

## On the Theory of Division Algebras

R. E. MacRae

*Department of Mathematics*

*University of Colorado*

*Boulder, Colorado*

Submitted by Bryan Cain

---

### ABSTRACT

The theory of division algebras (of finite dimension over the center) is reduced to an application of two simple principles from general linear algebra. Along the way, a simple proof of Wedderburn's theorem on finite division algebras is given.

---

### 1. INTRODUCTION

One of the more interesting extensions of the theory of algebraic fields resides in the theory of division algebras. This theory was developed originally as an adjunct to class field theory, and this use was later supplanted by the development of Galois cohomology during the 1950s. Nonetheless, the theory remains of some independent interest. It is my purpose here to give new and simpler proofs for several of the basic structural theorems (in this regard see particularly Theorems 2.20, 2.21 and Corollary 2.22). By dealing with division algebras themselves rather than with simple algebras (i.e. matrix algebras over a division algebra) it is possible to base the theory on two simple facts from linear algebras: (1) a commuting set of diagonalizable matrices is simultaneously diagonalizable and (2) there are no proper invariant subspaces of a total matrix algebra over a field. The appropriate extension of the results on division algebras to simple algebras is not difficult to effect and is not included here. The point is that the part of the theory of most interest can be

treated directly in a straightforward way. One should note that Corollary 2.22 is the theorem asserting the nonexistence of nontrivial finite division algebras. The proof here is quite different from the usual one that involves the structure of cyclotomic polynomials.

## 2. GENERAL THEORY

For the record we begin with several propositions and simple facts.

**DEFINITION 2.1.** A *division ring* is an associative ring with identity in which every nonzero element is invertible.

**PROPOSITION 2.2.** *The center of a division ring is a field.*

**DEFINITION 2.3.** A division ring  $D$  with center  $k$  will be called of *algebraic type* if every element of  $D$  is algebraic over  $k$ , and will be called a *division algebra* if it is finite dimensional as a vector space over  $k$ . When  $k_0$  is a subfield of  $k$ , we may speak of  $D$  as being of algebraic type over  $k_0$  when every element of  $D$  is algebraic over  $k_0$ .

**PROPOSITION 2.4.** *A division algebra is of algebraic type.*

We next note two general facts from linear algebra.

**THEOREM 2.5.** *Let  $V$  be an  $n$  dimensional vector space over the field  $k$ . Let  $S$  be a set of pairwise commuting linear transformations of  $V$  into itself such that for each member of  $S$  there is a basis for  $V$  relative to which the matrix representation of the transformation is diagonal. Then there is a basis for  $V$  which simultaneously diagonalizes all members of  $S$ .*

**THEOREM 2.6.** *Let  $V$  be an  $n$  dimensional vector space over the field  $k$ . Then there is no proper nonzero subspace of  $V$  which is invariant under all linear transformations of  $V$  to itself.*

The proofs of these facts are well known.

**PROPOSITION 2.7.** *Let  $D$  be a division algebra. If  $U$  is a subring of  $D$  that contains  $k$ , then  $U$  is also a division ring which is finite dimensional over  $k$ . (The center of  $U$  may be properly larger than  $k$ .)*

*Proof.* If  $u$  is member of  $U$ , then the subring  $k[u]$  is an integral domain which is finite dimensional as a vector space over  $k$ . Thus  $k[u]$  is a field. In other words, the inverse of  $u$  is also in  $U$ . ■

**DEFINITION 2.3.** If  $D$  is a division ring with center  $k$ , and  $U$  is a subring of  $D$ , then we will denote by  $U'$  the set of elements of  $D$  that commute with all the elements of  $U$ .

**PROPOSITION 2.9.** *Let  $D$  be a division algebra.*

- (1) *If  $U$  is a subring, then  $U'$  is also a subring and (by Proposition 2.7) a division ring.*
- (2) *If  $U \leq V$  are subrings then  $V' \leq U'$ .*
- (3)  *$U \leq U''$ .*
- (4)  *$U' = U'''$ .*

This proposition is an essentially trivial observation.

Let us now denote by  $D^0$  the division algebra with center  $k$  that is antiisomorphic to  $D$ . When  $M$  is a bimodule over  $D$ , then we can equivalently regard it as a left module over  $DX_k D^0$ . We also note the natural morphism of  $DX_k D^0$  into  $\text{End}_k(D)$  which associates with  $aXb^0$  the endomorphism that maps  $x$  to  $axb$ .

**THEOREM 2.10.** *Regarding  $D$  itself as a left module over  $DX_k D^0$ , the natural ring morphism of  $DX_k D^0$  into  $\text{End}_k(D)$  is an isomorphism.*

*Proof.* Let  $\{u_1, \dots, u_r\}$  be a  $k$ -linearly independent subset of  $D$ . We claim that there exist  $k$ -endomorphisms  $\{f_1, \dots, f_r\}$  that lie in the image of the natural morphism such that  $f_i(u_j) = \delta_{ij}$ . The proof proceeds by induction on  $r$ . When  $r = 1$ , let  $f_1(x) = xu_1^{-1}$ . Suppose that such a construction is possible for every set of  $r - 1$  linearly independent elements of  $D$ , and let  $\{u_1, \dots, u_r\}$  be an arbitrary set of  $r$  linearly independent elements. Let  $\{g_1, \dots, g_{r-1}\}$  be a set of  $k$ -endomorphisms in the image of the natural morphism such that  $g_i(u_j) = \delta_{ij}$ . In case  $g_i(u_r)$  is in  $k$  for all  $i$ , let  $f_r(x) = \sum g_i(x)u_i - x$ . It is clear that  $f_r$  lies in the image of the natural morphism, and  $f_r(u_i) = 0$  for  $i < r$ , and  $f_r(u_r)$  does not vanish. The latter fact arises because of the assumed linear independence over  $k$ . If, on the other

hand, some  $g_i(u_r)$  is not in  $k$ , then there is an element  $\alpha$  in  $D$  such that  $\alpha g_i(u_r) - g_i(u_r)\alpha$  does not vanish. Let  $f_r(x) = \alpha g_i(x) - g_i(x)\alpha$ . Certainly  $f_r$  lies in the image of the natural morphism,  $f_r(u_i) = 0$  for  $i < r$ , and  $f_r(u_r)$  does not vanish. In both of these cases let  $g_r(x) = f_r(x)f_r(u_r)^{-1}$ . Now repeat this construction with each  $u_i$  in turn at the end of the list. We ultimately arrive at the required set of endomorphisms. Finally let  $\{u_1, \dots, u_n\}$  be a  $k$ -basis for  $D$ . Then the  $k$ -endomorphisms  $\{g_1, \dots, g_n\}$  that we construct as above have the property that  $g_i(u_j) = \delta_{ij}$ . Since the  $k$ -dimension of  $D$  is  $n$ , it follows that these  $k$ -endomorphisms form a basis for  $\text{End}_k(D)$  and lie in the image of the natural morphism. Thus the natural morphism is surjective. Finally, a comparison of dimensions [both  $DX_k D^0$  and  $\text{End}_k(D)$  have dimension  $n^2$  over  $k$ ] shows that the natural morphism is also injective. ■

This theorem extends easily to subalgebras  $U$  of  $D$  by virtue of the fact that  $UX_k D^0$  is contained naturally in  $DX_k D^0$  and the fact that  $U'$  is a division algebra.

**THEOREM 2.11.** *Let  $D$  be a division algebra with center  $k$ . If  $U$  is a subalgebra of  $D$ , then the isomorphism of  $DX_k D^0$  with  $\text{End}_k(D)$  constructed in Theorem 2.10 induces a monomorphism of  $UX_k D^0$  into  $\text{End}_k(D)$ . The image of this morphism is precisely  $\text{End}_{U'}(D)$ , considered as a subring of  $\text{End}_k(D)$ .*

*Proof.* The first assertion is clear from the fact that  $UX_k D^0$  is contained naturally in  $DX_k D^0$ . It is also clear that the image of  $UX_k D^0$  is contained in  $\text{End}_{U'}(D)$ . On the other hand, since  $U'$  is a division ring,  $D$  has a left  $U'$ -basis. The argument given in Theorem 2.10 can be extended to show that  $UX_k D^0$  is mapped onto  $\text{End}_{U'}(D)$ . One need only replace the use of  $k$  with  $U$  and  $U'$  in the inductive step of that proof. ■

**COROLLARY 2.12.** *Let  $U$  be a subalgebra of  $D$ . Then  $[U:k] = [D:U']$ . Moreover,  $U = U''$ .*

**COROLLARY 2.13.** *The following are equivalent:*

- (1)  $K$  is a maximal subfield of  $D$ ;
- (2)  $K = K'$ ;
- (3)  $[K:k] = [D:K]$ .

*Proof.* (2) follows from (1) because  $K[u]$  is an integral domain which is finite dimensional over  $K$  whenever  $u$  is in  $K'$ . Thus  $K[u]$  is a field, and so  $u$

is in  $K$  when  $K$  is maximal. (3) Follows from (2) by Corollary 2.12. Likewise (1) follows from (3) as a result of Corollary 2.12. ■

Since maximal subfields certainly exist, we have:

COROLLARY 2.14.  $[D:k] = n^2$ .

DEFINITION 2.15. Such maximal subfields are called *splitting fields*.

THEOREM 2.16.  $D$  contains a separable splitting field.

*Proof.* We may assume that  $k$  is infinite, since a finite field is perfect. Suppose first that there is an element  $u$  of  $D$  that is not contained in  $k$  and is separable over  $k$ . Let  $k[u] = k_1$  and let  $k'_1 = D_1$ . By an induction hypothesis  $D_1$  contains a separable splitting field  $K$ . An examination of relative degrees shows that  $K$  is also a splitting field of  $D$ . Clearly  $K$  is separable over  $k$ . Since, on the other hand, that every element of  $D$  is purely inseparable over  $k$ . Since  $D$  is of finite degree over  $k$ , it follows that, for a suitable exponent  $e$  of the characteristic  $p$ , say  $q = p^e$ , we have  $u^q$  in  $k$ , for every  $u$  in  $D$ . Let  $u_1, \dots, u_n$  be a  $k$ -basis for  $D$ . Then the typical element of  $D$  is of the form  $\sum x_i u_i$  where each  $x_i$  is in  $k$ . Thus  $(\sum x_i u_i)^q = \sum \Phi_i(x_1, \dots, x_n) u_i$  is a member of  $k$  with suitable universal polynomials  $\Phi_i(x_1, \dots, x_n)$ . Since we may assume without loss of generality that  $u_1 = 1$ , it will follow that  $\Phi_i(x_1, \dots, x_n) = 0$  for all  $x_1, \dots, x_n$  in  $k$  and all  $i > 1$ . Since  $k$  is infinite, it follows that each  $\Phi_i \equiv 0$  for  $i > 1$ . Consequently we have the universal equation  $(\sum x_i u_i)^q = \Phi_1(x_1, \dots, x_n)$ . It will continue to hold in the ring  $KX_k D^0$  which is also of dimension  $n$  over  $K$ . Pick  $K$  to be a splitting field of  $D$ . We have already shown that  $KX_k D^0$  is isomorphic to the ring of  $n \times n$  matrices over  $K$ . The universal equation above can therefore be interpreted as asserting that the  $q$ th power of every  $n \times n$  matrix over the field  $K$  is contained in the subfield of diagonal matrices. This is certainly not the case unless  $n = 1$ . The case  $n = 1$  is, however, not of great interest. ■

It would be very nice if it could now be proved that every division algebra contains not only a separable splitting field but a normal separable splitting field as well. Examples to the contrary exist, however, and one of the more striking results of class field theory asserts that, in the case when  $k$  is a number field or a finitely generated field of transcendence degree 1 over a finite field, every division algebra over  $k$  does contain a normal, separable splitting field (in fact a cyclic splitting field). In the interest of a general theory, however, we must take into account the possibility that  $D$  contains

no Galois splitting fields. To this end let  $D$  be a division algebra with center  $k$ , and let  $K$  be a separable splitting field of  $D$  contained in  $D$ . Moreover let  $L$  be the Galois closure of  $K$  with  $[K:k] = n$  and  $[L:K] = r$ . Since right multiplication of the elements of  $L$  by elements of  $L$  can be regarded as a  $K$ -endomorphism of  $L$ , we have the usual right, regular representation of  $L$  as a subring of the ring  $\text{End}_K(L)$ . This latter ring is isomorphic to the ring of  $r \times r$  matrices over  $K$  as soon as we select a  $K$ -basis for  $L$ . Since  $K \leq D$ , every  $r \times r$  matrix over  $K$  is also an  $r \times r$  matrix over  $D$ . We will thus regard  $L$  as a subfield of the ring of  $r \times r$  matrices over  $D$ . The exact embedding is dependent on the choice of a  $K$ -basis for  $L$  and thus is not natural.

**LEMMA 2.17.** *The complete matrix ring  $M_r(D)$  contains no nontrivial two sided ideals.*

The proof of this is well known.

**THEOREM 2.18.** *Let  $D$  be a division algebra with center  $k$ , and  $K$  a separable splitting field contained in  $D$  with  $[D:K] = [K:k] = n$ . Let  $L$  be the Galois closure of  $K$ , and let  $L$  be embedded in  $A = M_r(D)$  as described above. Then the induced natural morphism of  $LX_k A^0$  into  $\text{End}_L(A)$  is an isomorphism.*

*Proof.* Now it is quite obvious that  $DX_k M_r(k) \approx M_r(D)$  and that  $LX_K K \approx L$ . One therefore can easily verify that  $LX_k M_r(D)^0 \approx LX_K KX_k M_r(D)^0 \approx LX_K M_r(KX_k D^0)^0 \approx LX_K M_{nr}(K)^0 \approx M_{nr}(L)^0$ . Since the ring  $M_{nr}(L)$  has no nontrivial two sided ideals, the natural morphism of  $LX_k A^0$  to  $\text{End}_L(A)$  is a monomorphism. A comparison of the dimensions of these rings as vector spaces over the field  $k$  establishes the fact that we have an isomorphism. ■

(Note that this theorem is quite similar to Theorem 2.11 but does not use the same argument, because  $A$  is not a division ring. We have assumed that  $A$  is a total matrix algebra, however, so simple facts about tensor products replace the more complicated construction of Theorem 2.11.)

**COROLLARY 2.19.** *With the same notation as in Theorem 2.18, we have  $L' = L$ .*

*Proof.* Suppose there is an element  $u$  in  $L'$  but not in  $L$ . It follows that  $uA$  is a left  $LX_k A^0$  module. However,  $LX_k A^0$  is isomorphic to  $M_{nr}(L)$  and

$\text{End}_L(A)$ . Thus  $uA = 0$  or  $uA = A$ , since  $A$  has no proper invariant subspaces. The first possibility cannot hold, since  $u$  is not zero. Consequently there is an element  $v$  in  $A$  such that  $uv = 1$ . Since these are matrices, it follows that  $vu = 1$  as well. This argument shows that  $L'$  is in fact a division ring. Now the general ring morphism maps  $LX_k A^0$  into  $\text{End}_L(A)$  which is contained in  $\text{End}_L(A)$ . Thus  $\text{End}_L(A) = \text{End}_{L'}(A)$ . A comparison of dimensions (over  $k$ ) shows that  $L' = L$ . ■

We come now to the main structural results of the theory.

**THEOREM 2.20.** *With the same notation as in Theorem 2.18, there exists an  $L$ -basis  $u_\sigma, \dots, u_\tau$ , indexed by the elements of the Galois group of  $L$  over  $k$ , such that for all  $\alpha$  in  $L$  we have  $\alpha^\sigma u_\sigma = u_\sigma \alpha$ . Moreover, each  $u_\sigma$  is invertible in  $A$ , and  $u_\sigma u_\tau = \Gamma_{\sigma, \tau} u_{\sigma\tau}$  for suitable  $\Gamma_{\sigma, \tau}$  in  $L^*$  (the multiplicative group of  $L$ ).*

*Proof.* Let  $\alpha$  be an element of  $L$ , and let  $P_k(x)$  be the minimal polynomial for  $\alpha$  as an element of  $L$  over  $K$ .  $P_k(x)$  splits into distinct linear factors over  $L$ , since  $L$  is a normal, separable extension of  $k$ . Now represent right multiplication of elements of  $A$  by  $\alpha$  as a matrix with entries in  $L$ . Let  $P_L(x)$  be the minimal polynomial for this matrix. Since  $P_k(\alpha) = 0$  it follows that  $P_L(x)$  divides  $P_k(x)$  and so  $P_L(x)$  splits into distinct linear factors. Thus there is an  $L$ -basis for  $A$  relative to which the matrix representation for  $\alpha$  is a diagonal matrix. Since  $L$  is commutative, there is an  $L$ -basis for  $A$  that simultaneously diagonalizes all the elements of  $L$ . Let  $u$  be one of these basis elements. We claim that  $u$  is an invertible element of  $A$ . What we do know about  $u$  is that there is a function  $f: L \rightarrow L$  such that  $f(\alpha)u = u\alpha$  for all  $\alpha$  in  $L$ . This equation says that  $uA$  is a left  $LX_k A^0$  submodule of  $A$ . However,  $LX_k A^0$  is isomorphic to  $\text{End}_L(A)$ , so there are no proper invariant subspaces. Consequently,  $uA = 0$  or  $uA = A$ . Since  $u$  is nonzero, only the second possibility can hold. Thus there is an element  $v$  of  $A$  such that  $uv = 1$ . Since these are matrices, it follows that  $vu = 1$  as well. We have shown that  $f(\alpha) = u\alpha u^{-1}$  for all  $\alpha$  in  $L$ . From this equation it is clear that  $f$  is in fact a  $k$ -automorphism of  $L$ . We next show that there is a one-to-one correspondence between the members of the basis obtained above and the  $k$ -automorphisms of  $L$ . Suppose that  $u$  and  $w$  are two such basis elements and that there is a  $k$ -automorphism  $\sigma$  such that  $\alpha^\sigma = u\alpha u^{-1} = w\alpha w^{-1}$ . From this equation it follows that  $w^{-1}u$  is a member of  $L'$ . However, we know that  $L' = L$ . Consequently  $u$  and  $w$  could not be linearly independent over  $L$ . The final assertion follows because  $u_{\sigma\tau}^{-1}u_\sigma u_\tau$  is in  $L'^*$  and thus in  $L^*$ . ■

**THEOREM 2.21.** *With the same notation as in Theorem 2.18,  $A \approx \text{End}_k(L)$  if and only if  $u_\sigma, \dots, u_\tau$  can be picked in such a way that  $u_\sigma u_\tau = u_{\sigma\tau}$ .*

*Proof.* Suppose first that  $A \approx \text{End}_k(L)$ . Each  $k$ -automorphism of  $L$  is a member of  $\text{End}_k(L)$  and thus of  $A$ . Call the element associated with  $\sigma$  by the name  $u_\sigma$ . Clearly  $u_\sigma u_\tau = u_{\sigma\tau}$ . Conversely suppose that the elements  $u_\sigma$  can be selected so that  $u_\sigma u_\tau = u_{\sigma\tau}$ . Map  $A$  into  $\text{End}_k(L)$  by associating to  $\sum \alpha_\sigma u_\sigma$  the endomorphism that sends  $x$  in  $L$  onto the element  $\sum \alpha_\sigma x_\sigma$ . The hypothesis of the theorem guarantees that this map is a ring morphism. However,  $A$  has no nontrivial two sided ideals (Lemma 2.17), so the map is a monomorphism. A comparison of dimensions over the field  $k$  shows that the map is an isomorphism. ■

**COROLLARY 2.22.** *There are no nontrivial division algebras over a finite field (i.e., all finite division algebras are fields).*

*Proof.* If  $D$  is a finite division algebra with center  $k$ , then  $k$  is a finite field. Since all finite extension fields of  $k$  are cyclic Galois extensions, it follows that  $D$  has a Galois splitting field. Let  $u_1 = 1$ , and pick an arbitrary  $u_\sigma$  for  $\sigma$  equal to the Frobenius automorphism of the splitting field. Let the other elements  $u_\tau$  be powers of  $u_\sigma$  with  $u_\sigma^n$  in  $k$ . Here  $n$  is the degree of the splitting field over  $k$ . However, it is easy to verify that every element of  $k$  is the norm of some element of the splitting field. Thus we can pick  $u_\sigma$  in such a way that  $u_\sigma^n = 1$ . Thus  $D$  is isomorphic to a complete matrix ring and so cannot be a division ring.

## REFERENCES

- 1 Artin et al., *Rings with Minimum Condition*, Univ. of Michigan, Ann Arbor, 1944.
- 2 M. Deuring, *Algebren*, Chelsea, New York, 1948.

*Received 31 July 1987; final manuscript accepted 20 September 1988*