SOME REMARKS ON THE HASSE NORM THEOREM

HANS OPOLKA

Abstract. A substitute for the Hasse norm theorem in Galois extensions of number fields is made more explicit.

1. Let $k$ be a finite extension of $\mathbb{Q}$, let $\tilde{k}$ be an algebraic closure of $k$ and let $K \subset \tilde{k}$ be a finite Galois extension of $k$ with Galois group $G = G(K/k)$. According to A. Scholz the abelian group

$$\mathfrak{N} = \mathfrak{N}(K/k) = \{a \in k^* : a \text{ a norm locally everywhere in } K\}/\{a \in k^* : a \text{ a global norm in } K\}$$

is called the number knot of $K/k$. It is known to be finite. In [4, 6] it is shown that there is a solution of $\mathfrak{N}$, i.e. there is a Galois extension $L$ of $k$ containing $K$ such that $G(L/K)$ is contained in the center of $G(L/k)$ and such that the following modified norm principle holds:

If $x \in k^*$ is a norm locally everywhere in $L$ then $x$ is a global norm in $K$.

In this note we ask for the minimum $m(\mathfrak{N})$ of the set $\{L : K \subset L \text{ is a solution of } \mathfrak{N}\}$ and the following result will be proved.

Theorem. Let $K/k$ be a finite Galois extension of number fields with number knot $\mathfrak{N}$ and let $r$ denote the rank of $\mathfrak{N}$. Then $m(\mathfrak{N}) \leq (K : k)^r$.

Some remarks are added in the last section.

I am grateful to the referee for his suggestions.

2. We shall use Tate’s cohomological description of $\mathfrak{N}$, see [1, p. 198], namely

$\mathfrak{N}$ is dual to the kernel $\mathfrak{K} = \mathfrak{K}(K/k)$ of the localization map

$$H^2(G, C^*) \rightarrow \prod_v H^2(G_{\mathfrak{v}}, C^*),$$

$C^*$ with trivial action, $v$ runs over all places of $k$, $G_{\mathfrak{v}}$ denotes the decomposition group of some extension $\mathfrak{v}$ of $v$ to $K$.

The following statement is easy to prove, see [6, §2].

A central extension $L$ of $K/k$ is a solution of $\mathfrak{N}$ iff $\mathfrak{K}$ becomes trivial under inflation $H^2(G, C^*) \rightarrow H^2(G(L/k), C^*)$.

Following I. Schur we shall construct for every cohomology class $\hat{f} \in \mathfrak{K}$ an abstract central group extension $1 \rightarrow B \rightarrow \hat{G} \rightarrow G \rightarrow 1$ which satisfies the following conditions: $\hat{f}$ becomes trivial under inflation $H^2(G, C^*) \rightarrow H^2(\hat{G}, C^*)$, $|B| = K : k$, ...

Received by the editors April 15, 1981 and, in revised form, September 23, 1981.

1980 Mathematics Subject Classification. Primary 12A10, 12A65.

Key words and phrases. Algebraic numbers, Hasse’s norm theorem.

© 1982 American Mathematical Society

0002-9939/81/0000-1085/$01.75
the corresponding embedding problem is solvable. If $L_j$ is a solution of this embedding problem then the compositum $L$ of all $L_j$, $j$ runs over a basis of $\mathcal{S}$, is a solution of $\mathcal{S}$ which satisfies $L : K \leq (K : k)'.

3. So take $\bar{f} \in \mathcal{S}$ and let $m = \text{order of } \bar{f}, n = K : k$. Since $C$ is algebraically closed we may represent $\bar{f}$ by a 2-cocycle $f : G \times G \to C^*$ which takes all its values in $W_m$, the group of all $m$th roots of unity. $W_m$ is a subgroup of $B := W_n$ and $f : G \times G \to B$ defines a central extension $1 \to B \to G \to G \to 1$ such that $|B| = K : k$ and $\bar{f}$ becomes trivial under inflation.

4. In order to show that the corresponding embedding problem is solvable we shall use a criterium of Hoechsmann [3]: Let $A$ be a finite $G$-module and let $\mathcal{S} = G(\bar{k}/k)$. The group $\hat{A} := \text{Hom}(A, \bar{k}^*)$ becomes a $\mathcal{S}$-module under the action $x\cdot(a) = (\chi(a^{-1}))^x$, $x \in \hat{A}, a \in A, \hat{a} \in \mathcal{S}$. Let $\mathcal{S}_x$ be the fixed group of $x \in \hat{A}$. Then $\chi : A \to \bar{k}^*$ is a $\mathcal{S}_x$-homomorphism. Consider the following composition of maps:

$$\chi : H^2(G, A) \xrightarrow{\text{inf}} H^2(\mathcal{S}, A) \xrightarrow{\text{res}} H^2(\mathcal{S}_x, A) \xrightarrow{x^*} H^2(\mathcal{S}_x, \bar{k}^*).$$

So for $\bar{e} \in H^2(G, A)$ the image $\chi(\bar{e})$ defines an element in the Brauer group of the fixed field $k_x$ of $\mathcal{S}_x$. Combining Hoechsmann [3, p. 88 and p. 96] with Neukirch [5, p. 80], we get the following

(4.1) Proposition. If $A$ is a trivial $G$-module then the embedding problem given by $\bar{e} \in H^2(G, A)$ is solvable if $\chi(\bar{e})$ splits locally everywhere for all $x \in \hat{A}$.

5. Now we apply (4.1) in the situation of §3, i.e. $A = B = W_n, \bar{f} \in \mathcal{S}, e = f$. Let $\chi \in \hat{B}$ be of order $n$. Then $k_x = k(\xi)$, where $\xi$ is a primitive $n$th root of unity. Since the restriction $f_{\hat{e}}$ of $\bar{f}$ to any decomposition group $G_{\hat{e}}$ is trivial there exists a function $\beta : G_{\hat{e}} \to C^*$ such that $f_{\hat{e}}(x, y) = \beta(x)\beta(y)/\beta(xy)$ for all $x, y \in G_{\hat{e}}$. This implies that the Brauer class $\chi(\bar{e})$ can be represented by a 2-cocycle $f_{\hat{e}, \bar{e}}$, such that all values of $f_{\hat{e}, \bar{e}}$ are roots of unity of order dividing $m$ and such that $f_{\hat{e}, \bar{e}}(x, y) = \alpha(x)\alpha(y)/\alpha(xy)$ for all $x, y \in G_k(\xi)/k(\xi)$, where $\alpha$ is some function on $G(K_\xi(\xi)/k(\xi))$ with values in $\bar{k}^*$. Since $f_{\bar{e}, \bar{e}} = 1$ the function $\alpha^m$ is a character. So for $e = |G_{\hat{e}}|$ we have $\alpha^{e} = 1$. But $m \cdot e$ divides $n$ because

$$H^2(G, C^*) \xrightarrow{\text{res}} H^2(G_{\hat{e}}, C^*) \xrightarrow{\text{cor}} H^2(G, C^*) = G : G_{\hat{e}}.$$

Hence $\alpha^n = 1$ and it follows that $\chi(\bar{e})$ splits at $v$. A similar argument applies to all powers of $\chi$. The proof of our theorem is therefore complete.

6. Some final remarks. (a) In general $|\mathcal{R}| \leq m(\mathcal{R})$ (obvious), but one can extract examples from Scholz [7, p. 229], for which $|\mathcal{R}| < m(\mathcal{R})$ and $m(\mathcal{R}) = (K : k)'.

(b) Using the same method as above one can show that $m(\mathcal{R}) = \mathcal{R}$ if $k$ contains a primitive root of unity of order $K : k$, see [6, (3.2)].

(c) Let $n$ be between $\exp(\mathcal{R})$ and $K : k$ and denote by $K'$ the maximal abelian extension of $k$ contained in $K$. A refined version of the proof of the theorem yields the following result.
We have \( m(\xi) \leq n' \) if a primitive \( n \)th root of unity \( \xi \) is a norm locally everywhere in \( K'(\xi)/k(\xi) \).

(d) Instead of trying to find the minimum degree of a solution of the number knot of a Galois extension \( K/k \) one can ask for a solution with small conductor. This question leads to genus theory. The following result may serve as an example.

Let \( K/Q \) be some finite Galois extension. If \( x \in Q^* \) is a norm locally everywhere in the narrow central Hilbert class field \( H_+ \) of \( K \) then \( x \) is a global norm in \( K \).

A proof of it is implicit in [4, §4]. In the notation of [4] take \( k = Q, m = P_\infty = \) the archimedean prime of \( Q \). The only unit in \( Z \) which is \( \equiv 1(P_\infty) \) is 1, a global norm from any extension. A slightly sharper variant of this is:

Let \( K/Q \) be some finite Galois extension. If \( x \in Q^* \) is a norm locally everywhere in \( K \) and if it is a norm locally in \( H^+ \) at the infinite places and at those places where it is a nonunit then it is a global norm in \( K \).

This is true because in an unramified local extension a local unit is a norm of a local unit.

References


Mathematisches Institut, Roxeler Strasse 64, D-4400 Münster, Germany