On Division Algebras

Author(s): J. H. M. Wedderburn

Source: *Transactions of the American Mathematical Society*, Apr., 1921, Vol. 22, No. 2 (Apr., 1921), pp. 129-135

Published by: American Mathematical Society

Stable URL: https://www.jstor.org/stable/1989011

1920

ON DIVISION ALGEBRAS*

BY

J. H. M. WEDDERBURN

§ 1. The object of this paper is to develop some of the simpler properties of division algebras, that is to say, linear associative algebras in which division is possible by any element except zero.

The determination of all such algebras in a given field is one of the most interesting problems in the theory of linear algebras. Early in the development of the subject, Frobenius showed that quaternions and its subalgebras form the only division algebras in the field of real numbers and, with the exception of the single theorem that there is no non-commutative division algebra in a finite field, no further definite result of importance was known till Dickson discovered the algebra referred to in § 4.

It is shown in the present paper that the Dickson algebra is the only non-commutative algebra of order 9 so that the only division algebras of order not greater than 9 are (i) the Dickson algebras of order 4 and 9, (ii) the ordinary commutative fields, (iii) algebras of order 8 which reduce to a Dickson algebra of order 4 when the field is extended to include those elements of the algebra which are commutative with every other element.

§ 2. Lemma 1. *If B is a subalgebra of order b in a division algebra A of order a, there exists a complex C of order c such that*

$$A = BC, \qquad a = bc.$$

Denoting elements of B by y with appropriate suffixes, let x_2 be an element of A which does not lie in B; the order of the complex $B + Bx_2$ is then $2b$ as otherwise there would be a relation of the form $y_1 + y_2 x_2 = 0$, $(y_2 \neq 0)$, which would lead to $x_2 = - y_2^{-1} y_1 < B$. Similarly, if $x_3 \not< B + Bx_2$, the order of $B + Bx_2 + Bx_3$ is $3b$ since otherwise there would be a relation of the form $y_1 + y_2 x_2 + y_3 x_3 = 0$, $(y_3 \neq 0)$, which would lead to

$$x_3 = - y_3^{-1} y_1 - y_3^{-1} y_2 x_2 < B + Bx_2 .$$

Since the basis of A is finite, the truth of the lemma follows by an easy induction.

* Presented to the Society, February 28, 1920.

LEMMA 2. *If a polynomial* $a_0 \xi^n + a_1 \xi^{n-1} + \cdots + a_n$ in a scalar variable ξ is divided on the right and left by $\xi - b$, the remainders are $a_0 b^n + a_1 b^{n-1} + \cdots + a_n$ and $b^n a_0 + b^{n-1} a_1 + \cdots + a_n$ respectively.*

The proof of this lemma is exactly the same as in ordinary algebra, due care being taken to distinguish between multiplication on the right and on the left.

A factor which divides a polynomial on the right (left) will be referred to as a R.F. (L.F.).

LEMMA 3. *If*

$$A = a_0 \xi^m + a_1 \xi^{m-1} + \cdots + a_m$$

and

$$B = b_0 \xi^n + b_1 \xi^{n-1} + \cdots + b_n$$

are polynomials in a scalar variable ξ, there exists a highest common right-hand factor (H.C.R.F.) C_1 and a highest common left-hand factor (H.C.L.F.) C_2 and polynomials L_1, M_1, L_2, M_2 such that

$$L_1 A + M_1 B \equiv C_1, \qquad AL_2 + BM_2 \equiv C_2.$$

If $n \leqq m$, we can, by right-hand division, determine polynomials Q_1 and R_1 in ξ such that $A \equiv Q_1 B + R_1$, where R_1 is of lower degree in ξ than B. Obviously any C.R.F. of B and R_1 is a R.F. of A; we can therefore proceed with the proof exactly as in ordinary algebra.

The theory of linear factors of a polynomial in a scalar variable is by no means so simple as in commutative algebras. Their properties depend mainly on the following considerations. Let $A = BC$ be a polynomial in ξ expressed as the product of two polynomial factors B and C, and suppose that $\xi - x$ is a right factor of A but not of C; we have then $C = Q_1(\xi - x) + R$, where Q_1 is a polynomial and R is independent of ξ and is not zero. Multiplying by B we get $A = BQ_1(\xi - x) + BR$, whence $\xi - x$ is a R.F. of BR so that we can set $BR = Q_2(\xi - x)$ or $B = Q_2 R^{-1}(\xi - RxR^{-1})$, i.e., $\xi - RxR^{-1}$ is a R.F. of B.

A case of some importance arises when the algebra is quadrate i.e., where scalars are the only elements commutative with every element of the algebra, and when $A = 0$ is the reduced equation of this algebra. Regarding these algebras we have the following

LEMMA 4. *If $\phi(x_1) = 0$ is the reduced equation of an element of a quadrate division algebra, then, if p is the degree of ϕ, the scalar polynomial $\phi(\xi)$ can be expressed rationally as the product of p linear factors which may be permuted cyclically.*

Since $\phi(x_1) = 0$, $\xi - x_1$ is both a right and a left factor of $\phi(\xi)$, and so

* Throughout this paper all elements such as a_0, a_1, $\cdots$ are to be considered as belonging to a division algebra unless the contrary is stated explicitly.

is also $\xi - x'$ if x' is any transform of x_1. Let $\phi(\xi) = B(\xi - x_1)$, then, if x' is a transform which is not equal to x_1, we have

$$\phi(\xi) = B(\xi - x_1) = B(\xi - x') + B(x' - x_1);$$

hence, as above, $\xi - x_2 \equiv \xi - (x' - x_1)x'(x' - x_1)^{-1}$ is a R.F. of B. Similarly if $B = B'(\xi - x_2)$, and x'' is a transform of x_1 such that $\xi - x''$ is not a R.F. of $(\xi - x_2)(\xi - x_1)$, we find as above that

$$\xi - x_3 \equiv \xi - Rx''R^{-1}, \qquad R = x''^2 - (x_2 + x_1)x'' + x_2 x_1 \neq 0,$$

is a R.F. of B'; and so on. Continuing this process we get finally

$$\phi(\xi) = C(\xi - x_m)(\xi - x_{m-1}) \cdots (\xi - x_2)(\xi - x_1) \equiv CD \qquad (m \leqq p),$$

where, if y is any transform of x_1, then $\xi - y$ is a R.F. of D. If therefore $D \equiv \xi^m + \alpha_1 \xi^{m-1} + \cdots + \alpha_m$, then

$$y^m + \alpha_1 y^{m-1} + \cdots + \alpha_m = 0 \tag{1}$$

for every transform y of x_1. If the α's are not all scalar, let z be an element which is not commutative with at least one of them and let $\alpha_i' = z\alpha_i z^{-1}$. Since (1) is satisfied by every transform of x_1, it follows that every transform also satisfies

$$y^m + \alpha_1' y^{m-1} + \cdots + \alpha_m' = 0 \tag{2}$$

in which at least one coefficient differs from the corresponding coefficient in (1). Subtracting (1) from (2), we get therefore a new equation of lower degree than m which is not identically zero and which is satisfied by every transform of x_1, say

$$y^q + \beta_1 y^{q-1} + \cdots + \beta_q = 0. \tag{3}$$

If the β's are not all scalars, the degree can again be lowered by a repetition of this process, till finally an equation is reached with scalar coefficients not all zero; we can therefore regard the β's as scalars without loss of generality. Since however the identical equation is irreducible, the left-hand side of (3), with y replaced by ξ must be divisible by $\phi(\xi)$ whence it follows immediately that $\phi \equiv D$ i.e., $m = p$ and

$$\phi(\xi) = (\xi - x_p)(\xi - x_{p-1}) \cdots (\xi - x_1).$$

The linear factors are permutable cyclically since their product is a scalar.

The necessary modifications in the lemma when the algebra is not quadrate, will be obvious after the proof of theorem 1 below.

§ 3. Theorem I. *If its field, F, be suitably extended, any division algebra, A, can be expressed as the direct product of a commutative algebra, B, and a simple matric algebra. B is composed of all elements of A which are commutative with every other element, and its basis may be so chosen as to be rational in F.*

It has been shown elsewhere* that a division algebra, A, of order a, reduces to the direct sum of a number of simple matric algebras when the field is extended by the adjunction of a finite number of suitably chosen algebraic irrationalities. In this extended field, F', we may therefore write

$$A = A_1 + A_2 + \cdots + A_b,$$

where

$$A_i = (e_{pq}^{(i)}) \qquad (p, q = 1, 2, \cdots, a_i;\ \Sigma a_i^2 = a),$$

$$e_{pq}^{(i)} e_{qr}^{(i)} = e_{pr}^{(i)}, \qquad e_{pq}^{(i)} e_{rt}^{(i)} = 0 \quad (q \neq r), \qquad e_{pq}^{(i)} e_{rt}^{(j)} = 0 \qquad (i \neq j).$$

It is then obvious that the algebra, B, whose basis is $e_i = \sum_p e_{pp}^{(i)}$ $(i = 1, 2, \cdots, b)$ is composed of all elements of A which are commutative with every element of A. By expressing the basis of B in terms of any rational basis, any element y of B can be expressed in the form $y = \sum \xi_i x_i$, where the x's are rational elements of A, not all zero, and the ξ's are marks of F' which are linearly independent in F. If now x is any rational element, we have, from the definition of B, $xy = yx$; hence

$$0 = xy - yx = \sum \xi_i (x x_i - x_i x),$$

and therefore, since the ξ's are linearly independent in F, it follows that $x x_i - x_i x = 0$ for every x_i and x. The elements of the subalgebra generated by the elements x_i are therefore commutative with every element of A and this algebra, which is rational, is equivalent to B in F'.

If we extend the field F so as to include the elements of B, we get a new division algebra, A', of order a/b and when this field is again extended, A' reduces to a matric algebra which is simple, as otherwise B would not contain all elements commutative with every element of A. It follows immediately that all the algebras $A_1, A_2, \cdots, A_b$ have the same order a/b and that, in F', A is the direct product of a simple matric algebra C and the commutative algebra B.

If B reduces to the identity, A is said to be quadrate: its order is a square, and scalars are the only elements commutative with every element of the algebra.

THEOREM II. *If a division algebra, A, contains a quadrate subalgebra, B, it can be expressed as the direct product of B and another algebra C.*

If F' is the field F so extended as to render B reducible to the simple matric form, then it is known that A can be expressed as the direct product of B and an algebra C which contains all elements of A which are commutative with every element of B. Any element z of C can be expressed in the form $z = \sum \xi_s x_s$, where the x's are rational elements of A and the ξ's are marks

*Proceedings of the London Mathematical Society, Vol. 6 (1907), p. 102.

of F' which are linearly independent in F. If y is any element of B which is rational in F, then $yz = zy$; whence

$$0 = yz - zy = \sum \xi_s (yx_s - x_s y),$$

so that, as before, $yx_s = x_s y$ for every y of B. Hence the elements x_s belong to C which has therefore a basis rational in F.

THEOREM III. *If A is a quadrate division algebra whose order, p^2, is the square of a prime, then the adjunction to the field F of any irrationality which renders any number of A wholly or partially reducible also reduces A to a matric algebra; or, in any field in which A is not primitive, it is equivalent to a matric algebra.*

This theorem follows immediately from theorem 1 and the theorem that any simple algebra is the direct product of a division algebra and a simple matric algebra, the latter being necessarily of order p^2 since p is a prime.

§ 4. The only types of division algebras hitherto discovered all come under the type described by L. E. Dickson.* These algebras are defined by the relations

$$xy = y\theta(x), \qquad y^n = g,$$

where the identical equation of x is a uniserial Abelian equation of degree n, and g is an element of the field of the coefficients which is not the norm of any rational polynomial in x. The following investigation serves to show the manner in which these algebras arise.

Let x be an element of a division algebra A in a field F, and let the order of the algebra, X, generated by x, be m, then by lemma 1 we can determine a complex $Z = (z_1, z_2, \cdots, z_n)$ such that $A = Xz_1 + Xz_2 + \cdots + Xz_n$, where A is of order mn. Every element y of A can therefore be expressed in the form $y = \sum g_r z_r$ where the g's are polynomials in x, and in particular we may set

$$\begin{aligned} z_1 x &= g_{11} z_1 + g_{12} z_2 + \cdots + g_{1n} z_n \\ z_2 x &= g_{21} z_1 + g_{22} z_2 + \cdots + g_{2n} z_n \\ &\cdots\cdots\cdots\cdots \\ z_n x &= g_{n1} z_1 + g_{n2} z_2 + \cdots + g_{nn} z_n . \end{aligned}$$

If G is the matrix (g_{pq}), whose coefficients lie in the field $F(x)$, these equations may be put in the form

$$(z_1, z_2, \cdots, z_n) x = G(z_1, z_2, \cdots, z_n),$$

and it follows immediately that

$$(z_1, z_2, \cdots, z_n) x^r = G^r (z_1, z_2, \cdots, z_n).$$

* Cf. Dickson, these Transactions, vol. 15 (1914), p. 31, and Wedderburn, ibid., p. 162.

Hence, if $m = n$, the matrix G satisfies the same identical equation as x and in any case G satisfies an equation of degree n whose coefficients may however contain x.*

In the field $F(x)$, x is always a root of this equation, the corresponding invariant axis being the modulus of the algebra. If now the identical equation of G is abelian, its roots are polynomials in x which are rational in F, say $\theta_r(x)$ $(r = 1, 2, \cdots, n;\ \theta_1(x) \equiv x)$, and to each root there corresponds a rational element of the algebra, say y_r, such that

$$y_r x = \theta_r(x) y_r;$$

and this leads to Dickson's algebra when the abelian equation is uniserial.†

§ 5. We shall now show that the Dickson algebra is the only quadrate division algebra of order 9.

Let x_1 be an element of such an algebra which is not commutative with any of its transforms so that its identical equation,

$$f(\xi) \equiv \xi^3 + a_1 \xi^2 + a_2 \xi + a_3 = 0, \tag{4}$$

is not abelian. By lemma 4, we can express $f(\xi)$ in the form

$$f(\xi) = (\xi - x_3)(\xi - x_2)(\xi - x_1)$$

where the factors may be permuted cyclically and no two of the x's are commutative.‡ Since $\xi - x_2$ is a right-hand factor of $f(\xi)$, and

$$x_2 = (x_2 - x_1) x_2 (x_2 - x_1)^{-1}$$

leads to $x_1 x_2 = x_2 x_1$ contrary to our assumption, therefore

$$x_3 = (x_2 x_1 - x_1 x_2) x_2 (x_2 x_1 - x_1 x_2)^{-1} \tag{5}$$

and by symmetry, permuting the suffixes cyclically, also

$$x_2 = (x_1 x_3 - x_3 x_1) x_1 (x_1 x_3 - x_3 x_1)^{-1},$$

$$x_1 = (x_3 x_2 - x_2 x_3) x_3 (x_3 x_2 - x_2 x_3)^{-1}.$$

But, from (4),

$$x_3 x_2 + x_2 x_1 + x_3 x_1 = a_2;$$

hence, permuting cyclically,

$$x_3 x_2 + x_2 x_1 + x_3 x_1 = x_2 x_1 + x_2 x_3 + x_1 x_3 = x_1 x_2 + x_1 x_3 + x_3 x_2,$$

* It can be proved in the same way that, to every element y_i of A, there corresponds a matrix Y_i, whose coefficients are scalar polynomials in x, such that $(z) y_i = Y_i(z)$; and if y_j is a second element of A and Y_j the corresponding matrix, the matrix belonging to $y_j y_i$ is $Y_i Y_j = (Y_j' Y_i')'$.

† I have been unable to construct an algebra of this type which is not also a Dickson algebra i.e., one for which the equation is uniserial, but it appears probable that they exist.

‡ As the roots of $f(\xi)$ are necessarily distinct, any number commutative with x_1 is a scalar polynomial in x_1.

whence

$$x_2 x_1 - x_1 x_2 = x_1 x_3 - x_3 x_1 = x_3 x_2 - x_2 x_3 = y,$$

say, so that from (5)

$$x_1 = y x_3 y^{-1}, \qquad x_2 = y x_1 y^{-1}, \qquad x_3 = y x_2 y^{-1} = y^2 x_1 y^{-2}.$$

Therefore y^3 is commutative with x_1 and, as y is not a polynomial in x_1, it follows that $y^3 = h$ is a scalar. We may then assume that the identical equation of x_1 has the same form, say $x_1^3 = g$.

Let now $z_1 = x_1 y$, $z_2 = x_1 z_1 x_1^{-1} = x_1^2 y x_1^{-1}$, then

$$z_1 z_2 - z_2 z_1 = x_1 y x_1^2 y x_1^{-1} - x_1^2 y^2 = x_1 (y x_1^2 y - x_1 y^2 x_1) x_1^{-1};$$

but, since $x_2 x_1 x_3 = g$, we have $x_2 x_1 = x_3^2$, so that

$$0 = x_2 x_1 - x_3^2 = y x_1 y^{-1} x_1 - y^2 x_1^2 y^{-2} = y (x_1 y^2 x_1 - y x_1^2 y)/h,$$

since $y^3 = h$, and therefore $z_1 z_2 - z_2 z_1 = 0$, i.e., z_2 is a polynomial in z_1 so that the identical equation is a uniserial abelian equation and the algebra is of Dickson's type.

The identical equation of z_1 is easily found as follows:

$$z_1^2 = x_1 y x_1 y = y x_3 y x_3 = y^2 x_2 x_3 = y^2 x_3 x_2 - h,$$

therefore

$$z_1^3 + h z_1 = x_1 y \cdot y^2 x_3 x_2 = h x_1 x_3 x_2 = hg.$$

PRINCETON UNIVERSITY