ACTA ARITHMETICA
108.4 (2003)

Relations among certain number knots

by

Kuniaki Horie (Hiratsuka) and Mitsuko Horie (Tokyo)

Let k be a global field, namely, either a finite extension over the field of rational numbers or an algebraic function field in one variable over a finite constant field. Let Ω be a separable algebraic closure of k. From now on, we assume all global fields to be contained in Ω. For each global field E, let J_E denote the idele group of E, and $E^\times$ the multiplicative group of E. We then consider $E^\times$ to be a subgroup of J_E by means of the canonical injection $E^\times \to J_E$. Given any finite Galois extension F over k contained in Ω, we write $N_{F/k}$ for the norm map $J_F \to J_k$ so that the restriction $N_{F/k}|F^\times$ coincides with the norm map $F^\times \to k^\times$. The *number knot* of F/k is defined as the quotient group of $k^\times \cap N_{F/k}(J_F)$ modulo $N_{F/k}(F^\times)$, and we denote it simply by $\nu(F)$:

$$\nu(F) = (k^\times \cap N_{F/k}(J_F))/N_{F/k}(F^\times).$$

In general, the abelian group $\nu(F)$ is known to be finite: $|\nu(F)| < \infty$. On the other hand, the so-called Hasse norm theorem states that if F/k is a cyclic extension, then

$$\nu(F) = 1, \quad \text{i.e.,} \quad k^\times \cap N_{F/k}(J_F) = N_{F/k}(F^\times).$$

A global field E is called a *central extension* of F/k if E is a Galois extension over k containing F such that the Galois group $\mathrm{Gal}(E/F)$ lies in the centre of the Galois group $\mathrm{Gal}(E/k)$. In particular, a central extension of F/k is abelian over F. It follows that the composite of F and any finite abelian extension over k in Ω is a central extension of F/k. Hence, for any abelian extension k' over k in Ω, each finite extension over F in the composite Fk' is a central extension of F/k.

Now, let L/K be an extension of global fields which are Galois extensions over k so that L/K is a finite Galois extension. We then define the *natural map* $\nu(L) \to \nu(K)$ to be the homomorphism from $\nu(L)$ into $\nu(K)$ induced by the canonical injection $k^\times \cap N_{L/k}(J_L) \to k^\times \cap N_{K/k}(J_K)$. In this paper, we shall mainly prove the following results.

2000 *Mathematics Subject Classification*: Primary 11R56; Secondary 11R23, 20J05.

Theorem 1. *L/K being as above, assume that every central extension of K/k in L is a subfield of the composite of K and the maximal abelian extension over k in L. Then the natural map $\nu(L) \to \nu(K)$ is surjective*:

$$k^\times \cap N_{K/k}(J_K) = (k^\times \cap N_{L/k}(J_L))N_{K/k}(K^\times).$$

Consequently, in the case where L is the composite of K and an abelian extension over k, the natural map $\nu(L) \to \nu(K)$ is surjective.

Theorem 2. *Let K and k' be global fields such that K is a Galois extension over k and k' an abelian extension over k not contained in K; $Kk' \neq K$. For each prime number p, let $\mathfrak{K}_p$ denote the maximal intermediate field of the abelian extension Kk'/K such that* $\mathrm{Gal}(\mathfrak{K}_p/K)^p = 1$:

$$\mathrm{Gal}(Kk'/\mathfrak{K}_p) = \mathrm{Gal}(Kk'/K)^p.$$

Then $\nu(Kk') = 1$ if and only if $\nu(\mathfrak{K}_p) = 1$ for all prime numbers p dividing $[Kk' : K]$. Furthermore, in the case where $[Kk' : K]$ is a power of some prime number q, $\nu(L) = 1$ for every intermediate field L of Kk'/K if and only if $\nu(L) = 1$ for some intermediate field L of $Kk'/\mathfrak{K}_q$.

Theorem 3. *Let K be a finite Galois extension over k in Ω, and k' a cyclic extension over k in Ω. Let t denote the exponent of* $\mathrm{Gal}(K/k)$. *Then, for any extension E/F of intermediate fields of Kk'/K with*

$$\gcd(t, [E : K]) = \gcd(t, [F : K]),$$

the natural map $\nu(E) \to \nu(F)$ is an isomorphism, so that

$$N_{F/k}(F^\times) \cap N_{E/k}(J_E) = N_{E/k}(E^\times).$$

Owing much to cohomological arguments of Razar [7], we shall base our discussions upon the explicit description of the relation between number knots made by means of the Hopf formula for Schur multipliers. We should note that an essential part of Theorem 2 for the case $K = k$ is given by Gerth [2] and [7]. In addition, since $\nu(k) = 1$, Theorem 3 for the case $K = k$ coincides with the Hasse norm theorem. Among immediate consequences of Theorems 2 and 3 are the following results on Iwasawa-theoretical extensions of global fields.

Corollary 1. *Let K be a finite Galois extension over k in Ω. Given any prime number p, let $\mathbb{Z}_p$ denote as usual the ring of p-adic integers, and let k_∞ be a $\mathbb{Z}_p$-extension over k in Ω (namely, an abelian extension over k in Ω whose Galois group over k is isomorphic to the additive group of $\mathbb{Z}_p$ as a topological group). Let*

$$K = K^{(0)} \subset \ldots \subset K^{(n)} \subset K^{(n+1)} \subset \ldots \subset Kk_\infty$$

be the tower of all intermediate fields of the $\mathbb{Z}_p$*-extension* Kk_∞/K *such that* $[K^{(n)} : K] = p^n$, *with* n *ranging over the non-negative integers. Then*

$$\nu(K^{(n)}) = 1 \quad \textit{for all } n \geq 0$$

if and only if

$$\nu(K^{(n)}) = 1 \quad \textit{for some } n \geq 1.$$

COROLLARY 2. *Let* K *be a finite Galois extension over* k *in* Ω *as in Corollary* 1, *and let* t *denote the exponent of* $\mathrm{Gal}(K/k)$. *Let* $\widehat{\mathbb{Z}}$ *denote the direct product of* $\mathbb{Z}_p$ *for all prime numbers* p, *and let* $\widetilde{k}$ *be an abelian extension over* k *in* Ω *such that* $\mathrm{Gal}(\widetilde{k}/k)$ *is isomorphic to the additive group of* $\widehat{\mathbb{Z}}$ *as a topological group*: $\mathrm{Gal}(\widetilde{k}/k) \cong \widehat{\mathbb{Z}}$. *Then*, *for every extension* E/F *of global fields with*

$$K \subseteq F, \quad E \subset K\widetilde{k}, \quad \gcd(t, [E:K]) = \gcd(t, [F:K]),$$

the natural map $\nu(E) \to \nu(F)$ *is an isomorphism.*

COROLLARY 3. *Under the assumption of Corollary* 2, *let* Γ *be any infinite extension over* K *in* $K\widetilde{k}$. *Let* K_Γ *denote the maximal intermediate field of* Γ/K *such that* $[K_\Gamma : K]$ *divides* t. *Then*, *for every global field* L *with* $K_\Gamma \subseteq L \subset \Gamma$, *the natural map* $\nu(L) \to \nu(K_\Gamma)$ *is an isomorphism. In particular*, *when* p, k_∞, *and* $K^{(n)}$ *for all integers* $n \geq 0$ *are the same as in Corollary* 1, *the natural map* $\nu(K^{(m')}) \to \nu(K^{(m)})$ *is an isomorphism for every pair* (m, m') *of integers with* $0 \leq m \leq m'$ *such that* p^{m+1} *does not divide the exponent of* $\mathrm{Gal}(K/k)$.

1. In this section and the next, we shall discuss some preliminary results for the proofs in Section 3. Let H be any finite group. For each positive integer n, let $\mathbb{P}_n(H)$ denote the free module with a basis the direct product of n copies of H. Now, let us take the homomorphisms

$$\partial : \mathbb{P}_3(H) \to \mathbb{P}_2(H), \quad \partial' : \mathbb{P}_2(H) \to \mathbb{P}_1(H)$$

such that

$$\begin{aligned} \partial((\sigma_1, \sigma_2, \sigma_3)) &= (\sigma_2, \sigma_3) - (\sigma_1\sigma_2, \sigma_3) + (\sigma_1, \sigma_2\sigma_3) - (\sigma_1, \sigma_2), \\ \partial'((\sigma_1, \sigma_2)) &= \sigma_2 - \sigma_1\sigma_2 + \sigma_1 \end{aligned}$$

for every $(\sigma_1, \sigma_2, \sigma_3) \in H \times H \times H$. Noting that $\mathrm{Im}(\partial) \subseteq \mathrm{Ker}(\partial')$, we put

$$M(H) = \mathrm{Ker}(\partial')/\mathrm{Im}(\partial).$$

This is called the *Schur multiplier* of H and is nothing but the second homology group of H with coefficients in the additive group $\mathbb{Z}$ of (rational) integers where we understand that H acts trivially on $\mathbb{Z}$. Next, let $\pi : \mathcal{F} \to H$ be a free presentation of H, that is, let $\mathcal{F}$ be a free group and π a homomorphism of $\mathcal{F}$ onto H. Put $\mathcal{R} = \mathrm{Ker}(\pi)$, so that $[\mathcal{F}, \mathcal{R}]$ (i.e. the subgroup of

$\mathcal{F}$ generated by $[x,y]=xyx^{-1}y^{-1}$ for all $x\in\mathcal{F}$ and all $y\in\mathcal{R}$) is a normal subgroup of the groups $\mathcal{F}$, $[\mathcal{F},\mathcal{F}]$ and $\mathcal{R}$. For each σ in H, take an element x_σ of $\mathcal{F}$ with $\pi(x_\sigma)=\sigma$. The Hopf formula for the Schur multiplier $M(H)$ can be stated explicitly as follows (cf. Eilenberg–MacLane [1], Karpilovsky [5, Ch. 2], Robinson [8, Ch. 11]):

Lemma 1. *Let f be the homomorphism $\mathbb{P}_2(H)\to\mathcal{R}/[\mathcal{F},\mathcal{R}]$ mapping each $(\sigma,\tau)\in H\times H$ to $x_\sigma x_\tau x_{\sigma\tau}^{-1}[\mathcal{F},\mathcal{R}]$. Then*

$$f(\mathrm{Ker}(\partial'))=([\mathcal{F},\mathcal{F}]\cap\mathcal{R})/[\mathcal{F},\mathcal{R}],\qquad \mathrm{Ker}(f)\cap\mathrm{Ker}(\partial')=\mathrm{Im}(\partial),$$

$f|\mathrm{Ker}(\partial')$ does not depend on the choice of $\{x_\sigma\mid\sigma\in H\}$, and hence f defines an isomorphism

$$\widetilde{\pi}:M(H)\xrightarrow{\sim}([\mathcal{F},\mathcal{F}]\cap\mathcal{R})/[\mathcal{F},\mathcal{R}]$$

that depends only on π.

Proof. Let $\mathcal{F}_0$ be the free group freely generated by $|H|$ symbols X_σ for all $\sigma\in H$, let ω be the homomorphism $\mathcal{F}_0\to H$ such that $\omega(X_\sigma)=\sigma$ for all $\sigma\in H$, and let $\mathcal{R}_0=\mathrm{Ker}(\omega)$. Let g be the homomorphism $\mathbb{P}_2(H)\to\mathcal{R}_0/[\mathcal{R}_0,\mathcal{R}_0]$ mapping each $(\sigma,\tau)\in H\times H$ to $X_\sigma X_\tau X_{\sigma\tau}^{-1}[\mathcal{R}_0,\mathcal{R}_0]$. Then g turns out to be an isomorphism, because $\mathcal{R}_0$ is a free group freely generated by its $|H|^2$ elements $X_\sigma X_\tau X_{\sigma\tau}^{-1}$ for all $(\sigma,\tau)\in H\times H$ (see, e.g., [5, Theorem 2.7.1(iii)]). Next, take an element

$$\alpha=\sum_{\sigma,\tau\in H}a_{\sigma,\tau}(\sigma,\tau)$$

of $\mathbb{P}_2(H)$, with each $a_{\sigma,\tau}$ in $\mathbb{Z}$. For each $\tau\in H$, we put

$$b_\tau=\sum_{\sigma\in H}(a_{\sigma,\tau}-a_{\sigma,\sigma^{-1}\tau}+a_{\tau,\sigma}).$$

It follows that α belongs to $\mathrm{Ker}(\partial')$ if and only if

$$b_\tau=0\quad\text{for every }\tau\in H.\tag{1}$$

Since the homomorphism $\mathcal{R}_0/[\mathcal{R}_0,\mathcal{R}_0]\to\mathcal{F}_0/[\mathcal{F}_0,\mathcal{F}_0]$ induced by the inclusion $\mathcal{R}_0\to\mathcal{F}_0$ maps $g(\alpha)$ to

$$\prod_{\sigma,\tau\in H}(X_\sigma X_\tau X_{\sigma\tau}^{-1})^{a_{\sigma,\tau}}[\mathcal{F}_0,\mathcal{F}_0]=\prod_{\tau\in H}(X_\tau[\mathcal{F}_0,\mathcal{F}_0])^{b_\tau},$$

it also follows that the condition $g(\alpha)\in([\mathcal{F}_0,\mathcal{F}_0]\cap\mathcal{R}_0)/[\mathcal{R}_0,\mathcal{R}_0]$ is equivalent to (1). Hence we have

$$g(\mathrm{Ker}(\partial'))=([\mathcal{F}_0,\mathcal{F}_0]\cap\mathcal{R}_0)/[\mathcal{R}_0,\mathcal{R}_0].$$

Furthermore, for each $(\varrho,\sigma,\tau)\in H\times H\times H$,

$$\begin{aligned}g(\partial((\varrho,\sigma,\tau)))&=X_\sigma X_\tau X_{\sigma\tau}^{-1}X_\varrho X_{\sigma\tau}X_{\varrho\sigma\tau}^{-1}X_{\varrho\sigma\tau}X_\tau^{-1}X_{\varrho\sigma}^{-1}X_{\varrho\sigma}X_\sigma^{-1}X_\varrho^{-1}[\mathcal{R}_0,\mathcal{R}_0]\\&=(X_\sigma X_\tau X_{\sigma\tau}^{-1})X_\varrho(X_\sigma X_\tau X_{\sigma\tau}^{-1})^{-1}X_\varrho^{-1}[\mathcal{R}_0,\mathcal{R}_0],\end{aligned}$$

so that

$$g(\mathrm{Im}(\partial)) = [\mathcal{F}_0, \mathcal{R}_0]/[\mathcal{R}_0, \mathcal{R}_0].$$

Now let h be the composite of g and the natural homomorphism $\mathcal{R}_0/[\mathcal{R}_0, \mathcal{R}_0] \to \mathcal{R}_0/[\mathcal{F}_0, \mathcal{R}_0]$. Then, from the above properties of g, we obtain

$$(2) \qquad h(\mathrm{Ker}(\partial')) = ([\mathcal{F}_0, \mathcal{F}_0] \cap \mathcal{R}_0)/[\mathcal{F}_0, \mathcal{R}_0], \quad \mathrm{Ker}(h) = \mathrm{Im}(\partial).$$

We denote by ϕ the homomorphism $\mathcal{F}_0 \to \mathcal{F}$ such that $\phi(X_\sigma) = x_\sigma$ for every $\sigma \in H$, namely, $\pi \circ \phi = \omega$. On the other hand, since $\mathcal{F}$ is a free group and ω is surjective, there exists a homomorphism $\psi : \mathcal{F} \to \mathcal{F}_0$ which satisfies $\omega \circ \psi = \pi$. Naturally, ψ defines a homomorphism

$$\overline{\psi} : ([\mathcal{F}, \mathcal{F}] \cap \mathcal{R})/[\mathcal{F}, \mathcal{R}] \to ([\mathcal{F}_0, \mathcal{F}_0] \cap \mathcal{R}_0)/[\mathcal{F}_0, \mathcal{R}_0]$$

while ϕ defines a homomorphism

$$\overline{\phi} : ([\mathcal{F}_0, \mathcal{F}_0] \cap \mathcal{R}_0)/[\mathcal{F}_0, \mathcal{R}_0] \to ([\mathcal{F}, \mathcal{F}] \cap \mathcal{R})/[\mathcal{F}, \mathcal{R}].$$

We then easily find that $\overline{\psi} \circ \overline{\phi}$ is the identity map on $([\mathcal{F}_0, \mathcal{F}_0] \cap \mathcal{R}_0)/[\mathcal{F}_0, \mathcal{R}_0]$, $\overline{\phi} \circ \overline{\psi}$ is the identity map on $([\mathcal{F}, \mathcal{F}] \cap \mathcal{R})/[\mathcal{F}, \mathcal{R}]$, $\overline{\phi}$ does not depend on the choice of $\{x_\sigma \mid \sigma \in H\}$, and

$$f|\mathrm{Ker}(\partial') = \overline{\phi} \circ (h|\mathrm{Ker}(\partial')).$$

Because of (2), the assertions of the lemma follow immediately from these facts. ∎

Next, let H_1 and H_2 be finite groups such that there exists a surjective homomorphism $\lambda : H_1 \to H_2$. Let $\theta : \mathcal{E} \to H_1$ be a free presentation of H_1. Then the composite $\lambda \circ \theta : \mathcal{E} \to H_2$ is a free presentation of H_2. One can therefore apply Lemma 1 to the case $\pi = \lambda \circ \theta$ as well as to the case $\pi = \theta$. Clearly, the homomorphism $\mathbb{P}_2(H_1) \to \mathbb{P}_2(H_2)$ mapping each $(\sigma, \tau) \in H_1 \times H_1$ to $(\lambda(\sigma), \lambda(\tau))$ defines a homomorphism

$$\lambda^* : M(H_1) \to M(H_2),$$

which is called the *residuation map* for λ (cf. Nakayama [6]). Put

$$\mathcal{R}_1 = \mathrm{Ker}(\theta), \quad \mathcal{R}_2 = \mathrm{Ker}(\lambda \circ \theta),$$

so that $\mathcal{R}_1 \subseteq \mathcal{R}_2$. The inclusion $[\mathcal{E}, \mathcal{E}] \cap \mathcal{R}_1 \to [\mathcal{E}, \mathcal{E}] \cap \mathcal{R}_2$ then induces a homomorphism

$$j : ([\mathcal{E}, \mathcal{E}] \cap \mathcal{R}_1)/[\mathcal{E}, \mathcal{R}_1] \to ([\mathcal{E}, \mathcal{E}] \cap \mathcal{R}_2)/[\mathcal{E}, \mathcal{R}_2].$$

LEMMA 2. *The diagram*

$$\begin{array}{ccc} M(H_1) & \xrightarrow{\widetilde{\theta}} & ([\mathcal{E}, \mathcal{E}] \cap \mathcal{R}_1)/[\mathcal{E}, \mathcal{R}_1] \\ {\scriptstyle\lambda^*}\downarrow & & \downarrow{\scriptstyle j} \\ M(H_2) & \xrightarrow{\widetilde{\lambda\circ\theta}} & ([\mathcal{E}, \mathcal{E}] \cap \mathcal{R}_2)/[\mathcal{E}, \mathcal{R}_2] \end{array}$$

is commutative. Furthermore, there exists an exact sequence

$$M(H_1) \xrightarrow{\lambda^*} M(H_2) \to ([H_1, H_1] \cap \mathrm{Ker}(\lambda))/[H_1, \mathrm{Ker}(\lambda)] \to 1.$$

Proof. It is not difficult to deduce the first part from Lemma 1. As

$$\theta([\mathcal{E}, \mathcal{E}] \cap \mathcal{R}_2) = [H_1, H_1] \cap \mathrm{Ker}(\lambda),$$

θ induces a surjective homomorphism

$$([\mathcal{E}, \mathcal{E}] \cap \mathcal{R}_2)/[\mathcal{E}, \mathcal{R}_2] \to ([H_1, H_1] \cap \mathrm{Ker}(\lambda))/[H_1, \mathrm{Ker}(\lambda)].$$

However, using $\theta(\mathcal{R}_2) = \mathrm{Ker}(\lambda)$, we easily check that the kernel of the above homomorphism is

$$([\mathcal{E}, \mathcal{E}] \cap \mathcal{R}_1)[\mathcal{E}, \mathcal{R}_2]/[\mathcal{E}, \mathcal{R}_2] = \mathrm{Im}(j).$$

Hence the second part follows from the first and Lemma 1 (cf. [8, Ch. 11]). ∎

2. Let F be any global field which is a Galois extension over k. Let G_F denote the Galois group of F over k: $G_F = \mathrm{Gal}(F/k)$. Note that the natural action of G_F on J_F makes the idele class group $J_F/F^\times$ of F into a G_F-module. In $J_F/F^\times$, let

$$A_F = \{uF^\times \mid u \in J_F,\ N_{F/k}(u) \in k^\times\},$$

and let B_F denote the group generated by $(uF^\times)^{\sigma-1} = u^\sigma u^{-1} F^\times$ for all $(u, \sigma) \in J_F \times G_F$. Then A_F is a subgroup of $J_F/F^\times$ containing B_F, and the quotient A_F/B_F is none other than the Tate cohomology group of G_F in dimension -1 with coefficients in $J_F/F^\times$. Let P be the set of all primes of k. For each $v \in P$, we fix a prime $\overline{v}$ of Ω lying above v, denote by G_F^v the decomposition group of $\overline{v}|F$ for F/k, and denote by Cor_F^v the corestriction map $M(G_F^v) \to M(G_F)$. Let γ_F denote the homomorphism from the direct sum $\bigoplus_{v \in P} M(G_F^v)$ into $M(G_F)$ such that

$$\gamma_F((c_v)_{v \in P}) = \sum_{v \in P} \mathrm{Cor}_F^v(c_v) \quad \text{for each } (c_v)_{v \in P} \in \bigoplus_{v \in P} M(G_F^v).$$

Then, as is well known, the composite of the so-called Tate isomorphism $M(G_F) \xrightarrow{\sim} A_F/B_F$ and the homomorphism $A_F/B_F \to \nu(F)$ induced by $N_{F/k}$ gives rise to an isomorphism

$$\mathrm{Coker}(\gamma_F) \xrightarrow{\sim} \nu(F).$$

We write Ψ_F for this isomorphism.

Now, let L be any finite Galois extension over k in Ω, and K any Galois extension over k in L. Let $R(L/K)$ denote the residuation map $M(G_L) \to M(G_K)$ for the restriction map $G_L \to G_K$ (i.e., the homomorphism from G_L onto G_K mapping each $\sigma \in G_L$ to $\sigma|K$). Given any $v \in P$, let $R_{L/K}^v$ denote the residuation map $M(G_L^v) \to M(G_K^v)$ for the restriction map $G_L^v \to G_K^v$.

Then the diagram

$$\begin{tikzcd} M(G_L^v) \arrow[r, "\mathrm{Cor}_L^v"] \arrow[d, "R_{L/K}^v"'] & M(G_L) \arrow[d, "R(L/K)"] \\ M(G_K^v) \arrow[r, "\mathrm{Cor}_K^v"] & M(G_K) \end{tikzcd}$$

is commutative, since Cor_L^v and Cor_K^v are induced by the inclusions $G_L^v \to G_L$ and $G_K^v \to G_K$, respectively. We therefore obtain a commutative diagram

$$\begin{tikzcd} \bigoplus_{v\in P} M(G_L^v) \arrow[r, "\gamma_L"] \arrow[d] & M(G_L) \arrow[d, "R(L/K)"] \\ \bigoplus_{v\in P} M(G_K^v) \arrow[r, "\gamma_K"] & M(G_K) \end{tikzcd} \tag{3}$$

Here the left vertical arrow is the homomorphism, from $\bigoplus_{v\in P} M(G_L^v)$ into $\bigoplus_{v\in P} M(G_K^v)$, mapping each $(c_v)_{v\in P}$ in $\bigoplus_{v\in P} M(G_L^v)$ to $(R_{L/K}^v(c_v))_{v\in P}$. Thus $R(L/K)$ induces a homomorphism

$$\mathrm{Coker}(\gamma_L) \to \mathrm{Coker}(\gamma_K).$$

We denote this by $\varrho_{L/K}$. The following result is essentially well known (cf. Jehne [4], Kuniyoshi [9, §4]; for a proof, see [3]):

LEMMA 3. *With the symbol (L/K) denoting the natural map $\nu(L) \to \nu(K)$, the diagram*

$$\begin{tikzcd} \mathrm{Coker}(\gamma_L) \arrow[r, "\Psi_L", "\sim"'] \arrow[d, "\varrho_{L/K}"'] & \nu(L) \arrow[d, "(L/K)"] \\ \mathrm{Coker}(\gamma_K) \arrow[r, "\Psi_K", "\sim"'] & \nu(K) \end{tikzcd}$$

is commutative.

3. Let us prove the theorems stated in the introduction.

Proof of Theorem 1. Let $N = \mathrm{Gal}(L/K)$. Then $[G_L, N] \subseteq [G_L, G_L] \cap N$, and hence the assumption of Theorem 1 means that $[G_L, N] = [G_L, G_L] \cap N$. Indeed (by Galois theory), $[G_L, N]$ is the Galois group of L over a central extension of K/k in L, and $[G_L, G_L] \cap N$ coincides with the Galois group of L over the composite of K and the maximal abelian extension over k in L. It therefore follows from Lemma 2 that the residuation map $R(L/K)$ is surjective (cf. [7, Lemma 3]), so that $\varrho_{L/K}$ is also surjective. Hence Lemma 3 proves Theorem 1. ∎

To give a proof of Theorem 2, we first prove two lemmas under the assumption of Theorem 2.

LEMMA 4. *Let E/F be an extension of intermediate fields of Kk'/K. Then $R(E/F)$ is surjective. Moreover, for every $v \in P$, $R^v_{E/F}$ is surjective.*

Proof. We may just consider the case where E/F coincides with Kk'/K; because F/k is a Galois extension, $E = Fk''$ for some intermediate field k'' of k'/k, and obviously, for any finite group H, the residuation map $M(H) \to M(H)$ for the identity map $H \to H$ is an identity map. Let v be any prime of k, and let N^v denote the kernel of the restriction map $G^v_{Kk'} \to G^v_K$. As $[G_{Kk'}, G_{Kk'}] \cap \mathrm{Gal}(Kk'/K) = 1$ by the assumption that k'/k is abelian, we obtain $[G^v_{Kk'}, G^v_{Kk'}] \cap N^v = 1$ from $N^v \subseteq \mathrm{Gal}(Kk'/K)$. Lemma 2 therefore proves that $R(Kk'/K)$ and $R^v_{Kk'/K}$ are surjective. ∎

LEMMA 5. *For any prime number p,*

$$pM(G_{Kk'}) \supseteq \mathrm{Ker}(R(Kk'/\mathfrak{K}_p)).$$

Proof. Let $\pi : \mathcal{F} \to G_{Kk'}$ be a free presentation of $G_{Kk'}$ and let $\mathcal{R} = \mathrm{Ker}(\pi)$. For any Galois extension L over k in Kk', we let $\mathcal{S}(L)$ denote the kernel of the composite of π and the restriction map $G_{Kk'} \to G_L$. Then π induces an isomorphism $\mathcal{S}(L)/\mathcal{R} \xrightarrow{\sim} \mathrm{Gal}(Kk'/L)$, while Lemma 2 gives us a commutative diagram

$$\begin{array}{ccc} M(G_{Kk'}) & \xrightarrow{\widetilde{\pi}} & ([\mathcal{F},\mathcal{F}] \cap \mathcal{R})/[\mathcal{F},\mathcal{R}] \\ {\scriptstyle R(Kk'/\mathfrak{K}_p)}\big\downarrow & & \big\downarrow \\ M(G_{\mathfrak{K}_p}) & \xrightarrow{\widetilde{\omega_p}} & ([\mathcal{F},\mathcal{F}] \cap \mathcal{S}(\mathfrak{K}_p))/[\mathcal{F},\mathcal{S}(\mathfrak{K}_p)] \end{array}$$

where ω_p denotes the free presentation of $G_{\mathfrak{K}_p}$ defined as the composite of π and the restriction map $G_{Kk'} \to G_{\mathfrak{K}_p}$, and the vertical map on the right is the homomorphism induced by the inclusion $[\mathcal{F},\mathcal{F}] \cap \mathcal{R} \to [\mathcal{F},\mathcal{F}] \cap \mathcal{S}(\mathfrak{K}_p)$. Therefore, the assertion of Lemma 5 is equivalent to

$$([\mathcal{F},\mathcal{S}(\mathfrak{K}_p)] \cap \mathcal{R})/[\mathcal{F},\mathcal{R}] \subseteq (([\mathcal{F},\mathcal{F}] \cap \mathcal{R})/[\mathcal{F},\mathcal{R}])^p. \tag{4}$$

As $\mathrm{Gal}(Kk'/\mathfrak{K}_p) = \mathrm{Gal}(Kk'/K)^p$, i.e., $\mathcal{S}(\mathfrak{K}_p)/\mathcal{R} = (\mathcal{S}(K)/\mathcal{R})^p$, we obtain

$$\mathcal{S}(\mathfrak{K}_p) = \{y^p z \mid y \in \mathcal{S}(K),\ z \in \mathcal{R}\}.$$

Now, take any $x \in \mathcal{F}$, $y \in \mathcal{S}(K)$, and $z \in \mathcal{R}$. Then

$$[x, y^p z] = xy^p z x^{-1} z^{-1} y^{-p} \in xy^p x^{-1} y^{-p} [\mathcal{F},\mathcal{R}] = ([x,y]y)^p y^{-p} [\mathcal{F},\mathcal{R}].$$

We also see, by the fact $\pi(y) \in \mathrm{Gal}(Kk'/K)$, that

$$\pi([x,y]) \in [G_{Kk'}, \mathrm{Gal}(Kk'/K)] \subseteq [G_{Kk'}, G_{Kk'}] \cap \mathrm{Gal}(Kk'/K) = 1.$$

Therefore, $[x,y]$ belongs to $\mathcal{R}$ so that $([x,y]y)^p y^{-p}[\mathcal{F},\mathcal{R}] = [x,y]^p[\mathcal{F},\mathcal{R}]$. Consequently, we have

$$[x, y^p z] \in [x,y]^p [\mathcal{F},\mathcal{R}], \qquad [x,y] \in [\mathcal{F},\mathcal{F}] \cap \mathcal{R}.$$

Since (4) follows from these, the lemma is proved. ∎

Proof of Theorem 2. Let F be any intermediate field of Kk'/K such that

$$\mathrm{Coker}(\gamma_F) = 1, \quad \text{i.e.,} \quad \nu(F) = 1.$$

Since Lemma 4 implies that $R^v_{Kk'/F}$ is surjective for every $v \in P$, (3) yields a commutative diagram

$$\begin{array}{ccc} \bigoplus_{v\in P} M(G^v_{Kk'}) & \xrightarrow{\gamma_{Kk'}} & M(G_{Kk'}) \\ \downarrow & & \downarrow{\scriptstyle R(Kk'/F)} \\ \bigoplus_{v\in P} M(G^v_F) & \xrightarrow{\gamma_F} & M(G_F) \end{array}$$

in which the vertical map on the left is surjective. Hence $R(Kk'/F)\circ\gamma_{Kk'}$ is surjective. It thus follows that $M(G_{Kk'})$ is generated by the image of $\gamma_{Kk'}$ and the kernel of $R(Kk'/F)$:

$$M(G_{Kk'}) = \mathrm{Im}(\gamma_{Kk'}) + \mathrm{Ker}(R(Kk'/F)). \tag{5}$$

Next, let q be a prime number dividing $[Kk' : K]$. Note that such a prime q certainly exists by $Kk' \neq K$. We then see from Theorem 1 that the natural map $\nu(\mathfrak{K}_q) \to \nu(K)$ is surjective. In particular,

$$\nu(K) = 1 \quad \text{if } \nu(\mathfrak{K}_q) = 1. \tag{6}$$

Now, we assume that $\nu(\mathfrak{K}_p) = 1$ for all prime numbers p dividing $[Kk' : K]$. As $\mathfrak{K}_p = K$ for any prime number p not dividing $[Kk' : K]$, we have, by (5) and (6),

$$M(G_{Kk'}) = \mathrm{Im}(\gamma_{Kk'}) + \mathrm{Ker}(R(Kk'/\mathfrak{K}_p))$$

for every prime number p. Therefore, Lemma 5 shows that

$$M(G_{Kk'}) = \mathrm{Im}(\gamma_{Kk'}) + pM(G_{Kk'})$$

for every prime number p, so that we have, by induction,

$$M(G_{Kk'}) = \mathrm{Im}(\gamma_{Kk'}) + nM(G_{Kk'})$$

for every positive integer n. However, $|G_{Kk'}|M(G_{Kk'}) = 0$. Hence

$$M(G_{Kk'}) = \mathrm{Im}(\gamma_{Kk'}), \quad \text{i.e.,} \quad \mathrm{Coker}(\gamma_{Kk'}) = 1.$$

This just shows $\nu(Kk') = 1$.

Conversely, it follows from Theorem 1 that if $\nu(Kk') = 1$, then $\nu(\mathfrak{K}_p) = 1$ for every prime number p dividing $[Kk' : k]$. The first assertion of Theorem 2 is therefore proved.

Suppose now that $[Kk' : K]$ is a power of a prime number q and that $\nu(L) = 1$ for some intermediate field L of $Kk'/\mathfrak{K}_q$. Then $\nu(\mathfrak{K}_q) = 1$ by Theorem 1. Hence $\nu(Kk') = 1$ by the first assertion proved above. Therefore, we see again from Theorem 1 that $\nu(L) = 1$ for all intermediate fields L of Kk'/K. The proof of Theorem 2 is thus completed. ■

Proof of Theorem 3. As in the statement of Theorem 3, let E/F be any extension of global fields such that

$$K \subseteq F, \quad E \subset K\widetilde{k}, \quad \gcd(t, [E:K]) = \gcd(t, [F:K]).$$

Let $\pi : \mathcal{F} \to G_E$ be a free presentation of G_E. We put

$$\mathcal{R} = \mathrm{Ker}(\pi), \quad \mathcal{S}(K) = \pi^{-1}(\mathrm{Gal}(E/K)), \quad \mathcal{S}(F) = \pi^{-1}(\mathrm{Gal}(E/F)).$$

Since E/K is a cyclic extension and $\gcd(t, [E:K])$ divides $[F:K]$,

$$\mathrm{Gal}(E/F) = \mathrm{Gal}(E/K)^{[F:K]} \subseteq \mathrm{Gal}(E/K)^t.$$

Therefore, it follows that

$$\mathcal{S}(F) \subseteq \mathcal{S}(K)^t\mathcal{R} = \{y^t z \mid y \in \mathcal{S}(K),\, z \in \mathcal{R}\}.$$

On the other hand, Lemma 2 implies that

$$\mathrm{Ker}(R(E/F)) \cong ([\mathcal{F}, \mathcal{S}(F)] \cap \mathcal{R})/[\mathcal{F}, \mathcal{R}]. \tag{7}$$

Now, take arbitrary $x \in \mathcal{F}$, $y \in \mathcal{S}(K)$ and $z \in \mathcal{R}$. Noting that E is the composite of K and an intermediate field of $\widetilde{k}/k$, we have

$$[x, y^t z] \in [x, y]^t[\mathcal{F}, \mathcal{R}], \quad [x, y] \in \mathcal{R},$$

as in the proof of Lemma 5. Hence

$$[x, y^t z] \in x^t(x^{-1}[x, y])^t[\mathcal{F}, \mathcal{R}] = x^t y x^{-t} y^{-1}[\mathcal{F}, \mathcal{R}].$$

It also follows from $\mathcal{F}/\mathcal{S}(K) \cong G_K$ and $\mathcal{S}(K)/\mathcal{R} \cong \mathrm{Gal}(E/K)$ that there exist $a, b \in \mathbb{Z}$, $z_1, z_2 \in \mathcal{R}$, and $y_0 \in \mathcal{S}(K)$ satisfying

$$x^t = y_0^a z_1, \quad y = y_0^b z_2.$$

Consequently,

$$[x, y^t z] \in y_0^a z_1 y_0^b z_2 z_1^{-1} y_0^{-a} z_2^{-1} y_0^{-b}[\mathcal{F}, \mathcal{R}] = z_1 z_2 z_1^{-1} z_2^{-1}[\mathcal{F}, \mathcal{R}] = [\mathcal{F}, \mathcal{R}].$$

This shows that $[\mathcal{F}, \mathcal{S}(F)] = [\mathcal{F}, \mathcal{R}]$. Hence, by (7) and Lemma 4, $R(E/F)$ turns out to be an isomorphism. Lemma 4 and (3) give us, however, a commutative diagram

$$\begin{array}{ccc}
\bigoplus_{v\in P} M(G_E^v) & \xrightarrow{\gamma_E} & M(G_E) \\
\downarrow & & \downarrow{\scriptstyle R(E/F)} \\
\bigoplus_{v\in P} M(G_F^v) & \xrightarrow{\gamma_F} & M(G_F)
\end{array}$$

in which the vertical map on the left is surjective. Therefore,

$$\varrho_{E/F} : \mathrm{Coker}(\gamma_E) \to \mathrm{Coker}(\gamma_F)$$

must be an isomorphism. Hence Lemma 3 completes the proof of Theorem 3. ∎

References

[1] S. Eilenberg and S. MacLane, *Cohomology theory in abstract groups*, *I*, Ann. of Math. 48 (1947), 51–78.
[2] F. Gerth, *The Hasse norm principle for abelian extensions of number fields*, Bull. Amer. Math. Soc. 83 (1977), 264–266.
[3] K. Horie and M. Horie, *Deflation and residuation for class formation*, J. Algebra 245 (2001), 607–619 ("A_F" in the diagram of Theorem 1 on page 610 should be read as "A_L").
[4] W. Jehne, *On knots in algebraic number theory*, J. Reine Angew. Math. 311/312 (1979), 215–254.
[5] G. Karpilovsky, *The Schur Multiplier*, Oxford Univ. Press, 1987.
[6] T. Nakayama, *A remark on fundamental exact sequences in cohomology of finite groups*, Proc. Japan Acad. 32 (1956), 731–735.
[7] M. J. Razar, *Central and genus class fields and the Hasse norm theorem*, Compositio Math. 35 (1977), 281–298.
[8] D. J. S. Robinson, *A Course in the Theory of Groups*, Grad. Texts in Math. 80, Springer, 1982.
[9] T. Tannaka, H. Kuniyoshi, F. Terada and S. Takahashi, *Number-theoretical properties of cohomology groups*, Sūgaku 6 (1954), 30–42 (in Japanese).

Department of Mathematics
Tokai University
1117 Kitakaname, Hiratsuka
Kanagawa 259-1292, Japan

Department of Mathematics
Ochanomizu University
2-1-1 Otsuka, Bunkyo-ku
Tokyo 112-8610, Japan
E-mail: horie@math.ocha.ac.jp

Received on 9.2.2001
and in revised form on 29.7.2002 (3970)