JOURNAL OF ALGEBRA 159, 343–346 (1993)

Cyclic Reduction of Central Embedding Problems

HANS OPOLKA

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

Communicated by Walter Feit

Received October 14, 1991

It is shown that every central embedding problem E for the absolute Galois group $\mathcal{G}$ of a number field has a so-called cyclic reduction E'; this is a central embedding problem for $\mathcal{G}$ with a cyclic quotient group J of $\mathcal{G}$ such that E is solvable if and only if E' is solvable. Some information about the minimal order of J is also provided. © 1993 Academic Press, Inc.

Let $\mathcal{G}$ be a profinite group, let p be a prime number, and for every natural number n put $C_n := (1/p^n)\, Z/Z$. 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 $\mathcal{G}$ 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. Our first result is as follows.

(1) PROPOSITION. *Assume that $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Let $E_n = E(G, C_n, \varepsilon)$ be a central embedding problem for $\mathcal{G}$ as above. Then there is a cyclic quotient group J of $\mathcal{G}$ and some $(c) \in H^2(J, C_n)$ such that the corresponding central embedding problem $E(J, C_n, c)$ for $\mathcal{G}$ is solvable if and only if E_n is solvable. $E(J, C_n, c)$ is called a* cyclic reduction *of E_n.*

Proof. 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

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

0021-8693/93 $5.00

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

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

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

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

This equation implies the assertion, in view of the following criterion [H, 1.1].

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

It is known that $H^2(\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$ if $\mathcal{G}$ is the absolute Galois group of a number field; see, e.g., [S, Sect. 6]. In this case we can estimate the order of J in a cyclic reduction as follows.

(3) THEOREM. *Let k be a number field and let S be a finite set of places of k. Assume that the extension k^∞/k which is generated over k by all roots of unity of p-power order in an algebraic closure of k is cyclic. Then there is a natural number $f = f(k, S)$, depending only on k and S, such that the following holds: Every central embedding problem $E_n = E(G, C_n, \varepsilon)$ for the absolute Galois group of k which is unramified outside S, i.e., the finite Galois extension K/k with Galois group $G = G(K/k)$ is unramified outside S, has a cyclic reduction $E(J, C_n, c)$ with the property $|J| \leqslant p^f$.*

Let k be a field of characteristic 0, let $\bar{k}$ be an algebraic closure and denote by $G_k = G(\bar{k}/k)$ the absolute Galois group of k. Let E_n be a central embedding problem for G_k which corresponds to a finite Galois subextension K/k of $\bar{k}/k$ with Galois group $G = G(K/k)$, to C_n and to some $(\varepsilon) \in H^2(G, C_n)$. Denote by μ_n the G_k-module of all roots of unity in $\bar{k}$ of order dividing p^n. Furthermore, if k is a number field and if v is a place of k we denote by k_v the completion of k at v and by G_{k_v} its absolute Galois group.

Proof of (3). Since we have assumed that k^∞/k is syclic, the localization map

$$H^2(G_k, C_n) \xrightarrow{l_n} \prod_v H^2(G_{k_v}, C_n) \tag{4}$$

is injective for every n; see, e.g., [H, Sect. 6]. For $\tilde{n} \geqslant n$ denote by $j_{n,\tilde{n}}: H^2(-, C_n) \to H^2(-, C_{\tilde{n}})$ the homomorphism which is induced by the canonical injection $C_n \hookrightarrow C_{\tilde{n}}$, $a/p^n \to a \cdot p^{\tilde{n}-n}/p^{\tilde{n}}$. Clearly, $j_{n,\tilde{n}}$ commutes with the inflation map and with the localization map (4). If v is a place of k which is unramified in K/k then the v-local component of $l_n(\inf((\varepsilon)))$ is trivial, because H^2 of the Galois group of the maximal unramified extension of k_v with respect to C_n is trivial. For a place v of k such that $k_v \neq \mathbb{C}$ define

(5) $\quad p^{f_v} := p$-part of the order of the group of roots of unity in k_v

$$f := \max\{f_v \mid \mu_{f_v} \leqslant k_v^*,\ v \in S,\ k_v \neq \mathbb{C}\}$$

$$m := n + f.$$

Then we claim that $(l_m(j_{n,m}(\inf(\varepsilon))))$ is trivial. To see this we apply the local duality theorem [P]. It shows that $H^2(G_{k_v}, C_m)$ is dual to $H^0(G_{k_v}, \mu_m) \cong \mu_m \cap k_v^*$ and that the map $j_{n,m}$ dualizes the map $\mu_m \cap k_v^* \mapsto \mu_n \cap k_v^*$, $x \mapsto x^{p^f}$, which, by the definition of f, is trivial provided $k_v \neq \mathbb{C}$. Since l_m is injective we see that $j_{n,m}(\inf((\varepsilon)))$ is trivial. This implies that $j_{n,m}(\varepsilon)$ is contained in the kernel of the inflation map $H^2(G, C_m) \to H^2(G_k, C_m)$. Consider the following commutative diagram with exact rows—these being induced by the exact sequence $0 \to C_n \to C_m \xrightarrow{p^n} C_f \to 0$:

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & \mathrm{Hom}(G_k, C_f) & \xrightarrow{\delta} & H^2(G_k, C_n) & \xrightarrow{j_{n,m}} & H^2(G_k, C_m) & \longrightarrow \cdots \\
& \uparrow{\scriptstyle \inf} & & \uparrow{\scriptstyle \inf} & & \uparrow{\scriptstyle \inf} & \\
\cdots \longrightarrow & \mathrm{Hom}(G, C_f) & \xrightarrow{\delta} & H^2(G, C_n) & \xrightarrow{j_{n,m}} & H^2(G, C_m) & \longrightarrow \cdots
\end{array}$$

It shows that $\inf((\varepsilon))$ in $H^2(G_k, C_n)$ is the image of some $\chi \in \mathrm{Hom}(G_k, C_f)$ under the coboundary map δ. Put $J := G_k/\mathrm{Ker}(\chi)$. Obviously $|J| \leqslant p^f$, and in view of (2) the equation

$$\inf((\varepsilon)) = (\delta\chi) \tag{6}$$

shows that $E(J, C_n, (\delta\chi))$ is a cyclic reduction of $E(G, C_n, \varepsilon)$.

From Eq. (6) we deduce

(7) COROLLARY. *Under the assumptions of* (3) *we have*: *If* $E_n = E(G, C_n, \varepsilon)$ *is any central embedding problem for* G_k *which is unramified outside S then the central embedding problem* $E(G, C_n, p^f \cdot \varepsilon)$, *where f is the natural number defined under* (5), *is solvable.*

So we may call $f = f(k, S)$ a universal embedding exponent with respect to k, p, and S.

In special cases one can also give information about the ramification set of a cyclic reduction of a central embedding problem; namely we prove

(8) THEOREM. *Let* $k=\mathbb{Q}$ *or* $k=\mathbb{Q}(\mu_{p^j})$ *for some* $j\geq 0$, *where* p *is assumed to be odd and regular. Let* S *be a finite set of places of* k *which contains all places above* p *and* ∞. *Then there is a natural number* $f=f(k, S)$, *depending only on* k *and* S, *such that the following holds: Every central embedding problem* E_n *for* G_k *which is unramified outside* S *has a cyclic reduction* $E(J, C_n, c)$ *which is unramified outside* S *and such that* $|J|\leq p^f$.

Proof of (8). Let f be defined as in (5). Then it was shown in the proof of (3) that the central embedding problem $E_n^m := E(G, C_n, j_{n,m}(\varepsilon))$, $m=n+f$, is solvable. It is solvable as an embedding problem for $G_k(S)$, the Galois group of the maximal subextension of $\bar{k}/k$ which is unramified outside S, if and only if $\inf((j_{n,m}(\varepsilon)))\in H^2(G_k(S), C_m)$ is trivial; see (2). Since E_n^m is solvable the element $\inf((j_{n,m}(\varepsilon)))$ belongs to the kernel of the localization map

$$H^2(G_k(S), C_m)\to \coprod_{v\in S} H^2(G_{k_v}, C_m).$$

This kernel is trivial if the class number of $k(\mu_m)$ is prime to m or if $k=\mathbb{Q}$; see [N, (8.1) ff., (8.2)] and of course [SF]. But these conditions are satisfied by our assumptions and [I].

Question. Let k be a number field, let p be a prime number, and let S be a finite set of places of k which contains all places above p and ∞. Is there a natural number $f=f(k, S)$, depending only on k and S, such that the following holds: If $E_n=E(G, C_n, \varepsilon)$ is a central embedding problem for $G_k(S)$ then $E(G, C_n, \varepsilon^f)$ has a solution which is unramified outside S? Even if one assumes the p-adic Leopoldt conjecture or $H^2(G_k(S), \mathbb{Q}_p/\mathbb{Z}_p)=0$ the answer is not known to me.

REFERENCES

[H] K. HOECHSMANN, Zum Einbettungsproblem, *J. Reine Angew. Math.* **229** (1968), 81–106.

[I] K. IWASAWA, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258.

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

[P] G. POITOU, "Cohomologie Galoisienne des modules finis," Dunod, Paris, 1967.

[S] J. P. SERRE, Modular forms of weight one and Galois representations, *in* "Algebraic Number Fields" (A. Fröhlich, Ed.), pp. 193–268, Academic Press, London, 1977.

[SF] I. R. SHAFAREVIC, Extensions with given ramification points, *Inst. Hautes Études Sci. Publ. Math.* **18** (1964), 295–319; *Amer. Math. Soc. Transl. Ser. 2* **59** (1966), 128–149.