J. Math. Soc. Japan
Vol. 23, No. 2, 1971

On certain character groups attached to algebraic groups

By Takashi TASAKA

(Received Dec. 8, 1969)

§ 0. Introduction.

This paper is a continuation of my previous papers [9] and [10]. Using the duality theorems of Tate [1], we simplify the results in [9] and [10]. Our main tools are the auxiliary $\mathfrak{g}$-modules defined in [11]. Then our main results become mere applications of the duality theorems of Tate to the fundamental groups of simple algebraic groups. The $\mathfrak{g}(\bar{k}/k)$-module structures of the fundamental groups and their Galois cohomology over an algebraic number field k are already treated in Ono's [6] which is mainly concerned with the relative Tamagawa number of algebraic groups.

Let F be a quasi-split simple algebraic group defined over an algebraic number field k, and Z be the fundamental group of F (in the sense of algebraic groups) which is a finite $\mathfrak{g}$-module. Note that we denote by $\mathfrak{g}$ the Galois group of an algebraic closure $\bar{k}$ of k over k. We denote by F_A the adele group of F over k. It is shown in [9] and [10] that $F_k \cdot [F_A, F_A]$ is closed in F_A, where $[F_A, F_A]$ is the commutator subgroup of F_A, and that the quotient group $A_k(F) = F_A/F_k \cdot [F_A, F_A]$ is a totally disconnected compact group. In this paper, we consider the dual group $\Phi_k(F)$ of $A_k(F)$ in the sense of Pontrjagin, and show that

$$\Phi_k(F) \simeq H^1(\mathfrak{g}, Z'),$$

where $Z' = \mathrm{Hom}(Z, \boldsymbol{G}_m)$ (See Theorem 4). This is our main theorem.

In § 2, we investigate the $\mathfrak{g}$-module structure of the fundamental group Z, using the auxiliary $\mathfrak{g}$-modules defined in (4) and (5). In § 3, we consider their cohomology groups. In § 4, we give an alternative proof of the Hasse principle to the fundamental group Z (Theorem 2) (cf. [6], p. 106-107). In § 5, we prove our main theorems (Theorem 3 and Theorem 4). In § 6, we investigate more explicit structure of $H^1(\mathfrak{g}, Z')$ for some cases. In § 7, we apply our main theorems to calculate the class number of a lattice in its genus.

Some special notations.

We denote by μ_e the group of e-th roots of unity in $\bar{k}$ which has a natural $\mathfrak{g}$-module structure, and by $\boldsymbol{Z}_e$ the cyclic group of order e on which $\mathfrak{g}$ operates trivially. For a locally compact abelian group G, we denote by G^* the dual group of G in the sense of Pontrjagin. For a field k, we denote by $k^{\times}$ the multiplicative group $k-\{0\}$ of k, and by $(k^{\times})^e$ the subgroup of k generated by x^e, where x is contained in $k^{\times}$.

§ 1. Preliminaries.

Let F be a linear algebraic group defined over an algebraic number field k. The adele group F_A of F over k is, by definition, a restricted direct product of F_v, where v runs the set of all places of k and F_v denotes F_{k_v}. We call a *class character* of F over k a continuous representation of F_A into $\boldsymbol{R}/\boldsymbol{Z}$ which is trivial on F_k. We denote by $\Phi_k(F)$ the group of all class characters of F over k. Thus, if we put $B_k(F)=F_A/\overline{F_k\cdot[F_A, F_A]}$, where $[F_A, F_A]$ is the commutator subgroup of F_A, then $\Phi_k(F)$ is the dual group of $B_k(F)$ in the sense of Pontrjagin.

We assume that F is contained in $GL(V)$, where V is a finite dimensional vector space defined over k. We assume also that the canonical injection of F into $GL(V)$ is defined over k. A lattice L in V is a finitely generated $\mathfrak{o}$-module which spans V_k over k, where $\mathfrak{o}$ is the ring of integers of k. For a finite place $v=\mathfrak{p}$, we put $L_{\mathfrak{p}}=\mathfrak{o}_{\mathfrak{p}}\cdot L$, where $\mathfrak{o}_{\mathfrak{p}}$ is the ring of $\mathfrak{p}$-adic integers in $k_{\mathfrak{p}}$. Then $L_{\mathfrak{p}}$ is an $\mathfrak{o}_{\mathfrak{p}}$-lattice in $V_{k_{\mathfrak{p}}}$. Put $F_{\mathfrak{p}}(L)=\{g\in F_{\mathfrak{p}}: gL_{\mathfrak{p}}=L_{\mathfrak{p}}\}$. Then $F_{\mathfrak{p}}(L)$ is an open compact subgroup of $F_{\mathfrak{p}}$. We fix a finite set S of places of k containing the set S_∞ of all infinite places of k. We put

$$F_{A(S,L)}=\prod_{v\in S}F_v\times\prod_{v\notin S}F_v(L)\,. \tag{1}$$

DEFINITION 1. For a class character $\chi\in\Phi_k(F)$, we define a symbol $\mathfrak{f}(\chi)$ which will be called the conductor of χ. For a lattice L in V, and a finite set S of places of k, we define a symbol $\mathfrak{f}(S, L)$. We define that

$$\mathfrak{f}(\chi)\supset\mathfrak{f}(S, L) \tag{2}$$

means that χ is trivial on $F_{A(S,L)}$, and we say that the conductor $\mathfrak{f}(\chi)$ of χ contains $\mathfrak{f}(S, L)$.

We put

$$Cl_F(S, L)=\{\chi\in\Phi_k(F):\ \mathfrak{f}(\chi)\supset\mathfrak{f}(S, L)\}\,. \tag{3}$$

We call the class number of the lattice L relative to S the order $h_F(S, L)$ of $Cl_F(S, L)$ which may be infinite. M. Kneser has shown that, if F is semi-simple (and has no simple factors of certain type of E_8) and $F_S=\prod_{v\in S}F_v$ is not compact, then $h_F(S, L)$ is finite and equal to the number of double cosets in $F_k\backslash F_A/F_{A(S,L)}$, and that this number is also equal to the class number of the genus of the lattice L if $S=S_\infty$ ([3]). If F is the multiplicative group G_m of the universal domain of k, then $h_F(S_\infty, L)$ is equal to the class number of the field k, where L is a canonical lattice. If F is the additive group G_a of the universal domain, then $B_k(G_a)=(G_a)_A/(G_a)_k=k_A/k$ is a compact group. It is easy to see that $\Phi_k(G_a)\simeq k$. By the strong approximation theorem, we have $h(S, L)=1$ for any non-empty set S and any lattice L.

In this paper, we concern ourselves mainly with the quasi-split simple algebraic groups. In this paper, simple group means the algebraic group defined over k which is simple over the algebraic closure $\bar{k}$ of k, and which may have non-trivial center (of course, whose order is finite).

§ 2. $\mathfrak{g}$-module structures of the fundamental groups of simple algebraic groups.

Let k be a field of characteristic zero, and K be a finite extension of k of degree d, and $\bar{k}$ be an algebraic closure of k. We denote by $\mathfrak{g}$ the Galois group of $\bar{k}$ over k, and by $\mathfrak{h}$ that of $\bar{k}$ over K. Clearly $\mathfrak{g}$ has the Krull topology, and $\mathfrak{h}$ is an open subgroup of $\mathfrak{g}$ in this topology.

We consider three auxiliary $\mathfrak{g}$-modules defined in the following way (cf. [11] n°1);

$$\Lambda=\boldsymbol{Z}[\mathfrak{g}/\mathfrak{h}]=\sum_{i=1}^{d}\boldsymbol{Z}a_i\,, \tag{4}$$

$$0\longrightarrow C\longrightarrow \Lambda\xrightarrow{c}\boldsymbol{Z}\longrightarrow 0 \tag{5}$$

$$0\longrightarrow \boldsymbol{Z}u\xrightarrow{r}\Lambda\longrightarrow R\longrightarrow 0 \tag{6}$$

where $a_i=g_i\mathfrak{h}$ is the coset of g_i modulo $\mathfrak{h}$, and the map c is such that $c(\sum p_ia_i)=\sum p_i$, and $u=\sum a_i$, and r is the canonical injection and $R=\Lambda/r(\boldsymbol{Z}\cdot u)$. Thus $\boldsymbol{Z}\cdot u\simeq\boldsymbol{Z}$ as $\mathfrak{g}$-modules. These modules Λ, C and R are $\boldsymbol{Z}$-free $\mathfrak{g}$-modules whose ranks over $\boldsymbol{Z}$ are d, $d-1$ and $d-1$, respectively. It is known that, for any $\mathfrak{g}$-module M, we have

$$H^i(\mathfrak{g}, \Lambda\otimes M)\simeq H^i(\mathfrak{h}, M)\,,\qquad (i\geqq 1)\,. \tag{7}$$

Tensoring (5) and (6) by M, we have the following exact sequences:

$$0\longrightarrow C\otimes M\longrightarrow \Lambda\otimes M\xrightarrow{c\otimes 1}M\longrightarrow 0\,, \tag{8}$$

$$0\longrightarrow M\xrightarrow{r\otimes 1}\Lambda\otimes M\longrightarrow R\otimes M\longrightarrow 0\,. \tag{9}$$

In the derived cohomology sequences, through the identifications (7), $c\otimes 1$ induces the corestriction map of $H^i(\mathfrak{h}, M)$ into $H^i(\mathfrak{g}, M)$, and $r\otimes 1$ induces the restriction map of $H^i(\mathfrak{g}, M)$ into $H^i(\mathfrak{h}, M)$ (See [11] n°1).

Sometimes, we denote C and R by ${}^dC$ and ${}^dR$, respectively, to emphasize the degree d of the extension K of k. It is easy to see that $C \simeq R$ as $\mathfrak{g}$-modules if K is a cyclic extension of k.

Let F_1 be an algebraic group defined over k which is simple over $\bar{k}$. Let E_1 be a universal covering group of F_1, and π_1 be the covering isogeny of E_1 onto F_1. We may suppose that these are both defined over k. We call the fundamental group of F_1 the kernel Z_1 of π_1 which is contained in the center of E_1. When the fundamental group of F_1 coincides the center of E_1, we call F_1 the adjoint group. It is known that F_1 is an inner twist of certain quasi-split group F defined over k. So the fundamental group Z_1 of F_1 is $\mathfrak{g}$-isomorphic to that of F. Thus the problem is reduced to the problem to determine the $\mathfrak{g}$-module structure of the center of simply connected quasi-split group and to determine the $\mathfrak{g}$-submodules of this center. We express the $\mathfrak{g}$-module structures of these centers using the auxiliary $\mathfrak{g}$-modules defined above. Then it becomes easy to describe their cohomology groups.

Let F be a quasi-split simple group defined over k which is of adjoint type. Then there exists a unique finite Galois extension K of k such that F is quasi-split over k with respect to K (See [**10**] n°1). We denote the type of F by ${}^dX_n$, where $d=[K:k]$ and X_n is the type of F over the universal domain of k. Let E be a universal covering of F, and π be the covering isogeny of E onto F. We assume that these are defined over k. Then the kernel of π is the center Z of E which is a finite $\mathfrak{g}$-module.

According to Tate [**1**], we put $A' = \mathrm{Hom}(A, \boldsymbol{G}_m)$, for a finite $\mathfrak{g}$-module A. Clearly $(A')' = A$ as $\mathfrak{g}$-modules. For example, if we put $A = \mu_e$ (the group of e-th root of the unity in $\boldsymbol{G}_m$), then $A' \cong \boldsymbol{Z}_e$ (the cyclic group of order e on which $\mathfrak{g}$ operates trivially).

LEMMA 1. *Let k be a field of characteristic zero, and K be its finite extension. Let $\mathfrak{g}$ be the Galois group of $\bar{k}$ over k, and $\mathfrak{h}$ be that of $\bar{k}$ over K. We define $\mathfrak{g}$-modules Λ, C and R as in* (4), (5) *and* (6). *For a finite $\mathfrak{g}$-module A, we have*

$$(\Lambda \otimes A)' \simeq \Lambda \otimes A', \tag{10}$$

$$(C \otimes A)' \simeq R \otimes A' \tag{11}$$

where tensor products are taken over $\boldsymbol{Z}$.

PROOF. For a $\boldsymbol{Z}$-free $\mathfrak{g}$-module Y whose rank over $\boldsymbol{Z}$ is finite, we put $Y^0 = \mathrm{Hom}(Y, \boldsymbol{Z})$. It suffices to show that

$$(Y \otimes A)' \simeq Y^0 \otimes A', \tag{12}$$

because, in our case, we have $\Lambda^0 \simeq \Lambda$ and $C^0 \simeq R$ ([**11**]). The proof of (12) can be done by straightforward computations. (q. e. d.)

THEOREM 1. *Let Z be the fundamental group of an adjoint group F defined over a field k which is simple over $\bar{k}$. For the $\mathfrak{g}$-module structures of Z and Z', we have the following table:*

${}^dX_n$:	Z	Z'
${}^1A_n$:	μ_{n+1}	$\boldsymbol{Z}_{n+1}$
${}^2A_n$:	${}^2C\otimes\mu_{n+1}$	${}^2C\otimes\boldsymbol{Z}_{n+1}$
B_n, C_n :	μ_2	$\boldsymbol{Z}_2$
${}^1D_{2m}$:	$\mu_2\times\mu_2$	$\boldsymbol{Z}_2\times\boldsymbol{Z}_2$
${}^2D_{2m}$:	${}^2\Lambda\otimes\mu_2$	${}^2\Lambda\otimes\boldsymbol{Z}_2$
${}^1D_{2m+1}$:	μ_4	$\boldsymbol{Z}_4$
${}^2D_{2m+1}$:	${}^2C\otimes\mu_4$	${}^2C\otimes\boldsymbol{Z}_4$
${}^1E_6$:	μ_3	$\boldsymbol{Z}_3$
${}^2E_6$:	${}^2C\otimes\mu_3$	${}^2C\otimes\boldsymbol{Z}_3$
E_7 :	μ_2	$\boldsymbol{Z}_2$
E_8, F_4, G_2 :	trivial	
${}^3D_4$:	${}^3C\otimes\mu_2$	${}^3C\otimes\boldsymbol{Z}_2$
${}^6D_4$:	$C_1\otimes\mu_2$	$C_1\otimes\boldsymbol{Z}_2$

where C_1 and R_1 are the $\mathfrak{g}$-modules defined in (5) *and* (6) *relative to a cubic extension L of k which is contained in the Galois extension K of k whose Galois group is the symmetric group on three letters.*

Of course, we have $\mu_2\simeq\boldsymbol{Z}_2$ as $\mathfrak{g}$-modules. Note also that, in the case ${}^6D_4$, we have

$$R_1\otimes\mu_2\simeq C_1\otimes\mu_2\,.$$

PROOF. Let A be a maximal k-trivial torus of F. Then $T=Z(A)$ is a maximal torus of F defined over k ([**10**]). Let $\tilde{A}$ and $\tilde{T}$ be the corresponding tori of E. Then $\tilde{T}$ contains the center Z of E, and the kernel of the restriction of π to $\tilde{T}$ is equal to Z. If $[K:k]=1$, that is, F is a split group defined over k, the results are clear. We restrict ourselves to the case ${}^3D_4$. The others can be proved also in the similar way. For example, in the case ${}^2A_n$ (see [7], p. 245).

In the case ${}^3D_4$, we have $T\simeq\tilde{T}\simeq R_{K/k}(\boldsymbol{G}_m)\times\boldsymbol{G}_m$, where K is a cyclic extension of degree 3 ([**10**]). The covering isogeny π is given by

$$\pi(t_1,t_2,\bar{t}_2,\bar{\bar{t}}_2)=(t_1^2\cdot(t_2\bar{t}_2\bar{\bar{t}}_2)^{-1},\ t_2^2\cdot t_1^{-1},\ \bar{t}_2^2\cdot t_1^{-1},\ \bar{\bar{t}}_2^2\cdot t_1^{-1})\,,$$

where $t_1\in\boldsymbol{G}_m$ and $(t_2,\bar{t}_2,\bar{\bar{t}}_2)\in R_{K/k}(\boldsymbol{G}_m)$. So the kernel of π consists of the elements $(t_1,t_2,\bar{t}_2,\bar{\bar{t}}_2)$, where $t_1=1$, $t_2=\pm1$, $\bar{t}_2=\pm1$, $\bar{\bar{t}}_2=\pm1$, and $t_2\cdot\bar{t}_2\cdot\bar{\bar{t}}_2=1$. Then it is easy to see that the kernel of π and ${}^3C\otimes\mu_2$ are isomorphic $\mathfrak{g}$-modules. (q. e. d.)

Now it is easy to determine the $\mathfrak{g}$-submodules of Z. Except the case ${}^1A_n$, ${}^2A_n$, ${}^1D_n$ and ${}^2D_n$, there are no proper $\mathfrak{g}$-submodules of Z.

In the case ${}^1A_n$, the $\mathfrak{g}$-submodules of Z are μ_e, where e divides $n+1$. In the case ${}^2A_n$, the $\mathfrak{g}$-submodules of Z are ${}^2C\otimes\mu_e$, where e divides $n+1$. In the case ${}^1D_{2m+1}$, there are three proper $\mathfrak{g}$-submodules which are isomorphic to μ_2, and the special orthogonal group corresponds to one of them. In the case ${}^2D_{2m+1}$, ${}^1D_{2m}$ and ${}^2D_{2m}$, there is only one proper $\mathfrak{g}$-submodule which is isomorphic to μ_2.

§ 3. Determination of $H^1(k, Z)$ and $H^2(k, Z)$.

Let $Z=\mu_e$ be the group of e-th roots of the unity in $\boldsymbol{G}_m$. Putting $M=\bar{k}^\times=(\boldsymbol{G}_m)_{\bar{k}}$, we have the following exact sequence

$$0\longrightarrow\mu_e\longrightarrow M\overset{e}{\longrightarrow}M\longrightarrow 0 \tag{13}$$

where $e(x)=x^e$. Considering the derived cohomology sequence, we have, by the theorem 90 of Hilbert,

$$H^1(k,\mu_e)=k^\times/(k^\times)^e\,, \tag{14}$$

$$H^2(k,\mu_e)=\{\alpha\in B(k):\ e\alpha=0\} \tag{15}$$

where $B(k)$ is the Brauer group of k. Note that we use the notations $H^i(k, Z)$ $=H^i(\mathfrak{g}, Z)$, etc.

Let K be a quadratic extension of k. Tensoring (13) by $C={}^2C$, we have

$$0\longrightarrow C\otimes\mu_e\longrightarrow C\otimes M\overset{e}{\longrightarrow}C\otimes M\longrightarrow 0\,.$$

We know that

$$H^0(\mathfrak{g}, C\otimes M)\cong D(K^\times)=\{x\in K^\times:\ Nx=1\} \tag{16}$$

$$H^1(\mathfrak{g}, C\otimes M)\cong k^\times/NK^\times \tag{17}$$

$$H^2(\mathfrak{g}, C\otimes M)\simeq\{\beta\in B(K):\ c(\beta)=0\} \tag{18}$$

where N is the norm map of $K^\times$ into $k^\times$, and c is the corestriction map of $B(K)$ into $B(k)$ (See [11] n°2). So the derived cohomology sequence becomes

$$\begin{aligned}0&\longrightarrow H^0(C\otimes\mu_e)\longrightarrow D(K^\times)\overset{e}{\longrightarrow}D(K^\times)\\&\longrightarrow H^1(C\otimes\mu_e)\longrightarrow k^\times/NK^\times\overset{e^*}{\longrightarrow}k^\times/NK^\times\\&\longrightarrow H^2(C\otimes\mu_e)\longrightarrow H^2(C\otimes M)\overset{e}{\longrightarrow}H^2(C\otimes M)\,.\end{aligned}$$

It is easy to see that e^* is the identity map if e is odd, and that e^* is zero-map if e is even. We denote by $D_{K/k}(e)$ the quotient group $D(K^\times)/D(K^\times)^e$.

Sometimes we denote this group by $D_k(e)$ or $D(e)$. Thus we have

PROPOSITION 1. *Let K be a quadratic extension of k, and C be the $\mathfrak{g}$-modules defined in* (5). *Let μ_e be the group of e-th roots of unity.*

(i) *If e is odd, we have*

$$H^1(k, C\otimes\mu_e)\simeq D(e) \tag{19}$$

$$H^2(k, C\otimes\mu_e)\simeq\{\beta\in B(K):\ e\beta=0,\ c(\beta)=0\}. \tag{20}$$

(ii) *If e is even, we have*

$$0\longrightarrow D(e)\longrightarrow H^1(k, C\otimes\mu_e)\longrightarrow k^\times/NK^\times\longrightarrow 0 \tag{21}$$

$$0\longrightarrow k^\times/NK^\times\longrightarrow H^2(k, C\otimes\mu_e)\longrightarrow Q\longrightarrow 0, \tag{22}$$

where $Q=\{\beta\in B(K):\ e\beta=0,\ c(\beta)=0\}$.

In my previous paper [11] n°3, we have given more exact structure of $H^2(k, C\otimes\mu_e)$ which is characterized as that of the center of the group of type ${}^2A_{e-1}$. That is, when e is even, we have

$$H^2(k, C\otimes\mu_e)=\left\{(\alpha, \beta)\in B(k)\times B(K):\ 2\alpha=0,\ r(\alpha)=\frac{e}{2}\beta,\ c(\beta)=0\right\}, \tag{22$'$}$$

where r is the restriction map of $B(k)$ into $B(K)$.

Now we determine $H^1(k, Z')$ in the foregoing two cases. When $Z'\simeq \boldsymbol{Z}_e$, we know that

$$H^1(\mathfrak{g}, \boldsymbol{Z}_e)\simeq \mathrm{Hom}(\mathfrak{g}, \boldsymbol{Z}_e), \tag{23}$$

where $\mathrm{Hom}(\mathfrak{g}, \boldsymbol{Z}_e)$ is the group of all continuous homomorphisms of $\mathfrak{g}$ into $\boldsymbol{Z}_e$.

Tensoring (5) by $\boldsymbol{Z}_e$, we have

$$0\longrightarrow C\otimes \boldsymbol{Z}_e\longrightarrow \Lambda\otimes\boldsymbol{Z}_e\longrightarrow \boldsymbol{Z}_e\longrightarrow 0.$$

The derived cohomology sequence becomes

$$\begin{aligned}0\longrightarrow H^0(\mathfrak{g}, C\otimes\boldsymbol{Z}_e)\longrightarrow H^0(\mathfrak{h}, \boldsymbol{Z}_e)&\xrightarrow{c_0} H^0(\mathfrak{g}, \boldsymbol{Z}_e)\\ \longrightarrow H^1(\mathfrak{g}, C\otimes\boldsymbol{Z}_e)\longrightarrow \mathrm{Hom}(\mathfrak{h}, \boldsymbol{Z}_e)&\xrightarrow{c_1} \mathrm{Hom}(\mathfrak{g}, \boldsymbol{Z}_e).\end{aligned}$$

Clearly $H^0(\mathfrak{h}, \boldsymbol{Z}_e)$ and $H^0(\mathfrak{g}, \boldsymbol{Z}_e)$ are equal to $\boldsymbol{Z}_e$, and the map $c_0:\boldsymbol{Z}_e\to\boldsymbol{Z}_e$ is given by $c_0(x)=2x$, where $x\in\boldsymbol{Z}_e$. We denote by $\Delta_{K/k}(e)$ the kernel of c_1 which we will investigate in the later section. Sometimes we denote this group simply by $\Delta_k(e)$ or $\Delta(e)$. Thus we have

PROPOSITION 2. *The notations being as above.*

(i) *If e is odd, we have*

$$H^1(\mathfrak{g}, C\otimes\boldsymbol{Z}_e)\simeq\Delta(e). \tag{24}$$

(ii) *If e is even, we have*

(25) $$0 \longrightarrow \boldsymbol{Z}_2 \longrightarrow H^1(k, C\otimes \boldsymbol{Z}_e) \longrightarrow \Delta(e) \longrightarrow 0\,.$$

In § 6, we will show that

(25)′ $$H^1(k, C\otimes \boldsymbol{Z}_e) \simeq \boldsymbol{Z}_2 \times \Delta(e) \qquad \text{(direct product)}\,.$$

But this decomposition in direct product is not a canonical one (cf. Proposition 5).

If $Z = \Lambda\otimes A$, with a finite $\mathfrak{g}$-module A, we can utilize the formula (7). That is,

(26) $$H^i(k, \Lambda\otimes A) \simeq H^i(K, A)\,.$$

The same holds for $Z' = \Lambda\otimes A'$ (cf. Lemma 1).

Now let K be a cubic extension of k (cyclic or non-cyclic). We consider the exact sequence

(27) $$0 \longrightarrow C\otimes \mu_2 \longrightarrow C\otimes M \xrightarrow{\;2\;} C\otimes M \longrightarrow 0\,.$$

The derived cohomology sequence becomes

$$\begin{aligned} 0 &\longrightarrow H^0(C\otimes \mu_2) \longrightarrow D(K^\times) \longrightarrow D(K^\times) \\ &\longrightarrow H^1(C\otimes \mu_2) \longrightarrow k^\times/NK^\times \xrightarrow{\;2^*\;} k^\times/NK^\times \\ &\longrightarrow H^2(C\otimes \mu_2) \longrightarrow H^2(C\otimes M) \longrightarrow H^2(C\otimes M)\,. \end{aligned}$$

It is clear that 2^* is the inverse map, that is, $2^*(y) = y^{-1}$ for any element $y \in k^\times/NK^\times$. Thus

PROPOSITION 3. *Let K be a cubic extension of k, and $C = {}^3C$. Then we have*

(28) $$H^1(k, C\otimes \mu_2) \simeq D(K^\times)/D(K^\times)^2$$

(29) $$H^2(k, C\otimes \mu_2) \simeq \{\beta \in B(K) :\ 2\beta = 0,\ c(\beta) = 0\}\,.$$

In this case, $Z' \simeq Z$, because $\boldsymbol{Z}_2 \simeq \mu_2$.

§ 4. Localizations and Hasse principle.

Let k be an algebraic number field of finite degree over $\boldsymbol{Q}$. We denote by v a place of k, and by k_v the completion of k with respect to v. We denote by $\mathfrak{g}$ the Galois group of $\bar{k}$ over k, and by $\mathfrak{g}_v$ the Galois group of $\bar{k}_v = \bar{k}\cdot k_v$ over k_v. The group $\mathfrak{g}_v$ can be identified with the decomposition group of an extension w of v in $\bar{k}$. For a finite $\mathfrak{g}$-module A, by restriction of the group of operators to $\mathfrak{g}_v$, we have a finite $\mathfrak{g}_v$-module which we will denote by A_v. We denote $H^i(\mathfrak{g}_v, A_v)$ by $H^i(k_v, A_v)$. For an infinite place v of k, we use the Tate cohomology groups, that is, $H^i(k_v, A_v) = \hat{H}^i(k_v, A_v)$. In particular, if v is a complex place, we have $H^i(k_v, A_v) = 0$. When v is a finite place of k, we denote by $k_v(nr)$ the maximal unramified extension of k_v, whose Galois group over k_v will be denoted by $\mathfrak{a}_v$. Thus we have $\mathfrak{a}_v \simeq \mathfrak{g}_v/\mathfrak{b}_v$, where $\mathfrak{b}_v$ denotes the Galois group of $\bar{k}_v$ over $k_v(nr)$. A finite $\mathfrak{g}$-module A is called to be unramified over v if $\mathfrak{b}_v$ operates trivially on A_v. In this case, A_v becomes $\mathfrak{a}_v$-module in natural way, whose cohomology group $H^i(\mathfrak{a}_v, A_v)$ will be denoted by $H^i(\mathfrak{o}_v, A_v)$ or by $H^i_{nr}(k_v, A_v)$ (See [1] and [8]).

It is easy to see that a finite $\mathfrak{g}$-module A is unramified over almost all v (that is, except finite number of places). According to Serre [8], we denote by $P^i(k, A)$ the restricted direct product of $H^i(k_v, A_v)$ with respect to $H^i(\mathfrak{o}_v, A_v)$

$$P^i(k, A) = \prod_v (H^i(k_v, A_v), H^i(\mathfrak{o}_v, A_v))\,, \tag{30}$$

where $H^i(\mathfrak{o}_v, A_v) = H^i(k_v, A_v)$ if A is ramified over v. It is known that $P^0(k, A)$ is the direct product of $H^0(k_v, A_v)$, and $P^2(k, A)$ is the direct sum of $H^2(k_v, A_v)$. Because $H^i(k_v, A_v)$ are finite groups, $P^0(k, A)$ has a compact topology, and $P^2(k, A)$ has a discrete topology. But, in general, $P^1(k, A)$ is locally compact.

For the finite $\mathfrak{g}$-module $A' = \mathrm{Hom}(A, \boldsymbol{G}_m)$, we have $(A_v)' = (A')_v$. So we denote this $\mathfrak{g}_v$-module by A_v'.

THEOREM (Tate [**1**]). *$H^i(k_v, A_v)$ and $H^{2-i}(k_v, A'_v)$ are in exact duality with respect to the pairing "cup product".*

If A and A' are unramified over v, the annihilator of the subgroup $H^1(\mathfrak{o}_v, A_v)$ is exactly $H^1(\mathfrak{o}_v, A'_v)$.

Thus $P^i(k, A)$ and $P^{2-i}(k, A')$ are in exact duality (in the sense of Pontrjagin) for $i = 0, 1, 2$.

From the restriction map $H^i(k, A) \to H^i(k_v, A_v)$, we have the natural map

$$\rho_i : H^i(k, A) \longrightarrow P^i(k, A)\,. \tag{31}$$

Then the fundamental exact sequence of Tate is described in the following way;

$$\begin{array}{ccccccccc} 0 \longrightarrow H^0(k, A) & \xrightarrow{\rho_0} & P^0(k, A) & \longrightarrow & H^2(k, A')^* & \longrightarrow & H^1(k, A) & \overset{\rho_1}{\searrow} & \\ & & & & & & & & P^1(k, A)\,. \\ 0 \longleftarrow H^0(k, A')^* & \longleftarrow & P^2(k, A) & \xleftarrow{\rho_2} & H^2(k, A) & \longleftarrow & H^1(k, A')^* & \swarrow & \end{array} \tag{32}$$

For the meaning of unlabelled arrows, see [**1**].

THEOREM 2 (Hasse principle).*) *Let Z be the fundamental group of an algebraic group F defined over an algebraic number field k which is simple over $\bar{k}$. Then the map ρ_2 relative to Z is injective. It follows that*

$$0 \longrightarrow \rho_1(H^1(k, Z)) \longrightarrow P^1(k, Z) \longrightarrow H^1(k, Z')^* \longrightarrow 0$$

*) In T. Ono [**6**], 3.2, an equivalent assertion that $i^1(\hat{M}) = 1$ in the notation of [**6**] was proved. So the proof of Theorem 2 is an alternative one.

is an exact sequence. This means that $H^1(k, Z')$ is the exact annihilator of $\rho_1(H^1(k, Z))$ in $P^i(k, Z')=P^1(k, Z)^*$.

PROOF. It suffices to show the Hasse principle for the $\mathfrak{g}$-modules given in the Theorem 1.

If $Z=\mu_e$, then Z_v is also μ_e considered in $\bar{k}_v$, and the Hasse principle is clear from the class field theory.

Let K be a quadratic extension of k, and C is the $\mathfrak{g}$-module relative to K defined in (5). We consider the $\mathfrak{g}$-module $C\otimes\mu_e$. If a place v of k decomposes in K, then $(C\otimes\mu_e)_v\simeq\mu_e$. If v does not decompose in K, we denote by V the unique extension of v in K. Then $(C\otimes\mu_e)\simeq C_v\otimes\mu_e$, where C_v is the $\mathfrak{g}_v$-module relative to K_v defined in (5). It is well-known that, in the local fields, the corestriction map c of $B(L)$ into $B(k_v)$ is injective, where L is a finite extension of k_v. If e is odd, it follows from Proposition 1 that

$$P^2(k, C\otimes\mu_e)=\sum_v{}' H^2(k_v, \mu_e),$$

where v runs the set of all places of k decomposing in K. So the Hasse principle is clear, because the algebra class β of $B(K)$ such that $c(\beta)=0$ has the local invariant 0 at v if v does not decompose, and the local invariants y and $-y$ at V_1 and at V_2, respectively, if v decomposes, where V_1 and V_2 are the two extensions of v in K. Note that $y\in\boldsymbol{Q}/\boldsymbol{Z}$, and that, if $e\beta=0$, then $ey=0$.

Now suppose that e is even. From Proposition 1, it follows that $H^2(k_v, (C\otimes\mu_e)_v)\simeq\boldsymbol{Z}_2$ if v does not decompose, and that $H^2(k_v, (C\otimes\mu_e)_v)\simeq\boldsymbol{Z}_e$ if v decomposes. Thus we have

$$P^2(k, C\otimes\mu_e)=\sum_v{}' \boldsymbol{Z}_e\oplus\sum{}'' \boldsymbol{Z}_2,$$

where $\sum'$ means the direct sum over the places decomposing in K, and $\sum''$ means the direct sum over the places which do not decompose in K. Considering the local invariants of a pair $(\alpha, \beta)\in B(k)\times B(K)$ such that $2\alpha=0$, $r(\alpha)=\frac{e}{2}\beta$ and $c(\beta)=0$, which is a general element of $H^2(k, C\otimes\mu_e)$ according to (22)$'$, we can see that the Hasse principle holds. Note that r is the restriction map of $B(k)$ into $B(K)$.

Now consider the case where $Z\simeq\Lambda\otimes\mu_e$. Note that Λ is the $\mathfrak{g}$-module relative to a quadratic extension K defined in (4). If v decomposes, then $Z_v\simeq\mu_e\times\mu_e$ (direct product). If v does not decompose, then $Z_v=\Lambda_v\otimes\mu_e$, where Λ_v is the $\mathfrak{g}_v$-module relative to K_v defined in (4). Thus we have $P^2(k, \Lambda\otimes\mu_e)\simeq P^2(K, \mu_e)$, and the Hasse principle holds clearly, because of the formula (7).

Let K be a cubic extension of k (cyclic or non-cyclic), and $C={}^3C$ be the $\mathfrak{g}$-module relative to K defined in (5). We put $Z=C\otimes\mu_e$.

If v decomposes completely, that is, v has three extensions V_1, V_2 and V_3

in K, then $K_{V_i} \simeq k_v$, and $\mathfrak{g}_v$ is contained in the maximal normal subgroup of $\mathfrak{g}$ contained in $\mathfrak{h}$. Thus we have $(C\otimes\mu_e)_v \simeq \mu_e\times\mu_e$ (direct product).

If v does not decompose in K, denoting by V the unique extension of v in K, the completion K_V is a cubic extension of k_v. It is easy to see that $(C\otimes\mu_e)_v \simeq C_v\otimes\mu_e$, where C_v is the $\mathfrak{g}_v$-module relative to K_V defined in (5).

If v decomposes partially, that is, v has two extensions V_1 and V_2 in K such that one of K_{V_i} is equal to k_v, and the other is a quadratic extension of k_v. We assume that K_{V_2} is a quadratic extension of k_v. So $K_{V_1}=k_v$. Note that this case occurs only if K is not cyclic over k. We consider the Galois group $\mathfrak{g}_v$ as the decomposition group of an extension w of v in $\bar{k}$ which is also an extension of V_1. Let N be the minimal Galois extension of k containing K, and $\mathfrak{n}$ be the Galois group of $\bar{k}$ over N. Then the Galois group $G=\mathfrak{g}/\mathfrak{n}$ of N over k is isomorphic to the symmetric group on 3 letters. The group G is generated by s and t such that $s^2=1$, $t^3=1$ and $sts=t^{-1}$. We suppose that the Galois group $H=\mathfrak{h}/\mathfrak{n}$ of N over K is equal to the subgroup generated by s. Then the decomposition group of V_1 is equal to H. Thus $\mathfrak{g}_v$ is contained in $\mathfrak{h}$. The Galois group of $\bar{k}_v$ over K_{V_2} is $\mathfrak{n}_v=\mathfrak{n}\cap\mathfrak{g}_v$. In this case, we have

$$(C\otimes\mu_e)_v \simeq \Lambda_v\otimes\mu_e \tag{33}$$

where Λ_v is the $\mathfrak{g}_v$-module relative to K_{V_2} defined in (4).

We prove (33). The $\mathfrak{g}$-module C is $\mathfrak{g}$-isomorphic to a $\boldsymbol{Z}$-free module generated by $c_1=a_1-a_0$ and $c_2=a_2-a_0$, where $a_0=H$, $a_1=tH$ and $a_2=t^2H$. Obviously $\mathfrak{n}_v$ operates trivially on C. Fix an element of $\mathfrak{g}_v-\mathfrak{n}_v$. This element induces the element s of H. It is easy to see that $sc_1=c_2$ and $sc_2=c_1$. This proves the formula (33).

Now we consider $H^2(k_v, (C\otimes\mu_2)_v)$. From the arguments above, it follows that $H^2(k_v, (C\otimes\mu_2)_v)\simeq\boldsymbol{Z}_2\times\boldsymbol{Z}_2$ if v decomposes completely, and $H^2(k_v, (C\otimes\mu_2)_v)=0$ if v does not decompose, and $H^2(k_v, (C\otimes\mu_2)_v)=\boldsymbol{Z}_2$ if v decomposes partially. An algebra class $\beta\in B(K)$ such that $c(\beta)=0$ has the local invariants y_1, y_2 and y_3 at V_1, V_2 and V_3, respectively, where $\sum y_i=0$, if v decomposes completely, and the local invariant 0 at V if v does not decompose, and the local invariants y and $-y$ at V_1 and V_2, respectively, if v decomposes partially. If $2\beta=0$, then each local invariant y is such that $2y=0$. This shows that the Hasse principle holds for $Z={}^3C\otimes\mu_2$. For the behaviour of the local invariants under the restriction map and the corestriction map, see Artin-Tate [2] Chapter 7, 3.

The rest of the theorem is clear from the duality theorem of Pontrjagin. This completes the proof.

§ 5. The character group $\Phi_k(F)$.

Let F be a quasi-split simple algebraic group over a field k of characteristic zero with respect to a finite Galois extension K of k, and Z be its fundamental group. Let A be a maximal k-trivial torus of F, and $T=Z(A)$ be the centralizer of A in F. It is known that T is a maximal torus of F defined over k. We denote by $\tilde{T}$ the maximal torus of the universal covering group E of F corresponding to T by the covering isogeny π. It is known that $H^1(k, \tilde{T})=0$ ([11] n°3), and that the following two formulae hold ([10] Theorem 1):

$$[E_k, E_k]=E_k\,, \tag{34}$$

$$F_k/\pi(E_k)\simeq T_k/\pi(\tilde{T}_k)\simeq H^1(k, Z) \tag{35}$$

where $[E_k, E_k]$ is the commutator subgroup of E_k. It follows that the sequence

$$1 \longrightarrow Z_k \longrightarrow E_k \xrightarrow{\pi} F_k \longrightarrow H^1(k, Z) \longrightarrow 1 \tag{36}$$

is exact.

Now suppose that k is an algebraic number field. It is easy to see that, for a place v of k, the group F is quasi-split over k_v with respect to K_V, where V is an extension of v in K, except the case where F is of type ${}^6D_4$ and v decomposes partially in K, and that, in the exceptional case, the group F is quasi-split over k_v with respect to K_{V_2}, where V_2 is an extension of v in K such that K_{V_2} is a quadratic extension of k_v. For these, it suffices to examine the structure of T over k_v, because T is characterized as $T=Z(A)$. It follows from these that $\mathfrak{g}_v$-module Z_v is isomorphic to the fundamental group of F considered as an algebraic group defined over k_v, where Z is the fundamental group of F over k which is a finite $\mathfrak{g}$-module (cf. Theorem 1 and the proof of Theorem 2). By abuse of notation, we use the notations $F_v=F_{k_v}$, etc.

THEOREM 3. *Let F be a quasi-split simple group defined over an algebraic number field k, and Z be its fundamental group. Then the commutator subgroup $[F_A, F_A]$ of the adele group F_A of F over k is closed in F_A. For the quotient group, we have a topological isomorphism*

$$F_A/[F_A, F_A]\cong P^1(k, Z)\,, \tag{37}$$

where $P^1(k, Z)$ is the group defined in (30).

PROOF. The first statement is already shown in [10], p. 163. It is easy to see that

$$F_A/[F_A, F_A]\simeq \prod_v (F_v/\pi(E_v),\, F_{\mathfrak{o}_v}\cdot\pi(E_v)/\pi(E_v)) \tag{38}$$

where the second term means the restricted direct product of $F_v/\pi(E_v)$ with respect to $F_{\mathfrak{o}_v}\cdot\pi(E_v)/\pi(E_v)$ ([10] the formula (53)). Note that $\pi(E_v)$ coincides with $[F_v, F_v]$ ([10], Theorem 1). From the exact sequence (36), it follows that $F_v/\pi(E_v)\simeq H^1(k_v, Z_v)$ for all places v of k. Thus it suffices to show that $F_{\mathfrak{o}_v}\cdot\pi(E_v)/\pi(E_v)$ is isomorphic to $H^1(\mathfrak{o}_v, Z_v)$ for almost all v.

Consider the set of finite places v of k which are unramified in the finite Galois extension K, and which do not divide the order of Z. Then it is easily seen that Z is unramified over places of this set, and that almost all places of k are contained in this set. For a place v of this set, we have

$$(39)\qquad F_{\mathfrak{o}_v}\cdot\pi(E_v)/\pi(E_v)\simeq F_{\mathfrak{o}_v}/F_{\mathfrak{o}_v}\cap\pi(E_v)\simeq F_{\mathfrak{o}_v}/\pi(E_{\mathfrak{o}_v})\simeq T_{\mathfrak{o}_v}/\pi(\tilde{T}_{\mathfrak{o}_v})\,.$$

(See [10], Theorem 3 and its proof). Let $k_v(nr)$ be the maximal unramified extension of k_v, and $\mathfrak{a}_v$ be its Galois group over k_v. We denote by U the unit group of $k_v(nr)$, and by $T_v(U)$ the group of all $k_v(nr)$-rational points of T whose coordinates are contained in U. Then we have the following exact sequence of $\mathfrak{a}_v$-modules:

$$(40)\qquad 0\longrightarrow Z_v\longrightarrow \tilde{T}_v(U)\xrightarrow{\ \pi\ } T_v(U)\longrightarrow 0\,.$$

The surjectivity of π comes from the following fact: If v does not divide a natural number e, then the sequence

$$(41)\qquad 0\longrightarrow \mu_e\longrightarrow U\xrightarrow{\ e\ } U\longrightarrow 0$$

is exact, where $e(x)=x^e$ for $x\in U$. From the theorem of Nakayama [4], Theorem 2, considering the derived cohomology sequence of (40), it follows that

$$(42)\qquad 0\longrightarrow Z_v^{\mathfrak{a}_v}\longrightarrow \tilde{T}_{\mathfrak{o}_v}\xrightarrow{\ \pi\ } T_{\mathfrak{o}_v}\longrightarrow H^1(\mathfrak{a}_v, Z_v)\longrightarrow 0\,.$$

(See also [5], footnotes 10 and 11 in p. 118). From the definition, $H^1(\mathfrak{a}_v, Z_v)$ is equal to $H^1(\mathfrak{o}_v, Z_v)$ (cf. § 4). Thus our theorem is proved.

REMARK. The references are made only for non-split quasi-split groups. The corresponding results for split groups have been proved in [9].

COROLLARY. *Under the isomorphism* (37), *the subgroup* $F_k\cdot[F_A, F_A]/[F_A, F_A]$ *is mapped onto the subgroup* $\rho_1(H^1(k, Z))$, *where* ρ_1 *is the mapping defined in* (31).

PROOF. Because of the sequence (36), this corollary is clear.

THEOREM 4. *Let F be a quasi-split simple algebraic group over an algebraic number field k, and Z be its fundamental group. We denote by $\Phi_k(F)$ the group of all class characters of F. Then we have*

$$(43)\qquad \Phi_k(F)\simeq H^1(k, Z')$$

where $Z'=\mathrm{Hom}\,(Z, \boldsymbol{G}_m)$.

PROOF. We denote by $X(F_A)$ the group of all continuous representations of F_A into $\boldsymbol{R}/\boldsymbol{Z}$. Then $X(F_A)$ is the dual group of $F_A/[F_A, F_A]$. From Theorem

3, this dual group is isomorphic to $P^1(k, Z)^* \simeq P^1(k, Z')$. A class character of F is a character of F_A which annihilates $F_k \cdot [F_A, F_A]$. From the Corollary to Theorem 3, it follows that $\Phi_k(F)$ is isomorphic to the annihilator of $\rho_1(H^1(k, Z))$. Thus the theorem follows from the theorem 2 in § 4. (q. e. d.)

§ 6. Dihedral extensions.

Let k be a field of characteristic zero, and K be its quadratic extension. We denote by $\mathfrak{g}$ the Galois group of $\bar{k}$ over k, and by $\mathfrak{h}$ the Galois group of $\bar{k}$ over K. We investigate the group $\Delta(e) = \Delta_{K/k}(e)$ which is the kernel of the corestriction map c of $\mathrm{Hom}(\mathfrak{h}, \boldsymbol{Z}_e)$ into $\mathrm{Hom}(\mathfrak{g}, \boldsymbol{Z}_e)$. At first, we know that $H^1(\mathfrak{h}, \boldsymbol{Z}_e) \simeq H^1(\mathfrak{g}, \Lambda \otimes \boldsymbol{Z}_e)$, where Λ is the $\mathfrak{g}$-module relative to K defined in (4). We make the explicit correspondence between these groups. For an element φ of $H^1(\mathfrak{h}, \boldsymbol{Z}_e) = \mathrm{Hom}(\mathfrak{h}, \boldsymbol{Z}_e)$, we put

$$(44) \qquad \begin{cases} \varphi_1(S) = \varphi(S) \\ \varphi_1(\sigma S) = \varphi(\sigma S \sigma), \end{cases} \qquad \begin{cases} \varphi_2(S) = \sigma\varphi(\sigma^{-1} S \sigma) \\ \varphi_2(\sigma S) = \sigma\varphi(S) \end{cases}$$

where $S \in \mathfrak{h}$, and σ is a fixed element of $\mathfrak{g} - \mathfrak{h}$, and $\sigma\varphi(S) = \sigma(\varphi(S))$, for example. So we have $\varphi_2(S) = \varphi(\sigma^{-1} S \sigma)$ and $\varphi_2(\sigma S) = \varphi(S)$ in our case. Then $a_1 \otimes \varphi_1(X) + a_2 \otimes \varphi_2(X)$ with $X \in \mathfrak{g}$ is 1-cocycle of $\mathfrak{g}$ into $\Lambda \otimes \boldsymbol{Z}_e$, where a_1 and a_2 are the canonical base of Λ. The inverse correspondence is given by the restriction of φ_1 to $\mathfrak{h}$. The corestriction map c of $\mathrm{Hom}(\mathfrak{h}, \boldsymbol{Z}_e)$ into $\mathrm{Hom}(\mathfrak{g}, \boldsymbol{Z}_e)$ is given by $c(\varphi)(X) = \varphi_1(X) + \varphi_2(X)$. Thus $c(\varphi) = 0$ means that

$$(45) \qquad \begin{cases} \varphi(S) + \varphi(\sigma^{-1} S \sigma) = 0 \\ \varphi(\sigma S \sigma) + \varphi(S) = 0. \end{cases}$$

This condition is equivalent to

$$(46) \qquad \begin{cases} \varphi(\sigma^{-1} S \sigma) = -\varphi(S) \\ \varphi(\sigma^2) = 0. \end{cases}$$

We denote by $\mathfrak{d}$ the closed subgroup of $\mathfrak{h}$ generated by $[\mathfrak{h}, \mathfrak{h}]$ and τ^2 ($\tau \in \mathfrak{g} - \mathfrak{h}$). Clearly $\mathfrak{d}$ is a normal subgroup of $\mathfrak{g}$. It is easy to see that, for an element φ of $\mathrm{Hom}(\mathfrak{h}, \boldsymbol{Z}_e)$, the condition $c(\varphi) = 0$ is equivalent to the condition $\ker \varphi \supset \mathfrak{d}$.

For an element $\varphi \in \Delta(e)$, we denote by $\mathfrak{n}$ the kernel of φ, and by N the extension of K corresponding to $\mathfrak{n}$. Clearly $\mathfrak{n}$ is a normal subgroup of $\mathfrak{g}$.

PROPOSITION 4. *We put $G = \mathfrak{g}/\mathfrak{n}$ and $H = \mathfrak{h}/\mathfrak{n}$. Then G is a dihedral group of degree f with the canonical cyclic subgroup H, where $f = [N : K]$ is the order of H which is equal to that of the image of φ.*

PROOF. From the first equation of (46), the operation of G on H is clearly that of the dihedral groups. As τ^2 is contained in $\mathfrak{d}\subset\mathfrak{n}$ for $\tau\in\mathfrak{g}-\mathfrak{h}$, the elements of $G-H$ are of order two. This shows that G is a dihedral group. (q. e. d.)

DEFINITION 2. We call an element φ of $\Delta(e)$ a dihedral character of $\mathfrak{h}$. Let N be the extension of K corresponding to $\mathfrak{n}=\ker\varphi$. We call N a dihedral extension of k of degree f relative to K, where $f=[N:K]$.

Now we will prove (25)′. That is

PROPOSITION 5. *Let C be the $\mathfrak{g}$-module relative to K defined in* (5). *If e is an even number, we have*

$$H^1(\mathfrak{g}, C\otimes \boldsymbol{Z}_e)\simeq \boldsymbol{Z}_2\times\Delta(e) \qquad \text{(direct product)}. \tag{25'}$$

But this decomposition is not a canonical one.

PROOF. We put $b=a_2-a_1$ which is the canonical base of C, where a_1 and a_2 are the canonical base of Λ. Thus $C\otimes\boldsymbol{Z}_e=\{b\otimes\alpha:\ \alpha\in\boldsymbol{Z}_e\}$. We denote by λ the canonical generator of $\boldsymbol{Z}_e$. Note that we use the additive notation in $\boldsymbol{Z}_e$. Let $g_s=b\otimes\alpha_s$ be a 1-cocycle of $\mathfrak{g}$ into $C\otimes\boldsymbol{Z}_e$. From the cocycle condition $g_{st}=sg_t+g_s$, it follows that

$$\begin{cases} \alpha_{st}=\alpha_s+\alpha_t: & s\in\mathfrak{h} \\ \alpha_{st}=\alpha_s-\alpha_t: & s\notin\mathfrak{h}\,. \end{cases} \tag{47}$$

Denoting by φ the restriction of α to $\mathfrak{h}$, we can see that φ is a dihedral character. Conversely for a dihedral character φ in $\Delta(e)$, we put $\alpha_S=\varphi(S)$ and $\alpha_{S\sigma}=\varphi(S)$ for $S\in\mathfrak{h}$, where σ is a fixed element of $\mathfrak{g}-\mathfrak{h}$. It is easy to see that $g_s=b\otimes\alpha_s$ is a 1-cocycle of $\mathfrak{g}$ into $C\otimes\boldsymbol{Z}_e$. This map gives a cross-section of $\Delta(e)$ into $H^1(\mathfrak{g}, C\otimes\boldsymbol{Z}_e)$ in the sequence (25). Note that this cross-section depends on the choice of σ.

Now we put

$$\begin{cases} \alpha_S=0\,, \\ \alpha_{S\sigma}=\lambda\,, \end{cases} \tag{48}$$

for $S\in\mathfrak{h}$. Then $g_s=b\otimes\alpha_s$ is a 1-cocycle of $\mathfrak{g}$ into $C\otimes\boldsymbol{Z}_e$ which is non-trivial because of the assumption that e is even. We denote by ω the element of $H^1(\mathfrak{g}, C\otimes\boldsymbol{Z}_e)$ corresponding to this cocycle. Clearly the order of ω is two. The subgroup $\langle 0,\omega\rangle$ of $H^1(\mathfrak{g}, C\otimes\boldsymbol{Z}_e)$ is the canonical image of $\boldsymbol{Z}_2$ in the sequence (25). This proves the proposition.

REMARK. Two elements σ and τ in $\mathfrak{g}-\mathfrak{h}$ give the same direct decomposition if and only if $\sigma\tau^{-1}\in\mathfrak{h}_2$, where $\mathfrak{h}_2$ is the subgroup of $\mathfrak{h}$ generated by S^2 with $S\in\mathfrak{h}$. Clearly $\mathfrak{h}_2$ is a normal subgroup of $\mathfrak{g}$.

Now we suppose that the base field k is a $\mathfrak{p}$-adic field, and that K is a quadratic extension of k. From the local class field theory, it follows that $k^\times/NK^\times\simeq\boldsymbol{Z}_2$. Thus the sequence (21) becomes

$$0 \longrightarrow D(e) \longrightarrow H^1(k, C\otimes\mu_e) \longrightarrow \boldsymbol{Z}_2 \longrightarrow 0. \tag{49}$$

From the local duality theorem of Tate, we know that $H^1(k, C\otimes\mu_e) \simeq H^1(k, C\otimes \boldsymbol{Z}_e)^*$. Moreover, we have

THEOREM 5. *Let k be a $\mathfrak{p}$-adic field, and K be its quadratic extension. We suppose that e is an even number. The annihilator of $D(e)$ in $H^1(k, C\otimes\mu_e)$ is exactly the subgroup $\langle 0, \omega\rangle$ of $H^1(k, C\otimes \boldsymbol{Z}_e)$, where ω is the element defined in* (48). *It follows that*

$$\Delta(e)^* \simeq D(e), \tag{50}$$

and this isomorphism is defined in a canonical way.

PROOF. It is known from the duality theorems of Pontrjagin that the order of the annihilator of $D(e)$ is two. Thus it suffices to show that ω is contained in this annihilator. The pairing between $H^1(k, C\otimes\mu_e)$ and $H^1(k, C\otimes \boldsymbol{Z}_e)$ is given by "cup-product". An element x of $D(K^\times)$ gives 1-cocycle $\xi_s = b\otimes y - s(b\otimes y)$ of $\mathfrak{g}$ into $C\otimes\mu_e$, where y is an element of $M=\bar{k}^\times$ such that $x=y^e$. These 1-cocycles generate the subgroup $D(e)$. Clearly $\xi_s = b\otimes(y\cdot s(y^{-1}))$ if $s\in\mathfrak{h}$, and $\xi_s = b\otimes(y\cdot s(y))$ if $s\notin\mathfrak{h}$. Note that we use the multiplicative notation in μ_e. Cup-product $\omega\cup\xi$ of ξ and ω is given by

$$(\omega\cup\xi)_{s,t} = \omega_s(s\xi_t) = \begin{cases} 1 & : \quad s\in\mathfrak{h}, \\ s(y^{-1})\cdot st(y) & : \quad s\notin\mathfrak{h},\ t\in\mathfrak{h}, \\ (s(y)\cdot st(y))^{-1} & : \quad s,\ t\notin\mathfrak{h}. \end{cases} \tag{51}$$

Note that λ is the canonical generator of $\boldsymbol{Z}_e = \mu_e'$. This is a 2-cocycle of $\mathfrak{g}$ into μ_e. It suffices to show that this 2-cocycle is split in $H^2(\mathfrak{g}, M)$, because $H^2(\mathfrak{g}, \mu_e)$ is mapped into $H^2(\mathfrak{g}, M)$ injectively. We put

$$z_s = \begin{cases} y_1\cdot s(y_1^{-1}) : & s\in\mathfrak{h}, \\ y_1\cdot s(y_1) \ : & s\notin\mathfrak{h}, \end{cases}$$

where y_1 is an element of M such that $y_1^2 = y$. Then it is easy to show that $(\omega\cup\xi)_{s,t}\cdot(\delta z)_{s,t} = 1$, where δz means the coboundary of 1-cochain z. This proves the first statement of the theorem. The rest is clear because of the Pontrjagin duality. (q. e. d.)

REMARK 1. The formula (50) holds also if e is an odd number.

REMARK 2. The formula (50) holds trivially for the real number field with respect to the complex number field, because $\Delta(e)=0$ and $D(e)=0$, in our case.

§ 7. Class number.

Let k be an algebraic number field, and K be its finite extension. We denote by $\mathfrak{g}$ the Galois group of $\bar{k}$ over k, and by $\mathfrak{h}$ the Galois group of $\bar{k}$ over K. We want to calculate the class number for a quasi-split simple group F defined over k (cf. § 1).

In view of Theorem 3 and Theorem 4, we define a class number for $P^1(k, Z)$ (with respect to some finite set S of places of k), where Z is a finite $\mathfrak{g}$-module. We assume that the Hasse principle holds for Z. That is, the map ρ_2 relative to Z in (31) is injective. From Tate's exact sequence, it follows that the map ρ_1' of $H^1(k, Z')$ into $P^1(k, Z')$ is injective, and that the annihilator of $\rho_1(H^1(k, Z))$ is exactly $H^1(k, Z')$ (cf. Theorem 2).

DEFINITION 3. Let S be a finite set of places of k containing all infinite places and all places over which Z or Z' is ramified (cf. § 4). Putting

$$(52) \qquad Cl_Z(S) = \{\chi \in H^1(k, Z') : \chi_v = 0 \text{ for all } v \in S \text{ and } \chi_v \in H^1(\mathfrak{o}_v, Z_v') \text{ for other } v\},$$

where χ_v denotes the canonical image of χ in $H^1(k_v, Z_v')$, we denote by $h_Z(S)$ the cardinality of $Cl_Z(S)$, and we call $h_Z(S)$ the class number of Z relative to S.

We can apply this class number to calculate the class number of a lattice in its genus for a quasi-split simple group defined over k with some modifications.

We calculate the class numbers for the finite $\mathfrak{g}$-modules $Z = \mu_e$, ${}^2C \otimes \mu_e$ and ${}^3C \otimes \mu_2$, and we denote these class numbers by $h_1(e, S)$, $h_2(e, S)$ and $h_3(2, S)$, respectively. Note that, if $Z = \Lambda \otimes \mu_e$, where Λ is the $\mathfrak{g}$-module relative to K defined in (4), the problem is reduced to the case where the base field is K.

CASE $h_1(e, S)$: We denote by $k(e)$ the composite of all cyclic extensions of k of degree f, where f is a divisor of e. We also denote by $L(S)$ the maximal unramified abelian extension of k in which the places in S decompose completely. Putting $L(e, S) = k(e) \cap L(S)$, we have the following proposition (cf. [**9**] Theorem 2):

PROPOSITION 6. *The notations being as above, we have*

$$(53) \qquad h_1(e, S) = [L(e, S) : k] .$$

PROOF. In our case, we have $H^1(k, Z') = \mathrm{Hom}(\mathfrak{g}, \boldsymbol{Z}_e)$. For an element χ of $Cl_1(e, S)$ (the class group for $Z = \mu_e$), we denote by N_χ the cyclic extension of k corresponding to the kernel of χ. From the class field theory, it follows that the composite of all N_χ with $\chi \in Cl_1(e, S)$ is equal to $L(e, S)$, and that the Galois group of $L(e, S)$ over k is isomorphic to $Cl_1(e, S)$. Thus (53) is proved. (q. e. d.)

CASE $h_2(e, S)$: We denote by $\bar{S}$ the set of all places above S in K. We denote by $\mathfrak{k}(e)$ the composite of all dihedral extensions of k of degree f, where f is a divisor of e. We also denote by $M(S)$ the maximal unramified abelian extension of K in which all places of K in $\bar{S}$ decompose completely. We put $M(e, S) = \mathfrak{k}(e) \cap M(S)$. Then $M(e, S)$ is a generalized dihedral extension of k, that is, a composite of dihedral extensions of k relative to K.

PROPOSITION 7. *The notations being as above*:

(i) *If e is odd, we have*

$$h_2(e, S) = [M(e, S) : K]. \tag{54}$$

(ii) *If e is even, we have*

$$h_2(e, S) \leqq [M(e, S) : K]. \tag{55}$$

PROOF. If e is odd, we have $H^1(k, Z') \simeq \Delta(e)$ (See Proposition 2). For an element of $\Delta(e)$, there corresponds a dihedral extension of k (See Proposition 4). Thus the proof of (54) is similar to that of (53). If e is even, then we have the following exact sequence:

$$0 \longrightarrow \boldsymbol{Z}_2 \longrightarrow H^1(k, Z') \xrightarrow{i} \Delta(e) \longrightarrow 0$$

(See (25)). Thus, for an element $\varphi \in \Delta(e)$, there exist exactly two elements χ and χ_1 of $H^1(k, Z')$ such that $i(\chi) = i(\chi_1) = \varphi$. Their difference $\chi - \chi_1$ is the element ω defined in (48). For a place v of k, $\omega_v = 0$ if v decomposes in K, and ω_v is the corresponding element in $H^1(k_v, C_v \otimes \boldsymbol{Z}_e)$ if v does not decompose. We fix a place v of k which is not contained in S. It is easy to see that ω_v is contained in $H^1(\mathfrak{o}_v, Z'_v)$, and that $\chi_v \in H^1(\mathfrak{o}_v, Z'_v)$ if and only if $(\chi_1)_v \in H^1(\mathfrak{o}_v, Z'_v)$. For example, use the Inflation-Restriction sequence. When v does not decompose we denote by $\Delta_{\mathfrak{o}_v}(e)$ the image $i_v(H^1(\mathfrak{o}_v, Z'_v))$ which is the kernel of the corestriction map of $H^1(\mathfrak{O}_V, \boldsymbol{Z}_e)$ into $H^1(\mathfrak{o}_v, \boldsymbol{Z}_e)$, where $\mathfrak{O}_V$ is the integer ring of K_V. When v decomposes, we denote also by $\Delta_{\mathfrak{o}_v}(e)$ the group $H^1(\mathfrak{o}_v, Z'_v)$.

For $\Delta(e)$, we put

$$Cl_2^0(e, S) = \{\varphi \in \Delta(e) : \varphi_v = 0 \text{ for all } v \in S \text{ and } \varphi_v \in \Delta_{\mathfrak{o}_v}(e) \text{ for other } v\}.$$

Then the cardinality $h_2^0(e, S)$ of $Cl_2^0(e, S)$ is equal to $[M(e, S) : K]$ as in the case (54). If $\varphi_v = 0$, then one of χ_v and $(\chi_1)_v$ is zero, and the other is equal to ω_v. Thus we have $h_2(e, S) \leqq h_2^0(e, S)$. This proves (55). (q. e. d.)

REMARK. In general, we can not expect the equality in the inequality (55). For example, put $e = 2$. Then $\mu_2 \simeq C \otimes \mu_2$, and we have $h_1(e, S) = h_2(2, S)$. But, in general, $h_2^0(2, S)$ is not equal to $h_1(2, S)$.

CASE $h_3(2, e)$: Let K be a cubic extension of k, and ${}^3C$ be the $\mathfrak{g}$-module relative to K defined in (5). We denote by $\bar{S}$ the set of all places above S in K. As in Proposition 2, we can see that $H^1(k, {}^3C \otimes \boldsymbol{Z}_2)$ is equal to the kernel of the corestriction map of $H^1(\mathfrak{h}, Z_2)$ into $H^1(\mathfrak{g}, Z_2)$. We denote this kernel by ${}^3\Delta(2)$. We put $Cl_3(2, S)=\{\chi\in{}^3\Delta(2): \chi_v=0$ for all $v\in S$ and $\chi_v\in H^1(\mathfrak{o}_v, Z')$ for other $v\}$. For an element $\chi\in Cl_3(2, S)$, we denote by N_χ the extension of K corresponding to the kernel of χ. It is clear that, if χ is not zero, N_χ is an unramified quadratic extension in which the place of $\bar{S}$ decomposes (completely). Denoting by $N(S)$ the composite of all N_χ with $\chi\in Cl_3(2, S)$, we have

$$h_3(2, S)=[N(S): K]\,. \tag{56}$$

Clearly, $h_3(2, S)$ is a power of 2.

I have no idea to characterize the quadratic extension N_χ of K, or the extension $N(S)$ of K.

College of General Education
University of Tokyo

References

[1] J. Tate, Duality theorems in Galois cohomology over number fields, Proc. Congress, Stockholm, 1962, 288–295.
[2] E. Artin and J. Tate, Class field theory, Harvard, 1961.
[3] M. Kneser, Strong approximation, Algebraic groups and discontinuous subgroups, Proc. of Symp. in pure Math., Amer. Math. Soc., IX (1966), Part II, 187–196.
[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 relative theory of Tamagawa numbers, Ann. of Math., 82 (1965), 88–111.
[7] I. Satake, Symplectic representations of algebraic groups satisfying a certain analyticity condition, Acta Math., 117 (1967), 215–279.
[8] J.-P. Serre, Cohomologie galoisienne, Lecture notes in Math., 5 (1965), Springer-Verlag.
[9] T. Tasaka, Sur les groupes algébriques semi-simples déployés, J. Math. Soc. Japan, 20 (1968), 390–399.
[10] T. Tasaka, On the quasi-split simple algebraic groups defined over an algebraic number field, J. Fac. Sci. Univ. Tokyo Sect. I, 15 (1968), 147–168.
[11] T. Tasaka, On the second cohomology groups of the fundamental group of simple algebraic groups over perfect field, J. Math. Soc. Japan, 21 (1969), 244–258.