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

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

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 $\{L: K \mid L \text{ is a solution of } \mathfrak{N}\}$ 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 $\mathfrak{S} = \mathfrak{S}(K/k)$ of the localization map

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

$\mathbf{C}^*$ with trivial action, v runs over all places of k , $G_{\bar{v}}$ denotes the decomposition group of some extension $\bar{v}$ 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 $\mathfrak{S}$ becomes trivial under inflation $H^2(G, \mathbf{C}^) \rightarrow H^2(G(L/k), \mathbf{C}^*)$.*

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

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 $L_{\bar{f}}$ is a solution of this embedding problem then the compositum L of all $L_{\bar{f}}$, $\bar{f}$ runs over a basis of $\mathfrak{S}$, is a solution of $\mathfrak{S}$ which satisfies $L: K \leq (K:k)'$.

3. So take $\bar{f} \in \mathfrak{S}$ 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 $f: G \times G \rightarrow C^*$ 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 $f: G \times G \rightarrow B$ defines a central extension $1 \rightarrow B \rightarrow \tilde{G} \rightarrow G \rightarrow 1$ 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 $\mathfrak{G} = G(\bar{k}/k)$. The group $\hat{A} := \text{Hom}(A, \bar{k}^*)$ becomes a $\mathfrak{G}$ -module under the action $\chi^\beta(a) = (\chi(a^{\beta^{-1}}))^\beta$, $\chi \in \hat{A}$, $a \in A$, $\beta \in \mathfrak{G}$. Let $\mathfrak{G}_\chi$ be the fixed group of $\chi \in \hat{A}$. Then $\chi: A \rightarrow \bar{k}^*$ is a $\mathfrak{G}_\chi$ -homomorphism. Consider the following composition of maps:

$$\bar{\chi}: H^2(G, A) \xrightarrow{\text{inf}} H^2(\mathfrak{G}, A) \xrightarrow{\text{res}} H^2(\mathfrak{G}_\chi, A) \xrightarrow{\chi^*} H^2(\mathfrak{G}_\chi, \bar{k}^*).$$

So for $\bar{\varepsilon} \in H^2(G, A)$ the image $\bar{\chi}(\bar{\varepsilon})$ defines an element in the Brauer group of the fixed field k_χ of $\mathfrak{G}_\chi$. 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 $\bar{\varepsilon} \in H^2(G, A)$ is solvable if $\bar{\chi}(\bar{\varepsilon})$ splits locally everywhere for all $\chi \in \hat{A}$.*

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

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

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

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

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

(c) Let n be between $\exp \mathfrak{R}$ 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 $m(\mathbb{R}) \leq n'$ if a primitive n th root of unity ξ 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 $K/\mathbb{Q}$ be some finite Galois extension. If $x \in \mathbb{Q}^*$ 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 $k = \mathbb{Q}$, $\mathfrak{m} = P_\infty$ = the archimedean prime of $\mathbb{Q}$. 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 $K/\mathbb{Q}$ be some finite Galois extension. If $x \in \mathbb{Q}^*$ 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

1. J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, London and New York, 1967.
2. D. Garbanati, *The Hasse norm theorem for 1-extensions of the rationals*, Number Theory and Algebra (Ed., H. Zassenhaus), Academic Press, London and New York, 1977, pp. 77–90.
3. K. Hoeschmann, *Zum Einbettungsproblem*, J. Reine Angew Math. **229** (1968), 81–106.
4. F. Lorenz, *Über eine Verallgemeinerung des Hasseschen Normensatzes*, Math. Z. **173** (1980), 203–210.
5. J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973), 59–116.
6. H. Opolka, *Zur Auflösung zahlentheoretischer Knoten*, Math. Z. **173** (1980), 95–103.
7. A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtobelscher Körpererweiterungen*. II, J. Reine Angew Math. **182** (1940), 217–234.

MATHEMATISCHES INSTITUT, ROXELER STRASSE 64, D-4400 MÜNSTER, GERMANY