COMPOSITIO MATHEMATICA

MICHAEL J. RAZAR

Central and genus class fields and the Hasse norm theorem

Compositio Mathematica, tome 35, n° 3 (1977), p. 281-298

<http://www.numdam.org/item?id=CM_1977__35_3_281_0>

COMPOSITIO MATHEMATICA, Vol. 35, Fasc. 3, 1977, pag. 281–298
Noordhoff International Publishing
Printed in the Netherlands

CENTRAL AND GENUS CLASS FIELDS AND THE HASSE NORM THEOREM

Michael J. Razar

§1. Introduction

Let K/k be a finite Galois extension of global fields. The group $N_{K/k}K^\times$ of global norms of $k^\times$ is a subgroup of finite index in the group of elements of $k^\times$ which are local norms in every completion. Denote this index by $i(K/k)$. The classical Hasse norm theorem (HNT) asserts that if K/k is cyclic, then $i(K/k) = 1$. We say, more generally, that HNT holds for K/k if $i(K/k) = 1$.

Let L/K be an abelian extension, and let L_z/K be the maximum subextension of L/K such that $G(L_z/K)$ is contained in the center of $G(L_z/k)$. Let L_g be the compositum of K and the maximum abelian subextension of L/k. Theorem 1 of this paper asserts that there is an ideal $\mathfrak{A}$ of the ring of integers of k such that if L is the maximum abelian extension of K whose conductor divides $\mathfrak{A}$, then $i(K/k) = [L_z : L_g]$. Theorem 2 says that HNT holds for an abelian extension K/k if and only if it holds for every (maximal) subextension of prime exponent. Theorem 3 gives $i(K/k)$ for an abelian extension K/k as the index of $\Sigma \Lambda^2 G_v$ in $\Lambda^2 G$, where $G = G(K/k)$, G_v is the decomposition group of the prime v, the sum is over all ramified primes v of k and Λ^2 is the second exterior power.

This paper was motivated by some recent work of D. Garbanati ([3] and [4]) in which he studies Galois extensions K of the rationals for which HNT holds. In [3], using some ingenious and intricate index computations, he proves that if $K/\mathbb{Q}$ is Galois and if L/K is the narrow genus class field, then $i(K/\mathbb{Q}) = [L_z : L_g]$. From here, he goes on to give a criterion, in the form of the maximality of rank of a certain matrix, for HNT to hold for some special types of extensions of the rationals. In [4], he extends this result to abelian extensions of $\mathbb{Q}$ of (odd) prime power degree which are composites of cyclic extensions with relatively prime descriminants.

The present paper is an attempt to better understand Garbanati's theorems and to simplify his arguments by interpreting the relevant indices cohomologically. In §2, the problem is placed in a cohomological setting and the indices are related to each other (Proposition 2). In §3, the construction of L/K is carried out and Theorem 1 is proved. In §4 a powerful technique of Tate is used to study the index $i(K/k)$. In effect, Tate's method reduces the computation of $i(K/k)$ to group theory once one knows the decomposition groups for the ramified primes. In §5, this method is applied to prove Theorem 3.

In light of the results of §4 and §5, the results of §3 should probably be used as *consequences* of HNT rather than *criteria* for HNT. In particular, it should be possible to say a considerable amount about towers of fields $L \supset K \supset k$ where L/K and K/k are abelian but L/k is not. A simple example of this is mentioned in Remark 2 following Theorem 1.

I would like to express thanks to Professor Dennis Garbanati for introducing me to this problem and for several informative conversations. I would also like to thank Professor Walter Hill who first suggested that the problem might be susceptible to a cohomological approach and whose initial ideas along these lines provided much of the impetus for this work.

§2. Index computations

Most of this section consists of cohomological index computations. The notation is fairly standard but is summarized below for the convenience of the reader.

G = a finite group, written multiplicatively
A = a G-module, written additively or multiplicatively
$A^G = H^0(G, A) = \{a \in A | \sigma a = a \text{ for all } \sigma \in G\}$
$N = \Sigma_{\sigma \in G} \sigma \in \mathbb{Z}[G]$
I_G = ideal in $\mathbb{Z}[G]$ generated by $\{(\sigma - 1) | \sigma \in G\}$
$A_N = \{a \in A | Na = 0\}$
$NA = \{Na | a \in A\}$.

The Tate cohomology is used:

$$\hat{H}^n(G, A) = \begin{cases} H^n(G, A) & \text{if } n \geq 1 \\ H_{-n-1}(G, A) & \text{if } n \leq -2 \\ A_N/I_G A & \text{if } n = -1 \\ A^G/NA & \text{if } n = 0. \end{cases}$$

The following lemma is an easy consequence of the definitions and no proof is given here.

LEMMA 1: *Let* $0 \longrightarrow A' \xrightarrow{f} A \xrightarrow{g} A'' \longrightarrow 0$ *be an exact sequence of G-modules. Identify A' with its image f(A') in A. In the induced long exact sequence*

$$\hat{H}^{-1}(G, A') \xrightarrow{f_{-1}} \hat{H}^{-1}(G, A) \xrightarrow{g_{-1}} \hat{H}^{-1}(G, A'') \xrightarrow{\delta} \hat{H}^{0}(G, A') \xrightarrow{f_0} \hat{H}^{0}(G, A)$$

(a) $\operatorname{Im}\delta = \operatorname{Coker} g_{-1} = \operatorname{Ker} f_0 = \dfrac{(A')^G \cap NA}{NA'}$,

(b) $\operatorname{Im} g_{-1} = \operatorname{Ker}\delta = \dfrac{A_N \cdot A'}{(I_G A)\cdot A'}$,

(c) $\operatorname{Im} f_{-1} = \operatorname{Ker} g_{-1} = \dfrac{(I_G A)\cdot A'_N}{I_G A} = \dfrac{A'_N}{(I_G A)\cap A'_N}$,

(d) $\operatorname{Im} f_0 = \operatorname{Coker}\delta = \dfrac{(A')^G \cdot NA}{NA} = \dfrac{(A')^G}{(A')^G \cap NA}$.

The above lemma is applied several times to G-modules arising in class field theory. The notation is as follows.

k = (fixed) global field
K/k = (fixed) Galois extension
$G = G(K/k)$.

v and w respectively, denote valuations of k and K, respectively. If w extends v, the notation w/v is used. The completions are denoted by K_w and k_v and the units by U_w and U_v, if v is non-archimidean. If v is archimidean, $U_v = K_v^{\times}$.

For any field L, J_L and C_L respectively, are the idele group and idele class group, respectively.

$$U_K = \prod_w U_w \subset J_K$$

$$U_k = \prod_v U_v \subset J_k.$$

Various class fields are constructed in this paper, corresponding to certain subgroups of J_K (more precisely, of C_K). The subgroups of J_K are of the form

$$V_K = \prod_w V_w$$

where, for each valuation w of K,

(i) V_w is an open subgroup of finite index in U_w.
(ii) $V_w = U_w$ for all but finitely many w.
(iii) $V_{\sigma w} = \sigma V_w$ for all w and all $\sigma \in G$.

These conditions insure that $(J_K : K^\times V_K) < \infty$ and that V_K is a G-submodule of J_K. Let

$$E_K = K^\times \cap V_K \quad \text{and} \quad T_K = \frac{V_K}{E_K} = \frac{K^\times V_K}{K^\times} \subset C_K.$$

Then T_K is an open subgroup of finite index in C_K and hence defines a unique abelian extension L/K. The Galois group $G(L/K)$ is a G-module which is isomorphic (as a G-module) to H_K, where

$$H_K = C_K/T_K = J_K/K^\times V_K.$$

For example, if $V_K = U_K$, then L is the Hilbert class field of K, H_K is the ideal class group of K, and E_K is the group of (global) units of K.

Now, put $D_K = J_K/U_K$ and $P_K = K^\times/E_K$ and collect everything into a commutative diagram with exact rows and columns:

(2.1)

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & E_K & \longrightarrow & V_K & \longrightarrow & T_K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & K^\times & \longrightarrow & J_K & \longrightarrow & C_K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & P_K & \longrightarrow & D_K & \longrightarrow & H_K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

The above diagram induces another commutative diagram with exact rows and columns. The maps are labelled for easy reference later.

$$\begin{array}{ccccc} \hat{H}^{-1}(G, V_K) & \xrightarrow{\lambda} & \hat{H}^{-1}(G, T_K) & \xrightarrow{\rho} & \hat{H}^{0}(G, E_K) \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \tau} \\ \hat{H}^{-1}(G, J_K) & \xrightarrow{\theta} & \hat{H}^{-1}(G, C_K) & \xrightarrow{\delta} & \hat{H}^{0}(G, K^{\times}) \\ \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \sigma} & & \\ \hat{H}^{-1}(G, D_K) & \xrightarrow{\mu} & \hat{H}^{-1}(G, H_K). & & \end{array} \tag{2.2}$$

Some of the maps in the above have interesting number theoretic interpretations. Let

$$V_k = V_K^G,\ E_k = E_K^G = k^{\times} \cap V_k \quad \text{and} \quad T_k = V_k/E_k.$$

LEMMA 2:

(a) $\operatorname{Im} \delta = \operatorname{Coker} \theta = \dfrac{k^{\times} \cap NJ_K}{NK^{\times}}.$

(b) $\operatorname{Im} \sigma = \operatorname{Coker} \beta = \dfrac{(C_K)_N \cdot T_K}{(I_G C_K) \cdot T_K}.$

(c) $\operatorname{Im} \rho = \dfrac{E_k \cap NV_K}{NE_K}.$

(d) $\operatorname{Im} \tau = \dfrac{E_k}{E_k \cap NK^{\times}}.$

(e) $\operatorname{Ker} \tau = \dfrac{E_k \cap NK^{\times}}{NE_K}.$

PROOF: (a), (c), (e) follow from Lemma 1a.
(b) follows from Lemma 1b.
(d) follows from Lemma 1d.

The main objects studied in this paper are $\operatorname{Im} \delta$ and $\operatorname{Im} \sigma$. The image of δ is the group of elements of $k^{\times}$ which are everywhere local norms modulo the group of global norms. Thus, $\operatorname{Im} \delta = 0$ if and only if HNT holds for K/k.

The interpretation of $\operatorname{Im}\sigma$ requires some definitions. Let L be the abelian extension of K corresponding to T_K. The *central class field* of K/k (relative to T_K) is the maximum subextension L_z/K of L/K such that L_z/k and is Galois and $G(L_z/K)$ is contained in the center of $G(L_z/k)$. The *genus class field* of K/k (relative to T_K) is the compositum $L_g = K \cdot L_{ab}$, where L_{ab}/k is the maximum abelian subextension of L/k. Equivalently, L_g/K is the maximum subextension of L/K such that L_g is the compositum of K with an abelian extension of k.

It is clear that $L_g \subset L_z$. The corollary to the following proposition says that $G(L_z/L_g)$ is isomorphic to $\operatorname{Im}\sigma$.

PROPOSITION 1: *Let T_K be an open subgroup of finite index in C_K and let L/K be class field to T_K. Then L_z/K is class field to $I_G C_K \cdot T_K$ and L_g/K is class field to $(C_K)_N \cdot T_K$.*

PROOF: Let M/K be a subextension of L/K Galois over k and suppose M/K is class field to $S_K \supset T_K$. Then $G(M/K)$ is isomorphic (as a G-module) to C_K/S_K.

(a) In order that $G(M/K)$ be in the center of $G(M/K)$ it is necessary and sufficient that the action of G on $G(M/K)$ (by conjugation) be trivial. Since $G(M/K)$ and C_K/S_K are isomorphic G-modules, M/K is central if and only if $I_G C_K \subset S_K$. Since the correspondence between class fields and subgroups of C_K is order reversing, L_z/K is class field to $I_G C_K \cdot T_K$.

(b) Note that $L_g = L_{ab}K$ is characterized as being the smallest subextension M/K of L/K such that $L_{ab} \subset M$. Now L_{ab}/k is class field to $N_{L/k}C_L = NT_K$ and M_{ab}/k is class field to NS_K. Since $M \subset L$, $S_K \supset T_K$ and, since $L_{ab} \subset M_{ab}$, $NS_K \subset NT_K$. If $M = L_g$, S_K is the largest subgroup of C_K such that $S_K \supset T_K$ and $NS_K = NT_K$. Thus,

$$S_K = N^{-1}(NT_K) = (C_K)_N \cdot T_K.$$

COROLLARY: *The image of σ is isomorphic (as a G-module) to $G(L_z/L_g)$.*

PROOF: Consider the exact sequence of G-modules:

$$0 \longrightarrow \frac{(C_K)_N \cdot T_K}{I_G C_K \cdot T_K} \longrightarrow \frac{C_K}{I_G C_K \cdot T_K} \longrightarrow \frac{C_K}{(C_K)_N \cdot T_K} \longrightarrow 0.$$

By Proposition 1, the second and third terms are isomorphic to $G(L_z/K)$ and $G(L_g/K)$ respectively. By Lemma 1b, the first term is

isomorphic to Im σ. The corollary follows now by Galois theory.

The next proposition describes a relationship between Im δ and Im σ.

PROPOSITION 2:

(a) $$\frac{\text{Im } \sigma}{\text{Im } \sigma\theta} = \frac{\text{Im } \delta}{\text{Im } \delta\beta}.$$

(b) $$\text{Im } \delta\beta = \frac{E_k \cap NV_K}{E_k \cap NV_K \cap NK^\times} = \frac{k^\times \cap NV_K}{NK^\times \cap NV_K}.$$

(c) $$\text{Im } \sigma\theta = \frac{(J_K)_N \cdot K^\times V_K}{I_G J_K \cdot K^\times V_K}.$$

PROOF: (a) Straightforward application of exactness and commutativity of diagram.

(b) Since $\delta\beta = \tau\rho$, $\text{Im } \delta\beta = \text{Im } \tau\rho = \dfrac{\text{Im } \rho}{\text{Im } \rho \cap \text{Ker } \tau}$.

Apply Lemma 2c and 2e.

(c) Apply Lemma 1b to the cohomology map $\sigma\theta : \hat{H}^{-1}(G, J_K) \to \hat{H}^{-1}(G, H_K)$ which is induced by the exact sequences

$$1 \longrightarrow K^\times V_K \longrightarrow J_K \longrightarrow H_K \longrightarrow 1.$$

§3. Construction of a class field

Define $i(K/k) = |\text{Im } \delta|$. In particular, $i(K/k) = 1$ if and only if HNT holds for K/k. By Proposition 1 and Proposition 2a,

$$\frac{i(K/k)}{|\text{Im } \delta\beta|} = \frac{[L_z : L_g]}{|\text{Im } \sigma\theta|}. \tag{3.1}$$

It seems hard to say in general when $|\text{Im } \delta\beta| = |\text{Im } \sigma\theta|$. But it is easy to see when both are trivial. Namely,

$$\sigma\theta = 0 \Leftrightarrow \text{Im } \theta \subset \text{Im } \beta$$
$$\delta\beta = 0 \Leftrightarrow \text{Im } \beta \subset \text{Im } \theta.$$

Thus $\sigma\theta = 0$ and $\delta\beta = 0$ if and only if $\text{Im } \theta = \text{Im } \beta$.

The remainder of this section is devoted to the construction of a

subgroup T_K of C_K for which $\sigma\theta = 0$ and $\delta\beta = 0$. The corresponding class field L/K then satisfies the equation

$$[L_z : L_g] = i(K/k). \tag{3.2}$$

The cohomology groups $\hat{H}^q(G, J_K)$ and $\hat{H}^q(G, V_K)$ can be computed locally. It is a routine application of Shapiro's lemma that

$$\hat{H}^q(G, J_K) = \coprod_v \hat{H}^q\left(G, \prod_{w/v} K_w^\times\right) = \coprod_v \hat{H}^q(G_w, K_w^\times)$$

and

$$\hat{H}^q(G, V_K) = \coprod_v \hat{H}^q\left(G, \prod_{w/v} V_w\right) = \coprod_v \hat{H}^q(G_w, V_w)$$

where, in the last products a single prime w of K lying over each prime v of k has been chosen. This choice of one w for each v is fixed for the remainder of the discussion.

The map $\gamma: \hat{H}^{-1}(G, V_K) \to \hat{H}^{-1}(G, J_K)$ respects the above decomposition in the sense that $\gamma = \coprod \gamma_w$ where

$$\gamma_w: \hat{H}^{-1}(G_w, V_w) \longrightarrow \hat{H}^{-1}(G_w, K_w^\times)$$

is the map induced by the inclusion $V_w \subset K_w^\times$. For all but finitely many v, $V_w = U_w$. But if $V_w = U_w$ the valuation exact sequence (if w is non-archimedean)

$$1 \longrightarrow U_w \longrightarrow K_w^\times \xrightarrow{w} \mathbb{Z} \longrightarrow 0$$

yields the fact that

$$\hat{H}^{-1}(G_w, U_w) \xrightarrow{\gamma_w} \hat{H}^{-1}(G_w, K_w^\times) \longrightarrow \hat{H}^{-1}(G_w, \mathbb{Z})$$

is exact. Since $\hat{H}^{-1}(G_w, \mathbb{Z}) = 0$, γ_w is surjective whenever $V_w = U_w$.

Now the cokernel of γ may be expressed as a finite sum

$$\text{Coker } \gamma = \coprod_v \text{Coker } \gamma_w$$

where the sum is over all v for which $V_w \neq U_w$.

On the other hand, (even if $V_w \neq U_w$) if w is unramified over v, or if w is archimedean, G_w is cyclic and hence $\hat{H}^{-1}(G_w, K_w^\times) = H^1(G_w, K_w^\times) = 0$. Thus Coker $\gamma_w = 0$ in these cases too.

The following proposition is now immediate.

PROPOSITION 3: *If $V_w = U_w$ for all ramified non-archimedean v, then* Im $\nu =$ Coker $\gamma = 0$ *and consequently* $\sigma\theta = 0$.

The problem of constructing V_K so that $\delta\beta = \tau\rho = 0$ seems to be more difficult to do explicitly. The problem is solved below in a somewhat non-constructive manner. However, in any given case, it should be possible to do explicitly. Part of a theorem from the Artin–Tate notes ([1], p. 82) is needed and is paraphrased below:

Let k be a global field, S a finite set of primes of k and n a positive integer. Then

$$k \cap \bigcap_{v \notin S} k_v^{2n} \subset k^n.$$

PROPOSITION 4: *Let S be a finite set of primes of k and let $n = [K:k]$. There is a finite set of primes S' disjoint from S such that if $V_v \subset U_v^{2n}$ for all $v \in S'$, then the image of*

$$\tau\colon \hat{H}^0(G, E_K) \longrightarrow \hat{H}^0(G, K^\times)$$

is zero.

PROOF: It is equivalent (by Lemma 1d) to show that $E_k = V_k \cap k^\times \subset NK^\times$. Since $k^{\times n} \subset NK$, it is enough to show that $E_k \subset (k^\times)^n$.

Let $U_k = \Pi_v U_v$ and $F_k = k^\times \cap U_k$. Then F_k is the group of all global units of k and so is finitely generated. Since $V_w \subset U_w$ for all w, $V_k \subset U_k$ and $E_k \subset F_k$. By the result quoted from Artin–Tate,

$$F_k \cap \bigcap_{v \notin S} k_v^{2n} \subset F_k \cap k^n = F_k^n.$$

Now, since F_k is finitely generated, F_k/F_k^n is a finite group. Hence one can find a *finite* set S' of primes disjoint from S such that

$$F_k \cap \bigcap_{v \in S'} k_v^{2n} \subset F_k^n$$

or,

$$\bigcap_{v \in S'} (F_k \cap U_v^{2n}) \subset F_k^n.$$

Thus, if $V_v \subset U_v^{2n}$ for all $v \in S'$, then

$$E_k = V_k \cap k^\times \subset F_k^n \subset k^{\times n}.$$

The non-constructive aspect of Proposition 4 is in determining the set S'. Once S' is known it is easy to construct suitable V_w as follows. If w is non-archimedean let U_w^1 denote the subgroup of U_w consisting of u such that $w(u-1) > 0$. Define U_v^1 similarly and note that $(U_w^1)^G = U_v^1$. If v does not divide $2n = 2[K:k]$, then by Hensel's lemma $U_w^1 \subset (U_w)^{2n}$. Thus, as long as the set S in Proposition 4 contains all the prime divisors of n and all archimedean primes, it is sufficient to put $V_w = U_w^1$ for all w lying over some $v \in S'$. The advantage of choosing

$$V_K = \prod_{w \in S'} U_w^1 \times \prod_{w \notin S'} U_w \tag{3.3}$$

is that this choice makes L/K quite amenable to an easy arithmetic description. To be precise, define an ideal of the ring of integers O_K of K by

$$\mathfrak{b} = \prod_{w \in S'} w.$$

Let V_K be given by (3.3) and let L/K be class field to $K^\times V_K$. Then L is the maximum abelian extension of K whose conductor divides $\mathfrak{b}$. Note that since all primes dividing $\mathfrak{b}$ are unramified, $\mathfrak{b}$ is the extension to O_K of an ideal $\mathfrak{A}$ of O_k which is relatively prime to the discriminant of K/k. Also, $\mathfrak{A}$ is a product of primes to the first power.

Propositions 3 and 4 are combined with the above remarks to give a theorem.

THEOREM 1: *Let K/k be a finite Galois extension of global fields. There are ideals $\mathfrak{A}$ in the ring of integers O_k of k which are prime to the discriminant of K/k such that if ϵ is a (global) unit in O_k and $\epsilon \equiv 1 \pmod{\mathfrak{A}}$, then $\epsilon \in N_{K/k}K^\times$. Let $\mathfrak{A}$ be any such ideal and let L be the maximal abelian extension of K whose conductor divides $\mathfrak{A}$. Then $(k^\times \cap NJ_K)/NK^\times$ is isomorphic to $G(L_z/L_g)$ and, consequently, $i(K/k) = [L_z : L_g]$.*

COROLLARY: *Let L be as in Theorem 1. If M is any abelian*

extension of K such that $L \subset M$ and if the discriminant of M/K is relatively prime to the discriminant of K/k, then

$$i(K/k) = [M_z : M_g].$$

PROOF: Since $L \subset M$, one can find $V'_K = \Pi V'_w$ where $V'_w \subset V_w$ for all w and $V'_w = V_w = U_w$ for all ramified w such that M/K is class field to $K^\times V'_K$. It is clear from the construction that $\delta\beta$ and $\sigma\theta$ are still 0.

REMARKS:

(1) In some cases the construction can be made more explicit. For example, if $k = \mathbb{Q}$, then $F_k = \{\pm 1\}$. Thus the biggest $|\mathrm{Im}\ \tau|$ can be is 2. Indeed, if -1 is a norm from K, then V_k may be taken to be U_k so that L is just the Hilbert class field. If -1 is not a norm from K, take

$$V_K = \prod_{\substack{w \\ \text{archimedean}}} U_w^2 \times \prod_{\substack{w \text{ non-} \\ \text{archimedean}}} U_w.$$

Then -1 is not a local norm at the archimedean primes. For $V_w = \mathbb{C}$ or $V_w = \mathbb{R}^{\times 2}$ and in either case $-1 \notin NV_w$. Thus, by Lemma 2c, $\mathrm{Im}\ \rho = \{+1\}$ and so $|\mathrm{Im}\ \tau\rho| = 1$. It follows that if L is the narrow Hilbert class field of K, then $i(K/k) = [L_z : L_g]$. The results in this remark are originally due to Garbanati [3].

(2) If it is known that $i(K/k) = 1$, the whole construction may be considerably simplified. For if $i(K/k) = 1$, then it is automatic that $\delta\beta = 0$. Thus by (3.1) and Proposition 3, if V_K is simply chosen to satisfy $V_w = U_w$ for all ramified primes, then $[L_z : L_g] = 1$. The arithmetic meaning of this is that if $i(K/k) = 1$ and if L/K is any abelian extension whose discriminant is relatively prime to that of K/k, then $L_z = L_g$. In particular, if K/k is abelian, all non-abelian central extensions L/k of K/k must have some ramified prime of K/k ramify further.

§4. Tate's method

Using the isomorphism from $\hat{H}^q(G, \mathbb{Z})$ onto $\hat{H}^{q+2}(G, C_K)$ induced by the cup product with the canonical class $\alpha \in H^2(G, C_K)$, one gets a fairly computational interpretation of $\mathrm{Im}\ \delta$. This technique, which is due to Tate, is described briefly in his article on global class field theory in [2] (p. 198). Some consequences of this method are described in this section.

The whole idea is contained in the following commutative diagram.

$$\begin{array}{ccc} \coprod_v \hat{H}^{-3}(G_w, \mathbb{Z}) & \xrightarrow{\varphi} & \hat{H}^{-3}(G, \mathbb{Z}) \\ \downarrow{\scriptstyle \amalg \nu\alpha_w} & & \downarrow{\scriptstyle \nu\alpha} \\ \hat{H}^{-1}(G, J_K) = \coprod_v \hat{H}^{-1}(G_w, K_w^{\times}) & \xrightarrow{\theta} & \hat{H}^{-1}(G, C_K). \end{array} \tag{4.1}$$

In this diagram, one prime w of K is chosen over each prime v of k, α_w denotes the canonical class in $\hat{H}^2(G_w, K_w^{\times})$, and α is the canonical class in $H^2(G, C_K)$. The vertical arrows are isomorphisms induced by cup product with the appropriate canonical classes and the horizontal arrow φ takes an element $(\ldots a_w \ldots)$ to $\Sigma_v \operatorname{Cor}_{G^w}^{G}(a_w)$, where $\operatorname{Cor}_{G^w}^{G}$ is the corestriction map. If G_w is cyclic, (as it is for all unramified primes v) $\hat{H}^{-3}(G_w, \mathbb{Z}) = 0$. Thus the direct sum $\amalg_v \hat{H}^{-3}(G_w, \mathbb{Z})$ is finite. Now, since the vertical arrows are isomorphisms, the Cokernels of θ and φ are isomorphic. In particular, since $\operatorname{Coker} \theta = \operatorname{Im} \delta$ (see (2.2)), HNT holds for K/k if and only if φ is surjective and, more generally,

$$i(K/k) = |\operatorname{Coker} \varphi|. \tag{4.2}$$

The group $\hat{H}^{-3}(G, \mathbb{Z}) = H_2(G, \mathbb{Z})$ is called the Schur multiplier. By duality it is isomorphic to $H^2(G, \mathbb{Q}/\mathbb{Z})$. Applying purely group theoretic and homological arguments to the above description of $i(K/k)$ one can prove some facts about Galois extensions for which HNT holds. In particular, for abelian extensions the situation is quite explicit and is discussed in §5.

The following lemma contains some easy homological facts which are used to prove statements about the Hasse norm theorem. For brevity $H_2(G)$ is written for $H_2(G, \mathbb{Z})$.

LEMMA 3:

(a) *If G_1 and G_2 are finite groups of relatively prime order, then $H_2(G_1 \times G_2) = H_2(G_1) \oplus H_2(G_2)$.*

(b) *If G is a group and H is a normal subgroup, then the natural map $H_2(G) \to H_2(G/H)$ is onto if and only if $H \cap [G, G] = [G, H]$. If G, is abelian the map is always onto.*

(c) *If G is a finite abelian p-group (p prime) then the kernel of the natural map $H_2(G) \to H_2(G/pG)$ is $pH_2(G)$.*

PROOF: (a) Standard fact.

(b) From the Lyndon–Hochschild–Serre spectral sequence one deduces the following exact sequence for any group G and normal subgroup H.

$$H_2(G) \longrightarrow H_2(G/H) \longrightarrow \frac{H \cap [G, G]}{[G, H]} \longrightarrow 0. \tag{4.3}$$

If G is abelian, $[G, G] = 0$, so $H_2(G) \to H_2(G/H)$ is surjective.

(c) Suppose $G = C_1 \oplus C_2 \oplus \cdots \oplus C_r$ where the C_i are cyclic p-groups with $|C_i| = p^{n_i}$, $n_1 \leq n_2 \leq \cdots \leq n_r$. Then $pG = pC_1 \oplus pC_2 \oplus \cdots \oplus pC_r$. Iterating the Künneth theorem, one sees that

$$H_2(G) \cong \oplus \sum_{i<j} C_i \oplus C_j \cong \oplus \sum_{i=1}^{r-1} C_i^{r-i},$$

and, since the Künneth exact sequence is natural (the splitting is not used) the map from $H_2(G)$ to $H_2(G/pG)$ is just the obvious term by term map induced by the projections $C_i \to C_i/pC_i$. Thus the kernel is just $\oplus \Sigma_{i=1}^{r-1} (pC_i)^{r-i}$, that is, $pH_2(G)$.

PROPOSITION 5: *Let K_1/k and K_2/k be finite Galois extensions of relatively prime degree. Then $i(K_1K_2/k) = i(K_1/k)i(K_2/k)$. Thus HNT holds for K_1K_2/k if and only if it holds for K_1/k and K_2/k.*

PROOF: Since $[K_1:k]$ and $[K_2:k]$ are relatively prime, K_1K_2/k is Galois with Galois group $G = G_1 \times G_2$ where $G_1 = G(K_1/k)$ and $G_2 = G(K_2/k)$. If w is a prime of K lying over w_1 and w_2 of K_1 and K_2 respectively, then $G_w = (G_1)_{w_1} \times (G_2)_{w_2}$. Thus, by lemma 3a, we have a commutative diagram with vertical isomorphisms

$$\begin{array}{ccc} \coprod_v H_2(G_w) & \xrightarrow{\varphi} & H_2(G) \\ \uparrow & & \uparrow \\ \coprod_v H_2((G_1)_{w_1}) \oplus \coprod_v H_2(G_2)_{w_2}) & \xrightarrow{(\varphi_1, \varphi_2)} & H_2(G_1) \oplus H_2(G_2). \end{array}$$

Since the vertical maps are isomorphisms, Coker φ = Coker $\varphi_1 \oplus$ Coker φ_2 and the result follows.

LEMMA 4: *Let K/k be a Galois extension, $G = G(K/k)$ and H a normal subgroup of G. If the map $H_2(G) \to H_2(G/H)$ is surjective and*

if $E = K^H$ is the fixed field of H, then $i(E/k)$ divides $i(K/k)$ and hence HNT for K/k implies HNT for E/k.

PROOF: First note that $G(E/K) = G/H$. If w is a valuation of K which restricts to w_1 in E, then $(G/H)_{w_1} = G_w/(G_w \cap H)$. Moreover, the following diagram is obviously commutative with exact rows.

$$\begin{array}{ccccccc} \coprod_v H_2(G_w) & \xrightarrow{\varphi} & H_2(G) & \longrightarrow & \operatorname{Coker}\varphi & \longrightarrow & 0 \\ \downarrow & & \downarrow f & & \downarrow g & & \\ \coprod_v H_2(G_w/G_w \cap H) & \xrightarrow{\varphi_1} & H_2(G/H) & \longrightarrow & \operatorname{Coker}\varphi_1 & \longrightarrow & 0 \end{array}$$

The map f is surjective by hypothesis. Thus, g is surjective, and so $i(E/k)$ (the order of Coker φ_1) divides $i(K/k)$ (the order of Coker φ).

PROPOSITION 6: *If K/k is a finite abelian extension, then $i(E/k)$ divides $i(K/k)$ for all subextensions E. In particular, if HNT holds for K/k then it holds for all subextensions E/k.*

PROOF: Lemmas 3b and 4.

PROPOSITION 7: *Let K/k be a finite Galois extension. If E/k is a subextension of K/k such that the degrees $[E:k]$ and $[K:E]$ are relatively prime, then $i(E/k)$ divides $i(K/k)$.*

PROOF: In the exact sequence (4.3), the order of the group $(H \cap [G, G]/[G, H])$ divides the order of H. But the group $H_2(G/H)$ is killed by $|G/H|$, which, by hypothesis, is relatively prime to $|H|$. Since $(H \cap [G, G]/[G, H])$ is a quotient of $H_2(G/H)$, its order must be 1. Thus the map $H_2(G) \to H_2(G/H)$ is onto and Lemma 4 applies.

PROPOSITION 8: *If K_1/k and K_2/k are finite Galois extensions such that $K_1 \cap K_2 = k$ then $i(K_1/k)$ and $i(K_2/k)$ divide $i(K_1K_2/k)$. Thus if HNT holds for K_1K_2/k then it holds for K_1/k and K_2/k.*

PROOF: *If $G = G_1 \times G_2$ and $H = G_1 \times 1$ or $1 \times G_2$ then it is easy to see that $(H \cap [G, G]/[G, H]) = 0$* or, for that matter, to see directly that $H_2(G) \to H_2(G/H)$ is onto.

REMARK: Proposition 5 provides a converse to Proposition 8 in the case where $[K_1:k]$ and $[K_2:k]$ are relatively prime. No general

converse can hold since every abelian extension can be built up from cyclic extensions for which HNT automatically holds.

PROPOSITION 9: *If K/k is an abelian extension of p-power degree, and if K_0/k is the maximum subextension whose Galois group has exponent p, then HNT holds for K/k if and only if it holds for K_0/k.*

PROOF: If $G = G(K/k)$, then $G(K_0/k) = G/pG$ (G written additively). As in the proof of Lemma 4, look at the diagram

$$\begin{array}{ccc} \coprod_v H_2(G_w) & \xrightarrow{\varphi} & H_2(G) \\ \downarrow f & & \downarrow g \\ \coprod_v H_2(G_w/G_w \cap pG) & \xrightarrow{\varphi_1} & H_2(G/pG). \end{array}$$

Since g is surjective, if φ is surjective so is φ_1. By Lemma 3c, g has kernel $pH_2(G)$. Suppose φ_1 is surjective. Since f is surjective (by Lemma 3b), so is $g\varphi$. Thus $\operatorname{Im}\varphi + \operatorname{Ker} g = H_2(G)$ or,

$$\operatorname{Im}\varphi + pH_2(G) = H_2(G).$$

By induction, $\operatorname{Im}\varphi + p^n H_2(G) = H_2(G)$ for all n, and since $H_2(G)$ is a finite p-group, $\operatorname{Im}\varphi = H_2(G)$.

Combining Proposition 5 and Proposition 9 with the fundamental theorem on finite abelian groups reduces the question of whether HNT holds for a given abelian extension to checking whether it holds for all subextensions of prime exponent.

THEOREM 2: *Let K/k be a finite abelian extension, then HNT holds for K/k if and only if HNT holds for every (maximal) subextension of prime exponent.*

§5. Abelian extensions

In the important special case where K/k is abelian, the map $\amalg_v H_2(G_w) \to H_2(G)$ can be described in a very explicit manner – one which is quite amenable to computations in many cases. The key fact is that the homology group $H_2(G)$ is naturally isomorphic to $\Lambda^2 G$ (the second exterior power of G). This fact is probably well-known but a short proof is included here.

LEMMA 5: *If G is a finite abelian group there is a natural isomorphism from $\Lambda^2 G$ to $H_2(G)$.*

PROOF: The natural cup product pairing $H_2(G) \times H^2(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ is non-degenerate and sets the groups $H_2(G)$ and $H^2(G, \mathbb{Q}/\mathbb{Z})$ in perfect duality. Hence it suffices to give a natural isomorphism from $H^2(G, \mathbb{Q}/\mathbb{Z})$ to $\mathrm{Hom}(\Lambda^2 G, \mathbb{Q}/\mathbb{Z})$.

Let $f(\sigma, \tau)$ be a 2-cocycle on G with values in $\mathbb{Q}/\mathbb{Z}$. Then, since G acts trivially on $\mathbb{Q}/\mathbb{Z}$, f satisfies the cocycle identity $f(\sigma\tau, \mu) + f(\sigma, \tau) = f(\sigma, \tau\mu) + f(\tau, \mu)$ which may be rewritten as

$$f(\sigma\tau, \mu) - f(\sigma, \mu) - f(\tau, \mu) = f(\sigma, \tau\mu) - f(\sigma, \tau) - f(\sigma, \mu). \tag{5.1}$$

Since G is abelian, the left side of (5.1) is symmetric in σ and τ and the right side is symmetric in τ and μ. Therefore, the whole expression is fixed by all permutations of σ, τ and μ. Interchange τ and μ on the left side and σ and τ on the right side to get

$$f(\sigma\mu, \tau) - f(\sigma, \tau) - f(\mu, \tau) = f(\tau, \sigma\mu) - f(\tau, \sigma) - f(\tau, \mu). \tag{5.2}$$

Given any 2-cocycle f on G with values in $\mathbb{Q}/\mathbb{Z}$, define

$$f^*(\sigma, \tau) = f(\sigma, \tau) - f(\tau, \sigma) \tag{5.3}$$

for all $\sigma, \tau \in G$. Then by (5.2) f^* is an alternating bilinear map from $G \times G$ to $\mathbb{Q}/\mathbb{Z}$. Define a homomorphism $\varphi_0: Z^2(G, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\Lambda^2 G, \mathbb{Q}/\mathbb{Z})$ by $\varphi_0(f) = f^*$. The kernel of φ_0 consists of all symmetric 2-cocycles and so includes all 2-coboundaries. Hence φ_0 induces a homomorphism

$$\varphi: H^2(G, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\Lambda^2 G, \mathbb{Q}/\mathbb{Z}).$$

The kernel of φ consists of all classes of symmetric cocycles. But symmetric cocycles correspond to *abelian* central extensions of G by $\mathbb{Q}/\mathbb{Z}$. Thus $\mathrm{Ker}\,\varphi = \mathrm{Ext}(G, \mathbb{Q}/\mathbb{Z}) = 0$ and so φ is injective. To see that φ is an isomorphism, express G as a direct sum of cyclic groups and compute the order of $H^2(G, \mathbb{Q}/\mathbb{Z})$ by the Künneth theorem. The order of $\mathrm{Hom}(\Lambda^2 G, \mathbb{Q}/\mathbb{Z})$ is easy to compute directly and is the same. Thus φ is an isomorphism.

It is easy to use this lemma to compute with the map φ of (4.1). Note that since G is abelian, the decomposition group G_w depends

only on v and so G_v is written in place of G_w. The criterion of Tate now takes on the following form.

THEOREM 3: *If K/k is abelian, then $i(K/k)$ is equal to the order of the Cokernel of the map*

$$\varphi: \coprod_v \Lambda^2 G_v \longrightarrow \Lambda^2 G$$

(where the product is over primes v dividing the discriminant of K/k) given by $\varphi(\ldots, \sigma_v \wedge \tau_v, \ldots) = \Sigma_v \sigma_v \wedge \tau_v$. In particular φ is surjective if and only if HNT holds for K/k.

PROOF: Diagram (4.1) and Lemma 5.

Finally we give two examples of explicit number theoretic conditions which are equivalent to the HNT for certain kinds of extensions.

EXAMPLE 1: Let K/k have Galois group $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (p a prime). Then HNT holds for K/k if and only if there is a prime v of k which is the power of a prime of K.

PROOF: The only choice for a decomposition group G_v is G or $\mathbb{Z}/p\mathbb{Z}$. In the latter case $H_2(G_v) = \Lambda^2 G_v = 0$. In the former case the map φ is onto.

EXAMPLE 2: Let K/k have Galois group $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then HNT for K/k if and only if *either*

(a) There is a prime v of k which is a power of a prime of K.

(b) Every prime of k lies below more than one (p or p^2 or p^3) prime of K but there are primes v_1, v_2, v_3 of k with distinct decomposition groups such that the three groups $\{G_{v_i} \cap G_{v_j}\}$ $(i \neq j)$ span G.

PROOF: Clearly (a) implies the HNT. If (b) holds then each G_{v_i} has order p^2 and there is a basis of G $\{x, y, z\}$ such that $x \in G_{v_1} \cap G_{v_2}$, $y \in G_{v_1} \cap G_{v_3}$, $z \in G_{v_2} \cap G_{v_3}$. Thus $x \wedge y \in \Lambda^2 G_{v_1}$, $x \wedge z \in \Lambda^2 G_{v_2}$ and $y \wedge z \in \Lambda^2 G_{v_3}$ and so $\Sigma \Lambda^2 G_v = \Lambda^2 G$.

Conversely, if $\Sigma \Lambda^2 G_v = \Lambda^2 G$, then either some $G_v = G$ or else there are three primes v_1, v_2, v_3 of k such that G_{v_i} has order p^2 $(i = 1, 2, 3)$ and such that $\Lambda^2 G_{v_1} + \Lambda^2 G_{v_2} + \Lambda^2 G_{v_3} = \Lambda^2 G$. Now $G_{v_i} \neq G_{v_j}$, so $G_{v_i} \cap G_{v_j}$

is one dimensional. Let x, y and z span $G_{v_1} \cap G_{v_2}$, $G_{v_1} \cap G_{v_3}$ and $G_{v_2} \cap G_{v_3}$ respectively. Then x, y, z must be linearly independent in order that $\Lambda^2 G_{v_1} + \Lambda^2 G_{v_2} + \Lambda^2 G_{v_3} = \Lambda^2 G$.

REFERENCES

[1] E. ARTIN and J. TATE: *Class Field Theory.*

[2] J.W.S. CASSELS and A. FROHLICH: *Algebraic Number Theory.* Thompson Book Company, Washington D.C. (1967).

[3] D. GARBANATI: The Hasse norm theorem for non-cyclic extensions of the rational. Proceedings of London Math. Soc. (to appear).

[4] D. GARBANATI: The Hasse norm theorem for l-extensions of the rationals. Journal of Number Theory. (to appear)

(Oblatum 11-VII-1976)

Department of Mathematics
University of Maryland
College Park, Maryland 20742
U.S.A.