A THEOREM ON FINITE ALGEBRAS*

BY

J. H. MACLAGAN-WEDDERBURN†

FROBENIUS ‡ and C. S. PEIRCE § have shown that, in the domain of all real numbers, the only linear associative algebras every number of which, except zero, possesses an inverse, are quaternions and its subalgebras, and also that in the complex domain no algebra has that property. In the present paper it is shown that the Galois field is the only algebra of this type which possesses a finite number of elements.

§ 1.

Since addition is commutative in a linear associative algebra, it may be shown, as in the Galois field theory,|| that for any number x of the algebra there exists a prime integer p for which p times x is zero and further that p is the same for every x. It follows that, in the group formed by the numbers of the algebra under addition, every element is of period p and therefore the order of the group is of the form p^n where n is some positive integer. The numbers $\neq 0$ of the algebra thus form a group F, of order $p^n - 1$, under the operation of multiplication. The self-conjugate elements of F, together with the zero element, form a Galois field. For, if y_1 and y_2 are self-conjugate elements of F and x is any element,

$$(y_1 + y_2)x = y_1x + y_2x = xy_1 + xy_2 = x(y_1 + y_2),$$

i. e., the self-conjugate elements are closed under addition, as well as under multiplication, and hence with 0 form a Galois field. Since the identity is a self-conjugate element of F this Galois field always exists. If the order of the Galois field is p^m, the order of the subgroup of F, composed of its self-conjugate elements, is of order $p^m - 1$. The subgroup will be denoted by G and the corresponding Galois field by $GF[p^m]$.

Let x_1 be any element $\neq 0$ of the algebra; then there are exactly p^m distinct

* Presented to the Society (Chicago) April 22, 1905. Received for publication April 5, 1905.

† Carnegie Research Scholar (Scotland).

‡ G. FROBENIUS, Crelle, Bd. 84 (1878), p. 59.

§ C. S. PEIRCE, American Journal of Mathematics, vol. 4 (1881), p. 225.

|| As developed, for instance, in Professor DICKSON'S *Linear Groups*, p. 9.

numbers of the form $\xi_1 x_1$, where ξ_1 is a mark of $GF[p^m]$. If x_2 is any element not included in this set, there are p^{2m} distinct numbers of the form $\xi_1 x_1 + \xi_2 x_2$. Similarily if x_3 is any number, which is not of the form $\xi_1 x_1 + \xi_2 x_2$, there are p^{3m} numbers of the form $\xi_1 x_1 + \xi_2 x_2 + \xi_3 x_3$, and so on.

We can evidently enumerate in this way all the numbers of the algebra and hence we can find say s numbers $x_\alpha (\alpha = 1, 2, \cdots, s)$ such that any number x can be expressed uniquely in the form

$$x = \sum_{\alpha=1}^{s} \xi_\alpha x_\alpha$$

where $\xi_\alpha (\alpha = 1, 2, \cdots, s)$ are marks of $GF[p^m]$. The order of F is then $p^{ms} - 1$.

§ 2.

Let x_α be any number of the algebra which does not lie in $GF[p^m]$. Then, if y_1 and y_2 are any two numbers commutative with x_α, $y_1 + y_2$ and $y_1 y_2$ are also commutative with x_α and hence the set of all numbers commutative with x_α forms a subalgebra. The group, formed by the numbers of this algebra under multiplication, will be denoted by F_{x_α}. Since F_{x_α} contains G, we find as in § 1 that its order is of the form $p^{ms_\alpha} - 1$, where s_α is some positive integer. Hence on dividing the elements of F into conjugate classes we get

$$p^n - 1 = p^m - 1 + \sum_{\alpha=1}^{t} k_\alpha \frac{p^n - 1}{p^{ms_\alpha} - 1}. \tag{1}$$

This shows that, if the least common multiple of the $s_\alpha (\alpha = 1, 2, \cdots, t)$ is s', $p^m - 1$ is divisible by $(p^n - 1)/(p^{ms'} - 1)$. Therefore

$$(p^m - 1)(p^{ms'} - 1) = l(p^n - 1).$$

Reducing this modulo p^m we see that l must have the form $kp^m - 1$ $(k > 0)$. Since $ms' \leqq n$, we have $k = 1$ and $ms' = n = ms$.

§ 3.

It follows from the theory of hypercomplex numbers, that there is an equation of lowest degree,

$$f(x) \equiv x^r + a_1 x^{r-1} + a_2 x^{r-2} + \cdots + a_{r-1} = 0, \tag{2}$$

with coefficients in $GF[p^m]$, which is satisfied identically by any given number x of the algebra, irrespective of any special relation between the coördinates of x, except the condition that they lie in $GF[p^m]$. Further, there is at least one element of the algebra which satisfies no similar equation of lower degree. Indeed, (2) states that $x^{r-1}, x^{r-2}, \cdots, x^0$ are linearly independent with respect to

$GF[p^m]$, and the condition of independence can evidently be put in a form which states that certain determinants, whose elements are rational integral functions of the coördinates of x, do not all vanish identically. Hence there must be some set of values of the coördinates for which $x^{r-1}, x^{r-2}, \cdots, x^0$ are independent and hence the particular x so obtained can satisfy no equation of lower degree than r. (2) is called the characteristic or identical equation, while the equation of lowest degree satisfied by a given x is called its reduced* equation.

$f(x)$ is irreducible in $GF[p^m]$; for, were it reducible neither factor would possess an inverse, contrary to our hypotheses. Similarily, the reduced equation of a given number is irreducible.

For any given x all the roots of its characteristic equation $f(x) = 0$ are roots of its reduced equation† $\phi(x) = 0$, both being regarded as ordinary equations in the $GF[p^m]$, and therefore, since $\phi(x)$ is irreducible, $f(x)$ is a power of $\phi(x)$ and the degree of the reduced equation is a divisor of r.

We now assume that F_{x_a} is abelian for every x_a which does not lie in the $GF[p^m]$. It is shown below that the general case can be made to depend on this simpler one. Under this assumption F_{x_a} is the multiplicative group of a Galois field and is therefore cyclic.‡ If x_a is chosen as the generator of F_{x_a} and if s_a is the degree of the reduced equation of x_a, there are exactly $p^{ms_a} - 1$ different rational functions of x with coefficients in $GF[p^m]$; hence the order of F_{x_a} is $p^{ms_a} - 1$. Now it was shown above that, for some x_a, $s_a = r$ and also that each s_a is a factor of r. Hence r is the least common multiple of $s_1, s_2, \cdots$ and therefore $r = s$. But $ms = n$. Hence F_{x_a} is identical with F, i. e., the algebra is a Galois field.

Suppose now that F is not abelian. Then for some x, not contained in G, F_x is not abelian. Similarly there must be some element of F_x, which is not self-conjugate in F_x and is such that the group of those elements of F_x which are commutative with it, is not abelian; and so on. We could then deduce in this way a series of groups of decreasing order, no member of the series being abelian. This is however impossible since each group of necessity contains G and the order of F is finite. Hence F must be abelian.

§ 4.

The same result can be deduced as follows without the aid of the theory of the characteristic equation. It was shown in § 2 that, if F is not a field, its elements can be arranged in subgroups the orders of whose multiplicative groups

* FROBENIUS, loc. cit.

† Cf. FROBENIUS, loc. cit.; E. WEYR, Monatshefte für Mathematik und Physik, vol. 1 (1890), p. 163.

‡ Cf. DICKSON, loc. cit., p. 13.

are of the form $p^{ms_a} - 1$. It follows then from SYLOW's theorem, that every prime divisor of $p^n - 1$ is also a divisor of some $p^{ms_a} - 1$ ($ms_a < n$). This is however only possible in the following two cases:* (i) $p = 2$, $n = 6$; (ii) $p = 2^k - 1$, $n = 2$.

In case (i) we have $m = 1$ since the only divisors of n are 2 and 3, which are relatively prime, hence from (1), § 2,

$$2^6 - 1 = 1 + x_1 \frac{2^6 - 1}{2^3 - 1} + x_2 \frac{2^6 - 1}{2^2 - 1}$$

where x_1 and x_2 are integers not both zero. This gives $62 = 9x_1 + 21x_2$, an equation which cannot be satisfied by integers. Hence this case cannot occur. Case (ii) is evidently inadmissable since $n = 2$ is a prime.

§ 5.

The following proof is perhaps more direct. If all the elements of the algebra are multiplied successively by any one element except zero it is easily seen from the distributive law that they are permuted among themselves in such a way as to leave their additive relations unchanged, i. e., each such operation gives an isomorphism of the additive group with itself.† It follows that in the group of isomorphisms of the additive group there are two subgroups simply isomorphic with the multiplicative group; namely, one obtained by left and the other by right handed multiplication.

Each operation of one of these subgroups is commutative with every operation of the other, and it is easily seen that their greatest common subgroup corresponds to the set of the self-conjugate elements of F and is therefore of order $p^m - 1$. These two subgroups then generate a subgroup of order $(p^n - 1)^2/(p^m - 1)$ of the group of isomorphisms. Since the additive group is an abelian group of type $(1, 1, \cdots, 1)$, its group of isomorphisms is the general linear homogeneous group $GLH(n, p)$ of order $(p^n - 1)(p^n - p)\cdots(p^n - p^{n-1})$, an expression which is divisible by $(p^n - 1)^2/(p^m - 1)$ only in the two special cases mentioned above, unless $m = n$. Having excluded these two cases above, we must have $m = n$. Therefore F is abelian.‡

THE UNIVERSITY OF CHICAGO,
March 31, 1905.

* BIRKHOFF and VANDIVER, *On the Integral Divisors of* $a^n - b^n$, Annals of Mathematics, vol. 5 (1904), p. 177; L. E. DICKSON, *On the Cyclotomic Function*, American Mathematical Monthly, April, 1905.

† I am indebted to Professor E. H. MOORE for calling my attention to this point of view.

‡ Professor DICKSON has deduced the same result from the theory of canonical forms.