ACTA ARITHMETICA
102.4 (2002)

Number fields with the same index

by

Ilaria Del Corso and Roberto Dvornicich (Pisa)

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

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

where $\operatorname{ind}(\alpha) = [R_K : \mathbb{Z}[\alpha]]$ denotes the index of the element α.

The problem of determining necessary and sufficient conditions in order that two number fields of the same degree have the same index remains open. Usually, this problem is attacked locally; namely, for each prime p one defines $\operatorname{ind}_p(K)$ as the maximal exponent $s_p(K)$ for which $p^{s_p(K)} \mid \operatorname{ind}(K)$, and looks for conditions on two number fields K, K' such that $\operatorname{ind}_p(K) = \operatorname{ind}_p(K')$.

Dedekind [1] characterized when $\operatorname{ind}_p(K) \neq 0$ in terms of the form of the factorization of the ideal (p) in R_K. On the other hand, Ore [6] conjectured and Engstrom [3] proved that the factorization type of (p) in R_K is not sufficient, in general, for deciding what is the actual value of $\operatorname{ind}_p(K)$.

There remain a number of particular cases in which $\operatorname{ind}_p(K)$ can indeed be decided in terms of the factorization type of (p) in R_K: for instance, Engstrom himself [3] proved that this happens when p splits completely in K, and later Śliwa [7] generalized this result to the case when p is unramified in K. Moreover, Nart [5] showed that the mere factorization of (p) in R_K completely determines $\operatorname{ind}_p(K)$ when p splits into an unrestricted number of primes of degree 1 and a limited number of totally ramified primes.

An important remark in Nart's paper [5] is that one can determine $\operatorname{ind}_p(K)$ by studying the $\mathbb{Q}_p$-algebra $K \otimes \mathbb{Q}_p$. In fact, it can be shown that $\operatorname{ind}_p(K)$ is nothing else than the index, $I_p(K\otimes\mathbb{Q}_p)$, of $K\otimes\mathbb{Q}_p$, i.e., the maximal power of p which divides $\operatorname{ind}(\alpha) = [R_K\otimes\mathbb{Z}_p : \mathbb{Z}_p[\alpha]]$ for all $\alpha \in R_K\otimes\mathbb{Z}_p$ (see [5] and [2, Section 2]).

Now, the $\mathbb{Q}_p$-algebra $K\otimes\mathbb{Q}_p$ decomposes as a direct sum of fields, $K\otimes\mathbb{Q}_p \cong L^{(1)} \oplus \ldots \oplus L^{(n)}$, where the $L^{(i)}$'s are the completions of K at the primes lying over p. It is rather easy to see that the index of $K\otimes\mathbb{Q}_p$ depends only on

2000 *Mathematics Subject Classification*: 11R21, 11S99.

the isomorphism classes $[L^{(i)}]$ of the fields in its decomposition, so it is natural to adopt the notation $[K\otimes\mathbb{Q}_p] = n_1[L^{(1)}]+\ldots+n_s[L^{(s)}]$, where n_i denotes the multiplicity of the class $[L^{(i)}]$ in the decomposition of $K\otimes\mathbb{Q}_p$. Moreover, if $K/\mathbb{Q}$ is Galois, then the decomposition of $K\otimes\mathbb{Q}_p$ takes the simpler form $[K\otimes\mathbb{Q}_p] = n[L]$ for some integer n and some Galois extension L of $\mathbb{Q}_p$.

In a previous paper [2], we described a method for explicitly computing $I_p(n[L])$ for all n and all tamely ramified extensions of $\mathbb{Q}_p$.

The main object of this paper is to study under which conditions on two local fields L, L', tamely ramified over $\mathbb{Q}_p$, one can say that

$$I_p(n[L]) = I_p(n[L']) \quad \text{for all } n \in \mathbb{N}. \tag{1}$$

We shall use the approach introduced in [2], where, in particular, we found that (1) is true for all pairs L, L' of totally and tamely ramified extensions of the same degree e. Much more generally, we shall show that, for any two tamely ramified extensions L and L' of $\mathbb{Q}_p$, (1) holds if the defining equations of L and L' are related by an arithmetical condition (Theorem 2). If, moreover, L and L' are Galois over $\mathbb{Q}_p$, this arithmetical condition is equivalent to the following: *the Galois groups* $\mathrm{Gal}(L/\mathbb{Q}_p)$ *and* $\mathrm{Gal}(L'/\mathbb{Q}_p)$ *are isomorphic* (Theorem 1). Finally, these results can be reinterpreted in the case of global fields. Let K and K' be Galois extensions of $\mathbb{Q}$, tamely ramified at a prime p, in which the factorization of p has the same form; if K and K' have isomorphic decomposition groups over p, then $\mathrm{ind}_p(K) = \mathrm{ind}_p(K')$ (Corollary 3).

We remark that the condition $\mathrm{Gal}(L/\mathbb{Q}_p) \cong \mathrm{Gal}(L'/\mathbb{Q}_p)$ seems indeed a necessary one. In fact, already in the simplest case when the two Galois groups are the two non-isomorphic groups of order 4, we have given an example (see [2, Section 5]) showing that (1) is no longer true (for a more general discussion, see the comments at the end of the paper).

Moreover, it turns out that if $\mathrm{Gal}(L/\mathbb{Q}_p)$ and $\mathrm{Gal}(L'/\mathbb{Q}_p)$ are isomorphic groups, then there exists an isomorphism $\varphi : \mathrm{Gal}(L/\mathbb{Q}_p) \to \mathrm{Gal}(L'/\mathbb{Q}_p)$ which satisfies the further condition $\varphi(H) = H'$, where H and H' are the inertia groups of L and L', respectively (Remark 4). Since we use this special isomorphism in the proof of Theorem 1, we doubt whether the condition $\mathrm{Gal}(L/\mathbb{Q}_p) \cong \mathrm{Gal}(L'/\mathbb{Q}_p)$ remains sufficient, in the general case with wild ramification, in order that (1) holds.

2. Notation and preliminaries.

Throughout the paper, p will be a fixed prime number, and e, f will be positive integers with $(e, p) = 1$. Also, we shall let q be the integer p^f and we shall choose $\zeta = \zeta_{q-1}$ to be a fixed primitive $(q-1)$th root of unity. If m is a non-zero integer and r is a prime number, we shall use the notation $\nu_r(m)$ to denote the largest power of r dividing m.

Let $\overline{\mathbb{Q}}_p$ be a given algebraic closure of $\mathbb{Q}_p$. We denote by $|x|$ the p-adic valuation of $\overline{\mathbb{Q}}_p$, normalized so that $|p| = 1$. We shall denote by F the unique unramified extension of $\mathbb{Q}_p$ of degree f contained in $\overline{\mathbb{Q}}_p$ and by $\mathcal{L}(e,f)$ the set of all (tamely ramified) extensions L of $\mathbb{Q}_p$ ($L \subset \overline{\mathbb{Q}}_p$) with inertial degree f and ramification index e.

By classical theory (see for instance [4]), each field $L \in \mathcal{L}(e,f)$ is a totally and tamely ramified extension of F; moreover, we can write $L = F(\pi)$, where π is a root of the polynomial $X^e - \zeta^a p$ for some $a \in \mathbb{Z}$. Conversely, for any integer a the field $F[X]/(X^e - \zeta^a p)$ is a tamely and totally ramified extension of F of degree e, and hence determines an element $L \in \mathcal{L}(e,f)$ up to isomorphism (see also Remark 1 below).

We shall write $L = L_a$ if L can be obtained by adjoining to F a root of $X^e - \zeta^a p$.

Let Σ_{L_a} be the set of embeddings $\lambda : L_a \to \overline{\mathbb{Q}}_p$. Since $F \subset L_a$ is normal over $\mathbb{Q}_p$, any such λ restricts to an automorphism of F, hence $\lambda(\zeta) = \zeta^{p^i}$ for some $0 \le i < f$. Therefore λ must satisfy

$$(\lambda(\pi))^e = \lambda(\pi^e) = \zeta^{ap^i} p = \zeta^{a(p^i-1)}\pi^e.$$

Let ξ be a primitive $e(q-1)$th root of unity such that $\xi^e = \zeta$. It follows that for any $\mathbb{Q}_p$-isomorphism $\lambda : L_a \to \overline{\mathbb{Q}}_p$ there exist indices i, j such that

$$\begin{cases} \lambda(\zeta) = \zeta^{p^i}, \\ \lambda(\pi) = \xi^{a(p^i-1)+j(q-1)}\pi. \end{cases} \tag{2}$$

Since $L = \mathbb{Q}_p(\zeta, \pi)$, equations (2) completely determine the embedding λ. Calling λ_a^{ji} the embedding defined by (2), we have $\Sigma_{L_a} = \{\lambda_a^{ji} \mid 0 \le j < e, 0 \le i < f\}$.

Proposition 1. *The field L_a is a normal extension of $\mathbb{Q}_p$ if and only if $e \mid (a(p-1), q-1)$.*

Proof. Suppose that L_a is normal over $\mathbb{Q}_p$. Then L_a is also normal over F, $\mathrm{Gal}(L_a/F) = \langle\sigma\rangle$, where $\sigma(\pi) = \xi^{q-1}\pi$. It follows that ξ^{q-1}, a primitive eth root of unity, belongs to F and hence $e \mid q-1$. Further, from (2), we find that $\lambda_a^{0,1}(\pi) = \xi^{a(p-1)}\pi \in L_a$, hence $e \mid a(p-1)$.

Conversely, if $e \mid (a(p-1), q-1)$, one sees immediately that $\lambda_a^{ji}(L_a) \subseteq L_a$ for all i, j. ■

Remark 1. Since we have fixed the primitive $(q-1)$th root of unity ζ, the description of the embeddings of L_a given above shows that L_a and $L_{a'}$ are $\mathbb{Q}_p$-isomorphic if and only if $a' \equiv ap^i \pmod{(q-1, e)}$ for some $0 \le i < f$. If, moreover, L_a and $L_{a'}$ are normal over $\mathbb{Q}_p$, then they are isomorphic if and only if $a' \equiv a \pmod{e}$.

Definition 1. Suppose that L_a is normal over $\mathbb{Q}_p$. We define $G_a = \mathrm{Gal}(L_a/\mathbb{Q}_p)$, $H = \mathrm{Gal}(L_a/F)$, $K = \mathrm{Gal}(F/\mathbb{Q}_p)$. Moreover, since both H and K are cyclic, we shall write $H = \langle\sigma\rangle$ and $K = \langle\overline{\tau}\rangle$, where $\sigma(\pi) = \zeta^{(q-1)/e}\pi$ and $\overline{\tau}(\zeta) = \zeta^p$ (here and in the following we identify $\zeta^{1/e}$ with ξ). Finally, we denote by τ the extension of $\overline{\tau}$ to L_a such that $\tau(\pi) = \zeta^{a(p-1)/e}\pi$.

Proposition 2. *The group G_a has the following presentation*:

$$G_a = \langle\sigma, \tau \mid \sigma^e = 1,\ \tau^f = \sigma^a,\ \tau\sigma\tau^{-1} = \sigma^p\rangle.$$

Proof. It is trivial to check that G_a is generated by σ and τ and that $\sigma^e = 1$. By induction on i one easily proves that

$$\tau^i(\pi) = \zeta^{\frac{a(p-1)}{e}(1+p+\ldots+p^{i-1})}\pi,$$

whence $\tau^f(\pi) = \zeta^{a(q-1)/e}\pi$. Since $\tau^f(\zeta) = \zeta$, this yields $\tau^f = \sigma^a$.

From the equation $\tau^{-1}(\tau(\pi)) = \pi$ we obtain

$$\tau^{-1}(\pi) = \zeta^{-\frac{a(p-1)}{e}p^{f-1}}\pi$$

and hence

$$\begin{aligned}\tau\sigma\tau^{-1}(\pi) &= \tau\sigma(\zeta^{-\frac{a(p-1)}{e}p^{f-1}}\pi) = \tau(\zeta^{-\frac{a(p-1)}{e}p^{f-1}+\frac{q-1}{e}}\pi)\\ &= \zeta^{-\frac{a(p-1)}{e}q+\frac{q-1}{e}p+\frac{a(p-1)}{e}}\pi = \sigma^p(\pi).\end{aligned}$$

Since H is a normal subgroup of G_a, we get $\tau\sigma\tau^{-1} = \sigma^p$. Finally, it is trivial to see that the relations just given completely determine the structure of G_a. ∎

Corollary 1. *G_a is abelian if and only if $e \mid p-1$. If G_a is abelian, then*

$$G_a \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}, \quad \textit{where} \quad d_1 = \frac{fe}{(f,e,a)},\ d_2 = (f,e,a).$$

Proof. The condition for abelianity is clear from Proposition 2. If G_a is abelian and has two generators, then G_a can be written as a direct product $G_a \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$, where d_1 is the exponent of G_a and $d_1d_2 = \mathrm{ord}(G_a)$. In our case the exponent of G_a is

$$\exp(G_a) = \mathrm{lcm}\{\mathrm{ord}(\sigma), \mathrm{ord}(\tau)\} = \mathrm{lcm}\left\{e, \frac{fe}{(e,a)}\right\} = \frac{fe}{(f,e,a)}. \ ∎$$

3. Arithmetical conditions for the equivalence of fields. In the previous section we have seen how we can associate to every integer a an element $L_a \in \mathcal{L}(e,f)$ (up to isomorphism). Now we introduce an equivalence relation $\sim$ on the set of integers which will be used in the next section, where we shall show that $I_p(n[L_a])$ depends only on the equivalence class of a.

Definition 2. We shall say that two integers a and a' are (e,f)-*equivalent*, or simply *equivalent*, (and we shall write $a \sim a'$) if and only if

$$\left(\frac{q-1}{p-1}, e, a\right) = \left(\frac{q-1}{p-1}, e, a'\right). \tag{3}$$

Remark 2. Condition (3) says that $a \sim a'$ if and only if a and a' generate the same ideal in $\mathbb{Z}/d\mathbb{Z}$, where $d = \left(\frac{q-1}{p-1}, e\right)$, i.e. if and only if there exists an integer k with $(k,d) = 1$ such that

$$a' \equiv ka \pmod{d}. \tag{4}$$

Now, this is equivalent to saying that there exists a solution $k \in \mathbb{Z}$ of (4) which satisfies the stronger condition $(k, dm) = 1$ for any fixed integer m. In fact, the natural projection $\mathbb{Z}/dm\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ restricts to a surjective homomorphism $(\mathbb{Z}/dm\mathbb{Z})^* \to (\mathbb{Z}/d\mathbb{Z})^*$; hence any solution of (4) with $(k,d) = 1$ can be lifted to a solution with $(k, dm) = 1$.

In particular we deduce that $a \sim a'$ if and only if there exists $(s,t,k) \in \mathbb{Z}^3$ with $(k,e) = 1$ such that

$$a' + s\frac{q-1}{p-1} + te = ka. \tag{5}$$

Definition 3. We shall say that $L_a, L_{a'} \in \mathcal{L}(e,f)$ are *equivalent*, and we shall write $L_a \sim L_{a'}$, if $a \sim a'$.

We remark that although the integer a determines the field $L = L_a$ only up to isomorphism, the definition just given is consistent. In fact, by Remark 1, if two fields $L_a, L_{a'} \in \mathcal{L}(e,f)$ are $\mathbb{Q}_p$-isomorphic, then they are also equivalent.

Lemma 1. *Let $L_a/\mathbb{Q}_p$ be a normal extension and let $a \sim a'$. Then also $L_{a'}/\mathbb{Q}_p$ is normal.*

Proof. By Proposition 1, $L_a/\mathbb{Q}_p$ is normal if and only if $e \mid (a(p-1), q-1)$ and by (4) this condition is equivalent to $e \mid (a'(p-1), q-1)$. ∎

If $a \sim a'$ and $L_a, L_{a'}$ are normal extensions of $\mathbb{Q}_p$, then condition (3) can be expressed also in a different way. We shall need the following simple lemma, which we state without proof.

Lemma 2. *Let $f_0 \mid f$ and let r be a prime dividing $p^{f_0} - 1$. Then*

$$\nu_r\left(\frac{q-1}{p^{f_0}-1}\right) = \begin{cases} \nu_r(f/f_0) + \nu_r(p^{f_0}+1) - 1 & \textit{if } r = 2,\ p^{f_0} \equiv 3 \pmod 4 \\ & \qquad \textit{and } 2 \mid (f/f_0), \\ \nu_r(f/f_0) & \textit{otherwise.} \end{cases}$$

Proposition 3. *Let $L_a, L_{a'} \in \mathcal{L}(e,f)$ be normal over $\mathbb{Q}_p$. The following are equivalent*:

(i) $L_a \sim L_{a'}$;

$$\text{(ii)} \begin{cases} (2^m f, e, a) = (2^m f, e, a'), & \textit{where } m = \nu_2(p+1) - 1 \\ & \textit{if } p \equiv 3 \pmod 4 \textit{ and } 2 \mid f; \\ (f, e, a) = (f, e, a') & \textit{otherwise.} \end{cases}$$

Proof. We shall prove the proposition by showing that, for all primes r dividing e,

$$\nu_r\left(\frac{q-1}{p-1}, e, a\right) = \nu_r\left(\frac{q-1}{p-1}, e, a'\right) \tag{6}$$

$$\Leftrightarrow \begin{cases} \nu_r(2^m f, e, a) = \nu_r(2^m f, e, a') & \text{if } p \equiv 3 \pmod 4 \text{ and } 2 \mid f; \\ \nu_r(f, e, a) = \nu_r(f, e, a') & \text{otherwise.} \end{cases} \tag{7}$$

If $r \nmid p-1$, then, by Proposition 1, $\nu_r(e) \le \nu_r(a)$ and $\nu_r(e) \le \nu_r(a')$, hence both (6) and (7) are satisfied.

If $r \mid p-1$, we apply Lemma 2 with $f_0 = 1$ to obtain

$$\begin{cases} \nu_r(2^m f) = \nu_r\left(\dfrac{q-1}{p-1}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } 2 \mid f; \\ \nu_r(f) = \nu_r\left(\dfrac{q-1}{p-1}\right) & \text{otherwise. } \blacksquare \end{cases}$$

Assume again that $L_a, L_{a'}$ are normal extensions of $\mathbb{Q}_p$. We are now ready to interpret the arithmetical equivalence (3) in terms of the Galois groups of L_a and $L_{a'}$ over $\mathbb{Q}_p$.

We shall write $G_a = \langle \sigma, \tau \rangle$ as in Proposition 2 and, similarly,

$$G_{a'} = \langle \sigma', \tau' \mid \sigma'^e = 1,\ \tau'^f = \sigma'^{a'},\ \tau'\sigma'\tau'^{-1} = \sigma'^p \rangle.$$

Theorem 1. *Two normal extensions $L_a, L_{a'} \in \mathcal{L}(e, f)$ are equivalent if and only if their Galois groups G_a and $G_{a'}$ are isomorphic.*

Proof. Suppose that (3) holds, and let (k, s) be as in equation (5). We explicitly construct an isomorphism $\varphi : G_a \to G_{a'}$ as follows. Set

$$\varphi(\sigma) = \sigma'^k, \qquad \varphi(\tau) = \sigma'^s \tau'.$$

We can extend φ to G_a by multiplicativity, since it is easy to verify that

$$\varphi(\sigma^e) = 1, \qquad \varphi(\tau^f) = \sigma'^{ak} = \varphi(\sigma^a), \qquad \varphi(\tau\sigma\tau^{-1}) = \sigma'^{pk} = \varphi(\sigma^p).$$

Moreover, $G_{a'} = \langle \varphi(\sigma), \varphi(\tau) \rangle$ and, since G_a and $G_{a'}$ have the same order, $G_a \cong G_{a'}$.

Conversely, suppose $G_a \cong G_{a'}$. Let $m = \nu_2(p+1) - 1$ as in Proposition 3. We shall show that, for each prime r, this implies

$$\begin{cases} \nu_r(2^m f, e, a) = \nu_r(2^m f, e, a') & \text{if } p \equiv 3 \pmod 4 \text{ and } 2 \mid f; \\ \nu_r(f, e, a) = \nu_r(f, e, a') & \text{otherwise.} \end{cases} \tag{8}$$

Clearly, it suffices to consider only those primes r dividing e. If $r\nmid p-1$, then, by Proposition 1, $\nu_r(a)\geq\nu_r(e)$ and $\nu_r(a')\geq\nu_r(e)$, so condition (8) is automatically satisfied.

Let $r\,|\,p-1$, and consider first the case when $r=2$, $p\equiv 3\pmod 4$ and $2\,|\,f$. We construct a 2-Sylow subgroup of G_a as follows. Let $e=2^{\nu_2(e)}e_2$, $f=2^{\nu_2(f)}f_2$ and $a=2^{\nu_2(a)}a_2$. Let also b_2 be an integer such that $a_2b_2\equiv 1 \pmod{2^{\nu_2(e)}}$. Define

$$\sigma_2=\sigma^{e_2}\quad\text{and}\quad\tau_2=\tau^{f_2b_2e_2},$$

and let $S_{2,a}=\langle\sigma_2,\tau_2\rangle$. We have

$$(9)\quad \sigma_2^{2^{\nu_2(e)}}=1,\quad \tau_2^{2^{\nu_2(f)}}=\tau^{fb_2e_2}=\sigma^{2^{\nu_2(a)}a_2b_2e_2}=\sigma_2^{2^{\nu_2(a)}},\quad \tau_2\sigma_2\tau_2^{-1}=\sigma_2^k,$$

where $k=p^{f_2b_2e_2}$. Note that, since $f_2b_2e_2$ is odd, $k\equiv 3\pmod 4$ and $\nu_2(p^{f_2b_2e_2}+1)=\nu_2(p+1)$. From (9) it follows that $S_{2,a}$ is a 2-Sylow subgroup of G_a.

Now remember that, by Proposition 1, $\nu_2(e)\leq\nu_2(a)+\nu_2(p-1)=\nu_2(a)+1$, whence

$$\tau_2^{2^{\nu_2(f)}}=\begin{cases}\sigma_2^{2^{\nu_2(e)-1}} & \text{if } \nu_2(a)=\nu_2(e)-1,\\ 1 & \text{if } \nu_2(a)\geq\nu_2(e).\end{cases}$$

If $\nu_2(2^mf)\leq\nu_2(e)-1$, then condition (8) is obviously satisfied, hence we may suppose $\nu_2(2^mf)\geq\nu_2(e)$. We now count the elements of $S_{2,a}$ of exponent $2^{\nu_2(f)}$. Let $g=\sigma_2^x\tau_2^y\in S_{2,a}$, where $0\leq x<2^{\nu_2(e)}$ and $0\leq y<2^{\nu_2(f)}$. We have

$$(\sigma_2^x\tau_2^y)^{2^{\nu_2(f)}}=\sigma_2^{x\{1+k^y+\ldots+k^{y(2^{\nu_2(f)}-1)}\}}\tau_2^{2^{\nu_2(f)}y}.$$

If y is even, the number of solutions of $(\sigma_2^x\tau_2^y)^{2^{\nu_2(f)}}=1$ does not depend on a. If y is odd, then

$$\nu_2(1+k^y+\ldots+k^{y(2^{\nu_2(f)}-1)})=\nu_2\biggl(\frac{k^{y2^{\nu_2(f)}}-1}{k^y-1}\biggr)=\nu_2(2^mf),$$

by Lemma 2. Since we have assumed $\nu_2(2^mf)\geq\nu_2(e)$, this implies that, for y odd and for all x,

$$(10)\qquad (\sigma_2^x\tau_2^y)^{2^{\nu_2(f)}}\begin{cases}\neq 1 & \text{if } \nu_2(a)=\nu_2(e)-1,\\ =1 & \text{if } \nu_2(a)\geq\nu_2(e).\end{cases}$$

Consider the analogous 2-Sylow subgroup $S_{2,a'}$ of $G_{a'}$ and the analogue of condition (10) for elements of $S_{2,a'}$. If $G_a\cong G_{a'}$, then $S_{2,a}\cong S_{2,a'}$ and therefore $S_{2,a}$ and $S_{2,a'}$ have the same number of elements of exponent $2^{\nu_2(f)}$. It follows that either $\nu_2(a)=\nu_2(a')=\nu_2(e)-1$ or $\min\{\nu_2(a),\nu_2(a')\}\geq\nu_2(e)$. In both cases condition (8) is satisfied.

For the remaining cases, we shall consider the maximal r-power dividing the order of elements of G_a, $\nu_r(G_a)=\max_{g\in G_a}\nu_r(\mathrm{ord}(g))$. Let $g=\sigma^x\tau^y\in G_a$, where $0 \le x < e$ and $0 \le y < f$. Assume first that $y \ne 0$, and let $(y,f) = f_0$, $y = f_0 z$, where $(z, f/f_0) = 1$. The least power of g that belongs to the subgroup generated by σ is g^{f/f_0}. By simple calculations as above, we get

$$g^{f/f_0} = \sigma^{x\frac{q^z-1}{p^{f_0 z}-1}+az}$$

and hence

$$\operatorname{ord}(g) = \frac{f}{f_0}\cdot\frac{e}{\left(x\dfrac{q^z-1}{p^{f_0 z}-1}+az, e\right)}.$$

LEMMA 3. *Let $f_0 < f$ be fixed. Then the maximum value of* $\operatorname{ord}(g)$ *is equal to*

$$\frac{f}{f_0}\cdot\frac{e}{\left(\dfrac{q-1}{p^{f_0}-1}, a, e\right)}.$$

Proof. Since $(z, f/f_0) = 1$, we have $(p^{f_0 z}-1, q-1) = p^{f_0}-1$. Now $p^{f_0 z}-1 \mid q^z - 1 = (q-1)\frac{q^z-1}{q-1}$, whence

$$\frac{p^{f_0 z}-1}{p^{f_0}-1}\,\Big|\,\frac{q^z-1}{q-1} \quad\text{or, equivalently,}\quad \frac{q-1}{p^{f_0}-1}\,\Big|\,\frac{q^z-1}{p^{f_0 z}-1}.$$

Therefore,

$$\left(\frac{q-1}{p^{f_0}-1}, a, e\right)\,\Big|\,\left(x\frac{q^z-1}{p^{f_0 z}-1}+az, e\right)$$

for all x and all z.

On the other hand, let $z = 1$ and choose x such that, for all primes r dividing e,

$$x \equiv \begin{cases} 1 \pmod r & \text{if } \nu_r\left(\dfrac{q-1}{p^{f_0}-1}\right) < \nu_r(a), \\ 0 \pmod r & \text{if } \nu_r\left(\dfrac{q-1}{p^{f_0}-1}\right) \ge \nu_r(a). \end{cases}$$

With this choice we have, for $r \mid e$,

$$\nu_r\left(x\frac{q-1}{p^{f_0}-1}+a, e\right) = \min\left\{\nu_r\left(\frac{q-1}{p^{f_0}-1}\right), \nu_r(a), \nu_r(e)\right\}$$

and the lemma follows. ∎

Consider the maximal r-power dividing the order of g. By Lemma 2, and taking into account that we have already excluded the case $r = 2$, $p \equiv 3 \pmod 4$ and $2 \mid f$, Lemma 3 translates into

$$\begin{aligned}\max_{y\ne 0}\nu_r(\operatorname{ord}(\sigma^x\tau^y)) &= \max_{f_0<f}\left\{\nu_r\left(\frac{f}{f_0}\right)+\nu_r(e)-\nu_r\left(\frac{q-1}{p^{f_0}-1}, e, a\right)\right\} \\ &= \max_{f_0<f}\left\{\nu_r(e), \nu_r\left(\frac{f}{f_0}\right), \nu_r\left(\frac{f}{f_0}\right)+\nu_r(e)-\nu_r(a)\right\}.\end{aligned}$$

Clearly, this maximum is reached for $f_0 = 1$. Since, moreover, if $y = 0$ then $\operatorname{ord}(\sigma^x) \mid e$, we get

$$\nu_r(G_a) = \max\{\nu_r(e), \nu_r(f), \nu_r(f) + \nu_r(e) - \nu_r(a)\}.$$

Considering the analogous equation for $\nu_r(G_{a'})$, we have

$$\begin{cases} \nu_r(G_a) = \nu_r(G_{a'}) = \max\{\nu_r(e), \nu_r(f)\} \Leftrightarrow \nu_r(a), \nu_r(a') \geq \min\{\nu_r(f), \nu_r(e)\}, \\ \nu_r(G_a) = \nu_r(G_{a'}) > \max\{\nu_r(e), \nu_r(f)\} \Leftrightarrow \nu_r(a) = \nu_r(a') < \min\{\nu_r(f), \nu_r(e)\}. \end{cases}$$

In any case, condition (8) is satisfied. ■

Remark 3. We note that in the abelian case, when $p \equiv 3 \pmod 4$ and $2 \mid f$ we have $(2^m f, e, a) = (f, e, a)$. In fact, since $e \mid p-1$, we have $\nu_2(e) \leq 1 \leq \nu_2(f) < \nu_2(2^m f)$.

Remark 4. For Galois groups of normal extensions of $\mathbb{Q}_p$ one could also consider the following equivalence relation, more restrictive than pure isomorphism.

Let G and G' be the Galois groups of two normal extensions of $\mathbb{Q}_p$. Let $G \supseteq G_0 \supset G_1 \supset \ldots \supset G_h = \{1\}$ and $G' \supseteq G'_0 \supset G'_1 \supset \ldots \supset G'_{h'} = \{1\}$ be the chains of the ramification groups of G and G', respectively. Then we call G and G' *strongly isomorphic* if $h = h'$ and there exists an isomorphism $\varphi : G \to G'$ such that $\varphi(G_i) = G'_i$ for all $i = 0, \ldots, h$.

The explicit isomorphism constructed in the proof of Theorem 1 shows that, in the case of tamely ramified Galois extensions of $\mathbb{Q}_p$, two Galois groups are isomorphic if and only if they are strongly isomorphic.

In the proof of Theorem 1, we have constructed from a solution (s, k) of the congruence

$$a' + s\frac{q-1}{p-1} \equiv ka \pmod e \tag{11}$$

an isomorphism $\varphi = \varphi_{(s,k)} : G \to G'$ such that

$$\varphi(\sigma^j \tau^i) = \sigma'^{kj + s\frac{p^i - 1}{p-1}} \tau'^i.$$

More generally, if $a \sim a'$, from a solution (s, k) of (11) we can construct a map $\varphi = \varphi_{(s,k)} : \Sigma_{L_a} \to \Sigma_{L_{a'}}$ by mimicking the case of normal extensions; namely, we define

$$\varphi(\lambda_a^{ji}) = \lambda_{a'}^{kj + s\frac{p^i - 1}{p-1}, i}. \tag{12}$$

Proposition 4. *If $a \sim a'$ are related by* (11), *then the map $\varphi_{(s,k)}$ is one-to-one.*

Proof. It is enough to observe that the map $\mathbb{Z}/e\mathbb{Z} \to \mathbb{Z}/e\mathbb{Z}$ given by $j \mapsto kj + s(p^i - 1)/(p-1)$ is one-to-one, and this is true because $(k, e) = 1$. ■

4. Invariance of the index under equivalence of fields. We shall now apply the results of the previous sections to obtain a sufficient local condition in order that two number fields have the same index (Theorem 2). When the number fields are Galois over $\mathbb{Q}$, we shall reinterpret this condition in terms of their Galois groups (Corollary 3). Finally, at the end of the paper we shall briefly discuss the necessity of our local condition in order that the conclusion of Theorem 2 holds true.

We first recall briefly how the p-component of the index of a number field K can be described in terms of the completions of K at the primes lying over p.

Let L be a finite extension of $\mathbb{Q}_p$ and denote by $\mathcal{O}_L$ the integral closure of $\mathbb{Z}_p$ in L. Let α, β be integral generators of L and denote by f_α and f_β their minimal polynomials over $\mathbb{Z}_p$. We let $\operatorname{disc}(\alpha)$ be the discriminant of f_α, $\operatorname{Res}(\alpha,\beta)$ be the resultant of f_α and f_β and $\operatorname{ind}(\alpha) = [\mathcal{O}_L : \mathbb{Z}_p[\alpha]]$. Finally, we put $\operatorname{disc}_p(\alpha) = |\operatorname{disc}(\alpha)|$, $\operatorname{ind}_p(\alpha) = |\operatorname{ind}(\alpha)|$ and $\operatorname{Res}_p(\alpha,\beta) = |\operatorname{Res}(f_\alpha, f_\beta)|$ (here $|0| = \infty$).

Definition 4. Let $L^{(1)}, \ldots, L^{(n)}$ be finite extensions of $\mathbb{Q}_p$. For $\boldsymbol{\alpha} = (\alpha^{(1)}, \ldots, \alpha^{(n)}) \in \mathcal{O}_{L^{(1)}} \oplus \ldots \oplus \mathcal{O}_{L^{(n)}}$, where $\alpha^{(i)}$ is a generator of $L^{(i)}$ for all i, we define

$$I_p(\boldsymbol{\alpha}) = \Big\{ \sum_{1\le i<j\le n} \operatorname{Res}_p(\alpha^{(i)}, \alpha^{(j)}) + \sum_{i=1}^{n} \operatorname{ind}_p(\alpha^{(i)}) \Big\}.$$

We also put $I_p(\boldsymbol{\alpha}) = \infty$ when some of the $\alpha^{(i)}$ is not a generator.

It is immediate to verify that the set of values of $I_p(\boldsymbol{\alpha})$ depends only on the isomorphism class of the fields $L^{(i)}$.

Consider the set $\mathcal{E}$ of isomorphism classes $[L]$ of finite extensions 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 $\Gamma = [L^{(1)}] + \ldots + [L^{(n)}] \in \bar{\mathcal{E}}$ we define

$$I_p(\Gamma) = \min_{\boldsymbol{\alpha} \in \mathcal{O}_{L^{(1)}} \oplus \ldots \oplus \mathcal{O}_{L^{(n)}}} I_p(\boldsymbol{\alpha}).$$

In the particular case when $\Gamma = n[L]$ we can also write

$$I_p(n[L]) = \min_{\substack{A \subset \mathcal{O}_L \\ |A| = n}} I_p(A). \tag{13}$$

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

$$I_p(\{\alpha^{(1)}, \ldots, \alpha^{(n)}\}) = \sum_{i=1}^{n} \operatorname{ind}_p(\alpha^{(i)}) + \sum_{1\le i<j\le n} \operatorname{Res}_p(\alpha^{(i)}, \alpha^{(j)}) \tag{14}$$

is clearly symmetric in the $\alpha^{(i)}$.

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

$$[K \otimes \mathbb{Q}_p] = n_1[L_1] + \ldots + n_s[L_s],$$

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 5 (Nart). *For every number field K,*

$$\mathrm{ind}_p(K) = I_p([K \otimes \mathbb{Q}_p]).$$

Proof. See [5, Thm. 1]. ∎

Corollary 2. *Let K be a Galois number field, and let L be the completion of K at any prime over p. Then there exists $n \in \mathbb{N}$ such that*

$$\mathrm{ind}_p(K) = I_p(n[L]).$$

Proof. It is enough to observe that the completions of K at the primes lying over p are all isomorphic; hence $[K \otimes \mathbb{Q}_p] = n[L]$, where n is the number of distinct primes of $\mathcal{O}_K$ over p, and Proposition 5 applies. ∎

We can now state our main result on the index of local fields.

Theorem 2. *Let $L, L' \in \mathcal{L}(e, f)$. If $L \sim L'$, then $I_p(n[L]) = I_p(n[L'])$ for each $n > 0$.*

We remark that, if either e or f is equal to 1, then (5) is trivially satisfied for all a, a'. Hence, in particular, Theorem 2 includes the analogous result proved in [2] for the case of totally ramified extensions.

Proof. Let a, a' be such that $L = L_a$ and $L' = L_{a'}$, and let $\pi \in L, \pi' \in L'$ be roots of the polynomials $X^e - \zeta^a p, X^e - \zeta^{a'} p$, respectively. Since $L \sim L'$, then $a \sim a'$ and (5) holds.

In the following we fix once and for all a solution $(s, t, k) \in \mathbb{Z}^3$ of (5) with $(k, e(q-1)) = 1$.

We recall that each element $\alpha \in \mathcal{O}_L$ can be written uniquely as a series $\alpha = \sum_{h=0}^{\infty} \alpha_h \pi^h$, where either $\alpha_h = 0$ or $\alpha_h = \zeta^{x_h}$ for some $x_h \in \mathbb{Z}$. If $H = H(\alpha)$ is the set of indices h for which $\alpha_h \neq 0$, we shall also write $\alpha = \sum_{h \in H} \zeta^{x_h} \pi^h$.

We give some preliminary lemmas.

Lemma 4. *The map $\psi : \mathcal{O}_L \to \mathcal{O}_{L'}$ defined by*

$$\psi\Big(\sum_{h \in H} \zeta^{x_h} \pi^h\Big) = \sum_{h \in H} \zeta^{k x_h + t h} \pi'^h$$

is one-to-one.

Proof. We can write $\psi(\alpha) = \sum_{h=0}^{\infty} \psi_h(\alpha_h) \pi'^h$, where $\psi_h(0) = 0$ and $\psi_h(\zeta^{x_h}) = \zeta^{k x_h + t h}$ for all $h \geq 0$, $x_h \in \mathbb{Z}$. Since $(k, q-1) = 1$, all maps

$\widetilde{\psi}_h : \mathbb{Z}/(q-1)\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$ defined by $\widetilde{\psi}_h(x) = kx + th$ are one-to-one, and the lemma follows immediately. ■

Lemma 5. *Let $\lambda_1, \lambda_2 \in \Sigma_{L_a}$, and let $\alpha^{(1)}, \alpha^{(2)} \in \mathcal{O}_{L_a}$. Then for $\varphi = \varphi_{(s,k)}$ we have*

$$|\lambda_1(\alpha^{(1)}) - \lambda_2(\alpha^{(2)})| = |\varphi(\lambda_1)(\psi(\alpha^{(1)})) - \varphi(\lambda_2)(\psi(\alpha^{(2)}))|.$$

In particular, α and $\psi(\alpha)$ have the same degree over $\mathbb{Q}_p$ for all $\alpha \in L_a$.

Proof. For $i = 1, 2$, let $\alpha^{(i)} = \sum_{h=0}^{\infty} \alpha_h^{(i)} \pi^h$. We have

$$\lambda_1(\alpha^{(1)}) - \lambda_2(\alpha^{(2)}) = \sum_{h=0}^{\infty} (\lambda_1(\alpha_h^{(1)}\pi^h) - \lambda_2(\alpha_h^{(2)}\pi^h)),$$

$$\begin{aligned}\varphi(\lambda_1)&(\psi(\alpha^{(1)})) - \varphi(\lambda_2)(\psi(\alpha^{(2)})) \\ &= \sum_{h=0}^{\infty} (\varphi(\lambda_1)(\psi_h(\alpha_h^{(1)})\pi^h) - \varphi(\lambda_2)(\psi_h(\alpha_h^{(2)})\pi^h)).\end{aligned}$$

By [2, Lemma 3], either $\lambda_1(\alpha_h^{(1)}\pi^h) - \lambda_2(\alpha_h^{(2)}\pi^h)$ is equal to zero or its p-adic valuation is equal to h/e, and the same is true for $\varphi(\lambda_1)(\psi_h(\alpha_h^{(1)})\pi^h) - \varphi(\lambda_2)(\psi_h(\alpha_h^{(2)})\pi^h)$. Hence it suffices to prove that

$$\begin{aligned}(15)\qquad \lambda_1(\zeta^{x_h^{(1)}}\pi^h) &= \lambda_2(\zeta^{x_h^{(2)}}\pi^h) \\ &\Leftrightarrow\ \varphi(\lambda_1)(\psi(\zeta^{x_h^{(1)}}\pi^h)) = \varphi(\lambda_2)(\psi(\zeta^{x_h^{(2)}}\pi^h)).\end{aligned}$$

Let $\lambda_1 = \lambda_a^{i_1 j_1}$, $\lambda_2 = \lambda_a^{i_2 j_2}$. An explicit computation gives that the left-hand side of (15) holds if and only if $j_1, j_2, i_1, i_2, x_h^{(1)}, x_h^{(2)}$ satisfy

$$\begin{aligned}(16)\qquad e(x_h^{(1)}p^{i_1} - x_h^{(2)}p^{i_2}) + ah(p^{i_1} - p^{i_2}) + (j_1 - j_2)h(q-1) \\ \equiv 0 \pmod{e(q-1)}\end{aligned}$$

and the right-hand side of (15) holds if and only if $j_1, j_2, i_1, i_2, x_h^{(1)}, x_h^{(2)}$ satisfy

$$\begin{aligned}(17)\qquad e[(kx_h^{(1)} + ht)p^{i_1} - (kx_h^{(2)} + ht)p^{i_2}] + a'h(p^{i_1} - p^{i_2}) \\ + \left[k(j_1 - j_2) + s\frac{p^{i_1} - p^{i_2}}{p-1}\right]h(q-1) \equiv 0 \pmod{e(q-1)}.\end{aligned}$$

Finally, it is easy to check that, multiplying (16) by k and using (5), we obtain (17). Since $(k, e(q-1)) = 1$, equations (16) and (17) are equivalent.

As to the last statement, it is sufficient to note that (15) implies that $\lambda_1(\alpha) = \lambda_2(\alpha)$ if and only if $\varphi(\lambda_1)(\psi(\alpha)) = \varphi(\lambda_2)(\psi(\alpha))$. ■

Lemma 6. *Let $A \subset \mathcal{O}_L$ be finite. Then $I_p(A) = I_p(\psi(A))$.*

Proof. Let $A = \{\alpha^{(1)}, \ldots, \alpha^{(n)}\}$. By Lemma 5, A contains a non-generator of L_a if and only if $\psi(A)$ contains a non-generator of $L_{a'}$. Then it suffices to consider the case when the $\alpha^{(i)}$ are all generators. We have

$$I_p(A) = I_p(\{\alpha^{(1)}, \ldots, \alpha^{(n)}\}) = \sum_{i=1}^{n} \mathrm{ind}_p(\alpha^{(i)}) + \sum_{1\le i<j\le n} \mathrm{Res}_p(\alpha^{(i)}, \alpha^{(j)}).$$

We recall that

$$\text{(18)}\quad \mathrm{ind}_p(\alpha) = \frac{|\mathrm{disc}(\alpha)| - (e-1)}{2} = \frac{e\sum_{\lambda\in\Sigma_{L_a}} |\lambda(\alpha) - \alpha| - (e-1)}{2}$$

and

$$\text{(19)}\qquad \mathrm{Res}_p(\alpha^{(i)}, \alpha^{(j)}) = \sum_{\lambda_1,\lambda_2\in\Sigma_{L_a}} |\lambda_1(\alpha^{(i)}) - \lambda_2(\alpha^{(j)})|.$$

By Lemma 5, we have $\mathrm{ind}_p(\alpha^{(i)}) = \mathrm{ind}_p(\psi(\alpha^{(i)}))$, $\mathrm{Res}_p(\alpha^{(i)}, \alpha^{(j)}) = \mathrm{Res}_p(\psi(\alpha^{(i)}), \psi(\alpha^{(j)}))$ and the lemma follows. ■

We are now ready to conclude the proof of the theorem. Take the minimum of $I_p(A)$ as A varies over all subsets of $\mathcal{O}_L$ with n elements. By (13) and Lemma 6 we get

$$I_p(n[L]) = \min_{\substack{A\subset\mathcal{O}_L\\ |A|=n}} I_p(A) = \min_{\substack{A'\subset\mathcal{O}'_L\\ |A'|=n}} I_p(A') = I_p(n[L']). \ ■$$

The next corollary gives an application of Theorem 2 to the case of global fields.

COROLLARY 3. *Let $n, e, f \in \mathbb{N}$ and suppose that $p\nmid e$. Let K, K' be Galois extensions of $\mathbb{Q}$ of degree nef. Assume that*: (i) *pR_K and $pR_{K'}$ have the same factorization type $(P_1\ldots P_n)^e$*; (ii) *the decomposition groups of the primes over p in $\mathcal{O}_K$ and $\mathcal{O}_{K'}$ are isomorphic. Then*

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

Proof. Under our hypotheses, we have $[K\otimes\mathbb{Q}_p] = n[L]$ and $[K'\otimes\mathbb{Q}_p] = n[L']$ for some $L, L' \in \mathcal{L}(e,f)$. Now, L and L' are normal over $\mathbb{Q}_p$ and $\mathrm{Gal}(L/\mathbb{Q}_p)$ (resp. $\mathrm{Gal}(L'/\mathbb{Q}_p)$) is isomorphic to the decomposition group of any prime of $\mathcal{O}_K$ (resp. $\mathcal{O}_{K'}$) over p. Hence $L \sim L'$ and Theorem 2 applies. ■

We have given in [2] a recursive algorithm for computing $I_p(n[L])$ when L is tamely ramified over $\mathbb{Q}_p$. By Theorem 2, the value of $I_p(n[L_a])$ depends only on the equivalence class of a, but unfortunately we do not have an expression in closed terms for the function $I_p(n[L_a]) = I_p(n; e, f, [a])$ (where $[a]$ denotes the equivalence class of a).

We are not able to prove that if $L_a \not\sim L_{a'}$, then there exists an integer n such that $I_p(n[L_a]) \ne I_p(n[L_{a'}])$; however, we remark that the actual computation of $I_p(n[L])$ with our algorithm requires, essentially, the knowledge of $I_p(m_E[E])$ for all subfields E of L_a of type $E = \mathbb{Q}_p(\zeta^x\pi^h)$ and suitable integers $m_E < n$ depending on E, and that the lattice of these subfields depends on the equivalence class of a.

In fact, let $\mathcal{S}(L)$ be the set of subfields E of L of type $E = \mathbb{Q}_p(\zeta^x\pi^h)$, where $h \geq 0$ and $0 \leq x < q-1$. We have the following

PROPOSITION 6. *There exists a one-to-one map between $\mathcal{S}(L_a)$ and $\mathcal{S}(L_{a'})$ which preserves the ramification index and the inertial degree if and only if $L_a \sim L_{a'}$.*

Proof. If $L_a \sim L_{a'}$, then the map $\boldsymbol{\psi} : \mathcal{S}(L_a) \to \mathcal{S}(L_{a'})$ defined by $\boldsymbol{\psi}(\mathbb{Q}_p(\zeta^x\pi^h)) = \mathbb{Q}_p(\psi(\zeta^x\pi^h))$ is one-to-one and preserves the degree, by Lemmas 4 and 5.

Moreover, the ramification index of both $\mathbb{Q}_p(\zeta^x\pi^h)$ and $\mathbb{Q}_p(\psi(\zeta^x\pi^h))$ is $e/(h,e)$, and therefore also their inertial degrees coincide.

On the other hand, let $\left(e, \frac{q-1}{p-1}\right) = d$ and let m be any divisor of d. A field $\mathbb{Q}_p(\zeta^x\pi^h)$ in $\mathcal{S}(L_a)$ is totally ramified over $\mathbb{Q}_p$ of degree m if and only if $(e,h) = e/m$ and x is a solution of $xm + ah' \equiv 0 \left(\operatorname{mod} \frac{q-1}{p-1}\right)$, where $h' = hm/e$. Now, the last congruence is solvable if and only if $m \mid a$ and therefore $\mathcal{S}(L_a)$ contains a totally ramified subextension of degree m if and only if a is a multiple of m. It follows that if L_a and $L_{a'}$ are not equivalent, then there is no degree-preserving bijection between the totally ramified extensions of $\mathbb{Q}_p$ contained in $\mathcal{S}(L_a)$ and $\mathcal{S}(L_{a'})$. ∎

In view of the last proposition, we can interpret the example of non-equivalent fields given in [2], where $p = 3$ and $L_a = L_0$, $L_{a'} = L_1$ are elements of $\mathcal{L}(2,2)$, as follows: L_0 has two totally ramified subextensions of degree 2, L_1 has no such subextension, and we get different values for $I_3(n[L_0])$ and $I_3(n[L_1])$ as soon as the algorithm requires to investigate the existence of such subfields.

More generally, if $L_a \not\sim L_{a'}$, our algorithm says that, for n sufficiently large, the two indices must be computed quite differently, and it seems very unlikely to us that they can nevertheless be the same for all n.

Acknowledgements. We wish to thank the referee for his/her helpful suggestions, and in particular for correcting an error in our original formulation of Lemma 2.

References

[1] R. Dedekind, *Über Zusammenhang der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Abh. König. Ges. Wiss. Göttingen 23 (1878), 1–23.

[2] I. Del Corso and R. Dvornicich, *On Ore's conjecture and its developments*, submitted.

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

[4] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer, 1990.

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

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

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

Dipartimento di Matematica
via Buonarroti, 2
56127 Pisa, Italy
E-mail: delcorso@dm.unipi.it
dvornic@dm.unipi.it

Received on 5.11.2000
and in revised form on 31.5.2001 (3913)