ISRAEL JOURNAL OF MATHEMATICS, Vol. 52, No. 3, 1985

CYCLOTOMIC SPLITTING FIELDS AND STRICT COHOMOLOGICAL DIMENSION

BY

HANS OPOLKA

Mathematisches Institut, Westfälische Wilhelms-Universität Münster, Einsteinstrasse 62, D-4400 Münster, FRG

ABSTRACT

The purpose of this note is to characterize fields of strict cohomological dimension two in terms of Brauer groups.

§1. Introduction

The purpose of this note is to characterize fields of strict cohomological dimension two in terms of Brauer groups, especially in terms of cyclotomic splitting fields of central simple algebras. As an application we obtain a well-known result of Tate on the cohomology of the absolute Galois group of a local or global number field, which is used in various contexts of algebraic number theory.

This approach was presented at the Oberwolfach conference on Brauer groups in January 1984. I am grateful to D. Saltman and J. Sonn for some helpful questions and to the referee for a critical remark.

§2. Embedding problems

Our approach uses the framework of the embedding problem. We recall some basic definitions and facts. Let k be a field, let $\bar{k}$ be a separable algebraic closure of k and for an intermediate field E, $k \subset E \subset \bar{k}$, let $G_E = \mathrm{Gal}(\bar{k}/E)$. We shall consider embedding problems $E(G, A, c)$ over k consisting of a finite Galois extension K/k, $K \subset \bar{k}$, with Galois group $G = \mathrm{Gal}(K/k)$, a finite G-module A of order prime to the characteristic of k, the so-called kernel of the embedding problem, and a cohomology class $(c) \in H^2(G, A)$ representing a group extension

Received April 1, 1984 and in revised form January 1, 1985

$1 \to A \to G(c) \to G \to 1$. The embedding problem $E(G,A,c)$ is called solvable if there is a homomorphism $\psi : G_k \to G(c)$ such that ψ composed with the natural projection $G(c) \to G$ is equal to the natural map $G_k \to G$. From [4], 1.1, we quote

(2.1) *The following conditions are equivalent*:

(i) $E(G,A,c)$ *is solvable*,

(ii) (c) *becomes trivial under the inflation map* $\inf : H^2(G,A) \to H^2(G_k,A)$.

Now we assume that G acts trivially on A, i.e. the corresponding embedding problem $E(G,A,c)$ is central. For any $\chi \in A^* := \mathrm{Hom}(A, \bar{k}^*)$ denote by $k(\chi)$ the field which is generated over k by all values of χ. Then $G_{k(\chi)}$ is the fixed group of χ in G_k under the natural action of G_k on A^* ($\chi^\sigma(a) = (\chi(a))^\sigma$, $\chi \in A^*$, $\sigma \in G_k$, $a \in A$), and χ induces a map on cohomology

$$\bar{\chi} : H^2(G,A) \xrightarrow{\inf} H^2(G_k,A) \xrightarrow{\mathrm{res}} H^2(G_{k(\chi)},A) \xrightarrow{\chi^*} H^2(G_{k(\chi)},\bar{k}^*) \cong \mathrm{Br}(k(\chi)).$$

Hence $\bar{\chi}$ maps (c) to the Brauer group of $k(\chi)$. From [4], 3.8, we quote

(2.2) *If the extension* $k(A^*)$ *which is generated over* k *by all values of all* $\chi \in A^*$ *is cyclic, then* $E(G,A,c)$ *is solvable if and only if the Brauer class* $\chi(c) \in \mathrm{Br}(k(\chi))$ *splits for all* $\chi \in A^*$.

For a natural number m denote by ξ_m a primitive m-th root of unity in $\bar{k}$. From (2.2) we deduce

(2.3) *Let p be a prime number not equal to* $\mathrm{char}(k)$ *and let* $A = \mathbf{Z}/p^n$. *For $p = 2$ assume that* $k(\xi_{2^n})$ *is cyclic. Then* $E(G,A,c)$ *is solvable if and only if* $\chi(c) \in \mathrm{Br}(k(\chi))$ *splits for a generator* $\chi \in A^*$.

Let p be a prime number not equal to $\mathrm{char}(k)$. A central embedding problem $E(G,Z/p^n,c)$ is called *weakly solvable* if there is some natural number $m \geqq n$ such that the induced embedding problem $E(G,\mathbf{Z}/p^m,c)$, where $c : G \times G \to \mathbf{Z}/p^n \hookrightarrow \mathbf{Z}/p^m$ is considered with values in $\mathbf{Z}/p^m$, is solvable.

§3. Cyclotomic splitting fields and central embedding problems

Let k be a field and let p be a prime number not equal to $\mathrm{char}(k)$. Denote by k^p the subfield of $\bar{k}$ which is generated over k by all p-power roots of unity in k.

(3.1) THEOREM. *Assume that k^p/k is cyclic. Then the following statements are equivalent*:

(i) *For all finite extensions k'/k, $k' \subset k^p$, every central simple k'-algebra of p-power exponent has a cyclotomic splitting field $E \subset k^p$.*

(ii) *For all finite extensions k'/k, $k' \subset k^p$, every central embedding problem over k' with a cyclic kernel of p-power order is weakly solvable.*

(iii) *For all finite extensions k'/k, $k' \subset k^p$, the cohomology group $H^3(G_{k'}, \mathbf{Z}_p)$ vanishes.*

The implications (ii)$\Leftrightarrow$(iii)$\Rightarrow$(i) *hold also when k^p/k is not cyclic.*

PROOF. (ii) implies (iii): Let k'/k be a finite extension such that $k' \subset k^p$ and let K/k' be a finite Galois extension, $K \subset \bar{k}$, with Galois group $G = \mathrm{Gal}(K/k')$. It is sufficient to show that the inflation map $\inf : H^2(G, \mathbf{Q}_p/\mathbf{Z}_p) \to H^2(G_{k'}, \mathbf{Q}_p/\mathbf{Z}_p)$ is trivial. Take $(f) \in H^2(G, \mathbf{Q}_p/\mathbf{Z}_p)$. Then there is a natural number n such that (f) is in the image of the natural map $H^2(G, \mathbf{Z}/p^n) \to H^2(G, \mathbf{Q}_p/\mathbf{Z}_p)$. By assumption the central embedding problem $E(G, \mathbf{Z}/p^n, f)$ is weakly solvable. Hence by (2.3) there is some $m \geqq n$ such that $(f) \in H^2(G, \mathbf{Z}/p^m)$ becomes trivial under the inflation map $\inf : H^2(G, \mathbf{Z}/p^m) \to H^2(G_{k'}, \mathbf{Z}/p^m)$, and so $\inf((f))$ is trivial in $H^2(G_{k'}, \mathbf{Q}_p/\mathbf{Z}_p)$, as was to be shown.

(iii) implies (ii): Let $E(G, \mathbf{Z}/p^n, f)$ be a central embedding problem over a finite extension k'/k, $k' \subset k^p$. By (2.1) it is sufficient to show that there is some $m \geqq n$ such that $(f) \in H^2(G, \mathbf{Z}/p^m)$ becomes trivial under the inflation map $\inf : H^2(G, \mathbf{Z}/p^m) \to H^2(G_{k'}, \mathbf{Z}/p^m)$. By assumption $H^2(G_{k'}, \mathbf{Q}_p/\mathbf{Z}_p)$ is trivial. Hence $\inf(f) = \delta\alpha$ for some function $\alpha : G_{k'} \to \mathbf{Q}_p/\mathbf{Z}_p$. Since all values of $\inf(f)$ have order $\leqq p^n$, the values of α have order $\leqq p^m$ for some $m \geqq n$, as was to be shown.

(iii) implies (i): Let k'/k be a finite extension, $k' \subset k^p$, and assume that $(\varepsilon) \in \mathrm{Br}(k')$ is of exponent p^n. Denote by (ε') the image of (ε) in $\mathrm{Br}(k'(\xi_{p^n}))_{p^n} \cong H^2(G_{k'(\xi_{p^n})}, \mathbf{Z}/p^n)$ under the natural restriction map. By assumption $H^2(G_{k'(\xi_{p^n})}, \mathbf{Q}_p/\mathbf{Z}_p) = 0$. Hence (ε') is in the image of the connecting homomorphism

$$\delta : \mathrm{Hom}(G_{k'(\xi_{p^n})}, \mathbf{Q}_p/\mathbf{Z}_p) \to H^2(G_{k'(\xi_{p^n})}, \mathbf{Z}/p^n)$$

which corresponds to the exact sequence

$$0 \to \mathbf{Z}/p^n \to \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{p^n} \mathbf{Q}_p/\mathbf{Z}_p \to 0.$$

Therefore $\varepsilon' = \delta\alpha$ for some $\alpha \in \mathrm{Hom}(G_{k'(\xi_{p^n})}, \mathbf{Q}_p/\mathbf{Z}_p)$. All values of α are of order $\leqq p^m$ for some $m \geqq n$. Therefore $k'(\xi_{p^m})$ splits (ε), as was to be shown.

(i) implies (ii) (or (iii)): Let k'/k be a finite extension, $k' \subset k^p$, and let $E(G, \mathbf{Z}/p^n, c)$ be a central embedding problem over k'. Choose embeddings

$\chi_i : \mathbf{Z}/p^i \hookrightarrow \bar{k}^*$ such that χ_{i-1} is the restriction of χ_i to $\mathbf{Z}/p^{i-1}$. We have $k(\chi_i) = k(\xi_{p^i})$. By assumption the Brauer class $\chi_n(c) \in \mathrm{Br}(k(\xi_{p^n}))$ is split by an extension $k(\xi_{p^m})$ for some $m \geqq n$. Hence by (2.3) the induced embedding problem $E(G, \mathbf{Z}/p^m, c)$ is solvable.

§4. Applications

We maintain the notations of §3.

(4.1) THEOREM. *Let p be a prime number, not equal to* char(k). *Assume that the cohomological p-dimension of G_k is* 2. *Then the strict cohomological p-dimension of G_k is* 2 *if and only if for all finite extensions k'/k, $k' \subset \bar{k}$, every central simple k'-algebra of p-power exponent has a cyclotomic splitting field $E \subset k' \cdot k^p$.*

PROOF. At first we remark that the p-part of $H^3(G_{k'}, \mathbf{Z}) = H^2(G_{k'}, \mathbf{Q}/\mathbf{Z})$ is equal to $H^3(G_{k'}, \mathbf{Z}_p)$; this is easily seen, using the divisibility of $\mathbf{Q}/\mathbf{Z}$.

For k^p/k cyclic the theorem follows from (3.1) and a result of Serre [6], I-21, Corollaire 4.

As shown in (3.1), the splitting field property follows from $H^3(G_{k'}, \mathbf{Z}_p) = 0$. Conversely, assume the splitting field property. Then (3.1) implies that the strict cohomological 2-dimension of $G_{k(\xi_4)}$ is 2. Using a result of Serre [6], I-20, Proposition 14, it follows that the strict cohomological 2-dimension of G_k is 2.

(4.2) REMARK. The condition that the cohomological p-dimension of G_k is 2 can be stated in terms of Brauer groups, see [7], p. 99, Theorem 23 in connection with p. 96, Corollary 1. So (4.1) gives a characterization of fields of strict cohomological dimension 2 entirely in terms of Brauer groups.

The following result is well known.

(4.3) *If k is a local or global number field then every central simple k-algebra of exponent p^n, p a prime number, has a* (*cyclic*) *cyclotomic splitting field $E \subset k^p$.*

In the local case one has to choose m in such a way that $k(\xi_{p^m})$ contains a (cyclic) subextension E/k such that $E : k \equiv 0 \bmod p^n$. Then E is a splitting field for every central simple k-algebra of exponent p^n.

If k is global and if A is a central simple k-algebra of exponent p^n which splits outside a given finite set of places S of k one has to choose m in such a way that $k(\xi_{p^m})$ contains a (cyclic) subextension E/k such that $E_{\bar{v}} : k_v \equiv 0 \bmod p^n$ for all places $v \in S$. Then E is a splitting field for A by the local-global principle in the theory of central simple algebras over a number field, see e.g. [1], VII, §5.

The following result of Tate is used in various contexts of algebraic number theory, see e.g. [2]. It can be deduced from (4.3) and (4.1), see [3], p. 28, Proposition 13.

(4.4) THEOREM (Tate). *If k is a local or global number field then $H^3(G_k, \mathbf{Z}) = 0$.*

Our approach yields also the following effective version of (3.1), (ii), which is implicit in our preceding discussion.

(4.5) PROPOSITION. *Let k be a number field, let K/k be a finite Galois extension with Galois group G, let p be a prime number such that k^p/k is cyclic and let $E(G, \mathbf{Z}/p^n, c)$ be a central embedding problem. Assume that the extension K/k is unramified outside the finite set of places S of k. If $m \geqq n$ is the smallest natural number such that the local degrees $k_v(\xi_{p^m}) : k_v$, $v \in S$, are divisible by p^n, then the induced embedding problem $E(G, \mathbf{Z}/p^m, c)$ is solvable.*

§5. Concluding remarks

Let k be a number field, let p be a prime number and assume $\xi_p \in k$. It follows from (4.4) that the connecting homomorphism

$$\delta : \mathrm{Hom}(G_k, \mathbf{Q}_p/\mathbf{Z}_p) \rightarrow H^2(G_k, \mathbf{Z}/p) \cong \mathrm{Br}(k)_p$$

corresponding to the exact sequence

$$0 \longrightarrow \mathbf{Z}/p \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p \stackrel{p}{\longrightarrow} \mathbf{Q}_p/\mathbf{Z}_p \rightarrow 0$$

is surjective. This may be stated in terms of algebras as follows.

(5.1) *Every central simple k-algebra of exponent p is similar to a crossed product $(K/k, \xi_p)$ for some cyclic extension K/k.*

The point in (5.1) is that ξ_p occurs as a "universal cocycle". One may then ask for a canonical set of cyclic extensions $\{K/k\}$ representing all central simple k-algebras of exponent p.

Let k be a number field, but not necessarily $\xi_p \in k$. Let S be a finite set of places of k containing all places above p and ∞. It is known that the so-called p-adic Leopoldt conjecture is closely related to the vanishing of $H^3(G_k(S), \mathbf{Z}_p)$, where $G_k(S)$ is the Galois group of the maximal Galois extension k_S/k, $k_S \subset \bar{k}$, which is unramified outside S, see e.g. [3], section 4.4, and by (3.1) this statement is seen to be equivalent to the following.

(5.2) *Every central embedding problem $E(G(K/k), \mathbf{Z}/p^n, c)$ with K/k unramified outside S, is weakly solvable, unramified outside S.*

References

1. M. Deuring, *Algebren*, Springer-Verlag, Berlin, Zweite Auflage, 1968.
2. A. Fröhlich, *Central extensions, Galois groups and ideal class groups of number fields*, Contemp. Math. **24**, American Mathematical Society, Providence, RI, 1983.
3. K. Haberland, *Galois cohomology of algebraic number fields*, Deutscher Verlag d. Wiss., Berlin, 1978.
4. K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106.
5. J. P. Serre, *Modular forms of weight one and Galois representations*, in *Algebraic Number Fields* (A. Fröhlich, ed.), Academic Press, New York, 1977.
6. J. P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math. **5**, Springer-Verlag, Berlin, 1965.
7. S. S. Shatz, *Profinite groups, arithmetic, and geometry*, Annals of Mathematics Studies **67**, Princeton University Press, 1972.