ON INVARIANT SUBSPACES OF DIVISION ALGEBRAS

By Shigemoto Asano

1. Introduction.

The well known Cartan-Brauer-Hua theorem states that if a division subring Δ of a division ring D with center Z is invariant relative to all inner automorphisms (in short, *invariant*), then either $\Delta=D$ or $\Delta\subseteq Z$ (see for instance [16], p. 186). Relating to this theorem, Hattori [10] proved: If T is an invariant subring of a (not necessarily finite dimensional) simple algebra A over a field Φ satisfying the minimum condition for left ideals, then either $T=A$ or $T\subseteq Z$, Z being the center of A, with one exception (the case when A is a matrix ring of degree 2 over $Z=GF(2)$). Similar (but somewhat more general) results were obtained by Kasch [19] independently. Namely, he proved that if U is an invariant submodule of the ring A of all linear transformations of a left vector space V over a division ring D with center Z, then either $U\subseteq Z$[1] or $B\subseteq U$, where B=the submodule generated by $\{De_{ij},\ i\neq j;\ D(e_{ii}-e_{jj});\ [d_1, d_2]e_{ii},\ d_1, d_2\in D\}$. Here, it is assumed that the left dimension $[V:D]_L$ of V over D is not 1, and not both $[V:D]=2$ and $D=GF(2)$; $e_{ij}(i, j=1, 2, \cdots)$ is an element of A which maps u_i to u_j and other u_k to 0, $u_i(i=1, 2, \cdots)$ being a basis of V over D; and finally, $[d_1, d_2]$ denotes the commutator $d_1d_2-d_2d_1$. From this he derived, in the case when $n=[V:D]_L<\infty$, the same result on invariant subrings as Hattori's.

These results have been further generalized by a number of authors ([2], [5], [13], [21]). In particular, Amitsur [2] showed that if A is a simple algebra with center Z over a field $\Phi\neq GF(2)$, containing an idempotent$\neq 1$ and A is not a 4-dimensional algebra over a field of characteristic 2, then for every invariant subspace U of A it holds either $U\subseteq Z$ or $[A, A]$=the submodule generated by $\{[a_1, a_2];\ a_1, a_2\in A\}\subseteq U$. From these results, however, we cannot deduce a corresponding one on invariant submodules (or subspaces) of division rings, since the proofs of them essentially utilize the assumption that the ring in question has at least one non-trivial idempotent.

The main purpose of this paper is to prove: If M is an invariant subspace of an algebraic division algebra D with center Z over a field Φ, then either $M\subseteq Z$ or $[D, D]\subseteq M$. The finite dimensional case is of particular interest, and for this case we give a quite self-contained proof (up to the classical theory of finite dimensional simple algebras). In the proof of the general case, nevertheless, we need a theorem of Herstein [11] on the Lie structure of simple rings. We also prove a result which is in a sense a sharpening of another theorem of Herstein [12]. That is: Every

Received February 24, 1966.

1) D is regarded to be a subring of A, as usual.

non-central element a of a non-commutative and infinite dimensional division algebra D over an infinite field Φ has an infinite number of conjugates which are linearly independent over Φ. This and some other results (one of them is a characterization of $[D, D]$, where D is finite dimensional over the center Z, and another one is the normal basis theorem for finite dimensional central simple algebras) are obtained through a series of discussions which constitute the proof of the main theorem.

2. Preliminary results on subspaces of a division algebra.

One of the basic ideas of this paper is to notice certain "linear separability" property of subspaces of a division algebra D, relative to right (or left) multiplications by elements of D. In this section we give a number of results concerning this property. These results will be useful in later sections.

Let D be a (not necessarily finite dimensional) division algebra over a (commutative) field Φ. If S is a subset of D and a is an element in D, we write Sa [aS] for the subset $\{sa; s\in S\}$ [$\{as; s\in S\}$]. We first prove the following

PROPOSITION 1. *Let D be a division algebra over a field Φ. Let a be an arbitrary element of D and let M and N be two Φ-subspaces of D such that $M\frown N=0$. Suppose* card Φ, *cardinal number of Φ as a set, is greater than the dimension $[M:\Phi]$ of M over Φ. Then there exists at least one element ξ in Φ satisfying $M(\xi+a)\frown N=0$. If moreover Φ is an infinite field, then there exist infinitely many elements in Φ with this property.*

Proof. If $a\in\Phi$, the proposition is trivial. Hence we assume $a\notin\Phi$. Now consider a subspace

$$V(\xi)=(M(\xi+a)\frown N)(\xi+a)^{-1}$$

of M, for each element ξ in Φ. We shall see that $\{V(\xi); \xi\in\Phi\}$ is *an independent set of subspaces of M.*[2] Thus assume that $\Sigma_{\xi\in\Phi,\xi\neq\xi_0}V(\xi)\frown V(\xi_0)$ contains a non-zero element x, for some $\xi_0\in\Phi$. Then we can write $x=x_1+\cdots+x_r$ where $x_i\in V(\xi_i)$, ξ_i being a finite number of different elements of Φ. Assume this expression of x is a shortest one. Then it is clear that x_i are linearly independent over Φ. From the definition of $V(\xi_i)$, we have $x_i(\xi_i+a)\in N$, hence $\Sigma\xi_ix_i+(\Sigma x_i)a=\Sigma\xi_ix_i+xa\in N$. Since on the other hand $x(\xi_0+a)=\xi_0\Sigma x_i+xa\in N$, this implies $\Sigma(\xi_i-\xi_0)x_i=0$ and, since x_i are linearly independent, $\xi_i=\xi_0$ $(i=1, 2, \cdots, r)$, contrary to assumption. Now, by the assumption card $\Phi>[M:\Phi]$, it is clear that Φ contains at least one ξ such that $V(\xi)=0$, i.e. $M(\xi+a)\frown N=0$. The last statement of the proposition follows immediately from the same argument.

2) See for example Jacobson [16], p. 60. Also, we shall say at times simply subspaces instead of saying Φ-subspaces, if there is no possibility of misunderstanding.

Applying the proposition just proved, we have the following result.

PROPOSITION 2. *Let D be a division algebra over Φ, let L and N be two linearly independent Φ-subspaces: $L\frown N=0$, and let H be a subspace of N. Assume that for a non-zero element a of D the subspaces L, N, Ha are linearly independent (that is, the sum of them is direct). Then there is at least one $\xi\in\Phi$ such that $(L+H)(\xi+a)\frown N=0$, provided that card $\Phi>[L:\Phi]$. If, moreover, Φ is an infinite field then Φ contains infinitely many elements with this property.*

Proof. Since $L\frown(N+Ha)=0$ and card $\Phi>[L:\Phi]$, Proposition 1 shows that there exists an element $\xi\in\Phi$ such that $L(\xi+a)\frown(N+Ha)=0$. From this we have $L(\xi+a)\frown(N+H(\xi+a))=0$, for $H(\xi+a)\subseteq N+Ha$ by the hypothesis. On the other hand, $N\frown Ha=0$ and $H\subseteq N$ clearly imply $H(\xi+a)\frown N=0$. We can verify directly that the element $\xi\in\Phi$ has the required property. The last assertion concerning the case of infinite Φ follows from Proposition 1.

REMARK. In Propositions 1 and 2 we confined ourselves to the properties of subspaces of a division algebra D relative to the (right) multiplications by elements of D. But, it is possible to generalize the propositions somewhat. In fact, we may replace D by an arbitrary vector space V over Φ, and M, N, etc. by subspaces of V. (Thereby the multiplication by an element $a\in D$ is replaced by an Φ-isomorphism σ of a pertinent subspace (M, etc.) into V.)

We can now prove

THEOREM 1. *Let D be a division algebra over Φ, M a finite dimensional subspace, N an arbitrary subspace. Suppose that $[D-N:\Phi]\geq[M:\Phi]$, $D-N$ being the difference space of D modulo N, and that* card $\Phi\geq[M:\Phi]$. *Then there exists a non-zero element a in D such that $Ma\frown N=0$.*[3] *If moreover Φ is an infinite field, then D has infinitely many elements with this property. Finally, if K is a proper division subalgebra of D, then these elements can be chosen outside of K.*

Proof. The last two statements are direct consequences of the first assertion and Proposition 1. Hence it suffices to prove the existence of a non-zero $a\in D$ with $Ma\frown N=0$. If $M\frown N=0$, we can take $a=1$. We assume therefore $M\frown N\neq 0$. Now let b be a non-zero element of D, and suppose $V=Mb\frown N\neq 0$. Let L denote a complementary Φ-subspace of V in Mb: $Mb=V\oplus L$ (direct sum). Then $L\frown N=0$ and $L+N$ is a proper subspace of D. It follows that for any element $x\neq 0$ in V we can choose an element c in D such that $xc\notin L+N$. Clearly $c\notin\Phi$. Let $H'(\neq 0)$

3) This result was proved by the present author ([4], Proposition 2) under the assumption $[D:\Phi]<\infty$, and used to deal with a different problem. For the sake of completeness, we include the proof here, which is a modification of the original one. Cf. also footnote 4.

be a complementary subspace of $Vc\frown(L+N)$ in Vc. We set $H=H'c^{-1}$. Since L, N, Hc are linearly independent and $H\subseteq V\subseteq N$, Proposition 2 can be applied. (Note that $[L:\Phi]<[L+V:\Phi]=[M:\Phi]\leq$card Φ.) The conclusion is that there is an element ξ in Φ with $(L+H)(\xi+c)\frown N=0$. On the other hand, if we set $b(\xi+c)=d$, then $d\neq 0$ and $(L+H)(\xi+c)\subseteq Md$, for $L+H\subseteq Mb$ by definition. From these we can easily verify that $[Md\frown N:\Phi]<[V:\Phi]=[Mb\frown N:\Phi]$. Applying this arguement successively, we can construct a sequence of non-zero elements of D: $\{a_1=1, a_2, a_3, \cdots\}$ satisfying

$$[Ma_i\frown N:\Phi]>[Ma_{i+1}\frown N:\Phi] \qquad (i=1, 2, \cdots).$$

But, the construction must break off in a finite number of steps, since the dimensions $[Ma_i\frown N:\Phi]$ does not exceed $[M:\Phi]$ which was assumed to be finite. Thus we must have $Ma_k\frown N=0$ for some k. This completes the proof.

In Theorem 1, the assumption of finiteness of $[M:\Phi]$ is not superfluous. In fact, consider the rational function field $R(x)$ of one variable over the field R of real numbers. The ring $R[x]$ of all polynomials in x is an R-subspace of $R(x)$. If we set $D=R(x)$ and $M=N=R[x]$ then the conditions of the theorem are satisfied except $[M:\Phi]<\infty$. But the conclusion of the theorem does not hold, since for any non-zero $a\in D$ we have $Ma\frown N\neq 0$.

By specializing our result to the finite dimensional case we have the following

COROLLARY 1. *Let D be a division algebra over Φ with $[D:\Phi]=n<\infty$ and let M and N be Φ-subspaces of D. Suppose that Φ contains at least $[n/2]$ elements.*[4] *Then there exists an element $a\neq 0$ in D such that $Ma\frown N=0$ or $Ma+N=D$, according as $[M:\Phi]+[N:\Phi]\leq n$ or $[M:\Phi]+[N:\Phi]\geq n$, respectively. If Φ is an infinite field then D has an infinite number of such elements. If moreover K is a proper division subalgebra of D then these elements can be taken outside of K.*

We note at this place that if A is a Φ-algebra and if the subspaces of A have the property described in the corollary relative to the multiplications by elements of A, then A is necessarily a division algebra.

COROLLARY 2. *Let D be a division algebra over Φ such that $[D:\Phi]=\infty$; assume that Φ is an infinite field. If M is a finite dimensional subspace of D over Φ then $Ma\frown M=0$ for infinitely many elements a in D. Moreover, if K is a proper division subalgebra of D then these elements can be taken such that $a\notin K$.*

Proof. Take $N=M$ in the theorem. The conditions of the theorem is obviously fulfilled.

4) $[n/2]$ means the greatest integer $\leq n/2$. In [4], the result (cf. footnote 3) was stated in the form of this corollary, in the case when M and N satisfy $[M:\Phi]+[N:\Phi]=n$.

We remark finally that the arguements and the results of this section remain still valid if we replace *right* by *left* everywhere. (In Theorem 1, for example, we may replace Ma by aM).

3. Invariant subspaces of arbitrary and algebraic division algebras.

Let D be again a division algebra over a field Φ and let Z be its center. As usual we identify Φ with a subfield of Z: $\Phi \subseteq Z$. We call a submodule U of D an invariant submodule if U is mapped into itself by every inner automorphism of D. An invariant (Φ-) subspace of D is defined similarly. It is obvious that the subspace generated by an invariant submodule is invariant. Also, every submodule (or subspace) of Z is invariant; in view of this we shall henceforth assume D to be non-commutative.

The starting point of our considerations on invariant subspaces is a simple arguement concerning inner mappings in an arbitrary division ring, which goes back to Brauer [6]. For the convenience of later references, we shall briefly summarize Brauer's method and obtain, by modifying it slightly, an almost obvious but useful identity.

Let a, x be two elements of D and assume $a \notin \Phi$. Then we have the relations

$$ax=(xI_a)a^{5)} \qquad \text{and} \qquad (a+1)x=(xI_{a+1})(a+1).$$

By subtracting the first from the second one obtains

$$(B_1) \qquad x-xI_{a+1}=(xI_{a+1}-xI_a)a.$$

Now take $a+\xi$, where ξ is an arbitrary non-zero element of Φ, instead of $a+1$. Then in the same way we have $\xi(x-xI_{a+\xi})=(xI_{a+\xi}-xI_a)a$. From this it follows readily that $(xI_a-xI_{a+\xi})(a+\xi)=\xi(xI_a-x)$ and finally

$$(B_2) \qquad \xi^{-1}(xI_a-xI_{a+\xi})=(xI_a-x)(a+\xi)^{-1}.$$

Observe that the relation (B_2) will remain valid if we assume $a \notin Z$ and $\xi(\neq 0) \in Z$.[6)]

Now let D be an infinite dimensional division algebra over an infinite field Φ,

---

5) I_a is the inner automorphism in D defined by a: $x \to axa^{-1}$; xI_a represents the image of x under the automorphism I_a, etc.

6) Starting from the relations $xa=a(xI_{a'})$ (where $I_{a'}$ denotes the inner mapping $x \to a^{-1}xa$) etc., we can also derive similar identities: $(B_1)'$ $x-xI'_{a'+1}=a(xI'_{a'+1}-xI_{a'})$ and $(B_2)'$ $\xi^{-1}(xI_{a'}-xI'_{a'+\xi})=(a+\xi)^{-1}(xI_{a'}-x)$. In $(B_2)'$ we make substitutions: $\xi=1$, $a+1=a'$ and $x^{-1}=x'$; then if a' and x' are such that $a'x' \neq x'a'$ we have the relation

$$a'=(x'^{-1}-(a'-1)^{-1}x'^{-1}(a'-1))(a'^{-1}x'^{-1}a'-(a'-1)^{-1}x'^{-1}(a'-1))^{-1}.$$

This is nothing but the identity which was the starting point of Hua's [14].

M an invariant subspace such that $M\not\subseteq Z$. Suppose that x is a non-central element of M. Then $V_D(x)$[7] is a proper division subalgebra of D. Let a be an arbitrary element not contained in $V_D(x)$. Then by (B_1) we have $x-xI_{a+1}=(xI_{a+1}-xI_a)a\neq 0$, which implies that $M\frown Ma\neq 0$. Corollary 2 to Theorem 1 now shows that we must have $[M:\Phi]=\infty$. This proves the following

THEOREM 2. *Let D be a division algebra over an infinite field Φ such that $[D:\Phi]=\infty$, and M an invariant subspace of D. Then we have either $M\subseteq Z$, the center of D, or $[M:\Phi]=\infty$.*

The following result is, in the case of infinite dimensional D, a sharpened form of a theorem proved by Herstein [12],[8] which states that every non-central element of a division ring has infinite conjugates.

COROLLARY. *Let D, Φ, Z be as in the theorem. Then every non-central element a of D has an infinite number of conjugates (i.e. elements of the form aI_d, $d\in D$) which are linearly independent over the base field Φ.*

Proof. Let M be the subspace generated by all conjugates of a. Since M is invariant and $M\not\subseteq Z$, we have $[M:\Phi]=\infty$ by the theorem.

As usual, the additive commutator $ab-ba$ of two elements $a, b\in D$ is denoted by $[a, b]$. Also, if U, V are submodules of D, $[U, V]$ shall mean the submodule of D generated by all $[u, v]$ where $u\in U$, $v\in V$. If $a\in D$ and U is a submodule then we define $[a, U]=\{[a, u]; u\in U\}$; the definition of $[U, a]$ is similar. Clearly $[U, V]=[V, U]$ and $[a, U]=[U, a]$. $[U, V]$ and $[a, U]$ are subspaces when U is a subspace.

We now proceed to prove

PROPOSITION 3. *Let D be a division algebra over Φ, a an algebraic element of D relative to Φ and M an invariant subspace of D. Suppose Φ has at least $[\Phi(a):\Phi]$ (=degree of a) non-zero elements. Then M contains the subspace $[a, M]$.*

Proof. Let x be an element of M. We have to show that $[a, x]=ax-xa$ is in M. If x commutes with a then certainly $[a, x]=0\in M$. Otherwise, we have $ax\neq xa$; when that is so, clearly both a and x are not in Z, the center of D. Now let $[\Phi(a):\Phi]=s$ (finite) and let $\xi_1, \xi_2, \cdots, \xi_s$ be s (distinct) non-zero elements of Φ. Then, by (B_2), we have

$$(xI_a-x)(a+\xi_i)^{-1}=\xi_i^{-1}(xI_a-xI_{a+\xi_i})\in M \qquad (1\leq i\leq s).$$

---

7) If S is a subset of D, we denote the totality of those elements in D that are commutative with every element of S as $V_D(S)$. This is clearly a division subalgebra of D containing Z.

8) Cf. also Faith [7], [8].

But $(a+\xi_i)^{-1}$ are s linearly independent elements of $\Phi(a)$ over Φ.[9] From this it follows that

$$(xI_a-x)\Phi(a)\subseteq M,$$

which implies, specifically, that $(xI_a-x)a=ax-xa$ lies in M.

Next we assume $M\not\subseteq Z$ and $a\notin Z$. Then there exists at least one element $x\in M$ which does not commute with a. To see this, we need only to note that the division subalgebra generated by M is D itself,[10] and so that $V_D(M)=Z$. Set $v=xI_a-x$. Then v is a non-zero element of M and we have $v\Phi(a)\subseteq M$ by the proof of above proposition. Also, since $\Phi(a)a=\Phi(a)$, we have $v\Phi(a)\subseteq Ma$. Thus we have proved the following

LEMMA 1. *Let D be a division algebra with center Z over Φ, a an algebraic element and M an invariant subspace of D. Assume that $a\notin Z$, $M\not\subseteq Z$ and Φ has at least $[\Phi(a):\Phi]$ non-zero elements. Then M contains an element $v\neq 0$ such that $v\Phi(a)\subseteq M\frown Ma$. The element v can be taken as $v=xI_a-x$ where x is any element of M not commuting with a.*

Hereafter we shall be concerned with algebraic division algebras. Suppose D is an algebraic division algebra over Φ (i.e., every element of D is algebraic). Then we know that if Φ is a finite field then D is commutative (Jacobson [15]). We may therefore assume that Φ is an infinite field.

THEOREM 3. *Let D be an algebraic division algebra with center Z over an (infinite) field Φ and let M be an invariant subspace of D such that $M\not\subseteq Z$. Then M contains the subspace $[D, M]$, which is itself an invariant Z-subspace not contained in Z.*

Proof. That $[D, M]\subseteq M$ and that $[D, M]$ is an invariant Z-subspace follow immediately from Proposition 3 and the definitions. It remains to prove that $[D, M]$ is not contained in Z. Let a be a non-central element of D. By Lemma 1 there is an element $x\in M$ with $[a, x]\neq 0$. If $[a, x]\notin Z$ we are enough. If, on the other hand, $[a, x]=\lambda\in Z$ then we have $(xI_a-x)a^2=[a, x]a=\lambda a\in M$, for $v\Phi(a)=(xI_a-x)\Phi(a)\subseteq M$ by the same lemma. From this it follows that $[D, a]=[D, \lambda a]\subseteq[D, M]$. Now suppose $[D, M]$ is contained in Z. Then $[D, M]=[D, D]\subseteq Z$ by what we have just proved. But the last inclusion does not hold since D is non-commutative.[11] This con-

9) This fact can be verified easily in a straight-forward manner.

10) Cartan-Brauer-Hua theorem. See for example Brauer [6].

11) In fact: Let $[D, D]\subseteq Z$ and let $a\in D$ be a non-central element. Then there is an element $b\in D$ such that $ab-ba\neq 0$. Set $ab-ba=\lambda_1$, $ba^{-1}-a^{-1}b=\lambda_2$ $(\lambda_1, \lambda_2\in Z)$. Then we have $aba^{-1}-b=\lambda_1a^{-1}=\lambda_2a$, and hence $a^2=\lambda_1\lambda_2^{-1}\in Z$. Since this $(a^2\in Z)$ holds for any element of D, D must be commutative. (Cf. Kaplansky [17].)

tradiction proves the theorem.

If M is moreover minimal in the sense that there is no proper invariant Φ-subspace of M not contained in Z, then our result indicates that $M=[D, M]$ $(\neq Z)$ and hence that M is at the same time an invariant Z-subspace.

4. The case of finite dimensional division algebras.

The results of sections 2 and 3 will be now applied to prove the main theorem of this paper that has been announced in the introduction (section 1). In this section we shall consider finite dimensional division algebras over the base field Φ. As we have seen in Theorem 3, every invariant Φ-subspace M of a non-commutative, algebraic division algebra D with center Z over Φ (such that $M\neq Z$) contains an invariant Z-subspace that is not contained in Z. In view of this it will be sufficient if we further restrict ourselves to the case of finite dimensional central division algebras: $Z=\Phi$. Our proof below is in close connection with the classical theory of subalgebras of finite dimensional central simple algebras. We shall also state some results on these algebras which will be obtained as by-products in the proof of the main theorem.

Let D be a central division algebra over Φ with finite dimension and let the index of D be s: $[D:\Phi]=n=s^2$. As before we assume that D is non-commutative, i.e. $n>1$; the center Φ has then an infinite number of elements. It is well known that D possesses a maximal subfield of degree s which is separable over Φ. In connection with this, Corollary 1 to Theorem 1 may be sharpened somewhat. The precise result is the following

LEMMA 2. *Let D be a central division algebra of finite dimension n (>1) over Φ and let M, N be subspaces of D. Then there exists a separable element a of D over Φ such that* (1) *$\Phi(a)$ is a maximal subfield of D, and* (2) *a satisfies either $Ma\frown N=0$ or $Ma+N=D$ according as $[M:\Phi]+[N:\Phi]\leq n$ or $[M:\Phi]+[N:\Phi]\geq n$, respectively.*

Proof. Clearly it suffices to consider the case $[M:\Phi]+[N:\Phi]\leq n$. We shall first prove that D contains a separable element $a(\neq 0)$ over Φ such that $Ma\frown N=0$. By Corollary 1 to Theorem 1 there is a non-zero element b in D satisfying $Mb\frown N=0$. If b is separable then we are through. Suppose therefore b is inseparable over Φ. Then we have $T(b)=0$.[12] Now let c be an element of D for which $T(c)\neq 0$ holds. (Since the discriminant of D[13] does not vanish, D contains an element d not in Φ with non-zero trace). We set $x=b^{-1}c$. Now Proposition 1 implies that $Mb(\xi+x)\frown N=M(b\xi+c)\frown N=0$ for an element ξ in Φ. Since $T(b\xi+c)=T(c)\neq 0$, $b\xi+c$ is a separable element over Φ. Thus there is a non-zero element $a\in D$ which

12) The (reduced) trace function in D.

13) See for instance Albert [1], p. 124.

is separable over Φ and which satisfies $Ma\frown N=0$. Now, if $\Phi(a)$ is a maximal subfield of D then there remains nothing to prove. Otherwise there exists a maximal separable subfield $\Phi(d)$ of D containing $\Phi(a)$ as a proper subfield. Set $y=a^{-1}d$. It follows again from Proposition 1 that Φ contains infinitely many elements ξ such that $Ma(\xi+y)\frown N=M(a\xi+d)\frown N=0$. To complete the proof we have only to observe that the elements $a\xi+d$ are primitive elements of $\Phi(d)$ except (possibly) for a finite number of them.

Next we state the following

LEMMA 3. *Let D be a finite dimensional central division algebra over Φ and suppose $[D:\Phi]=n(>1)$. Then the Φ-subspace $[D, D]$ is a proper invariant subspace of dimensionality $n-1$ over Φ: $[[D, D]:\Phi]=n-1$. Moreover, an element x of D is in $[D, D]$ if and only if $T(x)=0$.*

This result is generally well known.[14)15)] It should be noted that $\Phi\subseteq[D, D]$ if and only if the characteristic of the base field is a factor of n.

Now let M be an invariant subspace of D, a central division algebra with finite dimension $n=s^2(>1)$ over its center Φ, and suppose $M\not\subseteq\Phi$. We note that $M\frown[D, D]$ is also an invariant subspace not contained in Φ. In fact, from Lemma 1 we have $Ma\frown M\neq 0$ for every element $a\notin\Phi$; this, combined with Corollary 1 to Theorem 1, implies that $[M:\Phi]>n/2$. Since $n\geq 4$ and $[[D, D]:\Phi]=n-1$, we have $[M\frown[D, D]:\Phi]>1$ and so $M\frown[D, D]\not\subseteq\Phi$. (The fact that $M\frown[D, D]$ is invariant is obvious. Cf. also Theorem 3.) In view of this we shall assume for some time $M\subseteq[D, D]$. Observe that $[M:\Phi]>n/2$ still holds.

By Lemma 2, we can choose an element $a\in D$ such that $[\Phi(a):\Phi]=s$, i.e. a is a primitive element of a separable maximal subfield of D, and such that $Ma+M=D$. Moreover, we may assume $T(a)\neq 0$; this can be seen from the proof of Lemma 2. (In fact, $\Phi(a)$ contains an element with non-zero trace, even if $T(a)=0$.) Note that this implies $\Phi(a)\not\subseteq M$ since we assumed $M\subseteq[D, D]$. On the other hand, Lemma 1

14) The proof may be carried out as follows. Let $n=s^2$, let $\{u_i;\ 1\leq i\leq n\}$ be a basis of D over Φ and let Ω be a splitting field of D over Φ. As is well known, $D_\Omega=D\otimes_\Phi\Omega$ can be identified with Ω_s, the total matrix algebra over Ω. Now it is obvious that $[D, D]$ is generated by $[u_i, u_j]$, $1\leq j$, $j\leq n$; this is also true for $[D_\Omega, D_\Omega]=[\Omega_s, \Omega_s]$. But the Ω-subspace $[\Omega_s, \Omega_s]$ of Ω_s has dimensionality s^2-1 over Ω (a simple proof of this fact will be found in Kasch [19]), and hence the set $\{[u_i, u_j];\ 1\leq i, j\leq n\}$ contains exactly $n-1$ linearly independent elements. These are of course linearly independent over Φ, as elements of D. Thus $[[D, D]:\Phi]=n-1$. As to the second assertion we note that $T([a, b])=0$ for all $a, b\in D$. The subset $U=\{x;\ x\in D, T(x)=0\}$ of D is therefore a subspace containing $[D, D]$. On the other hand, since D contains an element with non-zero trace, we have $[U:\Phi]\leq n-1$. This implies that $U=[D, D]$.

15) The result does not hold for an arbitrary division ring D with center Φ. In fact, Harris [9] constructed an example of division rings such that $[D, D]=D$.

shows that M contains an element x_1 which does not commute with a, and that if $v_1=x_1I_a-x_1$ then $v_1\Phi(a)\subseteq M\frown Ma$; we have hence $[M\frown Ma:\Phi]\geq s$. From these we obtain:

$$2[M:\Phi]=[M:\Phi]+[Ma:\Phi]=[D:\Phi]+[M\frown Ma:\Phi]\geq s^2+s,$$

i.e. $[M:\Phi]\geq(s^2+s)/2$. We shall now prove the following preliminary result on the dimensionality $[M:\Phi]$.

(P) Under the same assumptions and notations as above, we have $[M:\Phi]\geq s^2-s/2$.

Proof of (P). We have already seen that $[M:\Phi]\geq(s^2+s)/2$. If $s=2$, this inequality gives $[M:\Phi]\geq 3$, which coincides with the inquality of (P). Consequently we assume $s\geq 3$. We have then (*) $[M:\Phi]\geq(s^2+s)/2\geq 2s$. Let x_1 and v_1 be as before: $x_1\in M$, $\notin V_D(a)$; $v_1=x_1I_a-x_1$, $v_1\Phi(a)\subseteq M\frown Ma$. Suppose x_2 be a second element of M satisfying the same conditions as x_1 and set $v_2=x_2I_a-x_2$. We now consider under what circumstances v_2 is contained in $v_1\Phi(a)$. The condition $v_2\in v_1\Phi(a)$ may be stated as follows: There is a polynomial $f(\lambda)\in\Phi[\lambda]$ such that $x_2I_a-x_2=(x_1I_a-x_1)f(a)$, or equivalently, $(x_2-x_1f(a))I_a=x_2-x_1f(a)$. This means $x_2-x_1f(a)\in V_D(a)=\Phi(a)$, and so we have $x_2\in x_1\Phi(a)+\Phi(a)$. Now $[x_1\Phi(a)+\Phi(a):\Phi]=2s$ and $\Phi(a)\subsetneqq M$, by assumption; hence we have $[(x_1\Phi(a)+\Phi(a))\frown M:\Phi]<2s$. It follows from (*) that we can find an element x_2 which is in M and not in $x_1\Phi(a)+\Phi(a)$. If we set $v_2=x_2I_a-x_2$, as above, then $v_2\neq 0$ and $v_2\notin v_1\Phi(a)$ by what we have seen. Since $v_2\Phi(a)$ is also contained in $M\frown Ma$ (Lemma 1), $v_1\Phi(a)+v_2\Phi(a)$ (direct sum) is a subspace of $M\frown Ma$. Hence $[M\frown Ma:\Phi]\geq 2s$. And, this implies

$$2[M:\Phi]=[D:\Phi]+[M\frown Ma:\Phi]\geq s^2+2s,$$

as before. Similarly, we can easily verify successively the following inequalities:

$$2[M:\Phi]\geq s^2+3s,\ \cdots,\ 2[M:\Phi]\geq s^2+(s-1)s.$$

The details of the verification will be omitted since we have only to repeat the same arguement as above, with obvious modifications. Now from the last inequality we have $[M:\Phi]\geq s^2-s/2$, which was to be proved.

Let M be again an invariant subspace of D satisfying $M\subsetneqq\Phi$, $M\subseteq[D,D]$. Suppose that b is an element of D such that $\Phi(b)$ is a separable maximal subfield of D: $[\Phi(b):\Phi]=s$.[16] Since we know that $[M:\Phi]\geq s^2-s/2>(s-1)s$, a similar arguement as in the proof of (P) will be available. Thus we can choose a set of elements $y_1, y_2, \cdots, y_{s-1}$ of M with the following property: If we set $w_i=y_iI_b-y_i$ then $w_i\neq 0$ and $w_i\Phi(b)\subseteq M(1\leq i\leq s-1)$; and moreover $w_i\Phi(b)$ are independent subspaces of M. By symmetry we have $\Phi(b)w_i\subseteq M$.[17]

16) It is easy to see that $\Phi(b)$ contains an element with non-zero trace. (Note that the reduced trace $T(x)$ coincides with the usual trace of x for $\Phi(b)$ over Φ, if $x\in\Phi(b)$.) Thus $\Phi(b)\nsubseteq M$.

17) Cf. the proof of Lemma 1. Also see the footnote 6.

We now consider D as a $(\Phi(b), \Phi(b))$-module; but this is equivalent to considering D as a $(\Phi(b)\otimes_{\Phi}\Phi(b))$-module.[18] Since $\Phi(b)\otimes_{\Phi}\Phi(b)$ is a semi-simple algebra of finite dimension over Φ (remember that $\Phi(b)$ is separable over Φ), D is completely reducible as a $(\Phi(b)\otimes_{\Phi}\Phi(b))$-module. The subfield $\Phi(b)$ is evidently a $(\Phi(b)\otimes_{\Phi}\Phi(b))$-submodule; moreover, this is a homogeneous component[19] of $(\Phi(b)\otimes_{\Phi}\Phi(b))$-module D. Hence, we have a (unique) direct sum decomposition

$$D=\Phi(b)\oplus B(b)$$

of D as a $(\Phi(b), \Phi(b))$-module.

Now let U be the $(\Phi(b), \Phi(b))$-submodule of D generated by the elements $w_i (1\leq i\leq s-1)$. As we have seen, $w_i\Phi(b)\subseteq M$ and $\Phi(b)w_i\subseteq M (1\leq i\leq s-1)$. From this we see that $U\subseteq M$. In fact, we decompose the elements y_ι according to the decomposition $D=\Phi(b)+\sum_{i=1}^{s-1}w_i\Phi(b)$: $y_\iota=y_\iota'+y_\iota''$. Then for each i we have $y_\iota''\Phi(b)\subseteq M$ and $w_i=y_i''I_b-y_i''$; and, if $c_\iota (\neq 0)$ is an element of $\Phi(b)$ then $w_ic_\iota=(y_i''c_\iota)I_b-y_i''c_\iota$. This gives $\Phi(b)w_ic_\iota\subseteq M$, for we may replace y_i and w_i by $y_i''c_\iota$ and w_ic_ι, respectively, in our previous arguements. Thus $\Phi(b)w_i\Phi(b)\subseteq M$, since c_ι was arbitrary. This proves the inclusion $U\subseteq M$. We have then $\Phi(b)\nsubseteq U$. On the other hand, $\Phi(b)+U=D$. From these we can easily deduce that $U=B(b)=\sum_{i=1}^{s-1}w_i\Phi(b)\subseteq M$.

We shall prove next that the Φ-subspace B of D, generated by all the $B(b)$ as above (i.e. b is a primitive element of a separable maximal subfield), coincides with $[D, D]$. In fact: The inclusion $B\subseteq[D, D]$ is already proved above. We have therefore to show $[a, b]\in B$ for any $a, b\in D$. If one of the two elements, say a, is a primitive element of a separable maximal subfield, we decompose b according to $D=\Phi(a)\oplus B(a)$: $b=b'+b''$; then $[a, b]=[a, b'']=ab''-b''a\in B(a)\subseteq B$. Next, if a, say, is separable over Φ, we imbed $\Phi(a)$ in a separable maximal subfield $\Phi(c)$; then we have $[a, b]\in B(c)$, similarly as above. Finally, let a be arbitrary. We may suppose that $T(a)=0$. We take an element c with $T(c)\neq 0$; then $[c, b]\in B$ and $[a+c, b]\in B$. Hence $[a, b]=[a+c, b]-[c, b]\in B$. Thus we have $B=[D, D]$. On the other hand, $B\subseteq M\subseteq[D, D]$ as we have seen, and so we have $M=[D, D]$.

Our result may be summarized in the following main theorem.

THEOREM 4. *Let D be a division algebra of finite dimension over an (infinite) field Φ. Suppose M is an invariant subspace. Then either M is contained in Z, the center of D, or M contains $[D, D]$. In particular, if D is moreover central then the only subspaces of D are $0, \Phi, [D, D]$ and D.*

Concerning separable maximal subfields and the submodule $[D, D]$ we have

THEOREM 5. *Let D be a central division algebra over Φ and let $[D:\Phi]=n<\infty$. Suppose that K is a separable maximal subfield of D and that b is a primitive element: $K=\Phi(b)$. Then there is a unique direct sum decomposition of D as a*

18) See for example Jacobson [16], p. 102.

19) In the sense of Jacobson [16], section 4.2.

$(\Phi(b), \Phi(b))$-module: $D=\Phi(b)\oplus B(b)$; and when that is so, $B(b)=[b, D]$.[20] *Furthermore, $[D, D]$ is characterized as the minimal submodule containing all such submodules as $B(b)$.*

Proof. It remains only to show $B(b)=[b, D]$. The inclusion $[b, D]\subseteq B(b)$ is clear from the proof of $B=[D, D]$ (in the proof of Theorem 4). Conversely, let y be in $B(b)$. y is expressible as $y=\sum_{i=1}^{s-1} w_i c_i$, $c_i\in\Phi(b)$, notations being the same as before. But, it follows easily from the definition of w_i that $w_i c_i\in[b, D]$. Hence $B(b)=[b, D]$.

Finally we state the normal basis theorem for a central division algebra D of finite dimension over Φ.

THEOREM 6. *Let D be a finite dimensional central division algebra over Φ and let $[D:\Phi]=n$. Suppose x is an element of D not in the center Φ. Then x generates a normal basis over Φ (i.e. there exist n inner automorphisms $I_{a_i}(1\leq i\leq n)$ such that $\{xI_{a_i}\}$ constitutes a Φ-basis of D) if and only if $T(x)\neq 0$, where $T(x)$ denotes the (reduced) trace of x. (There exist infinitely many elements in D with this property.)*[21]

Proof. Let M be the invariant subspace generated by x. Since $x\notin\Phi$, Theorem 4 implies $[D, D]\subseteq M$. On the other hand, it is clear that x generates a normal basis if and only if $M=D$. But this is the case if and only if $x\notin[D, D]$, which is equivalent to the condition $T(x)\neq 0$. The last statement (in parentheses) is obvious.

5. Another proof of the main theorem and extension to the case of algebraic division algebras.

In this section we shall give an alternative proof of Theorem 4 and at the same time extend the result to an arbitrary algebraic division algebra. The proof is short, but not elementary, since it requires a result of Herstein [11][22] from the theory of Lie ideals of simple rings. Suppose A is a ring and U a submodule of A. If $[U, A]\subseteq U$ then U is called a *Lie ideal* of A. Herstein's theorem states that if U is a Lie ideal of a simple ring A then either $U\subseteq Z$, the center of A, or $U\supseteq[A, A]$ except if A is of characteristic 2 and is of dimension 4 over Z.

THEOREM 7. *Let D be an algebraic division algebra with center Z over Φ. Suppose that M is an invariant Φ-subspace of D. Then either $M\subseteq Z$ or $M\supseteq[D, D]$.*

Proof. If Φ is a finite field then D is commutative and the theorem is trivial. Hence we may assume Φ is an infinite field. Then by Proposition 3 we have

20) This has been proved by Kasch [19] (Hilfssatz 2).

21) From this result we can also deduce the existence of a normal basis of a finite dimensional central simple algebra. Cf. Kasch [19], Satz 4.

22) See also Amitsur [3], Herstein [13].

$[M, D] \subseteq M$; M is therefore a Lie ideal of D. Herstein's theorem now implies that either $M \subseteq Z$ or $M \supseteq [D, D]$.[23]

References

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

[2] Amitsur, S. A., Invariant submodules of simple rings. Proc. Amer. Math. Soc. **7** (1956), 987-989.

[3] ———, Derivations in simple rings. Proc. London Math. Soc. **7** (1957), 87-112.

[4] Asano, S., Note on some generalizations of quasi-Frobenius rings. Kōdai Math. Sem. Rep. **13** (1961), 227-234.

[5] Baxter, W., Lie simplicity of a special class of associative rings. Proc. Amer. Math. Soc. **7** (1956), 855-863.

[6] Brauer, R., On a theorem of H. Cartan. Bull. Amer. Math. Soc. **55** (1949), 619-620.

[7] Faith, C. C., On conjugates in division rings. Canad. J. Math. **10** (1958), 374-380.

[8] ———, Submodules of rings. Proc. Amer. Math. Soc. **10** (1959), 596-606.

[9] Harris, B., Commutators in division rings. Proc. Amer. Math. Soc. **9** (1958), 628-630.

[10] Hattori, A., On invariant subrings. Jap. J. Math. **21** (1951), 121-129.

[11] Herstein, I. N., On the Lie and Jordan rings of a simple associative rings. Amer. J. Math. **77** (1955), 279-285.

[12] ———, Conjugates in division rings. Proc. Amer. Math. Soc. **7** (1956), 1021-1022.

[13] ———, Lie and Jordan structures in simple, associative rings. Bull. Amer. Math. Soc. **67** (1961), 517-531.

[14] Hua, L. K., Some properties of a sfield. Proc. Nat. Acad. Soc. **35** (1949), 533-537.

[15] Jacobson, N., Structure theory for algebraic algebras of bounded degree. Ann. Math. **46** (1945), 695-707.

[16] ———, Structure of rings. Amer. Math. Soc. Coll. Publ. **37** (1956).

[17] Kaplansky, I., A theorem on division rings. Canad. J. Math. **3** (1951), 290-292.

[18] Kasch, F., Über den Endomorphismenring eines Vektorraumes und den Satz von der Normalbasis. Math. Ann. **126** (1953), 447-463.

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

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

[21] Rosenberg, A., The Cartan-Brauer-Hua theorem for matrix and local matrix rings. Proc. Amer. Math. Soc. **7** (1956), 891-898.

Department of Mathematics,
Tokyo Institute of Technology.

23) The exceptional case, when D is of characteristic 2 and is 4-dimensional over Z, is to be considered separately.