

**Zeitschrift:** L'Enseignement Mathématique  
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique  
**Band:** 20 (1974)  
**Heft:** 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** SOME CLASSICAL THEOREMS ON DIVISION RINGS  
**Autor:** Taylor, D. E.  
**DOI:** <https://doi.org/10.5169/seals-46912>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 12.07.2025

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

# SOME CLASSICAL THEOREMS ON DIVISION RINGS

by D. E. TAYLOR

The theorem of Wedderburn [15] that every finite division ring is a field, and the theorem of Frobenius [6] characterizing the quaternions as a non-commutative real division algebra can both be obtained as immediate and easy consequences of theorems on central simple algebras—particularly the Skolem-Noether theorem (van der Waerden [14, p. 199]). The purpose of this note is to use elementary linear algebra to prove a version of the Skolem-Noether theorem sufficient to yield the results of Wedderburn and Frobenius.

## 1. SOME LINEAR ALGEBRA

All the results of this section are quite elementary and can be found in most texts on linear algebra (for example: Hoffman and Kunze [9]).

Let  $V$  be a vector space over a field  $F$  and let  $T$  be a linear transformation of  $V$ . Suppose that  $f(X)$  is a polynomial with coefficients in  $F$  such that  $f(T) = 0$ . If  $f(X) = f_1(X)f_2(X)$  where  $f_1(X)$  and  $f_2(X)$  are coprime, then there are polynomials  $g_1(X)$  and  $g_2(X)$  such that  $1 = f_1(X)g_1(X) + f_2(X)g_2(X)$ . Then for each  $v$  in  $V$  the vector  $v_1 = f_2(T)g_2(T)v$  belongs to the kernel,  $V_1$ , of  $f_1(T)$ , the vector  $v_2 = f_1(T)g_1(T)v$  belongs to the kernel,  $V_2$ , of  $f_2(T)$  and  $v = v_1 + v_2$ . Thus  $V$  is the (direct) sum of  $V_1$  and  $V_2$ . Moreover, the restriction  $T_i$  of  $T$  to  $V_i$  satisfied the equation  $f_i(T_i) = 0$  for  $i = 1, 2$ .

It follows by induction on the degree that if  $f(X)$  can be factorized over  $F$  into distinct linear factors, then  $V$  is the direct sum of the eigenspaces of  $T$ . Note that  $V$  is not assumed to be finite dimensional.

Recall that the minimal polynomial of  $T$  is the monic polynomial  $m(X)$  of least degree such that  $m(T) = 0$ . It is immediate that each eigenvalue  $\lambda$  of  $T$  satisfies the equation  $m(\lambda) = 0$  and conversely, the above considerations show that each root of  $m(X)$  is an eigenvalue of  $T$ .

## 2. DIVISION RINGS

By *division ring* we mean an associative ring with identity in which every non-zero element has an inverse. If  $D$  is a division ring, the *normalizer*  $N(F)$  of a subfield  $F$  consists of those elements  $d$  such that  $dF = Fd$ , while the *centralizer*  $C(F)$  consists of those elements  $d$  such that  $dx = xd$  for all  $x$  in  $F$ ; the centralizer is a subdivision ring of  $D$ .

From now on  $D$  will denote a division ring with centre  $K$  and  $F$  will denote a maximal subfield of  $D$ . We shall assume that  $F = K(\theta)$  where  $\theta$  satisfies an irreducible monic polynomial  $f$  with coefficients in  $K$  which splits into distinct linear factors over  $F$ . We shall see below that this assumption allows us to apply the results of §1 to  $D$  considered as a vector space over  $F$  (multiplying on the left with elements of  $F$ ). For each element  $a$  of  $D$ , the assignment  $T_a(d) = da$  defines a linear transformation  $T_a$  of this vector space.

If  $d$  is an eigenvector of  $T_\theta$ , then for some  $\lambda$  in  $F$ ,  $d\theta = \lambda d$ . This implies that  $d\theta d^{-1} = \lambda$  and hence  $dFd^{-1} = F$ ; thus  $d \in N(F)$ . Conversely, if  $d \in N(F)$  and  $d \neq 0$ , then  $d\theta d^{-1} = \lambda \in F$  for some  $\lambda$  and hence  $d$  is an eigenvector of  $T_\theta$ . This proves

(2.1) *A non-zero element  $d$  of  $D$  is an eigenvector of  $T_\theta$  if and only if it belongs to  $N(F)$ .*

Since  $f(T_\theta) = 0$ , the conditions of §1 apply and we have

(2.2) *The vector space  $D$  is the direct sum of the eigenspaces of  $T_\theta$ .*

Let  $\lambda$  be an eigenvalue of  $T_\theta$  with eigenvector  $d$ , then as above  $d\theta = \lambda d$ . If  $d'$  is another eigenvector, then  $d'd^{-1}\lambda d d'^{-1} = \lambda$  and  $d'd^{-1}$  centralizes  $F$  since  $F = K(\lambda)$ . However,  $F$  is a maximal subfield, and therefore self-centralizing, so  $d' = ed$  for some  $e$  in  $F$ . Thus we obtain

(2.3) *Each eigenspace of  $T_\theta$  has dimension one.*

Next, we wish to show that  $f(X)$  is the minimal polynomial of  $T_\theta$ . Let  $\theta = \theta_1, \theta_2, \dots, \theta_m$  be the eigenvalues of  $T_\theta$  and let  $1 = d_1, d_2, \dots, d_m$  be corresponding eigenvectors. Because  $N(F)$  is multiplicatively closed  $d_i d_j$  must correspond to an eigenvalue  $\theta_k$ , say, and hence  $d_i d_j \theta = \theta_k d_i d_j$ , which implies that  $d_i \theta_j = \theta_k d_i$ . This shows that the mapping which takes  $\theta_j$  to  $d_i \theta_j d_i^{-1}$  permutes the eigenvalues among themselves. Consequently, the coefficients of  $g(X) = (X - \theta_1) \dots (X - \theta_m)$  commute with all the eigen-

vectors and they therefore belong to the centre of  $D$  since the eigenvectors span  $D$ . Each eigenvalue is a root of  $f(X)$  so the degree of  $g(X)$  is no larger than that of  $f(X)$ . But  $g(\theta) = 0$  so we must have  $g(X) = f(X)$ . Since each  $\theta_i$  must be a root of the minimal polynomial of  $T_\theta$  this proves

(2.4) *The minimal polynomial of  $T_\theta$  is  $f(X)$ .*

As immediate consequences we have

(2.5)  $\dim_F D = \dim_K F = \text{degree of } f = m.$

(2.6)  $\dim_K D = m^2.$

Finally, we prove

(2.7) *If  $E = K(\theta')$  and  $f(\theta') = 0$ , then for some non-zero element  $d$  of  $D$ ,  $d E d^{-1} \subseteq F$ .*

To see this, consider the linear transformation  $T_{\theta'}$ . Since  $f(T_{\theta'}) = 0$  there is an eigenvalue  $\lambda \in F$  of  $T_{\theta'}$  and a corresponding eigenvector  $d$  such that  $d \theta' = \lambda d$ ; it follows that  $d E d^{-1} \subseteq F$ .

*Remark.* The assumption on the field  $F$  amounts to supposing that  $F/K$  is a finite Galois extension and the proof of (2.4) shows that  $N(F)^\# / F^\#$  is isomorphic to its Galois group. (Where  $F^\#$  denotes the set of non-zero elements of  $F$ .)

### 3. WEDDERBURN'S THEOREM

This proof follows van der Waerden [14, p. 203]. The counting argument was used by Artin [1] in his proof of the same theorem.

**THEOREM.** *Every finite division ring is a field.*

*Proof.* Suppose that  $D$  is a finite division ring with centre  $K$  and maximal subfield  $F$ . If the order of  $F$  is  $q$ , then the elements of  $F$  constitute all the roots of the polynomial  $X^q - X$ ; hence any two finite fields of the same order are isomorphic. The multiplicative group of a finite field is cyclic, so  $F = K(\theta)$  for some  $\theta$ . Any element of  $D$  is contained in a maximal subfield, which by (2.5) has the same order as  $F$  and hence by (2.7) any element of the multiplicative group  $G$  of non-zero elements of  $D$  belongs to a conjugate of  $H$ , the multiplicative group of non-zero elements of  $F$ . The

number of conjugates of a subgroup is the index of its normalizer, so  $H$  has at most  $|G : H|$  conjugates in  $G$  and hence the union of the conjugates contains at most  $|G : H| (|H| - 1) + 1 = |G| - |G : H| + 1$  elements. This number is less than  $|G|$  except when  $G = H$ . Hence  $D = F$  is a field.

#### 4. FROBENIUS' THEOREM

Let  $\mathbf{R}$  denote the field of real numbers,  $\mathbf{C}$  the field of complex numbers and  $\mathbf{H}$  the division ring of quaternions. The following proof makes use of the fundamental theorem that every polynomial with coefficients in  $\mathbf{C}$  has a root in  $\mathbf{C}$ .

**THEOREM.** *Let  $D$  be a division ring which contains the real numbers  $\mathbf{R}$  in its centre and suppose that every element of  $D$  satisfies a polynomial with coefficients in  $\mathbf{R}$ . Then  $D$  is isomorphic to one of  $\mathbf{R}$ ,  $\mathbf{C}$  or  $\mathbf{H}$ .*

*Proof.* Suppose that  $D$  is not isomorphic to  $\mathbf{R}$  or  $\mathbf{C}$ . It follows that the maximal subfield  $F$  of  $D$  is isomorphic to  $\mathbf{C}$ , the centre  $K$  of  $D$  is isomorphic to  $\mathbf{R}$  and  $F = K(i)$  where  $i^2 = -1$ . Let  $j$  be an eigenvector of  $T_i$  corresponding to the eigenvalue  $-i$ . Then  $ji = -ij$  and  $j^2$  commutes with  $j$  and  $F$ . From (2.2) and (2.3) the elements 1 and  $j$  form an  $F$ -basis for  $D$  and therefore  $j^2 = \alpha$  belongs to  $K$ . If  $\alpha = \beta^2$  for some  $\beta \in K$  then  $(j - \beta)(j + \beta) = 0$  and  $j$  belongs to  $K$ , which is not the case; hence  $\alpha = -\beta^2$  for some  $\beta \in K$ . Replacing  $j$  by  $j\beta^{-1}$  we obtain a  $K$ -basis 1,  $i$ ,  $j$ ,  $ij$  for  $D$  such that  $i^2 = j^2 = -1$  and  $ij = -ji$ . That is,  $D$  is isomorphic to  $\mathbf{H}$ .

An almost identical argument shows that if the dimension of  $D$  over its centre  $K$  is 4 and the characteristic is not 2, then  $D$  has a  $K$ -basis 1,  $i$ ,  $j$ ,  $ij$  where  $i^2 = \alpha$ ,  $j^2 = \beta$  and  $ij = -ji$  for some  $\alpha, \beta \in K$ .

#### 5. OTHER PROOFS OF WEDDERBURN'S THEOREM

The original proofs of the theorem of §3 were given first by Wedderburn [15] in 1905 and then by Dickson [5] in the same year; they depend on certain divisibility properties of the integers. The neatest proof along these lines is that of Witt [16]. Elementary proofs which avoid the use of such number theory have been given by Artin [1] and Herstein [7]. And

proofs which deduce the theorem using finite group theory have been given by Zassenhaus [17], Brandis [3] and Scott [11, p. 426].

Perhaps the most interesting proofs are those which present the result as a consequence of a more general theory. There are two such proofs in the book of van der Waerden [14]: the first (on p. 203) uses the theory of central simple algebras, the second (sketched on p. 215) relates the theorem to cohomology and the Brauer group (see also, Serre [12, p. 170]). The theorem is also a consequence of the work of Tsen [13] and Chevalley [4]. Further comments on the history of the theorem can be found in an article by Artin [2] and in the book by Herstein [8] where many interesting generalisations are also given. One such generalization is a theorem of Jacobson: a division ring in which  $x^{n(x)} = x$  for all  $x$  is commutative. Laffey [10] has recently given an elementary proof of this using Wedderburn's theorem and linear algebra similar to that used here. See also [18].

#### REFERENCES

- [1] ARTIN, E. Über einen Satz von Herrn J. H. Maclagan-Wedderburn. *Abh. Math. Sem. Univ. Hamburg*, 5 (1928), pp. 245-250.
- [2] ——— The influence of J. H. M. Wedderburn on the development of modern algebra. *Bull. Amer. Math. Soc.*, 56 (1950), pp. 65-72.
- [3] BRANDIS, A. Ein gruppentheoretischer Beweis für die Kommutativität endlicher Divisionringe, *Abh. Math. Sem. Univ. Hamburg*, 26 (1964), pp. 234-236.
- [4] CHEVALLEY, C. Démonstration d'une hypothèse de M. Artin. *Abh. Math. Sem. Univ. Hamburg*, 11 (1936), pp. 73-75.
- [5] DICKSON, L. E. On finite algebras. *Nachr. Ges. Wiss. Göttingen*, (1905), p. 379.
- [6] FROBENIUS, G. Über lineare Substitutionen und bilineare Formen. *Crelle*, 84 (1878), p. 59.
- [7] HERSTEIN, I. N. Wedderburn's theorem and a theorem of Jacobson. *Amer. Math. Monthly*, 68 (1961), pp. 249-251.
- [8] ——— *Noncommutative rings*. Carus Monograph 15, The Mathematical Society of America, 1968.
- [9] HOFFMAN K. and R. KUNZE. *Linear algebra*. Prentice-Hall, Englewood Cliffs, New Jersey, 1971.
- [10] LAFFEY, T. J. Infinite rings with all proper subrings finite. *Amer. Math. Monthly*, 81 (1974), pp. 270-272.
- [11] SCOTT, W. R. *Group theory*. Prentice-Hall, Englewood Cliffs, New Jersey, 1965.
- [12] SERRE, J.-P. *Corps locaux*. Hermann, Paris, 1968.
- [13] TSEN, C. C. Divisionalgebren über Funktionenkörpern. *Nachr. Ges. Wiss. Göttingen* (1933), p. 335.
- [14] van der WAERDEN, B. L. *Modern Algebra, vol. II*. Fredereick Ungar, New York, 1950.
- [15] MACLAGAN-WEDDERBURN, J. H. A theorem on finite algebras. *Trans. Amer. Math. Soc.*, 6 (1905), pp. 349-352.

- [16] WITT, E. Über die Kommutativität endlicher Schiefkörper. *Abh. Math. Sem. Univ. Hamburg*, 8 (1931), p. 433.
- [17] ZASSENHAUS, H. J. A group theoretic proof of a theorem of MacLagen-Wedderburn. *Glasgow Math. J.*, 1 (1952), pp. 53-63.
- [18] NAGAHARA, T. and H. TOMINAGA. Elementary proofs of a theorem of Wedderburn and theorem of Jacobson. *Abh. Math. Sem Univ. Hamburg*, 41 (1974), pp. 72-74.

( Reçu le 28 octobre 1974 )

D. E. Taylor,  
Department of Mathematics  
La Trobe University  
Bundoora  
Victoria, Australia 3083