JOURNAL OF NUMBER THEORY 52, 7–16 (1995)

Some Numerical Invariants Related to Central Embedding Problems

NGUYEN QUANG DO THONG

Université de Franche-Comté, Laboratoire de Mathématiques, Route de Gray, F-25030 Besancon Cedex, France

AND

HANS OPOLKA

TU Braunschweig, Institut für Algebra und Zahlentheorie, Pockelsstrasse 14, D-W-3300 Braunschweig, Germany

Communicated by Alan C. Woods

Received May 20, 1992; revised June 4, 1993

For every central embedding problem three numerical invariants which give information about its solvability are defined. Furthermore, in the number field case universal estimates for these invariants are given.

1. THE REDUCTION INDEX, THE GENUS INDEX, AND THE EMBEDDING INDEX OF A CENTRAL EMBEDDING PROBLEM

Let $\mathcal{G}$ be a profinite group, let p be a prime number and for every natural number n put $C_n := (1/p^n)\,\mathbb{Z}_p/\mathbb{Z}_p$. Let G be a finite quotient group of $\mathcal{G}$ which acts trivially on C_n and for a cocycle class $(\varepsilon) \in H^2(G, C_n)$ denote by $G(\varepsilon)$ the central group extension of G with kernel C_n which corresponds to ε. The central embedding problem $E_n = E(G, C_n, \varepsilon)$ for $\mathcal{G}$ corresponding to G, C_n and ε is said to be solvable if there is a homomorphism $\phi: \mathcal{G} \to G(\varepsilon)$ such that ϕ composed with the natural projection $G(\varepsilon) \to G$ is the given epimorphism $\mathcal{G} \to G$; every such ϕ is called a solution of E_n. Let J be another quotient group of $\mathcal{G}$ and let $(c) \in H^2(J, C_n)$. The central embedding problem $E(J, C_n, c)$ for $\mathcal{G}$ is said to be a cyclic reduction of $E(G, C_n, \varepsilon)$ if J is cyclic and if $\inf(\varepsilon) = \inf(c)$ in $H^2(\mathcal{G}, C_n)$. So $E(G, C_n, \varepsilon)$ is solvable if and only if $E(J, C_n, C)$ is solvable, see (1.3). The reduction index of the central embedding problem $E_n = E(G, C_n, \varepsilon)$ for $\mathcal{G}$ is the smallest natural number $r = r_n(G)$—if it exists—such that E_n has a cyclic reduction $E(J, C_n, c)$ with the property $|J| \leqq p^r$; if such a natural

0022-314X/95 $6.00

number r does not exist then the reduction index is said to be infinite. The genus index of $E_n = E(G, C_n, \varepsilon)$ is the smallest natural number $s = s_n(G)$—if it exists—such that the central embedding problem $E_n^s := E(G, C_{n+s}, \varepsilon_s)$ for $\mathscr{G}$, where (ε_s) is the image of (ε) under the homomorphism

$$j_{n,n+s}: H^2(G, C_n) \to H^2(G, C_{n+s})$$

induced by the canonical injection $C_n \hookrightarrow C_{n+s}$ is solvable; if such a natural number does not exist then the genus index of E_n is said to be infinite. The embedding index of $E(G, C_n, \varepsilon)$ is the smallest natural number $t = t_n(G)$ such that the embedding problem $E(G, C_n, p^t \cdot \varepsilon)$ is solvable. Obviously, $t_n(G)$ exists and is always $\leqq n$.

(1.1) PROPOSITION. *Assume that $H^2(\mathscr{G}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$; then the reduction index $r_n(G)$ and the genus index $s_n(G)$ of every central embedding problem $E_n = E(G, C_n, \varepsilon)$ for $\mathscr{G}$ exist, i.e., are finite, and are equal. The embedding index $t_n(G)$ satisfies $t_n(G) \leqq r_n(G)$.*

Proof of (1.1). The exact sequence

$$0 \longrightarrow C_n \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p^n} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$

yields the exact sequence of cohomology groups

$$\cdots \longrightarrow \operatorname{Hom}(\mathscr{G}, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\delta} H^2(\mathscr{G}, C_n) \longrightarrow H^2(\mathscr{G}, \mathbb{Q}_p/\mathbb{Z}_p) = 0.$$

Hence there is a homomorphism $\chi: \mathscr{G} \to \mathbb{Q}_p/\mathbb{Z}_p$ such that the image of $(\varepsilon) \in H^2(G, C_n)$ under the inflation map $\inf: H^2(G, C_n) \to H^2(\mathscr{G}, C_n)$ satisfies

$$\inf((\varepsilon)) = (\delta\chi). \tag{1.2}$$

Put $J := \mathscr{G}/\ker(\chi)$. Then by construction $(\delta\chi)$ is the image of some element $(c) \in H^2(J, C_n)$ under the inflation map $\inf: H^2(J, C_n) \to H^2(\mathscr{G}, C_n)$:

$$\inf((\varepsilon)) = (\delta\chi) = \inf((c)).$$

This equation implies the existence of the reduction index $r < \infty$ of E_n, in view of the following well known criterium [H], 1.1.

(1.3) PROPOSITION. *A central embedding problem $E_n = E(G, C_n, \varepsilon)$ for $\mathscr{G}$ is solvable if and only if (ε) belongs to the kernel of the inflation map* $\inf: H^2(G, C_n) \to H^2(\mathscr{G}, C_n)$.

Now put $m := n + r$ and consider the exact sequence

$$0 \longrightarrow C_n \longrightarrow C_m \xrightarrow{p^n} C_r \longrightarrow 0$$

which induces the following commutative diagram with exact rows

$$\begin{array}{ccccc} \cdots \longrightarrow \mathrm{Hom}(\mathcal{G}, C_r) & \xrightarrow{\delta} & H^2(\mathcal{G}, C_n) & \longrightarrow & H^2(\mathcal{G}, C_m) \\ \uparrow{\scriptstyle \mathrm{inf}} & & \uparrow{\scriptstyle \mathrm{inf}} & & \uparrow{\scriptstyle \mathrm{inf}} \\ \cdots \longrightarrow \mathrm{Hom}(G, C_r) & \xrightarrow{\delta} & H^2(G, C_n) & \longrightarrow & H^2(G, C_m). \end{array} \tag{1.4}$$

Then the inflation of (ε) in $H^2(\mathcal{G}, C_n)$ is in the image of δ, hence the image (ε_r) of (ε) in $H^2(G, C_m)$ becomes trivial under the inflation map $H^2(G, C_m) \to H^2(\mathcal{G}, C_m)$, and therefore by (1.3) the embedding problem $E'_n = E(G, C_m, \varepsilon_r)$ is solvable. Conversely, using again (1.3) and the diagram (1.4), we see that if E'_n is solvable then the inflation of (ε) in $H^2(\mathcal{G}, C_n)$ is in the image of δ:

$$\mathrm{inf}((\varepsilon)) = (\delta\chi) \qquad \text{for some} \quad \chi \in \mathrm{Hom}(\mathcal{G}, C_r). \tag{1.5}$$

Altogether this shows that the reduction index r is equal to the genus index s of E_n. Finally, it follows from the equation (1.5) that the inflation of $(p^r \cdot \varepsilon)$ in $H^2(\mathcal{G}, C_n)$ is trivial, hence by (1.3) the embedding problem $E(G, C_n, p^r \cdot \varepsilon)$ is solvable. Therefore the embedding index t of $E(G, C_n, \varepsilon)$ satisfies $t \leq r$.

Remarks. (a) The genus index occurs already—in different terminology—in [O] and [MO].

(b) $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p)$ is the Pontrjagin dual of the p-part of the Schur multiplicator of the profinite group $\mathcal{G}$.

2. On the p-Triviality of the Schur Multiplicator

We now examine the case of a number field k. We fix an algebraic closure $\bar{k}$ of k, and for any subextension K/k of $\bar{k}/k$, we denote by $G_K = G(\bar{k}/K)$ the absolute Galois group of K. Let p be a prime. Denote by μ_n the G_k-module of all roots of unity in $\bar{k}$ of order dividing p^n, $\mu_\infty = \bigcup_{n \geq 1} \mu_n$, and for any K contained in $\bar{k}$, $\mu(K) = \mu_\infty \cap K$. Finally, let $S_p = S_p(k)$ be the set of all places of k dividing p, $S_\infty = S_\infty(k)$ the set of all archimedian places of k, and $\sum = \sum(k) = S_p \cup S_\infty$; let $S = S(k)$ be any set (finite or not) of places of k containing Σ. We will consider central embedding problems for the Galois group $G_k(S)$ of the maximal algebraic extension k_S of k which is unramified outside S (in short: S-ramified).

First, we review some conditions for the triviality of $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p)$. For convenience, we will always suppose that we are in the non-exceptional case, i.e. the extension $k_\infty = k(\mu_\infty)$ is pro-cyclic over k. The following result is well known:

(2.1) PROPOSITION. *Let S be any finite set of places of k containing Σ. Then the triviality of $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p)$ is equivalent to the validity of Leopoldt's conjecture for k and p.*

See e.g. [HA], 4.4.

For any set of places S of k containing Σ and K in $\bar{k}$, let $\mathcal{O}_S(K)$ be the ring of S-integers of K, $\mathrm{Cl}_S(K)$ the ideal class group of $\mathcal{O}_S(K)$, $A_S(K)$ the p-rimary part of $\mathrm{Cl}_S(K)$. Then we have:

(2.2) LEMMA. *Let S be any set of places of k containing Σ. Then the triviality of $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p)$ is equivalent to the finiteness of the group of co-invariants $A_S(k_\infty)(-1)_\Gamma$, where $\Gamma = G(k_\infty/k)$ and $(\ldots)(-1)$ denotes the "Tate twist."*

Again, this is more or less known for finite $S \supset \Sigma$. For arbitrary $S \supset \Sigma$, we will use theorems of Galois cohomology which are usually proved only for finite S; a star (*) behind the references will then mean that the relevant results are easily extended to $S \supset \Sigma$.

Proof of (2.2). For any $\mathbb{Z}_p$-module M on which $G_k(S)$ acts, denote by $M(n)$ the nth "Tate twist." In the non-expectional case, $cd_p\,\Gamma \leqq 1$, and Hochschild-Serre's spectral sequence boils down to the exact sequence:

$$0 \to H^1(\Gamma, H^1(k_S/k_\infty, \mathbb{Q}_p/\mathbb{Z}_p(n))) \to H^2(k_S/k, \mathbb{Q}_p/\mathbb{Z}_p(n))$$
$$\to H^2(k_S/k_\infty, \mathbb{Q}_p/\mathbb{Z}_p)(n) \to 0.$$

But $H^2(k_S/k_\infty, \mathbb{Q}_p/\mathbb{Z}_p)(1) = H^2(k_S/k_\infty, \mu_\infty)$ is the p-part of the Brauer group of $\mathcal{O}_S(k_\infty)$, and this is trivial because the degree of k_∞/k is divisible by p (this is a consequence of functorial properties of Brauer groups; see [S], 4.7*). So $H^2(k_S/k, \mathbb{Q}_p/\mathbb{Z}_p(n)) \cong H^1(\Gamma, H^1(k_S/k_\infty, \mathbb{Q}_p/\mathbb{Z}_p(n))$ for any $n \in \mathbb{Z}$. Now consider the twisted Kummer exact sequence:

$$0 \to \mathcal{O}_S(k_\infty)^* \otimes \mathbb{Q}_p/\mathbb{Z}_p(-1) \to H^1(k_S/k_\infty, \mathbb{Q}_p/\mathbb{Z}_p) \to A_S(k_\infty)(-1) \to 0.$$

Tate's lemma ([S, 2.8]) shows that $H^1(\Gamma, \mathcal{O}_S(k_\infty)^* \otimes \mathbb{Q}_p/\mathbb{Z}_p(-1)) = 0$. Combining this with $\mathrm{cd}_p\,\Gamma \leqq 1$, we get $H^1(\Gamma, H^1(k_S/k_\infty, \mathbb{Q}_p/\mathbb{Z}_p)) \cong H^1(\Gamma, A_S(k_\infty)(-1))$. Since Γ is pro-cyclic $H^1(\Gamma, M) = M_\Gamma$. To end the proof, just note that $cd_p(G_k(S)) \leqq 2$ ([HA], 2.27), so $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p)$ is divisible.

As easy consequences of the above lemma, we get (always in the non-exceptional case):

(2.3). Leopoldt's conjecture for k and p implies the triviality of $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p)$ for any $S \supset \Sigma$ (because $A_S(k_\infty)$ is a quotient of $A_\Sigma(k_\infty)$).

(2.4). $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p) = 0$ if $A_S(k_\infty)$ is finite. This happens, e.g.,

(a) if $S = \{$all places of $k\}$, i.e., $G_k(S) = G_k$ (in this case $A_S(k_\infty) = (0)$)

(b) more generally, if $S(k)$ is of density one (again, $A_S(k_\infty) = (0)$)

(c) if the Iwasawa invariants λ_S and μ_S attached to $A_S(k_\infty)$ are trivial (cases of triviality of λ_Σ and μ_Σ can be found in [F]).

In order to get further information, we must use global-local techniques. For any place v of k, we denote by k_v the completion of k at v, and by G_{k_v} the absolute Galois group of k_v, identified with the decomposition subgroup of some extension of v to $\bar{k}$. For any discrete torsion $G_k(S)$-module M whose order is an S-unit we have localization maps

$$H^i(G_k(S), M) \to \prod_{v \in S}{}' H^i(G_{k_v}, M),$$

where $\prod'$ denotes the topological restricted product ([HA], 1.2). Let us denote by $\mathrm{Ker}^i_S(M)$ or $\mathrm{Ker}^i_S(M, k)$ the kernels of these localization maps. Then Poitou–Tate's duality ([HA], 1.3) says that

(2.5). If M is finite, the kernels $\mathrm{Ker}^i_S(M)$ are finite, and there is a canonical perfect pairing

$$\mathrm{Ker}^1_S(M) \times \mathrm{Ker}^2_S(\mathrm{Hom}(M, k_S^*)) \to \mathbb{Q}/\mathbb{Z}.$$

We will use this to prove:

(2.6) Proposition. *For any $S \supset \Sigma$ the following statements are equivalent:*

(i) $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p) = 0$

(ii) *the orders of the kernels $\mathrm{Ker}^2_S(C_n)$ are bounded for all $n \geqq 1$*

(iii) *the sequence $\mathrm{Ker}^2_S(C_n)$ stabilizes.*

Proof. It is known that the local groups $H^2(G_{k_v}, \mathbb{Q}_p/\mathbb{Z}_p)$ are trivial ([S, 3.2]) so that $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p) = 0$ if and only if $\varinjlim \mathrm{Ker}^2_S(C_n) = 0$ (or is finite). If the groups $\mathrm{Ker}^2_S(C_n)$ are bounded, then $\varinjlim \mathrm{Ker}^2_S(C_n)$ is evidently finite. To show the converse, let us first characterize $\mathrm{Ker}^2_S(C_n)$ as a module of Galois descent

(2.7) Lemma. *For $n \geqq 1$, put $k_n = k(\mu_n)$ and $G_n = G(k_n/k)$. Then class field theory and the corestriction map induce isomorphisms*

$$(A_S(k_n)/p^n)(-1)_{G_n} \simeq \mathrm{Ker}^2_S(C_n, k_n)_{G_n} \simeq \mathrm{Ker}^2_S(C_n, k)$$

Proof. By Poitou–Tate's duality, it is the same to consider the map induced by restriction: $\mathrm{Ker}^1_S(\mu_n, k) \to \mathrm{Ker}^1_S(\mu_n, k_n)^{G_n}$. The well known G_n-cohomological triviality of μ_n (for details, see [NK, 4.8]) then shows that this map is an isomorphism. Moreover, since k_n contains μ_n, Kummer theory and class field theory give an isomorphism $\mathrm{Ker}^1_S(\mu_n, k_n) \simeq \mathrm{Hom}(A_S(k_n), \mu_n)$. This proves the lemma.

Suppose now that $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p) = 0$. We want to bound $(A_S(k_n)/p^n)(-1)_{G_n}$ or, more crudely, $A_S(k_n)(-1)_{G_n}$. As $G(k_\infty/k_n)$ acts trivially on $A_S(k_n)(-1)$, we have $A_S(k_n)(-1)_{G_n} = A_S(k_n)(-1)_\Gamma$. A theorem of Iwasawa ([I, 5.3.12*]) asserts that the kernels of the natural maps $A_S(k_n) \to A_S(k_\infty)$ are bounded. To bound the $A_S(k_n)(-1)_\Gamma$, it is then already sufficient (by the snake lemma) to show that $A_S(k_\infty)(-1)^\Gamma$ and $A_S(k_\infty)(-1)_\Gamma$ are finite. Since we are in the non-exceptional case, standard reduction arguments allow us to suppose that k contains μ_1. Let us consider the module $\mathrm{Hom}(A_S(k_\infty)(-1), \mathbb{Q}_p/\mathbb{Z}_p)$ over the Iwasawa algebra $\Lambda = Z_p[[\Gamma]]$: this is a Λ-torsion module ([I, 4.3.8*]), and the structure theorem then shows that $A_S(k_\infty)(-1)^\Gamma$ is finite if and only if $A_S(k_\infty)(-1)_\Gamma$ is finite. But this last property is true by hypothesis and Lemma (2.2). In order to show the last equivalence of proposition (2.6), remark that by Lemma (2.7), for $m \geqq n$, corestriction induces a map

$$\mathrm{Ker}^2_S(C_m) \simeq (A_S(k_m)/p^m)(-1)_{G_m} \to \mathrm{Ker}^2_S(C_n) \simeq (A_S(k_n)/p^n)(-1)_{G_n}.$$

But for $n >> 0$, no prime above p splits in k_∞/k_n, ([I, 6.2]), hence the norm map $A_S(k_m) \to A_S(k_n)$ is surjective, and so is the above map.

(2.8) *Remark.* By the above considerations, it is easily seen that $\varprojlim \mathrm{Ker}^1_S(\mu_n)$ injects into $\mathrm{Ker}^1_S(\mu_\infty)$. For S finite, the two groups are equal, but in general these are not equal if S is infinite. It is known that $\mathrm{Ker}^1_S(\mu_\infty)$ is independent of $S \supset \Sigma$, and it is finite if and only if Leopoldt's conjecture holds for k and p (see [S, NG]). This gives another proof for (2.3), as well as a bound for $\varprojlim \mathrm{Ker}^1_S(\mu_n)$ (see (3.2) below).

3. A Universal Bound for the Genus Index

We maintain the hypotheses and notations of Section 2. In particular, we suppose that we are in the non-exceptional case. Central embedding problems $E_n = E(G, C_n, \varepsilon)$ for $G_k(S)$ will also be denoted by $E(K/k, C_n, \varepsilon)$, with $G(K/k) = G$. The main result is

(3.1) Theorem. *Let S be any set of places of k containing Σ, T a finite subset of S. Assume that $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Then there is a natural* *integer $g = g(k, T, S)$, depending only on k, T, S and on a choice of a basis of $H^2(G_k(T \cup \Sigma), \mathbb{Q}_p/\mathbb{Z}_p)$, such that g is an upper bound for the genus index —hence, according to (1.1), also for the reduction index and the embedding index—of every central embedding problem $E_n = E(K/k, C_n, \varepsilon)$ for $G_k(S)$ such that K/k is T-ramified.*

Proof. We proceed in three steps:

(1) Changing notations if necessary, we may suppose that T contains Σ. In the nonexceptional case, $\mathrm{cd}_p G_k(T) \leqq 2$ and it is known ([S, NG]) that $H^2(G_k(T), \mathbb{Q}_p/\mathbb{Z}_p)$ is divisible of rank d (=the defect of Leopoldt's conjecture). Choose a basis $\{\theta_1, ..., \theta_i, ..., \theta_d\}$ of $H^2(G_k(T), \mathbb{Q}_p/\mathbb{Z}_p)$. For all $n \leqq m = n + s$, we have commutative diagrams with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C_n & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{p^n} & \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & 0 \\
 & & \cap\downarrow & & \Vert & & \downarrow p^s & & \\
0 & \longrightarrow & C_m & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{p^m} & \mathbb{Q}_p/\mathbf{Z}_p & \longrightarrow & 0
\end{array}$$

and

$$\begin{array}{ccccccc}
\xrightarrow{p^n} & H^1(G_k(T), \mathbb{Q}_p/\mathbb{Z}_p) & \xrightarrow{\delta_n} & H^2(G_k(T), C_n) & \longrightarrow & H^2(G_k(T), \mathbb{Q}_p/\mathbb{Z}_p) & \xrightarrow{p^n} \\
 & \downarrow p^s & & \downarrow j_{n,m} & & \Vert & \\
\xrightarrow{p^m} & H^1(G_k(T), \mathbb{Q}_p/\mathbb{Z}_p) & \xrightarrow{\delta_m} & H^2(G_k(T), C_m) & \longrightarrow & H^2(G_k(T), \mathbb{Q}_p/\mathbb{Z}_p) & \xrightarrow{p^m}
\end{array}$$

Since $H^2(G_k(T), \mathbb{Q}_p/\mathbb{Z}_p) = \varinjlim H^2(G_k(T), C_n)$, each θ_i is defined as an inductive system $(\theta_{i,n})$, with $\theta_{i,n} \in H^2(G_k(T), C_n)$ and $j_{n,m}(\theta_{i,n}) = \theta_{i,m}$ for $m \geqq n$. For any fixed m, the images of the $\theta_{i,n}$ in ${}_{p^m}H^2(G_k(T), \mathbb{Q}_p/\mathbb{Z}_p)$ generate the latter group.

(2) Now take inflation from $H^2(G_k(T), C_1)$ to $H^2(G_k(S), C_1)$. By the triviality of $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p)$, we get d characters $\chi_{i,1} \in H^1(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p)$ such that $\delta_1(\chi_{i,1}) = \inf(\theta_{i,1})$ for $1 \leqq i \leqq d$. Construct inductively systems of characters $\{\chi_{i,n}\}_{1 \leqq i \leqq d}$ by putting $\chi_{i,n} = \chi_{i,1}^{p^{n-1}}$. By the above diagrams (replacing T by S), we have $\delta_n(\chi_{i,n}) = \inf(\theta_{i,n})$ for any $1 \leqq i \leqq d$ and any $n \geqq 1$. Let U be the union of T and of the (finite) set of places outside which all characters $\chi_{i,1}$ (hence all $\chi_{i,n}$) are unramified. Now fix n and a class $(\varepsilon) \in H^2(K/k, C_n)$. Since K/k is T-ramified, we first inflate (ε) to a class $(\varepsilon_T) \in H^2(G_k(T), C_n)$ which, by (1), can be written

$$(\varepsilon_T) = \left(\prod_{i=1}^{d} \theta_{i,n}^{a_i} \right) \cdot \delta_n(\chi_T),$$

with $\chi_T \in H^1(G_k(T), \mathbb{Q}_p/\mathbb{Z}_p)$. Inflating then everything to $G_k(S)$, we get a class $(\varepsilon_S) \in H^2(G_k(S), C_n)$ such that $(\varepsilon_S) = \delta_n((\prod_{i=1}^d \chi_{i,n}^{a_i}) \cdot \inf(\chi_T))$. The character $\chi \in H^1(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p)$ which appears inside the parentheses is unramified outside U.

(3) To kill the obstruction (ε_S), we use the standard local-global techniques. Denote by

$$l_n: H^2(G_k(S), C_n) \to \bigoplus_{v \in S} H^2(G_{k_v}, C_n)$$

the localization map, and by $X_k^n(S, U)$ the preimage of $\bigoplus_{v \in U} H(G_{k_v}, C_n)$ under l_n. This s a finite group defined by the exact sequence

$$0 \to \mathrm{Ker}_S^2(C_n) \to X_k^n(S, U) \to \bigoplus_{v \in U} H^2(G_{k_v}, C_n).$$

Since $H^2(k_v^{nr}/k_v, C_n) = 0$, where k_v^{nr} is the maximal unramified extension of k_v, and since χ is unramified outside U, we have $\delta_m(\chi) \in X_k^m(S, U)$ for any $m = n + s$. We now construct the bound $g = g(k, T_S)$. Since $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p) = 0$ the Pontrjagin dual $H^2(G_k(S), C_m)^\wedge$ is canonically isomorphic to the p^m-torsion part of the maximal pro-p-quotient $G_k^{ab}(S) \otimes \mathbb{Z}_p$ of the abelianized group $G_k(S)^{ab}$. Similarly, the Pontrjagin duals $H^2(G_{k_v}, C_m)^\wedge$ are isomorphic to $\mu_m(k_v)$. Define $g = g(k, T, S)$ by

$$p^g = (\max_{v \in U} \#\mu(k_v)) \cdot (\max_{q \geqq 1} \#\mathrm{Ker}_S^2(C_q))$$

Note that the orders of the groups $\mathrm{Ker}_S^2(C_q)$ are bounded, according to proposition (2.6). For $s \leqq g$, p^s clearly kills $X_k^m(S, U)$. The second diagram in (1) then shows $j_{n,m}(\varepsilon_S) = (\delta_m(\chi))^{p^s} = 0$. This means that g is an upper bound for the genus index of E_n for all n.

(3.2) *Particular Cases.* The bound $g(k, T, S)$ defined above can be improved in some cases:

(a) If S is of density 1, Hasse's principle is known to hold, i.e., $\mathrm{Ker}_S^2(C_n) = 0$ for all n (see e.g. [NK, 4.7]). Then we can take $g = g(k, T)$ such that $p^g = \max\{\#\mu(k_v), v \in T\}$.

(b) Assume Leopoldt's conjecture (but S arbitrary). Then, by (2.8), we can take $g = g(k, T)$ such that $p^g = \max\{\#\mu(k_v), v \in T\} \cdot \#\mathrm{Ker}_\Sigma^1(\mu_\infty)$. The case $\mathrm{Ker}_\Sigma^1(\mu_\infty) = 0$ looks particularly interesting, in that it provides a universal bound $g(k, T)$ which depends only on local parameters for $v \in T$.

Examples. (a) Take $p = 3$, $k = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, square-free. Then for $|d| < 200$ and $d \neq -107, 67, 103, 106, 139$, we have $\mathrm{Ker}_\Sigma^1(\mu_\infty) = 0$ (see [HE]).

(b) In general, little is known about fields for which $\mathrm{Ker}^1_\Sigma(\mu_\infty)=0$. In [MN] fields k are studied for which a cruder invariant is trivial: Let $\mathcal{T}_k(\Sigma)$ be the $\mathbb{Z}_p$-torsion submodule of the (finitely generated) $\mathbb{Z}_p$-module $G_k(\Sigma)^{ab}\otimes\mathbb{Z}_p$; then $\mathrm{Ker}^1_\Sigma(\mu_\infty)$ is a quotient of $\mathcal{T}_k(\Sigma)$, and the field k is called p-rational if $\mathcal{T}_k(\Sigma)=0$ (evidently: the maximal pro-p-factor of $G_k(\Sigma)$ is a free pro-p-group). A typical example is $k=\mathbb{Q}(\mu_p)$, p a regular prime. For other examples, see [MN].

(c) Suppose that S is finite (then the hypotheses of (3.1) imply Leopoldt's conjecture). We get a weaker bound if we replace $g(k, T, S)$ by $f=f(k, S)$ such that p^f is the order of the torsion submodule $\mathcal{T}_k(S)$ of $G_k(S)^{ab}\otimes\mathbb{Z}_p$. Recall that $\mathcal{T}_k(S)$ is described by an exact sequence ([NG], 4.2):

$$0\to\mu(k)\to\bigoplus_{v\in S}\mu(k_v)\to\mathcal{T}_k(S)\to\mathrm{Ker}^1_\Sigma(\mu_\infty)\to 0.$$

and $\mathcal{T}_k(S)$ and $\mathcal{T}_k(\Sigma)$ are related by the exact sequence

$$0\to\bigoplus_{v\in S-\Sigma}\mu(k_v)\to\mathcal{T}_k(S)\to\mathcal{T}_k(\Sigma)\to 0.$$

E.g.: Take $p=3$, $k=\mathbb{Q}(\sqrt{d})$. The following examples have been computed by Hémard (see also [HE]):

d	29	43	62	67	82	122	199	257	717	1413
$\#\mathcal{T}_k(\Sigma)$	3^2	3	3	3^2	3	3^4	3	3^3	3^2	3^2

(d) Moreover, suppose that the field k is totally real. Then the genus index bound $f(k, S)$ defined above admists an analytical interpretation. Actually, a classical formula of Coates (see e.g. [NG, 2.1]), giving the order of $\mathcal{T}_k(\Sigma)$ yields here: For $p\neq 2$,

$$p^f=\left(p\text{-part of }\frac{hR}{\sqrt{D}}\prod_{v|p}(1-(Nv)^{-1})\right)\cdot\#\mu(k)^{-1}\cdot\prod_{v\in S-\Sigma}\#\mu(k_v),$$

where h is the class number of k, D the absolute value of the discriminant, R the p-adic regulator, Nv the absolute norm of a prime ideal associated with v.

References

[F] E. Friedman, Iwasawa invariants, *Math. Ann.* **271** (1985), 13–30.
[HA] K. Haberland, "Galois Cohomology of Algebraic Number Fields," Deutscher Verlag der Wissenschaften, Berlin, 1978.
[HE] D. Hémard, Modules galoisiens de torsion et plongements dans les Z_p-extensions, *J. Number Theory* **30** (1988), 357–374.

[H] K. HOECHSMANN, Zum Einbettungsproblem, *JRAM* **229**, (1968), 81–106.

[I] K. IWASAWA, On Z_l-extensions of algebraic number fields, *Ann. Math.* **98** (1973), 246–326.

[MO] K. MIYAKE AND H. OPOLKA, Indices of central embedding problems and applications, *J. Number Theory* **31** (1988), 191–200.

[MN] A. MOVAHHEDI AND T. NGUYEN QUANG DO, Sur l'arithmétique des corps de nombres p-rationnels, "Sém. Th. des Nombres Paris 1987–88," pp. 155–200, Birkhäuser, Basel, 1990.

[NG] T. NGUYEN QUANG DO, Sur la Z_p-torsion de certains modules galoisiens, *Ann. Inst. Fourier* **36 2** (1986), 27–46.

[NK] J. NEUKIRCH, Über das Einbettungsproblem der algebraischen Zahlentheorie, *Invent. Math.* **21** (1973), 59–116.

[O] H. OPOLKA, Cyclotomic splitting fields and strict cohomological dimension, *Israel J. Math.* **52** (1985), 225–230.

[S] P. SCHNEIDER, Über gewisse Galoiskohomologiegruppen, *Math. Z.* **168** (1979), 181–205.