Journal of the Mathematical Society of Japan Vol. 6, Nos. 3~4, December, 1954

On the multiplicative group of simple algebras.

By Goro TOYODA and Akira HATTORI

(Received Nov. 12, 1953)

Let A be a central simple algebra of finite dimension over a commutative field F which contains an infinite number of elements. Let B be a subalgebra of A different from both A and F. A subalgebra B' is called *conjugate* to B if there exists a regular element t of A such that $B'=tBt^{-1}$. If we denote by $[B]$ the totality of subalgebras of A conjugate to B, the multiplicative group A^* of regular elements of A may be regarded as a transitive group of substitutions on $[B]$ in a natural manner, and every element of the subgroup F^* of A^* (the multiplicative group of regular elements of F) gives rise to the identity substitution. Now, we have

THEOREM. *F^* is precisely the kernel of the representation of A^* as a group of substitutions on $[B]$.*

This was proved previously by one of the writers in case where B is a simple subalgebra of A, and was applied to the structure-problem of the three dimensional rotation groups [3]. Our aim in the present paper is to show that the theorem is valid in the general form as above, and can be proved in even simpler way than in [3].

§1. We need a simple lemma on Kronecker product.

LEMMA. *Let B and C $(\neq F)$ be algebras with identity over F, and $A=B\times C$ their Kronecker product over F. If $t=b+c$ $(b\in B,\ c\in C,\ c\notin F)$ is a regular element of A, we have $B\cap tBt^{-1}=V_B(b)$, where $V_B(b)$ denotes the set of all elements of B commutable with b.*

PROOF. If $x\in tBt^{-1}$, there exists $y\in B$ such that $(b+c)y=x(b+c)$, or equivalently, $(by-xb)\cdot 1=(x-y)c$. If, further, $x\in B$, we have $by=xb$ as well as $x=y$ in virtue of the linear disjointness of B and C over F. Hence $x\in V_B(b)$, i.e. $B\cap tBt^{-1}\subseteq V_B(b)$. Conversely, it is easily verified that $V_B(b)\subseteq B\cap tBt^{-1}$.

Now we proceed to the proof of the theorem. Let $N(B)$ be the totality of those regular elements of A which give rise to the identity substitution on $[B]$, then $N(B)$ is a normal subgroup of A^*. We shall show $N(B)=F^*$, which is just the assertion of the theorem. Set $B'=V_A(B)$, then we have $N(B)\leqq N(B')$, and B' contains the identity of A. Hence we may, and shall, suppose that B itself contains the identity of A.

First, we consider the case where A is a division algebra. Then B is also a division algebra whose center Z is a commutative field over F, and we have obviously $N(Z)\geqq N(B)$. Since the fact $N(Z)=F^*$ is easily proved for such a subfield $Z\subset A$ provided $Z\neq F$, as was shown in [3] (p. 207), we shall only consider here the case where B is also a central division algebra over F. Let $V_A(B)=C$, then $C\neq F$ and $A=B\times_F C$. Let b be an arbitrary element of B not contained in F, then $t=b+c$ is obviously regular for any non-scaler $c\in C$. Hence we have $B\frown tBt^{-1}=V_B(b)$ by the above lemma. Let K be the center of $V_B(b)$, then we have $N(B)\leqq N(V_B(b))\leqq N(K)$. Since K is a commutative field essentially containing $F(K\geqq F(b)\supset F)$, we have $N(K)=F^*$ as is remarked above, and a fortiori $N(B)=F^*$.

Next, let A be not a division algebra. Let S be the commutator subgroup of A, then the factor group $S/(S\frown F^*)$ is a simple group [1]. Thus, if $N(B)\neq F^*$, it follows $N(B)\geqq S$ by [2] Theorem 4. Hence $S\frown B^*$ is a normal subgroup of S. If $S\frown B^*=S$, i. e. if $B^*\geqq S$, we have $B=A$ (see [2] Corollary 1 to Theorem 1), which, however, contradicts our first assumption $B\neq A$. $S\frown B^*\leqq F^*$. Let b be an arbitrary element of B fixed for a moment; then for $t\in N(B)$, we have $tbt^{-1}b^{-1}=\tau\in F^*$. The mapping $t\rightarrow\tau$ is a homomorphism of $N(B)$ into an abelian group. Since S is the commutator group of $N(B)$ as well, we have $\tau=1$ for $t\in S$, which means that every $b\in B^*$ commutes with every element of S. Since B^* and S generate B and A respectively, this, in turn, means $B=F$, which is also excluded at the beginning. Hence we have always $N(B)=F^*$, and the theorem is proved.

§ 2. We shall add an immediate consequence of the lemma used in § 1. Namely:

PROPOSITION. *Let F, A, B, C be as in the lemma, and suppose that the following condition (C) holds:*

(C) *For every $b\in B$ there exists a non-scaler $c\in C$ such that $b+c$ is regular inA.*

If, under this condition, a subalgebra B' of B is a commuter algebra $V(B'')$ in B of a certain subalgebra B'' of B, then B' is an intersection of subalgebra of A conjugate to B under the inner automorphisms of A.

PROOF. Suppose $B'=V_B(B'')$. Take a generator system $\{b_\alpha\}$ of B'', and select, for each b_α, a regular element $t_\alpha=b_\alpha+c_\alpha$, where $c_\alpha\in C$, $\notin F$. Then, by the lemma, we have certainly:

$$B\cap(\bigcap_\alpha t_\alpha Bt_\alpha^{-1})=\bigcap_\alpha(B\cap t_\alpha Bt_\alpha^{-1})=\bigcap_\alpha V_B(b_\alpha)=V_B(B'')=B'.$$

If B'' is of finite dimension over F, we may take an F-basis of B'' as a generator system. Hence B' is represented, in this case, as an intersection of a finite number of conjugate subalgebras.

The condition (C) is satisfied in the following cases for instance:

i) *A satisfies the ascending chain condition for right dieals, and every non-zero-divisor of A is a regular element.*

For, let a be an element of A. The left multiplication by a is a linear transformation of the underlying vector space of A over F. Let $\{\lambda_\nu;\nu\in N\}$ be the set of all eigenvalues of this linear transformation, and $E(\lambda_\nu)$ the space of eigenvectors belonging to λ_ν. Then every $E(\lambda_\nu)$ is a right ideal of A, and the sum $\bigcup_\nu E(\lambda_\nu)$ is direct. Hence N must be a finite set in view of the ascending chain condition. It follows that there exists $\mu\in F$ such that $a+\mu$ is a non-zero-divisor, since the field F is not a finite field. By assumption, $a+\mu$ is then a regular element of A. Thus, if $b\in B$ is given, take a non-scaler $c\in C$, then $b+(c+\mu)$ is regular with some $\mu\in F$.

ii) *A is an algebraic algebra over F.*

In this case, an element a of A satisfies an algebraic equation $f(x)=0$, say, over F. If λ is an eigenvalue of the left multiplication by a, $\lambda\in F$ satisfies also $f(\lambda)=0$. Obviously the number of such λ's is finite, and we can argue quite similarly as above, since a non-zero-divisor of A is certainly a regular element in this case.

Tateno High School and
University of Tokyo.

References

[1] J. DIEUDONNÉ, *Les déterminants sur un corps non-commutatif*, Bull. Soc. Math. France, vol. 71 (1943).

[2] A. HATTORI, *On invariant subrings*, Japanese Journ. of Math. vol. 21 (1951), pp. 121-129.

[3] A. HATTORI, *On the multiplicative group of simple algebras and orthogonal groups of three dimensions*, Journ. of Math. Soc. Japan, vol. 4 (1952), pp. 205-217.