ON THE AUTOMORPHISM RING OF DIVISION ALGEBRAS

BY SHIGEMOTO ASANO

1. Introduction.

Let A be an (associative) ring with an identity 1 and S a subring of A containing 1. Suppose S is Galois in A in the sense that $I(H(S))=S$, where $H(S)$ is the group of all automorphisms of A leaving S elementwise invariant (i.e. the Galois group of A over S and $I(H(S))$ is the set of all elements of A invariant under every automorphism of $H(S)$.[1] The Galois group $\mathfrak{G}=H(S)$ and the set S_R of right multiplications by elements of S generate a subring $\mathfrak{R}=\mathfrak{G}S_R=S_R\mathfrak{G}$ of the ring $\mathfrak{E}$ of S-endomorphisms of A as an S-left module. The ring $\mathfrak{R}$ is called the *automorphism ring* of A over S.

In a series of papers [7—9], Kasch investigated the properties of $\mathfrak{R}$ and of A as an $\mathfrak{R}$-module, assuming mostly that A is a simple ring satisfying minimum condition for right ideals (a division ring, in particular) and that S is a Galois subring of A such that $[A: S]<\infty$.[2] The main problem he discussed was: Under what conditions $\mathfrak{R}$ and A are isomorphic as $\mathfrak{R}$-modules? The problem is related to the normal basis theorem and to this he gave a quite satisfactory answer ([7]).[3] Also, he started the study of the structure of $\mathfrak{R}$ and of A as an $\mathfrak{R}$-module.[4] In this direction, he obtained the following remarkable result ([9]).

Let $A=Z_m$ be the total matrix algebra over a commutative field Z of degree $m>1$ and $\mathfrak{G}$ the group of all inner automorphisms of A (i.e. the Galois group of A over Z). Suppose that Z is not the prime field of characteristic 2 and that the degree m is not divisible by the characteristic of Z. If $\mathfrak{R}=\mathfrak{G}Z_R=\mathfrak{G}Z$ is the automorphism ring of A over Z then:

(a) A is completely reducible as $\mathfrak{R}$-module and has a (unique) direct sum decomposition $A=Z\oplus B$, where $B=[A, A]$ is the submodule of A generated by (additive) commutators $[a_1, a_2]=a_1a_2-a_2a_1$, $a_1, a_2\in A$.

(b) $\mathfrak{R}$ induces all linear transformations of B over Z.

(c) $\mathfrak{R}$ is semi-simple and moreover is expressible as the direct sum of Z and Z_{m^2-1}, the total matrix algebra of degree m^2-1 over Z; hence $[\mathfrak{R}: Z]=(m^2-1)^2+1$.

Received April 2, 1966.

1) Cf. Jacobson [5], Chapters 6–7.

2) In the case of simple A, we have to add some other conditions to the definition of Galois subrings. (The definition that we mentioned above is, in this case, too general.)

3) A supplementary result was obtained by Nagahara-Onodera-Tominaga [10].

4) Concerning this problem, only preliminary results have been obtained.

In the present note we shall show that the same statements remain valid in case when A is an arbitrary finite dimensional central simple algebra over Z.

2. The case of central division algebras.

Let D be a division algebra over its center Z such that $[D: Z]=n=s^2<\infty$. Then D is Galois over Z and the Galois group $\mathfrak{G}$ is the totality of all inner automorphisms of D. As in the introduction we set $\mathfrak{R}=\mathfrak{G}Z_R=\mathfrak{G}Z$ (the automorphism ring of D over Z) and $B=[D, D]$ (the submodule of D generated by all $[a_1, a_2]=a_1a_2-a_2a_1$, $a_1, a_2 \in D$). Clearly D is an $\mathfrak{R}$-(right) module. As usual, we shall denote the inner automorphism by a non-zero element a of D as I_a: $xI_a=axa^{-1}$, $x\in D$. If U is a submodule of D then U is an $\mathfrak{R}$-submodule if and only if U is an invariant Z-subspace of D, i.e. $UZ=U$ and $UI_a=U$ for all non-zero a of D. The discussion of the case $D=Z$ is trivial; so we shall assume D is non-commutative.

Recently we have proved that the only invariant subspaces of D are $0, Z, B=[D, D]$ and D ([3], Theorem 4). Moreover, $[B: Z]=n-1$ and $Z\subseteq B$ if and only if the characteristic of the base field Z is a factor of n. Thus we have the following

PROPOSITION 1. *Let D be a finite dimensional central division algebra over Z and let $\mathfrak{R}$ be the automorphism ring. Then Z and $B=[D, D]$ are the only non-trivial $\mathfrak{R}$-submodules of D. Moreover, $Z\nsubseteq B$ if and only if the characteristic of Z does not divide $[D: Z]$. And, when that is so, D is decomposed into a (unique) direct sum of irreducible $\mathfrak{R}$-submodules Z and B: $D=Z\oplus B$.*

Now we consider the irreducible $\mathfrak{R}$-module B; we wish to prove that *the centralizer*[5] *of B as an $\mathfrak{R}$-module is Z*, namely, that *every $\mathfrak{R}$-endomorphism of B is realized by the (left) multiplication by a suitable element of Z.* The proof will be carried out in several steps.

(1) Let σ be an $\mathfrak{R}$-endomorphism of B; we may assume $\sigma\neq 0$. Since $Z_R\subseteq\mathfrak{R}$ σ is a linear transformation of B over Z. By Schur's lemma σ is moreover a Z-isomorphism of B onto itself. Now let x be an element of B; let y be a non-zero element of D such that $xy=yx$. Then we have $x\sigma-(x\sigma)I_y=x\sigma-(xI_y)\sigma=(x-xI_y)\sigma=0$,[6] i.e. $(x\sigma)y=y(x\sigma)$. Hence $V_D(x)\subseteq V_D(x\sigma)$.[7] By symmetry $V_D(x)\supseteq V_D(x\sigma)$. *Thus $V_D(x)=V_D(x\sigma)$. This implies in particular that $x\sigma$ commutes with x.*

(2) Suppose a is an element of D such that $Z(a)$ is a separable maximal subfield of D. We recall that D is uniquely decomposed into a direct sum $D=Z(a)\oplus B(a)$, as a $(Z(a), Z(a))$-module. $B(a)$ is contained in $B=[D, D]$ and is expressible as $B(a)=[a, D]$ $(=\{ax-xa;\ x\in D\})$; furthermore, the minimal submodule of D containing all such $B(a)$ coincides with B. ([3], Theorem 5.) *We assert that σ, when contracted to $B(a)$, gives a $(Z(a), Z(a))$-endomorphism of $B(a)$ onto itself.*

5) Cf. Jacobson [5], p. 24.
6) We write the image of x under the mapping σ as $x\sigma$, etc.
7) If S is a subset of D, we denote the set $\{y\in D;\ ys=sy$ for all $s\in S\}$ by $V_D(S)$.

To see this suppose a is as above and x is in B. Then from the identity (B_2) in [3] we have

$$\xi^{-1}(xI_{a+\xi}-xI_a)=(x-xI_a)(a+\xi)^{-1},$$

where ξ is an arbitrary non-zero element of Z.[8] Similarly $\xi^{-1}((x\sigma)I_{a+\xi}-(x\sigma)I_a)=(x\sigma-(x\sigma)I_a)(a+\xi)^{-1}$, so that

$$\xi^{-1}(xI_{a+\xi}-xI_a)\sigma=((x-xI_a)\sigma)(a+\xi)^{-1}.$$

Hence $((x-xI_a)(a+\xi)^{-1})\sigma=((x-xI_a)\sigma)(a+\xi)^{-1}$. Now let c be an element of $Z(a)$. As we remarked in the proof of [3], Proposition 3, we may write $c=\sum_{i=1}^{s}(a+\xi_i)^{-1}\gamma_i$ where γ_i are in Z and ξ_i are s distinct non-zero elements of Z.[9] Since σ is a linear transformation of B over Z, this implies

$$((x-xI_a)c)\sigma=((x-xI_a)\sigma)c.$$

We have noted that $B(a)=[a, D]$; it is clear that $[a, D]$ is the totality of elements of the form $d-dI_a$, $d\in D$. But in view of the decomposition $D=Z(a)\oplus B(a)$ we may restrict the elements d to those of B. Consequently, the contraction of σ to $B(a)$ is a $Z(a)$-endomorphism of $B(a)$ as a right $Z(a)$-module. By symmetry this is also true for left-hand side operators.

(3) Next let b be a non-zero element of $B(a)$. Then $(ba)\sigma=(b\sigma)a$ by what we have just seen. From (1) it follows that $(b\sigma)a$ and ba are commutative: $(b\sigma)aba=ba(b\sigma)a$, hence $(b\sigma)ab=ba(b\sigma)$. This implies $b^{-1}(b\sigma)a=a(b\sigma)b^{-1}=ab^{-1}(b\sigma)$ (observe that $b\sigma$ commutes with b^{-1}), and so $b^{-1}(b\sigma)\in V_D(a)=Z(a)$. Also, $b^{-1}(b\sigma)\in V_D(b)$. Thus *$b^{-1}(b\sigma)$ lies in $Z(a)\frown V_D(b)$ for every non-zero $b\in B(a)$.*

(4) It is known that there exists a conjugate a' of a in D (in the sense that $a'=aI_y$) such that $D=Z(a, a')$. (See Jacobson [5], p. 182. Cf. also Albert [2], Kasch [6].) We decompose a' according to the decomposition $D=Z(a)\oplus B(a)$: $a'=a''+b$. Then clearly $b\notin Z$ and $D=Z(a, b)$. By (3) this implies that $b^{-1}(b\sigma)$ is an element α of Z: $b^{-1}(b\sigma)=\alpha\in Z$, i.e. $b\sigma=\alpha b$. Hence *$(bI_d)\sigma=(b\sigma)I_d=\alpha(bI_d)$ for any non-zero d of D.* Since B has a basis $\{bI_{d_i};\ d_i\in D,\ 1\leqq i\leqq n-1\}$ over Z, this proves the result: $x\sigma=\alpha x$ for all $x\in B$.

From the fact we have proved above it follows that *the automorphism ring $\mathfrak{R}$ induces the complete ring of linear transformations of B over Z.*[10] Now *we assume that the characteristic of Z does not divide n.* Then by Proposition 1 D is decomposed as $D=Z\oplus B$ (as an $\mathfrak{R}$-module). We have therefore the inequalities: $[\mathfrak{R}: Z]\geqq(n-1)^2$ and $[\mathfrak{R}: Z]\leqq(n-1)^2+1$. If $[\mathfrak{R}: Z]=(n-1)^2$, $\mathfrak{R}$ is simple and isomorphic to Z_{n-1}, the total matrix algebra of degree $n-1$ over Z. But $\mathfrak{R}$ is contained in the Z-endomorphism ring of D, which is isomorphic to Z_n. Since $Z=Z_R\subseteq\mathfrak{R}$ and

8) Cf. also Brauer [4].

9) Observe that Z is an infinite field since we have assumed $D\neq Z$.

10) See for instance Jacobson [5], Chapter 2.

$((n-1)^2, n)=1$, this is a contradiction.[11] Hence we must have $[\mathfrak{R}: Z]=(n-1)^2+1$. It is now easy to see that $\mathfrak{R}$ *is semi-simple and is isomorphic to the direct sum* $Z\oplus Z_{n-1}$.[12]

3. The case of central simple algebras. Conclusion.

Let A be a finite dimensional central simple algebra over Z. It is well known that A is (isomorphic to) the ring of all (say) $m\times m$ matrices with coefficients taken from a central division algebra D over Z. We set $[D: Z]=s^2$, so that $n=[A: Z]=m^2s^2$. The case $s=1$ and the case $m=1$ have been discussed in Kasch's [9] and in the previous section, respectively. We shall therefore assume $s>1$ and $m>1$. Let $\mathfrak{G}$ be the group of all inner automorphisms of $A=D_m$ by regular elements of A (the Galois group of A over Z), and $\mathfrak{R}=\mathfrak{G}Z$ the automorphism ring. As before, we set $B=[A, A]$, the submodule of A generated by all $[a_1, a_2]=a_1a_2-a_2a_1$, $a_1, a_2\in A$. Observe that B is generated by the set $\{Dd_{ij}, i\neq j;\ D(d_{ii}-d_{jj});\ [k_1, k_2]d_{ii}, k_1, k_2\in D\}$, where $d_{ij}(1\leqq i, j\leqq m)$ are the matrix units of A.

We now state, corresponding to Proposition 1, the following

PROPOSITION 2. *Let $A=D_m$ be the matrix ring of degree $m>1$ over D, which is a central division algebra over Z such that $[D: Z]=s^2>1$. Suppose $\mathfrak{R}$ be the automorphism ring of A over Z. Then Z and $B=[A, A]$ are the only non-trivial $\mathfrak{R}$-submodules of A; moreover, $Z\subseteq B$ if and only if the characteristic p of Z is a divisor of $n=[A: Z]=m^2s^2$. If p does not divide n then A has a unique decomposition $A=Z\oplus B$ as an $\mathfrak{R}$-module.*

Proof. We first note that a submodule U of A is an $\mathfrak{R}$-submodule if and only if it is a Z-subspace and invariant relative to all inner automorphisms of A. It follows that for every $\mathfrak{R}$-submodule U of A we have either $U=Z$ or $U\supseteq B$ (Kasch [8]). On the other hand, B is maximal as Z-subspace, i.e. $[B: Z]=n-1$, as is easily seen. Hence Z and B are the only non-trivial $\mathfrak{R}$-submodules. To see the second assertion on the condition of $Z\subseteq B$, suppose Ω be a splitting field of A over Z. Then $A_\Omega=A\otimes_Z\Omega\cong\Omega_{ms}$. Clearly $Z\subseteq B$ if and only if $\Omega\subseteq B_\Omega=[A_\Omega, A_\Omega]$, which is equivalent to the condition that p divides $n=m^2s^2$ by Kasch [9]. The last assertion follows immediately from what we have seen.

Next we consider the $\mathfrak{R}$-submodule B of A under the assumption that the characteristic p of Z does not divide n. Then, by virtue of our discussion in the previous section, we have the following result: $\mathfrak{R}$-*induces the complete ring of linear transformations of B over Z.* The proof of this fact can be performed, as Kasch remarked, quite similarly as that of [9], Hilfssatz, although the details becomes somewhat complicated. As in the last section this implies that $\mathfrak{R}$ *is semi-simple and isomorphic to* $Z\oplus Z_{n-1}$.

11) See for example Albert [1], Chapter 4.

12) The arguement of these several lines is the same as in Kasch [9], p. 61.

We have thus completed the proof of the following main theorem.

THEOREM. *Let A be a finite dimensional central simple algebra over a field Z, n its dimensionality: $[A: Z]=n$, and $\mathfrak{G}$ the group of all inner automorphisms of A over Z. Let $\mathfrak{R}$ be the automorphism ring of A over Z: $\mathfrak{R}=\mathfrak{G}Z$. Suppose that Z is not the prime field of characteristic* 2 *and that the characteristic of Z is not a factor of n. Then* (a) *A is completely reducible as $\mathfrak{R}$-module and is decomposed as $A=Z\oplus B$, where Z and $B=[A, A]$ are uniquely determined irreducible $\mathfrak{R}$-submodules;* (b) *$\mathfrak{R}$ induces the complete ring of linear transformations of B over Z; and* (c) *$\mathfrak{R}$ is semi-simple and is isomorphic to the direct sum $Z\oplus Z_{n-1}$, and hence* $[\mathfrak{R}: Z]=(n-1)^2+1$.

REFERENCES

[1] ALBERT, A, A., Structure of algebras. Amer. Math. Soc. Coll. Publ. **24** (1939).

[2] ———, Two element generation of a separable algebra. Bull. Amer. Math. Soc. **50** (1944), 786–788.

[3] ASANO, S., On invariant subspaces of division algebras. Kōdai Math. Sem. Rep. **18** (1966), 322–334.

[4] BRAUER, R., On a theorem of H. Cartan. Bull. Amer. Math. Soc. **55** (1949) 619–620.

[5] JACOBSON, N., Structure of rings. Amer. Math. Soc. Coll. Publ. **37** (1956).

[6] KASCH, F., Über den Satz vom primitiven Element bei Schiefkörpern. J. reine angew. Math. **189** (1951), 150–159.

[7] ———, Über den Endomorphismenring eines Vektorraumes und den Satz von der Normalbasis. Math. Ann. **126** (1953), 447–463.

[8] ———, Invariante Untermoduln des Endomorphismenrings eines Vektorraums. Arch. Math. **4** (1953), 182–190.

[9] ———, Über den Automorphismenring einfacher Algebren. Arch. Math. **6** (1955), 59–65.

[10] NAGAHARA, T., T. ONODERA, AND H. TOMINAGA, On normal basis theorem and strictly Galois extensions. Math. J. Okayama Univ. **8** (1958), 133–142.

DEPARTMENT OF MATHEMATICS,
TOKYO INSTITUTE OF TECHNOLOGY.