Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Number Theory 115 (2005) 230–248
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

# An equivalence between local fields

Ilaria Del Corso*, Roberto Dvornicich

*Dipartimento di Matematica, via Buonarroti, 2 56127 Pisa, Italy*

Received 8 April 2004

Available online 2 February 2005

Communicated by D. Goss

**Abstract**

The $p$-component of the index of a number field $K$ depends only on the completions of $K$ at the primes over $p$. In this paper we define an equivalence relation between $m$-tuples of local fields such that, if two number fields $K$ and $K'$ have equivalent $m$-tuples of completions at the primes over $p$, then they have the same $p$-component of the index. This equivalence can be interpreted in terms of the decomposition groups of the primes over $p$ of the normal closures of $K$ and $K'$.

*Keywords:* Local fields; Galois groups; Index

## 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 $\alpha$.

* Corresponding author.
*E-mail addresses:* delcorso@dm.unipi.it (I. Del Corso), dvornic@dm.unipi.it (R. Dvornicich).

0022-314X/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2004.10.011

It is known that the form of the factorization of the ideal $(p)$ in $R_K$ is not sufficient, in general, to determine the $p$-component, $\text{ind}_p(K)$, of the index of $K$ (see [4]). On the other hand, $\text{ind}_p(K)$ is completely determined by the $p$-adic completion $K \otimes \mathbb{Q}_p$ of the field $K$. In fact, it can be shown that $\text{ind}_p(K)$ is nothing else that the index, $I_p(K \otimes \mathbb{Q}_p)$, of $K \otimes \mathbb{Q}_p$, i.e., the minimum power of $p$ which divides $\text{ind}(f)$ when $f$ runs over all monic polynomials of $\mathbb{Z}_p[X]$ such that $\mathbb{Q}_p[X]/(f(X)) \cong K \otimes \mathbb{Q}_p$ (see [6; 2, Section 2]).

Now, the $\mathbb{Q}_p$-algebra $K \otimes \mathbb{Q}_p$ decomposes as a direct sum of fields, $K \otimes \mathbb{Q}_p \cong E_1 \oplus \ldots \oplus E_m$, where the $E_i$'s are the completions of $K$ at the primes lying over $p$. We can extend the definition of the index $I_p$ to all elements of the free abelian monoid generated by the finite extensions of $\mathbb{Q}_p$ so that $I_p(K \otimes \mathbb{Q}_p) = I_p(E_1 + \cdots + E_m)$. If $K/\mathbb{Q}$ is Galois, then the decomposition of $K \otimes \mathbb{Q}_p$ takes the simpler form $K \otimes \mathbb{Q}_p \cong E^n$ for some integer $n$ and some Galois extension $E$ of $\mathbb{Q}_p$; in our notation, $I_p(K \otimes \mathbb{Q}_p)$ takes the form $I_p(nE)$.

In two previous papers we examined this last case in detail. In [2] we described a method for explicitly computing $I_p(nE)$ for all $n$ and all normal and tamely ramified extensions of $\mathbb{Q}_p$. In [3] we introduced an equivalence relation on local fields, more general than isomorphism, which is sufficient to guarantee that, if two local fields $E, E'$ tamely ramified over $\mathbb{Q}_p$ are equivalent, $E \sim E'$, then

$$I_p(nE) = I_p(nE') \qquad \text{for all } n \in \mathbb{N}. \tag{1}$$

The equivalence relation can be expressed as a purely arithmetical condition. If, moreover, $E$ and $E'$ are Galois over $\mathbb{Q}_p$, we showed that our arithmetical condition is also equivalent to the fact that the Galois groups $\text{Gal}(E/\mathbb{Q}_p)$ and $\text{Gal}(E'/\mathbb{Q}_p)$ are isomorphic.

In the present paper the problem of finding more general results on the index has been our motivation for studying in more detail the equivalence relation between local fields defined in [3], and for extending its definition to $m$-tuples of local fields.

In Section 3 we reexamine the case of single fields and generalize the results of [3] to tamely ramified extensions $E$ and $E'$, not necessarily normal. We show that the following are equivalent (see Theorems 1 and 2):

(i) $E \sim E'$;
(ii) $\text{Gal}(\underline{E}/\mathbb{Q}_p) \cong \text{Gal}(\underline{E}'/\mathbb{Q}_p)$, where $\underline{E}$ and $\underline{E}'$ are the normal kernels of $E$ and $E'$, respectively;
(iii) there exists an isomorphism $\varphi : \text{Gal}(\bar{E}/\mathbb{Q}_p) \to \text{Gal}(\bar{E}'/\mathbb{Q}_p)$ such that $\varphi(\text{Gal}(\bar{E}/E)) = \text{Gal}(\bar{E}'/E')$, where $\bar{E}$ and $\bar{E}'$ denote the normal closures of $E$ and $E'$, respectively.

In Section 4 we extend our definition of equivalence to $m$-tuples of tamely ramified extensions of $\mathbb{Q}_p$ (see Definition 3), and we characterize the pairs $(E_1, \ldots, E_m)$ and $(E'_1, \ldots, E'_m)$ of equivalent $m$-tuples in terms of the Galois groups of the normal closures of the composita $E_1 \cdots E_m$ and $E'_1 \cdots E'_m$ (Theorem 3).

As an application, we show that, if $(E_1, \ldots, E_m)$ and $(E'_1, \ldots, E'_m)$ are equivalent, then

$$I_p(n_1E_1 + \cdots + n_mE_m) = I_p(n_1E'_1 + \cdots + n_mE'_m) \qquad \text{for all } n_1, \ldots, n_m \in \mathbb{N} \quad (2)$$

(see Theorem 4).

Reading these results in a global context, we obtain a sufficient condition in order that two number fields $K$ and $K'$ have the same $p$-component of the index. This condition is given in terms of the decomposition groups of the primes over $p$ of the normal closures of $K$ and $K'$ (Corollary 2 and Proposition 9).

In Section 7 we consider the simplest case of two non-equivalent pairs $(E_1, E_2)$ and $(E'_1, E'_2)$ and we show that there exist two integers $n_1, n_2$ such that $I_p(n_1E_1+n_2E_2) \neq I_p(n_1E'_1+n_2E'_2)$. In practice, this shows that the equivalence between $m$-tuples of fields is likely to be also a necessary condition in order that (2) holds.

Since we do not have a general procedure for computing such indices, checking our example has required a rather long analysis. On the other hand, already this example shows also that a recursive algorithm of the type described in [2] for computing $I_p(nE)$ cannot exist in the general case (see Remark 7).

## 2. Notation and preliminary results

Throughout the paper, $p$ will be a fixed prime number, $e, f$ will be positive integers with $(e, p) = 1$, and $q = p^f$.

Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in the complex numbers, $\bar{\mathbb{Q}}_p$ be a given algebraic closure of $\mathbb{Q}_p$, and $\imath : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$ be a fixed embedding. We shall denote by $| \ |$ the $p$-adic valuation of $\bar{\mathbb{Q}}_p$ normalized so that $|p| = 1$ and, for any positive integer $n$, by $\zeta_n$ the image of $\exp(\frac{2\pi i}{n})$ under the embedding $\imath$. Finally, we shall denote by $U_f = \mathbb{Q}_p(\zeta_{q-1})$ the unique unramified extension of $\mathbb{Q}_p$ of degree $f$ contained in $\bar{\mathbb{Q}}_p$ and by $\mathcal{L}(e, f)$ the set of all (tamely ramified) extensions $L$ of $\mathbb{Q}_p$ ($L \subset \bar{\mathbb{Q}}_p$) with inertial degree $f$ and ramification index $e$.

By classical theory (see for instance [5]), $\mathcal{L}(e, f)$ has exactly $e$ elements and each field $L \in \mathcal{L}(e, f)$ is a totally and tamely ramified extension of $U_f$. Moreover, we can write $L = U_f(\pi)$, where $\pi$ is a root of the polynomial $X^e - \zeta_{q-1}^a p$ for some $a \in \mathbb{Z}$. Conversely, for any integer $a$ the field $U_f[X]/(X^e - \zeta_{q-1}^a p)$ is a tamely and totally ramified extension of $U_f$ of degree $e$, and hence determines an element $L \in \mathcal{L}(e, f)$ up to isomorphism.

We describe a procedure to select a particular root of the polynomial $X^e - \zeta_{q-1}^a p$ and hence to associate to each $a \in \mathbb{Z}$ a unique element $L_a \in \mathcal{L}(e, f)$. For $e \in \mathbb{N}$, let $\pi_{0,e}$ be the image by the fixed embedding $\imath$ of the positive real $e$-th root of $p$. Now, a particular root of $X^e - \zeta_{q-1}^a p$ is $\pi_{a,e,f} = \zeta_{e(q-1)}^a \pi_{0,e}$ and we define

$$L_a = U_f(\pi_{a,e,f}) = U_f(\zeta_{e(q-1)}^a \pi_{0,e})$$

(note that, with the definition just given, $\pi_{a,e,f}^d = \pi_{a,\frac{e}{d},f}$, for each $d|e$).

We observe that $L_a = L_{a'}$ if and only if $a \equiv a' \pmod{e}$ and hence $\mathcal{L}(e, f) = \{L_0, \dots, L_{e-1}\}$.

Let $\Sigma_a$ be the set of embeddings $\lambda : L_a \to \bar{\mathbb{Q}}_p$. It is easily verified that $\Sigma_a = \{\lambda_a^{ij} \mid 0 \leqslant i < f, 0 \leqslant j < e\}$, where $\lambda_a^{ij}$ is defined by

$$\begin{cases} \lambda_a^{ij}(\zeta_{q-1}) = \zeta_{q-1}^{p^i}, \\ \lambda_a^{ij}(\pi_{a,e,f}) = \zeta_{e(q-1)}^{a(p^i-1)+j(q-1)} \pi_{a,e,f}. \end{cases} \tag{3}$$

An easy computation shows that $L_a$ is normal over $\mathbb{Q}_p$ if and only if

$$e \mid (q-1, a(p-1)). \tag{4}$$

**Definition 1.** We shall say that two fields $L_a, L_{a'} \in \mathcal{L}(e, f)$ are equivalent (and we shall write $L_a \sim L_{a'}$) if and only if there exist integers $s, t, k$ with $(k, e) = 1$ such that

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

It is immediate to see that (5) holds if and only if

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

**Remark 1.** We recall that two fields $L_a, L_{a'} \in \mathcal{L}(e, f)$ are isomorphic over $\mathbb{Q}_p$ if and only if $a' \equiv p^i a \pmod{(e, q-1)}$ for some integer $i$. Hence isomorphic fields are also equivalent.

For convenience of the reader, we quote some results of [3]. In the following, whenever $L_a \sim L_{a'}$, we shall let $s, t, k$ be integers with $(k, e) = 1$ such that (5) holds.

For a finite extension $L$ of $\mathbb{Q}_p$, we shall denote by $\mathcal{O}_L$ its ring of integers. If $L \in \mathcal{L}(e, f)$, $\zeta = \zeta_{q-1}$ and $\pi$ is an integer of $L$ such that $|\pi| = \frac{1}{e}$, each element $\alpha \in \mathcal{O}_L$ can be written uniquely as a power series in $\pi$ with coefficients in the set $\{0, 1, \zeta, \dots, \zeta^{q-2}\}$ of Teichmüller representatives of $\mathcal{O}_L/(\pi)$, and hence in the form $\alpha = \sum_{h \in H} \zeta^{x_h} \pi^h$, where $H = H(\alpha)$ is the subset of natural numbers $h$ for which the coefficient of $\pi^h$ is non-zero.

**Lemma 1.** *Let $L_a \sim L_{a'}$, $\pi = \pi_{a,e,f}$, $\pi' = \pi_{a',e,f}$. Then the map $\psi = \psi_{L_a, L_{a'}, (k,t)} : \mathcal{O}_{L_a} \to \mathcal{O}_{L_{a'}}$ defined by*

$$\psi\left(\sum_{h \in H} \zeta^{x_h} \pi^h\right) = \sum_{h \in H} \zeta^{kx_h + th} \pi'^h$$

*is one-to-one.*

**Lemma 2.** *Let $L_a \sim L_{a'}$. Then the map $\varphi = \varphi_{L_a,L_{a'},(k,s)} : \Sigma_a \to \Sigma_{a'}$ defined by*

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

*is one-to-one. If, moreover, $L_a$ and $L_{a'}$ are Galois extensions of $\mathbb{Q}_p$, then $\varphi : \mathrm{Gal}(L_a/\mathbb{Q}_p) \to \mathrm{Gal}(L_{a'}/\mathbb{Q}_p)$ is an isomorphism.*

**Lemma 3.** *Let $L_a \sim L_{a'}$, let $\lambda_1, \lambda_2 \in \Sigma_a$, and $\alpha^{(1)}, \alpha^{(2)} \in \mathcal{O}_{L_a}$. Then, for $\varphi = \varphi_{L_a,L_{a'},(k,s)}$, we have*

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

**Proposition 1.** *Let $L, L' \in \mathcal{L}(e, f)$. If $L \sim L'$, then $I_p(n[L]) = I_p(n[L'])$ for each $n > 0$.*

## 3. More on the equivalence of two local fields

Let $L$ be an extension of $\mathbb{Q}_p$; we denote by $\underline{L}$ its *normal kernel*, i.e. the biggest normal extension of $\mathbb{Q}_p$ contained in $L$, and by $\bar{L}$ the normal closure of $L$ over $\mathbb{Q}_p$.

**Proposition 2.** *Let $L = L_a \in \mathcal{L}(e, f)$. Then*

(i) $\underline{L} = \underline{L_a} \in \mathcal{L}(\varepsilon, f)$, *where* $\varepsilon = (q-1, e, a(p-1))$;
(ii) $\bar{L} = \bar{L}_{\bar a} \in \mathcal{L}(e, \bar f)$, *where, setting* $\bar q = p^{\bar f}$ *and* $\bar a = a\frac{\bar q-1}{q-1}$, $\bar f$ *is the least multiple of $f$ such that* $e|(\bar q - 1, \bar a(p-1))$.

**Proof.** (i) First we observe that $\underline{L}$ has the same inertial degree as $L$, hence $\underline{L} = \underline{L_\alpha} \in \mathcal{L}(\varepsilon, f)$ for some $\alpha, \varepsilon$. Since $\pi_{\alpha,\varepsilon,f}/\pi_{a,e,f}^{e/\varepsilon}$ is a root of unity contained in $U_f$, we have $\underline{L} = U_f(\pi_{a,e,f}^{e/\varepsilon})$, and therefore $\underline{L} = \underline{L_a}$. The value of $\varepsilon$ follows from (4) and from the maximality of $\underline{L_a}$ in the set of normal extensions of $\mathbb{Q}_p$ contained in $L$.

(ii) We have $\bar L = U_{\bar f}(\pi_{a,e,f})$, where $\bar f$ is the inertial degree of $\bar L$. Now $\pi_{a,e,f} = \zeta_{e(q-1)}^{a}\pi_{0,e} = \zeta_{e(\bar q-1)}^{\bar a}\pi_{0,e} = \pi_{\bar a,e,\bar f}$, hence $\bar L = \bar L_{\bar a}$. The value of $\bar f$ follows from (4) and from the minimality of $\bar L_{\bar a}$ in the set of normal extensions of $\mathbb{Q}_p$ containing $L$. □

**Theorem 1.** *Let $L_a, L_{a'} \in \mathcal{L}(e, f)$. Then the following are equivalent:*

(i) $L_a \sim L_{a'}$;
(ii) $\underline{L_a} \sim \underline{L_{a'}}$;
(iii) *The Galois groups* $\mathrm{Gal}(\underline{L_a}/\mathbb{Q}_p)$ *and* $\mathrm{Gal}(\underline{L_{a'}}/\mathbb{Q}_p)$ *are isomorphic.*

**Proof.** (i) ⇒ (ii). We first prove that $\underline{L_a}$ and $\underline{L_{a'}}$ have the same ramification index over $\mathbb{Q}_p$. By the description of the normal kernel given in Proposition 2, this amounts to show that $\varepsilon = (q-1, e, a(p-1))$ is equal to $\varepsilon' = (q-1, e, a'(p-1))$. Since $L_a \sim L_{a'}$, Eq. (6) holds; multiplying this equation by $p-1$ we get $\varepsilon = \varepsilon'$. Since $\varepsilon | e$, Eq. (6) gives also $\left(\frac{q-1}{p-1}, \varepsilon, a\right) = \left(\frac{q-1}{p-1}, \varepsilon, a'\right)$, hence $\underline{L}_a \sim \underline{L}_{a'}$.

(ii) $\Rightarrow$ (i). $\underline{L}_a \sim \underline{L}_{a'}$ is equivalent to conditions $\varepsilon = (q-1, e, a(p-1)) = (q-1, e, a'(p-1))$ and $(\frac{q-1}{p-1}, \varepsilon, a) = (\frac{q-1}{p-1}, \varepsilon, a')$; by substituting the value of $\varepsilon$ in the last formula, we get $L_a \sim L_{a'}$.

(ii) $\Leftrightarrow$ (iii): see [3, Theorem 1]. □

**Proposition 3.** *Let $L_a, L_{a'} \in \mathcal{L}(e, f)$. If $L_a \sim L_{a'}$ then $\bar{L}_{\bar{a}}$ and $\bar{L}_{\bar{a}'}$ have the same ramification index, the same inertial degree, and $\bar{L}_{\bar{a}} \sim \bar{L}_{\bar{a}'}$.*

**Proof.** Clearly $\bar{L}_{\bar{a}}$ and $\bar{L}_{\bar{a}'}$ both have ramification index equal to $e$. We show that they have also the same inertial degree. In fact, let $\hat{f}$ be any multiple of $f$ satisfying $e | p^{\hat{f}} - 1$. Then, multiplying the equation

$$a' + s\frac{q-1}{p-1} + te = ka \tag{7}$$

by $\frac{p^{\hat{f}}-1}{q-1}(p-1)$ we get

$$\frac{p^{\hat{f}}-1}{q-1}a'(p-1) \equiv k\frac{p^{\hat{f}}-1}{q-1}a(p-1) \pmod{e}.$$

Since $(k, e) = 1$,

$$e \left| \frac{p^{\hat{f}}-1}{q-1}a(p-1) \right. \Longleftrightarrow e \left| \frac{p^{\hat{f}}-1}{q-1}a'(p-1) \right. ,$$

whence the inertial degrees of $\bar{L}_{\bar{a}}$ and $\bar{L}_{\bar{a}'}$ are the same.

Finally, if $\bar{f}$ is the common inertial degree of $\bar{L}_{\bar{a}}$ and $\bar{L}_{\bar{a}'}$, then $\bar{a} = a\frac{\bar{q}-1}{q-1}$ and $\bar{a}' = a'\frac{\bar{q}-1}{q-1}$, so multiplying (7) by $\frac{\bar{q}-1}{q-1}$ we get that $\bar{L}_{\bar{a}} \sim \bar{L}_{\bar{a}'}$. □

**Remark 2.** The converse of Proposition 3 is not true. For an example, consider the case $p = 3$, $e = 10$, $f = 2$. Then $\frac{q-1}{p-1} = 4$; since $(10, 4) = 2$, we have two different equivalence classes for the extensions $L_a \in \mathcal{L}(10, 2)$, one for $a$ odd and one for $a$ even. Independently of $a$, it is immediate to check that the normal closure of $L_a$ has inertial degree equal to 4, so $\bar{q} = 81$, $\bar{a} = 10a$ and $\frac{\bar{q}-1}{p-1} = 40$. It follows that $(10a, 10, 40) = 10$ for all $a$, so the normal closures of the $L_a$ are all equivalent.

Let $G = \mathrm{Gal}(\bar{L}_{\bar{a}}/\mathbb{Q}_p)$, $G' = \mathrm{Gal}(\bar{L}_{\bar{a}'}/\mathbb{Q}_p)$ and let $H$ (resp. $H'$) the subgroup of $G$ (resp. $G'$) fixing $L_a$ (resp. $L_{a'}$). Setting $\sigma = \lambda_{\bar{a}}^{0,1}$, $\tau = \lambda_{\bar{a}}^{1,0}$, we have (see [3])

$$G = \langle \sigma, \tau \mid \sigma^e = 1, \tau^{\bar{f}} = \sigma^{\bar{a}}, \tau\sigma\tau^{-1} = \sigma^p \rangle. \tag{8}$$

With this notation, it is easy to check that $G_0 = \langle\sigma\rangle$ is the inertia subgroup of $G$ (i.e., $G_0 = \mathrm{Gal}(\bar{L}_{\bar{a}}/U_{\bar{f}})$), and $H = \langle\sigma^{-a}\tau^f\rangle$. Clearly, letting $\sigma' = \lambda_{\bar{a}'}^{0,1}$ and $\tau' = \lambda_{\bar{a}'}^{1,0}$, analogous relations hold for $G'$, $G_0'$ and $H'$.

**Definition 2.** We say that an isomorphism $\varphi : G \to G'$ is an *inertia-preserving isomorphism* if $\varphi(G_0) = G_0'$.

**Theorem 2.** *Let $L_a, L_{a'} \in \mathcal{L}(e, f)$. Then the following are equivalent*:

(i) $L_a \sim L_{a'}$;
(ii) *There exists an inertia-preserving isomorphism $\varphi : G \to G'$ such that $\varphi(H) = H'$.*
(iii) *There exists an isomorphism $\varphi : G \to G'$ such that $\varphi(H) = H'$.*

**Proof.** (i) ⇒ (ii). Assume that $L_a \sim L_{a'}$, and let $k, s$ be such that

$$a' + s\,\frac{q-1}{p-1} \equiv ka \pmod{e}. \tag{9}$$

Then

$$\bar{a}' + s\,\frac{\bar{q}-1}{p-1} \equiv k\bar{a} \pmod{e}$$

and $\varphi = \varphi_{\bar{L}_{\bar{a}},\bar{L}_{\bar{a}'},(k,s)} : G \to G'$, defined as in Lemma 2, is an inertia-preserving isomorphism. Moreover,

$$\varphi(\sigma^{-a}\tau^f) = \sigma'^{-ka+s\frac{q-1}{p-1}}\tau'^f = \sigma'^{-a'}\tau'^f$$

and hence $\varphi(H) = H'$.

(ii) ⇒ (iii) is trivial.

(iii) ⇒ (i). Let $\varphi : G \to G'$ be an isomorphism such that $\varphi(H) = H'$ and let

$$\mathcal{H} = \left\langle \bigcup_{\lambda\in G} \lambda H \lambda^{-1} \right\rangle \qquad \text{and} \qquad \mathcal{H}' = \left\langle \bigcup_{\lambda\in G'} \lambda H' \lambda^{-1} \right\rangle.$$

Clearly $\mathcal{H}$ (resp. $\mathcal{H}'$) is the smallest normal subgroup of $G$ (resp. $G'$) containing $H$ (resp. $H'$), and hence $\underline{L}_a$ (resp. $\underline{L}_{a'}$) is just the subfield of $\bar{L}_{\bar{a}}$ (resp. $\bar{L}_{\bar{a}'}$) fixed by $\mathcal{H}$ (resp. $\mathcal{H}'$). Moreover, $\varphi(\mathcal{H}) = \mathcal{H}'$, and therefore the isomorphism $\varphi$ induces an isomorphism $\tilde{\varphi} : G/\mathcal{H} \to G'/\mathcal{H}'$. Now, $G/\mathcal{H}$ and $G'/\mathcal{H}'$ are the Galois groups of $\underline{L}_a$ and $\underline{L}_{a'}$, respectively, and, by Theorem 1, (i) follows. □

**Remark 3.** Let $L_a, L_{a'} \in \mathcal{L}(e, f)$ be such that $L_a \not\sim L_{a'}$ but $\bar{L}_{\bar{a}} \sim \bar{L}_{\bar{a}'}$ (see Remark 2).

Applying Theorem 2 to $\bar{L}_{\bar{a}}$ and $\bar{L}_{\bar{a}'}$, we obtain that there exists an inertia-preserving isomorphism between $G$ and $G'$. On the other hand, applying Theorem 2 to $L_a$ and $L_{a'}$, we get that no isomorphism $\varphi : G \to G'$ satisfies $\varphi(H) = H'$.

## 4. Equivalence in the general case

We generalize the definition of equivalence to generic $m$-tuples of tamely ramified local fields. Let $m > 0$ and, for $\mu = 1, \dots, m$, let $L_{a_\mu}, L_{a'_\mu} \in \mathcal{L}(e_\mu, f_\mu)$. For the sake of simplicity, we shall often omit the reference to the ramification index and the inertial degree of such fields. We shall let also $\pi_\mu = \pi_{a_\mu, e_\mu, f_\mu}$, $\pi'_\mu = \pi_{a'_\mu, e_\mu, f_\mu}$, $q_\mu = p^{f_\mu}$ and $e = [e_1, \dots, e_m] := lcm\{e_1, \dots, e_m\}$.

**Definition 3.** We say that $(L_{a_1}, \dots, L_{a_m})$ is *equivalent* to $(L_{a'_1}, \dots, L_{a'_m})$, and we write $(L_{a_1}, \dots, L_{a_m}) \sim (L_{a'_1}, \dots, L_{a'_m})$, if there exist integers $k, s, i_1, \dots, i_m$ with $(k, e) = 1$ such that

$$a'_\mu + s\,\frac{q_\mu - 1}{p - 1} \equiv k p^{i_\mu} a_\mu \,(\mathrm{mod}\,(e_\mu, q_\mu - 1)) \quad \text{for } \mu = 1, \dots, m. \tag{10}$$

We note that, if $L_{a'_\mu}$ is a conjugate of $L_{a_\mu}$ for $\mu = 1, \dots, m$, then $(L_{a_1}, \dots, L_{a_m}) \sim (L_{a'_1}, \dots, L_{a'_m})$. In fact, $L_{a_\mu}$ is conjugate to $L_{a'_\mu}$ if and only if $a'_\mu \equiv p^{i_\mu} a_\mu\,(\mathrm{mod}(e_\mu, q_\mu - 1)$ (see Remark 1), which is a special case of (10) with $k = 1$ and $s = 0$.

**Definition 4.** We say that $(L_{a_1}, \dots, L_{a_m})$ is *strongly equivalent* to $(L_{a'_1}, \dots, L_{a'_m})$, and we write $(L_{a_1}, \dots, L_{a_m}) \approx (L_{a'_1}, \dots, L_{a'_m})$ if there exist integers $k, s$ with $(k, e) = 1$ such that

$$a'_\mu + s\,\frac{q_\mu - 1}{p - 1} \equiv k a_\mu \,(\mathrm{mod}\, e_\mu) \quad \text{for } \mu = 1, \dots, m, \tag{11}$$

or, equivalently, if there exist integers $k, s, t_1, \dots, t_m$ with $(k, e) = 1$ such that

$$a'_\mu + s\,\frac{q_\mu - 1}{p - 1} + t_\mu e_\mu = k a_\mu \quad \text{for } \mu = 1, \dots, m. \tag{12}$$

We observe that the preceding definitions in the case of a single field reduce to Definition 1. Moreover,

$$(L_{a_1}, \dots, L_{a_m}) \sim (L_{a'_1}, \dots, L_{a'_m}) \Longrightarrow L_{a_\mu} \sim L_{a'_\mu} \quad \text{for } \mu = 1, \dots, m.$$

In fact, one can see the strong equivalence of two $m$-tuples as a 'coherent' equivalence between corresponding fields, where 'coherent' means that in Eq. (12) $k$ and $s$ can be chosen independent of $\mu$.

The basic relations between equivalence and strong equivalence are the following.

**Proposition 4.** *Let $L_{a_1}, \dots, L_{a_m}, L_{a'_1}, \dots, L_{a'_m}$ be finite tamely ramified extensions of $\mathbb{Q}_p$. Then $(L_{a_1}, \dots, L_{a_m}) \sim (L_{a'_1}, \dots, L_{a'_m})$ if and only if there exist fields $L_{a^*_1}, \dots, L_{a^*_m}$, conjugate to $L_{a_1}, \dots, L_{a_m}$, respectively, such that $(L_{a^*_1}, \dots, L_{a^*_m}) \approx (L_{a'_1}, \dots, L_{a'_m})$. In particular, for normal fields equivalence and strong equivalence coincide.*

**Proof.** Suppose $(L_{a_1}, \dots, L_{a_m}) \sim (L_{a'_1}, \dots, L_{a'_m})$. Since $(e_\mu, k(q_\mu - 1)) = (e_\mu, q_\mu - 1)$, we may rewrite (10) in the form

$$a'_\mu + s\,\frac{q_\mu - 1}{p - 1} + t_\mu e_\mu = kp^{i_\mu} a_\mu + kj_\mu(q_\mu - 1) \quad \text{for } \mu = 1, \dots, m$$

for suitable integers $t_\mu$, $j_\mu$. Choosing $a^*_\mu = p^{i_\mu} a_\mu + j_\mu(q_\mu - 1)$, we obtain that $L_{a^*_\mu}$ is conjugate to $L_{a_\mu}$ (see Remark 1) and $(L_{a^*_1}, \dots, L_{a^*_m}) \approx (L_{a'_1}, \dots, L_{a'_m})$.

The converse is trivial, since strong equivalence implies equivalence and this is stable under conjugation. □

**Proposition 5.** *If $(L_{a_1}, \dots, L_{a_m}) \sim (L_{a'_1}, \dots, L_{a'_m})$, then the m-tuples of their normal kernels and the m-tuples of their normal closures are strongly equivalent.*

**Proof.** In view of Proposition 4, we may assume that $(L_{a_1}, \dots, L_{a_m}) \approx (L_{a'_1}, \dots, L_{a'_m})$ and that (12) holds. Let $\varepsilon_\mu$ be the ramification index of the normal kernels $\underline{L}_{a_\mu}$ and $\underline{L}_{a'_\mu}$. Substituting $e_\mu = \varepsilon_\mu \delta_\mu$ in Eq. (12) and taking into account Proposition 2, we obtain $(\underline{L}_{a_1}, \dots, \underline{L}_{a_m}) \sim (\underline{L}_{a'_1}, \dots, \underline{L}_{a'_m})$. The statement about the normal closures can be shown by multiplying (12) by $\frac{\bar{q}_\mu - 1}{q_\mu - 1}$. □

**Remark 4.** Let $N$ be the compositum of normal closures $\bar{L}_{\bar{a}_1}, \dots, \bar{L}_{\bar{a}_m}$ of $L_{a_1}, \dots, L_{a_m}$ (the same as the normal closure of the compositum $L_{a_1} \cdots L_{a_m}$). Let $e$ and $f$ be the ramification index and the inertial degree of $N$, respectively. Clearly, $\tilde{e} = [e_1, \dots, e_m] | e$ and $\tilde{f} = [\bar{f}_1, \dots, \bar{f}_m] | f$.

We claim that in fact $e = \tilde{e}$. Let $\tilde{q} = p^{\tilde{f}}$ and $\tilde{\zeta} = \zeta_{\tilde{q}-1}$. Setting $\tilde{a}_\mu = \frac{\tilde{q}-1}{q_\mu - 1} a_\mu$, we have $\pi_\mu = \zeta_{e(\tilde{q}-1)}^{\tilde{a}_\mu} \pi_{0,e_\mu} = \tilde{\zeta}^{\frac{\tilde{a}_\mu}{\tilde{e}}} \pi_{0,e_\mu}$ (where $\tilde{\zeta}^{\frac{x}{y}}$ denotes the image in $\bar{\mathbb{Q}}_p$ of $\exp(\frac{2\pi i x}{(\tilde{q}-1)y})$).

Moreover, fix once and for all integers $\alpha_1, \dots, \alpha_m$ such that

$$\alpha_1 \frac{\tilde{e}}{e_1} + \cdots + \alpha_m \frac{\tilde{e}}{e_m} = 1. \tag{13}$$

Then $\pi = \pi_1^{\alpha_1} \cdots \pi_m^{\alpha_m} \in N$ and verifies $\pi = \zeta_{e(\tilde{q}-1)}^{\tilde{b}} \pi_{0,\tilde{e}} = \tilde{\zeta}^{\frac{\tilde{b}}{\tilde{e}}} \pi_{0,\tilde{e}}$ where

$$\tilde{b} = \tilde{a}_1 \alpha_1 \frac{\tilde{e}}{e_1} + \cdots + \tilde{a}_m \alpha_m \frac{\tilde{e}}{e_m}.$$

Moreover, by Abhyankar's lemma (see [5, Chapter 5, Corollary 4]), $N = \mathbb{Q}_p(\tilde{\zeta}, \pi_1, \ldots, \pi_m)$ is unramified over $\mathbb{Q}_p(\pi)$, proving the claim.

Concerning the value of $f$, we observe that, for each $\mu = 1, \ldots, m$, we have $\pi_\mu = \tilde{\zeta}^{\frac{\tilde{a}_\mu - \tilde{b}}{e_\mu}} \pi^{\frac{e}{e_\mu}}$, and therefore $N = \mathbb{Q}_p(\tilde{\zeta}, \tilde{\zeta}^{\frac{\tilde{a}_1 - \tilde{b}}{e_1}}, \ldots, \tilde{\zeta}^{\frac{\tilde{a}_m - \tilde{b}}{e_m}}, \pi)$. Hence

$$f = [\mathbb{Q}_p(\tilde{\zeta}, \tilde{\zeta}^{\frac{\tilde{a}_1 - \tilde{b}}{e_1}}, \ldots, \tilde{\zeta}^{\frac{\tilde{a}_m - \tilde{b}}{e_m}}) : \mathbb{Q}_p].$$

If $q = p^f$ and $b = \frac{q-1}{\tilde{q}-1}\tilde{b}$, then $N = L_b \in \mathcal{L}(e, f)$ and $\pi = \pi_{b,e,f}$.

**Lemma 4.** *Let $L_{a_1}, \ldots, L_{a_m}, L_{a'_1}, \ldots, L_{a'_m}$ be finite tame extensions of $\mathbb{Q}_p$ and let $N = \bar{L}_{\bar{a}_1} \cdots \bar{L}_{\bar{a}_m}$, $N' = \bar{L}_{\bar{a}'_1} \cdots \bar{L}_{\bar{a}'_m}$.*

*Assume $(L_{a_1}, \ldots, L_{a_m}) \sim (L_{a'_1}, \ldots, L_{a'_m})$. If $N \in \mathcal{L}(e, f)$ and $N' \in \mathcal{L}(e', f')$, then $(e, f) = (e', f')$ and $N \sim N'$.*

*Assume $(L_{a_1}, \ldots, L_{a_m}) \approx (L_{a'_1}, \ldots, L_{a'_m})$ and let $k, s, t_1 \ldots, t_m$ be such that* (12) *holds. Then, in the notation of Remark* 4, *$N = L_b$ and $N' = L_{b'}$ with $b' + s\frac{q-1}{p-1} + te = kb$, where $q = p^f$, and*

$$t = \alpha_1 \frac{q-1}{q_1 - 1} t_1 + \cdots + \alpha_m \frac{q-1}{q_m - 1} t_m.$$

**Proof.** First we observe that replacing the fields $L_{a_\mu}$ by any of their conjugates does not change the normal closure, hence, by Proposition 4, we may assume throughout that $(L_{a_1}, \ldots, L_{a_m}) \approx (L_{a'_1}, \ldots, L_{a'_m})$ and that (12) holds.

We have trivially $e = e'$ and $\tilde{f} = \tilde{f}'$. To show that $f = f'$ is equivalent to show that the maximal unramified subextensions of $N$ and $N'$ coincide, namely that $\mathbb{Q}_p(\tilde{\zeta}, \tilde{\zeta}^{\frac{\tilde{a}_1 - \tilde{b}}{e_1}}, \ldots, \tilde{\zeta}^{\frac{\tilde{a}_m - \tilde{b}}{e_m}}) = \mathbb{Q}_p(\tilde{\zeta}, \tilde{\zeta}^{\frac{\tilde{a}'_1 - \tilde{b}'}{e_1}}, \ldots, \tilde{\zeta}^{\frac{\tilde{a}'_m - \tilde{b}'}{e_m}})$. Multiplying (12) by $\frac{\tilde{q}-1}{q_\mu - 1}$, we get

$$\tilde{a}'_\mu + s\frac{\tilde{q}-1}{p-1} + \frac{\tilde{q}-1}{q_\mu - 1} t_\mu e_\mu = k\tilde{a}_\mu. \tag{14}$$

Multiplying (14) by $\alpha_\mu \frac{e}{e_\mu}$ and summing over $\mu$, we obtain

$$\tilde{b}' + s\frac{\tilde{q}-1}{p-1} + \sum_{\mu=1}^{m} \alpha_\mu \frac{\tilde{q}-1}{q_\mu - 1} t_\mu e = k\tilde{b}. \tag{15}$$

From (14) and (15), it follows that $\tilde{a}'_\mu - \tilde{b}' \equiv k(\tilde{a}_\mu - \tilde{b}) \pmod{e_\mu}$. Hence, for $1 \leqslant \mu \leqslant m$, the fields generated by $\tilde{\zeta}^{\frac{\tilde{a}_\mu - \tilde{b}}{e_\mu}}$ and $\tilde{\zeta}^{\frac{\tilde{a}'_\mu - \tilde{b}'}{e_\mu}}$ over $\mathbb{Q}_p(\tilde{\zeta})$ are the same.

Finally, the relation between $b$ and $b'$ is obtained multiplying (15) by $\frac{q-1}{\tilde{q}-1}$. □

With the notation of Lemma 4, let $G = \mathrm{Gal}(N/\mathbb{Q}_p)$, $G' = \mathrm{Gal}(N'/\mathbb{Q}_p)$. Further, for $1 \leqslant \mu \leqslant m$, let $H_\mu$ (resp. $H'_\mu$) be the subgroup of $G$ (resp. $G'$) which fixes $L_{a_\mu}$ (resp. $L_{a'_\mu}$).

**Theorem 3.** *Let $L_{a_1}, \ldots, L_{a_m}, L_{a'_1}, \ldots, L_{a'_m}$ be finite extensions of $\mathbb{Q}_p$. Then the following are equivalent*:

(i) $(L_{a_1}, \ldots, L_{a_m}) \sim (L_{a'_1}, \ldots, L_{a'_m})$;

(ii) *there exists an inertia-preserving isomorphism $\varphi : G \to G'$ such that $\varphi(H_\mu)$ is conjugate to $H'_\mu$ for $1 \leqslant \mu \leqslant m$.*

**Proof.** We start by showing that, if $(L_{a_1}, \ldots, L_{a_m}) \approx (L_{a'_1}, \ldots, L_{a'_m})$, then there exists an inertia-preserving isomorphism $\varphi : G \to G'$ such that $\varphi(H_\mu) = H'_\mu$ for $1 \leqslant \mu \leqslant m$.

Assume $(L_{a_1}, \ldots, L_{a_m}) \approx (L_{a'_1}, \ldots, L_{a'_m})$, and let $k, s, t_1, \ldots, t_m$ as in (12). By Lemma 4 we have $N = L_b \sim N' = L_{b'}$ and, by the proof of Theorem 2, we have that $\varphi = \varphi_{L_b, L_{b'}, (k,s)} : G \to G'$ is an inertia-preserving isomorphism. Recalling that now $\sigma = \lambda_b^{0,1}, \tau = \lambda_b^{1,0}$, an easy computation shows that

$$H_\mu = \langle \sigma^{e_\mu}, \sigma^{-a_\mu}\tau^{f_\mu} \rangle = \{\sigma^{je_\mu - \frac{q_\mu^i - 1}{q_\mu - 1}a_\mu}\tau^{if_\mu}\} \tag{16}$$

and similar expressions hold for $H'_\mu$. It is now straightforward to check that

$$\varphi(\sigma^{e_\mu}) = (\sigma')^{ke_\mu}, \qquad \varphi(\sigma^{-a_\mu}\tau^{f_\mu}) = (\sigma')^{-ka_\mu + s\frac{q_\mu - 1}{p-1}}(\tau')^{f_\mu} = (\sigma')^{-a'_\mu - t_\mu e_\mu}(\tau')^{f_\mu}$$

and hence $\varphi(H_\mu) = H'_\mu$.

Suppose now that $(L_{a_1}, \ldots, L_{a_m}) \sim (L_{a'_1}, \ldots, L_{a'_m})$. By Proposition 4, there exist fields $L_{a^*_\mu}$ conjugate to the $L_{a_\mu}$ such that $(L_{a^*_1}, \ldots, L_{a^*_m}) \approx (L_{a'_1}, \ldots, L_{a'_m})$. Since $L_{a^*_\mu}$ is conjugate to $L_{a_\mu}$, the normal closure of the compositum of all $L_{a^*_\mu}$ is again $N$. Moreover, the subgroup $H^*_\mu$ of $G$ fixing $L_{a^*_\mu}$ is conjugate to $H_\mu$. By the argument above, there exists an inertia-preserving isomorphism $\varphi : G \to G'$ such that $\varphi(H^*_\mu) = H'_\mu$ and, since $H_\mu$ and $H^*_\mu$ are conjugate, $\varphi(H_\mu)$ and $H'_\mu$ are conjugate too.

Conversely, let $\varphi : G \to G'$ be an inertia-preserving isomorphism such that $\varphi(H_\mu)$ is conjugate to $H'_\mu$ for $1 \leqslant \mu \leqslant m$. Then, for each $\mu$, there exists a conjugate $H^*_\mu$ of $H_\mu$ in $G$ such that $\varphi(H^*_\mu) = H'_\mu$. If $L_{a^*_\mu}$ denotes the fixed field of $H^*_\mu$, we have that $L_{a^*_\mu}$ is conjugate to $L_{a_\mu}$; since $(L_{a^*_1}, \ldots, L_{a^*_m}) \sim (L_{a_1}, \ldots, L_{a_m})$, it is enough to show that $(L_{a_1}, \ldots, L_{a_m}) \sim (L_{a'_1}, \ldots, L_{a'_m})$ under the stronger hypothesis that the isomorphism $\varphi$ satisfies $\varphi(H_\mu) = H'_\mu$.

Let $\varphi : G \to G'$ be such an isomorphism. Then $\varphi(\sigma) = \sigma'^k$ and $\varphi(\tau) = \sigma'^s\tau'^l$ for suitable integers $k, s, l$ satisfying certain conditions; in particular, $(k, e) = 1$, $(l, f) = 1$

and $p^l \equiv p \pmod e$. Possibly replacing $l$ with another integer in the same congruence class modulo $f$, we can also suppose that $(l, q-1) = 1$. By hypothesis, we have

$$\varphi(\sigma^{-a_\mu}\tau^{f_\mu}) = (\sigma')^{-ka_\mu + s\frac{q_\mu^l - 1}{p^l-1}}(\tau')^{lf_\mu} \in H'_\mu \tag{17}$$

for $1 \leqslant \mu \leqslant m$. By (16), considering the exponent of $\tau'$, (17) implies that for each $\mu$ there exists $j_\mu$ such that $-ka_\mu + s\frac{q_\mu^l-1}{p^l-1} \equiv j_\mu e_\mu - \frac{q_\mu^l-1}{q_\mu-1}a'_\mu \pmod e$. Since $e_\mu | e$, this gives

$$\frac{q_\mu^l - 1}{q_\mu - 1}a'_\mu + s\,\frac{q_\mu^l - 1}{p^l - 1} \equiv ka_\mu \pmod{e_\mu}.$$

Now, from $\frac{q_\mu^l-1}{q_\mu-1} = q_\mu^{l-1} + q_\mu^{l-2} + \cdots + 1 \equiv l \pmod{(q_\mu - 1)}$ and $p^l \equiv p \pmod e$ we obtain

$$la'_\mu + s\,\frac{q_\mu - 1}{p - 1} \equiv ka_\mu \pmod{(e_\mu, q_\mu - 1)}. \tag{18}$$

Finally, since $e|q-1$, $q_\mu - 1 \,|\, q-1$ and $(l, q-1) = 1$, multiplying (18) by the inverse of $l$ modulo $q-1$ we get that $(L_{a_1}, \ldots, L_{a_m})$ and $(L_{a'_1}, \ldots, L_{a'_m})$ are equivalent. □

We observe that, if there exists an inertia-preserving isomorphism $\varphi : G \to G'$ such that $\varphi(H_\mu)$ is conjugate to $H'_\mu$, then there exists also an isomorphism of the special kind $\varphi_{L_b, L_{b'}, (k,s)} : G \to G'$ with the same properties. In fact, by Theorem 3 condition (ii) implies $(L_{a_1}, \ldots, L_{a_m}) \sim (L_{a'_1}, \ldots, L_{a'_m})$. Let $k, s$ be integers satisfying Eq. (10); then there exist conjugates $L_{a^*_\mu}$ of the $L_{a_\mu}$ such that $(L_{a^*_1}, \ldots, L_{a^*_m}) \approx (L_{a'_1}, \ldots, L_{a'_m})$ and the same integers $k, s$ satisfy Eq. (11). By the proof of Theorem 3 the isomorphism $\varphi_{L_b, L_{b'}, (k,s)}$ has the required properties.

**Remark 5.** Unlike the case where $m = 1$ (see Theorem 2), when $m > 1$ the condition that there exists an *inertia-preserving* isomorphism $\varphi : G \to G'$ cannot be relaxed. In fact, it is possible that there exist isomorphisms between $G$ and $G'$ such that $\varphi(H_\mu)$ is conjugate to $H'_\mu$ for all $\mu$ but none of them is inertia-preserving.

To see an example, consider the case where $p = 11$, $e = 5$, $f = 1$. It is straightforward to check that $(L_1, L_2, L_3) \not\sim (L_1, L_2, L_4)$ (see Proposition 6 below), and therefore there is no inertia-preserving isomorphism between $G$ and $G'$ sending $H_\mu$ into a conjugate of $H'_\mu$ for all $\mu$.

On the other hand, with the notation of Theorem 3, we have that $N = N'$: in fact, both fields are obtained as the splitting field of the polynomial $X^5 - 11$ over the unique unramified extension $F$ of $\mathbb{Q}_{11}$ of degree 5 (see Remark 4). We have $G = G' = \langle \sigma, \tau \,|\, \sigma^5 = \tau^5 = 1, \sigma\tau = \tau\sigma\rangle \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, and $H_\mu = \langle \sigma^{-\mu}\tau\rangle$ for

$\mu = 0, 1, 2, 3, 4$. The isomorphism $\varphi : G \to G'$ given by $\varphi(\sigma^{-i}\tau^j) = \sigma^{2i+2j}\tau^i$ satisfies $\varphi(H_1) = H_1$, $\varphi(H_2) = H_2$, and $\varphi(H_3) = H_4$.

## 5. Arithmetical conditions for the equivalence

In some cases, the condition in Definition 3 for the equivalence of $m$-tuples of fields can be translated into a relatively simple arithmetical condition on the numbers $a_\mu$, $a'_\mu$, $e_\mu$, $f_\mu$. We give an explicit condition for totally ramified extensions.

**Proposition 6.** *Let $L_{a_1}, \ldots, L_{a_m}, L_{a'_1}, \ldots, L_{a'_m}$ be totally and tamely ramified extensions of $\mathbb{Q}_p$, and let $e = [e_1, \ldots, e_m]$ where $e_\mu$ denotes the ramification index of $L_{a_\mu}$ and $L_{a'_\mu}$. Then $(L_{a_1}, \ldots, L_{a_m}) \sim (L_{a'_1}, \ldots, L_{a'_m})$ if and only if there exists an integer $k$ such that $(k, e) = 1$ and*

$$a'_\mu - a'_\nu \equiv k(a_\mu - a_\nu) \pmod{(e_\mu, e_\nu, p-1)} \qquad \text{for } 1 \leqslant \mu < \nu \leqslant m. \tag{19}$$

**Proof.** If $(L_{a_1}, \ldots, L_{a_m}) \sim (L_{a'_1}, \ldots, L_{a'_m})$, then, taking the difference of Eq. (10) corresponding to the indices $\mu$ and $\nu$, we obtain

$$a'_\mu - a'_\nu \equiv k(a_\mu - a_\nu) \pmod{(e_\mu, e_\nu, p-1)}. \tag{20}$$

Conversely, assume (19). Then $ka_\mu - a'_\mu \equiv ka_\nu - a'_\nu \pmod{(e_\mu, e_\nu, p-1)}$. By the Chinese Remainder Theorem, there exists an integer $s$ such that $ka_\mu - a'_\mu \equiv s \pmod{(e_\mu, p-1)}$ for all $1 \leqslant \mu \leqslant m$, that is, $(L_{a_1}, \ldots, L_{a_m}) \sim (L_{a'_1}, \ldots, L_{a'_m})$. □

**Corollary 1.** *With the notation of Proposition 6, we have $(L_{a_1}, \ldots, L_{a_m}) \sim (L_{a'_1}, \ldots, L_{a'_m})$ if and only if $(\underline{L}_{a_1}, \ldots, \underline{L}_{a_m}) \approx (\underline{L}_{a'_1}, \ldots, \underline{L}_{a'_m})$.*

**Proof.** Assume that $(\underline{L}_{a_1}, \ldots, \underline{L}_{a_m}) \approx (\underline{L}_{a'_1}, \ldots, \underline{L}_{a'_m})$. Then there exists an integer $k$ such that

$$a'_\mu - a'_\nu \equiv k(a_\mu - a_\nu) \pmod{(\varepsilon_\mu, \varepsilon_\nu, p-1)} \qquad \text{for } 1 \leqslant \mu < \nu \leqslant m. \tag{21}$$

By Proposition 2, we have $\varepsilon_\mu = (p-1, e_\mu, a_\mu(p-1))$. Substituting the values of $\varepsilon_\mu$ and $\varepsilon_\nu$ into (21), we get (19). Since $k$ is coprime to $\varepsilon = [\varepsilon_1, \ldots, \varepsilon_m]$, in the class of $k$ modulo $\varepsilon$ we can find a representative which is also coprime to $\varepsilon$. The converse implication has already been proved in Proposition 5. □

**Remark 6.** In Corollary 1, the condition that $L_{a_1}, \ldots, L_{a_m}, L_{a'_1}, \ldots, L_{a'_m}$ are totally ramified extensions of $\mathbb{Q}_p$ is indeed a necessary one.

In fact, let $p = 17$, $m = 2$, $e_1 = e_2 = 9$, $f_1 = f_2 = 2$, and consider the pairs in $\mathcal{L}(9, 2)$ given by $(L_1, L_4)$, $(L_2, L_2)$. By (6), we have $L_1 \sim L_2$, since $(18, 9, 1) = (18, 9, 2) = 1$ and, similarly, $L_4 \sim L_2$, since $(18, 9, 4) = (18, 9, 2) = 1$. Moreover, by

Proposition 2, all fields $\underline{L}_1$, $\underline{L}_2$ and $\underline{L}_4$ are equal to the unique unramified extension of $\mathbb{Q}_{17}$ of degree 2, whence clearly $(\underline{L}_1, \underline{L}_4) \sim (\underline{L}_2, \underline{L}_2)$.

On the other hand, $(L_1, L_4) \not\sim (L_2, L_2)$. In fact, by Definition 3, the condition $(L_1, L_4) \sim (L_2, L_2)$ is equivalent to the solvability in the integers $s, k, i_1, i_2$, with $(k, 9) = 1$, of the system

$$\begin{cases} 2 + 18s \equiv 17^{i_1} k \pmod{(9, 17^2 - 1)}, \\ 2 + 18s \equiv 17^{i_2} \cdot 4k \pmod{(9, 17^2 - 1)}. \end{cases}$$

Now, the first equation implies $k \equiv \pm 2 \pmod 9$, while the second equation implies $k \equiv \pm 5 \pmod 9$, and hence the system is not solvable.

## 6. Invariance of the index under equivalence

Let $\alpha, \beta \in \bar{\mathbb{Q}}_p$ be integral elements and denote by $F_\alpha$ and $F_\beta$ their minimal polynomials over $\mathbb{Z}_p[X]$. We let disc$(\alpha)$ be the discriminant of $F_\alpha$, Res$(\alpha, \beta)$ be the resultant of $F_\alpha$ and $F_\beta$ and $\mathrm{ind}(\alpha) = [\mathcal{O}_{\mathbb{Q}_p(\alpha)} : \mathbb{Z}_p[\alpha]]$. Finally, we put $\mathrm{disc}_p(\alpha) = |\mathrm{disc}(\alpha)|$, $\mathrm{ind}_p(\alpha) = |\mathrm{ind}(\alpha)|$ and $\mathrm{Res}_p(\alpha, \beta) = |\mathrm{Res}(F_\alpha, F_\beta)|$.

**Definition 5.** Let $X = \{x_1, \ldots, x_n\}$ be a finite subset of integral elements of $\bar{\mathbb{Q}}_p$, we define

$$I_p(X) = \left\{ \sum_{1 \leqslant i < j \leqslant n} \mathrm{Res}_p(x_i, x_j) + \sum_{i=1}^{n} \mathrm{ind}_p(x_i) \right\}. \tag{22}$$

Let $\mathcal{E}$ be the free abelian monoid generated by the finite extensions $E$ of $\mathbb{Q}_p$ in $\bar{\mathbb{Q}}_p$. For $E_1 + \cdots + E_m \in \mathcal{E}$, we define

$$I_p(E_1 + \cdots + E_m) = \min_{x_i \in E_i} I_p(\{x_1, \ldots, x_m\}). \tag{23}$$

It is immediate to verify that the minimum in (23) depends only on the isomorphism classes of the $E_i$. Hence we have the following:

**Proposition 7.** *Let $E_1, \ldots, E_m, E_1^*, \ldots, E_m^*$ be local fields such that $E_\mu^*$ is a conjugate of $E_\mu$ for $\mu = 1, \ldots, m$. Then*

$$I_p(E_1 + \cdots + E_m) = I_p(E_1^* + \cdots + E_m^*).$$

Now let $K$ be a number field, and let $E_1, \ldots, E_m$ be the completions of $K$ at the primes over $p$. Then $K \otimes \mathbb{Q}_p \cong E_1 \oplus \cdots \oplus E_m$ (see [1, Theorem, p. 57]), and we associate to $K$ the element

$$E_p(K) = E_1 + \cdots + E_m \in \mathcal{E}.$$

With this notation we have [6, Theorem 1]:

**Proposition 8** (*Nart*). *For every number field $K$,*

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

We can now state our main result on the index of finite $\mathbb{Q}_p$-algebras.

**Theorem 4.** *Let $E_1, \ldots, E_m, E'_1, \ldots, E'_m$ be tamely ramified local fields. If $(E_1, \ldots, E_m) \sim (E'_1, \ldots, E'_m)$ then, for all $n_1, \ldots, n_m \in \mathbb{N}$,*

$$I_p(n_1E_1 + \cdots + n_mE_m) = I_p(n_1E'_1 + \cdots + n_mE'_m).$$

We remark that in the statement of the preceding theorem the numbers $n_i$ need not necessarily be the multiplicities of the fields $E_i$ (resp. $E'_i$) in the sum $n_1E_1 + \cdots + n_mE_m$ (resp. $n_1E'_1 + \cdots + n_mE'_m$). In fact, the theorem can be applied, for instance, in the case where $(E_1, E_2) \sim (E'_1, E'_2)$, $E_1 = E_2$ but $E'_1 \neq E'_2$. Actually, it is enough to prove the theorem in the case $n_1 = \cdots = n_m = 1$.

We need the following lemma.

**Lemma 5.** *Assume $(E_1, \ldots, E_m) \approx (E'_1, \ldots, E'_m)$ and let $k, s, t_1, \ldots, t_m$ be such that* (12) *holds. For $1 \leqslant \mu, v \leqslant m$, let $\lambda_\mu \in \Sigma_{E_\mu}$, $\lambda_v \in \Sigma_{E_v}$ and $\alpha_\mu \in \mathcal{O}_{E_\mu}$, $\alpha_v \in \mathcal{O}_{E_v}$. Moreover, for $\mu = 1, \ldots, m$, let $\varphi_\mu = \varphi_{E_\mu, E'_\mu, (k,s)}$ and $\psi_\mu = \psi_{E_\mu, E'_\mu, (k,t_\mu)}$ be the maps defined in Lemmas* 1 *and* 2. *Then*

$$|\lambda_\mu(\alpha_\mu) - \lambda_v(\alpha_v)| = |\varphi_\mu(\lambda_\mu)(\psi_\mu(\alpha_\mu)) - \varphi_v(\lambda_v)(\psi_v(\alpha_v))|. \tag{24}$$

**Proof.** Let $N = L_b$ and $N' = L_{b'}$ be the normal closures of $E_1 \cdots E_m$ and of $E'_1 \cdots E'_m$, respectively. Then, by Lemma 4, $N \sim N'$ and $b' + s\frac{q-1}{p-1} + te = kb$, where

$$t = \alpha_1 \frac{q-1}{q_1 - 1} t_1 + \cdots + \alpha_m \frac{q-1}{q_m - 1} t_m$$

and $\alpha_1, \ldots, \alpha_m$ satisfy (13). Let $\varphi = \varphi_{N,N',(k,s)}$ and $\psi = \psi_{N,N',(k,t)}$: by Lemmas 3 and 4, we have

$$|\lambda^{(1)}(\alpha^{(1)}) - \lambda^{(2)}(\alpha^{(2)})| = |\varphi(\lambda^{(1)})(\psi(\alpha^{(1)})) - \varphi(\lambda^{(2)})(\psi(\alpha^{(2)}))| \tag{25}$$

for all $\lambda^{(1)}, \lambda^{(2)} \in \mathrm{Gal}(N/\mathbb{Q}_p)$ and for all $\alpha^{(1)}, \alpha^{(2)} \in \mathcal{O}_N$.

We have to show that, when we chose $\alpha^{(1)} = \alpha_\mu \in E_\mu$ and $\alpha^{(2)} = \alpha_\nu \in E_\nu$, (25) specializes to (24). First we show that the restriction of the map $\psi$ to $E_\mu$ coincides with $\psi_\mu$ for all $\mu$. Let $\zeta = \zeta_{q-1}$ and $\tilde{\zeta} = \zeta_{\tilde{q}-1}$ as in Remark 4. On one hand, for any root of unity $\omega \in N$ we have $\psi(\omega\pi^h) = \omega^h \zeta^{th} \pi'^h$. On the other hand, from (14) and (15) we get

$$k(\tilde{a}_\mu - \tilde{b}) - (\tilde{a}'_\mu - b') = t_\mu \frac{\tilde{q}-1}{q_\mu - 1} e_\mu - te \frac{\tilde{q}-1}{q-1},$$

so that

$$\tilde{\zeta}^{k\frac{\tilde{a}_\mu - \tilde{b}}{e_\mu}} \tilde{\zeta}^{-\frac{\tilde{a}'_\mu - \tilde{b}'}{e_\mu}} = \tilde{\zeta}^{t_\mu \frac{\tilde{q}-1}{q_\mu - 1} - t\frac{e}{e_\mu}\frac{\tilde{q}-1}{q-1}} = \zeta_{q_\mu - 1}^{t_\mu} \zeta^{-t\frac{e}{e_\mu}}.$$

Hence, recalling that $\pi_\mu = \tilde{\zeta}^{\frac{\tilde{a}_\mu - \tilde{b}}{e_\mu}} \pi^{\frac{e}{e_\mu}}$, we can evaluate $\psi$ on $\zeta_{q_\mu - 1}^x \pi_\mu^h$ as follows:

$$\begin{aligned}\psi(\zeta_{q_\mu-1}^x \pi_\mu^h) &= \psi(\zeta_{q_\mu-1}^x \tilde{\zeta}^{h\frac{\tilde{a}_\mu - \tilde{b}}{e_\mu}} \pi^{h\frac{e}{e_\mu}}) = \zeta_{q_\mu-1}^{kx} \tilde{\zeta}^{kh\frac{\tilde{a}_\mu - \tilde{b}}{e_\mu}} \zeta^{th\frac{e}{e_\mu}} (\pi')^{h\frac{e}{e_\mu}} \\ &= \zeta_{q_\mu-1}^{kx} \tilde{\zeta}^{kh\frac{\tilde{a}_\mu - \tilde{b}}{e_\mu}} \zeta^{th\frac{e}{e_\mu}} \tilde{\zeta}^{-h\frac{\tilde{a}'_\mu - \tilde{b}'}{e_\mu}} (\pi'_\mu)^h = \zeta_{q_\mu-1}^{kx + t_\mu h} (\pi'_\mu)^h.\end{aligned}$$

A similar argument shows that $\lambda_{\tilde{b}}^{ij}\big|_{E_\mu} = \lambda_{a_\mu}^{ij}$, whence $\varphi(\lambda_{\tilde{b}}^{ij}\big|_{E_\mu}) = \varphi_\mu(\lambda_{a_\mu}^{ij})$ for each $\mu$ and (24) follows. □

**Proof of Theorem 4.** By Proposition 5 there exist fields $E_1^*, \dots, E_m^*$ conjugate to $E_1, \dots, E_m$, respectively, such that $(E_1^*, \dots, E_m^*) \approx (E'_1, \dots, E'_m)$. Since the index $I_p(n_1 E_1^* + \dots + n_m E_m^*)$ depends only on the absolute values $|\lambda_\mu^*(\alpha_\mu^*) - \lambda_\nu^*(\alpha_\nu^*)|$, where $\lambda_\mu^*$ are embeddings of $E_\mu^*$ in $\bar{\mathbb{Q}}_p$ and $\alpha_\mu^*$ are elements of $E_\mu^*$, by Lemma 5 we have

$$I_p(n_1 E_1^* + \dots + n_m E_m^*) = I_p(n_1 E'_1 + \dots + n_m E'_m).$$

But $E_\mu^*$ is a conjugate of $E_\mu$ for $\mu = 1, \dots, m$, and, by Proposition 7, the theorem follows. □

The preceding local results can be reinterpreted in terms of global fields. Let $p$ be a rational prime, and $K$, $K'$ be number fields tamely ramified at $p$.

**Definition 6.** We say that $K$ and $K'$ are *locally equivalent at* $p$, $K \sim_p K'$, if $K \otimes \mathbb{Q}_p \cong E_1 \oplus \dots \oplus E_m$, $K' \otimes \mathbb{Q}_p \cong E'_1 \oplus \dots \oplus E'_m$ and, up to a permutation of the $E_\mu$, we have $(E_1, \dots, E_m) \sim (E'_1, \dots, E'_m)$.

Clearly, if $K \sim_p K'$ then the form of the factorizations of $p$ in $K$ and $K'$ is the same; if, moreover, $p$ is unramified, then also the converse holds.

**Corollary 2.** *Let $K$ and $K'$ be number fields, and let $p$ be a prime tamely ramified both in $K$ and in $K'$. Assume $K \sim_p K'$. Then* $\mathrm{ind}_p(K) = \mathrm{ind}_p(K')$.

**Proof.** The statement follows immediately from Proposition 8 and Theorem 4. □

We now characterize local equivalence at $p$ in terms of some suitable Galois groups. Denote by $P_1, \ldots, P_m$ the primes of $K$ lying over $p$. Also, let $\bar{K}$ be the normal closure of $K$ and let $Q_1, \ldots, Q_s$ be the primes of $\bar{K}$ over $p$. Trivially, all completions of $\bar{K}$ at the primes $Q_j$ coincide and, if $N$ is any such completion, we have $\bar{K} \otimes \mathbb{Q}_p \cong N^s$, and hence $E_p(\bar{K}) = sN$. We recall without proof the following simple characterization of $N$.

**Lemma 6.** *If $N$ is the completion of $\bar{K}$ at any of the primes $Q_j$ and $E_1, \ldots, E_m$ are the completions of $K$ at the primes $P_1, \ldots, P_m$, respectively, then*

$$N = \bar{E}_1 \cdot \ldots \cdot \bar{E}_m,$$

*where, as usual, $\bar{E}_i$ denotes the normal closure of $E_i$.*

For $j = 1, \ldots, s$, let $D(Q_j|p)$ be the decomposition group of the prime $Q_j$ over $p$, and let $D = D(Q_1|p)$. It is known that all $D(Q_j|p)$ are isomorphic to $D$ via conjugation in $\mathrm{Gal}(\bar{K}/\mathbb{Q})$; let $g_j : D(Q_j|p) \to D$ be any such isomorphism. Whenever $P_\mu \subseteq Q_j$, we have that $g_j(D(Q_j|P_\mu))$ is independent of $j$, hence we may define $D_\mu = g_j(D(Q_j|P_\mu))$ for any $j$ such that $P_\mu \subseteq Q_j$. We shall also denote by $I$ the inertial group of $Q_1$ over $p$. Finally, we shall use an analogous notation with the superscript $'$ for the field $K'$.

**Proposition 9.** *Let $K$ and $K'$ be number fields tamely ramified at $p$. Then the following are equivalent*:

(a) $K \sim_p K'$;
(b) *there exists an isomorphism $\varphi : D \to D'$ such that*
  (i) $\varphi(I) = I'$;
  (ii) *up to a permutation of the $D_\mu$, $\varphi(D_\mu)$ is a conjugate of $D'_\mu$ for $\mu = 1, \ldots, m$.*

**Proof.** There is a canonical isomorphism $\iota : D \to G = \mathrm{Gal}(N/\mathbb{Q}_p)$ (see for instance [1, Chapter 1.10, Proposition 3]). Also, $\iota(D_\mu) = H_\mu = \mathrm{Gal}(N/E_\mu)$ for all $\mu$. Letting $\iota'$ be the analogous isomorphism between $D'$ and $G' = \mathrm{Gal}(N'/\mathbb{Q}_p)$, we obtain that there exists an isomorphism $\varphi : D \to D'$ if and only if there exists an isomorphism $\tilde{\varphi} = \iota' \circ \varphi \circ \iota^{-1} : G \to G'$. Now, condition (i) expresses the property that the isomorphism $\varphi$ is inertia-preserving and condition (ii) is equivalent to the fact that, up to a permutation, $\tilde{\varphi}(H_\mu)$ is conjugate to $H'_\mu$ for all $\mu$. Hence Theorem 3 applies. □

## 7. A counterexample

Let $p = 5$, $e = 4$ and $f = 1$, so $\mathcal{L}(4,1) = \{L_0, L_1, L_2, L_3\}$. By Proposition 6, $(L_0, L_1) \not\sim (L_0, L_2)$. We want to show that $I_5(56L_0 + 55L_1) \neq I_5(56L_0 + 55L_2)$, whence Theorem 4 fails to be true in the case of $m$-tuples of non-equivalent fields, even if, as in this case, all fields involved are pairwise equivalent.

Let $\pi_a = \pi_{a,4,1} = \zeta_{16}^a \sqrt[4]{5}$ for $a = 0, 1, 2$. We remark that $\mathbb{Q}_5(\pi_0^2) \cap \mathbb{Q}_5(\pi_1^2) = \mathbb{Q}_5$, while $\mathbb{Q}_5(\pi_0^2) \cap \mathbb{Q}_5(\pi_2^2) = \mathbb{Q}_5(\sqrt{5})$. We shall see that this difference is the key for understanding why the two indices are not equal.

We now outline our procedure for proving that $I_5(56L_0 + 55L_1) \neq I_5(56L_0 + 55L_2)$, leaving to the reader all the lenghty calculations involved.

Let $I_5(56L_0 + 55L_1) = I(\Omega \cup \Theta)$, $I_5(56L_0 + 55L_2) = I(\Omega' \cup \Theta')$, where $\Omega, \Omega' \in \mathcal{O}_{L_0}{}^{56}$, $\Theta \in \mathcal{O}_{L_1}{}^{55}$, $\Theta' \in \mathcal{O}_{L_2}{}^{55}$. We write $\Omega = \cup_{i=0}^{4} \Omega_i$, where $\Omega_i$ is the subset of $\Omega$ consisting of the elements congruent to $i$ modulo $\pi_0$, and we partition the sets $\Omega', \Theta, \Theta'$ similarly.

Although this is not obvious 'a priori' (and even not true in the general case), a direct computation allows to check that the elements of $\Omega$ must be evenly distributed in the classes modulo $\pi_0$; namely, up to a permutation of $\{0, 1, 2, 3, 4\}$, we must have $|\Omega_0| = |\Omega_0'| = 12$ and $|\Omega_i| = |\Omega_i'| = 11$ for $i \neq 0$. Similarly, $|\Theta_i| = |\Theta_i'| = 11$ for all $i$.

Now, the resultant between two elements belonging to different classes modulo the maximal ideal has valuation 0, and therefore

$$\begin{aligned} I_5(\Omega \cup \Theta) &= I_5(\Omega_0 \cup \Theta_0) + \cdots + I_5(\Omega_4 \cup \Theta_4), \\ I_5(\Omega' \cup \Theta') &= I_5(\Omega_0' \cup \Theta_0') + \cdots + I_5(\Omega_4' \cup \Theta_4'). \end{aligned}$$

For $i \neq 0$, again a direct computation shows that the mininum value of $I_5(\Omega_i \cup \Theta_i)$ is 1032, and this value can be obtained when both $\Omega_i$ and $\Theta_i$ contain 10 elements of order 1 (i.e. with valuation $\frac{1}{4}$) and one element of order 2 (i.e. with valuation $\frac{1}{2}$).

For $i = 0$ the situation is different. Concerning $I_5(\Omega_0 \cup \Theta_0)$, the minimum value is 1130, and is obtained by choosing 2 elements of $\Omega_0$ and one element of $\Theta_0$ of order 2 and all the other elements of order 1. It is important to observe that the contribution to the index given by the resultants between the three elements of order 2 is $3 \times 8 = 24$ and therefore is as small as possible (choose for instance $\alpha \equiv \sqrt{5} \pmod{\pi_0^3}$, $\beta \equiv \zeta_4\sqrt{5} \pmod{\pi_0^3}$, $\gamma \equiv \zeta_8\sqrt{5} \pmod{\pi_1^3}$).

The same kind of choice made for $\Omega_0' \cup \Theta_0'$ would produce a larger value: in fact, since $\pi_2^2 = \zeta_4\sqrt{5}$, for any choice of three elements of order 2, two in $L_0$ and one in $L_2$, there exists at least one pair $(x, y)$ for which $\mathrm{Res}_5(x, y) \geqslant 10$, and consequently the index of any sequence $\Omega_2^* \cup \Theta_2^* \subset L_0 \cup L_2$ including three such elements is at least 1132.

Actually, the index $I_5(\Omega_0' \cup \Theta_0')$ is 1131, and is obtained by choosing 10 elements of order 1 and one element of order 2 in both $L_0$ and $L_2$ plus one element of order

3 in $L_0$. Summing up all terms we get

$$I_5(56L_0 + 55L_1) = 5258 \quad \text{and} \quad I_5(56L_0 + 55L_2) = 5259.$$

**Remark 7.** Let $E$ be a normal extension of $\mathbb{Q}_p$, $m > n$ be natural mumbers, and $\Omega_n$ be a sequence in $E$ such that $I_p(nE) = I_p(\Omega_n)$. In [2] we showed that we can enlarge $\Omega_n$ to a sequence $\Omega_m$ such that $I_p(mE) = I_p(\Omega_m)$. This property is no longer true for general indices of the type $I_p(n_1E_1 + \cdots + n_mE_m)$. In fact, set $I_5(55L_1) = I_5(\Theta'')$. Following the algorithm described in [2], one can check that $\Theta''$ must contain exactly 44 elements of order zero, 9 elements of order 1 and 2 elements of order 2. It follows that $\Theta \not\supset \Theta''$, and therefore the sequence $\Omega \cup \Theta$ cannot be found by just enlarging $\Theta''$.

## References

[1] J.W.S. Cassels, A. Fröhlich (Eds.), Algebraic Number Theory, Academic Press, New York, 1967.

[2] I. Del Corso, R. Dvornicich, On Ore's conjecture and its developments, Trans. Amer. Math. Soc., to appear.

[3] I. Del Corso, R. Dvornicich, Number fields with the same index, Acta Arith. 102 (2002) 323–337.

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

[5] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, second ed., Springer, Berlin, 1990.

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