170. *On Extensions with Given Ramification*

By Toyofumi TAKAHASHI
Mathematical Institute Tôhoku University, Sendai

(Comm. by Kenjiro SHODA, M. J. A., Oct. 12, 1968)

Let k be a number field of finite degree, and let S be a set of primes of k, including the achimedean ones. Let G be the Galois group of the maximal extension Ω of k unramified outside S. Throughout this paper we assume that S contains all primes above a fixed prime number l. Tate [7] has asserted that G has strict cohomological dimension 2 with respect to l, if k is totally imaginary in case $l=2$, but the proof has been unpublished. (Brumer [3] showed that G has cohomological dimension 2 with respect to l under the same assumptions.) We shall give here the proof of the above Tate's theorem (Section 1). As a corollary of this theorem, we obtain an arithmetic theorem and we get the l-adic independence of independent units (Section 2). Finally, we shall determine the structure of the connected component of the S-idèle class group. This is a generalization of the results of Weil [10] and Artin [1] (see also [2; Chap. IX]).

1. Cohomological dimension. Throughout this paper notations and terminologies are the same as in Tate [7]. By m we shall always understand a positive integer such that $mk_S=k_S$ where k_S is the ring of all S-integers of k. For any abelian group A, let $A(l)$ denote the l-torsion part of A. Let μ denote the group of all roots of unity, and let μ_m denote the group of m-th roots of unity.

Theorem 1. *Let $\bar{J}^S$ denote the projection to S_0 of the idèle group of Ω, where S_0 is the set of non-archimedean primes in S. We put $E=\bar{J}^S(l)/\mu(l)$. Suppose that k is totally imaginary if $l=2$. Then, for any l-torsion module M, we have an isomorphism*

$$H^2(k_S, M)^* \cong \mathrm{Hom}_G(M, E).$$

Proof. By our assumptions G has cohomological l-dimension 2. Let $\bar{E}$ be a *module dualisant* for G with respect to l. We shall show $E=\bar{E}$. By [5; Chap. I, Annexe] we have $\bar{E}=\varinjlim_{t} D_2(\boldsymbol{Z}/l^t\boldsymbol{Z})$ where $D_2(\boldsymbol{Z}/m\boldsymbol{Z})=\varinjlim_{K\subset\Omega} H^2(K_S, \boldsymbol{Z}/m\boldsymbol{Z})^*$, the inductive limit is taken with respect to cores*. By Tate's duality theorem, we have a commutative exact diagram

$$\begin{array}{ccccccc} H^0(K_S,\mu_m) \rightarrow & \prod_{v\in S_0} H^0(K_v,\mu_m) & \rightarrow & H^2(K_S, Z/mZ)^* & \rightarrow & H^1(K_S,\mu_m) \\ \downarrow \text{can.} & \downarrow \text{can.} & & \downarrow \text{cores}^* & & \downarrow \text{res} \\ H^0(L_S,\mu_m) \rightarrow & \prod_{w\in S_0} H^0(L_w,\mu_m) & \rightarrow & H^2(L_S, Z/mZ)^* & \rightarrow & H^1(L_S,\mu_m) \end{array}$$

for $K\subset L\subset \Omega$. Hence we have an exact sequence $\mu_m\rightarrow \bar{J}^S_m\rightarrow D_2(Z/mZ)\rightarrow 0$, where $\bar{J}^S_m$ is the subgroup of elements x of $\bar{J}^S$ such that $mx=0$. Thus we get an exact sequence $\mu(l)\rightarrow \bar{J}^S(l)\rightarrow \bar{E}\rightarrow 0$, and the assertion is proved.

Lemma 1. *For $v\notin S$, we have $H^1(\mathfrak{O}_v, \mu(l))=0$, where $\mathfrak{O}_v$ is the ring of integers of the completion k_v of k at v.*

Proof. Let s be a generator of the Galois group of the maximal unramified extension of k_v. We have $H^1(\mathfrak{O}_v, \mu(l))^*\cong H^0(\mathfrak{O}_v, \mu(l)^*)=(\mu(l)/\mu(l)^{1-s})^*$. Since the sequence $0\rightarrow H^0(\mathfrak{O}_v, \mu(l))\rightarrow \mu(l)\xrightarrow{1-s}\mu(l)^{1-s}\rightarrow 0$ is exact and $H^0(\mathfrak{O}_v, \mu(l))$ is finite, $\mu(l)^{1-s}$ is not finite. On the other hand, all proper subgroups of $\mu(l)$ are finite. Hence we get $\mu(l)=\mu(l)^{1-s}$. Q.E.D.

Lemma 2. *The kernel* $\mathrm{Ker}^1(k_S, \mu(l))$ *of the canonical map* $H^1(k_S, \mu(l))\rightarrow \prod_{v\in S} H^1(k_v, \mu(l))$ *is finite.*

Proof. By Lemma 1 we have a commutative exact diagram

$$\begin{array}{ccccc} 0\rightarrow \mathrm{Ker}^1(k_S, \mu(l))\rightarrow & H^1(k_S, \mu(l)) & \rightarrow & \prod_{v\in S} H^1(k_v, \mu(l))\times & \prod_{v\notin S} H^1(\mathfrak{O}_v, \mu(l)) \\ & \downarrow \text{inf} & & & \downarrow \text{id.}\times\text{inf} \\ 0\rightarrow \mathrm{Ker}^1(k, \mu(l))\rightarrow & H^1(k, \mu(l)) & \rightarrow & \prod_{v\in S} H^1(k_v, \mu(l))\times & \prod_{v\notin S} H^1(k_v, \mu(l)). \end{array}$$

Hence the inflation $H^1(k_S, \mu(l))\rightarrow H^1(k, \mu(l))$ induces an injection $\mathrm{Ker}^1(k_S, \mu(l))\rightarrow \mathrm{Ker}^1(k, \mu(l))$. Therefore it is sufficient to show that $\mathrm{Ker}^1(k, \mu(l))$ is finite. Let $Q(m)$ be the set of elements of k which are local m-th powers everywhere. Then $(Q(m):k^m)\leq 2$([2; Chap. X, Theorem 1]). Since $\mathrm{Ker}^1(k, \mu_m)=Q(m)/k^m$, we see that $\mathrm{Ker}^1(k, \mu(l))=\varinjlim_t \mathrm{Ker}^1(k, \mu_{l^t})$ is a finite group of order at most 2. Q.E.D.

Theorem 2. *G has strict cohomological l-dimension* 2, *except if $l=2$ and k is not totally imaginary.*

Proof. It is sufficient to show that $H^0(k_S, E)$ never contains any subgroups isomorphic to Q_l/Z_l (cf. [5; Chap. I, Annexe]). We have the exact sequence $0\rightarrow \mu(l)\rightarrow \bar{J}^S(l)\rightarrow E\rightarrow 0$. Passing to cohomology, we obtain the sequence $0\rightarrow H^0(k_S, \mu(l))\rightarrow \prod_{v\in S_0} H^0(k_v, \mu(l))\rightarrow H^0(k_S, E)\rightarrow H^1(k_S, \mu(l))\rightarrow \prod_{v\in S_0} H^1(k_v, \mu(l))$. Hence we obtain an exact sequence $0\rightarrow \mathrm{H}^0(k_S, \mu(l))\rightarrow \prod_{v\in S_0} H^0(k_v, \mu(l))\rightarrow H^0(k_S, E)\rightarrow \mathrm{Ker}^1(k_S, \mu(l))\rightarrow 0$. Since $\mathrm{H}^0(k_S, \mu(l))$, $H^0(k_v, \mu(l))$ and $\mathrm{Ker}^1(k_S, \mu(l))$ are finite, $H^0(k_S, E)$ has no divisible element except 0. Q.E.D.

Corollary. *For any G-module M, we have isomorphisms*

$$H^i(k_S, M)(l) \cong \prod_{v \text{ arch}} H^i(k_v, M)(l) \qquad (i \geq 3).$$

Proof. This is an immediate consequence of [6; Lemma 3].

Let $G(l)$ denote the Galois group of the maximal l-extension of k unramified outside S. It is easy to determine the number of generators and that of relations of $G(l)$, using the exact sequence of Tate [7] and the equality [8; Theorem 2.2]. We omit the proof.

Proposition. *Let r_2 be the number of complex primes of k. Suppose that S is finite. Then $G(l)$ is a pro-l-group on $-\delta+\sum_{v\in S}\delta_v+1+\dim Q(l,S)/k^l$ generators with $-\delta+\sum_{v\in S}\delta_v-r_2+\dim Q(l,S)/k^l$ relations, where $Q(l,S)$ is the set of elements x of k such that $x\in k_v^l$ for all $v\in S$ and $\mathrm{ord}_v x\equiv 0$ mod. l for all $v\notin S$, and δ (resp. δ_v) is equal to 0 if $\mu_l\not\subset k$ (resp. $\mu_l\not\subset k_v$) and to 1 if $\mu_l\subset k$ (resp. $\mu_l\subset k_v$).*

Remark. If $\delta=1$ (i.e., k contains the l-th roots of unity), $Q(l,S)/k^l=\mathrm{Ker}^1(k_S,\mu_l)=\mathrm{Ker}^1(k_S,\boldsymbol{Z}/l\boldsymbol{Z})=(Cl_S/Cl_S^l)^*$, where Cl_S is the quotient of the ideal class group of k by the subgroup generated by the classes of all primes in S. This is the case obtained by Brumer [3]. See also Šafarevič [4].

2. The l-adic independence of independent units.

Theorem 3. *Let $Q(m,S)$ be the set of all elements x of k such that $x\in k_v^m$ for all $v\in S$ and $\mathrm{ord}_v x\equiv 0$ mod. m for all $v\notin S$. Then, for each m, there exists an integer m' such that $m'k_S=k_S$ and $Q(m',S)\subset k^m$.*

Proof. By Corollary of Theorem 2 we have $\mathrm{H}^2(k_S,\boldsymbol{Q}_p/\boldsymbol{Z}_p)=H^3(k_S,\boldsymbol{Z})(p)=0$ for $p\mid m$. According to [7; Theorem 3.1 (a)], we have an exact sequence $0\to\mathrm{Ker}^1(k_S,\mu_m)^*\to H^2(k_S,\boldsymbol{Z}/m\boldsymbol{Z})$. Using the exact sequence $0\to\mu_m\to\Omega\to\Omega^m\to 0$, we obtain $H^1(k_S,\mu_m)=k\cap\Omega^m/k^m$. By the theory of ramification in Kummer extensions, $k\cap\Omega^m$ coincides with the set of elements whose orders are divisible by m at each prime not in S. Hence we have $\mathrm{Ker}^1(k_S,\mu_m)=Q(m,S)/k^m$ and we get a commutative exact diagram

$$\begin{array}{ccc}
0\to[Q(m,S)/k^m]^*\to & H^2\left(k_S,\frac{1}{m}\boldsymbol{Z}/\boldsymbol{Z}\right) \\
\downarrow & \downarrow \\
0\to[Q(m',S)/k^{m'}]^*\to & H^2\left(k_S,\frac{1}{m'}\boldsymbol{Z}/\boldsymbol{Z}\right)
\end{array}$$

for $m\mid m'$. We obtain $\varprojlim_m Q(m,S)/k^m=0$. Since $Q(m,S)/k^m=\mathrm{Ker}^1(k_S,\mu_m)$ are finite, the assertion is proved.

Corollary. *Let $\varepsilon_1,\cdots,\varepsilon_r$ be a system of independent units of k such that $\varepsilon_i\equiv 1$ mod. v for all v above l. The ε_i are naturally imbed-*

ded in the direct product $\prod_{v|l}(1+P_v)$ *where* P_v *is the prime ideal of* k_v. *Since* $\prod_{v|l}(1+P_v)$ *is a abelian pro-l-group, it can be regarded as a* Z_l-*module.*

Then $\varepsilon_1, \cdots, \varepsilon_r$ are independent over Z_l in $\prod_{v|l}(1+P_v)$.

This corollary can be proved by the similar way as the proof of [2; Chap. IX, Theorem 2].

3. The structure of the connected component of the S-idèle class group. Let K/k be a Galois extension of finite degree unramified outside S with Galois group $\bar{G}$. We use following notations:

J: the idèle group of K, $U^S=\prod_{w\notin S} U_w$ where U_w is the unit group of K_w, J_0: the group of idèles of K of absolute value 1, $C^S=J/KU^S$: the S-idèle class group of K, $C_0^S=J_0/KU^S$, H: the connected component of J, D^S: the connected component of C^S, $H^S=KU^SH/KU^S$, $H_0^S=H^S\cap C_0^S$ and $D_0^S=D^S\cap C_0^S$.

We remark that C^S is a class formation for extensions unramified outside S (cf. [9]) and D^S is nothing but the kernel of the reciprocity map of C^S onto the Galois group of the maximal abelian extension of K unramified outside S. By the elementary theory of topological groups, the subgroup H^S of C^S is dense in D^S. Hence D^S is the completion of H^S. We have $D^S=\boldsymbol{R}\times D_0^S$ and $H^S=\boldsymbol{R}\times H_0^S$. Let r_1 and r_2 be the number of real primes of K and that of complex primes of K respectively. As usual we put $r=r_1+r_2-1$.

H_0^S is isomorphic to $W\times \boldsymbol{T}^{r_2}$, where $\boldsymbol{T}$ is the unit circle of $\boldsymbol{C}$ and W is a vector space over $\boldsymbol{R}$ of dimension r. Of course, the topology of W is different to the ordinary one. Let $\varepsilon_1, \cdots, \varepsilon_r$ be a system of independent totally positive units such that $\varepsilon_i\equiv 1$ mod. v for all non-archimedean primes v in S. By E we denote the group of units generated by the ε_i. Then by Unit Theorem, E can be regarded as a lattice in W. By $\mathfrak{m}$ we shall always understand a *module* whose prime factors are contained in S. Let $E_\mathfrak{m}$ denote the group of elements of E which are congruent to 1 mod. $\mathfrak{m}$. Let $V=\boldsymbol{R}e_1+\cdots+\boldsymbol{R}e_r$ be a vector space over $\boldsymbol{R}$ of dimension r with the ordinary topology, and let f be the linear map of V into W such that $f(e_i)=\varepsilon_i$. We put $L=\boldsymbol{Z}e_1+\cdots+\boldsymbol{Z}e_r=f^{-1}(E)$ and $L_\mathfrak{m}=f^{-1}(E_\mathfrak{m})$. For a subset X of V, $f(X)$ is an open neighbourhood of 0 if and only if X is open and contains one of the lattices $L_\mathfrak{m}$. Hence the completion $\hat{W}$ of W is isomorphic to $\varprojlim_{\mathfrak{m}} V/L_\mathfrak{m}$. Therefore we have

$$D^S=\boldsymbol{R}\times(\varprojlim_{\mathfrak{m}} V/L_\mathfrak{m})\times \boldsymbol{T}^{r_2}.$$

Proposition. D^S/H^S *is uniquely l-divisible.*

Proof. Since $D^S/H^S=\hat{W}/W$ and W is uniquely divisible, it is sufficient to show that $\hat{W}$ is uniquely l-divisible. It is clear that $\hat{W}$ is divisible. By Corollary of Theorem 3, for each module $\mathfrak{m}$ there exists a module $\mathfrak{m}'$ such that $E_{\mathfrak{m}'}\subset E_{\mathfrak{m}}^l$, hence $L_{\mathfrak{m}'}\subset lL_{\mathfrak{m}}$. This means that $\hat{W}=\varprojlim_{\mathfrak{m}} V/L_{\mathfrak{m}}$ has no l-torsion part. Q.E.D.

Corollary.

$$\hat{H}^i(\bar{G}, D^S)(l)=\begin{cases}(\boldsymbol{Z}/2\boldsymbol{Z})^{\alpha}, & \text{if } i \text{ is even and } l=2,\\ 0, & \text{if } i \text{ is odd or } l\neq 2,\end{cases}$$

where α is the number of ramified archimedean primes of k.

Theorem 4. *Let S be a set of rational primes, including the archimedean one. Then we have*

$$D^S\cong \boldsymbol{R}\times(V^S/\boldsymbol{Z})^r\times \boldsymbol{T}^{r_2}$$

and

$$(D^S)^*\cong \boldsymbol{R}\times \boldsymbol{Q}_S^r\times \boldsymbol{Z}^{r_2},$$

where $V^S=\boldsymbol{R}\times\prod_{p\in S_0}\boldsymbol{Z}_p$ in which $\boldsymbol{Z}$ is imbedded diagonally and $\boldsymbol{Q}_S$ is the additive group of S-integers of $\boldsymbol{Q}$ with the discrete topology.

Proof. By Corollary of Theorem 3, the filters $\{L_{\mathfrak{m}}\}$ and $\{mL\}$ are cofinal. Therefore we have $\varprojlim_{\mathfrak{m}} V/L_{\mathfrak{m}}=\varprojlim_{m} V/mL=(\varprojlim_{m} \boldsymbol{R}/m\boldsymbol{Z})^r$. Since $(\varprojlim_{m} \boldsymbol{R}/m\boldsymbol{Z})^*=\boldsymbol{Q}_S=(V^S/\boldsymbol{Z})^*$, the theorem is proved.

References

[1] E. Artin: Representatives of the connected component of the idèle class group. Proc. Int. Symp. Alg. Number Theory, Tokyo-Nikko, 51–54 (1955).

[2] E. Artin and J. Tate: Class Field Theory. Harvard (1961).

[3] A. Brumer: Galois groups of extensions of algebraic number fields with given ramification. Michigan Math. J., **13**, 33–40 (1966).

[4] I. R. Šafarevič: Extensions with given ramification points (in Russian). Publ. Math. I.H.E.S., No. 18 (1963).

[5] J.-P. Serre: Cohomologie Galoisienne. Springer Lecture Series, No. 5 (1963).

[6] T. Takahashi: Galois cohomology of finitely generated modules (to appear in Tôhoku Math. J.).

[7] J. Tate: Duality theorems in Galois cohomology over number fields. Proc. Int. Congr., Stockholm, 288–295 (1962).

[8] ——: On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. Sém. Bourbaki, exp. 306 (1965–66).

[9] K. Uchida: On Tate's duality theorems in Galois cohomology (to appear in Tôhoku Math. J.).

[10] A. Weil: Sur la théorie du corps de classes. J. Math. Soc. Japan, **3**, 1–35 (1951).