# A TYPE OF PRIMITIVE ALGEBRA*

BY

J. H. M. WEDDERBURN

In a recent paper,† L. E. Dickson has discussed the linear associative algebra, $A$, defined by the relations

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

where $\theta(x)$ is a polynomial in $x$ which is rational in the field $F$ in which $A$ is defined. In this paper Dickson shows for $n = 2$ and $n = 3$ that, when $\theta$ and $g$ are properly chosen, $A$ is primitive, i. e., every element in it with the exception of zero has an inverse: $A$ is in fact in the case $n = 2$ a direct generalization of quaternions.

So far as I am aware no algebra other than these two and fields has been proved to be primitive; hence it is of considerable interest to find that for any value of $n$, $\theta$ and $g$ can be so chosen as to make Dickson's algebra primitive.

In discussing primitive algebras we may without any real loss of generality assume that any element commutative with every other element of the algebra is a scalar, i. e., an element of the field $F$. For, all such elements generate a commutative subalgebra $B$ and, as in the theory of groups, we can find a complex $C$ for which

$$A = BC = CB.$$

We can therefore regard $A$ as an algebra whose coefficients lie in the field $F$ extended by the elements of the commutative primitive algebra $B$ and, in this algebra, scalars are the only elements commutative with every other element.

A primitive algebra will be called *normal* when reduced in this manner.

It follows from the general theory of linear associative algebras‡ that a normal primitive algebra is of order $n^2$ and that, when the field is sufficiently extended, it is equivalent to the simple matric algebra $e_{pq}$ $(p, q = 1, 2, \cdots, n)$, so that its identical equation is of degree $n$. We shall now investigate the consequences that result from the assumption that the normal primitive

* Presented to the Society, December 31, 1913.

† These Transactions, vol. 15 (1914), pp. 31–46.

‡ See, for instance, my paper in the Proceedings of the London Mathematical Society, ser. 2, vol. 6 (1907), pp. 77–118, where references are given.

algebra $A$ contains an element for which the group of the corresponding identical equation is the cyclic group of order $n$.

1. Let $A$ be a normal primitive algebra of order $n^2$ and let $x$ be an element of it for which the group of the identical equation $f(x) = 0$ is cyclic.

If $\xi_1, \xi_2, \cdots, \xi_n$ are the roots of $x$, the corresponding primitive idempotent elements are

$$e_r \equiv e_{rr} = \frac{(x-\xi_1)\cdots(x-\xi_{r-1})(x-\xi_{r+1})\cdots(x-\xi_n)}{(\xi_r-\xi_1)\cdots(\xi_r-\xi_{r-1})(\xi_r-\xi_{r+1})\cdots(\xi_r-\xi_n)} \qquad (r=1,2,\cdots,n)$$

and* when $F$ is extended by the roots of $x$, $A$ contains a matric† algebra $(e_{pq})$ which does not reduce to $e_1, e_2, \cdots, e_n$, since then $x$ would be commutative with every element of $A$. We may therefore suppose $e_{12} \neq 0$, so that there is an element $y_1$, rational in $F$, for which $e_1 y_1 e_2$ is not zero. The conjugates of $e_1 y_1 e_2$ in $F$ are $e_r y_1 e_{r+1}$ $(r = 1, 2, \cdots, n)$, none of which can therefore be zero.

If we set

$$e_r\, y_1\, e_{r+1} = \eta_{r,\,r+1}\, e_{r,\,r+1},$$

the element

$$y = \sum_{r=1}^{n} \eta_{r,\,r+1}\, e_{r,\,r+1}$$

is rational since it is the sum of the conjugates of $e_1 y_1 e_2$; its $n$th power is evidently the scalar $\eta_{12}\,\eta_{23}\cdots\eta_{n1} = g$, say, which is therefore rational. Since

$$x = \sum_{r=1}^{n} \xi_r\, e_r,$$

$$xy = \sum_{r=1}^{n} \xi_r\, \eta_{r,\,r+1}\, e_{r,\,r+1} = yx_1,$$

where

$$x_1 = \sum_{r=1}^{n} \xi_{r-1}\, e_r.$$

The element $x_1$ is commutative with $x$ and is therefore a rational polynomial in $x$, say $\theta(x)$, since the identical equation, $f(x) = 0$, has no repeated roots. Evidently $x$ and $y$ generate $A$ when expressed in its matric form and therefore also in its rational form.

We have therefore the following

THEOREM. *A normal primitive algebra which contains an element $x$ whose group is cyclic is generated by $x$ and an element $y$ which satisfies the relations*

* See Proceedings of the London Mathematical Society, *l. c.*, p. 97.

† A matric algebra is one for which a basis $(e_{pq})$ can be chosen for which $e_{pq}\, e_{rs} = 0$, $q \neq r$, $e_{pq}\, e_{qr} = e_{pr}$, $\Sigma e_{rr} = 1$. Some of the elements $e_{pq}$ may be zero, but if so the algebra is reducible.

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

*where $\theta(x)$ and $g$ are rational* in the field of the coefficients and $y^n$ is the first power of $y$ which is commutative with $x$.*

Conversely if $x$ and $y$ satisfy these conditions, the group of $x$ is the cyclic group of order $n$. This may be shown as follows.

Since

$$xy = y\theta(x),$$

therefore

$$xy^r = y^r\theta^r(x),$$

where $\theta^r(x)$ denotes the function $\theta$ iterated $r$ times. If $\theta^r(x) = x$, then $y^r$ is commutative with $x$, which is contrary to the given conditions unless $r = n$.

The matric form of $y$ can be considerably simplified by choosing the units $e_{pq}$ in such a way that $\eta_{r,r+1}e_{r,r+1}$ is replaced by $e_{r,r+1}$ for $r=1, 2, \cdots, n-1$, $e_{n1}$ being chosen so that

$$e_{12}e_{23}\cdots e_{n-1,n}e_{n1} = e_{11}.$$

This change in the basis of $(e_{pq})$ leaves $e_{rr}$ $(e = 1, 2, \cdots n)$ unaltered so that $x$ has the same form as before while $y$ becomes

$$y = e_{12} + e_{23} + \cdots + e_{n-1,n} + ge_{n1}.$$

It is easily shown from the forms given above for $x$ and $y$ that any element, $z$, of $A$ can be expressed uniquely in the form

$$y^{n-1}h_0 + y^{n-2}h_1 + \cdots + yh_{n-2} + h_{n-1},$$

where $h_r$ $(r = 0, 1, \cdots, n-1)$ are rational polynomials in $x$.

Now

$$y^r = e_{1,r+1} + e_{2,r+2} + \cdots + e_{n-r,n} + g(e_{n-r+1,1} + \cdots + e_{nr})$$

and

$$y^r x^s = \xi^s_{r+1}e_{1,r+1} + \xi^s_{r+2}e_{1,r+2} + \cdots,$$

so that in the matric form of any element of $A$ all the coefficients to the left of the principal diagonal are multiplied by $g$, and if any particular coefficient is zero all the coefficients in the same diagonal are zero.

2. We shall now determine the conditions which $g$ must satisfy in order that an algebra of Dickson's type shall be primitive.

Let us consider an element of the form

$$z = y^r + y^{r-1}h_1 + \cdots + yh_{r-1} + h_r \qquad (h_r \neq 0)$$

* We may evidently modify $y$ so that $g$ is an algebraic integer of the field.

and let $k_1, k_2, \cdots, k_{n-r}$ be polynomials in $x$ to be determined later, then

$$(y^{n-r} + y^{n-r-1} k_1 + \cdots + k_{n-r})z = g + y^{n-1} h_1 + y^{n-2} h_2 + \cdots + y^{n-r} h_r$$
$$+ y^{n-1} y^{-r} k_1 y^r + y^{n-2} y^{-r+1} k_1 y^{r-1} h_1 + \cdots + y^{n-2} y^{-r} k_2 y^r + \cdots + \cdots .$$

If we put $k_1 = - y^r h_1 y^{-r}$, which is a known rational polynomial in $x$, the coefficient of $y^{n-1}$ is zero. Similarly the coefficient of $y^{n-2}$ vanishes if

$$k_2 = - y k_1 y^{r-1} h_1 y^{-r} - y^r h_2 y^{-r},$$

which is also a known polynomial in $x$, and so on till the coefficient of $y^r$ is reached, after which the process terminates. We can therefore in general determine the $k$'s so that the product commences with a term $y^{r-s} h(x)$ $(s < r)$ and, after multiplying on the right by $1/h(x)$, which exists if $h \neq 0$, we have a number which begins with the term $y^{r-s}$. If this number has an inverse, $z$ will also have one, since, by a well-known theorem on matrices, if a product has an inverse, the same is true of each factor. We have therefore only two types of elements to consider: first, those which may be reduced to the form $y + \varphi(x)$ by repeated applications of the process given above; and second elements for which at some stage the product is independent of $y$.

If $y + \varphi(x)$ is expressed in its matric form, its determinant is easily seen to be

$$\varphi(\xi_1)\, \varphi(\xi_2) \cdots \varphi(\xi_n) - g,$$

so that, if $g$ is not the norm of any rational function of $\xi$, any element of this type has an inverse.

Suppose now that $z$ is an element of the second of the two types mentioned above, so that there exists an element

$$z_1 = y^{n-r} + y^{n-r-1} k_1 + \cdots + k_{n-r},$$

such that $z_1 z$ is independent of $y$. The determination of the coefficients $k_1, \cdots, k_{n-r}$ is wholly independent of $g$, as the transform of any polynomial in $x$ by a power of $y$ depends solely on $\theta(x)$. We may therefore set

$$z_1 z = g + k,$$

where $k$ is independent of $g$, which may be regarded as a variable scalar.

If $k$ is not itself a scalar, $g + k$ certainly has an inverse and therefore $z$ has also. We may assume therefore that $k$ is a scalar, so that the matrix corresponding to $z_1$ differs from the adjoint of the matrix corresponding to $z$ merely by a scalar factor which must be an integral function of $g$ since $z_1$, $z$ and $g + k$ are all integral in $g$. Since the determinant of the adjoint of a matrix is a power of the determinant of that matrix, the determinant of $z$,

say $|z|$, must be a power of $g+k$, and as $|z|$ is obviously of the $r$th degree in $g$, beginning with the term $(-1)^{n-r} g^r$, we have

$$|z| = (-1)^{n-r} (g+k)^r.$$

But, when $g = 0$, $|z|$ becomes the norm of $h_r$ so that

$$(-1)^{n-r} k^r = N(h_r).$$

Unless the scalar $g+k$ is zero, $z$ has an inverse. In the contrary case, $g^r = N(-h_r)$. Hence, *if no power of $g$ less than the $n$th is the norm of a rational polynomial in $x$, every element of the algebra, except zero, has an inverse.**

*The existence of such rational numbers $g$ follows from Satz 33 of Hilbert's *Bericht*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4 (1897), p. 198.