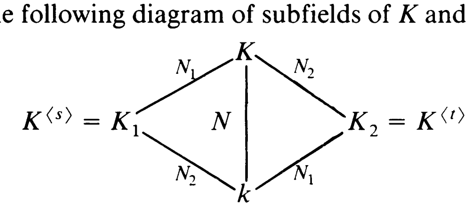
PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 93, Number 3, March 1985

ON THE EXPONENT OF NORM RESIDUE GROUPS

W. HÜRLIMANN[1] AND D. SALTMAN

ABSTRACT. We compute the exponent of some norm residue groups in the number theoretic case (global fields). We use the method of Galois cohomology and the theory of the Brauer group over a global field.

Let n be a natural number and let K/k be a Galois extension of arbitrary fields with bicyclic group $G = \mathbf{Z}/n \times \mathbf{Z}/n$ generated by s and t. By $H^r(G, K^*)$, $r \in \mathbf{Z}$, we mean the Tate cohomology groups of G with coefficients in the multiplicative group of K. We consider the following diagram of subfields of K and relative norms:



We use the known structure of the third Galois cohomological groups (see [**4** and **5**]):

$$H^3(G, K^*) = Z^3/B^3 \cong N_1K_2^* \cap N_2K_1^*/NK^*, \tag{1}$$

where the 3-cocycles are

$$Z^3 = \{c = (a, b) \in K_1^* \times K_2^* \mid N_2 a N_1 b = 1\}$$

and the 3-coboundaries are

$$B^3 = \{c = (a, b) \in K_1^* \times K_2^* \mid \text{ there exists } (x, y, z) \in K_1^* \times K_2^* \times K^* \text{ such that } t(x)N_1 z = ax,\ s(y) = byN_2 z\}.$$

The sets Z^3 and B^3 are multiplicative groups through the operation $(a, b)(a', b') = (aa', bb')$. The isomorphism in (1) is induced by the map $Z^3 \to N_1K_2^* \cap N_2K_1^*/NK^*$ which sends $c = (a, b)$ to $N_2 a = N_1 b^{-1} \bmod NK^*$.

The Diophantine equation $N(x) = a^n$, $a \in k^*$, x an indeterminate with value in K, is of interest.

LEMMA. *Let K/k be a Galois extension of arbitrary fields with group $G = \mathbf{Z}/n \times \mathbf{Z}/n$, $n \in \mathbf{N}$. If $H^3(G, K^*) = 0$, then k^*/NK^* has exponent at most n, that is, every nth power of k^* is a norm.*

PROOF. For all $a \in k^*$, the 3-cocycle $c = (a, a^{-1})$ is a coboundary. Hence the equation $N(x) = a^n$ has a solution.

Received by the editors January 16, 1984.
1980 *Mathematics Subject Classification*. Primary 12A60; Secondary 12G05, 12E15.

[1] This is a joint work done while the first author was staying at Yale University under a Swiss National Science Foundation fellowship.

©1985 American Mathematical Society
0002-9939/85 $1.00 + $.25 per page

It is possible to improve on this.

THEOREM 1. *Let K/k be a Galois extension of global fields with group $G = Z/p \times Z/p$, p an odd prime. Then the abelian group k^*/NK^* is of exponent p.*

PROOF. As $k^*/NK^* = H^0(G, K^*)$ has exponent at most p^2, it suffices to show that $a^p = N(x)$ has a k-rational point for every $a \in k^*$. The equation $N(x) = a^p$ can be written as $N_1(aN_2(x^{-1})) = 1$. Using Hilbert 90, it suffices to find $d \in K_2^*$, $x \in K^*$ such that

$$a = N_2(x)s(d)d^{-1}. \tag{2}$$

We interpret this equation in terms of central simple algebras. We introduce the cyclic crossed products $A = (K/K_2, a)$, $B = (K_1/k, a)$ and $C = (K/K_2, d)$. In the Brauer group, we have the following similarity (square brackets denote similarity):

$$[A] = [B \otimes_k K_2] \qquad [\mathbf{3}, (29.13)]. \tag{3}$$

We write C^s for the algebra C with the new K_2-module structure defined by $k \cdot d = s(k)d$, $k \in K_2$, $d \in C$. One can show that $C^s = (K/K_2, s(d))$. We observe that solving (2) is the same as finding a central simple K_2-algebra C such that

$$[A] = \left[C^s \otimes_{K_2} C^{\mathrm{op}}\right]. \tag{4}$$

If $a \in N_2K^*$, there is nothing to show. Hence we suppose that A is not the trivial algebra. We use the local invariants of Hasse for the description of the Brauer group of a global field [**3**, Chapter 8, or **2**, Chapter VII]. We will need the exact sequence [**3**, (32.14)] for the extension K/K_2. As A is obtained from B by extension of the base field, we have from [**2**, Theorem 4, p. 113]

$$(A/w) = n_v(B/v) \quad \text{for all places } w \text{ of } K_2 \text{ above the place } v \text{ of } k. \tag{5}$$

Here $(A/w), (B,/w)$ respectively n_v denote the local invariants of the classes of A, B respectively the local degree of the extension $(K_2)_w/k_v$. Thus the computation of the local invariants for the class of A is reduced to a computation concerning the algebra B. Let w be a place of K_2 and v its restriction to k. Three cases are possible.

Case 1. If w is an infinite place, it is clear that $(A/w) = 0$. Indeed, if $(A/w) = \frac{1}{2}$, then the local index 2 divides the exponent p of the algebra A, which is impossible.

Case 2. If w is a finite place invariant under the action of s, then $n_v = p$ and $(A/w) = (B/v)p$. But $(B/v) = 0$ or s_v/p, with $(s_v, p) = 1$, since $[B] \in \mathrm{Br}(K_1/k)$ is of exponent 1 or p. It follows that $(A/w) = 0$.

Case 3. If the finite place w is not invariant under s, we have p places $w = w_1, w_2, \ldots, w_p$ above v and $n_v = 1$. It follows that $(A/w_i) = (B/v) = 0$ or s_v/p with $(s_v, p) = 1$.

As the next step, we construct a class $[C]$ by giving its local invariants. If $(A/w) = 0$, we put $(C/w) = 0$. We remark that s is transitive on $w_1, w_2, \ldots, w_p$ and that $(C^s/w^s) = (C/w)$. If $(A/w_i) = s_v/p$ for $i = 1, \ldots, p$, we take the sequence of local invariants

$$\{(C/w_1), (C/w_2), \ldots, (C/w_p)\} = \{s_v/p, 2s_v/p, \ldots, (p-1)s_v/p, 0\}$$

such that after appropriate numbering of the w_i's, we have

$$\{(C^s/w_1),\ldots,(C^s/w_p)\} = \{2s_v/p, 3s_v/p,\ldots,0, s_v/p\}.$$

As $\sum_{w|v}(C/w) = (p-1)s_v/2 \equiv 0 \mod \mathbf{Z}$ if p is odd, the class $[C]$ is uniquely determined. The field K splits C, since if $(C/w) \neq 0$, then $(A/w) \neq 0$, and so K has local degree p at w. From the theory of crossed products and the fact that $\mathrm{Br}(K/K_2) \cong H^2(\langle t\rangle, K^*) \cong K_2^*/NK^*$, there exists $d \in K_2^*$ such that $C = (K/K_2, d)$. By construction, the class of $C^s \otimes_{K_2} C^{\mathrm{op}}$ possesses the same local invariants as the class of A. It follows that the algebra $(K/K_2, a^{-1}s(d)d^{-1})$, which is similar to the algebra $A^{\mathrm{op}} \otimes C^s \otimes C^{\mathrm{op}}$, is a matrix algebra. Therefore we have $a^{-1}s(d)d^{-1} \in N_2K^*$ and the proof is complete.

REMARK. The above proof is not valid if we omit the assumption p is odd. In fact there are biquadratic bicyclic extensions K/k such that k^*/NK^* is of exponent 4 as we will show below. This illustrates once more the difference in number theory between 2 and the other primes.

THEOREM 2. *Let K/k be a Galois extension of global fields with group $G = \mathbf{Z}/2 \times \mathbf{Z}/2$. Then we have*:

(I) *If $H^3(G, K^*) = 0$, then k^*/NK^* is of exponent* 2.

(II) *If $H^3(G, K^*) \neq 0$, then k^*/NK^* is of exponent* 4.

PROOF. In view of the lemma, it remains to show (II). The first author has computed that $H^3(G, K^*) = k^*/\prod_{i=1}^3 N_iK_i^*$, where N_3 is the norm from $K_3 = K^{\langle st\rangle}$ to k. (Details of proof will appear elsewhere; a connection with the Hasse problem is given below.) On the other side, we have $\prod_{i=1}^3 N_iK_i^* = \{x \in k^* | x^2 \in NK^*\}$ [**1**, Exercise 5, p. 360]. Since $H^3(G, K^*) \neq 0$, there exists $x \in k^*$ with $x^2 \notin NK^*$. We are done.

REMARK. One can show that $H^3(G, K^*) = N_1K_2^* \cap N_2K_1^*/NK^*$ is equal to the group {local norms}/{global norms}. The question whether a local norm is equal to a global norm is known as the Hasse problem. In the biquadratic case, consider the explicit isomorphism $N_1K_2^* \cap N_2K_1^*/NK^* \cong k^*/\prod_{i=1}^3 N_iK_i^*$, which sends a class $N_1a = N_2b^{-1} \mod NK^*$ to the class $aN_{K/K_1}(d) \mod \prod_{i=1}^3 N_iK_i^*$, where d satisfies $ab = st(d)d^{-1}$. Using this isomorphism and Exercise 5 in [**1**], the first author has produced an algorithm which solves the Hasse problem in this particular case (details will appear elsewhere).

REFERENCES

1. J. W. S. Cassels and A. Fröhlich (Editors), *Algebraic number theory*, Academic Press, London; Thompson, Washington, D. C., 1967.

2. M. Deuring, *Algebren*, Springer-Verlag, New York, 1966.

3. I. Reiner, *Maximal orders*, Academic Press, New York, 1975.

4. S. Takahashi, *Cohomology of finite abelian groups*, Tôhoku Math. J. (2) **4** (1952), 294–302.

5. T. Tannaka, *On the normal form of cohomology groups*, J. Math. Soc. Japan **6** (1954), 16–31.

FORSCHUNGSINSTITUT FÜR MATHEMATIK DER ETH, CH - 8092 ZÜRICH, SWITZERLAND

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS, AUSTIN, TEXAS 78712