T. Ono
Nagoya Math. J.
Vol. 79 (1980), 131–140

ON THE GROUP OF AUTOMORPHISMS OF A HOPF MAP

TAKASHI ONO

§1. Introduction

Let K be an infinite field of characteristic not 2. Let q_X, q_Y be nonsingular quadratic forms on vector spaces X, Y over K, respectively. Assume that there is a bilinear map $B: X \times Y \to Y$ such that $q_Y(B(x, y)) = q_X(x)q_Y(y)$. To each such triple $\{q_X, q_Y, B\}$ one associates the Hopf map $h: Z = X \times Y \to W = K \times Y$ by $h(z) = (q_X(x) - q_Y(y), 2B(x, y))$, $z = (x, y)$. Denote by q_Z, q_W quadratic forms on Z, W, respectively, defined by $q_Z(z) = q_X(x) + q_Y(y)$, $q_W(w) = u^2 + q_Y(v)$, $w = (u, v)$. One sees easily that $q_W(h(z)) = q_Z(z)^2$, which means that h sends a sphere into a sphere. We shall denote by G the group of automorphisms of h, i.e. the group formed by all automorphisms $s \in GL(Z)$ such that $h(sz) = h(z)$ for all $z \in Z$. After the model of the relationship of quadratic forms and orthogonal groups, it is natural to ask questions such as: what is the structure of G, how G acts on the fibre, what the 1st cohomology of G looks like, and how about the Hasse principle for G when the ground field is a number field? In the present paper, we shall limit our considerations to the case where X is an algebra with 1 over K together with a nonsingular quadratic form q_X such that $q_X(xy) = q_X(x)q_X(y)$, $x, y \in X$. Thanks to a theorem due to A. Hurwitz, such algebras, called composition algebras, are completely determined (cf. [1], Theorem 3.25, p. 73). Namely, an algebra (X, q_X) is one of the following: (I) $X = K$; (II) $X = K + K$; (III) $X =$ a quadratic extension of K; (IV) $X =$ a quaternion algebra over K; (V) $X =$ a Cayley algebra over K. Furthermore, if $X = K$, then $q_X(x) = x^2$; otherwise q_X is the norm form on X. Except for some easy arguments which work for an arbitrary triple $\{q_X, q_Y, B\}$, our results depend on the above theorem of Hurwitz. One can answer completely the questions mentioned above. For the general case, I have, at present, no definite idea how to handle it except the feeling that one needs detailed study of representations of Clifford algebras.

Received March 20, 1979.

§ 2. The subgroup N

Notations being as in § 1, since we have $q_W(hz) = q_Z(z)^2$, for $s \in G$, we have $q_Z(sz) = e(s, z)q_Z(z)$ with $e(s, z) = \pm 1$. Let $E = \{z \in Z, q_Z(z) \neq 0\}$. Since E is a non-empty open subset of the irreducible set Z, E is also irreducible. Let f_s be a function $E \to K$ defined by $f_s(z) = q_Z(sz)/q_Z(z)$. As f_s is a continuous map, its image which is a subset of $\{\pm 1\}$ must be irreducible, and so $e(s, z) = \chi(s)$, a function of s only.*) Obviously, $\chi(s)$ is a homomorphism of G into $\{\pm 1\}$. Call N the kernel of χ. In this section, we consider N. Later on, we shall study the complement $G - N$ to decide whether $G = N$ or $[G: N] = 2$.

An endomorphism $s: Z \to Z$ can be written as

$$s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad \text{where } \alpha, \beta, \gamma, \delta$$

are linear maps $X \to X$, $Y \to X$, $X \to Y$, $Y \to Y$, respectively. Using the column notation for $z = (x, y)$, we have

$$s(z) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix} .$$

Now, we have

$$s \in N \Longleftrightarrow h(sz) = h(z) \quad \text{and} \quad q_Z(sz) = q_Z(z) .$$

In other words, we have

$$s \in N \Longleftrightarrow \begin{cases} q_X(\alpha x + \beta y) - q_Y(\gamma x + \delta y) = q_X(x) - q_Y(y) , \\ q_X(\alpha x + \beta y) + q_Y(\gamma x + \delta y) = q_X(x) + q_Y(y) , \\ B(\alpha x + \beta y, \gamma x + \delta y) = B(x, y) , \end{cases}$$

or

$$s \in N \Longleftrightarrow \begin{cases} q_X(\alpha x + \beta y) = q_X(x) , & (2.1) \\ q_Y(\gamma x + \delta y) = q_Y(y) , & (2.2) \\ B(\alpha x + \beta y, \gamma x + \delta y) = B(x, y) . & (2.3) \end{cases}$$

Let $(\ ,\ )_X$, $(\ ,\ )_Y$ be the inner product associated to q_X, q_Y, respectively. Then, (2.1) can be written as

$$q_X(\alpha x) + q_Y(\beta y) + 2(\alpha x, \beta y)_X = q_X(x) . \tag{2.4}$$

*) We assumed the field K infinite because we needed the Zariski topology here.

Similarly, (2.2) can be written as

$$q_Y(\gamma x) + q_Y(\delta y) + 2(\gamma x, \delta y)_Y = q_Y(y) . \tag{2.5}$$

If we put $x = 0$ in (2.1), then we have $q_X(\beta y) = 0$. If, on the other hand, we put $y = 0$ in (2.1), then we have $q_X(\alpha x) = q_X(x)$ and hence $\alpha \in O(q_X)$, the orthogonal group of q_X. Substituting these results back in (2.4), we see that $(\alpha x, \beta y)_X = 0$ for all $x \in X$, $y \in Y$. Since α is invertible, this implies that $\beta y = 0$ for all y, i.e. $\beta = 0$. Similarly, using (2.2), (2.5), we see that $\gamma = 0$ and $\delta \in O(q_Y)$. We have therefore proved that

$$N = \left\{ s = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}, \ \alpha \in O(q_X), \ \delta \in O(q_Y), \ B(\alpha x, \delta y) = B(x, y) \right\} . \tag{2.6}$$

(2.7) *Remark.* Let e be a vector in X such that $q_X(e) = 1$. If such e is available, the map t defined by $t(y) = B(e, y)$ belongs to $O(q_Y)$ in view of the relation $q_Y(B(x, y)) = q_X(x)q_Y(y)$. Therefore, if we put $B_0(x, y) = t^{-1}B(x, y)$, then we get a bilinear map $X \times Y \to Y$ with the property $B_0(e, y) = y$, $y \in Y$, in addition to the property $q_Y(B_0(x, y)) = q_X(x)q_Y(y)$. Hence, without much loss of generality, we may assume from the beginning that the bilinear map B satisfies the condition that $B(e, y) = y$ for an $e \in X$ with $q_X(e) = 1$. It then follows that $\delta y = B(e, \delta y) = B(\alpha^{-1}e, y)$ and so we have a group isomorphism:

$$N \approx \{\alpha \in O(q_X), \ B(\alpha x, B(\alpha^{-1}e, y)) = B(x, y)\} . \tag{2.8}$$

§ 3. The set $G - N$

First of all, we have

$$s \in G - N \Longleftrightarrow h(sz) = h(z) \quad \text{and} \quad q_Z(sz) = -q_Z(z) .$$

Therefore,

$$s \in G - N \Longleftrightarrow \begin{cases} q_X(\alpha x + \beta y) - q_Y(\gamma x + \delta y) = q_X(x) - q_Y(y) , \\ q_X(\alpha x + \beta y) + q_Y(\gamma x + \delta y) = -q_X(x) - q_Y(y) , \\ B(\alpha x + \beta y, \ \gamma x + \delta y) = B(x, y) , \end{cases}$$

or

$$s \in G - N \Longleftrightarrow \begin{cases} q_X(\alpha x + \beta y) = -q_Y(y) , & (3.1) \\ q_Y(\gamma x + \delta y) = -q_X(x) , & (3.2) \\ B(\alpha x + \beta y, \ \gamma x + \delta y) = B(x, y) . & (3.3) \end{cases}$$

Here (3.1) can be written as

$$q_X(\alpha x) + q_X(\beta y) + 2(\alpha x, \beta y)_X = -q_Y(y) \tag{3.4}$$

and (3.2) can be written as

$$q_Y(\gamma x) + q_Y(\delta y) + 2(\gamma x, \delta y)_Y = -q_X(x)\,. \tag{3.5}$$

If we put $y = 0$ in (3.1), we have $q_X(\alpha x) = 0$. If we put $x = 0$ in (3.1), we have $q_X(\beta y) = -q_Y(y)$ and hence β is injective, i.e. β embeds $(Y - q_Y)$ into (X, q_X). Similarly, from (3.2), (3.5), $q_Y(\delta y) = 0$ and $q_Y(\gamma x) = -q_X(x)$ where the latter implies that γ embeds (X, q_X) into $(Y, -q_Y)$. In other words, β and γ are isometries of (X, q_X) and $(Y, -q_Y)$. Since (3.4) implies $(\alpha x, \beta y)_X = 0$ for all $x \in X$, $y \in Y$, we have $\alpha x = 0$, i.e. $\alpha = 0$. Similarly, by (3.5), we have $\delta = 0$. We have therefore proved that

$$G - N = \left\{ s = \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix},\ q_X\beta = -q_Y,\ q_Y\gamma = -q_X,\ B(\beta y, \gamma x) = B(x, y) \right\}. \tag{3.6}$$

(3.7) *Remark.* As in (2.7), assume that B satisfies the additional condition $B(e, y) = y$. Then we have $\gamma x = B(e, \gamma x) = B(x, \beta^{-1}e)$ and so a bijection of sets:

$$G - N \approx \left\{ \beta,\ (Y, -q_Y) \xrightarrow[\sim]{\beta} (X, q_X),\ B(\beta y, B(x, \beta^{-1}e)) = B(x, y) \right\}. \tag{3.8}$$

(3.9) *Remark.* As (3.6) shows, we have $G = N$ unless (X, q_X) and $(Y, -q_Y)$ are isometric. For example, if $\dim X \neq \dim Y$, then $G = N$, always. One can also determine the structure of the triple $\{q_X, q_Y, B\}$ with isometries

$$(X, q_X) \underset{\beta}{\overset{\gamma}{\rightleftarrows}} (Y, -q_Y)$$

by making use of the theorem of Hurwitz.

§ 4. Composition algebras

Let (X, q_X) be a composition algebra over K. This is a special case of the triple $\{q_X, q_Y, B\}$ where $Y = X$, $q_Y = q_X$, $B(x, y) = xy$. Moreover, X has the identity 1 and so the remarks (2.7), (3.7) are available. If we put $a = \alpha^{-1}(1)$, $b = \delta^{-1}(1)$, the last equality of (2.6) implies that $\alpha x = xb$ and $\delta y = ay$. Substituting these in (2.8), we have the group isomorphism:

$$(4.1)\qquad \begin{aligned} N &\approx \{a \in X,\ q_X(a) = 1,\ (xa^{-1})(ay) = xy \text{ for all } x, y \in X\} \\ &= \{a \in X,\ q_X(a) = 1,\ x(ay) = (xa)y \text{ for all } x, y \in X\}\ . \end{aligned}$$

If the algebra X is *associative*, then we have simply:

$$(4.2)\qquad N \approx \{a \in X,\ q_X(a) = 1\}\ ,$$

the group of norm one in X. In view of the theorem of Hurwitz, it remains the case where X is the Cayley algebra. In this case, we have $X = Y + Y\omega$, $Y = K + Ki + Kj + Kk$, a quaternion algebra. The multiplication and conjugation in X are given as follows: $\omega^2 = \mu \in K^\times$, $\omega x = \bar{x}\omega$, $x(y\omega) = (yx)\omega$, $(x\omega)y = (x\bar{y})\omega$, $(x\omega)(y\omega) = \mu\bar{y}x$, $\overline{x + y\omega} = \bar{x} - y\omega$, $x, y \in Y$. Now, write $a = b + c\omega$, $b, c \in Y$ and put $x = i$, $y = j$ in the relation $x(ay) = (xa)y$. Then, we end up with the equality $ibj - ck\omega = ibj + ck\omega$, which implies that $c = 0$, i.e. $a = b \in Y$. Next, put $x = y\omega$, $y = \omega$ in $x(ay) = (xa)y$. It then follows that $a \in K$, the center of Y. We have therefore proved that

$$(4.3)\qquad N \approx \{\pm 1\} \qquad \text{when } X \text{ is a Cayley algebra}\ .$$

We now turn to the set $G - N$. If we put $a = \gamma^{-1}(1)$, $b = \beta^{-1}(1)$, the last equality of (3.6) implies that $\gamma x = xb$, $\beta y = ay$. Note that $q_X(a) = q_X(b) = -1$ because $q_X\beta = -q_X = q_X\gamma$. Substituting these in (3.8), we have the bijection of sets:

$$(4.4)\qquad \begin{aligned} G - N &\approx \{a \in X,\ q_X(a) = -1,\ (ay)(xa^{-1}) = xy \text{ for all } x, y \in X\} \\ &= \{a \in X,\ q_X(a) = -1,\ (ay)x = (xa)y \text{ for all } x, y \in X\}\ . \end{aligned}$$

If the algebra X is *commutative*, then we have simply:

$$(4.5)\qquad G - N \approx \{a \in X,\ q_X(a) = -1\}\ .$$

In view of the theorem of Hurwitz, it remains the cases where X is a quaternion algebra or a Cayley algebra. Putting $y = 1$ in the relation $(ay)x = (xa)y$, we see that $a \in K$ because these algebras are central. But then we must have $xy = yx$ if there is an $a \in K$ such that $q_X(a) = a^2 = -1$. Thus the set $G - N$ is empty, i.e.

(4.6) $G = N$ when X is either a quaternion algebra or a Cayley algebra.

From (4.1)–(4.6), we get the following

(4.7) THEOREM. *Let K be an infinite field of characteristic not 2, X be a composition algebra over K and $n(x)$ be the norm form on X. Let $h\colon Z = X \times X \to W = K \times X$ be the Hopf map given by $h(z) = (n(x) - n(y), 2xy)$,*

$z = (x, y)$, G be the group of automorphisms $s \in GL(Z)$ such that $h(sz) = h(z)$ and N be the subgroup of G consisting of s such that $q_Z(sz) = q_Z(z)$, where $q_Z(z) = n(x) + n(y)$. According to the theorem of Hurwitz, classify X as (I) $X = K$; (II) $X = K + K$; (III) $X =$ a quadratic extension of K; (IV) X a quaternion algebra over K; (V) $X =$ a Cayley algebra over K. Then we have the following table:

type of X	N	$[G: N]$
(I)	$\{\pm 1\}$	1 when $\sqrt{-1} \notin K$ 2 when $\sqrt{-1} \in K$
(II)	$K^\times$	2
(III)	$\{x \in X,\ n(x) = 1\}$	1 when $n(x) = -1$ has no solutions 2 when $n(x) = -1$ has a solution
(IV)	$\{x \in X,\ n(x) = 1\}$	1
(V)	$\{\pm 1\}$	1

(4.8) In the table, the groups described are not the group N itself but isomorphic images of N.

(4.9) For $t \in K^\times$, put $S_Z(t) = \{z \in Z = X \times X,\ q_Z(z) = t\}$. Then, h induces a map $h_t\colon S_Z(t) \to S_W(t^2) = \{w \in W = K \times X,\ q_W(w) = t^2\}$. Let $w \in S_W(t^2)$ be such that the fibre $h_t^{-1}(w) \neq \emptyset$. Since $z \in Z$ belongs to this fibre if and only if $h(z) = w$ and $q_Z(z) = t$, the group N acts on $h_t^{-1}(w)$. As $q_Z(z) = n(x) + n(y)$, $q_W(w) = u^2 + n(v)$, $z = (x, y)$, $w = (u, v)$, we have

$$z \in h_t^{-1}(w) \iff \begin{cases} n(x) + n(y) = t \\ n(x) - n(y) = u \\ 2xy = v \end{cases} \iff \begin{cases} n(x) = r \\ n(y) = s\,, \\ 2xy = v \end{cases}$$

with $r = \frac{1}{2}(t + u)$, $s = \frac{1}{2}(t - u)$. Since $t \neq 0$, either r or $s \neq 0$. If $r \neq 0$, then x is invertible and $y = \frac{1}{2}x^{-1}v$. We have therefore the bijection $h_t^{-1}(w) \approx \{x \in X,\ n(x) = r\}$. If we identify N with $\{a \in X,\ n(a) = 1,\ x(az) = (xa)y\}$ by (4.1), then the action of N on $h_t^{-1}(w)$ is given by $x \mapsto xa^{-1}$ or $x \mapsto ax$ according as $r \neq 0$ or $s \neq 0$. From the table of (4.7), we see that N acts transitively on the fibre when X is of type (II), (III), (IV).

§5. Tate-Shafarevich set for algebraic groups

Let k be an algebraic number field of finite degree over the field $\boldsymbol{Q}$ of rational numbers. Let G be an algebraic group defined over k. Using the standard notation in Galois cohomology, we put

$$Ш(k, G) = \operatorname{Ker}\left(H^1(k, G) \longrightarrow \prod_v H^1(k_v, G)\right),$$

and call this the Tate-Shafarevich set for G over k. Basic references for Galois cohomology are [2] and [3]. In this section, we shall prove two lemmas which will be needed in the next section.

(5.1) LEMMA. *Let K/k be a finite Galois extension and G be an algebraic group defined over k. If $Ш(K, G) = 0$, then there is a bijection $Ш(k, G) \approx Ш(K/k, G_K)$, where*

$$Ш(K/k, G) = \operatorname{Ker}\left(H^1(K/k, G_K) \longrightarrow \prod_v H^1(K_v/k_v, G_{K_v})\right)$$

and K_v is the field which is the completion of K taken in the algebraic closure $\bar{k}_v$ of k_v.

Proof. Consider the following commutative diagram:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 \longrightarrow & & Ш(K/k, G_K) & \xrightarrow{\alpha} & Ш(k, G) & \xrightarrow{\beta} & Ш(K, G) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 \longrightarrow & & H^1(K/k, G_K) & \xrightarrow{\text{inf}} & H^1(k, G) & \xrightarrow{\text{res}} & H^1(K, G) \\
 & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow \\
0 \longrightarrow & & \prod_v H^1(K_v/k_v, G_{K_v}) & \xrightarrow{\varepsilon} & \prod_v H^1(k_v, G) & \longrightarrow & \prod_w H^1(K_w, G)
\end{array}$$

where all columns and the middle row are exact, α, inf, ε are injective and K_w is the completion of K at a place w of K. We shall show that $\operatorname{Im}\alpha = \operatorname{Ker}\beta$. In fact, take $x \in Ш(K/k, G_K)$. Then we have $\beta\alpha(x) = \operatorname{res}\operatorname{inf}(x) = 0$ and hence $\operatorname{Im}\alpha \subset \operatorname{Ker}\beta$. Next, take $y \in \operatorname{Ker}\beta \subset \operatorname{Ker}(\text{res})$. Then $y = \operatorname{inf}(x)$ for some $x \in H^1(K/k, G_K)$. It then follows that $0 = \delta(y) = \delta\operatorname{inf}(x) = \varepsilon\gamma(x)$. Since ε is injective, we have $\gamma(x) = 0$, i.e. $x \in Ш(K/k, G_K)$ which shows that $\operatorname{Ker}\beta \subset \operatorname{Im}\alpha$. Now, if $Ш(K, G) = 0$, then the relation $\operatorname{Im}\alpha = \operatorname{Ker}\beta$ means that α is surjective, which proves our assertion, q.e.d.

(5.2) Lemma. *We have* Ш$(k, G) = 0$ *if* G *is a finite abelian group consisting of* k*-rational points only.*

Proof. Denote by $\mathfrak{g}$ (resp. $\mathfrak{g}_v$) the Galois group of $\bar{k}/k$ (resp. $\bar{k}_v/k_v$). By the assumption, $\mathfrak{g}$ and $\mathfrak{g}_v$ act trivially on G. Hence, Ш(k, G) is nothing else than the kernel of the canonical map

$$\theta\colon \mathrm{Hom}(\mathfrak{g}, G) \longrightarrow \prod_v \mathrm{Hom}(g_v, G)$$

where Hom means the continuous homomorphisms with respect to the Krull topology on the Galois group and the discrete topology on G. Now, take any $\xi \in \mathrm{Ker}\,\theta$. Because of the continuity of ξ, there is an open normal subgroup $\mathfrak{h}$ of $\mathfrak{g}$ such that $\xi(\mathfrak{h}) = 0$, and hence $\xi(\mathfrak{g}_v\mathfrak{h}) = 0$ for all v. Call K/k the finite Galois extension corresponding to $\mathfrak{h}$. To $\mathfrak{g}_v h$ corresponds the field $(K \cap k_v)/k$ which is the decomposition field of a valuation of K which induces v on k. For any $\sigma \in \mathfrak{g}$, put $s = \sigma\mathfrak{h} \in \mathfrak{g}(K/k)$, the Galois group of K/k. By Tschebotareff density theorem, one has $tst^{-1} \in \mathfrak{g}(K/K \cap k_{\mathfrak{p}})$ for some finite prime $\mathfrak{p}$ of k, and for some $t \in \mathfrak{g}(K/k)$. If one puts $t = \tau\mathfrak{h}$ with $\tau \in \mathfrak{g}$, then $\tau\sigma\tau^{-1} \in \mathfrak{g}_{\mathfrak{p}}\mathfrak{h}$. Hence $\xi(\sigma) = \xi(\tau\sigma\tau^{-1}) = 0$ since $\xi \in \mathrm{Ker}\,\theta$, and so $\xi = 0$, q.e.d.

§ 6. Hasse principle for G attached to a composition algebra

Let (X, n) be a composition algebra defined over a number field k. By definition, there is a composition algebra (X_k, n_k) over k such that (X, n) is obtained by extending the ground field k to a universal domain Ω containing k. The Hopf map

$$h\colon Z = X \times X \longrightarrow W = \Omega \times X$$

is given by $h(z) = (n(x) - n(y), 2xy)$, $z = (x, y)$, and the group G of automorphisms of h becomes an algebraic group defined over k. Our main result is the

(6.1) Theorem. *Let* G *be the group of automorphisms of the Hopf map associated to a composition algebra defined over a number field* k. *Then, we have* Ш$(k, G) = 0$, *i.e. the Hasse principle holds for* G.

Proof. We split the proof into five cases according to the type of the algebra (X_k, n_k) described in the theorem of Hurwitz.

Type (I). In this case $X = \Omega$, $n(x) = x^2$ and $h(z) = (x^2 - y^2, 2xy)$. By (2.6), (3.6) (or by a direct calculation) we see that G is a finite abelian group consisting of elements $\pm 1, \pm\gamma$ where

$$\gamma = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \qquad i = \sqrt{-1}\,.$$

Put $K = k(i)$. Then, since every element of G is K-rational, we have $Ш(K, G) = 0$ by (5.2). Thus $Ш(k, G) = 0$ if $i \in k$. On the other hand, in case where $i \notin k$, we have $Ш(k, G) \approx Ш(K/k, G_K)$ by (5.1). We now prove that $H^1(K/k, G_K) = 0$ which, of course, implies that $Ш(K/k, G_K) = 0$. In fact, let $(a_\sigma) = \{1, a\}$ be a cocycle of $\mathfrak{g}(K/k)$ in G_K. This simply means that $aa^s = 1$ where s is the generator of $\mathfrak{g}(K/k)$. One sees easily that $a = \pm 1$ and $1 = 1^{-1}1^s$, $-1 = \gamma^{-1}\gamma^s$, which shows that (a_σ) is trivial.

Type (II). In this case, from (4.7), it follows that

$$0 \longrightarrow N \longrightarrow G \xrightarrow{\ \chi\ } \{\pm 1\} \longrightarrow 0 \qquad \text{(exact)}\,,$$

where $N \approx \Omega^\times$ and hence $H^1(k, N) = 0$ by Hilbert theorem 90. Take a cocycle (a_σ) from $Ш(k, G)$. Then, $b_\sigma = \chi(a_\sigma)$ defines a cocycle (b_σ) in $Ш(k, \{\pm 1\})$ which is 0 by (5.2). This implies that $b_\sigma = 1$, i.e. $a_\sigma \in N$. Since $H^1(k, N) = 0$, we have $a_\sigma \sim 0$ in N and hence in G. We have thus proved that $Ш(k, G) = 0$.

Type (III). In this case, $X_k = K$, a quadratic extension, n_k is the norm for K/k and $N = \{x \in X, n(x) = 1\}$, a torus of dimension one which is split by K. Hence, we have $H^1(K, N) = 0$ by Hilbert theorem 90. Take a cocycle (a_σ) from $Ш(K, G)$. Then $b_\sigma = \chi(a_\sigma)$ defines a cocycle (b_σ) in $Ш(K, \{\pm 1\})$ which is 0 by (5.2). Hence $b_\sigma = 1$ and so $a_\sigma \in N$. Then, Hilbert theorem 90 for N over K implies that $a_\sigma \sim 0$ in N and hence in G, which proves that $Ш(K, G) = 0$. Therefore, by (5.1), we have $Ш(k, G) \approx Ш(K/k, G_K)$. Having reduced the problem to the case of quadratic extension K/k, we write $K = k(\theta)$ with $\theta^2 = m \in k$. Hence, we have $n(z) = x^2 - my^2$ if $z = x + y\theta$, $x, y \in \Omega$. From (4.5), we see that, for any field extension L/k, we have $[G_L : N_L] = 2$ if and only if $x^2 - my^2 = -1$ has solutions x, y in L. Now, take a cocycle (a_σ) from $Ш(K/k, G_K)$. By a similar argument as above, using $Ш(K/k, \{\pm 1\}) = 0$, we see that $a_\sigma \in N_K$. We shall prove that $a_\sigma \sim 0$ in N_{K_v} for all v in k. If that is so, our assertion will follow from the known fact $Ш(K/k, N_K) = 0$ (See [4] Proposition 4.5.1). First of all, if the valuation v is such that $K_v = k_v$, then the matter is trivial because $(a_\sigma) = \{1\}$. So, from now on, we shall only consider the case where $[K_v : k_v] = 2$. In this case, we have $(a_\sigma) = \{1, a\}$ with $a \in N_K$. The assumption $a_\sigma \sim 0$ in G_{K_v} means that $a = g_v^{-1} g_v^s$, where s is the conjugation in K_v/k_v. If $g_v \in N_{K_v}$, then $a_\sigma \sim 0$ in N_{K_v} already. If not, we write $g_v = wt_v$ with $t_v \in N_{K_v}$ and

w, any element of $G_K - N_K$. We now show that we can find w such that $w^s = -w$. Namely, identifying X with Ω^2 by setting $x_1 + x_2\theta = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, put $\beta(x) = \begin{pmatrix} 0 & \theta \\ \theta^{-1} & 0 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$. Then, by (3.6), we see that $w = \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix} \in G_K - N_K$ because $n(\beta(y)) = (\theta y_2)^2 - m(\theta^{-1}y_1)^2 = my_2^2 - y_1^2 = -n(y)$ and $(\beta y)(\beta x) = (\theta y_2 + \theta(\theta^{-1}y_1))(\theta x_2 + \theta(\theta^{-1}x_1)) = mx_2y_2 + x_1y_1 + \theta(x_1y_2 + x_2y_1) = (x_1 + \theta x_2)(y_1 + \theta y_2) = xy$. It is obvious that $w^s = -w$. Using this w, we have $a = g_v^{-1}g_v^s = t_v^{-1}w^{-1}w^st_v^s = -t_v^{-1}t_v^s$. We next show that we can find $u \in N_{K_v}$ such that $-1 = u^{-1}u^s$. In fact, take $\xi, \eta \in k_v$ such that $\xi + \eta = 1$, $\xi - \eta = m^{-1}$, and put $x = \theta\xi$, $y = \eta$, $u = x + \theta y$. Then, $u^s = x^s - \theta y^s = -x - \theta y = -u$ and $n(u) = x^2 - my^2 = m\xi^2 - m\eta^2 = m(\xi + \eta)(\xi - \eta) = 1$. We have therefore $a = g_v^{-1}g_v^s = (t_vu)^{-1}(t_vu)^s$ and hence $a_\sigma \sim 0$ in N_{K_v}, again.

Type (IV). In this case, $G = N$ and $N = \{x \in X, n(x) = 1\}$. Denote by X_0 the subspace of X consisting of quaternions of trace zero and by n_0 the quadratic form induced on X_0 by n. Then N is a simply connected group (the spin group) which forms a double covering of the rotation group $O^+(n_0)$. Then, we have $\text{Ш}(k, G) = 0$ as is well-known (See [3]).

Type (V). In this case, $G = N = \{\pm 1\}$ and our assertion follows from (5.2), q.e.d.

References

[1] R. Schafer, An introduction to nonassociative algebras, Academic Press, New York, 1966.
[2] J.-P. Serre, Cohomologie galoisienne, Lecture Notes in Mathematics, Springer-Verlag, 1964.
[3] M. Kneser, Lectures on Galois cohomology of classical groups, Tata Institute, Bombay, 1969.
[4] T. Ono, On the Tamagawa number of algebraic tori, Ann. of Math. **78** (1963), 47–73.

The Johns Hopkins University