J. Math. Soc. Japan
Vol. 21, No. 2, 1969

On the second cohomology groups of the fundamental groups of simple algebraic groups over perfect fields

By Takashi TASAKA

(Received June 17, 1968)

Introduction.

In this paper, we determine the first and second cohomology groups of the following tori: $\boldsymbol{G}_m$, $R_{K/k}(\boldsymbol{G}_m)$, and some tori associated with $R_{K/k}(\boldsymbol{G}_m)$ (U and V defined in § 2) and discuss relations between them. As an application, we also determine $H^2(k, Z)$, where Z is the center of a simply connected simple algebraic group F defined over a perfect field k. Since any simply connected simple algebraic group F defined over k is obtained by an inner twist from a certain quasi-split simple algebraic group F_1 defined over k, in order to determine $H^2(k, Z)$, it suffices to determine $H^2(k, Z_1)$, where Z_1 is the center of F_1.

In n°1, we state some lemmas which are well-known. In n°2, we determine the cohomology groups of some special tori, applying the lemmas to the case $M = k_s^*$, where k_s is the separable closure of k. In n°3 and n°4, we determine $H^2(k, Z)$ and define an H^2-invariant of a k-form of a simple algebraic group. N°5 has a nature of an appendix which will explain in a certain sense the meaning of the table obtained in n°3. Let K be a separable quadratic extension of an arbitrary field k. We prove that a central simple algebra B over K has an anti-automorphism over k if and only if $\beta+\bar{\beta}=0$, where β is the class of B in the Brauer group $B(K)$ of K. We also prove that B has an involution over k if and only if $c(\beta)=0$, where c is the corestriction of $B(K)$ into $B(k)$.

The author would like to express his hearty thanks to Dr. T. Kondo and Dr. H. Hijikata who have read his first manuscript critically and have given him useful suggestions.

§ 1. Preliminaries.

Let $\mathfrak{g}$ be an arbitrary group and $\mathfrak{h}$ be its subgroup of finite index n. Put $\mathfrak{g} = \bigcup_{i=1}^{n} g_i \mathfrak{h}$, with $g_1 = 1$. Putting

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

where $a_i = g_i \mathfrak{h}$ is the left coset of g_i modulo $\mathfrak{h}$, we can easily see that Λ is a left $\mathfrak{g}$-module of $\boldsymbol{Z}$-rank n. In this paper, we assume that all $\mathfrak{g}$-modules are left $\mathfrak{g}$-modules. For any $\mathfrak{g}$-modules A and B, $\mathrm{Hom}(A, B)$ is the group of $\boldsymbol{Z}$-homomorphism of A into B, and $A \otimes B$ is the tensor product of A and B taken over $\boldsymbol{Z}$. These can be considered as $\mathfrak{g}$-modules in natural way. For an arbitrary $\mathfrak{g}$-module A, we put $A^0 = \mathrm{Hom}(A, \boldsymbol{Z})$. A^0 is called the dual $\mathfrak{g}$-module of A.

LEMMA 1. *We have $\Lambda^0 \cong \Lambda$, as $\mathfrak{g}$-modules.*

PROOF. Any element x of $\mathfrak{g}$ induces a permutation on $(a_1, \cdots, a_n)$. It is clear that the permutation representation is self-dual.

LEMMA 2. *Let M be a $\mathfrak{g}$-module. Then we have*

$$\Lambda \otimes M \cong \mathrm{Hom}_{\boldsymbol{Z}[\mathfrak{h}]}(\boldsymbol{Z}[\mathfrak{g}], M) , \tag{1}$$

as $\mathfrak{g}$-modules, where $\mathrm{Hom}_{\boldsymbol{Z}[\mathfrak{h}]}(\boldsymbol{Z}[\mathfrak{g}], M)$ is considered as $\mathfrak{g}$-module in the following way: for $f \in \mathrm{Hom}_{\boldsymbol{Z}[\mathfrak{h}]}(\boldsymbol{Z}[\mathfrak{g}], M)$ and $s \in \mathfrak{g}$, we put $sf(x) = f(xs)$, for $x \in \boldsymbol{Z}[\mathfrak{g}]$.

PROOF. $\Lambda \otimes M = \{a_i \otimes g_i m_i : m_i \in M\}$. On the other hand, we have $\mathfrak{g} = \cup \mathfrak{h} g_i^{-1}$. For $f \in \mathrm{Hom}_{\boldsymbol{Z}[\mathfrak{h}]}(\boldsymbol{Z}[\mathfrak{g}], M)$, we put $f_i = f(g_i^{-1})$. Then f is completely determined by $(f_1, \cdots, f_n)$. We put $\alpha_i(m) = a_i \otimes g_i m$, and determine $\beta_i(m) \in \mathrm{Hom}_{\boldsymbol{Z}[\mathfrak{h}]}(\boldsymbol{Z}[\mathfrak{g}], M)$ by putting $\beta_i(m)(g_j^{-1}) = \delta_{ij} m$. The map $\alpha_i(m) \to \beta_i(m)$ is clearly a $\boldsymbol{Z}$-isomorphism. For $x \in \mathfrak{g}$, we write $x = g_j h g_i^{-1}$. If we fix i, then j is uniquely determined by x and i. So we have $x\alpha_i(m) = x(a_i \otimes g_i m) = a_j \otimes g_j hm = \alpha_j(hm)$, and we have $(x\beta_i(m))(g_j^{-1}) = \beta_i(m)(hg_i^{-1}) = hm$, and $(x\beta_i(m))(g_s^{-1}) = \beta_i(m)(hg_t^{-1}) = 0$, if $s \neq j$, that is, $x\beta_i(m) = \beta_j(hm)$. This proves that the above $\boldsymbol{Z}$-isomorphism is a $\mathfrak{g}$-isomorphism. (q. e. d.).

COROLLARY 1. *Let $\mathfrak{g}$ be a group and $\mathfrak{h}$ be its subgroup of finite index. For a $\mathfrak{g}$-module M, we have*

$$H^i(\mathfrak{g}, \Lambda \otimes M) \cong H^i(\mathfrak{h}, M) , \tag{2}$$

for $i \geqq 0$.

COROLLARY 2. *Let $\mathfrak{g}$ be a pro-finite group* (that is, a compact and totally disconnected group (Serre [7]. I.1.1.)), *and $\mathfrak{h}$ be its open subgroup. We suppose that M is a discrete $\mathfrak{g}$-module. If we consider the topological cohomology group* (that is, the cohomology group defined by continuous cocycles and continuous coboundaries), *we also have*

$$H^i(\mathfrak{g}, \Lambda \otimes M) \cong H^i(\mathfrak{h}, M) , \tag{3}$$

for $i \geqq 0$.

COROLLARY 3. *Let G be a finite group and H be its subgroup. We consider the Tate cohomology group of G* (Serre [**6**]. VIII.1), *then we have*

(4) $$H^i(G, \Lambda\otimes M)\cong H^i(H, M),$$

for any $i\in \boldsymbol{Z}$.

PROOF. In each case, we have

$$H^i(\mathfrak{g}, \mathrm{Hom}_{\boldsymbol{Z}[\mathfrak{h}]}(\boldsymbol{Z}[\mathfrak{g}], M))\cong H^i(\mathfrak{h}, M),$$

(Shapiro's Theorem). For example, in case Corollary 2, see Serre [7]. I.2.5.

Thus we have a canonical isomorphism of $H^i(\mathfrak{g}, \Lambda\otimes M)$ onto $H^i(\mathfrak{h}, M)$. Sometimes we identify $H^i(\mathfrak{g}, \Lambda\otimes M)$ with $H^i(\mathfrak{h}, M)$ by this canonical isomorphism.

Now we consider the following exact sequences.

(5) $$0\longrightarrow C\longrightarrow \Lambda\xrightarrow{c} \boldsymbol{Z}\longrightarrow 0,$$

(6) $$0\longrightarrow \boldsymbol{Z}u\xrightarrow{r} \Lambda\longrightarrow R\longrightarrow 0,$$

where $c(\sum p_i a_i)=\sum p_i$, and $u=\sum a_i$ and r is the injection. So we have $\boldsymbol{Z}u=\boldsymbol{Z}$ as $\mathfrak{g}$-modules. One can easily see that $C^0\cong R$ and $R^0\cong C$ as $\mathfrak{g}$-modules. As the sequences (5) and (6) are split over $\boldsymbol{Z}$, we have for any $\mathfrak{g}$-module M the following exact sequences.

(7) $$0\longrightarrow C\otimes M\longrightarrow \Lambda\otimes M\longrightarrow M\longrightarrow 0,$$

(8) $$0\longrightarrow M\longrightarrow \Lambda\otimes M\longrightarrow R\otimes M\longrightarrow 0.$$

Taking the cohomology of these exact sequences, we have, through the above mentioned identifications, the following exact sequences.

(9) $$0\longrightarrow H^0(\mathfrak{g}, C\otimes M)\longrightarrow H^0(\mathfrak{h}, M)\xrightarrow{c} H^0(\mathfrak{g}, M)\longrightarrow H^1(\mathfrak{g}, C\otimes M)\longrightarrow$$
$$\cdots\longrightarrow H^i(\mathfrak{g}, C\otimes M)\longrightarrow H^i(\mathfrak{h}, M)\xrightarrow{c} H^i(\mathfrak{g}, M)\longrightarrow H^{i+1}(\mathfrak{g}, C\otimes M)\longrightarrow,$$

(10) $$0\longrightarrow H^0(\mathfrak{g}, M)\xrightarrow{r} H^0(\mathfrak{h}, M)\longrightarrow H^0(\mathfrak{g}, R\otimes M)\longrightarrow H^1(\mathfrak{g}, M)\longrightarrow$$
$$\cdots\longrightarrow H^i(\mathfrak{g}, M)\xrightarrow{r} H^i(\mathfrak{h}, M)\longrightarrow H^i(\mathfrak{g}, R\otimes M)\longrightarrow H^{i+1}(\mathfrak{g}, M)\longrightarrow.$$

These are valid for a pro-finite group $\mathfrak{g}$ and its open subgroup $\mathfrak{h}$, with respect to the (topological) cohomology groups. If G is a finite group and we use the Tate cohomology groups, we have

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

(12) $$\longrightarrow H^i(G, M)\xrightarrow{r} H^i(H, M)\longrightarrow H^i(G, R\otimes M)\longrightarrow H^{i+1}(G, M)\longrightarrow,$$

for any $i\in \boldsymbol{Z}$.

LEMMA 3. *In each case, c is the corestriction and r is the restriction.*

PROOF. In case of pro-finite groups, see Serre [7]. I.2.5. The others also can be easily verified. (q. e. d.).

§ 2. Cohomology of some special tori.

Let k be a field and k_s be the separable closure of k. We denote by $\mathfrak{g}$ the Galois group of k_s over k. The group $\mathfrak{g}$ is a pro-finite group by the Krull topology. For an open subgroup $\mathfrak{h}$, there corresponds a subfield K of k_s which is a separable finite extension of k. If $\mathfrak{h}$ is normal in $\mathfrak{g}$, then K is a finite Galois extension of k, with the Galois group $G \cong \mathfrak{g}/\mathfrak{h}$.

We put $M=(\boldsymbol{G}_m)_{k_s}=k_s^*$, where $\boldsymbol{G}_m$ is the multiplicative group of the universal domain over k. Clearly M is a discrete $\mathfrak{g}$-module in natural way. Let T be a torus defined over k. We denote by $X(T)$ the character module of T. Then $X(T)$ is a discrete $\mathfrak{g}$-module. We see easily that $T_{k_s} \cong X(T)^0 \otimes M$. We put $H^i(k, T)=H^i(\mathfrak{g}, T_{k_s})$.

We put $S=R_{K/k}(\boldsymbol{G}_m)$ (for the definition and the properties of $R_{K/k}$, see Ono [3]. 1.4), then $X(S) \cong \Lambda=\boldsymbol{Z}[\mathfrak{g}/\mathfrak{h}]$, where K is a finite extension of k with the Galois group $\mathfrak{h}$ in k_s. By Lemma 2, we have

(13) $$H^1(k, S) \cong H^1(\mathfrak{h}, M)=0 . \quad \text{(Hilbert's theorem 90)}$$

(14) $$H^2(k, S) \cong H^2(\mathfrak{h}, M) \cong B(K) ,$$

where $B(K)$ is the Brauer group of K (see Serre [6]. X.4).

To the $\boldsymbol{Z}$-free $\mathfrak{g}$-modules C and R in (5) and (6), there correspond the tori U and V defined over k, respectively (cf. Ono [3] Prop. 1.2.3 and Prop. 1.2.4). So we have $U_{k_s}=C^0 \otimes M=R \otimes M$, and $V_{k_s}=R^0 \otimes M=C \otimes M$. Using the exact sequences (9) and (10), we have

$$0 \longrightarrow V_k \longrightarrow S_k \longrightarrow k^* \longrightarrow H^1(k, V) \longrightarrow 0 \longrightarrow 0 \longrightarrow H^2(k, V)$$
$$\longrightarrow B(K) \xrightarrow{c} B(k) ,$$
$$0 \longrightarrow k^* \longrightarrow S_k \longrightarrow U_k \longrightarrow 0 \longrightarrow 0 \longrightarrow H^1(k, U) \longrightarrow B(k)$$
$$\xrightarrow{r} B(K) \longrightarrow H^2(k, U) .$$

That is, $H^1(k, V)=k^*/NK^*$, $U_k=K^*/k^*$, and

(15) $$0 \longrightarrow H^2(k, V) \longrightarrow B(K) \xrightarrow{c} B(k) ,$$

(16) $$0 \longrightarrow H^1(k, U) \longrightarrow B(k) \xrightarrow{r} B(K) \longrightarrow H^2(k, U) .$$

If $\mathfrak{n}$ is an open and normal subgroup of $\mathfrak{g}$ contained in $\mathfrak{h}$, we put $G=\mathfrak{g}/\mathfrak{n}$

and $H=\mathfrak{h}/\mathfrak{n}$. Then the sequences (5) and (6) can be considered as

$$0 \longrightarrow C \longrightarrow \boldsymbol{Z}[G/H] \longrightarrow \boldsymbol{Z} \longrightarrow 0\,, \tag{17}$$

$$0 \longrightarrow \boldsymbol{Z} \longrightarrow \boldsymbol{Z}[G/H] \longrightarrow R \longrightarrow 0\,, \tag{18}$$

because $\mathfrak{n}$ operates trivially on each $\mathfrak{g}$-modules above.

In the following, we shall consider the case where $\mathfrak{h}$ is normal in $\mathfrak{g}$, and we put $\mathfrak{n}=\mathfrak{h}$ and $G=\mathfrak{g}/\mathfrak{h}$. Then the sequences (17) and (18) are the usual ones in the cohomology of finite groups. For any G-module M_1, we have

$$H^i(G, M_1) \cong H^{i+1}(G, C \otimes M_1) \cong H^{i-1}(G, R \otimes M_1)\,. \tag{19}$$

If we put $M_1 = Y \otimes M^{\mathfrak{h}} = Y \otimes K^*$, where Y is a $\boldsymbol{Z}$-free G-module considered as a discrete $\mathfrak{g}$-module, using the fact the $H^1(\mathfrak{h}, Y \otimes M)=0$, we have

$$0 \longrightarrow H^1(G, Y \otimes K^*) \xrightarrow{\text{inf}} H^1(\mathfrak{g}, Y \otimes M) \longrightarrow 0\,, \tag{20}$$

$$\begin{aligned} 0 \longrightarrow H^2(G, Y \otimes K^*) &\xrightarrow{\text{inf}} H^2(\mathfrak{g}, Y \otimes M) \\ &\longrightarrow H^2(\mathfrak{h}, Y \otimes M)^G \xrightarrow{\tau} H^3(G, Y \otimes K^*)\,, \end{aligned} \tag{21}$$

where inf is the inflation and τ is the transgression (Serre [**6**]. VII. 6). If we put $Y=\Lambda$ $(\cong \boldsymbol{Z}[G])$, we have

$$0 \longrightarrow H^2(\mathfrak{g}, \Lambda \otimes M) \longrightarrow H^2(\mathfrak{h}, \Lambda \otimes M)^G \longrightarrow 0\,. \tag{22}$$

By easy computation, we can show that $H^2(\mathfrak{h}, \Lambda \otimes M)^G \cong H^2(\mathfrak{h}, M)$. That is, $H^2(k, S) \cong B(K)$. Thus we have an explicit form of the isomorphism of $H^2(k, S)$ onto $B(K)$ in (14) when K is a finite Galois extension of k, which we will utilise in the following sections.

To determine $H^2(k, V)=H^2(\mathfrak{g}, C \otimes M)$ when $\mathfrak{h}$ is normal in $\mathfrak{g}$, we consider the following exact sequence, substituting M by $C \otimes M$ in (10),

$$H^1(\mathfrak{g}, R \otimes C \otimes M) \longrightarrow H^2(\mathfrak{g}, C \otimes M) \xrightarrow{r} H^2(\mathfrak{h}, C \otimes M) \longrightarrow H^2(\mathfrak{g}, R \otimes C \otimes M)\,.$$

By (19) and (20), we have

$$H^1(\mathfrak{g}, R \otimes C \otimes M) \cong H^1(G, R \otimes C \otimes K^*) \cong H^2(G, C \otimes K^*) \cong H^1(G, K^*) = 0\,.$$

So we have

$$0 \longrightarrow H^2(\mathfrak{g}, C \otimes M) \xrightarrow{r} H^2(\mathfrak{h}, C \otimes M) \longrightarrow H^2(\mathfrak{g}, R \otimes C \otimes M)\,. \tag{23}$$

Now we consider the simpler case where $G=\mathfrak{g}/\mathfrak{h} \cong \boldsymbol{Z}_2$, the group of order 2. Then $C \cong R$ and $C \otimes R \cong \boldsymbol{Z}$ as $\mathfrak{g}$-modules, and $C \cong R \cong \boldsymbol{Z}$ as $\mathfrak{h}$-modules. So we have

(24) $$0 \longrightarrow H^2(\mathfrak{g}, C\otimes M) \xrightarrow{r} H^2(\mathfrak{h}, M) \longrightarrow H^2(\mathfrak{g}, M).$$

That is,

(25) $$0 \longrightarrow H^2(\mathfrak{g}, C\otimes M) \longrightarrow B(K) \xrightarrow{\xi} B(k).$$

Using the isomorphism (22), we can show that $\xi = -c$, where c is the corestriction. Thus we have proved

PROPOSITION 1. *Let K be a separable quadratic extension of k. The kernel of the corestriction c of $B(K)$ into $B(k)$ is the subgroup of $B(K)$ of the classes of cocycles of $\mathfrak{h}$ into M which can be extended to the cocycles of $\mathfrak{g}$ into $C\otimes M$.*

We also suppose that $\mathfrak{g}/\mathfrak{h} = \boldsymbol{Z}_2$. In (21), we put $Y = C$. So we have

$$0 \longrightarrow H^2(\mathfrak{g}, C\otimes M) \longrightarrow H^2(\mathfrak{h}, C\otimes M)^G \longrightarrow H^3(G, C\otimes K^*),$$

because $H^2(G, C\otimes K^*) = H^1(G, K^*) = 0$. Moreover we have $H^3(G, C\otimes K^*) \cong H^2(G, K^*) \cong k^*/NK^*$, and $H^2(\mathfrak{h}, C\otimes M)^G \cong \{\beta \in B(K) : \beta + \bar{\beta} = 0\}$, where bar means the action of the non-trivial automorphism of K over k on $B(K)$.

In n°5, we will prove the following two propositions.

PROPOSITION 2. *Let B be a central simple algebra over K, and β be its class in $B(K)$. The algebra B has an anti-automorphism over k, if and only if $\beta + \bar{\beta} = 0$.*

PROPOSITION 3. *Let B be a central simple algebra over K, and β be its class in $B(K)$. The algebra B has an involution over k, if and only if $c(\beta) = 0$.*

REMARK. We mean by an anti-automorphism over k an anti-automorphism whose restriction on the center K is the non-trivial automorphism of K over k. An involution is an anti-automorphism of order 2.

In this place, we notice that the conditions (22. a, b and c) or (55; a, b and c) in Satake [**5**] are equivalent to $c(\lambda) = 0$ or $c(\mu) = 0$ (cf. n°5).

From the proposition 3 and (15), it follows

THEOREM. *To each element of $H^2(k, V)$, where V is the unique one dimensional torus defined over k which is not k-trivial and splits over separable quadratic extension K of k, there corresponds an algebra class of central simple algebra over K which has an involution over k.*

PROOF. The torus V is the torus whose character module is isomorphic to C or, what is the same, to R (cf. Ono [**3**]. Prop. 1.2.3 and Prop. 1.2.4).

§ 3. Applications to the Galois cohomology of simple algebraic groups.

From now on, we assume that the base field k is a perfect field having more than three elements. Let F be a simple algebraic group quasi-split over K/k ([**8**]. 1) (in this paper, we mean by a simple algebraic group a simple algebraic group over the algebraic closure $\bar{k}$ of k). Moreover we assume that F is of adjoint type. F is uniquely determined by K/k and its type over the algebraic closure. We denote by ${}^dX_n$ the type of F or that of the algebraic groups associated with F by (32) in n°4, where $d=[K;k]$ and X_n is the type of F over the algebraic closure of k. Suppose that A is a maximal k-trivial torus of F. Then $T=Z(A)$ is a maximal torus of F defined over k, where $Z(A)$ means the centraliser of A in F (ibid.). Let $\tilde{F}$ be the universal covering of F defined over k with the covering isogeny π, $\tilde{A}$ and $\tilde{T}$ be the corresponding tori of $\tilde{F}$ to A and T by π, respectively (for the definition and the existence of the universal covering, see Tits [**9**]. 2.6.1. Prop. 2). We have shown in our previous paper [8]. 3.(26), that $T\cong\tilde{T}\cong a[R_{K/k}(\boldsymbol{G}_m)]\times b[\boldsymbol{G}_m]$, except the type ${}^6D_4$, and that $T\cong\tilde{T}\cong R_{L/k}(\boldsymbol{G}_m)\times\boldsymbol{G}_m$ for the type ${}^6D_4$, where L is a subfield of K of degree 3 over k. Note that $b[\boldsymbol{G}_m]$ means the direct product of b-copies of $\boldsymbol{G}_m$, for example. Let Z be the kernel of π in $\tilde{T}$. Then Z is the center of $\tilde{F}$, and we have

$$0\longrightarrow Z\longrightarrow\tilde{T}\xrightarrow{\pi}T\longrightarrow 0\,.$$

So we have the exact sequence

$$0\longrightarrow Z_k\longrightarrow\tilde{T}_k\xrightarrow{\pi}T_k\longrightarrow H^1(k,Z)\longrightarrow H^1(k,\tilde{T})$$
$$\longrightarrow H^1(k,T)\longrightarrow H^2(k,Z)\longrightarrow H^2(k,\tilde{T})\xrightarrow{\pi^*}H^2(k,T)\,.$$

As $H^1(k,T)\cong H^1(k,\tilde{T})=0$ (see (13)), we have

$$H^1(k,Z)\cong T_k/\pi(\tilde{T}_k)\,, \tag{26}$$

$$H^2(k,Z)=\operatorname{Ker}\pi^*\,, \tag{27}$$

where $\pi^*: H^2(k,\tilde{T})\to H^2(k,T)$. On the other hand, we have

$$0\longrightarrow Z\longrightarrow\tilde{F}\longrightarrow F\longrightarrow 0\,.$$

So we have the following exact sequence of pointed sets.

$$0\longrightarrow Z_k\longrightarrow\tilde{F}_k\longrightarrow F_k\longrightarrow H^1(k,Z)\longrightarrow H^1(k,\tilde{F})\longrightarrow H^1(k,F)\xrightarrow{\delta}H^2(k,Z)\,.$$

In [8]. 2. Th. 1, we have the natural isomorphism of $F_k/\pi(\tilde{F}_k)$ onto $T_k/\pi(\tilde{T}_k)$. Thus we have

$$F_k/\pi(\tilde{F}_k)\cong T_k/\pi(\tilde{T}_k)\cong H^1(k,Z)\,.$$

It follows from these

$$0\longrightarrow H^1(k,\tilde{F})\longrightarrow H^1(k,F)\xrightarrow{\delta}H^2(k,Z)\,. \tag{28}$$

We shall determine $H^2(k,Z)$ in each case.

Suppose that F is split over k, that is, $T=A$. Let $(e_1, \cdots, e_n)$ be the elemental divisors of $X(T)$ in $X(\tilde{T})$. Then $Z=\prod_{i=1}^{n}\mu_{e_i}$, where μ_e is the group of e-th roots of unity in G_m. Using the following sequence,

$$0 \longrightarrow \mu_e \longrightarrow G_m \xrightarrow{e} G_m \longrightarrow 0,$$

where $e(x)=x^e$, we have $H^1(k, \mu_e)=k^*/(k^*)^e$, and

$$H^2(k, \mu_e)=\{\alpha \in B(k): e\alpha=0\}, \tag{29}$$

where $B(k)$ is the Brauer group of k.

If F is quasi-split over K/k, $\operatorname{Ker}\pi^*$ is the subgroup of $H^2(k, \tilde{T})$ containing $(\varepsilon_1, \cdots, \varepsilon_n)$ such that

$$(c(i, j))\cdot {}^t(\varepsilon_1, \cdots, \varepsilon_n)=0,$$

where $c(i, j)=2(a_i, a_j)/(a_j, a_j)$ is the Cartan integer and $\{a_i\}$ is the fundamental root system of F. Using the isomorphism (22), we can calculate explicitly $H^2(k, Z)=\operatorname{Ker}\pi^*$ in each case.

${}^2A_{2m}$: $H^2(k, Z)\cong\{\beta\in B(K): m\bar{\beta}=(m+1)\beta\}$.

${}^2A_{2m+1}$: 〃 $\cong\{(\alpha, \beta)\in B(k)\times B(K): r(\alpha)=(m+1)\beta,\ 2\alpha=mc(\beta)\}$.

${}^2D_n$: 〃 $\cong\{(\alpha, \beta)\in B(k)\times B(K): (n-2)r(\alpha)=2\beta,\ (n-1)\alpha=c(\beta)\}$.

${}^2E_6$: 〃 $\cong\{(\alpha, \beta)\in B(k)\times B(K): 2r(\alpha)=3\beta,\ 3\alpha=2c(\beta)\}$.

${}^3D_4$: 〃 $\cong\{(\alpha, \beta)\in B(k)\times B(K): r(\alpha)=2\beta,\ 2\alpha=c(\beta)\}$.

${}^6D_4$: 〃 $\cong\{(\alpha, \beta)\in B(k)\times B(L): r(\alpha)=2\beta,\ 2\alpha=c(\beta)\}$.

Explanation: (i) r is the restriction and c is the corestriction.

(ii) Bar (in $\bar{\beta}$) means the action of the non-trivial automorphism of K over k on $B(K)$, where K is a quadratic extension of k.

(iii) In ${}^6D_4$, L is a subfield of K of degree 3 over k.

Using the following facts, we can simplify the above table. When K is a quadratic extension of k, $c(r(\alpha))=2\alpha$; $r(c(\beta))=\beta+\bar{\beta}$; $c(\beta)=0$ implies $\beta+\bar{\beta}=0$; $\beta+\bar{\beta}=0$ implies $c(\beta)\in H^2(K/k)$ (the kernel of the restriction r in $B(k)$); and $\beta=\bar{\beta}$ implies $\beta\in r(B(k))$. The last statement can be obtained by putting $Y=\boldsymbol{Z}$ in (21). The similar formulae also hold for the case where K is not a quadratic extension of k. Thus we have the following table.

${}^1A_n$: $\{\alpha\in B(k): (n+1)\alpha=0\}$, $\alpha\sim-\alpha$.

${}^2A_{2m}$: $\{\beta\in B(K): (2m+1)\beta=0,\ c(\beta)=0\}$, $\beta\sim\bar{\beta}$.

${}^2A_{2m+1}$: $\{(\alpha, \beta)\in B(k)\times B(K): 2\alpha=0,\ r(\alpha)=(m+1)\beta,\ c(\beta)=0\}$, $(\alpha, \beta)\sim(\alpha, \bar{\beta})$.

B_n and C_n: $\{\alpha\in B(k): 2\alpha=0\}$.

${}^1D_{2m+1}$: $\{\alpha \in B(k): 4\alpha=0\}$, $\alpha \sim -\alpha$.

${}^2D_{2m+1}$: $\{(\alpha, \beta) \in B(k)\times B(K): 2\alpha=0,\ r(\alpha)=2\beta,\ c(\beta)=0\}$, $(\alpha, \beta) \sim (\alpha, \bar{\beta})$.

${}^1D_{2m}(m>2)$: $\{(\alpha_1, \alpha_2) \in B(k)\times B(k): 2\alpha_1=2\alpha_2=0\}$, $(\alpha_1, \alpha_2) \sim (\alpha_2, \alpha_1)$.

${}^2D_{2m}(m>2)$: $\{\beta \in B(K): 2\beta=0\}$, $\beta \sim \bar{\beta}$.

${}^1E_6$: $\{\alpha \in B(k): 3\alpha=0\}$, $\alpha \sim -\alpha$.

${}^2E_6$: $\{\beta \in B(K): 3\beta=0,\ c(\beta)=0\}$, $\beta \sim \bar{\beta}$.

E_7: $\{\alpha \in B(k): 2\alpha=0\}$.

E_8, F_4 and G_2: trivial.

${}^1D_4$: $\{(\alpha_1, \alpha_2) \in B(k)\times B(k): 2\alpha_1=2\alpha_2=0\}$, $(\alpha_1, \alpha_2) \sim (\alpha_1+\alpha_2, \alpha_2)$

$\sim (\alpha_2, \alpha_1+\alpha_2) \sim (\alpha_2, \alpha_1) \sim (\alpha_1, \alpha_1+\alpha_2) \sim (\alpha_1+\alpha_2, \alpha_1)$.

${}^2D_4$: $\{\beta \in B(K): 2\beta=0\}$, $\beta \sim \bar{\beta}$.

${}^3D_4$: $\{\beta \in B(K): 2\beta=0,\ c(\beta)=0\}$, $\beta \sim \bar{\beta} \sim \bar{\bar{\beta}}$.

${}^6D_4$: $\{\beta \in B(L): 2\beta=0,\ c(\beta)=0\}$.

For the meaning of equivalence relations $\sim$, see the next section.

If K is a quadratic extension of k, then the characterisation of $c(\beta)=0$ is done in the proposition 3. But if K is not a quadratic extension, the meaning of $c(\beta)=0$ is not known yet. Note that, if K is a quadratic extension of k, $2t\beta=0$ and $c(\beta)=0$ imply that $t\beta$ is contained in $\operatorname{Im} r \cap \operatorname{Ker} c$. Moreover we can easily see that $\operatorname{Im} r \cap \operatorname{Ker} c = \{r(\alpha): \alpha \in B(k), 2\alpha=0\}$.

§ 4. H^2-invariant of k-forms.

In this section, we utilise the terminology and several results in Serre's [7]. I.5 and III.1.

Let F be a simple algebraic group defined over k, and F_0 be the split adjoint form of F over k. We call F a k-form of F_0. By the theory of Galois cohomology of the algebraic groups, we have a one-to-one correspondence between k-forms of F_0 and the cohomology set $H^1(k, A(F_0))$, where $A(F_0)$ is the automorphism group of F_0. The structure of $A(F_0)$ is well-known, that is, $A(F_0)=F_0 \times U_0$, a semi-direct product, where F_0 is normal in $A(F_0)$, and $S_0=A(F_0)/F_0$ ($\cong U_0$) is the automorphism group of Dynkin diagram of F_0 on which $\mathfrak{g}$ operates trivially. Moreover we have

$$H^1(k, A(F_0)) \underset{\psi}{\overset{\varphi}{\rightleftarrows}} H^1(k, S_0) \longrightarrow 0, \tag{30}$$

where ψ is the canonical cross-section, that is, for $b \in H^1(k, S_0)$, there corresponds a certain Galois extension K of k, and to $\psi(b)$ corresponds a quasi-split group F_1 over K/k which we assume to be of adjoint type.

Let $\tilde{F}_0$ be the universal covering of F_0 over k and Z_0 be the center of $\tilde{F}_0$. We suppose that F corresponds to $f \in H^1(k, A(F_0))$. We put $\varphi(f) = b$, then we have

$$ {}_fZ_0 \cong {}_bZ_0 \,, \tag{31} $$

as $\mathfrak{g}$-modules, where ${}_fZ_0$ and ${}_bZ_0$ are the torsions of Z_0 by f and b, respectively. We put $S_1 = {}_bS_0$ and $Z_1 = {}_bZ_0$. We know that

$$ \varphi^{-1}(b) = H^1(k, F_1)/\sim \,, \tag{32} $$

where $\sim$ means the action of $H^0(k, S_1)$. For an element d of $H^0(k, S_1)$, we have the following commutative diagram.

$$ \begin{array}{ccc} H^1(k, F_1) & \xrightarrow{\delta} & H^2(k, Z_1) \\ d \downarrow & & d \downarrow \\ H^1(k, F_1) & \xrightarrow{\delta} & H^2(k, Z_1) \,, \end{array} \tag{33} $$

where the action of d in $H^2(k, Z_1)$ is induced by the automorphism of Z_1 induced by d (Kneser [2]. 4). So we have

$$ H^1(k, F_1)/\sim \xrightarrow{\Delta} H^2(k, Z_1)/\sim \,. \tag{34} $$

For an element g of $H^1(k, F_1)/\sim$, we may call $\Delta(g)$ is the H^2-invariant of F, where F corresponds to g.

We shall determine the group S_1, or $H^0(k, S_1)$, in each case.

(i) Except the type D_4, $S_1 \cong S_0$ as $\mathfrak{g}$-groups.

(ii) For the type D_4. If $\operatorname{Im} b = 1$, $H^0(k, S_1) = S_0$. If $\operatorname{Im} b = \boldsymbol{Z}_2$, $H^0(k, S_1) = \operatorname{Im} b$. If $\operatorname{Im} b = \boldsymbol{Z}_3$, $H^0(k, S_1) = \operatorname{Im} b$. If $\operatorname{Im} b = \mathfrak{S}_3$, $H^0(k, S_1) = 1$.

The action of $H^0(k, S_1)$ on Z_1 or on $H^2(k, Z_1)$ can easily be determined which we have given in the table of the last section.

§5. Involutorial algebras of the second kind.

Let k be an arbitrary field and K be its separable quadratic extension. A central simple algebra B over K is said to have an anti-automorphism over k, if there exists an anti-automorphism of B whose restriction on the center K is the non-trivial automorphism of K over k.

LEMMA 4. *Let $B = M_n(D)$, where D is a central division algebra over K. The algebra B has an anti-automorphism over k if and only if D has.*

PROOF. See, for example, Albert [**1**]. X. Th. 12.

PROOF OF THE PROPOSITION 2 (see n°2). By lemma 4, we can suppose that B is a crossed product (N, p), where N is a finite Galois extension of K and p is a 2-cocycle of $G(N/K)$ into N^*. Moreover we can suppose that N is a Galois extension of k. We put $G=G(N/k)$ and $H=G(N/K)$. We fix an element σ of $G-H$. We denote by β the class of p in $H^2(H, N^*)$. Then $\bar{\beta}$ corresponds to the class of $\bar{p}$, where $\bar{p}$ is the 2-cocycle defined by $\bar{p}(S, T) =\sigma(p(S^\sigma, T^\sigma))$. Note that we use the notation $S^\sigma=\sigma^{-1}S\sigma$ and ${}^\sigma S=\sigma S\sigma^{-1}$. The crossed product (N, p) is constructed in the following way. $B=\sum_{S\in H} Nu_S$, $u_S z =S(z)u_S$ $(z\in N)$ and $u_S u_T=p(S, T)u_{ST}$. Note that we suppose that H operates on N^* from the left.

Assume $\beta+\bar{\beta}=0$. That is, $p(S, T)\cdot\bar{p}(S, T)=m(ST)/m(S)\cdot Sm(T)$, where m is a 1-cochain of H into N^*. Changing $\{u_S\}$, we can suppose that $p(1, 1)=1$. Necessarily $m(1)=1$ and u_1 is the unit element of B. We put

$$\rho(\sum z_S u_S)=\sum(m({}^\sigma S)u\sigma_S)^{-1}\cdot\sigma(z_S)\,.$$

We can show that ρ is an anti-automorphism of B over k (cf. [**1**]. X. the proof of Th. 16).

Conversely assume that $B=(N, p)$ has an anti-automorphism ρ over k. We put $N_1=\rho(N)$. Of course, there exists an isomorphism of N onto N_1 over K. By [**1**]. IV. Th. 14, there exists an invertible element X in B such that $XN_1X^{-1}=N$. Put $\rho_1(u)=X\rho(u)X^{-1}$. Then $\rho_1(N)=N$ and ρ_1 is also an anti-automorphism of B over k. So we can suppose from the first that $\rho(N)=N$. The restriction of ρ on N is an element σ of $G-H$. Now one has $\rho(u_S x) =\sigma(x)\rho(u_S)=\rho(S(x)u_S)=\rho(u_S)\cdot\sigma S(x)$. So one has $u_{\sigma S}\rho(u_S)\cdot\sigma S(x)=u_{\sigma S}\cdot\sigma(x)\cdot\rho(u_S) ={}^\sigma S(\sigma(x))u_{\sigma S}\rho(u_S)=\sigma S(x)\cdot u_{\sigma S}\rho(u_S)$, for all $\sigma S(x)$ in N. As N is a maximal subfield of B, $u_{\sigma S}\rho(u_S)$ is contained in N^*. We put $u_{\sigma S}\rho(u_S)=m({}^\sigma S)^{-1}$, that is, $\rho(u_S)^{-1}=m({}^\sigma S)u_{\sigma S}$. From $u_S u_T=p(S, T)u_{ST}$, one has $\rho(u_T)\rho(u_S)=\rho(u_{ST})\cdot \sigma(p(S, T))$. From this, it follows that $\rho(u_S)^{-1}\cdot\rho(u_T)^{-1}=\sigma(p(S, T))^{-1}\cdot\rho(u_{ST})^{-1} =\sigma(p(S, T))^{-1}m({}^\sigma(ST))\cdot u_{\sigma_{(ST)}}$, and $\rho(u_S)^{-1}\cdot\rho(u_T)^{-1}=m({}^\sigma S)u_{\sigma S}\cdot m({}^\sigma T)u_{\sigma T}=m({}^\sigma S) \cdot{}^\sigma Sm({}^\sigma T)\cdot p({}^\sigma S, {}^\sigma T)\cdot u_{\sigma_{(ST)}}$. Thus we have $p(S, T)\cdot\sigma(p(S^\sigma, T^\sigma))=m(ST)/m(S) \cdot Sm(T)$. This proves that $\beta+\bar{\beta}=0$.

PROOF OF THE PROPOSITION 3. It is known that $B=M_n(D)$ has an involution over k, if and only if D does ([**1**]. X. Th. 12), where D is a central division algebra over K. So it is sufficient to prove the proposition in the case where B is a crossed product (N, p). Moreover we may suppose that N is a finite Galois extension of k. We put $G=G(N/k)$ and $H=G(N/K)$. Let p be a 2-cocycle of H into N^*. We put

$$\begin{cases} p_1(S, T) = p(S, T) \\ p_1(\sigma S, T) = p(\sigma S\sigma, \sigma^{-1}T\sigma) \\ p_1(S, \sigma T) = p(S, \sigma T\sigma) \\ p_1(\sigma S, \sigma T) = p(\sigma S\sigma, T) \end{cases} \qquad \begin{cases} p_2(S, T) = \sigma p(\sigma^{-1}S\sigma, \sigma^{-1}T\sigma) \\ p_2(\sigma S, T) = \sigma p(S, T) \\ p_2(S, \sigma T) = \sigma p(\sigma^{-1}S\sigma, T) \\ p_2(\sigma S, \sigma T) = \sigma p(S, \sigma T\sigma), \end{cases}$$

where S and T run in H. Then $a_1 \otimes p_1(S, T) + a_2 \otimes p_2(S, T)$ is a 2-cocycle of G into $\boldsymbol{Z}[G/H] \otimes N^*$. To the 2-cocycle $p_1(S, T) \cdot p_2(S, T)$ of G into N^* corresponds $c(\beta)$ in $B(k)$, where β is the class of $p(S, T)$ in $B(K)$. We assume that $c(\beta) = 0$, that is, $p_1(S, T) \cdot p_2(S, T) = m(ST)/m(S) \cdot Sm(T)$ for all S and T in G. From the definition of p_i, it follows that

$$p(S, T) \cdot \sigma p(\sigma^{-1}S\sigma, \sigma^{-1}T\sigma) = m(ST)/m(S) \cdot Sm(T), \tag{35}$$

$$p(\sigma S\sigma, \sigma^{-1}T\sigma) \cdot \sigma p(S, T) = m(\sigma ST)/m(\sigma S) \cdot \sigma Sm(T), \tag{36}$$

$$p(S, \sigma T\sigma) \cdot \sigma p(\sigma^{-1}S\sigma, T) = m(S\sigma T)/m(S) \cdot Sm(\sigma T), \tag{37}$$

$$p(\sigma S\sigma, T) \cdot \sigma p(S, \sigma T\sigma) = m(\sigma S\sigma T)/m(\sigma S) \cdot \sigma Sm(\sigma T). \tag{38}$$

From (38), we can deduce the following formulae.

$$m(\sigma) \cdot \sigma m(\sigma) = m(A), \tag{39}$$

$$m(\sigma^{-1}) \cdot \sigma^{-1}m(\sigma^{-1}) = m(A^{-1}), \tag{40}$$

where $A = \sigma^2$. Now we take an anti-automorphism ρ over k as in the proof of Proposition 2. Then ρ^2 is an automorphism of B over K. As the restriction of ρ^2 to N is $A = \sigma^2$, we have $\rho^2(u) = \lambda u_A u(\lambda u_A)^{-1}$, with some $\lambda \in N^*$. On the other hand, by direct calculation, we have $\rho^2(u_S) = [m({}^AS)/\sigma m({}^\sigma S)] \cdot u_{ASA^{-1}}$.

From (36) and (37), we have

$$p(A, S) = p(A, S) \cdot \sigma p(1, \sigma S\sigma^{-1}) = m(AS\sigma^{-1})/m(\sigma) \cdot \sigma m(\sigma S\sigma^{-1}),$$

$$p(ASA^{-1}, A) = p(ASA^{-1}, A) \cdot \sigma p(\sigma S\sigma^{-1}, 1) = m(AS\sigma^{-1})/m({}^AS) \cdot {}^ASm(\sigma).$$

If we put $\lambda = m(\sigma)$, then we have

$$m(\sigma)u_A z u_S = A(z)m(\sigma)p(A, S)u_{AS} = A(z)[m(AS\sigma^{-1})/\sigma m(\sigma S\sigma^{-1})]u_{AS},$$

$$\begin{aligned} \rho^2(zu_S)m(\sigma)u_A &= A(z)[m({}^AS)/\sigma m({}^\sigma S)] \cdot {}^ASm(\sigma) \cdot p(ASA^{-1}, A)u_{AS} \\ &= A(z)[m(AS\sigma^{-1})/m(\sigma S\sigma^{-1})]u_{AS}. \end{aligned}$$

Thus we have proved that $\rho^2(u) = m(\sigma)u_A u(m(\sigma)u_A)^{-1}$. By direct calculation, one can see that B has an involution over k if and only if there exists an invertible element X in B such that $X\rho(X)^{-1}m(\sigma)u_A = b$, where b is a certain element in K^*. That is, if we can solve the equation

$$m(\sigma)u_A X = b\cdot\rho(X)\,, \tag{42}$$

with an invertible element X in B, we can construct an involution of B over k.

If $\sigma^2=1$ $(A=1)$, from (39), it follows $m(\sigma)\cdot\sigma m(\sigma)=1$. There exists an element w in N^* such that $m(\sigma)=\sigma(w)/w$. Thus we have $m(\sigma)u_1 w=\sigma(w)$. So the equation (42) is solved with $b=1$ and $X=w$.

If $\sigma^2=A\neq 1$, we put $X=\sigma(y)/m(\sigma^{-1})+yu_{A^{-1}}$, where y is a certain element in N^*. From (40) and (41), it follows that

$$\begin{aligned} m(\sigma)u_A\cdot(\sigma(y)/m(\sigma^{-1})+yu_{A^{-1}}) &= m(\sigma)A(y)p(A,\,A^{-1})+[m(\sigma)A\sigma(y)/Am(\sigma^{-1})]u_A \\ &= A(y)/\sigma m(\sigma^{-1})+[A\sigma(y)m(\sigma)/Am(\sigma^{-1})]u_A\,, \\ \rho[\sigma(y)/m(\sigma^{-1})+yu_{A^{-1}}] &= A(y)/\sigma m(\sigma^{-1})+(m(A^{-1})u_{A^{-1}})^{-1}\cdot\sigma(y) \\ &= A(y)/\sigma m(\sigma^{-1})+[A\sigma(y)/Am(A^{-1})p(A,\,A^{-1})]u_A \\ &= A(y)/\sigma m(\sigma^{-1})+[A\sigma(y)m(\sigma)/Am(\sigma^{-1})]u_A\,. \end{aligned}$$

Thus the equation (42) is solved with $b=1$ and $X=\sigma(y)/m(\sigma^{-1})+yu_{A^{-1}}$. Note that $(u_{A^{-1}})^{-1}=[1/p(A,\,A^{-1})]u_A$. Let n be the order of A in G. $(u_{A^{-1}})^n=t$ is an element of N^*. If we put $Y=-[ym(\sigma^{-1})/\sigma(y)]u_{A^{-1}}$, then $Y^n=(-1)^n[\nu(m(\sigma^{-1}))\cdot\nu(y)/\sigma\nu(y)]t=c$ is an element of N^*, where $\nu(w)=\prod_{i=0}^{n-1}A^{-i}(w)$. Changing y appropriately, we can suppose that $c\neq 1$. Then X is invertible. More precisely,

$$X^{-1}=[1/(1-c)]\cdot\sum_{i=0}^{n-1}Y^i\cdot[m(\sigma^{-1})/\sigma(y)]\,.$$

Thus, if $c(\beta)=0$, B has an involution over k.

Conversely we assume that $B=(N,\,p)$ has an involution J over k. Put $N_1=J(N)$. As there exists an isomorphism over K of N onto N_1, there exists an inner automorphism x of B such that $x(N)=N_1$, where $x(u)=XuX^{-1}$. We put $\rho(u)=X^{-1}J(u)X$, that is, $J(u)=X\rho(u)X^{-1}$. Then clearly $\rho(N)=N$. Denoting by σ the restriction of ρ on N, we have $\rho(\sum z_S u_S)=\sum(m({}^{\sigma}S)u_{\sigma S})^{-1}\cdot\sigma(z_S)$, and

$$p(S,\,T)\cdot\sigma p(\sigma^{-1}S\sigma,\,\sigma^{-1}T\sigma)=m(ST)/m(S)\cdot Sm(T)\,, \tag{43}$$

for all S and T in H (cf. the proof of Prop. 2). On the other hand, putting $\sigma^2=A$, there exists λ in N^* such that

$$\rho^2(u)=\lambda u_A u(\lambda u_A)^{-1}\,. \tag{44}$$

We write $X=\sum x_S u_S$. As X is invertible, there exists an S such that $x_S\neq 0$. If we put $\rho_1(u)=x_S u_S X^{-1}J(u)X(x_S u_S)^{-1}$, then ρ_1 is an anti-automorphism of B over k such that $\rho_1(N)=N$. Thus we can assume from the first that $x_1=1$. As J is an involution of B over k, X is a solution of (42), that is,

(45) $$\lambda u_A X = b \cdot \rho(X),$$

where $b \in K^*$. We put $m(\sigma) = \lambda/b$. As b is contained in the center of B, the equation (44) holds also with $m(\sigma)u_A$.

Suppose that $\sigma^2 = 1$ $(A = 1)$. Comparing the coefficients of u_1 in (45), we have $\lambda = b$, that is, $m(\sigma) = 1$. As $X_0 = 1$ is also a solution of (45), ρ_0 is an involution of B over k. So we have $m({}^AS) = \sigma m({}^\sigma S)$. Thus we have $m(\sigma S\sigma^{-1}) = \sigma m(S)$. For each T in H, we put $m(\sigma T) = \sigma m(T)$. Then one can easily verify that the formulae (35), $\cdots$, (38) hold. That is, $c(\beta) = 0$, where β is the class of p in $B(K)$.

Now suppose that $\sigma^2 = A \neq 1$. Comparing the coefficients of u_1 and u_A in (45), we have $\lambda = b \cdot A\sigma(y)/p(A, A^{-1}) \cdot Am(A^{-1})$ and $\lambda \cdot A(y) \cdot p(A, A^{-1}) = b$, where $y = x_{A^{-1}}$. Note that $x_1 = 1$ from the assumption. From these, it follows that

(46) $$m(\sigma) \cdot \sigma m(\sigma) \cdot p(A, A^{-1}) \cdot \sigma p(A, A^{-1}) \cdot Am(A^{-1}) = 1,$$

where we have put $\lambda/b = m(\sigma)$. In (44), we put $u = u_S$, then we have

(47) $$m(\sigma)p(A, S) = m(ASA^{-1}) \cdot ASA^{-1}m(\sigma) \cdot p(ASA^{-1}, A)/\sigma m(\sigma S\sigma^{-1}).$$

Now we put

(48) $$m(\sigma T) = m(\sigma) \cdot \sigma m(T) \cdot p(A, \sigma^{-1}T\sigma).$$

Then, from (46), it follows that

(49) $$m(\sigma^{-1}) \cdot \sigma^{-1}m(\sigma^{-1}) = m(A^{-1}).$$

Note that $p(A, A^{-1}) = m(\sigma^{-1})/m(\sigma) \cdot \sigma m(A^{-1})$. From (43), (48) and (49), we have

(50) $$m(\sigma) \cdot \sigma m(\sigma) = m(A).$$

In (47), we substitute S by $A^{-1}SA$, then we have

(51) $$p(A, A^{-1}SA)/p(S, A) = m(S) \cdot Sm(\sigma)/m(\sigma) \cdot \sigma m(\sigma^{-1}S\sigma).$$

That is,

(52) $$Sm(\sigma) = m(\sigma) \cdot [p(A, A^{-1}SA) \cdot \sigma m(\sigma^{-1}S\sigma)/p(S, A) \cdot m(S)].$$

Now we can show that the formulae (35), $\cdots$, (38) hold. (35) holds trivially by (43). From (43) and (48), we have

$$\begin{aligned}
&m(\sigma ST)/m(\sigma S) \cdot \sigma Sm(T) \\
&\quad = \sigma[m(ST)/m(S) \cdot Sm(T)] \cdot p(A, \sigma^{-1}ST\sigma)/p(A, \sigma^{-1}S\sigma) \\
&\quad = \sigma p(S, T) \cdot Ap(\sigma^{-1}S\sigma, \sigma^{-1}T\sigma) \cdot p(A, \sigma^{-1}ST\sigma)/p(A, \sigma^{-1}S\sigma) \\
&\quad = p(\sigma S\sigma, \sigma^{-1}T\sigma) \cdot \sigma p(S, T).
\end{aligned}$$

Thus (36) holds. Note that p is a 2-cocycle of H. From (43), (48) and (51), we have

$$m(S\sigma T)/m(S)\cdot Sm(\sigma T)=p(S,\sigma T\sigma)\cdot\sigma p(\sigma^{-1}S\sigma,T).$$

Thus (37) also holds. From (43), (48), (50) and (52), in the similar but more complicated way, we have

$$m(\sigma S\sigma T)/m(\sigma S)\cdot\sigma Sm(\sigma T)=p(\sigma S\sigma,T)\cdot\sigma p(S,\sigma T\sigma).$$

Thus we have proved Proposition 3.

College of General Education,
University of Tokyo

References

[1] A. A. Albert, Structure of algebras, AMS Colloquium Publications, 1939.
[2] M. Kneser, Galois-Kohomologie halbeinfacher algebraischer Gruppen über $\mathfrak{p}$-adischen Körpern. II, Math. Z., **89** (1965), 250–272.
[3] T. Ono, Arithmetic of algebraic tori, Ann. of Math., **74** (1961), 101–139.
[4] T. Ono, On the Tamagawa number of algebraic tori, Ann. of Math., **78** (1963), 47–73.
[5] I. Satake, Symplectic representations of algebraic groups statisfying a certain analyticity condition, Acta Math., **117** (1967), 215–279.
[6] J-P. Serre, Corps locaux, Hermann, Paris, 1962.
[7] J-P. Serre, Cohomologie galoisienne, Cours au Collège de France, 1963.
[8] T. Tasaka, On the quasi-split simple algebraic groups defined over an algebraic number field, (to appear in J. Fac. Sci. Univ. Tokyo).
[9] J. Tits, Classification of algebraic semi-simple groups. Algebraic groups and discontinuous subgroups, Proc. of symposia in pure mathematics, vol. IX, 33–62.