $C(h, x_\Gamma)$.

By the inductive hypothesis, we are given an E -optimal sequence \mathcal{B}_1^E . Then $\mathcal{A}_\Gamma = x_\Gamma \pi^h(1 + \mathcal{B}_1^E)$ is an optimal sequence for Γ by Corollary 2. □

By Lemma 4, an optimal sequence \mathcal{A}_h for the set A_h can only be obtained by suitably ordering the union of all optimal sequences \mathcal{A}_Γ , and we shall prove in the next proposition that a suitable order exists. We shall pick the elements from the sequences \mathcal{A}_Γ one by one, so that at each step the index is kept as low as possible. To this aim, we introduce integer-valued functions on the elements of the sequences \mathcal{A}_Γ

that are our reference for deciding which choice gives the least possible increment of the index.

Definition 7. Let $h \geq 0$ and Γ be an equivalence class in A_h . We define

$$\Delta_\Gamma(a) = I_\Gamma(a + 1) - I_\Gamma(a) \quad \text{and} \quad \varphi_\Gamma(a) = \Delta_\Gamma(a) - hef^2a.$$

Remark 1. By Corollary 2 we have that

$$\varphi_\Gamma(a) = \Delta_\Gamma(a) - hef^2a = \frac{1}{2}[hef^2 - f(e + h - e_E)] + \Delta_{B_1}^E(a)$$

is an increasing function of a by inductive hypothesis.

We can now prove the existence of an optimal sequence \mathcal{A}_h for A_h . In order to also deal with the exceptional case $h = 0$, we let $\tilde{A}_0 = \{x \in A_0 \mid x_0 \notin \mathbb{Q}_p\}$. (Observe that $\tilde{A}_0 = \emptyset$ if $f = 1$.)

- Proposition 5.**
- (i) For $1 \leq h < e$ there exists an effectively computable optimal sequence $\mathcal{A}_h = \{\alpha_{h,0}, \alpha_{h,1}, \dots\}$ for A_h .
 - (ii) There exists an effectively computable optimal sequence $\tilde{\mathcal{A}}_0 = \{\alpha_{0,0}, \alpha_{0,1}, \dots\}$ for \tilde{A}_0 .

Proof. (i) We construct a sequence \mathcal{A}_h by ordering the elements of the union of the sequences \mathcal{A}_Γ according to the order of the values of the functions $\varphi_\Gamma(a)$ (no matter which order is chosen when two or more values coincide).

To be more precise, we describe a possible procedure in detail. Let $\{\Gamma_1, \dots, \Gamma_{r_h}\}$ be the equivalence classes of A_h , in an arbitrary but fixed order. We merge the increasing sequences $\varphi_{\Gamma_i}(0), \varphi_{\Gamma_i}(1), \dots$ into an increasing sequence of non-negative integers $\gamma_{h,0}, \gamma_{h,1}, \dots$ “lexicographically”, *i.e.* with the understanding that in case of equality we adopt the following rules:

- if $\varphi_{\Gamma_j}(m) = \varphi_{\Gamma_j}(m + 1)$ for some j, m , then $\varphi_{\Gamma_j}(m)$ precedes $\varphi_{\Gamma_j}(m + 1)$;
- if $\varphi_{\Gamma_j}(m) = \varphi_{\Gamma_l}(n)$ for some $j < l$, and some m, n , then $\varphi_{\Gamma_j}(m)$ precedes $\varphi_{\Gamma_l}(n)$.

Finally we define $\alpha_{h,m} = \alpha_{\Gamma_j,n}$ if $\gamma_{h,m} = \varphi_{\Gamma_j}(n)$.

We now show that the sequence \mathcal{A}_h so constructed is optimal, that is, that any m -element set $S \subseteq A_h$ satisfies $I_p(S) \geq I_p(\mathcal{A}_h(m))$.

For each equivalence class Γ contained in A_h , let $S_\Gamma = \Gamma \cap S$, $s_\Gamma = |S_\Gamma|$ and $a_\Gamma = |\Gamma \cap \mathcal{A}_h(m)|$, so that $\sum_\Gamma a_\Gamma = m = \sum_\Gamma s_\Gamma$. Also, by Lemma 4, it is enough to prove the inequality in the case when all S_Γ are optimal, or, even more, when $S_\Gamma = \mathcal{A}_\Gamma(s_\Gamma)$ for all Γ . We now prove the inequality $I_p(S) \geq I_p(\mathcal{A}_h(m))$ by induction on

$$r = r(S) = \sum_\Gamma \max\{s_\Gamma - a_\Gamma, 0\} = \sum_\Gamma \max\{a_\Gamma - s_\Gamma, 0\}.$$

If $r(S) = 0$, then necessarily $S = \mathcal{A}_h(m)$ and the inequality is true. If $r(S) > 0$, let Γ, Θ be two equivalence classes such that $s_\Gamma > a_\Gamma$ and $a_\Theta > s_\Theta$. Set $T = S \setminus \{\alpha_{\Gamma, s_\Gamma - 1}\}$ and $S' = T \cup \{\alpha_{\Theta, s_\Theta}\}$.

We have $r(S') = r(S) - 1$ and

$$I_p(S) = I_p(T) + \Delta_\Gamma(s_\Gamma - 1) + hef^2(m - s_\Gamma)$$

and

$$I_p(S') = I_p(T) + \Delta_\Theta(s_\Theta) + hef^2(m - 1 - s_\Theta).$$

Taking the difference we obtain

$$I_p(S) - I_p(S') = \varphi_\Gamma(s_\Gamma - 1) - \varphi_\Theta(s_\Theta)$$

and, since $s_\Gamma - 1 \geq a_\Gamma$ and $s_\Theta < a_\Theta$, the last difference is greater than or equal to $\varphi_\Gamma(a_\Gamma) - \varphi_\Theta(a_\Theta - 1)$, which is non-negative by our choice of the sequence $\{\gamma_{h,j}\}$. By the inductive hypothesis, we get $I_p(S) \geq I_p(S') \geq I_p(\mathcal{A}_h(m))$, as wanted.

(ii) The proof is the same as in case (i), except that we have to consider only the equivalence classes Γ for which the field $E = \mathbb{Q}_p(x_\Gamma)$ is different from \mathbb{Q}_p . \square

5.2. Construction of the optimal sequence. To construct an optimal sequence Ω we shall construct by induction its first n -segment $\Omega(n)$ for each n .

For the initial step, we recall that it is always possible to choose an element $\alpha \in \mathcal{O}_L$ such that $\text{ind}_p(\alpha) = 0$. Defining $\Omega(1) = \{\alpha\}$ we clearly have that $\Omega(1)$ is optimal.

As to the inductive step, given an optimal n -set $\Omega(n) = \{\omega_0, \dots, \omega_{n-1}\}$ of Ω , we shall construct a new element ω_n such that $\Omega(n + 1) = \Omega(n) \cup \{\omega_n\}$ is again optimal.

The following proposition shows how to produce an optimal set of n elements in B_e from $\Omega(n)$.

Proposition 6. *Let $B \subset B_e$, $B = pB^*$ be a subset of $p\mathcal{O}_L$ with m elements. Then*

$$I_p(B) = m \frac{ef(ef - 1)}{2} + \binom{m}{2} (ef)^2 + I_p(B^*).$$

Proof. Trivial. \square

So we can suppose to know the infinite sequences $\tilde{\mathcal{A}}_0, \mathcal{A}_1, \dots, \mathcal{A}_{e-1}$ and the first n -segment, $\mathcal{B}_e(n)$, of an optimal sequence \mathcal{B}_e in B_e .

For decreasing ‘levels’ $h = e - 1, e - 2, \dots, 1$, we suitably pick some elements of $\mathcal{B}_{h+1}(n)$ and some of the initial elements of \mathcal{A}_h to construct the initial n -segment of an optimal sequence \mathcal{B}_h . For the case $h = 0$, we first substitute in the initial segment of \mathcal{B}_1 each element $\beta_{1,i}$ with the p elements $\beta_{1,i}, \beta_{1,i} + 1, \dots, \beta_{1,i} + p - 1$ and then pick some of these new elements and some elements of $\tilde{\mathcal{A}}_0$ to construct the larger initial segment $\Omega(n + 1)$ of Ω .

The method of choosing the first n elements of \mathcal{B}_1 will be similar to the method used in the proof of Proposition 5. We introduce some integer-valued functions that will serve us as a reference to compare the elements with each other, and to guide us in order to make the best possible choices.

The reference functions for our construction are the following.

Definition 8. For $h > 0$ we define

$$\Delta_{A_h}(a) = I_{A_h}(a + 1) - I_{A_h}(a), \quad \Delta_{B_h}(b) = I_{B_h}(b + 1) - I_{B_h}(b)$$

and

$$\varphi_{A_h}(a) = \Delta_{A_h}(a) - hef^2a, \quad \varphi_{B_h}(b) = \Delta_{B_h}(b) - (h - 1)ef^2b.$$

For $h = 0$ we define

$$\Delta_{\tilde{A}_0}(a) = I_{\tilde{A}_0}(a + 1) - I_{\tilde{A}_0}(a), \quad \varphi_{\tilde{A}_0}(a) = \Delta_{\tilde{A}_0}(a)$$

and

$$\Delta_{B_0}(b) = I_{B_0}(b + 1) - I_{B_0}(b) = I_p((b + 1)[L]) - I_p(b[L]).$$

We remark that, by the proof of Proposition 5, $\varphi_{\tilde{A}_0}(a), \varphi_{A_1}(a), \dots, \varphi_{A_e}(a)$ are increasing functions of a . We shall need the same property for the functions $\varphi_{B_h}(b)$. Therefore, to describe our inductive step more precisely, we shall consider, for each $n \in \mathbb{N}$ and for each $h = 0, 1, \dots, e$, the following statement:

B(n, h): one can construct a subset $\mathcal{B}_h(n) = \{\beta_{h,0}, \dots, \beta_{h,n-1}\}$ of B_h such that $\mathcal{B}_h(m) = \{\beta_{h,0}, \dots, \beta_{h,m-1}\}$ is optimal for all $m \leq n$; moreover $\varphi_{B_h}(m)$ is increasing for $m \leq n - 1$.

We have already seen that **B(1, 0)** is true and we shall prove all **B(n, h)** according to the following scheme:

$$\mathbf{B}(n, 0) \Rightarrow \mathbf{B}(n, e) \Rightarrow \mathbf{B}(n, e - 1) \Rightarrow \mathbf{B}(n, e - 2) \Rightarrow \dots \Rightarrow \mathbf{B}(n, 1) \Rightarrow \mathbf{B}(n + 1, 0).$$

At each step, we shall also check that for each h and for each n the sequence $\mathcal{B}_h(n)$ is consistent with the previously-constructed sequence $\mathcal{B}_h(n - 1)$, *i.e.*, that it is obtained from it by just adding one new element (for $h = 0$, this is equivalent to checking that the choice of the sequence $\Omega(n + 1)$ is consistent with the sequence $\Omega(n)$). This will ensure that the initial n -segment of $\Omega = \bigcup_{n=1}^{\infty} \Omega(n)$ is indeed $\Omega(n)$, and therefore Ω is an optimal sequence. Similarly, considering the case $h = 1$, this will ensure that $\mathcal{B}_1(n)$ is the initial n -segment of the B_1 -optimal sequence $\mathcal{B}_1 = \bigcup_{n=1}^{\infty} \mathcal{B}_1(n)$, and therefore that $\Delta_{B_1}(n) = \varphi_{B_1}(n)$ is an increasing function of n .

Proof of B(n, e). We set $\mathcal{B}_e(n) = p\Omega(n)$, so clearly $\mathcal{B}_e(n) = \mathcal{B}_e(n - 1) \cup \{\beta_{e,n-1}\}$. By Proposition 6, studying the optimality of the set $\mathcal{B}_e(n)$ is the same as studying the optimality of $\mathcal{B}_e(n)^*$, *i.e.* as studying the optimality of $\Omega(n)$.

As to the function $\varphi_{B_e}(b)$, we use Proposition 6 again to obtain

$$\begin{aligned} \varphi_{B_e}(b) &= \frac{ef(ef - 1)}{2} + (ef)^2b + I_p(\mathcal{B}_e(b + 1)^*) - I_p(\mathcal{B}_e(b)^*) - (e - 1)ef^2b \\ &= \frac{ef(ef - 1)}{2} + ef^2b + \Delta(b) \end{aligned}$$

which shows, by **B(n + 1, 0)**, that $\varphi_{B_e}(b)$ is increasing for $b \leq n - 1$. □

Proof of B(n, h) (1 ≤ h < e). Our construction of the sequence $\mathcal{B}_h(n)$ is essentially the best choice we can make inside $\mathcal{A}_h(n) \cup \mathcal{B}_{h+1}(n)$ with respect of the reference functions introduced in Definition 8.

We merge the increasing n -sequence $\varphi_{A_h}(0), \dots, \varphi_{A_h}(n - 1)$ and the increasing n -sequence $\varphi_{B_{h+1}}(0), \dots, \varphi_{B_{h+1}}(n - 1)$ and rearrange the terms to obtain an increasing $2n$ -sequence $\gamma_{h,0}, \dots, \gamma_{h,2n-1}$. In case of equality between two terms, we decide once and for all that the rearrangement is such that $\varphi_{A_h}(m)$ precedes $\varphi_{A_h}(m + 1)$, $\varphi_{B_{h+1}}(l)$ precedes $\varphi_{B_{h+1}}(l + 1)$ and $\varphi_{A_h}(m)$ precedes $\varphi_{B_{h+1}}(l)$.

We associate to the first n -segment $\gamma_{h,0}, \dots, \gamma_{h,n-1}$ of the sequence just constructed, an n -sequence $\{\beta_{h,0}, \dots, \beta_{h,n-1}\} \in B_h$ in the following way: we choose $\beta_{h,i} = \alpha_{h,j}$ if $\gamma_{h,i} = \varphi_{A_h}(j)$ (with j minimum not already chosen) and $\beta_{h,i} = \beta_{h+1,j}$ if $\gamma_{h,i} = \varphi_{B_{h+1}}(j)$ (with j minimum not already chosen). Since, by induction, $\mathcal{B}_h(n - 1)$ was contained in the union of the two sequences $\mathcal{A}_h(n - 1)$ and $\mathcal{B}_{h+1}(n - 1)$, it is clear that our construction is consistent with the construction of $\mathcal{B}_h(n - 1)$, *i.e.* $\mathcal{B}_h(n)$ is obtained by adjoining to $\mathcal{B}_h(n - 1)$ the last element $\beta_{h,n-1}$.

The optimality of $\mathcal{B}_h(n)$ is obtained by the same argument used for $\mathcal{A}_h(m)$ in Proposition 5.

Finally, it is easy to check that $\Delta_{B_h}(m) = \gamma_{h,m} + hef^2m$, hence $\varphi_{B_h}(m) = \gamma_{h,m} + ef^2m$ is increasing for $m \leq n - 1$. \square

Proof of $\mathbf{B}(n + 1, 0)$. The case $h = 0$ requires a modification of the preceding argument, since in this case one cannot use induction to construct an optimal sequence for the set of elements having valuation equal to 0. This is why we have defined the set \tilde{A}_0 exactly as the set of those elements of 0 valuation on which our inductive arguments works. We define $\tilde{B}_0 = \bigcup_{i=0}^{p-1} (i + B_1)$ and we perform a preliminary construction of an optimal sequence $\tilde{\mathcal{B}}_0(pn) = \{\tilde{\beta}_{0,0}, \dots, \tilde{\beta}_{0,pn-1}\}$ of \tilde{B}_0 .

Our construction of the sequence $\tilde{\mathcal{B}}_0(pn)$ is the following. For $m = pi + r < pn$, $0 \leq r < p$, we set $\tilde{\beta}_{0,m} = \beta_{1,i} + r$.

Actually, at this stage we are only interested in the initial $(n + 1)$ -segment of $\tilde{\mathcal{B}}_0(pn)$. Since $\mathcal{B}_1(m + 1) = \mathcal{B}_1(m) \cup \{\beta_{1,m}\}$ for all $m \leq n$, it is also obvious that the initial $(n + 1)$ -segment of $\tilde{\mathcal{B}}_0(pn)$ satisfies $\tilde{\mathcal{B}}_0(n + 1) = \tilde{\mathcal{B}}_0(n) \cup \{\tilde{\beta}_{0,n}\}$. It is also clear that $\tilde{\mathcal{B}}_0(n + 1)$ is as well distributed as possible into the classes $0, 1, \dots, p - 1 \pmod{\pi}$. As to optimality, let W be an optimal set with $n + 1$ elements, and suppose that $W = W_0 \cup \dots \cup W_{p-1}$ is the decomposition of W into classes mod π . For $i = 0, \dots, p - 1$, set $|W_i| = w_i$ and $Z_i = W_i - i \subseteq B_1$. We have

$$I_p(W) = \sum_{i=0}^{p-1} I_p(Z_i).$$

We may clearly suppose that all Z_i are non-empty, hence $w_i \leq n$ for all i , since moving an element from a non-empty set to an empty one cannot increase the index (in fact, $I_p(x) = \text{ind}_p(x)$ and $I_p(S \cup \{y\}) = I_p(S) + \text{ind}_p(y) + \sum_{s \in S} \text{Res}_p(s, y)$). Moreover, if W is optimal, then all Z_i must be optimal, hence, by $\mathbf{B}(n, 1)$, $I_p(Z_i) = I_p(\{\beta_{1,0}, \dots, \beta_{1,w_i-1}\})$ for all i . Now let $n + 1 = qp + r$, $0 \leq r < p$. Again by $\mathbf{B}(n + 1, 1)$, we know that $I_p(\{\beta_{1,0}, \dots, \beta_{1,m-1}\})$ is a convex function for $m \leq n$, hence

$$I_p(W) \geq \sum_{i=1}^r I_p(\{\beta_{1,0}, \dots, \beta_{1,q}\}) + \sum_{i=1}^{p-r} I_p(\{\beta_{1,0}, \dots, \beta_{1,q-1}\}) = I_p(\tilde{\mathcal{B}}_0(n + 1)).$$

Finally, we observe that $\varphi_{\tilde{B}_0}(m) = I_p(\tilde{\mathcal{B}}_0(m + 1)) - I_p(\tilde{\mathcal{B}}_0(m)) = \Delta_{B_1}(\lfloor \frac{m}{p} \rfloor)$ is an increasing function for $m \leq n$.

We are now ready to construct the sequence $\Omega(n + 1)$. In the case $f = 1$ the set \tilde{A}_0 is empty and $B_0 = \tilde{B}_0$, hence $\Omega(n + 1) = \tilde{\mathcal{B}}_0(n + 1)$ and what we have proved for this sequence gives the required properties of $\Omega(n + 1)$.

Suppose now $f > 1$. Arguing as for the construction of $\mathcal{B}_h(n + 1)$ we merge the two increasing $(n + 1)$ -sequences $\varphi_{\tilde{A}_0}(0), \dots, \varphi_{\tilde{A}_0}(n)$ and $\varphi_{\tilde{B}_0}(0), \dots, \varphi_{\tilde{B}_0}(n)$ and we rearrange the terms to obtain an increasing $(2n + 2)$ -sequence $\gamma_{0,0}, \dots, \gamma_{0,2n+1}$. As before, we order equal terms respecting the initial ordering of $\{\varphi_{\tilde{A}_0}(j)\}$ and of $\{\varphi_{\tilde{B}_0}(m)\}$ and establishing the precedence of $\varphi_{\tilde{A}_0}(j)$ over $\varphi_{\tilde{B}_0}(m)$ when $\varphi_{\tilde{A}_0}(j) = \varphi_{\tilde{B}_0}(m)$. Also in this case, we reorder the set $\{\alpha_{0,0}, \dots, \alpha_{0,n}\} \cup \{\tilde{\beta}_{0,0}, \dots, \tilde{\beta}_{0,n}\}$ into a $(2n + 2)$ -sequence $\{\omega_0, \dots, \omega_{2n+1}\}$, according to the sequence $\gamma_{0,i}$, and we define $\Omega(n + 1)$ to be the first $(n + 1)$ -segment of the sequence just defined. Clearly $\Omega(n + 1) = \Omega(n) \cup \{\omega_n\}$. The optimality of this sequence can be obtained arguing as in the proof of Proposition 5.

Finally, $\Delta(m) = \gamma_{0,m}$ hence it is increasing. \square

Corollary 3. *For all normal and tamely ramified extensions L of \mathbb{Q}_p there is an explicit way to compute $I_p(nL)$ for all $n \in \mathbb{N}$.*

Proof. The construction made in Theorem 2 gives explicit values for $\Delta(m)$ for all $m \geq 0$. The corollary follows from the formula $I_p(nL) = \sum_{m=0}^{n-1} \Delta(m)$. \square

Remark 2. While proving Theorem 2 we have used the hypothesis that L is a normal extension of \mathbb{Q}_p only once, namely in the proof of Proposition 4. In the general case, it is not true that two equivalent classes $C(h, x_h)$ and $C(h, y_h)$ are conjugate to each other, and hence we may no longer suppose that all elements of an equivalence class Γ of A_h belong to a representative $C(h, x_\Gamma)$ of the class.

We believe that, using essentially the same ideas of the preceding proof, one could obtain an algorithm for finding an optimal sequence for any tamely ramified extension of \mathbb{Q}_p . However, to generalize Proposition 4 to the non-normal case one has to introduce a new recursive argument in the style of the entire proof, and the resulting algorithm would turn out to be much more involved.

Remark 3. To give a completely effective description of our computation of the index $I_p(nL)$, we sketch how one can decide whether two elements $x_h\pi^h$ and $y_h\pi^h$ are conjugate and what the relative extension $L/\mathbb{Q}_p(x_h\pi^h)$ looks like.

Let $\pi^e = \zeta^a p$ and $x_h = \zeta^x, y_h = \zeta^y$ for some $0 \leq a, x, y < q - 1$. If $\sigma : L \rightarrow \mathbb{Q}_p$ is an embedding, then $\sigma(x_h) = \zeta^{xp^i}$ for some $0 \leq i < f$ and $\sigma(\pi) = \xi_\sigma \pi$ for some $e(q - 1)$ -th root of unity ξ_σ . It is easy to verify that $\xi_\sigma^e = \zeta^{a(p^i - 1)}$; thus, $\xi_\sigma = \eta^{a(p^i - 1) + j(q - 1)}$ for some $0 \leq j < e$, where η is a primitive $e(q - 1)$ -th root of unity. Hence $x_h\pi^h$ and $y_h\pi^h$ are conjugate if and only if there exist i, j in the given range such that

$$x \cdot ep^i + h[a(p^i - 1) + j(q - 1)] \equiv y \cdot e \pmod{e(q - 1)}.$$

As for the field $E = \mathbb{Q}_p(\zeta^x \pi^h)$, let $(h, e) = h_0, h = h'h_0$ and $e = e'h_0$. One easily verifies that

- $\mathbb{Q}_p((\zeta^x \pi^h)^{e'}) = \mathbb{Q}_p(\zeta^{xe' + ah'})/\mathbb{Q}_p$ is unramified;
- $E/\mathbb{Q}_p((\zeta^x \pi^h)^{e'})$ is totally ramified of degree e' .

The inertial degree $f' = [\mathbb{Q}_p(\zeta^{xe' + ah'}) : \mathbb{Q}_p]$ can be computed by looking at the multiplicative order of $\zeta^{xe' + ah'}$; more precisely, f' is characterized by the following system of congruences:

$$\begin{cases} (p^{f'} - 1)(xe' + ah') \equiv 0 \pmod{q - 1}, \\ (p^{f^*} - 1)(xe' + ah') \not\equiv 0 \pmod{q - 1} \text{ for all } f^* | f, f^* < f'. \end{cases}$$

Then suppose $[\mathbb{Q}_p(\zeta^x \pi^h) : \mathbb{Q}_p] = e'f'$, where $e' = \frac{e}{h_0}$ and f' are the ramification index and the inertial degree, respectively. Let α, β be integers such that $\alpha h' + \beta e' = 1$. Then

$$\gamma = (\zeta^x \pi^h)^\alpha (\zeta^{-a} \pi^e)^\beta = \zeta^{x\alpha - a\beta} \pi^{h_0}$$

is a uniformizing element for $E = \mathbb{Q}_p(\zeta^x \pi^h)$. It follows that the extension L/E has inertial degree $\frac{f}{f'}$, ramification index $h_0 = \frac{e}{e'}$ and that one can write $L = F(\pi)$ where $\pi^{h_0} = \zeta^{-x\alpha + a\beta} \gamma$.

6. A COUNTEREXAMPLE TO NART’S CONJECTURE

Let $p = 3$ and $e = f = 2$. There are exactly 2 extensions of \mathbb{Q}_3 with such properties: they are both normal over \mathbb{Q}_3 and can be constructed as follows. Let $\zeta = \zeta_8$ be a primitive 8-th root of unity and let $F = \mathbb{Q}_3(\zeta)$. Let π_1 be a root of $X^2 - p$, π_2 be a root of $X^2 - \zeta p$ and

$$L_1 = F(\pi_1) , \quad L_2 = F(\pi_2) .$$

It can easily be verified that

$$Gal(L_1/\mathbb{Q}_3) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad Gal(L_2/\mathbb{Q}_3) \cong \mathbb{Z}/4\mathbb{Z}.$$

Moreover it is clear that, in both cases, the only non-trivial ramification group is the decomposition group which is cyclic of order 2, hence L_1 and L_2 have the same ramification numbers. We want to show that $I_p(n[L_1])$ is not equal to $I_p(n[L_2])$ for some $n > 0$.

To compute $I_p(n[L_i])$, for $i = 1, 2$, we specify for these particular cases the general construction we gave in Theorem 2. If Γ is an equivalence class of A_h , we shall assume, as in Proposition 4, that \mathcal{A}_Γ is contained in a representative $C(h, x_\Gamma)$ of the equivalence class Γ .

We start by noting that the conjugacy classes of the elements $x = x_0 \in \mathcal{O}_{L_i}$ ($i = 1, 2$) are

$$\{0\}, \{1\}, \{-1\}, \{\zeta, \zeta^3\}, \{\zeta^2, \zeta^6\}, \{\zeta^5, \zeta^7\}$$

and that the conjugacy classes of the elements of type $x = x_1\pi_i$ are

$$\begin{cases} \{\pm\pi_1\}, \{\pm\zeta^2\pi_1\}, \{\pm\zeta\pi_1, \pm\zeta^3\pi_1\} & \text{if } i = 1, \\ \{\pm\pi_2, \pm\zeta\pi_2\}, \{\pm\zeta^2\pi_2, \pm\zeta^3\pi_2\} & \text{if } i = 2. \end{cases}$$

Considering the conjugates of the elements $x = x_1\pi_i$ over F , in both cases we have the following distribution of conjugacy classes:

$$\{\pm\pi_i\}, \{\pm\zeta\pi_i\}, \{\pm\zeta^2\pi_i\}, \{\pm\zeta^3\pi_i\}.$$

Consider first an optimal sequence $\mathcal{A}_{0,j}^i$ in the set $A_{0,j}^i = \{\zeta^j + \pi_i \mathcal{O}_{L_i}\}$ for $j = 1, 2, 5$ and $i = 1, 2$. It is easily seen that the first 4 terms can be chosen as

$$\zeta^j + \pi_i, \zeta^j + \zeta\pi_i, \zeta^j + \zeta^2\pi_i, \zeta^j + \zeta^3\pi_i.$$

In fact, for $0 \leq l, l' \leq 3$ we have

$$I_3(\zeta^j + \zeta^l\pi_i) = 0, \quad \text{Res}_3(\zeta^j + \zeta^l\pi_i, \zeta^j + \zeta^{l'}\pi_i) = 4$$

and both values are minimal for elements in $A_{0,j}^i$. Hence we have the indices

$$I_3(\mathcal{A}_{0,j}^i(1)) = 0, \quad I_3(\mathcal{A}_{0,j}^i(2)) = 4, \quad I_3(\mathcal{A}_{0,j}^i(3)) = 12, \quad I_3(\mathcal{A}_{0,j}^i(4)) = 24.$$

Letting $\varphi_{\mathcal{A}_{0,j}^i}(a) = \Delta_{\mathcal{A}_{0,j}^i}(a) = I_3(\mathcal{A}_{0,j}^i(a+1)) - I_3(\mathcal{A}_{0,j}^i(a))$, we get

$$\varphi_{\mathcal{A}_{0,j}^i}(0) = 0, \quad \varphi_{\mathcal{A}_{0,j}^i}(1) = 4, \quad \varphi_{\mathcal{A}_{0,j}^i}(2) = 8, \quad \varphi_{\mathcal{A}_{0,j}^i}(3) = 12,$$

and $\mathcal{A}_0(12) = \{\zeta + \pi_i, \zeta^2 + \pi_i, \zeta^5 + \pi_i, \zeta + \zeta\pi_i, \zeta^2 + \zeta\pi_i, \zeta^5 + \zeta\pi_i, \zeta + \zeta^2\pi_i, \zeta^2 + \zeta^2\pi_i, \zeta^5 + \zeta^2\pi_i, \zeta + \zeta^3\pi_i, \zeta^2 + \zeta^3\pi_i, \zeta^5 + \zeta^3\pi_i\}$.

As for the sets $B_1^i = \{\pi_i \mathcal{O}_{L_i}\}$ for $i = 1, 2$, one can easily check that the optimal sequences give different indices in the two cases $i = 1$ and $i = 2$. In fact, we have

$$\min_{x'=x_1\pi_i+\dots\in\mathcal{O}_{L_i}} I_3(x_1\pi_i + x_2\pi_i^2 + \dots) = \begin{cases} 2 & \text{if } x_1\pi_i \text{ has 4 conjugates,} \\ 3 & \text{if } x_1\pi_i \text{ has 2 conjugates.} \end{cases}$$

Moreover, if $x_1\pi_i$ and $y_1\pi_i$ are non-conjugates, we have

$$\text{Res}_3(j + x_1\pi_i + x_2\pi_i^2 + \cdots, j + y_1\pi_i + y_2\pi_i^2 + \cdots) = 8.$$

It follows that $\mathcal{B}_1^i(2) = \{\zeta^3\pi_i, \pi_i\}$ is optimal in B_1^i and \mathcal{B}_1^i satisfies

$$\begin{cases} I_3(\mathcal{B}_1^1(1)) = 2, I_3(\mathcal{B}_1^1(2)) = 13 & \text{if } i = 1, \\ I_3(\mathcal{B}_1^2(1)) = 2, I_3(\mathcal{B}_1^2(2)) = 12 & \text{if } i = 2. \end{cases}$$

Hence the first values of $\varphi_{B_1^i}(b)$ are

$$\varphi_{B_1^i}(0) = 2, \quad \varphi_{B_1^i}(1) = \begin{cases} 11 & \text{if } i = 1, \\ 10 & \text{if } i = 2. \end{cases}$$

From the definition of \bar{B}_0^i it follows that

$$\bar{B}_0^i(6) = \{\zeta^3\pi_i, 1 + \zeta^3\pi_i, 2 + \zeta^3\pi_i, \pi_i, 1 + \pi_i, 2 + \pi_i\},$$

hence $\varphi_{\bar{B}_0^i}(n) = \varphi_{B_1^i}(\lfloor \frac{n}{3} \rfloor)$.

It is now immediate to see that an optimal sequence of $13[L_i]$ for $i = 1, 2$ must have 9 elements in A_0 (*i.e.* 3 elements in each of the classes $A_{0,j}^i$) and 4 elements in \bar{B}_0 (*i.e.* 2 elements in B_1 and 1 element in each of the classes $1 + B_1$ and $2 + B_1$). Finally we note that the resultants between elements of different classes among $A_{0,j}^i$ ($j = 1, 2, 5$) and $k + B_1^i$ ($k = 0, 1, 2$) give no contribution to the index, whence the index is just the sum of the indices of the individual classes. It follows that

$$I_3(13[L_1]) = 53 \neq I_3(13[L_2]) = 52.$$

REFERENCES

- [1] R. DEDEKIND, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, *Abh. König. Ges. Wiss. Göttingen* **23** (1878), 1-23.
- [2] H.T. ENGSTROM, On the common index divisor of an algebraic field, *Trans. Amer. Math. Soc.* **32** (1930), 223-237.
- [3] W. NARKIEWICZ, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd Edition, Springer Verlag, 1990. MR1055830 (91h:11107)
- [4] E. NART, On the index of a number field, *Trans. Amer. Math. Soc.* **289** (1985), 171-183. MR0779058 (86h:11092)
- [5] Ö. ORE, Newtonsche Polygone in der Theorie der Algebraischen Körper, *Math. Ann.* **99** (1928), 84-117.
- [6] J. ŚLIWA, On the nonessential discriminant divisors of an algebraic number field, *Acta Arith.* **42** (1982), 57-72. MR0678997 (85b:11097)

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI PISA, VIA BUONARROTI, 2, 56127 PISA, ITALY
E-mail address: delcorso@dm.unipi.it

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI PISA, VIA BUONARROTI, 2, 56127 PISA, ITALY
E-mail address: dvornic@dm.unipi.it