Journal of the Mathematical Society of Japan Vol. 4, Nos. 3~4, December, 1952.

On the multiplicative group of simple algebras and orthogonal groups of three dimensions.

By Akira HATTORI

(Received March 24, 1952)

It is known that the commutatorgroup of the general linear group over a division algebra is simple (modulo its center)[1], but little is known on the multiplicative group of a division algebra itself. In this paper we shall consider this group as a group of substitutions of a system of isomorphic subfields. We shall prove that this representation is always faithful. This fact constitutes a stronger result than a generalization of a theorem of H. Cartan[2], which we have proved in our previous note[3]. Geometrically expressed, the group of inner automorphisms of a central simple algebra becomes thus a group of linear transformations which operates transitively on an algebraic variety. Since a simple algebra is a symmetric algebra, this group is consisting of rotations with respect to some metric.

Next, we shall treat generalized quaternion algebras as the simplest case, and shall prove that their groups of inner automorphisms are isomorphic to rotation groups of three dimensions and that all rotation groups are found in this way. This is a generalization of the wellknown parametrization of the real rotation group by real quaternions on the one hand, and of the isomorphism of some rotation groups with the projective general groups of dimension two[4] on the other hand. This result, combined with an idea of J. Dieudonné by which he has given some examples of rotation groups having an infinite series of normal subgroups[5], permits us to determine completely the structure of rotation groups of three dimensions over the rational number field.

It is also the case for an arbitrary symmetric algebra that the multiplicative group of the algebra is represented into a rotation group. Then, what subgroup of the rotation group will be the image of this representation? In § 3, we shall prove that, if the image is the

whole rotation group then the algebra is, essentially, a generalized quaternion algebra. This fact was found first in the real scalar case by Mr. N. Iwahori, who gave us many advices on the whole of this paper, and to whom the author wishes to say many thanks.

§ 1. A class of representations of the multiplicative group of simple algebras.

Let F be a field, A a central simple algebra (of a finite dimension) over F. F will be assumed to contain an infinite number of elements, since our main interest lies in the case where A is a division algebra. If B is a simple subalgebra[6] of A other than A and F, we shall denote by $V(B)$ the commuter algebra of B in A. If another simple subalgebra B' is isomorphic to B over F, then the isomorphism of B with B' can be extended to an inner automorphism of A. Thus, denoting by $[B]$ the totality of subalgebras of A isomorphic to B, the group $I(A)$ of all inner automorphisms of A has a representation as a transitive group of substitutions on $[B]$. $I(A)$ is isomorphic to A^*/F^*, the asterisk being used as usual to denote the multiplicative group of a ring. If $aBa^{-1}=B'$ for a in A^*, we say simply a maps B onto B'.

Now, the non-existence of *invariant subrings* ($\neq A$, $\not\subset F$) in A (IS.[3] Theorem 1) implies the non-triviality of such a representation of $I(A)$ with respect to every simple B. We shall prove here moreover

PROPOSITION 1. *The representation of $I(A)$ as a group of substitutions on $[B]$ is faithful.*

When B is a commutative field K, we have a more precise result. Namely

PROPOSITION 2. *Let K be a subfield of A of degree $r>1$ over F.*

i) *If $K_i \in [K]$, $i=1, \ldots\ldots, l$, are such that $\bigcap_{i=1}^{l} V(K_i)=F$, the group of all inner automorphisms of A which map every K_i onto K_i itself ($i=1,\ldots\ldots, l$) is a finite group of order at most r^l.*

ii) *There are a finite number of subfields $K_i \in [K]$, $i=1, \ldots, m$, $K_1=K$, such that the only inner automorphism mapping every K_i onto K_i is the identity automorphism.*

PROOF OF PROPOSITION 2. By means of the non-existence of invariant subrings we can find actually a finite number of fields K_i, $i=1, \ldots\ldots, l$, such that $K_i \in [K]$, $K_1=K$ and $\cap V(K_i)=F$, since $\bigcap_{K_\alpha \in [K]} V(K_\alpha)$ is an invariant subring other than A. Let H be the totality of inner automorphisms which map every K_i onto K_i, $i=1, \ldots\ldots, l$, and assume that H contains r^l+1 distinct automorphisms. Since every one of these automorphisms induces an automorphism of K_1 over F, and since K_1 has at most r automorphisms over F, at least $r^{l-1}+1$ automorphisms in H induce on K_1 one and the same automorphism. These $r^{l-1}+1$ automorphisms map every K_i onto K_i, $i=2, \ldots\ldots, l$. Thus, in repeating this argument, we obtain finally two distinct automorphisms σ and τ which have the same effect on K_i, $i=1, \ldots\ldots, l$. Let a and b in A^* give rise to σ and τ, respectively, then $a^{-1}b$ commutes with every elements in any one of K_i, $i=1, \ldots\ldots, l$. Thus we have $a^{-1}b \in \cap V(K_i)=F$, which implies that σ and τ are identical; but this is a contradiction, and the first half i) of Proposition 2 is proved.

Therefore, the kernel of the homomorphic mapping of $I(A)$ into the group of substitutions on $[K]$ is of course a finite group. Now we have

LEMMA 1. *The only normal subgroup of $I(A)$ of finite order is the identity group.*

PROOF. We know that, if $N(\neq(1))$ is a normal subgroup of $I(A)$ then $I(A)$ can be considered as a group of automorphisms of N. (The last proposition in IS.) Since $I(A) \cong A^*/F^*$ is not a finite group by our assumption on F, N can, of course, not be a finite group.

By means of this Lemma, Proposition 1 is proved for the case where B is a commutative field.

This fact, together with i), yields immediately the second half ii) of Proposition 2.

PROOF OF THE GENERAL CASE OF PROPOSITION 1. Let $N(B)$ be the totality of elements of A mapping every B' in $[B]$ onto B' itself, then $N(B)$ is a normal subgroup of A^*. If the center K of B has a degree >1 over F then $N(B) \subset N(K)=F^*$, since K is a commutative field. Hence we shall confine ourselves to B whose center

coincides with F. A is then a Kronecker product of B with its commuter C, and $N(B)$ is contained in B^*C^*. We shall show $N(B)=F^*$.

a) First, we consider the case where A is not a division algebra. Then, A is a matrix algebra of a degree >1 over a division algebra D, and the commutator group S of A^* is simple mod. F^*. Thus, if $N(B) \neq F^*$, $N(B) \supset S$. Let e_{ij} denote the matrix units of A. Then $1+\lambda e_{ij}$, $\lambda \in D$, $i \neq j$, are all contained in S[7]. If $b \in B$ then

$$(1+\lambda e_{ij})\, b\, (1-\lambda e_{ij})-b \in B\,. \tag{1}$$

Thus, it is easy to see that B contains an element $b=\sum \beta_{kl} e_{kl}$ such that one of its coefficients not on the diagonal, say $\beta=\beta_{ij}$, $j \neq i$, is not zero. Applying (1) to this b with $\lambda=\lambda_1$, $\lambda_2 \neq 0$ in F, and subtracting the one result from the other, we have

$$(\lambda_1-\lambda_2)\,\beta\, e_{ij} \in B.$$

Take $\lambda_1 \neq \lambda_2$, then we have

$$\beta\, e_{ij} \in B\,.$$

Repeating the operation of the form (1) on this element we obtain

$$\beta\, e_{kl} \in B\,, \qquad k \neq l\,.$$

In the same way we see that

$$\gamma\, e_{kl} \in C\,, \qquad k \neq l\,.$$

with $\gamma \neq 0$ in D. Since $\gamma\, e_{kl}$ commutes with every element of B, we should have

$$\gamma\, e_{kl} \cdot \beta\, e_{lk}=\beta\, e_{lk} \cdot \gamma\, e_{kl}\,,$$

but this implies

$$\gamma\, \beta\, e_{kk}=\beta\gamma\, e_{ll}\,.$$

This is not the case, since e_{kk} and e_{ll} are linearly independent over D. Thus it remains only the case $N(B)=F^*$.

b) Next, let A be a division algebra.

LEMMA 2. *Let B be a central simple algebra over F. Any normal subgroup B_1 of B^*, containing F^* and not identical with F^*, contains an F-basis (u_i), $i=1,\ldots\ldots, r$, of B such that none of u_i is contained in F^*.*

PROOF. We can find in B_1 an F-basis (v_i) of B by Corollary 1 to Theorem 1 in IS. Then $(b^{-1}v_i)$ is also a basis for any b in B_1. Thus, if every F-basis contained in B_1 has an element of F, every element b of B_1 is expressible in the form $b=v_\rho f$, $1\leqq\rho\leqq r$, $f\in F^*$, Then B_1/F^* should be a finite group, but this is not the case by the preceding Lemma.

We shall assume that $N(B)\neq F^*$. Let B_1 be the totality of b in B^* for which we can find a c in C^* such that bc is in $N(B)$; B_1 is a normal subgroup of B^*. By the above Lemma, we can take an F-basis (u_i), $i=1,\ldots\ldots, r$, of B such that $u_i\in B_1$, $u_i\notin F$, $i=1,\ldots\ldots, r$. For each u_i, take c_i in C^* such that $u_ic_i\in N(B)$. We shall fix for a moment two suffixes s and t for which $u_tu_s\neq u_su_t$. Let C_t be a commutative subfield $\supsetneqq F$ of C, containing the element c_t. If $c\in C_t$ and $c\notin F$, we can find α_j in F, $j=1,\ldots\ldots, r$, and c' in C^* such that

$$u_tc_t(u_s+c)=(u_s+c)\ (\sum_j u_j\alpha_j)\ c'. \tag{2}$$

Since (u_i) are linearly independent over C, (2) implies r equalities on c_t, c, c' with coefficients in F, i.e.

$$\gamma_{kts}\ c_t=(\sum_j \gamma_{ksj}\ \alpha_j+\alpha_k\ c)\ c', \qquad k\neq t, \tag{3_k}$$

$$(\gamma_{tts}+c)\ c_t=(\sum_j \gamma_{tsj}\ \alpha_j+\alpha_t\ c)\ c', \tag{3_t}$$

where γ's are determined by $u_iu_j=\sum u_k\gamma_{kij}$. If every α_k, $k\neq t$, is zero, we may suppose $\alpha_t=1$, and (3) are reduced to

$$\gamma_{kts}\ c_t=\gamma_{kst}\ c', \qquad k\neq t, \tag{3_k)'}$$

$$(\gamma_{tts}+c)\ c_t=(\gamma_{tst}+c)\ c'. \tag{3_t)'}$$

$c_t\ (c')^{-1}$ is in F by $(3_k)'$, and then we have $c_t=c'$ by $(3_t)'$, as we have assumed c $\notin F$. But this should lead to $u_tu_s=u_su_t$, against our assumption.

Thus one of α_k, say α_T, $T\neq t$, is not zero; by (3_k) we have

$$\left.\begin{aligned}\alpha_k&=\frac{\gamma_{kts}}{\gamma_{Tts}}\ \alpha_T\ ,\\ \gamma_{kts}\sum_j\gamma_{Tsj}\ \alpha_j&=\gamma_{Tts}\sum_j\gamma_{ksj}\ \alpha_j\ .\end{aligned}\right\}\ k\neq t. \tag{4_k}$$

Since $\alpha_k\neq 0$ is equivalent to $\gamma_{kts}\neq 0$, $\alpha_T\neq 0$ is always the case for

$c \in C_t$, $\notin F$. We may suppose $\alpha_T=1$, then (4_k) are linear equations in α_t with constant coefficients. On the other hand, in combining (3_T) with (3_t) we have a non-trivial quadratic equation in c whose coefficients are linear functions of α_t; since this equation is satisfied by many values for c in the commutative field C_t, α_t can not be unique. Hence the coefficients of α_t in (4_k) must be zero, and we have

$$(5_k) \qquad \gamma_{kts}\gamma_{Tst}=\gamma_{kst}\gamma_{Tts}, \qquad k \neq t.$$

If we change the rôle of u_s and u_t, we find that there is a suffix $S \neq s$, such that

$$(6_h) \qquad \gamma_{hrt}\gamma_{Sts}=\gamma_{hts}\gamma_{Sst}, \qquad h \neq s.$$

If $S \neq t$, then (6_t) together with (5_S) gives

$$(5_t) \qquad \gamma_{tts}\gamma_{Tst}=\gamma_{tst}\gamma_{Tts}\,.$$

If $S=t$, but $T \neq s$, (6_T) is the same as (5_t). Finally, is $S=t$, and $T=s$ then one of γ_{hts}, $h \neq s$, t, is not zero (for otherwise we should have $u_tu_s=\mu u_t+\nu u_s$, μ, $\nu \in F$, whence $1=\mu\, u_s^{-1}+\nu\, u_t^{-1}$, which would imply $u_tu_s=u_su_t$), and (5_t) follows from (5_h) and (6_h).

We have therefore obtained for any i, $j=1, \ldots\ldots, r$,

$$u_ju_i=u_iu_j\delta_{ij}, \qquad \delta_{ij} \in F^*.$$

But, from these formulas follows that one of u_i must be in F^* by the argument used in IS n°6. This contradicts our choice of (u_i), and Proposition 1 is completely proved.

COROLLARY. *[B] contains an infinite number of simple subalgebras, except for the cases $B=A$ and $B=F$.*

We shall assume in the following that *the characteristic of F is not two.* Let F^n be a vector space of dimension n over F, and f be a non-degenerate quadratic form on F^n. f determines a metric of F^n, and the orthogonal group $O_n(F, f)$ is defined as the set of all linear transformations conserving this metric. The subgroup of $O_n(F, f)$ of index 2 consisting of the transformations with the determinant 1 is called the rotation group $O_n^+(F, f)$. The matrix M of f with respect to a basis of F^n is a non-singular symmetric matrix; conversely any non-singular symmetric matrix M defines a non-degenerate quadratic

form f. The condition for a non-singular T to be in $O_n^+(F, f)$ is that

$$(7) \qquad {}^tTMT=M, \quad \textit{and} \ \det T=1.$$

Now, let A be a symmetric algebra of dimension n over F, then the underlying vector space of A is F^n. An inner automorphism $t\to sts^{-1}$ of A induces on F^n a linear transformation I_s, whose matrix is

$$I(s)=S(s){}^tR(s)^{-1},$$

where S and R denote the left and the right regular representations of A, respectively. Since we have a non-singular symmetric matrix M intertwining S with R, and since $S(s)$ commutes with ${}^tR(s)^{-1}$, the matrix $I(s)$ satisfies the condition (7) with this M. Hence the group $I(A)$ is represented in some rotation group.

Now, let A be a central simple algebra, and let an irreducible equation

$$(8) \qquad G(t)=0$$

of a degree >1 in F have a solution in A. (8) is equivalent to a system of n equations

$$(9) \qquad G_i\ (t_1, \ldots\ldots, t_n)=0, \ i=1, \ldots\ldots, n,$$

in n coordinates $t_1, \ldots\ldots, t_n$ of t. Let V_G be the variety in F^n determined by (9). Then I_s maps V_G onto V_G itself; and for any two points t and t' of V_G, there exists a rotation I_s mapping t onto t', since t and t' determine in A isomorphic subfields[8]. Thus we have by Proposition 1

PROPOSITION 3. *The group $I(A)$ is represented faithfully as a group of rotations of F^n, which operates transitively on V_G.*

§ 2. Orthogonal groups of three dimensions.

We shall consider the case of generalized quaternion algebras in detail. Let $a\neq 0$ and $b\neq 0$ be in F, and $A=(a, b)$ be a generalized quaternion algebra over F whose basis elements are u_0, u_1, u_2, u_3, and whose table of multiplication is determined by

$$u_0=1\,,\quad u_3=u_1u_2=-u_2u_1\,,$$
$$u_1^2=a\,,\quad u_2^2=b\,.$$

Any inner automorphism I_s of A leaves fixed the straight line $\{u_0\}$, and I_s is a rotation of the space $F^3=\{u_1, u_2, u_3\}$ orthogonal to $\{u_0\}$. The restriction of the metric of A to F^3 has the form

$$\bar{f}(t)=t^2=at_1^2+bt_2^2-abt_3^2\,, \tag{10}$$

where $t=u_1t_1+u_2t_2+u_3t_3$. If we denote by I_s' the restriction of I_s on F^3, then the mapping $I_s\to I_s'$ is an isomorphism of $I(A)$ into $O_3^+(F, \bar{f})$. We then prove

PROPOSITION 4. *$I(A)$ is isomorphic with $O_3^+(F, \bar{f})$.*

PROOF. Let V be the variety in F^3 determined by $t^2=a$; V is mapped onto itself by every rotation of F^3. We shall show that the group $I(A)$ is transitive on V. If t^2-a is irreducible in F, this follows from Proposition 3. If it is reducible, A is a matrix algebra of degree two over F; it is easy to see that the elementary divisors of $x-t$ (where x is an indeterminate) are independent of the choice of $t\in V$, and the elements of V are conjugate with each other under inner automorphisms. Hence we have only to prove that any transformation leaving fixed the point (1,0,0) on V is of the form I_s'. In $I(A)$ such transformations are induced by elements of the form $s=u_1+\alpha$, $\alpha\in F$, and corresponding matrices $I'(s)$ have the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & (\alpha^2+a)/d & 2\alpha a/d \\ 0 & 2\alpha/d & (\alpha^2+a)/d \end{pmatrix}, \tag{11}$$

where $d=\alpha^2-a$. On the other hand, let $T=(\alpha_{ij})$ be a rotation which leaves fixed the point (1,0,0). If $\alpha_{32}=0$, then T is the identity. If $\alpha_{32}\neq 0$, put

$$\alpha=(1+\alpha_{22})/\alpha_{32}\,,$$

then T has the form (11) in view of the condition (7), as desired.

Next, let an arbitrary non-degenerate ternary quadratic form

$$f=pt_1^2+qt_2^2+rt_3^2$$

be given, multiply the form f by $-r/pq$, and denote $a=-r/q$, $b=-r/p$, then we have the form (9), and $O_3^+(F, f)=O_3^+(F, \bar{f})$. Hence by Proposition 4 we have

PROPOSITION 5. *The rotation group $O_3^+(F, f)$ is isomorphic to $I(A)$, where $A=(a, b)=(-qr,-pr)$.*

COROLLARY. *In $O_3^+(F, f)$, every normal subgroup $\neq(1)$ has the centralizer* (1).

This follows from the Theorem 4 of IS.

If f is a null form, i.e. if f represents zero non-trivially, then the algebra A has an element t such that $t^2=0$, and A is a matrix algebra of degree two over F, and hence $O_3^+(F, f)$ is isomorphic to the projective general linear group $PGL(F, 2)$[9], and it is known that the commutator group of $O_3^+(F, f)$ is simple in this case.

If f is not a null form, A is a division algebra. In this case the structure of $O_3^+(F, f)$ is not known in general. Let the ground field F be an algebraic number field, then the form f remains definite on some $\mathfrak{p}$-adic extensions $F_\mathfrak{p}$ of F[10], and the group $O_3^+(F_\mathfrak{p}, f)$ for such $\mathfrak{p}$ is isomorphic to $A_\mathfrak{p}^* / F_\mathfrak{p}^*$, where $A_\mathfrak{p}=(a, b)_\mathfrak{p}$ is a division algebra over $F_\mathfrak{p}$ If F has furthermore at most one real infinite prime, this is the case for a finite prime $\mathfrak{p}$, since there are at least two primes where A does not split[11]. Then, let π be a prime element of $F_\mathfrak{p}$, Π that of $A_\mathfrak{p}$ such that $\Pi^2=\pi$, and R a complete system of representatives of the residue class field of $A_\mathfrak{p}$; then every element t of $A_\mathfrak{p}$ is expanded in the form

$$t=\sum_{i=h}^{\infty} \tau_i \Pi^i, \quad \tau_i \in R, \quad \tau_h \not\equiv 0 \pmod{\pi}.$$

Let E_0 be the group of all units, i.e. elements for which $h=0$ and E_k be the subgroup of E_0 consisting of units congruent to 1 mod. Π^k, $k=1, 2, \ldots\ldots$[12]. Let N'_k be the subgroup of $O_3^+(F_\mathfrak{p}, f)$ corresponding to $E_k \cdot F_\mathfrak{p}^* / F_\mathfrak{p}^*$ under the isomorphism mentioned above; N'_k, $k=0, 1, 2, \ldots\ldots$are normal subgroups of $O_3^+(F_\mathfrak{p}, f)$ such that i) $N'_0 \geq N'_1 \geq \ldots\ldots$ ii) factor groups O^+/N'_0 and N'_k/N'_{k+1}, $k=0, 1, 2, \ldots\ldots$are abelian and iii) $\cap N'_k=(1)$.

Now, $O_3^+(F, f)$ may be considered as a subgroup of $O_3^+(F_\mathfrak{p}, f)$, and $N_k=N'_k \cap O_3^+(F, f)$ is a normal subgroup of $O_3^+(F, f)$. Since $O_3^+(F, f)$ is not solvable by Corollary to Proposition 5, we have

actually an infinite number of distinct N_k on account of the condition i), ii), iii) above. Thus we have proved

PROPOSITION 6[5]. *Let F be an algebraic number field having at most one real infinite prime, and f a ternary quadratic form on F. If f is not a null form, then the rotation group $O_3^+(F, f)$ has an infinite sequence of normal subgroups N_i, $i=1, 2, \ldots\ldots$, such that* i) $O^+ \supset N_1 \supset N_2 \supset \cdots\cdots$, ii) O^+/N_1, N_1/N_2, $\ldots\ldots$, *are all abelian and* iii) $\cap N_i=(1)$.

Remark. J. Dieudonné proposed an interesting problem: whether the principle of ((passage from local to global)) of H. Hasse is also true for orthogonal groups?[5] Since we have seen that the commutator group of $O_3^+(F, f)$ is simple if and only if the algebra $A=(-qr,-pr)$ is a matrix algebra, this problem is answered in affirmative in the three dimensional case for the field having the above property; for example, the rational number field Q, the field $Q(e^{2\pi i/n})$, and the imaginary Galois extensions of Q in general, etc.

§ 3. Impossibility of finding another rotation groups.

Let A be a non-commutative algebra over F with the identity 1, and let the center Z of A be non-isotropic[13] with respect to a non-degenerate quadratic form f. We shall denote by B the orthogonal complement of Z in A. Our aim is to determine the structure of algebras satisfying the following condition:

(R) *Every rotation of B with respect to f is induced by an inner automorphism of A*; that is, if u is a rotation of B there exists a regular element t of A such that $u(x)=txt^{-1}$ for every x in B.

Let A satisfy this condition. If B is of an even dimension, then the symmetry of A with respect to Z induces a rotation on B; by the condition (R) we have a regular element t of A such that $tbt^{-1}=-b$, $b \in B$. Since $ttt^{-1}=t$, we have $t \in Z$, but this is evidently not the case. Hence B *has an odd dimension*; in particular B has at least three dimensions.

First, we shall assume that A satisfies the following condition:

(r) *B contains a regular element.*

Let b be such a regular element, U be a non-isotropic subspace of

B of dimension two containing the vector b[14], and V its orthogonal complement. There exists a regular element $a \in A$ which induces the symmetry of B with respect to V; then, since the elements vb of Vb are transformed into $-vb$ by a, we have $Vb \leq U$, hence it holds that

$$\dim V = \dim Vb \leqq \dim U = 2 .$$

Since, on the other hand, V contains Z and a where $a \notin Z$, it follows that dim $V=2$, $V=\{1, a\}$, and $U=Vb=\{b, ab\}$. We have moreover
i) $ab=-ba$, by the definition of a,
ii) $a^2=\alpha \neq 0$ is in F, since a^2 commutes with every element of A, and
iii) $b^2=\beta \neq 0$ is in F, since b^2 commutes with both a and b.
Hence it is proved that *A is a generalized quaternion algebra.*

Next, we assume that B contains no regular element. Let b be a non-isotropic vector of B, and let a regular element t induce the symmetry of B with respect to the straight line $\{b\}$; then $Z+\{b\}$ is the ring consisting of elements of A which commute with t. Put $b^2=z_0+\beta b$, $z_0 \in Z$, $\beta \in F$; there is a rotation u such that $u(b)=-b$, and u leaves fixed the vector b^2-z_0, hence we must have $b^2=z_0 \in Z$. Since t is in $Z+\{b\}$, we may suppose that $t=z_1+b$, $z_1 \in Z$; from the fact $t^2 \in Z$, we see immediately $z_1 b=0$, whence we have $z_0=tb \neq 0$ and $z_1 t=z_1^2 \in Z$. Let U be the orthogonal complement of $\{b\}$ in B, and u be any vector of U, then we have by the definition of t that

$$z_1 t u=-z_1 u t=-u z_1 t$$

$$=z_1^2 u=u z_1^2=u z_1 t .$$

It follows that $u z_1 t=0$; since t is regular we have $u z_1=0$. Thus, combining with $z_1 b=0$, we see that

$$z_1 B=0 . \tag{12}$$

Now, let b_i, $i=1, 2,\ldots\ldots$ be an orthogonal basis of B, then $b_i^2 \neq 0$ is in Z, and $b_i b_j$, $i \neq j$, is in B. Let A_1 be the left annihilator of B in A, which is not the zero ideal by (12), and $s=z+\sum \beta_i b_i$, $z \in Z$ be an element of A_1; then we have

$$z b_j+\sum \beta_i b_i b_j=0 , \quad j=1, 2,\ldots\ldots ,$$

which implies that the element $\beta_j b_j^2$ of Z is written an the sum of

the elements of B, hence we have $\beta_j b_j^2=0$, so that $\beta_j=0$, $j=1,2,\ldots\ldots$. Thus we have seen that $s=z$ is in Z, and A_1 ($\leq Z$) is a two-sided ideal of A.

Let A_2 be the annihilator of A_1 in A. Since the regular element t has the decomposition $t=z_1+b$, $z_1\in A_1$, $b\in B\leq A_2$, we see that

i) $A_1\cap A_2=(0)$, since $x\in A_1\cap A_2$ annihilates t,

ii) A is the direct sum of A_1 and A_2, since every $y\in A$ is written as $y=z_1t^{-1}y+bt^{-1}y$, $z_1t^{-1}y\in A_1$ $bt^{-1}y\in A_2$, and

iii) b is regular in A_2, since b is the A_2-component of t.

It is evident that the center Z_2 of A_2, being the intersection $Z\cap A_2$, is the orthogonal complement of B in A_2. Thus, the algebra A_2 satisfies the condition (r), and is therefore a generalized quaternion algebra.

Conversely, let A_1 be an arbitrary commutative algebra with an identity and A_2 be a generalized quaternion algebra, then $A=A_1+A_2$ satisfies the condition (R) by Proposition 4. Thus, we have proved

PROPOSITION 7[15]. *An algebra A satisfies the condition* (R) *if and only if A is a direct sum of a generalized quaternion algebra and a commutative algebra with an identity.*

Mathematical Institute
University of Tokyo.

Notes and References.

1) Cf. M. Abe, Projective transformation groups over non-commutative fields, Sijo-Sugaku-Danwakai. **240** (1942) (in Japanese).
J. Dieudonné, Les déterminants sur un corps non-commutatif, Bull. Soc. Math. Fr. vol. **71** (1943).

2) "In a division algebra A, the only subalgebras invariant under every inner automorphism are the whole A and the center of A." This theorem was extended to any sfield and was simply proved by R. Brauer and L. K. Hua. See, for example: R. Brauer, On a theorem of H. Cartan, Bull. Amer. Math. Soc. vol. **55** (1949), pp. 619-620.

3) A. Hattori, On invariant subrings, Japanese Journ. of Math. vol. 21 (1951), pp. 121-129. This paper is referred to as IS in this paper.

4) B. L. van der Waerden, Gruppen von linearen Transformationen, Ergebnisse, (1935), p. 27.

5) J. Dieudonné, Sur les groupes classiques, Act. Sci. et Ind., **1040**, (1948), n°15 and n°16.

6) In the whole of this paper, we shall assume that the identity of every simple subalgebra considered is the same as the identity of A.
7) See Abe, loc. cit.; cf. also the proof of Theorem 1 of IS.
8) Cf. Artin, Nesbitt and Thrall, Rings with minimum condition, (1944), p. 66.
9) This fact has been proved in another way. See van der Waerden, loc. cit.
10) A theorem due to H. Hasse. See:
E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, Crelle's Journal, vol. 176 (1937), pp. 31-44. Satz 19.
11) As is well known, this follows from the sum-relation between $\mathfrak{p}$-invariants of A.
12) Cf. T. Nakayama and Y. Matsushima, Über die multiplikative Gruppe einer $\mathfrak{p}$-adischen Divisionsalgebra, Proc. Imp. Acad. Jap. vol. 19 (1944), pp. 622-628.
13) A subspace E is called non-isotropic if the restriction of f on E is non-degenerate, and a vector v is called non-isotropic if the straight line $\{v\}$ is non-isotropic. See, for example, J. Dieudonné, loc. cit.
14) If b is non-isotropic, take a non-isotropic c from the orthogonal complement of $\{b\}$, if b is isotropic, take a vector c not orthogonal to b, then $U=\{b, c\}$ is the desired one.
15) After leading the first manuscript of this paper which had been consisting of §§ 1 and 2 of the present paper, Mr. N. Iwahori informed to the author the following result: Let A be an algebra over the real number field with the center Z, and assume that the group of inner automorphisms of A gives rise to the whole rotation group of the real vector space A/Z, then A/Z has the dimension three. Our Proposition 7 was obtained in generalizing this result. Mr. N. Iwabori found a proof of this proposition, in case of characteristic zero, by a completely different argument.