J. Math. Soc. Japan
Vol. 22, No. 3, 1970

Remarks on the validity of Hasse's norm theorem

By Takashi TASAKA

(Received July 2, 1969)
(Revised Jan. 14, 1970)

Introduction.

Let k be an algebraic number field. It is well-known that the obstruction to the validity of Hasse's norm theorem for a finite Galois extension K/k is described as a factor group of certain cohomology group ([2], Th. 20.6). T. Ono has noticed that there is a very close connection between the validity of Hasse's norm theorem and the Tamagawa number of the torus $R_{K/k}^{(1)}(G_m)$ ([6], n°6).

In this paper, we extend slightly the problem to the case of an arbitrary finite extension L/k. Thus the problem becomes the following one; If an element x of k is "local norm" at every place $\mathfrak{p}$, that is, if $x \in NL_{\mathfrak{p}}^*$ for every $\mathfrak{p}$, where $NL_{\mathfrak{p}}^*$ is the subgroup of $k_{\mathfrak{p}}^*$ generated by $N_i L_{\mathfrak{q}_i}^*$, then is x contained in NL^*? Note that $\mathfrak{q}_i$ runs all places of L above $\mathfrak{p}$, and that N_i is the norm map of $L_{\mathfrak{q}_i}$ into $k_{\mathfrak{p}}$. This problem is affirmatively solved for any cubic extension of k (n°3, Example). But we do not know for which type of extension of k this problem can be solved affirmatively.

In our paper, we denote by V the torus $R_{K/k}^{(1)}(G_m)$, and by U the torus whose character module is the dual of that of V. These tori can be defined in general situation. It is comparatively easy to calculate the Tamagawa number of U (n°3, Prop. 4). Following Ono's method, we calculate the Tamagawa number of V (n°4, Th.).

It is probable that our results can be expressed in terms of cohomology groups. But it seems to the author that our method in this paper is useful in the theory of non-Galois extensions of fields of dimension one.

1. Preliminaries.

Let G be a finite group and H be its subgroup of index n. One puts $G = \bigcup_{i=0}^{n-1} g_i H$ with $g_0 = 1$ (the identity of G). We consider the following left G-module:

$$\Lambda = \boldsymbol{Z}[G/H], \tag{1}$$

where $Z[G/H]=\sum_{i=0}^{n-1} Za_i$, and $a_i=g_iH$.

Let A and B be (left) G-modules. Then $\mathrm{Hom}(A, B)=\mathrm{Hom}_Z(A, B)$ and tensor product $A\otimes B=A\otimes_Z B$ are G-modules in natural way. We put $A^0=\mathrm{Hom}(A, Z)$ which will be called the dual G-module of A. For a G-module M, we denote by M^G the submodule of M which consists of all G-invariant elements. We noticed in our previous paper ([7], n°1) that the following Lemma 1 and Lemma 2 hold:

LEMMA 1. *Let M be a G-module. If we consider the Tate cohomology groups of G, we have*

$$H^i(G, \Lambda\otimes M)\cong H^i(H, M), \qquad (i\in Z) \tag{2}$$

$$(\Lambda\otimes M)^G\cong M^H. \tag{2'}$$

Now consider the following exact sequences;

$$0\longrightarrow C\longrightarrow \Lambda\xrightarrow{c} Z\longrightarrow 0, \tag{3}$$

$$0\longrightarrow Zu\xrightarrow{r} \Lambda\longrightarrow R\longrightarrow 0, \tag{4}$$

where $c(\sum p_ia_i)=\sum p_i$, and $u=\sum a_i$ and r is the canonical injection. So $Zu\cong Z$ as G-modules. It is easy to see that $C\cong R^0$ and $R\cong C^0$. Clearly the sequences (3) and (4) split over Z. Thus we have the following exact sequences for a G-module M:

$$0\longrightarrow C\otimes M\longrightarrow \Lambda\otimes M\xrightarrow{c\otimes 1} M\longrightarrow 0, \tag{5}$$

$$0\longrightarrow M\xrightarrow{r\otimes 1} \Lambda\otimes M\longrightarrow R\otimes M\longrightarrow 0. \tag{6}$$

LEMMA 2. *The map $c\otimes 1$ in (5) induces the map of $H^i(H, M)$ into $H^i(G, M)$. Then this map is the corestriction map which we will denote by c. The map $r\otimes 1$ in (6) induces the map of $H^i(G, M)$ into $H^i(H, M)$. Then this map is the restriction map which we will denote by r.*

Considering the derived Tate cohomology sequences of (3) and (4), we have

PROPOSITION 1. *Let C and R be Z-free G-modules in (3) and (4), respectively. We have*

$$H^{-1}(G, C)\cong G/H\cdot G', \qquad H^0(G, C)=0, \qquad H^1(G, C)\cong Z_n;$$

$$H^{-1}(G, R)\cong Z_n, \qquad H^0(G, R)=0, \qquad H^1(G, R)\,\square\, G/H\cdot G';$$

where Z_n is the cyclic group of order n.

Note that $A\,\square\, B$ means that A and B are in (Pontrjagin) duality. So if

A and B are finite abelian groups, then A and B are isomorphic (but not canonically).

PROOF. If G is a Galois group of an extension of an algebraic number field, one can use the class field theory and Tate-Nakayama's theorem ([4], Cor. 3).

Or more directly, one can prove $C^G = R^G = 0$ (cf. n°4 Prop. 6 and 7), so it follows that $H^0(G, C) = H^0(G, R) = 0$. The cohomology group $H^{-1}(G, C)$ is the cokernel of the corestriction map of $H^{-2}(H, \boldsymbol{Z})$ into $H^{-2}(G, \boldsymbol{Z})$. As $H^{-2}(H, \boldsymbol{Z}) \cong H/H'$ and $H^{-2}(G, \boldsymbol{Z}) \cong G/G'$, and the corestriction map is given by $h \cdot H' \mapsto h \cdot G'$, it is clear that $H^{-1}(G, C) \cong G/H \cdot G'$. The rest is clear, because $H^1(G, R) \square H^{-1}(G, C)$. (q. e. d.)

Let M be a G-module such that $H^1(G, M) = H^1(H, M) = 0$. Considering the derived cohomology sequences (not Tate cohomology sequences) of (5) and (6), we have

$$0 \longrightarrow (C \otimes M)^G \longrightarrow M^H \xrightarrow{c} M^G \longrightarrow H^1(G, C \otimes M) \longrightarrow 0\,,$$

$$0 \longrightarrow H^2(G, C \otimes M) \longrightarrow H^2(H, M) \xrightarrow{c} H^2(G, M)\,,$$

$$0 \longrightarrow M^G \xrightarrow{r} M^H \longrightarrow (R \otimes M)^G \longrightarrow 0\,,$$

$$0 \longrightarrow H^1(G, R \otimes M) \longrightarrow H^2(G, M) \xrightarrow{r} H^2(H, M)\,.$$

PROPOSITION 2. *Let M be a G-module satisfying the conditions $H^1(G, M) = 0$, $H^1(H, M) = 0$. Then we have the following isomorphisms:*

$$(C \otimes M)^G \cong \ker (M^H \xrightarrow{c} M^G)\,; \tag{7}$$

$$H^1(G, C \otimes M) \cong M^G / c(M^H)\,; \tag{8}$$

$$H^2(G, C \otimes M) \cong \ker (H^2(H, M) \xrightarrow{c} H^2(G, M))\,; \tag{9}$$

$$(R \otimes M)^G \cong M^H / r(M^G)\,; \tag{10}$$

$$H^1(G, R \otimes M) \cong \ker (H^2(G, M) \xrightarrow{r} H^2(H, M))\,. \tag{11}$$

2. Ono's theorem on the Tamagawa numbers of tori.

Let k be a field of dimension one, that is, either an algebraic number field of finite degree over $\boldsymbol{Q}$, or an algebraic function field of one variable over a finite constant field. Suppose that K is a finite Galois extension of k with the Galois group G. We denote by J_k and J_K the idèle groups of k and K, respectively. We also denote by $\mathfrak{C}_k$ and $\mathfrak{C}_K$ the idèle class groups of k

and K, respectively. Then it is clear from the class field theory that J_K and $\mathfrak{C}_K$ are G-modules satisfying the conditions of Prop. 2, for any subgroup H.

Let T be a torus defined over k which splits over K. We denote by T_k the group of k-rational points of T, and by T_{A_k} the adèle group of T over k. Putting $\mathfrak{C}_k(T)=T_{A_k}/T_k$, we call $\mathfrak{C}_k(T)$ the adèle class group of T over k. We denote by $X(T)$ the character module of T which is a $\boldsymbol{Z}$-free G-module. There is an isomorphism between the category of tori defined over k and split over K, and the dual of the category of finitely generated $\boldsymbol{Z}$-free G-modules, which is defined by $T\mapsto X(T)^0$, where $X(T)^0$ is the dual G-module of $X(T)$. For a splitting field K of T, it is known that $T_K\cong X^0\otimes K^*$, $T_{A_K}\cong X^0\otimes J_K$, $\mathfrak{C}_K(T)\cong X^0\otimes\mathfrak{C}_K$, as G-modules, where $X^0=X(T)^0$ ([**6**], (2.1.2)). It is easy to see that $T_k=(T_K)^G$ and $T_{A_k}=(T_{A_K})^G$, but $\mathfrak{C}_k(T)\subseteqq\mathfrak{C}_K(T)^G$ and the equality does not hold in general.

T. Ono has defined the numbers $i(T)$, $h(T)$ and $\tau(T)$ for a torus T([**6**], n°3):

$$i(T)=[\mathfrak{C}_K(T)^G:\mathfrak{C}_k(T)]\,, \tag{12}$$

$$h(T)=[H^{-1}(G, X(T)^0)]\,, \tag{13}$$

and $\tau(T)$ is the Tamagawa number of T over k. Note that $[A:B]$ means the index of B in A, and $[A]=[A:1]$. It is known that $i(T)$ is finite ([**6**], n°2.3). Note also that $[H^{-1}(G, X(T)^0)]=[H^1(G, X(T))]$ because of the finiteness of $H^{-1}(G, X(T)^0)$ and the duality between them.

He has proved the following fundamental formula ([**6**], Main theorem):

$$\tau(T)i(T)=h(T)\,. \tag{14}$$

3. The tori V and U.

Let L be a separable extension of finite degree n over the field k of dimension one, and K be a finite Galois extension of k containing L. We denote by G and H the Galois group of K/k and K/L, respectively.

To the $\boldsymbol{Z}$-free G-modules C and R in (3) and (4), there correspond the tori U and V such that $X(U)=C$ and $X(V)=R$. So $X(U)^0=R$ and $X(V)^0=C$. From Prop. 1, it follows

$$h(V)=[H^{-1}(G, C)]=n_a\,, \tag{15}$$

$$h(U)=[H^{-1}(G, R)]=n\,, \tag{16}$$

where $n_a=[L_a;k]$ and L_a is the maximal abelian extension of k contained in L.

Now we consider the sequence

(17) $$0 \longrightarrow V_K \longrightarrow V_{A_K} \longrightarrow \mathfrak{C}_K(V) \longrightarrow 0\,.$$

As K^*, J_K and $\mathfrak{C}_K$ satisfy the conditions of Prop. 2, the derived cohomology sequence (not Tate cohomology sequence) of (17) can be written

$$\begin{aligned}0 \longrightarrow V_k \longrightarrow V_{A_k} \longrightarrow \mathfrak{C}_K(V)^G \longrightarrow k^*/NL^* \longrightarrow J_k/NJ_L \longrightarrow \mathfrak{C}_k/N\mathfrak{C}_L \\ \longrightarrow H^2(G, V_K) \longrightarrow H^2(G, V_{A_K}) \longrightarrow 0\,.\end{aligned}$$

Note that the map c in Prop. 2 is the norm map of L into k, and that $H^2(G, \mathfrak{C}_K(V))=0$ because this group is the kernel of the corestriction map of $H^2(H, \mathfrak{C}_K)$ into $H^2(G, \mathfrak{C}_K)$ which is known to be zero from the class field theory. Clearly the map $J_k/NJ_L \to \mathfrak{C}_k/N\mathfrak{C}_L$ is surjective. Taking inductive limit (with respect to the inflation map) of the above sequence to the separable closure Ω of k, and denoting by $\mathfrak{g}$ the Galois group of Ω over k, we have

PROPOSITION 3. *For the torus V, we have*

(18) $$0 \longrightarrow Q \longrightarrow k^*/NL^* \longrightarrow J_k/NJ_L \longrightarrow \mathfrak{C}_k/N\mathfrak{C}_L \longrightarrow 0\,,$$

(19) $$0 \longrightarrow H^2(\mathfrak{g}, V_\Omega) \longrightarrow H^2(\mathfrak{g}, V_{A_\Omega}) \longrightarrow 0$$

where $Q=\mathfrak{C}_K(V)^G/\mathfrak{C}_k(V)$.

From definition, we have $i(V)=[Q]$. The sequence (18) means that the validity of Hasse's norm theorem is equivalent to $Q=0$ or $i(V)=1$. For the exact structure of NJ_L, see the formula (27) of the next section. The sequence (19) is the Hasse principle for the (central simple) algebra class of L whose corestriction to k is zero. In particular, if L is a separable quadratic extension of k, we know that, to an element of $H^2(g, V_\Omega)$, there corresponds an algebra class of L which has involutions of the second kind over k ([7], n°2, Th.).

Next we consider the sequence

(20) $$0 \longrightarrow U_K \longrightarrow U_{A_K} \longrightarrow \mathfrak{C}_K(U) \longrightarrow 0\,.$$

The derived cohomology sequence (not Tate cohomology sequence) of (20) is

$$0 \longrightarrow U_k \longrightarrow U_{A_k} \longrightarrow \mathfrak{C}_K(U)^G \longrightarrow H^1(G, R\otimes K^*) \xrightarrow{\lambda} H^1(G, R\otimes J_K) \longrightarrow .$$

By Prop. 2 (11), we can consider $H^1(G, R\otimes K^*)$ as contained in $H^2(G, K^*)$, and $H^1(G, R\otimes J_K)$ as contained in $H^2(G, J_K)$. It follows from the class field theory that λ is injection ([2], Th. 20.3). Thus we have $\mathfrak{C}_K(U)^G \cong U_{A_K}/U_k = \mathfrak{C}_k(U)$. That is,

(21) $$i(U)=1\,.$$

It follows from (14) and (16),

PROPOSITION 4. *For the torus U, we have*

$$\tau(U)=h(U)/i(U)=n\,,$$

where $n=[L:k]$.

Now consider the derived Tate cohomology sequence of (5) in which we put $M=\mathfrak{C}_K$.

$$\begin{array}{ccccccc} \longrightarrow H^0(G,\mathfrak{C}_K) & \xrightarrow{r} & H^0(H,\mathfrak{C}_K) & \longrightarrow & H^0(G,R\otimes\mathfrak{C}_K) & \longrightarrow & 0. \\ \wr\Vert & & \wr\Vert & & & & \\ \mathfrak{C}_k/N_k\mathfrak{C}_K & & \mathfrak{C}_L/N_L\mathfrak{C}_K & & & & \end{array}$$

Though we do not need in the later, we summarize the above result.

PROPOSITION 5. *Let R be the G-module defined in* (4). *Then*

$$H^{-2}(G,R)=\mathfrak{C}_L/\mathfrak{C}_k\cdot N_L\mathfrak{C}_K\,,$$

and $H^{-2}(G,R)$ is the cokernel of " Verlagerung" of $H^{-2}(G,\boldsymbol{Z})$ into $H^{-2}(H,\boldsymbol{Z})$.

PROOF. By Tate-Nakayama's theorem [4], we have $H^0(G,R\otimes\mathfrak{C}_K)=H^{-2}(G,R)$. Our proposition follows from the above exact sequence. (q. e. d.)

EXAMPLE. Let L be a separable cubic (cyclic or not) extension of k. It is well-known that Hasse's norm theorem is valid for cyclic extensions ([3], p. 274-275). So we consider non-cyclic case. Let K be the minimal Galois extension of k containing L. Then the Galois group of K over k is the symmetric group S_3 on three letters, and the Galois group H of K over L is the subgroup of order 2 of S_3. Consider the Tate cohomology sequence derived from (17). We have

$$\longrightarrow H^0(G,C\otimes\mathfrak{C}_K)\longrightarrow k^*/NL^*\longrightarrow J_k/NJ_L\longrightarrow\,.$$

Now consider the sequence

$$H^{-3}(G,\boldsymbol{Z})\longrightarrow H^{-2}(G,C)\longrightarrow H^{-2}(H,\boldsymbol{Z})\xrightarrow{c} H^{-2}(G,\boldsymbol{Z})\,.$$

It is clear that the map c is an isomorphism and $H^{-3}(G,\boldsymbol{Z})=0$, because the group $G=S_3$ has the period 4 ([1], Chap. 12, n°11). By Tate-Nakayama's theorem, we have $H^0(G,C\otimes\mathfrak{C}_K)=0$. Thus we have

$$0\longrightarrow k^*/NL^*\longrightarrow J_k/NJ_L\longrightarrow \mathfrak{C}_k/N\mathfrak{C}_L\,.$$

This shows that Hasse's norm theorem is valid and $\tau(V)=1$ for a non-cyclic cubic extension L of k, because $n_a=1$ in our case.

4. Tamagawa number $\tau(V)$.

We investigate more precise structure of $C\otimes M$ and $R\otimes M$ for a G-module M.

We put $G=\bigcup_{i=0}^{n-1}g_iH$, with $g_0=1$. By definition, $\Lambda=\sum_{i=0}^{n-1}\boldsymbol{Z}a_i$. Then $C=\sum_{i=1}^{n-1}\boldsymbol{Z}c_i$

and $R=\sum_{i=1}^{n-1}\boldsymbol{Z}b_i$, where $c_i=a_i-a_0$ and $b_i=\bar{a}_i$ (the class of a_i mod $\boldsymbol{Z}u$), $1\leqq i\leqq n-1$. Note that $u=\sum_{i=0}^{n-1}a_i$. So we have $\bar{a}_0=-\sum_{i=1}^{n-1}b_i$.

For a G-module M, we define the map N of M^H into M^G, by putting

$$Nm=\sum_{i=0}^{n-1}g_i m\,. \tag{22}$$

This map is well-defined. We denote by $\nu(M^H)$ the kernel of N in M^H.

PROPOSITION 6. *For any G-module M, we have*

$$(C\otimes M)^G=\{\sum c_i\otimes g_i m\,;\ m\in\nu(M^H)\}\cong\nu(M^H)\,.$$

PROOF. If $h\in H$, then h induces a permutation on $\{c_i\}$. That is, $hc_i=c_{h(i)}$, where $hg_i\in g_{h(i)}H$.

If $f\notin H$, then f induces a permutation on $\{a_i\}$ which will be considered as a permutation on n letters $\{0,1,\cdots,n-1\}$ and will be denoted also by f. Clearly one has $f(0)\neq 0$. So we have

$$fc_i=\begin{cases} c_{f(i)}-c_{f(0)}\,; & f(i)\neq 0\,,\\ -c_{f(0)}\quad; & f(i)=0\,.\end{cases}$$

Then it is easy to conclude the proposition. (q. e. d.).

PROPOSITION 7. *If $H^1(G,M)=0$, we have*

$$(R\otimes M)^G=\{\sum b_i\otimes(g_i-1)m\,;\ m\in M^H\}\cong M^H/M^G\,.$$

PROOF. It is clear that $\sum b_i\otimes(g_i-1)m$ $(m\in M^H)$ is contained in $(R\otimes M)^G$. From the sequence (6), one has

$$0\longrightarrow M^G\longrightarrow M^H\longrightarrow(R\otimes M)^G\longrightarrow 0\,.$$

Thus we have $(R\otimes M)^G\cong M^H/M^G$. (q. e. d.).

$C\otimes\boldsymbol{Q}$ is a self-dual G-space, in the sense that, for the representation ρ of G defined over $\boldsymbol{Q}$ induced from G-module C, ${}^t\rho^{-1}$ is equivalent to ρ over $\boldsymbol{Q}$. (For example, take a G-invariant positive definite quadratic form on $C\otimes\boldsymbol{Q}$). So $R\otimes\boldsymbol{Q}\cong C\otimes\boldsymbol{Q}$ as G-space, that is, the tori U and V defined by C and R are isogeneous over k ([**5**], Prop. 1.3.2).

We will determine a canonical k-isogeny from V onto U. From now on, we suppose that the characteristic of k does not divide n. Under this assumption we can show that the isogeny defined below is separable.

The map $\varepsilon: c_i\mapsto d_i=b_i+\sum_{s=1}^{n-1}b_s$ is an injective G-homomorphism of C into R. The elementary divisors of the matrix $(1+\delta_{ij})$ are $\langle n,1,\cdots,1\rangle$, and $[\operatorname{cok}\varepsilon]=n$. Let M be a G-module such that $H^1(G,M)=0$. Putting

$$\varepsilon\otimes 1: C\otimes M\longrightarrow R\otimes M\,,$$

where $\varepsilon\otimes 1(\sum c_i\otimes g_i m_i)=\sum_s\sum_i b_s\otimes(1+\delta_{is})g_i m_i$, we call this map a canonical isogeny. This map induces the following map α:

(23) $$\alpha:(C\otimes M)^G\longrightarrow(R\otimes M)^G,$$

where $\alpha(\sum c_i\otimes g_i m)=\sum b_i\otimes(g_i-1)m$. Thus we have

PROPOSITION 8. *The canonical isogeny induces the following map which will be denoted also by* α:

$$\alpha:\nu(M^H)\longrightarrow M^H/M^G,$$

where $\alpha(m)=$ *the class of* $m \bmod M^G$ $(m\in\nu(M^H))$. *Thus we have*

$$\ker\alpha\cong\nu(M^H)\cap M^G,$$

$$\operatorname{cok}\alpha\cong M^H/\nu(M^H)\cdot M^G=N(M^H)/N(M^G),$$

where N is the map defined by (22).

REMARK. If one can prove directly that $(R\otimes M)^G=M^H/M^G$, then one may apply Prop. 8 to the G-module M.

Hereafter, we denote the composition in M multiplicatively, because we consider multiplicative G-modules in applications. So we have $N(M^G)=(M^G)^n$, where $(M^G)^n=\{x^n; x\in M^G\}$.

For a homomorphism $\beta:A\to B$, we put

(24) $$q(\beta)=[\operatorname{cok}\beta]/[\ker\beta].$$

T. Ono has proved the following theorem ([5], Th. 3.10.1).

THEOREM (Ono). *Let α be a separable k-isogeny of T onto T', where T and T' are tori defined over k. Then*

(25) $$\tau(T')/\tau(T)=\tau(\alpha)\cdot q(\hat{\alpha}_k),$$

where $\tau(\alpha)=q(\alpha_S)/q(\alpha_k^S)$, and S is a suitably large finite set of places of k.

In our case, U and V are anisotropic tori, so $q(\hat{\alpha}_k)=1$. We calculate the numbers $q(\alpha_S)$ and $q(\alpha_k^S)$.

Let $\mathfrak{p}$ be a place of k. Suppose that $\mathfrak{p}=\prod_{i=1}^t\mathfrak{q}_i^{e_i}$ is the decomposition of $\mathfrak{p}$ in L, and that, if $\mathfrak{p}$ is a finite place, $N\mathfrak{q}_i=\mathfrak{p}^{f_i}$. Let $\mathfrak{P}$ be a place of K above $\mathfrak{p}$. We denote by $G(\mathfrak{P})$ the decomposition group of $\mathfrak{P}$. We put

(26) $$M_{\mathfrak{p}}=\prod_{g\mathfrak{P}}K^*_{g\mathfrak{P}},$$

where g runs over the coset space $G/G(\mathfrak{P})$. Then $M_{\mathfrak{p}}$ is a G-module such that $H^1(G,M_{\mathfrak{p}})=H^1(H,M_{\mathfrak{p}})=0$ ([2], Th. 12.1). It is easy to see that $(M_{\mathfrak{p}})^H=\prod_{i=1}^t L^*_{\mathfrak{q}_i}$, $(M_{\mathfrak{p}})^G=k^*_{\mathfrak{p}}$, and

(27) $$N(M^H_{\mathfrak{p}})=NL^*_{\mathfrak{p}},$$

where $NL_{\mathfrak{p}}^*$ is the subgroup of $k_{\mathfrak{p}}^*$ generated by $N_i L_{\mathfrak{q}_i}^*$ $(1 \leqq i \leqq t)$ and N_i is the norm map of $L_{\mathfrak{q}_i}$ into $k_{\mathfrak{p}}$. In this case, we have

(28) $$q(\alpha_{\mathfrak{p}}) = [NL_{\mathfrak{p}}^* : (k_{\mathfrak{p}}^*)^n]/[\mu_n \cap k_{\mathfrak{p}}^*],$$

where μ_n is the group of n-th roots of unity in $\bar{k}_{\mathfrak{p}}$. We put

$$q(\alpha_\infty) = \prod q(\alpha_\lambda),$$

where λ runs over the set S_∞ of all infinite places of k. Then it is easy to see that

(29) $$q(\alpha_\infty) = (2^d \cdot n^{r_2})^{-1},$$

where r_2 is the number of complex places of k, and d is the number of real places which are totally ramified in L/k.

For a finite set S of places of k containing S_∞, and for a torus T defined over k, we put

$$T_A^S = \prod_{\mathfrak{p} \in S} T_{k_{\mathfrak{p}}} \times \prod_{\mathfrak{p} \notin S} T_{\mathfrak{o}_{\mathfrak{p}}},$$

$$T_k^S = T_k \cap T_A^S.$$

We call T_k^S the S-unit group of T over k.

Let S be a finite set of places of k satisfying the following conditions (i)~(iv), and $\bar{S}$ be the finite set of all places of L above $\mathfrak{p} \in S$:

(i) *S is a self-conjugate set with respect to the prime field $\boldsymbol{Q}$ which contains all infinite places of k and all places of k ramifying in K/k* (for an algebraic number field).

(i′) *S is a non-empty set of places of k which contains all places of k ramifying in K/k* (for an algebraic function field).

(ii) *S contains a complete system of representatives by prime ideals of the ideal classes in k.*

(iii) $J_L = L^* \cdot J_L^{\bar{S}}$.

(iv) $NL^* \cap E_k^S = N(E_L^{\bar{S}})$,

where $J_k^S = \prod_{\mathfrak{p} \in S} k_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin S} \mathfrak{u}_{\mathfrak{p}}$, and $E_k^S = k^* \cap J_k^S$ (the S-unit group of k^*), etc. Note that $\mathfrak{u}_{\mathfrak{p}}$ denotes the unit group of $k_{\mathfrak{p}}^*$.

The existence of such S comes from the finiteness of $[V_A : V_k \cdot V_A^{S_\infty}]$ and the fact that, under the condition (iii), one has $[V_A : V_k \cdot V_A^S] = [NL^* \cap E_k^S : N(E_L^{\bar{S}})]$.

Let $\tilde{S}$ be the set of all places of K above $\mathfrak{p} \in S$. We put

(30) $$M_{\mathfrak{o}_{\mathfrak{p}}} = \prod_{g\mathfrak{P}} \mathfrak{U}_{g\mathfrak{P}},$$

as in (26), where $\mathfrak{U}_{\mathfrak{P}}$ is the unit group of $K_{\mathfrak{P}}^*$. If $\mathfrak{p} \notin S$, then $\mathfrak{p}$ is unramified over K/k, so it follows that $H^1(G, M_{\mathfrak{o}_{\mathfrak{p}}}) = 0$ ([2], Th. 12.1), and we have

$$U_A^S=\prod_{\mathfrak{p}\in S}(M_{\mathfrak{P}}^H/M_{\mathfrak{P}}^G)\times\prod_{\mathfrak{p}\notin S}(M_{\mathfrak{o}_{\mathfrak{P}}}^H/M_{\mathfrak{o}_{\mathfrak{P}}}^G)\cong J_L^{\bar{S}}/J_k^S\,.$$

If we consider U_A^S and U_k as contained in J_L/J_k, then

$$U_A^S\cong J_L^{\bar{S}}\cdot J_k/J_k\,,$$

$$U_k\cong L^*\cdot J_k/J_k\,.$$

It follows that the S-unit group of U is

$$U_k^S=(J_L^{\bar{S}}\cdot J_k\cap L^*\cdot J_k)/J_k\,.$$

LEMMA 3. *If S is a finite set of places of k satisfying the conditions* (i)$\sim$(iv), *then one has*

$$L^*\cdot J_k\cap J_L^{\bar{S}}\cdot J_k=E_L^{\bar{S}}\cdot J_k\,.$$

PROOF. Suppose that ηJ_k is contained in $J_L^{\bar{S}}\cdot J_k$, where $\eta\in L^*$. One can choose an idèle $\mathfrak{a}$ of J_k such that $\eta\mathfrak{a}\in J_L^{\bar{S}}$. We denote by $\langle\eta\rangle$ the ideal of L defined by an idèle η, and by $\langle\mathfrak{a}\rangle$ the ideal of k defined by an idèle $\mathfrak{a}$. We also denote by $\langle\mathfrak{a}\rangle$ the extension of $\langle\mathfrak{a}\rangle$ to the ideal of L. As S contains a complete system of representatives by prime ideals of the ideal classes of k, there exists an idèle $\mathfrak{b}$ of J_k whose component is 1 outside S such that $\langle\mathfrak{a}\rangle\cdot\langle\mathfrak{b}\rangle=\langle\xi\rangle$ is a principal ideal in k. Then it is easy to see that $\eta\xi$ is an $\bar{S}$-unit of L. It follows

$$\eta J_k=(\eta\xi)J_k\in E_L^{\bar{S}}\cdot J_k\,.$$

The inverse inclusion is clear. (q. e. d.)

As $E_L^{\bar{S}}\cap J_k=E_k^S$, one has $U_k^S=E_L^{\bar{S}}/E_k^S=M_1^H/M_1^G$, where $M_1=E_K^{\tilde{S}}$. It is clear that $V_k^S=(C\otimes M_1)^G$. From definition, one has

$$\alpha_k^S:\,V_k^S\longrightarrow U_k^S\,.$$

So we can apply Prop. 8 to this module M_1, and we have

$$q(\alpha_k^S)=[N(E_L^{\bar{S}}):(E_k^S)^n]/[\mu_n\cap E_k]\,. \tag{31}$$

Note that $[\mu_n\cap E_k^S]=[\mu_n\cap E_k]$ is the number of n-th roots of unity contained in k.

Because $\tau(U)=n$, it follows from (25)

THEOREM. *Let L be a finite separable extension of k such that the characteristic of k does not divide $n=[L:k]$, and V be the torus defined over k whose k-rational points consist of the element x of L^* such that $Nx=1$, where N is the norm map of L into k. Let S be a finite set of places of k satisfying the conditions* (i)$\sim$(iv), *and put $S_f=S-S_\infty$. Then*

$$\tau(V)=2^d\cdot n^{r_2+1}\cdot q(\alpha_k^S)/\rho(S)\,, \tag{32}$$

where r_2 *is the number of complex places of* k, *and* d *is the number of real places of* k *which are totally ramified in* L/k, *and*

(33) $$\rho(S)=\prod_{\mathfrak{p}\in S_f}([NL_{\mathfrak{p}}^*:(k_{\mathfrak{p}}^*)^n]/[\mu_n\cap k_{\mathfrak{p}}^*]),$$

and $q(\alpha_k^S)$ *is the number given in* (31).

It is known that E_k^S is a direct product of the group of the roots of unity contained in k and the torsion free group of $\boldsymbol{Z}$-rank $s-1$, where s is the cardinality of the set S. From (iv), we have $q(\alpha_k^S)=n^{s-1}\cdot[E_k^S:E_k^S\cap NL^*]^{-1}$.

For a finite place $\mathfrak{p}$, we put

$$n_{\mathfrak{p}}=[k_{\mathfrak{p}}^*:NL_{\mathfrak{p}}^*].$$

This number has a certain meaning from the local class field theory. It is well-known that

$$[k_{\mathfrak{p}}^*:(k_{\mathfrak{p}}^*)^n]/[\mu_n\cap k_{\mathfrak{p}}^*]=n\cdot w_{\mathfrak{p}}(n)^{-1}.$$

(For example, Serre, Local class field theory. 1.7. Prop. 5. In the same volume as [**3**]). Note that $w_{\mathfrak{p}}(n)$ means the normalised valuation of n in $k_{\mathfrak{p}}$ in the sense of ([**2**], n°1). From the product formula, it follows

COROLLARY 1. *Let* k *be an algebraic number field. We assume that* S *satisfies the additional condition*

(v) S *contains all places dividing* n.

Then we have

$$\tau(V)=2^d\cdot(\prod_{\mathfrak{p}\in S_f}n_{\mathfrak{p}})\cdot[E_k^S:E_k^S\cap NL^*]^{-1},$$

where d *is the number of real places of* k *which are totally ramified in* L/k.

COROLLARY 2. *Let* k *be an algebraic function field of one variable over a finite constant field. We have*

$$\tau(V)=(\prod_{\mathfrak{p}\in S}n_{\mathfrak{p}})\cdot[E_k^S:E_k^S\cap NL^*]^{-1}.$$

Finally we remark that Hasse's norm theorem is valid for the extension L/k, if and only if

(34) $$i(V)=n_a/\tau(V)$$

is equal to 1.

College of General Education
University of Tokyo

References

[1] H. Cartan and S. Eilenberg, Homological algebra, Princeton, 1956.
[2] C. Chevalley, Class field theory, Nagoya, 1953–54.

[3] H. Hasse, History of class field theory, (Algebraic number theory, edited by J. Cassels and A. Fröhlich. Chap. 11), Academic press, 1967.
[4] T. Nakayama, Cohomology of class field theory and tensor product modules, I, Ann. of Math., **65** (1957), 255-267.
[5] T. Ono, Arithmetic of algebraic tori, Ann. of Math., **74** (1961), 101-139.
[6] T. Ono, On the Tamagawa number of algebraic tori, Ann. of Math., **78** (1963), 47-73.
[7] T. Tasaka, On the second cohomology groups of the fundamental groups of simple algebraic groups over perfect fields, J. Math. Soc. Japan, **21** (1969), 244-258.