

THE NORM EXPONENT IN GALOIS EXTENSIONS OF NUMBER FIELDS

HANS OPOLKA

ABSTRACT. The purpose of this note is to provide an upper bound for the exponent of the norm residue group $k^*/\text{Norm}_{K/k}(K^*)$ of a finite Galois extension K/k of number fields in terms of a certain central extension of K/k .

1. The norm exponent and the Hasse norm principle. Let K/k be a finite Galois extension of number fields with Galois group $G = \text{Gal}(K/k)$. We call

$$\lambda = \lambda(K/k) = \text{exponent of } k^*/\text{Norm}_{K/k}(K^*)$$

the norm exponent of K/k . An obvious upper bound for λ is the degree $(K : k)$. The purpose of this note is to obtain better bounds for λ in certain special cases. These will depend on the obstruction to the Hasse norm principle for K/k , i.e. on the kernel $\mathcal{K} = \mathcal{K}(K/k)$ of the natural map

$$(1.1) \quad \hat{H}^0(G, K^*) \rightarrow \hat{H}^0(G, \mathbf{A}_K^*),$$

where \hat{H}^0 denote the Tate-cohomology in dimension 0 and \mathbf{A}_K^* the group of units of the adèle-ring \mathbf{A}_K of K . For instance, using the local reciprocity map, we obtain

(1.2) If the Hasse norm principle holds for K/k then $\lambda(K/k)$ divides $\exp(G)$.

In general we use the result (2.5) in [6] which says that there is a finite central extension L of K/k (i.e. $\text{Gal}(L/K)$ is contained in the center of $\text{Gal}(L/k)$) with the following property:

(1.3) Every $x \in k^*$ which is a norm locally everywhere in L/K is a global norm in K/k .

We call every central extension of K/k with this property an extension defined by $\mathcal{K}(K/k)$. We denote by $\mu = \mu(K/k)$ the minimum of all $\exp(\text{Gal}(L/k))$ where L runs over all central extensions of K/k defined by $\mathcal{K}(K/k)$ and observe

(1.4) PROPOSITION. $\lambda(K/k)$ divides $\mu(K/k)$.

PROOF. Let L be a central extension of K/k such that $\mu(K/k) = \exp(\text{Gal}(L/k))$. Using the density theorem and local class field theory we see that $\mu(K/k)$ is the l.c.m. of all local norm exponents $\lambda_v(L/k) = \exp$ of $k_v^*/\text{Norm}_{L_{\bar{v}}/k_v}(L_{\bar{v}}^*)$ where v runs over all places of k and \bar{v} denotes an extension of v to L . Since L has property (1.3) the assertion is obvious.

In §3 we estimate $\mu(K/k)$ in some special cases.

2. The method. We shall make use of a well-known observation by Tate [2, p. 198], which says that $\mathcal{K}(K/k)$ is dual to the kernel $\mathcal{K}(K/k)$ of the localization map

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

Received by the editors May 29, 1985 and, in revised form, December 10, 1985.
 1980 *Mathematics Subject Classification*. Primary 12A10, 12A65.

where \mathbf{C}^* is considered with the trivial group action and where v runs over all places of k and $G_{\bar{v}}$ denotes the decomposition group of an extension \bar{v} of v to K . In [6] it is shown that a finite central extension L of K/k has property (1.3) if and only if $\mathcal{H}(K/k)$ is in the kernel of the inflation map $H^2(G, \mathbf{C}^*) \rightarrow H^2(\text{Gal}(L/k), \mathbf{C}^*)$. In order to construct such an L we represent every 2-cocycle class $\varepsilon \in \mathcal{H}(K/k)$ by a suitable 2-cocycle $f: G \times G \rightarrow \mu_n$ with values in a group of n th order roots of unity μ_n in an algebraic closure \bar{k} of k and consider the corresponding central group extension $G(f)$ of G with kernel μ_n . If n is large enough the embedding problem corresponding to $G(f)$ will be solvable and yields a central extension L_f of K/k with $\text{Gal}(L_f/k) \cong G(f)$ and ε in the kernel of the inflation map $H^2(G, \mathbf{C}^*) \rightarrow H^2(\text{Gal}(L_f/k), \mathbf{C}^*)$. Taking a basis $\varepsilon_1, \dots, \varepsilon_r$ of $\mathcal{H}(K/k)$ and representatives f_1, \dots, f_r as above the compositum L of L_{f_1}, \dots, L_{f_r} is a central extension of K/k with property (1.3). Then we apply (1.4).

3. The abelian case. It is well known that for an abelian G the group $H^2(G, \mathbf{C}^*)$ can be identified with the group of symplectic pairings on G , i.e.

$$H^2(G, \mathbf{C}^*) \xrightarrow{\sim} (G \wedge G)^\wedge,$$

by sending every 2-cocycle $f: G \times G \rightarrow \mathbf{C}^*$ to the pairing

$$\omega_f: G \times G \rightarrow \mathbf{C}^*, \quad \omega_f(x, y) := f(x, y)/f(y, x), \quad x, y \in G.$$

This fact will be used in the proof of the following result.

(3.1) **THEOREM.** *Assume that $G = \text{Gal}(K/k)$ is abelian. If $(K : k)$ is odd then $\mu(K/k)$ divides $\exp(G)$. If $(K : k)$ is even and $\sqrt{-1} \in k$ then $\mu(K/k)$ divides $2 \cdot \exp(G)$. Hence the norm exponent of K/k divides $\exp(G)$ if $(K : k)$ is odd and $2 \cdot \exp(G)$ if $(K : k)$ is even and $\sqrt{-1} \in k$.*

This result generalizes (3.4.9) in [9] and Theorem 1 in [5].

PROOF OF (3.1). Represent $\varepsilon \in \mathcal{H}(K/k)$ by a 2-cocycle $f: G \times G \rightarrow \mu_n$, $n = \exp(\mathcal{H}(K/k))$, as follows. If $\exp(G)$ is odd take $f(x, y) = (\omega_\varepsilon(x, y))^{1/2}$, $x, y \in G$, where $\omega_\varepsilon: G \times G \rightarrow \mu_n$ is the symplectic pairing corresponding to ε . Since f is locally trivial the central group extension $G(f)$ splits locally everywhere and therefore the corresponding embedding problem is solvable; see [3]. For the same reason the exponent of $G(f)$ divides the l.c.m. of n and the exponent of G . But n divides $\exp(G)$. Hence $\exp(G(f))$ divides $\exp(G)$. If $\exp(G)$ is even, write $\omega_\varepsilon(x, y) = f(x, y)/f(y, x)$, $x, y \in G$, where $f: G \times G \rightarrow W_n$ is a bilinear pairing. For every place v of k there is a function $\alpha_v: G_{\bar{v}} \rightarrow \mathbf{C}^*$ such that $f(x, y) = \alpha_v(x)\alpha_v(y)/\alpha_v(xy)$, $x, y \in G_{\bar{v}}$. We have

$$1 = f(x, x)^{2n(2n-1)/2} = f(x, x)f(x, x^2) \cdots f(x, x^{2n-1}) = \alpha_v(x)^{2n}$$

for all $x \in G_{\bar{v}}$. This shows that the central group extension $G(f)$ splits locally everywhere. Now the same reasoning as above proves (3.1) also in this case.

REMARK. The proof shows that the assertion of (3.1) remains true under the following apparently weaker assumption.

(3.2) $(K : k)$ is odd or $(K : k) = 2^t m$, $(2, m) = 1$, and for all places v above 2 the cyclotomic fields $k_v(\xi_{2^t})/k_v$ are cyclic.

(3.3) COROLLARY. *Let K/k be a finite Galois extension of number fields with Galois group $G = \text{Gal}(K/k)$ and assume that the Sylow subgroups of G are abelian. Then under the assumption (3.2) we have: The norm exponent $\lambda(K/k)$ divides $\exp(G)$ if $(K : k)$ is odd and divides $2 \cdot \exp(G)$ in any case.*

PROOF. For every prime divisor p of $(K : k)$ denote by G_p the p -Sylow subgroup of G . The assertion follows from the well-known fact that the restriction map $\hat{H}^0(G, K^*) \rightarrow \hat{H}^0(G_p, K^*)$ is injective on the p -part of $\hat{H}^0(G, K^*)$.

5. Remarks.

(5.1) Let k/\mathbb{Q} be a finite Galois extension. Then

$$\lambda(K/\mathbb{Q}) \text{ divides } h \cdot \exp(\text{Gal}(K/\mathbb{Q}))$$

where h is the narrow class number of K .

This follows from [7, §6], where it was shown that the central part of the narrow Hilbert class field of K is an extension defined by $K(K/\mathbb{Q})$.

(5.2) Let K/k be a finite Galois extension such that $(K : k)$ is equal to the l.c.m. of the local degrees $(K_{\bar{v}} : k_v)$ where v runs over all places of k . Then

$$\lambda(K/k) \text{ divides } \exp(\text{Gal}(K/k)).$$

Indeed, using the fact that the restriction $H^2(G, \mathbb{C}^*) \rightarrow H^2(G_{\bar{v}}, \mathbb{C}^*)$ composed with the corestriction $H^2(G_{\bar{v}}, \mathbb{C}^*) \rightarrow H^2(G, \mathbb{C}^*)$ is equal to the index $(G : G_{\bar{v}})$ we see that $\mathcal{N}(K/k)$ is trivial. This means that the map defined under (1.1) is injective. So the assertion follows in view of the local reciprocity law.

(5.3) Note that the condition in (5.2) is equivalent to the triviality of the Teichmüller-cocycle; see [1, p. 68]. So the Lemma in [5] is obvious.

ACKNOWLEDGMENT. The author is grateful to the referee and to K. Miyake for useful remarks.

REFERENCES

1. E. Artin and J. Tate, *Class field theory*, Benjamin, Elmsford, N.Y., 1967.
2. J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, New York, 1967.
3. K. Hoeffmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106.
4. B. Huppert, *Endliche Gruppen*. I, Springer-Verlag, Berlin, 1967.
5. W. Hürlimann and D. Saltman, *On the exponent of norm residue groups*, Proc. Amer. Math. Soc. **93** (1985), 417–419.
6. H. Opolka, *Zur Auflösung zahlentheoretischer Knoten*, Math. Z. **173** (1980), 95–103.
7. —, *Some remarks on the Hasse norm theorem*, Proc. Amer. Math. Soc. **84** (1982), 464–466.
8. J. P. Serre, *Modular forms of weight one and Galois representations*, Algebraic Number Fields (A. Fröhlich, ed.), Durham Symposium, Academic Press, London, 1977.
9. G. Steinke, *Über Auflösungen zahlentheoretischer Knoten*, Schriftenreihe Math. Inst. Univ. Münster, Ser. 2, Heft 25, 1982.

MATHEMATISCHES INSTITUT, BUNSENSTRASSE 3-5, D-3400 GÖTTINGEN, FEDERAL REPUBLIC OF GERMANY