ON HYPERCOMPLEX NUMBERS

By J. H. MACLAGAN WEDDERBURN.

(*Communicated by* W. BURNSIDE.)

[Received July 7th, 1907.—Read November 14th, 1907.]

INDEX OF TERMS.

THE object of this paper is in the first place to set the theory of hypercomplex numbers on a rational basis. The methods usually employed in treating the parts of the subject here taken up are, as a

rule, dependent on the theory of the characteristic equation, and are for this reason often valid only for a particular field or class of fields. Such, for instance, are the methods used by Cartan in his fundamental and far-reaching memoir, *Sur les groupes bilinéaires et les systèmes complexes*. It is true that the methods there used are often capable of generalisation to any field; but I do not think that this is by any means always the case.

My object throughout has been to develop a treatment analogous to that which has been so successful in the theory of finite groups. An instrument towards this lay to hand in the calculus developed by Frobenius, and used by him with great effect in the theory of groups. This calculus is, with slight additions, equally applicable to the theory of hypercomplex number-systems, or, as they will be called below, algebras. Although a short account of this calculus has already been given, it was thought advisable to give a more detailed account in the present paper.

A word or two on the nomenclature adopted will perhaps not be out of place. At Professor Dickson's suggestion I have used the word *algebra* as equivalent to Peirce's *linear associative algebra* which is too long for convenient use. An algebra which is composed of only a part of the elements (or numbers) of an algebra is called a *sub-algebra* of that algebra. It is assumed throughout that a finite basis can be chosen for any algebra which is under discussion, that is, we suppose that it is always possible to find a finite number of elements of the algebra which are linearly independent with regard to some given field, and are such that any other number of the algebra can be linearly expressed in terms of them. This excludes from the present paper an interesting class of algebras which I hope to discuss in a subsequent communication.

Most of the results contained in the present paper have already been given, chiefly by Cartan and Frobenius, for algebras whose coefficients lie in the field of rational numbers; and it is probable that many of the methods used by these authors are capable of direct generalisation to any field. It is hoped, however, that the methods of the present paper are, in themselves and apart from the novelty of the results, sufficiently interesting to justify its publication.

The greater part of Sections 1, 2, 4–6 was read in the Mathematical Seminar of the University of Chicago early in 1905, and owe much to Professor Moore's helpful criticism.

A list of memoirs referred to is given at the end of the paper, and these memoirs are quoted throughout by their number in this list.

1. *The Calculus of Complexes.*

The definition of the term *algebra* or *hypercomplex number-system* is now so well known that it is unnecessary to give here a formal set of postulates.*

Let $x_1, x_2, \ldots, x_n$ be a set of elements which are linearly independent in a given field F. The set of all elements of the form

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

the ξ's being any marks of F, is said to form an *algebra*, if

(i.) $\Sigma \xi_r x_r + \Sigma \xi'_r x_r = \Sigma (\xi_r + \xi'_r) x_r$.

(ii.) The product of any two x's is linearly dependent on $x_1, x_2, \ldots, x_n$ in F, in such a way that the multiplication so defined is associative.

(iii.) For any three elements x, y, z of the algebra

$$x(y+z) = xy+xz, \qquad (y+z)x = yx+zx.$$

The algebra is said to be of order n with respect to F. In what follows the term " linearly independent " will always be understood to be with respect to a given field F which is supposed to be constant throughout but otherwise arbitrary.

The *complex* $A = x_1, x_2, \ldots, x_a$ is defined as the set of all quantities linearly dependent on $x_1, x_2, \ldots, x_a$. The greatest number of linearly independent elements which can be simultaneously chosen, is called the *order* of the complex.

If A and B are two complexes, the complex formed by all elements of A and B and those linearly dependent on them, is called the *sum* of A and B, and is denoted by $A+B$. The operation of addition so defined is evidently associative and commutative.

If a complex B is contained in a complex A, we write $B < A$ or $A > B$. Similarly, if x is an element of a complex A, we write $x < A$. This amounts to representing a complex of order one by one of its elements, and will be found to lead to no confusion if certain obvious precautions are observed.

If $B < A$, we can always find C such that $B+C = A$. C is called the *supplement* of B with regard to A. It is obviously not uniquely

* The reader is referred to the following papers on this subject :—Dickson 2, 3.

determined, but if $B+C' = B+C$, any element of C' can be expressed as the sum of an element of B and an element of C. This is conveniently denoted by writing $C' = C \pmod{B}$.

The elements common to two complexes evidently also form a complex. The greatest complex common to A and B is denoted by $A \frown B$. Thus the statement that A and B have no element in common is equivalent to $A \frown B = 0$.

If A and B are any two complexes, and if x and y are any elements of A and B respectively, the complex of elements of the form xy and those linearly dependent on them, is called the *product* of A and B and is written AB. For instance, if $A = x_1, x_2 \ldots x_a$ and $B = y_1, y_2 \ldots y_b$, then

$$AB = \ldots, x_r y_s, \ldots \quad (r = 1, 2, \ldots, a\,;\ s = 1, 2, \ldots, b).$$

AB of course is not in general the same as BA. The operation of multiplication so defined is associative, and it is also distributive with regard to addition.

The following is a summary of the laws of the calculus described above:—

(i.) $A+B = B+A.$

(ii.) $A+(B+C) = (A+B)+C.$

(iii.) $A\,.\,BC = AB\,.\,C.$

(iv.) $A\,(B+C) = AB+AC, \quad (B+C)\,A = BA+CA.$

(v.) $A \frown (B \frown C) = (A \frown B) \frown C.$

(vi.) $A \frown B = B \frown A.$

(vii.) $A\,(B \frown C) \leqslant AB \frown AC.$

Integral powers of a complex are defined by the methods usually employed in hypercomplex numbers, *e.g.*, $A\,.\,A^m = A^{m+1} = A^m\,.\,A$. A necessary and sufficient condition that a complex A be an algebra is then obviously $A^2 \leqslant A$.

The above definitions will perhaps be made clearer by a special example. Consider the algebra (quaternions) formed by four units e_0, e_1, e_2, e_3, where

$$e_r e_s = -e_s e_r \quad (r, s \neq 0),$$

$$e_0 e_r = e_r \quad \text{and} \quad -e_0^2 = e_1^2 = e_2^2 = e_3^2 = -e_0.$$

If Greek letters are used to denote marks of the given field, elements of he form $\xi e_0 + \xi_1 e_1$ form a complex $A = e_0, e_1$. If $B = e_1, e_2$, then

$A \frown B = e_1$; we have also $A^2 = A$ and $B^2 = e_0, e_1, e_2, e_3 = A$. Again,

$$AB = B^2 = A \quad \text{and} \quad B(A \frown B) = e_0, e_2,$$

but

$$BA \frown B^2 = B^2 > B(A \frown B).$$

2. *The Theory of Invariant Sub-algebras.*

A sub-complex B of a complex A, which is such that $AB \leqslant B$ and $BA \leqslant B$, is called an *invariant** sub-complex of A. If B is contained in no other sub-complex of A which has this property, it is said to be maximal. B is necessarily an algebra, since $B^2 \leqslant BA \leqslant B$. An algebra which has no invariant sub-complex is said to be *simple.*†

The theory of invariant sub-algebras is of great importance, as will be seen in the succeeding sections. As most of the present section has already appeared elsewhere‡ it is given here in a somewhat condensed form.

THEOREM 1.—*If $AB \leqslant B$ and $A^2 \leqslant A$, either $BA = A$ or BA is an invariant sub-algebra of A.*

For $BA.A \leqslant BA$ and $A.BA \leqslant BA$. This theorem is frequently applied in the sequel.

We may also notice that $B+BA$ is also an invariant sub-algebra, unless it is identical with A.

THEOREM 2.—*If B_1 and B_2 are invariant sub-algebras of an algebra A, B_1+B_2 is also an invariant sub-algebra, unless $A = B_1+B_2$*

For

$$A(B_1+B_2) = AB_1+AB_2 \leqslant B_1+B_2,$$

$$(B_1+B_2)A = B_1A+B_2A \leqslant B_1+B_2.$$

COROLLARY.—If B_1 is maximal, then either $A = B_1+B_2$ or $B_2 < B_1$. Hence, if B_1 and B_2 are two different maximal invariant sub-algebras, we must necessarily have $B_1+B_2 = A$.

THEOREM 3.—*If B is an invariant sub-algebra of an algebra A, a new algebra can be derived from A by regarding as identical those elements of A which differ only by an element of B.*§

* Molien (10); Frobenius (6), p. 523; Cartan (1), p. 57.

† Cartan (1), p. 57.

‡ Epsteen and Maclagan Wedderburn (5).

§ This fundamental theorem is due to Molien.

The set of elements defined by regarding as identical those elements of A which differ only by an element of B, is evidently closed under the operations of addition and multiplication, and the distributive law holds. The only law that is not evidently satisfied is the associative law for multiplication. This law is shown to hold as follows.

Let $A = B+C$, and let elements of B and C be respectively denoted by x and y with subscripts attached. If, then, y_p, y_q and y_r are any three elements of C,

$$y_p \cdot y_q y_r = y_p (y_{qr}+x_{qr}) = y_p y_{qr} \pmod{B},$$

since $y_p x_{qr} < B$. Similarly,

$$y_p y_q \cdot y_r = (y_{pq}+x_{pq}) y_r = y_{pq} y_r \pmod{B};$$

therefore, since $$y_p \cdot y_q y_r = y_p y_q \cdot y_r,$$

we have $$y_p y_{qr} = y_{pq} y_r \pmod{B},$$

which shows that multiplication is associative.

The algebra defined in this way is called the *difference* algebra of A and B, and, on the analogy of the symbolism used for the quotient group in the theory of finite groups, it is conveniently denoted by $(A-B)$. $(A-B)$ is said to *accompany* A and to be *complementary** to B.

THEOREM 4.—*If B_1 and B_2 are invariant sub-algebras of an algebra A, and $B_1 > B_2$, $(A-B_2)$ has an invariant sub-algebra which is simply isomorphic with (B_1-B_2) and conversely.*

To show this, let $$A = B_1+C, \quad B_1 \frown C = 0,$$

$$B_1 = B_2+D, \quad B_2 \frown D = 0;$$

then $$A = B_2+D+C.$$

If D' is the complex of $(A-B_2)$, which corresponds to D, we have

$$(A-B_2) D' \leqslant D',$$

since $$(D+C) D \leqslant D \pmod{B_2}.$$

Similarly $$D' (A-B_2) \leqslant D'.$$

Now D' is derived from D by regarding those elements as equal which differ only by an element of B_2. Hence

$$D' \equiv (B_1-B_2).$$

---

* Molien (10), p. 92; Frobenius (6), p. 523.

Conversely, if $(A-B_2)$ has an invariant sub-algebra D', and if, as before, D is a complex of A which corresponds to D', then since

$$AD \leqslant D \pmod{B_2},$$

we have $$A(B_2+D) \leqslant B_2+D, \quad (B_2+D)A \leqslant B_2+D.$$

Hence B_2+D is an invariant sub-algebra of A.

COROLLARY.—An immediate consequence of this theorem is that $(A-B)$ is simple, if B is a maximal invariant sub-algebra.

THEOREM 5.—*If B_1 and B_2 are two different maximal invariant sub-algebras of an algebra A, then $D = B_1 \frown B_2$ is a maximal invariant sub-algebra of both B_1 and B_2. Further $(A-B_1)$ and $(A-B_2)$ are simply isomorphic with (B_2-D) and (B_1-D) respectively.*

Let $$B_1 = D+C_2, \qquad B_2 = D+C_1,$$

where $$D \frown C_1 = 0, \qquad D \frown C_2 = 0;$$

and therefore, since

$$D = B_1 \frown B_2 \quad \text{and} \quad A = B_1+B_2,$$

$$A = D+C_1+C_2, \quad C_1 \frown C_2 = 0.$$

If we denote simple isomorphism* by the symbol $\sim$, we have

$$(A-B_1) \sim C_1 \pmod{B_1},$$

and $$(B_2-D) \sim C_1 \pmod{D}, \qquad \sim C_1 \pmod{B_1},$$

since $C_1 < B_1$, and therefore any two elements of C_1 which are equal modulo B_1, are also equal modulo D. We have therefore

$$(A-B_1) \sim (B_2-D),$$

i.e., (B_2-D) is simple since $(A-B_1)$ is simple. Hence D is a maximal invariant sub-algebra of B_2. In exactly the same way it can be shown that it is a maximal invariant sub-algebra of B_2, and

$$(A-B_2) \sim (B_1-D).$$

If $A_1, A_2, \ldots, A_r$ is a series of algebras such that A_r is a maximal invariant sub-algebra of A_{r-1}, the series is called a *composition* series of A_1. The series $(A_1-A_2), (A_2-A_3), \ldots, (A_{r-1}-A_r), \ldots$ is said to be a *difference* series of A_1. An algebra can of course have many composition series.

* *I.e.*, isomorphism with regard both to addition and multiplication.

Let (i.) $A_1, A_2, A_3, \ldots,$ (ii.) $A_1, B_1, B_2, \ldots,$

be two composition series of A for which $A_2 \neq B_1$. Then, if $A_2 \frown B_1 = D$,

(iii.) $A_1, A_2, D, D_1, \ldots,$ (iv.) $A_1, B_1, D, D_1, \ldots,$

where $D, D_1, \ldots$ is a difference series for D, are two composition series for A_1, and, by Theorem 5, the corresponding differences are identical apart from the order of their terms. If we now assume that all possible difference series of the same algebra are equivalent for all algebras of order less than the order of A, (i.) and (ii.) are respectively equivalent to (iii.) and (iv.) and hence to each other. For algebras of one unit, there is only one difference series possible, hence we have by induction the following theorem.

THEOREM 6.—*Any two difference series of the same algebra are identical apart from the order of their terms.*

If in forming the series $A_1, A_2, \ldots$ we make each term the largest sub-algebra of the preceding algebra which is an invariant sub-algebra of A_1, the corresponding difference series is called a *principal* difference series. It can be shown by a method analogous to that used above, that the principal series is also independent of the particular composition series from which it is formed.

3. *Reducibility.*

If an algebra A is expressible as the sum of two algebras A_1 and A_2, which are such that $A_1A_2 = 0 = A_2A_1$, A is said to be *reducible*, and to be the *direct* sum of A_1 and A_2. It was in this sense that the word sum was first used by Scheffers. To avoid circumlocution, we shall in this section call A_1 an *integral* sub-algebra of A, if there is another sub-algebra A_2 such that $A = A_1 + A_2$, and $A_1A_2 = 0 = A_2A_1$. This term is not used except in this section. An integral sub-algebra is always invariant.

THEOREM 7.—*If B is an invariant sub-algebra of A, and both A and B have a modulus,* then A is reducible.*

Let $A = B + C', \quad B \frown C' = 0,$

* An algebra is said to have a modulus e, if e is an element such that $ex = x = xe$ for every element x of A.

and let e and e_1 be the moduli of A and B respectively, then

$$C \equiv (e-e_1)\, C'\, (e-e_1) = C' \pmod{B},$$

and

$$(e-e_1)\, B = 0 = B\,(e-e_1),$$

since, if $y < B$, then $ey = y = e_1 y$. Hence $BC = 0 = CB$; and $C^2 = C$, since $A^2 = A$. $e-e_1$ is evidently the modulus of C.

COROLLARY.—If B is an integral sub-algebra of A and both A and B have a modulus, A is expressible uniquely as the direct sum of B and an algebra C. For e and e_1 being as above, we have

$$C = (e-e_1)\, A\, (e-e_1).$$

THEOREM 8.—*If A_1 and A_2 are two different maximal integral sub-algebras of A, then $A = A_1+A_2$.*

Let $A = A_1+B_1$, $A_1B_1 = 0 = B_1A_1$, $A_1 \frown B_1 = 0$,

$= A_2+B_2$, $A_2B_2 = 0 = B_2A_2$, $A_2 \frown B_2 = 0$.

Every element of A_2 can be expressed in the form $x+y$, where $x < A_1$ and $y < B_1$, and the complex of y's so defined forms a sub-algebra C_2 of B_1 which does not vanish.

Similarly, any element of B_2 can be expressed in the form $x+y$, the y's defining a sub-algebra D_2 of B_1. But

$$A_1B_1 = B_1A_1 = 0 = A_2B_2 = B_2A_2;$$

therefore

$$C_2D_2 = 0 = D_2C_2.$$

Now $A = A_2+B_2$ and $A_1 \frown B_1 = 0$, hence we must have

$$B_1 = C_2+D_2.$$

But, since A_1 is maximal, B_1 must be irreducible; from which there results $D_2 = 0$. Hence B_2 is contained in A_1 and $A = A_1+A_2$. It follows also that B_1 is an integral sub-algebra of A_2. For, if the elements of A_2 are expressed in the form $x+y$ as before, the x's compose a sub-algebra D of A_1, which is also a sub-algebra of A_2, since the y's have been shown to be elements of A_2. Since

$$A_2 = D+B_1 \quad \text{and} \quad A_1 \frown B_1 = 0,$$

we must evidently have

$$D = A_1 \frown A_2.$$

If $A_1, A_2, \ldots$ be a series of algebras such that A_r is a maximal integral sub-algebra of A_{r-1}, the series (A_1-A_2), (A_2-A_3), ... is said to

form a *reduction* series of A_1. It then follows exactly as in Theorem 6, that—

THEOREM 9.—*Any two reduction series of an algebra are identical except as regards the order of their terms.**

There are evidently sub-algebras of the given algebra which are isomorphic with the terms of the reduction series, but, as Hölder has noticed, these sub-algebras are not in general uniquely defined. The following theorem is a slight extension of one by Scheffers† dealing with this point.

THEOREM 10.—*An algebra A can be uniquely expressed as the direct sum of irreducible algebras which have each a modulus, and an algebra which has no modulus.*

Let $$A = B+C, \quad BC = 0 = CB, \quad B \frown C = 0,$$

where B has a modulus e_1, and C has (1) no modulus, (2) no integral sub-algebra which has a modulus. A has then no integral sub-algebra which contains B, and at the same time has a modulus.

We can form an algebra A' by adjoining a modulus e' to the basis of A; and if e_1 is the modulus of B, and

$$C' = C+(e'-e_1),$$

then
$$\begin{aligned} A' &= B+(e'-e_1)\,C'\,(e'-e_1) \\ &= B+C'. \end{aligned}$$

Hence C', and therefore C, is unique for a given B by Theorem 7. Suppose there is another algebra B_1 satisfying the same conditions as B. As in Theorem 8, we can express B_1 as the direct sum of two algebras $B_2 < B$ and $C_2 < C$, where B_2 and C_2 have both moduli, unless one is zero, seeing that B has a modulus. Now

$$B_1 \leqslant AB_1 = BB_2+CC_2;$$

therefore $CC_2 = C_2$, and similarly $C_2C = C_2$; and therefore C_2 is an integral sub-algebra of C which has a modulus, contrary to the conditions previously laid down for C. Hence we must have $C_2 = 0$, from which it follows that $B = B_1$, *i.e.*, B is unique.

Let
$$\begin{aligned} B &= B_1+B_2+\ldots+B_n, \qquad (1) \\ &= B_1'+B_2'+\ldots+B_m', \end{aligned}$$

* Epsteen (4), p. 444.

† Scheffers (13).

be two expressions of B as the direct sum of irreducible algebras. From Theorem 9 we have $m = n$. Again, since B has a modulus, we have

$$B'_p = BB'_pB = \sum_{r,s} B_rB'_pB_s = \sum_r B_rB'_pB_r,$$

remembering that $B_rB'_pB_s$ $(r \neq s)$ is contained in both B_r and B_s, and that $B_r \frown B_s = 0$. But, since B'_p is irreducible, $B_rB'_pB_r$ must vanish except for some particular value r_p of r which is necessarily different for each value of p. We may therefore, by rearranging the terms, set $r_p = p$. But $B_pB'_pB_p = B_p$, since B_p is invariant. Hence $B_p = B'_p$.

4. *Nilpotent Algebras.*

It was mentioned in § 1 that a necessary and sufficient condition, that a complex A shall be an algebra, is that $A^2 \leqslant A$. If A has a modulus, *i.e.*, an element e such that $ex = x = xe$ for any element x of A, we must evidently have $A^2 = A$. In general, since we are dealing only with algebras which have a finite basis, we must have $A^{\alpha+1} = A^\alpha$ for some integer α. The smallest integer α for which this is the case is called the *index** of the algebra. For instance, in the algebra whose multiplication table is

	e_1	e_2
e_1	e_2	e_2
e_2	e_2	e_2

we find $A^2 = e_2 = A^3$. Hence its index is 2.

It may, of course, happen that some power of A vanishes as in the algebra

	e_1	e_2
e_1	e_2	0
e_2	0	0

where $A^3 = 0$.

If for some integer α, $A^\alpha = 0$, A is said to be *nilpotent*. Nilpotent algebras are of great importance in the discussion of the structure of algebras.

THEOREM 11.—*If α is the index of A, the elements of A can be divided into $\alpha-1$ complexes $B_1, B_2, \ldots, B_{\alpha-1}$, such that*

$$B_pB_q \leqslant B_{p+q} + B_{p+q+1} + \ldots + B_{\alpha-1},$$

* The index might also be suitably defined as the least integer α for which $(A^\alpha)^2 = A^\alpha$.

i.e., such that the product of two elements, belonging to complexes with subscripts p and q respectively, lies entirely in the sum of the complexes with subscripts greater than $p+q-1$.

For let $$A = B_1+A^2 = B_1+B_2+A^3 = \dots$$
$$= B_1+B_2+\dots+B_{\alpha-1},$$

where $$A^\beta = B_\beta+A^{\beta+1}, \quad A^{\alpha-1} = B_{\alpha-1};$$

then $$B_p B_q \leqslant A^p A^q \leqslant A^{p+q},$$

which proves the theorem.

This theorem is evidently considerably stronger than the similar theorems enunciated by Scheffers* and others.

COROLLARY.—Since $A = B_1+A^2$, we have on squaring
$$A^2 = B_1^2+B_1A^2+A^2B_1+A^4 = B_1^2+A^3;$$

hence $$B_1^2 = B_2 \pmod{A^3},$$

and similarly $$B_1^n = B_n \pmod{A^{n+1}}.$$

From this we readily derive the interesting result
$$A = B_1+B_1^2+\dots+B_1^{\alpha-1}+A^\alpha.$$

If $A^\alpha = 0$ is zero, A is said to be generated by B_1. In this case A is reducible if B_1 is reducible, and conversely.

If α is the index of a nilpotent algebra, we have $A^{\alpha-1} \neq 0$, $A^\alpha = 0$; and hence the product of any element of A and any element of $A^{\alpha-1}$ is zero. This is a simple proof of a theorem by Cartan† to the effect that there is at least one element in a nilpotent algebra whose product with any other element is zero. It must be noticed, however, the above definition of a nilpotent algebra is not verbally identical with Cartan's. The identity of the two definitions will be shown in the next section.

An algebra in which the product of any two elements is zero, may be called a *zero-algebra*. For example, if $A^2 < A$, A^2 is an invariant sub-algebra of A, and $(A-A^2)$ is a zero algebra. Let $A = B+A^2$, where

$$B = y_1, y_2, \dots, y_m, \quad A^2 = x_1, x_2, \dots, x_n,$$

and $m+n$ is the order of A. $A' = y_2, y_3, \dots, y_m, x_1, \dots, x_n$ is evidently

---

* Scheffers (12).

† Cartan (1), p. 31.

an invariant sub-algebra of A, such that $(A-A')$ is a zero algebra of order 1. This gives the following theorem regarding the difference series of such an algebra.

THEOREM 12.—*If a is the index of an algebra A, and if the difference of the orders of A and A^a is n, the difference series of A can be so arranged that the first n terms are zero algebras of order* 1.

The following theorem also simplifies the study of the difference series considerably.

THEOREM 13.—*If N is a maximal nilpotent invariant sub-algebra of an algebra A, all other nilpotent invariant sub-algebras of A are contained in N.*

Let N_1 be any nilpotent invariant sub-algebra of A, then, by Theorem 2, $N+N_1$ is also an invariant sub-algebra of A. It is, however, nilpotent. For, if $N_2 = N \frown N_1$, then

$$(N+N_1)^2 \leqslant N^2+N_2+N_1^2,$$

since $NN_1 \leqslant N_2$ and $N_1N \leqslant N_2$. Similarly,

$$(N+N_1)^a \leqslant N^a+N_1^a+N_2,$$

whence, if a is greater than the indices of N and N_1,

$$(N+N_1)^a \leqslant N_2.$$

But N_2 is nilpotent and therefore also $N+N_1$. Hence, since N is maximal, we must have $N_1 \leqslant N$.

An immediate deduction from this theorem is that $(A-N)$ has no nilpotent sub-algebra. This theorem is very important, its importance lying in the fact that, in studying the difference series, it enables us to confine our attention to algebras which have no nilpotent invariant sub-algebra. Such algebras are called *semi-simple.*

5. *Potent Algebras.*

An algebra which is not nilpotent is called a *potent* algebra. If the index of a potent algebra is a, the index of A^a is 1. It is therefore sufficient in many investigations to consider only algebras with unit index.

Let A be an algebra such that $A^2 = A$. There will in general be some complex $C < A$, such that $AC = A$. In fact, if A has a modulus e, it is possible to find elements x, such that $Ax = A$. Let us suppose,

however, that $Ax_1 < A$ for every $x_1 < A$. Again, suppose that $Ax_1x_2 < Ax_1$ for every $x_2 < Ax_1$, and so on. We thus derive a series of algebras each one containing the preceding one, and, as we are dealing with algebras with a finite basis, this process must terminate at some stage. This may happen in either of two ways. After, say $r-1$ steps, we must find either

$$Ax_1x_2 \dots x_{r-1}x_r = 0 \tag{1}$$

for every $x_r < Ax_1x_2 \dots x_{r-1}$, or

$$Ax_1x_2 \dots x_{r-1}x_r = Ax_1x_2 \dots x_{r-1} \tag{2}$$

for some $x_r < Ax_1x_2 \dots x_{r-1}$. In the first case, if $B = Ax_1x_2 \dots x_{r-1}A$, then

$$B^2 \leqslant (Ax_1x_2 \dots x_{r-1})^2 A = 0,$$

and $AB \leqslant B$, $BA \leqslant B$, *i.e.*, B is an invariant sub-algebra of A, unless $B = 0$ when $Ax_1 \dots x_{r-1}$ is an invariant sub-algebra of A. The first case then cannot arise if A is simple.

In the second case, if $A' = Ax_1 \dots x_{r-1}$, there is an element x, such that $A'x = A'$. Hence every element of A' can be put in the form $y = zx$. Here z is unique. For were $zx = z'x$, then $(z-z')x = 0$, and the order* of the basis of $A'x$ would be less than the order of the basis of A'. In particular we have $x = yx$, hence $yx = y^2x$ and therefore $y = y^2$. Such an element is said to be *idempotent*, and the result we have obtained may be stated in the form that a simple algebra always contains an idempotent element. By means of this result we can now establish the following important theorem:—

THEOREM 14.—*Every potent algebra contains an idempotent element.*

For, let B be a maximal invariant sub-algebra of A^a, where $A^{a+1} = A^a$. $(A^a - B)$ is simple and has 1 as its index.† A has therefore a non-nilpotent element x, namely any element which corresponds to an idempotent element of the simple algebra $(A^a - B)$ Now for some value of n, we must have

$$Ax^{2n+1} = Ax^n,$$

for otherwise we should have

$$A > Ax > Ax^3 > \dots > Ax^n > Ax^{2n+1} > \dots,$$

---

* In other words, if $e_1, e_2, \dots, e_a$ is a basis of A, $e_1x, e_2x, \dots, e_ax$ are necessarily independent if $Ax = A$.

† Since, if $A^a = B + C$, then $B + C^2 = A^{2a} = A^a = B + C$, and therefore $C = C^2 \pmod{B}$.

which as before is impossible. Ax^n, and *a fortiori* A, must therefore contain an idempotent element.*

The converse of this theorem is that an algebra, every one of whose elements is nilpotent, is itself nilpotent. This shows that the definition of a nilpotent algebra which was given in § 4, is identical with the one given by Cartan and others.

COROLLARY.—If x is nilpotent, then $Ax < A$.

The following extension of a theorem due to Peirce,† is easily deduced from the results obtained above.

THEOREM 15.—*If an algebra A possesses only one idempotent element e, every element which does not possess an inverse‡ with respect to e, is nilpotent.*

This is shown as follows. If for a given x there is no y, such that $xy = e$, the same is true of all elements of the form xz. For were $xzz' = e$, it would suffice to put $y = zz'$. It follows that e is not contained in xA, which is therefore nilpotent by Theorem 14. Hence $x^n = 0$ for some integer n.

An obvious corollary to this theorem is that if an algebra A contains only one idempotent element e and no nilpotent element, then every element possesses an inverse with respect to e. Further, e is the modulus of A. For, since $Ae = A$, every element x can be put in the form $x = ye$, and hence $xe = x$. Similarly $ex = x$. Such an algebra is said to be *primitive*. Also, if e is the only idempotent element of an algebra A, which is contained in eAe, e is said to be a *primitive idempotent* element of A.

THEOREM 16.—*Every algebra A, which does not possess a modulus, has a nilpotent invariant sub-algebra.*

If A is nilpotent, the theorem is obvious, and it may therefore be assumed that this is not the case. Under this assumption A has at least one idempotent element e_1. If $Ae_1 < A$, there must be elements x such that $xe_1 = 0$. All such elements form a sub-algebra B_1 of A; because, if $x_1e_1 = 0$, $x_2e_1 = 0$, then $(x_1+x_2)e_1 = 0$ and $x_1x_2e_1 = 0$. Let $A = B_1+C$,

* In most proofs of this theorem, the idempotent element which is found, is in general irrational. This objection does not apply to the proof given by Hawkes (7), p. 320.

† Peirce (11), p. 112.

‡ x is said to possess an inverse with respect to e, if there exist elements x_1 and x_2, such that $xx_1 = e = x_2x$.

where $B_1 \frown C = 0$. C can be chosen so that $Ce_1 = C$. For

$$Ce_1 \leqslant C \pmod{B_1},$$

and, if

$$Ce_1 < C \pmod{B_1},$$

there would be an element x of C such that $xe_1 < B$, which is impossible since $B_1 e_1 = 0$ and $xe_1 \neq 0$. $Ce_1 = Ae_1$ can therefore take the place of C, and $Ce_1 . e_1 = Ce_1$.

We have then $$A = B_1 + Ae_1, \quad B_1 e_1 = 0, \tag{1}$$

and similarly $$A = B_2 + e_1 A, \quad e_1 B_2 = 0. \tag{2}$$

From (1) follows $$e_1 A = e_1 B_1 + e_1 A e_1, \tag{3}$$

and, from (2), $$Ae_1 = B_2 e_1 + e_1 A e_1. \tag{4}$$

Now $e_1 B_1 \frown B_2 e_2 = 0$, since $B_1 e_1 = 0$ and $e_1 B_2 = 0$, hence

$$e_1 A \frown Ae_1 = e_1 A e_1,$$

and if $B = B_1 \frown B_2$, we find similarly that

$$B_1 = B + e_1 B_1, \qquad B_2 = B + B_2 e_1.$$

Hence, from (2) and (3),

$$A = B + e_1 B_1 + B_2 e_2 + e_1 A e_1.$$

If B is not nilpotent, it contains an idempotent element e_2, such that $e_1 e_2 = 0 = e_2 e_1$, $e_1 + e_2$ is then also idempotent and may take the place of e_1 in the above discussion.

Again, if e_1 is not primitive, $e_1 A e_1$ can be broken up in the same manner as A, and so, by repeated application of this process, A can be expressed in the form

$$\begin{aligned} A &= B + eB_1 + B_2 e + eAe \\ &= B + \Sigma e_p B_1 + \Sigma B_2 e_p + \Sigma e_p A e_q, \end{aligned} \tag{5}$$

where

$$B^\beta = 0, \quad B_1 = B + eB_1, \quad B_2 = B + B_2 e, \quad e = \Sigma e_p, \quad e_p e_q = 0 \quad (p \neq q),$$

and e_p $(p = 1, 2, \ldots, r)$ are primitive idempotent elements of A. This form is due to Peirce.* e is called a *principal* idempotent of A. If A has a modulus, it is evidently the only principal idempotent element. Hence two principal idempotent elements differ only by an element of the maximal invariant nilpotent sub-algebra.

* Peirce (11), p. 109.

If A has a modulus e', B_1 and B_2 are zero, and $e = e'$. For

$$(e'-e)^2 = e'-e \quad \text{and} \quad (e'-e)\,e = 0 = e\,(e'-e).$$

Hence $e'-e < B$, and is therefore zero.

In (5), B_1B_2 is nilpotent. For, from (5),

$$B_1A = B_1B_2 = AB_2,$$

and
$$B_2B_1 \leqslant B, \quad B^a = 0,$$

hence
$$(B_1A)^{a+1} \leqslant B_1B^aB_2 = 0.$$

But
$$AB_1A = A\,.\,AB_2 \leqslant AB_2 \leqslant B_1A,$$
$$B_1A\,.\,A \leqslant B_1A.$$

Hence $B_1A = B_1B_2$ is a nilpotent invariant sub-algebra of A. If $B_1B_2 = 0$, then

$$(B_1+B_2)^2 = B_2B_1 \leqslant B,$$
$$A\,(B_1+B_2) \leqslant AB_1 \leqslant B_1+B_2.$$
$$(B_1+B_2)\,A \leqslant B_2A \leqslant B_1+B_2 \quad \text{and} \quad B_1+B_2 \neq 0,$$

unless A has a modulus. Hence, if an algebra has no modulus, it has a nilpotent invariant sub-algebra.

COROLLARY 1.—B_1 and B_2 are also nilpotent. For suppose $y^2 = y$, $y < B_1$. y can be expressed in the form $y = y_1+y_2$, where $y_1 < B$, $y_2 < eB_1$, and therefore $y_2^2 = y_1y_2 = 0$. It follows, then, that

$$y_1^2 = (y-y_2)^2 = y-yy_2-y_2y+y_2^2$$
$$= y_1+y_2-y_2y_1.$$

But $eB_1B \leqslant eB_1$ and $B^2 \leqslant B$; hence we must have

$$y_1^2 = y_1, \qquad y_2 = y_2y_1,$$

which is impossible, since B, and therefore y_1, is nilpotent. Hence B_1 and B_2 are nilpotent.

COROLLARY 2.—Unless $eB_1B_2e = 0$, it is a nilpotent invariant sub-algebra of eAe.

COROLLARY 3.—If the index of A is 1, then $B = B_2eB_1$, and conversely. For from $A^2 = A$ we deduce

$$B = B^2+B_2eB_1 = B^2+C \text{ (say)}.$$

If $B^n = 0$, then
$$B = B^{n-1}C+B^{n-2}C+\ldots+C.$$

But $BC \leqslant C$; hence $B = C$, and

$$A = B_2eB_1 + eB_1 + B_2e + eAe.$$

If A has no modulus, it is always possible to add one to the algebra. Let e' be the added modulus and let $e_0 = e' - e$; then

$$A = e'Ae' = e_0Be_0 + eB_1e_0 + e_0B_2e + eAe.$$

This form will be of use later.

Algebras which have no nilpotent invariant sub-algebra form a very important class. Such algebras are called *semi-simple.** A semi-simple algebra always has a modulus.

THEOREM 17.—*A semi-simple algebra, which is not simple, is reducible.*

Let A be the algebra and B an invariant sub-algebra. A, having no nilpotent invariant sub-algebra, has a modulus. Hence $AB = B = BA$. If B has no modulus, it has a nilpotent invariant sub-algebra N. BNB is a nilpotent invariant sub-algebra of A and is therefore zero, seeing that A is semi-simple. Also ANA is an invariant sub-algebra of A which is contained in B, and, since A has a modulus, it is not zero unless N is zero. Now, since $ANA \leqslant B$, we have

$$(ANA)^3 = ANA.N.ANA \leqslant BNB = 0.$$

Hence $N = 0$ and B has a modulus, and, by Theorem 13, A is reducible. It follows immediately that A can be expressed in the form

$$A = A_1 + A_2 + \ldots + A_n,$$

where

$$A_pA_q = 0 = A_qA_p \quad (p \neq q)$$

and

$$A_p \quad (p = 1, 2, \ldots, n)$$

are simple. A is therefore the direct sum of $A_1, A_2, \ldots, A_n$.

THEOREM 18.—*If e is an idempotent element of a semi-simple algebra A, then eAe is semi-simple.*

If eAe is not semi-simple, it must necessarily have a nilpotent sub-algebra N. Then ANA is an invariant sub-algebra of A which is not zero. Also $ANA \neq A$, since

$$eANAe = eAeNeAe = N < eAe.$$

Hence, if A is simple the theorem is proved. The main theorem can now be made to depend on this particular case, since any semi-simple algebra

* Cartan (1), p. 57.

can be expressed as the direct sum of simple algebras. The following proof is more direct and also more comprehensive. Let e' be the modulus of A. If, then, $e_1 = e' - e$, we have $ee_1 = 0 = e_1 e$; and therefore

$$e_1 N = 0 = N e_1. \tag{1}$$

We have also $$A = eAe + e_1 Ae + eAe_1 + e_1 Ae. \tag{2}$$

From (1) and (2), it follows that

$$\begin{aligned} ANA &= eAeNeAe + eAeNeAe_1 + e_1 AeNeAe + e_1 AeNeAe_1 \\ &= N + NAe_1 + e_1 AN + e_1 ANAe_1, \end{aligned}$$

and $$\begin{aligned} (ANA)^2 &= ANANA = A(N^2 + N^2 Ae) \\ &= N^2 + e_1 AN^2 + N^2 Ae_1 + e_1 AN^2 Ae_1 = AN^2 A. \end{aligned}$$

Similarly $$(ANA)^3 = AN^3 A,$$

and so on. Hence ANA is nilpotent and therefore $N = 0$, since A is semi-simple.

COROLLARY.—If in the above theorem e is primitive, eAe is also primitive.

6. *The Classification of Potent Algebras.*

This section is chiefly concerned with the classification of semi-simple algebras. The result is, however, incomplete in so far as the classification is given in terms of primitive algebras which have themselves not yet been classified. At the same time, a considerable step is made towards the classification of non-nilpotent algebras in general.

Let e_p $(p = 1, 2, \ldots, n)$ be a set of primitive idempotent elements of A, which are so chosen that $e = \sum_{p=1}^{n} e_p$ is a principal idempotent element of A, and $e_p e_q = 0$ $(p \neq q)$. This was shown to be possible in the proof of Theorem 16, where it was also shown that A can be expressed in the form

$$A = B + eB_1 + B_2 e + eAe, \qquad eAe = \sum_{p,q} e_p A e_q.$$

The algebras $e_p A e_q$ occur so frequently in the sequel that the following notation is convenient, viz.,

$$e_p A e_q = A_{pq}, \qquad (e_p + e_q) A (e_r + e_s) = A_{p+q,\, r+s},$$

and so on. It is also convenient to denote elements of A_{pq} by x_{pq}, y_{pq}, ...

THEOREM 19.—*If A is simple, $A_{pq} \neq 0$ for any p and q; and if semi-simple, but not simple, then $A_{pq} = 0$ entails $A_{qp} = 0$.*

Suppose that $A_{pq} = 0$, then

$$A_{p+q,\,p+q}\,A_{qp} = (A_{pp}+A_{qp}+A_{qq})\,A_{qp} \leqslant A_{qp},$$

$$A_{qp}A_{p+q,\,p+q} \leqslant A_{qp}.$$

Hence A_{qp} is a nilpotent invariant sub-algebra of $A_{p+q,\,p+q}$, and is therefore zero by Theorem 18. This proves the second part of the theorem. To prove the first part, we observe that, if $e' = e_p+e_q$, A_{pp} is an invariant sub-algebra of $A_{p+q,\,p+q} = e'Ae'$ when $A_{pq} = 0 = A_{qp}$. But $AA_{pp}A \neq A$, since*

$$e'AA_{pp}Ae' = e'Ae'A_{pp}e'Ae' \leqslant A_{pp} < A_{p+q,\,p+q};$$

and therefore $AA_{pp}A$ is an invariant sub-algebra of A. Hence we cannot have $A_{pq} = 0$, if A is simple.

THEOREM 20.—*If A is simple, then $A_{pq}A_{qr} = A_{pr}$, and the order of A_{pq} is the same for all values of p and q.*†

Let $$A' = A_{pq}A_{qp}.$$

From the definition of A_{pp}, we have

$$A' = e_pA'e_p \leqslant A_{pp}.$$

But $$A'A_{pp} \leqslant A' \quad \text{and} \quad A_{pp}A' \leqslant A'.$$

Therefore, either A' is identical with A_{pp} or it is zero. If it is zero, then also $A_{qp}A_{pq} = 0$. For, were $A_{qp}A_{pq} = A_{qq}$, we should have

$$A_{qq}^2 = A_{qp}.A_{pq}A_{qp}.A_{pq} = 0,$$

which is impossible, since A_{qq} is primitive. If $A' = 0$, then

$$A_{p+q,\,p+q}\,A_{pq} = (A_{pp}+A_{pq}+A_{qp}+A_{qq})\,A_{pq} \leqslant A_{pq},$$

$$A_{pq}A_{p+q,\,p+q} \leqslant A_{pq},$$

which is impossible by Theorem 18, since A is simple and A_{pq} is nilpotent.

Hence $$A_{pq}A_{qp} = A_{pp}. \tag{1}$$

Again, since

$$(A_{pp}+A_{pq}+A_{qp}+A_{qq})^2 = A_{p+q,\,p+q}^2 = A_{p+q,\,p+q} = A_{pp}+A_{pq}+A_{qp}+A_{qq},$$

---

* Cf. the proof of Theorem 18.

† Cartan (1), p. 50.

on multiplying on the left by e_p and on the right by e_q, we get

$$A_{pp}A_{pq}+A_{pq}A_{qq}=A_{pq}.$$

But $$A_{pp}A_{pq}=A_{pq}A_{qp}A_{pq}=A_{pq}A_{qq}$$

by (1); hence $$A_{pp}A_{pq}=A_{pq}=A_{pq}A_{qq}, \tag{2}$$

and, finally, from (1) and (2),

$$A_{pq}A_{qr}=A_{pr}A_{rq}A_{qr}=A_{pr}A_{rr}=A_{pr}.$$

It will now be shown that, if x_{pq} and x_{qr} are any elements, not zero, of A_{pq} and A_{qr} respectively, then $x_{pq}x_{qr}\neq 0$.

If $x_{pq}x_{qr}=0$, then $x_{pq}x_{qr}A_{rq}=0$. But $x_{qr}A_{rq}\leqslant A_{qq}$, which is primitive; and therefore for any* y_{rq} such that $x_{qr}y_{rq}\neq 0$, there is an x_{qq}, such that $x_{qr}y_{rq}x_{qq}=e_q$. Hence, as $x_{pq}\neq 0$, $x_{pq}x_{qr}A_{rq}=0$ entails $x_{qr}A_{rq}=0$. It follows for any x_{rq} that $x_{qr}x_{rq}=0$; therefore, as above, $x_{rq}A_{qr}=0$; and, as this is true for any x_{rq}, we must have $A_{rq}A_{qr}=0$ in contradiction to the first part of the theorem. Hence $x_{pq}x_{qr}\neq 0$ for any x_{pq} and x_{qr}, and, since $x_{pq}A_{qr}\leqslant A_{pr}$ and $x_{qp}A_{pr}\leqslant A_{qr}$, we have evidently $x_{pq}A_{qr}=A_{pr}$, from which the second part of the theorem follows immediately.

COROLLARY.—For any $x_{pq}\neq 0$, there is an x_{qp} such that $x_{pq}x_{qp}=e_p$. This is evident from the relation $x_{pq}A_{qp}=A_{pp}$.

THEOREM 21.—*If A is simple, it is possible to find a set of n^2 elements e_{pq} $(p, q = 1, 2, \ldots, n)$ such that $e_{pq}e_{qr}=e_{pr}$ and $e_{pq}e_{rs}=0$ $(q\neq r)$; and $e=\Sigma e_{rr}$ is the modulus of A.*†

Let $e_{pp}=e_p$ $(p=1, 2, \ldots, n)$. By the corollary to the previous theorem, we can find for any $x_{pq}\neq 0$ an x_{qp} such that $x_{pq}x_{qp}=e_{pp}$. Forming the square of $x_{qp}x_{pq}$, we get

$$x_{qp}x_{pq}x_{qp}x_{pq}=x_{qp}e_px_{pq}=x_{qp}x_{pq};$$

therefore, since e_q is primitive,

$$x_{qp}x_{pq}=e_q=e_{qq}.$$

It is therefore possible to find an algebra of order 4 which has the required laws of combination. Suppose that m^2 elements e_{pq} $(p, q = 1, 2, \ldots, m)$

---

* As previously stated, x_{pq}, y_{pq}, ... will be used to denote elements of A_{pq}.

† Molien (10), p. 124; Cartan (1), p. 46; Frobenius (6), p. 527; Shaw (14), p. 275.

have been found which satisfy these laws, and let $e_{1,\,m+1}$ be any element of $A_{1,\,m+1}$. There is then an element $e_{m+1,\,1}$ of $A_{m+1,\,1}$ such that

$$e_{1,\,m+1}\,e_{m+1,\,1} = e_{11} = e_1.$$

Let

$$\left.\begin{aligned} e_{p1}\,e_{1,\,m+1} &= e_{p,\,m+1} \\ e_{m+1,\,1}\,e_{1p} &= e_{m+1,\,p} \end{aligned}\right\} \quad (p = 1, 2, \ldots, m).$$

Together with the previous m^2 elements and $e_{m+1,\,m+1}$, these form an algebra of $(m+1)^2$ elements satisfying the given laws; for

$$e_{pq}\,e_{q,\,m+1} = e_{pq}\,e_{q1}\,e_{1,\,m+1} = e_{p1}\,e_{1,\,m+1} = e_{p,\,m+1},$$

and similarly

$$e_{p,\,m+1}\,e_{m+1,\,r} = e_{pr}.$$

By induction it is therefore possible to find n^2 such elements.

This form of algebra we shall call a *simple* or *quadrate matric* algebra of order n^2.* When a semi-simple algebra is expressed as the sum of simple matric algebras, it is said to be a *matric* algebra.

In accordance with the corollary of Theorem 20, we have

$$A_{pp} = A_{p1}\,e_{1p} = e_{p1}\,A_{11}\,e_{1p}.$$

This gives a 1, 1-correspondence between the elements of the algebras A_{pp} and A_{11}, which is obviously preserved under the operations of addition and multiplication—*i.e.*, the two algebras are simply isomorphic. More generally,

$$A_{pq} = e_{p1}\,A_{11}\,e_{1q},$$

which establishes a 1, 1-relation between the elements of A_{pq} and A_{11}. Let x_{11} be any element of A_{11}, and let the element x_{pq} of A_{pq}, which is associated with it by the above relation, be denoted by

$$x_{pq} = \{x_{11},\, e_{pq}\}.$$

Then

$$x_{pq} = \{x_{11},\, e_{pq}\} = e_{p1}\,x_{11}\,e_{1q}.$$

Similarly, if $y_{rs} < A_{rs}$, we may write

$$y_{rs} = \{y_{11},\, e_{rs}\} = e_{r1}\,y_{11}\,e_{1s},$$

if y_{11} corresponds to y_{rs}. This form of relation is preserved under addition and multiplication, since

$$x_{pq}+y_{pq} = e_{p1}\,(x_{11}+y_{11})\,e_{1q} = \{(x_{pq}+y_{pq}),\, e_{pq}\},$$

$$x_{pq}\,y_{rs} = e_{p1}\,x_{11}\,e_{1q}\,e_{r1}\,y_{11}\,e_{1s}$$

$$= \begin{cases} 0 \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & (q \neq r), \\ e_{p1}\,x_{11}\,y_{11}\,e_{1s} = \{x_{11}\,y_{11},\, e_{pq}\,e_{qr}\} = \{x_{11}\,y_{11},\, e_{pr}\} & (q = r). \end{cases}$$

* The algebra is also said to be of degree n. Cartan calls this type of algebra a quaternion.

This result can be expressed as follows. If C is an algebra simply isomorphic with A_{11}, and D is a simple matric algebra of order n^2; and if every element of C is commutative with every element of D; then $A = CD$. In general, if C and D are any algebras such that every element of the one is commutative with every element of the other, and if the order of the complex $A = CD$ is the product of the orders of C and D, then A is an algebra which is called the *direct product** of C and D. The final result can therefore be stated as follows.

THEOREM 22.—*Any simple algebra can be expressed as the direct product of a primitive algebra and a simple matric algebra.*†

Since semi-simple algebras can be reduced to the direct sum of several simple algebras, Theorem 22 amounts to a determination of the form of all semi-simple algebras.

THEOREM 23.—*The direct product A of a primitive algebra B and a quadrate matric algebra C is simple; and any element which is commutative with every other element of A is an element of B.*

Let the basis of C be e_{pq} ($p, q = 1, 2, \ldots, n$), $e_p = e_{pp}$ ($p = 1, 2, \ldots, n$) being a primitive set of idempotent elements. If D is any invariant sub-algebra, then $e_{pp} D e_{qq} \leqslant D$, and is not zero for some value of p and q unless $D = 0$. But every element of $e_{pp} D e_{qq}$ is the product of e_{pq} and an element of B; and if $x < B$, then $Bx = B = xB$. Hence $Be_{pq} \leqslant D$.

We have, however,

$$Be_{pq} e_{qr} = Be_{pr}, \qquad e_{sp} Be_{pr} \equiv e_{sp} e_{pr} B = e_{sr} B,$$

for every value of s and r. This gives $A = D$, which proves the first part of the theorem.

---

* Scheffers used the term "product" in this sense. As this term is used in this paper in a different sense, I employ the term "direct product," which is used in the theory of groups in a similar sense. Cf. § 11.

† Cartan (1), p. 67, gives this form of a simple algebra in the field of all real numbers, apparently without observing that his result is capable of this simple description.

The theorem may also be proved as follows. If $x < A$, then

$$x = \Sigma x_{pq} \equiv \Sigma e_p x e_q,$$

$$x_{pq} = e_{pq} \sum_r e_{rp} x e_{qr} = \sum_r e_{rp} x e_{qr} \cdot e_{pq},$$

since

$$e_{rp} x e_{qr} = e_{rp} x_{pq} e_{qr}.$$

This method is fully developed in (9), where it is shown that, if B is any matric sub-algebra of A, which has the same modulus as A, then A can be expressed as the direct product of B and some other algebra C.

Again, if x is any element which is commutative with every element of A, then $x = \sum_{r,s} x_{rs} e_{rs}$, where $x_{rs} < B$. But $e_{pq} x = x e_{pq}$; hence

$$\sum_r x_{rp} e_{rq} = x e_{pq} = e_{pq} x = \sum_s x_{qs} e_{ps};$$

therefore $x_{rs} = 0$ $(r \neq s)$ and $x_{pp} = x_{qq}$, *i.e.*, x is an element of B.

This theorem is the converse of the preceding one.

COROLLARY.—The only element of a quadrate matric algebra which is commutative with every other element is the modulus.

THEOREM 24.—*If N is a maximal nilpotent invariant sub-algebra of an algebra A which possesses a modulus, and if $(A-N)$ is simple, then A can be expressed as the direct product of a simple matric algebra and an algebra which contains only one idempotent element.*

From Theorem 22, we have

$$A_{pq} A_{qp} = A_{pp} \pmod{N}.$$

Now $$A_{pp} A_{pq} A_{qp} \leqslant A_{pq} A_{qp}, \qquad A_{pq} A_{qp} A_{pp} \leqslant A_{pq} A_{qp}.$$

Hence, as any invariant sub-algebra of A_{pp} is necessarily nilpotent, we must have $A_{pq} A_{qp} = A_{pp}$. In particular, $A_{pp}^2 = A_{pp}$, and since, when $p = q$, the proof does not assume that e_p is primitive, we also have

$$A_{p+q,\,p+q}^2 = A_{p+q,\,p+q}.$$

It may now be proved, as in Theorem 20, that $A_{pq} A_{qr} = A_{pr}$. If x_{pq} is an element of A_{pq} which is not contained in N_{pq}, then $x_{pq} A_{qr} = A_{pr}$. The proof of this is almost exactly as it is given in the proof of Theorem 20, and it is therefore only necessary to give it very briefly. If $x_{pq} A_{qr} < A_{pr}$, there must be some x_{qr} such that $x_{pq} x_{qr} = 0$. But, by Theorem 20, there is an x_{qp} such that $x_{qq} = x_{qp} x_{pq}$ is not zero, and therefore has an inverse, y_{qq}, with respect to e_q. Hence

$$x_{qr} = e_q x_{qr} = y_{qq} x_{qq} x_{qr} = y_{qq} x_{qp} x_{pq} x_{qr} = 0;$$

and therefore $x_{pq} A_{qr} = A_{pr}$. An important consequence of this is that, for any x_{pq} which is not contained in N_{pq}, there is an x_{qp} such that

$$x_{pq} x_{qp} = e_p.$$

It can now be proved, exactly as in Theorems 21 and 22, that A contains a simple matric sub-algebra, and that it can be expressed as the direct product of this matric algebra and an algebra containing only one idempotent element.

It is possible at this point to state Cartan's main theorem regarding

the classification of algebras in the field of ordinary complex or real numbers, if use is made of the fact that, in the latter field, quaternions is the only primitive algebra; and in the former the algebra of one idempotent unit. The result for an arbitrary field seems much more difficult to obtain, the difficulties centring round the proof of the theorem that an algebra with only one idempotent element can be expressed as the sum of a primitive and a nilpotent algebra; a theorem which is obvious in the above two special cases. The proof given in the next section is rather long, but much additional information is obtained in the course of the work.

7. *The Identical Equation.*

This section is not intended as a development of the theory of the identical equation, and so only those points are dealt with which are of importance from our present point of view.

If x is any element of an algebra A, which has a finite basis, the algebra generated by x, being a sub-algebra of A, must itself have a finite basis. x therefore satisfies a relation of the form

$$x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n=0, \tag{1}$$

where $a_1, a_2, \ldots, a_n$ are marks of the given field, and a_n is to be taken as zero, if the algebra has no modulus, and otherwise as the product of the modulus and a mark of the field. If $x_1, x_2, \ldots, x_a$ is a basis of A and $x=\Sigma\xi_r x_r$, the r-th power of x can be expressed in the form

$$x^r=\Sigma\xi_s^{(r)}x_s,$$

where $\xi_s^{(r)}$ is a rational integral function of the ξ's; hence not more than a powers of x can be independent, and x satisfies an equation of the form (1), where $a_1, a_2, \ldots, a_n$ are now rational integral functions of the ξ's. This equation being an identity in the ξ's, there must be an equation of this form of lowest degree which is satisfied by x whatever values are assigned to the ξ's. This equation is called the *identical* or *characteristic* equation of the algebra. For particular values of the ξ's, x may satisfy an equation of lower degree; but there is evidently at least one x which satisfies no equation of lower degree. The equation of lowest degree satisfied by a particular x has been called by Frobenius the *reduced* equation of that element.

The characteristic of the identical equation will be denoted by $f(x)$, or by $f_x(x)$ where it is desirable to emphasise the fact that the coefficients are functions of x.

If N is the maximal nilpotent invariant sub-algebra of A, a being its index, and if $g(x) = 0$ is the identical equation of $(A-N)$, then $g(x) < N$. if $x < A$, and hence

$$\{g(x)\}^a = 0.$$

$\{g(x)\}^a$ is therefore divisible by $f(x)$. It may, of course, happen that $g(x) = f(x)$, as in the algebra

	e_1	e_2	e_3	e_4
e_1	e_1	0	e_3	0
e_2	0	e_2	0	e_4
e_3	0	e_3	0	0
e_4	e_4	0	0	0

where $$x^2-(\xi_1+\xi_2)x+\xi_1\xi_2 = 0,$$

if $$x = \xi_1 e_1+\xi_2 e_2+\xi_3 e_3+\xi_4 e_4.$$

In a primitive algebra, $f(x)$ is irreducible; for otherwise the product of two rational elements would be zero. An immediate consequence of this is that, if the given field is so extended that every equation is soluble, the only primitive algebra in the extended field is the algebra of one unit, $e = e^2$.

THEOREM 25.—*If A is an algebra which is semi-simple in a given field F, and if F' is another field containing F, then A is also semi-simple in F'.**

Since a semi-simple algebra is the direct sum of a number of simple algebras and a simple algebra can be expressed as the direct product of a matric and a primitive algebra, it is sufficient to consider the latter type of algebra.

Let the identical equation of the primitive algebra A be

$$f(x) = x^n+a_1x^{n-1}+\ldots+a_n = 0. \tag{1}$$

If A has a nilpotent invariant sub-algebra N in the extended field, the identical equation of $(A-N)$ is also $f(x) = 0$, since the latter has no multiple roots. Hence, if z is any element of N and x any element of A, x and $x+z$ have the same identical equation, since they are equal modulo N.

* It is here assumed that rational elements which are independent in F are also independent in F'.

Let $z = \sum_1^a \xi_r x_r$ be any element of N, the x's forming a rational basis for A. Then

$$z' \equiv x_s z - z x_s = \Sigma \xi_r (x_s x_r - x_r x_s) \equiv \Sigma \xi_r x_r',$$

where x_r' $(r = 1, 2, \ldots, a)$ are rational and $x_s' = 0$. Similarly

$$z'' \equiv x_t' z' - z' x' = \Sigma \xi_r (x' x_r' - x_r' x_t') \equiv \Sigma \xi_r x_r'',$$

where there are now at most $a-2$ terms under the summation sign. This process may be continued till each of the terms $x_r^{(p)}$ under the summation sign after the p-th operation is commutative with $z^{(p)}$, *i.e.*, $z^{(p+1)} = 0$. $z^{(p)}$, being commutative with each of $x_r^{(p)}$ $(r = 1, 2, \ldots, a)$, is also commutative with every element of the algebra generated by them. Let this algebra be denoted by B and its identical equation by $f(x) = 0$. Since $x_1^{(p)}, x_2^{(p)}, \ldots$ are rational, B has a rational basis and is therefore primitive in F. There is then a rational element x whose identical equation, with regard to B, is also its reduced equation, and a non-zero element z of B, which is also an element of N, such that $xz = zx$. Since z is nilpotent, we can obviously assume $z^2 = 0$. As before, $f(x+z) = 0$; hence, on expanding, we get

$$0 = f(x+z) = f(x) + f'(x) z = f'(x) z.$$

But, seeing that B is primitive, $f'(x)$, being of lower degree than $f(x)$, has an inverse; hence $z = 0$, *i.e.*, A has no nilpotent invariant subalgebra and is therefore semi-simple in F'.

THEOREM 26.—*If an algebra is rational in a field F and F' is any field containing F; and if B is the algebra composed of all elements of A which are, in F', commutative with every element of a sub-complex C of A; then, if a rational basis can be chosen for C every element of which possesses an inverse, B is also rational in F.*

Let $x_1, x_2, \ldots, x_a$ be a rational basis of A, then an arbitrary element y of B can be expressed in the form $y = \Sigma \xi_r' x_r$, where ξ_r' $(r = 1, 2, \ldots, a)$ are marks of F'. If b is the order of B, at least b of the ξ's are linearly independent in F. We may therefore suppose that the first n $(n \geqslant b)$ of the ξ's are linearly independent in F and that the remainder are zero.

Let x be any rational element of C which has an inverse. $xx_1, xx_2, \ldots, xx_a$ are then linearly independent and so also are $x_1 x, x_2 x, \ldots, x_a x$; hence

$$x_r x = \sum_1^a \eta_{rs} x x_s \quad (r = 1, 2, \ldots, a),$$

the η's being rational. Since $xy = yx$, we must have

$$0 = xy - yx = \sum_1^a (\xi_r - \sum_1^a \eta_{sr}\xi_s) x x_r ;$$

hence

$$\xi_r - \sum_{s=1}^{a} \eta_{sr}\xi_s = 0 \quad (r = 1, 2, \ldots, n).$$

But the ξ's are linearly independent and therefore these equations must reduce to identities. Hence

$$x x_r = x_r x \quad (r = 1, 2, \ldots, n). \tag{1}$$

Now a rational basis can be chosen for C in which every element has an inverse, so that (1) is true for every $x < C$. Hence it is possible to choose a rational basis for B, viz., $x_1, x_2, \ldots, x_n$.

THEOREM 27.—*If F' is a field, containing the given field F, in which every equation is soluble, and if a primitive algebra A is expressed in F' as the direct sum of r simple algebras $A_1, A_2, \ldots, A_r$, these algebras are simply isomorphic with each other and, in F', A can be expressed as the direct product of a commutative algebra, which is rational in F, and an algebra isomorphic with $A_1, A_2, \ldots, A_r$.*

Let $e_1, e_2, \ldots, e_r$ be the moduli of $A_1, A_2, \ldots, A_r$ respectively. Then every element of the algebra $B = e_1, e_2, \ldots, e_r$ is commutative with every element of A, and, conversely, every such element is, by Theorem 23, contained in B. Hence, by the previous theorem, a basis can be found for B which is rational in F. It is easily shown (as in the theory of finite groups) that we can find $a/b = c$ rational elements $x_1, x_2, \ldots, x_c$ such that any element of A can be expressed uniquely in the form

$$x = \sum_1^c y_r x_r,$$

y_r $(r = 1, 2, \ldots, c)$ being elements of B. Hence we have a primitive algebra C of c units in the field F'' obtained by adjoining B to F, and in this algebra, scalar multiples of the modulus are the only elements commutative with every element of C. In F'', C can therefore be expressed as a simple matric algebra $C = (e_{pq})$ of degree $n = \sqrt{c}$.* It follows that A can be expressed as the direct product of C and B.

---

* This gives a proof of a theorem by Allan to the effect that the order of a primitive algebra is of the form bn^2. I have only seen an abstract of this paper. See *Amer. Math. Soc. Bull.*, Vol. XI. (1905), p. 351.

THEOREM 28.—*If A is an algebra in which every element, which has no inverse, is nilpotent, it can be expressed in the form $A = B + N$, where B is a primitive algebra and N is the maximal nilpotent invariant sub-algebra.*

We shall first show that the theorem is true in the case where $(A - N)$ is commutative. To do this it is only necessary to show that there is a sub-algebra of A which has the same identical equation, $f(x) = 0$, as $(A - N)$. Let x be an element of A which corresponds to an element of $(A - N)$ whose identical equation is also its reduced equation. If $f(x) = 0$, the theorem is proved. We therefore set $f(x) = z \neq 0$, z being then an element of N which is commutative with x. Let us first suppose that $N^2 = 0$. Then, putting $x - z/f'(x)$ for x in $f(x)$, we get

$$f[x - z/f'(x)] = f(x) - z = 0.$$

The theorem is therefore true in this case and so is also true of $(A - N^2)$ when $N^2 \neq 0$. Hence we can so choose B' in $A = B' + N$ that $B'^2 = B' \pmod{N^2}$, and therefore $B' + N^2$ is an algebra which can be treated as before. The theorem then follows for commutative algebras by induction. If the given field is a Galois field, it can be shown * that there is no non-commutative primitive algebra. In this case, therefore, the proof of the theorem is complete at this point.

Let us now consider the case where $(A - N)$ is not commutative. Suppose, first, that $(A - N)$ is not simple when the given field is sufficiently extended. There is then a commutative sub-algebra whose elements are commutative with every element of $(A - N)$. To this algebra there corresponds a sub-algebra of A, in which the primitive part B' can be separated from the nilpotent part as above. Hence,† by adjoining B' to the given field as in Theorem 27, we obtain an algebra A' such that $(A' - N)$ remains simple when the given field is extended. It is, therefore, sufficient to confine our attention to such algebras. We shall therefore suppose that, in the extended field F', A can be expressed as the direct product of a simple matric algebra B and an algebra M', which consists of the modulus and a nilpotent algebra M, of index a. Since $M^a = 0$ and every element of M is commutative with every element of B, it follows that every element of M^{a-1} is commutative with every element of A, and therefore, by Theorem 26, we can choose a basis for M^{a-1} which is rational in F. Similarly there is a rational sub-algebra of $(A - N^{a-1})$ corresponding to $(M^{a-2} - M^{a-1})$. This means that we can

* Maclagan Wedderburn (8). † See p. 117.

choose a basis for M^{a-2} such that each element consists of a rational element and an element of M^{a-1} which is not necessarily rational. But, since M^{a-2} contains M^{a-1}, which has a rational basis, we may neglect the non-rational parts, *i.e.*, we can choose a rational basis for M^{a-2}, and hence, by induction, for M. The problem can now be still further simplified by showing that the general case can be made to depend on the case where M consists of a single unit. Let y be any element of M which is not an element of M^2; then, as in Theorem 12, we can express M in the form $M = y+M_1$, where AM_1 is an invariant subalgebra of A and $N = Ay+AM_1$ (since $N=BM=AM$). The algebra of $(A-AM_1)$ which corresponds to M then consists of a single unit. If, now, the theorem is true in this particular case, $(A-AM_1)$ can be expressed as the sum of a primitive and a nilpotent algebra, and hence A can be expressed in the form $A = B_1+N$, where $B_1^2 = B_1 \pmod{AM_1}$. Hence B_1+AM_1 is an algebra which can be treated as before, and so on till all the elements of M are exhausted. We shall, therefore, now suppose that the basis of M consists of a single element of y. N^2 is then zero.

For the remainder of the proof we require certain identities * which can be derived from the identical equation as follows:—

If in the identical equation $f_x(x) = 0$ we substitute $x+\xi y$ for x, ξ being a scalar, and expand as a polynomial in ξ, we have a relation which is true for any value of ξ, and hence the coefficients of the various powers of ξ vanish. The following notations are of value in expressing these identities. Let the coefficient of ξ^r in the expansion of $(x+\xi y)^n$ be denoted by $\binom{x \quad y}{n-r \quad r}$ and, similarly, the coefficient of $\xi_1^{r_1}\xi_2^{r_2}\dots\xi_s^{r_s}$ in $(\xi_1 x^{(1)}+\xi_2 x^{(2)}+\dots+\xi_s x^{(s)})^n$ by $\binom{x^{(1)}x^{(2)}\dots x^{(s)}}{r_1 \quad r_2 \quad \dots r_s}$. Thus

$$\binom{x \quad y}{n \quad 1} = x^n y+x^{n-1}yx+\dots+yx^n.$$

Also let the coefficient of x^{n-r} in $f_x(x)$ be denoted by $\left[\begin{matrix}x\\r\end{matrix}\right]$. $\left[\begin{matrix}x\\r\end{matrix}\right]$ is of degree r in the coefficients of x. Finally, let $\left[\begin{matrix}x^{(1)}x^{(2)}\dots x^{(s)}\\r_1 \quad r_2 \quad \dots r_s\end{matrix}\right]$ denote the coefficient of $\xi_1^{r_1}\xi_2^{r_2}\dots\xi_s^{r_s}$ in the expansion of $\left[\begin{matrix}\xi_1 x^{(1)}+\xi_2 x^{(2)}+\dots+\xi_s x^{(s)}\\ r\end{matrix}\right]$, where $r = r_1+r_2+\dots+r_s$. We may here observe that

$$x\binom{x \quad y}{r \quad s}-\binom{x \quad y}{r \quad s}x \equiv \binom{x \quad y}{r+1 \quad s-1}y-y\binom{x \quad y}{r+1 \quad s-1}.$$

* Sylvester (15); Shaw (14), p. 284.

With this notation the above mentioned identities can be expressed as follows :—

$$f_x(x) \equiv \sum_{r=0}^{n} \begin{bmatrix} x \\ n-r \end{bmatrix} x^r = 0, \tag{0}$$

$$\sum_{r=0}^{n-1} \begin{bmatrix} x \\ r \end{bmatrix} \begin{pmatrix} x & y \\ n-r-1 & 1 \end{pmatrix} + \sum_{r=0}^{n-1} \begin{bmatrix} x & y \\ r & 1 \end{bmatrix} x^{n-r-1} = 0, \tag{1}$$

$$\cdots \qquad \cdots \qquad \cdots \qquad \cdots \qquad \cdots$$

$$\sum_{s=0}^{r} \sum_{t=0}^{n-r} \begin{bmatrix} x & y \\ t & s \end{bmatrix} \begin{pmatrix} x & y \\ n-r-t & r-s \end{pmatrix} = 0, \tag{r}$$

$$\cdots \qquad \cdots \qquad \cdots \qquad \cdots$$

$$f_y(y) \equiv \sum_{r=0}^{n} \begin{bmatrix} y \\ n-r \end{bmatrix} y^r = 0. \tag{n}$$

Similar identities can easily be obtained by the same method for three or more elements.

In the algebra we are considering, the primitive algebra $(A-N)$ is, in F', equivalent to a matric algebra e_{pq} $(p, q = 1, 2, \ldots, n)$, which, by Theorem 24, is a sub-algebra of A in the extended field F'. Hence, if x_1', x_2', ..., x_m' are elements of $(A-N)$ corresponding to the rational elements $x_1, x_2, \ldots, x_m$ of A, we must have a relation of the form

$$x_r' = \Sigma \eta_{rpq} e_{pq}. \tag{1}$$

Consider these relations now as defining $x_1', x_2', \ldots, x_m'$ as elements of A and so giving a primitive algebra, isomorphic with $(A-N)$, but not necessarily rational in F. We have, however, $x_r = x_r' \pmod N$ or, say,

$$x_r' = x_r - x_r'' y,$$

where it is immaterial whether x_r'' is expressed in terms of $x_1', x_2', \ldots$ or $x_1, x_2, \ldots$, since these differ only by elements of N and $N^2 = 0$. We can choose one of the elements, say $x_1' \neq e$, so that $x_1' = x_1$. For this it is sufficient to choose x_1 so that $f_{x_1}(x_1) = 0$ and then to choose $e_{11}, e_{22}, \ldots, e_{nn}$ so that the primitive idempotent elements of the algebra generated by x_1 are linearly dependent on $e_{11}, e_{22}, \ldots, e_{nn}$. Further, if x_p' $(p \neq 1)$ is irrational, we may suppose $x_p'' = \Sigma \xi_{ps} x_s^{(3)}$, where $x_s^{(3)}$ $(s = 1, 2, \ldots)$ are rational and ξ_{ps} are irrational scalars which are linearly independent* in F. Let us now consider the r-th of the series of invariant relations

* In general we have $x_p'' = \Sigma \xi_{ps} x_s + x_{p_0}$, where x_{p_0} is rational. We may, however, suppose that the rational element $x_{p_0} y$ is included in x_p.

connecting x_1 and x_p' as elements of $(A-N)$, viz.,

$$\sum_s \sum_t \begin{bmatrix} x_1 & x_p' \\ t & s \end{bmatrix} \begin{pmatrix} x_1 & & x_p' \\ n-r-t & & r-s \end{pmatrix} = 0.$$

Putting $x_p'+x_p'' y$ for x_p' in the left-hand side, we get

$$\sum_s \sum_t \begin{bmatrix} x_1 & x_p \\ t & s \end{bmatrix} \begin{pmatrix} x_1 & & x_p' & x_p'' \\ n-r-t & & r-s-1 & 1 \end{pmatrix} y = z, \qquad \text{(i.)}$$

where z is rational, since $x_p = x_p'+x_p'' y$ is rational. Also

$$y \begin{pmatrix} x_1 & x_p'+x_p'' y & x_p'' \\ n-r-t & r-s-1 & 1 \end{pmatrix}$$

$$= y \left\{ \begin{pmatrix} x_1 & & x_p' & x_p'' \\ n-r-t & & r-s-1 & 1 \end{pmatrix} + y \begin{pmatrix} x_1 & & x_p' & x_p'' & x_p'' \\ n-r-t & & r-s-2 & 1 & 1 \end{pmatrix} \right\}$$

$$= y \begin{pmatrix} x_1 & & x_p' & x_p'' \\ n-r-t & & r-s-1 & 1 \end{pmatrix},$$

since $y^2 = 0$. Hence we may put x_p for x_p' in (i.). The left-hand side of (i.) then becomes a linear and homogeneous expression in ξ_{ps} $(s = 1, 2, \ldots)$ with rational coefficients and, as the ξ's are linearly independent in F, it cannot equal a rational quantity. Hence it must vanish identically, *i.e.*, $z = 0$. Hence $f(\xi_1 x_1+\xi_p x_p) = 0$ for all values of ξ_1 and ξ_p and for $p = 1, 2, \ldots, n$. By a repetition of this argument, $\xi_1 x_1+\xi_p x_p$ taking the place of x_1, we can show that $f(\Sigma \xi_s x_s) = 0$. Furthermore, in the above process x_1 may be replaced by a rational integral function of it, say $h(x_1)$, and, since

$$h(x_1) x_p = h(x_1') x_p'+h(x_1) x_p'' y,$$

which is linear in x_p'', x_p' may be replaced by $h(x_1) x_p'$. Hence

$$f(h_1(x_1)+h_2(x_1) x_p h_3(x_1)) = 0,$$

where $h_1(x_1)$, $h_2(x_1)$, and $h_3(x_1)$ are rational integral functions of x_1. Again,

$$x_p^2 = x_p'^2+(x_p x_p''+x_p'' x_p) y = x_{pp}'+x_{pp}'' y,$$

where

$$x_{pp}'' = \Sigma \xi_{ps} (x_p x_{ps}^{(3)}+x_{ps}^{(3)} x_p),$$

the ξ's remaining linearly independent. Hence x_p^2, or any rational integral function of x_p, may take the place of x_p. Combining these results, we find that, if x is any element of the algebra C generated by x_1 and x_p, then $f_x(x) = 0$. This algebra cannot be identical with A. For it would then contain the element y which is commutative with every

other element. Hence, since $f_x(x) = 0$ is the identical equation both of $(A-N)$ and of $C = A$, therefore $f_x(x+y) = 0$. But

$$f_x(x+y) = f_x(x)+f'_x(x)y = f'_x(x)y \neq 0.$$

Let the theorem be now assumed to hold for algebras of order less than the order of A. C then has a rational primitive sub-algebra C_1, which contains elements congruent to x_1 and x_p modulo N, and is therefore of higher order than the algebra generated by x_1. Let D be any rational primitive sub-algebra of A of order r. Since in the extended field it is equivalent to a matric algebra, we may suppose e_{pq} $(p, q = 1, 2, \ldots, n)$ so chosen that $x'_1, x'_2, \ldots, x'_r$ form a rational basis of D, and hence $x''_1 = \ldots = x''_r = 0$. But the algebra generated by D and x_p $(p > r)$ has, as we have shown, $f_x(x) = 0$ as its identical equation. As before, it cannot be equal to A; hence it has a rational primitive sub-algebra which is greater than D, since $x'_p \not< D$. Hence, by a repetition of this process, A can be expressed as the sum of a primitive and a nilpotent algebra. Now the theorem is obviously true of algebras of one unit. Hence, by induction, it is true for algebras of any order.

8. *The Classification of Potent Algebras (continued).*

The results of the preceding sections may be summarised as follows :—

(i.) An algebra can be expressed uniquely as the direct sum of two algebras, one of which has a modulus, and the other no modulus and no integral sub-algebra which has a modulus. (Theorem 10.)

(ii.) An algebra, which has a modulus, can be expressed uniquely as the direct sum of a number of irreducible algebras. (Theorem 10.)

(iii.) Any algebra can be expressed as the sum of a nilpotent algebra and a semi-simple algebra. The latter algebra is not unique, but any two determinations of it are simply isomorphic. (Theorems 24 and 28.)

(iv.) A semi-simple algebra can be expressed uniquely as the direct sum of a number of simple algebras. (Theorems 10 and 17.)

(v.) A simple algebra can be expressed as the direct product of a primitive and a simple quadrate algebra. (Theorems 22 and 23.)

(vi.) A simple quadrate algebra can be expressed as a matric algebra. (Theorem 22.)

The classification of algebras cannot be carried much further than this till a classification of nilpotent algebras has been found which is much more complete than any that has as yet been found.

9. *Non-associative Algebras.*

Many of the results of the previous sections are true of a much larger class of number-systems than the linear associative algebras. In this section I discuss the extension of some of these results to non-associative algebras.

A non-associative algebra differs from an associative one only in that, for some elements, the associative law does not hold true. Throughout this section the term "algebra" will be used to include non-associative algebras as well as associative ones, the appropriate adjective being affixed when it is necessary to distinguish between them.

The calculus of complexes is the same as in § 1, except that $A.BC$ is not necessarily the same as $AB.C$. Hence, any of the previous theorems which do not involve, directly or indirectly, products of more than two members, hold unaltered for non-associative algebras. Thus an invariant sub-complex of an algebra is itself an algebra, and so on, the terms "simple" and "invariant" being defined as in § 2. Hence also, if B_1 and B_2 are invariant sub-algebras of A, B_1+B_2 is also an invariant sub-algebra; and, if B_1 and B_2 are maximal, $A = B_1+B_2$, when $B_1 \neq B_2$.

If B is any sub-algebra of A and $A = B+C$, the elements of C define a new algebra if elements, which differ only by elements of B, are regarded as equal. This algebra, which may be said to be complementary to B, is not, however, unique, since C can be chosen in a variety of ways. But, if B is invariant, it is easily seen that the algebra is unique; it can therefore in this case be denoted by $(A-B)$. The proofs of Theorems 4–6 are therefore applicable word for word to non-associative algebras, the final result being that any two difference series of an algebra with a finite basis differ from one another merely in the order of their terms.

We may notice here a peculiar difference between associative and non-associative algebras, namely, that in the latter an algebra may have all its elements nilpotent and yet be simple. Consider the non-associative algebra A with three units whose multiplication table is

	e_1	e_2	e_3
e_1	0	e_1	e_2
e_2	e_1	0	e_3
e_3	e_2	e_3	0

the given field being $GF[2]$. Here

$$x^2 = (\xi_1 e_1+\xi_2 e_2+\xi_3 e_3)^2 = \xi_1^2 e_1^2+\ldots+\xi_1\xi_2(e_1e_2+e_2e_1)+\ldots = 0,$$

since $$e_1^2 = 0, \quad e_1e_2 + e_2e_1 = e_1 + e_1 = 0.$$

Also
$$e_1x = \hat{\xi}_2e_1 + \hat{\xi}_3e_2 = xe_1,$$
$$e_2x = \hat{\xi}_1e_1 + \hat{\xi}_3e_3 = xe_2,$$
$$e_3x = \hat{\xi}_1e_2 + \hat{\xi}_2e_3 = xe_3.$$

At least two of these are independent, say e_1x and e_2x. Then, if $B = e_1x, e_2x$, $AB = A$, this being also true if any other two be taken to be independent. A is therefore simple.

We may also observe that $A^2 = A$, although A has no idempotent element. This marks another difference between the two classes. Another interesting example of this is the algebra

	e_1	e_2
e_1	e_1+e_2	e_2
e_2	e_2	e_1

(2)

the field being the same as before. It is easily verified that, in this algebra, the equation $xy = z$ has, for given values of y and z, not both zero, a unique solution x. The algebra has therefore many of the properties of a primitive algebra, although it has no modulus.

The formation of powers in a non-associative algebra is rather complex. Thus $x.x^2$ is not necessarily the same as $x^2.x$, nor $A.A^2$ the same as $A^2.A$. We shall use the following notation :—

$$A(A(A \ldots (A) \ldots)) = A^n,$$
$$(A^n.A^m)A^p = A^{(n+m)+p},$$

and so on, the index indicating the manner in which the terms are grouped. All powers for which the sum of the indices is r, are said to be of the r-th degree.

If all the n-th powers of an algebra are zero, it is said to be a *nilpotent* algebra of *index* n. If A is nilpotent, the sum of the r-th powers is less than the sum of the $(r-1)$-th powers. To show this, let $A^{[s]}$ be the sum of the s-th powers, and suppose that the theorem holds for $s < r$. Then

$$A^{[r]} = A.A^{[r-1]} + A^{[r-1]}.A \leqslant A.A^{[r-2]} + A^{[r-2]}.A \leqslant A^{[r-1]}.$$

But $A^{[r]} \neq A^{[r-1]}$, and $A^{[2]} = A^2 < A$; hence the theorem follows by induction. Now $A^{[r]}A^{[s]} \leqslant A^{[r+s]}$, and $A^{[r]^2} \leqslant A^{[r]}$. Hence, as in Theorem 7, we may express A in the form

$$A = B_1 + B_2 + \ldots + B_{n-1},$$

where
$$B_pB_q \leqslant B_{p+q} + B_{p+q+1} + \ldots.$$

Every element of a nilpotent algebra is nilpotent in the sense that, for some n, all its n-th powers are zero. This condition is, however, not sufficient to render the algebra nilpotent, as may be seen from the first of the examples given on p. 110. A sufficient condition is, however, not difficult to find. If n is the index of a nilpotent algebra A, then $A^{[n]} = 0$, and in particular, if x and y are any two elements,

$$y(y(\dots y(yx)\dots)) = 0.$$

Now the proof of Theorem 14 holds for non-associative algebras step for step, except that we cannot deduce from $A'x = A'$ that A has an idempotent element. There is, however, an element y such that $yx = x$, from which it follows that

$$y(y(\dots y(yx)\dots)) \neq 0,$$

and A is therefore not nilpotent. Hence a necessary and sufficient condition that A is nilpotent is that it contains no pair of elements y and x such that $yx = x$ $(x \neq 0)$. y, of course, need not be distinct from x.

Of the remaining theorems of Section 5, Theorems 9 and 13 hold also for non-associative algebras. The others deal chiefly with idempotent elements and do not seem to have any direct analogue in the general theory.

A rough classification of non-associative algebras may, however, be obtained as follows.

In an algebra A there will, in general, be a sub-algebra M_1 composed of all elements z, such that $z.xy = zx.y$ for any elements x and y of A. The modulus, if the algebra has one, will be contained in it. For this reason I shall call it the *modular sub-algebra of the first kind.* Similarly, the elements z such that $x.zy = xz.y$ form an associative algebra M_2 which may be called the *modular sub-algebra of the second kind;* and elements such that $x.yz = xy.z$ form an associative algebra M_3 called the *modular sub-algebra of the third kind.* The elements common to all three will be called the *principal modular sub-algebra* of A. For example, in the algebra

	e_1	e_2	e_3	e_4
e_1	e_1	0	0	0
e_2	0	e_2	e_3	e_4
e_3	e_3	0	0	e_4
e_4	e_4	0	e_4	0

we have $$M_1 = M_2 = M_3 = M = e_1, e_2;$$

and in

	e_1	e_2	e_3
e_1	e_1	0	0
e_2	0	e_2	e_3
e_3	e_2	e_3-e_2	e_2

$$M_1 = e_1,\ e_2,\ M_2 = M_3 = M = (e_1+e_2).$$

If $e_1, e_2, \ldots, e_m$ is a primitive set of idempotent elements of M, we have

$$A = \sum_{p,q} A_{pq}, \quad A_{pq}A_{rs} = 0 \ (q \neq r), \quad A_{pq}A_{qr} \leqslant A_{pr}.$$

This is analogous to Pierce's form for a linear associative algebra, and a partial classification of non-associative algebras can obviously be based upon it.

10. *Semi-invariant Sub-algebras.**

A sub-algebra B of A is said to be semi-invariant if either $AB \leqslant B$ or $BA \leqslant B$. We shall assume throughout this section that $AB \leqslant B$.

If B_1 and B_2 are two different maximal semi-invariant sub-algebras of A, then evidently $B_1+B_2 = A$, since $A\,(B_1+B_2) \leqslant B_1+B_2$. Further, if $B = B_1 \frown B_2$, it may be shown that the difference algebras complementary to B_1, B_2 and B, may be so chosen† that

$$(A-B_1) \sim (B_2-B), \qquad (A-B_2) \sim (B_1-B).$$

It then follows, as in Theorem 6, that, if

$$A, B_1, B_2, \ldots; \quad A, B_1', B_2', \ldots$$

are two series of algebras such that each of them is a maximal semi-invariant sub-algebra of the preceding term, then the corresponding series of difference algebras can be so chosen that they differ merely in regard to the order in which their terms occur.

In a potent associative algebra A, a maximal nilpotent semi-

---

* The proofs of the theorems of this section are merely repetitions of what has already been done and are, therefore, for the most part omitted.

† Since $(A-B_1)$, ... are not uniquely determined, these symbols have no meaning unless it is shown how these algebras are to be determined, *e.g.*, in this case by setting

$$B_1 = C_1+B, \quad C_1 \frown B = 0; \qquad B_2 = C_2+B, \quad C_2 \frown B = 0;$$
$$A \quad C_1+C_2+B.$$

$(A-B)$ is of course not necessarily simple when B is maximal.

invariant sub-algebra is invariant, and is therefore unique. For

$$AN \leqslant N, \quad NA.A \leqslant NA, \quad A.NA \leqslant NA,$$

$$(NA)^2 = NANA \leqslant N^2A, \quad (NA)^a \leqslant N^aA = 0,$$

if $N^a = 0$. Hence NA is a nilpotent invariant sub-algebra of A, and therefore either $NA \leqslant N$ or $A = NA+N$. In the latter case,

$$A^a \leqslant N^aA+N^a;$$

and therefore A is nilpotent contrary to our assumption. Hence we must have $NA \leqslant N$, which proves the theorem.

Suppose now that both A and B have a modulus, the moduli being respectively e and e_1. Then, if $e_2 = e-e_1$,

$$A = Ae_1+e_1Ae_2+e_2Ae_2 = B+C+D,$$

where $$B = Ae_1, \quad C = e_1Ae_2, \quad D = e_2Ae_2,$$

and $$B \frown (C+D) = 0 \quad \text{and} \quad C \frown D = 0.$$

Since $A^2 = A$, we have

$$A = Ae_1Ae_1+e_1Ae_2Ae_1+e_2Ae_2Ae_1+Ae_1Ae_2+e_1Ae_2Ae_2+e_2Ae_2Ae_2.$$

Therefore $D^2 = D$, and the multiplication table of A has the form

	B	C	D
B	B	C	0
C	0	0	C
D	0	0	D

C is a nilpotent invariant sub-algebra of A whose complementary algebra is reducible. Hence no semi-invariant sub-algebra of a semi-simple algebra has a modulus. We may also notice that D is a left-hand semi-invariant sub-algebra, and that $B+C$ and $D+C$ are invariant sub-algebras of A.

A primitive algebra is the only type of algebra which has no semi-invariant sub-algebra. For, if A has no semi-invariant sub-algebra, it must have a modulus, and if x is any element of A which has no inverse, Ax is a semi-invariant sub-algebra of A.

11. *The Direct Product.*

Let $A = x_1, x_2, \ldots, x_a$, $B = y_1, y_2, \ldots, y_b$ be two complexes of order a and b respectively, such that every element of A is commutative with

every element of B; and further, let all the elements

$$x_r y_s \ (r = 1, 2, \ldots, a; \ s = 1, 2, \ldots, b)$$

be linearly independent; then the complex

$$C = x_1 y_1, x_1 y_2, \ldots, x_r y_s, \ldots$$

is called the *direct product* of A and B.

The following is an alternative definition. Consider all pairs of elements of the form (x, y) where $x < A$ and $y < B$. Let

$$(x+x', y+y') = (x, y)+(x', y')+(x, y')+(x', y)$$

and

$$(x, y)(x', y') = (xx', yy').$$

The elements (x, y) generate an algebra of which they themselves form a complex of order ab which is said to be the direct product of A and B and is denoted by $A \times B$. $A \times B$ is of course the same as $B \times A$.

We shall generally take A and B to be algebras, in which case $A \times B$ is an algebra.

The following relations follow immediately from the definition of $A \times B$.

$$A \times (B \times C) = (A \times B) \times C,$$

$$A \times (B+C) = A \times B + A \times C,$$

$$A \times (B \frown C) = A \times B \frown A \times C.$$

If $A = B \times C$ has a modulus, B and C must each have a modulus and conversely. In this case there is also a sub-complex of A isomorphic with B, namely, the direct product of B and the modulus of C. Also, if B' and C' are the sub-complexes of A which correspond to B and C, then

$$A = C'B' = B'C'.$$

If B has an invariant sub-algebra B_1, $B_1 \times C$ is evidently an invariant sub-algebra of A; hence, if A is simple, B and C are also simple. The converse of this is, however, not always true. For instance, let

e_1	e_2
e_2	$-e_1$

be the table of B, and let $C = B$; then the table of A is

e_1	e_2	e_3	e_4
e_2	$-e_1$	e_4	$-e_3$
e_3	e_4	$-e_1$	$-e_2$
e_4	$-e_3$	$-e_2$	e_1

where $e_1 = (e_1, e_1)$, $e_2 = (e_1, e_2)$, $e_3 = (e_2, e_1)$,

and $e_4 = (e_2, e_2)$.

If we put $e_1' = \frac{1}{2}(e_1+e_4)$, $e_2' = \frac{1}{2}(e_2-e_3)$,

$e_3' = \frac{1}{2}(e_1-e_4)$, $e_4' = \frac{1}{2}(e_2+e_3)$,

the table becomes

	e_1'	e_2'	e_3'	e_4'
e_1'	e_1'	e_2'	0	0
e_2'	e_2'	$-e_1'$	0	0
e_3'	0	0	e_3'	e_4'
e_4'	0	0	e_4'	$-e_3'$

Hence $B \times C$ is reducible. If, however, the given field is such that every simple algebra is matric, the converse does hold; therefore, in any field, the product of two simple algebras is simple or semi-simple.

It is interesting to note that the algebra given above can also be expressed as the direct product of B and the algebra C_1 whose table is

	e_1	e_2
e_1	e_1	0
e_2	0	e_2

Hence, from $A = B \times C = B \times C_1$, it does not necessarily follow that $C \sim C_1$. This is, however, probably true if the field is sufficiently extended.

12. *Conclusion.*

It is remarkable that the properties of a field with regard to division are not used in many of the theorems of the preceding sections. The first place, where it is used, is where it is assumed that, if $A^2 < A$, the order of A^2 is less than the order of A. Thus, if the table of an algebra is

	e_1	e_2
e_1	$2e_1$	$2e_2$
e_2	$2e_2$	$2e_1$

and the set of positive and negative integers takes the place of the given field, then $A^2 = 2e_1, 2e_2$, which is not equivalent to A, but is still contained in A. In other words, if $B < A$ and $A = B+C$, then, for every such C, B is contained in C.

If we now call B a proper sub-complex of A when we can find C such that $A = B+C$, $B \frown C = 0$, and, in Theorem 2, substitute "proper invariant sub-complex" for "invariant sub-complex" throughout, we find that all the theorems of the section hold without further modification. Most of the theorems of the other sections can be modified in a similar fashion. Thus, Theorem 15, when modified, would read:—*If A is an algebra with not more than one idempotent element, and x is any element such that Ax is a proper sub-complex of A, then x is nilpotent.*

I have not carried out this process in detail, as the results obtained do not seem to be of sufficient importance.

[*Added February 1st*, 1908.—Since the above paper was in print I have noticed a mistake in the proof of Theorem 28; this mistake is, however, easily remedied. The notation used below is that of page 105.

It is there assumed that the algebra B' is commutative with every element of A. Suppose that this is not the case, and let M be the maximum sub-algebra of N which is composed of elements commutative with every element of B'. As on page 105, we may assume $N^2 = 0$. Let x, y, and z be elements of A, B', and M respectively. From the definition of B', we have $xy-yx < N$, and therefore, since $N^2 = 0$ and $M \leqslant N$, $xzy = xyz = yxz$. Hence $xz < M$, *i.e.*, M is invariant. Now, if we prove the theorem for $(A-M)$, it follows for A as in the text; for if the theorem is true for $(A-M)$, then A can be expressed in the form A_1+N_1 where N_1 is nilpotent and A_1 is an algebra, containing B', of which M is the maximal invariant nilpotent sub-algebra; B' is then commutative with every element of A_1 and the proof proceeds as on page 105. We may therefore suppose that there are no elements of N commutative with every element of B', *i.e.*, $M = 0$.

If the given field is sufficiently extended, it follows from Theorems 22 and 27 that A contains a simple matric algebra A' such that $(A-N)$ is the direct product of A' and B'; and, since $M = 0$, evidently the elements of $A'B'$ are the only elements of A which are commutative with every element of B'. But B' is rational; hence, by Theorem 26, $A'B'$ is also rational if B' is of order greater than 1, *i.e.*, the theorem is true in this case. We may therefore assume that every element of B' is commutative with every element of A, as we have shown that the theorem follows if this is not the case.]

LIST OF MEMOIRS REFERRED TO.

1. E. Cartan.—"Sur les groupes bilinéaires et les sytèmes de nombres complexes," *Ann. de Toul.*, Vol. XII. (1898), B., pp. 1–99.
2. L. E. Dickson.—"Definitions of a Linear Associative Algebra by Independent Postulates," *Amer. Math. Soc. Trans.*, Vol. IV. (1903), pp. 21–26.
3. L. E. Dickson.—"On Hypercomplex Number Systems," *Amer. Math. Soc. Trans.*, Vol. VI. (1905), p. 344.
4. S. Epsteen.—"Semi-reducible Hypercomplex Number Systems," *Amer. Math. Soc. Trans.*, Vol. IV. (1903), pp. 436–444.
5. S. Epsteen and J. Wedderburn.—"On the Structure of Hypercomplex Number Systems," *Amer. Math. Soc. Trans.*, Vol. VI. (1905), pp. 172–178.
6. G. Frobenius.—"Theorie der Hypercomplexen Grössen," *Berl. Sitzber.* (1903), pp. 504–537, 634–645.
7. H. E. Hawkes.—"On Hypercomplex Number Systems," *Amer. Math. Soc. Trans.*, Vol. III. (1902), pp. 312–330.
8. J. Maclagan Wedderburn.—"On a Theorem on Finite Algebras," *Amer. Math. Soc. Trans.*, Vol. VI. (1905), pp. 349–352.
9. J. Maclagan Wedderburn.—"On a Theorem in Hypercomplex Numbers," *Proc. R. S. Edin.*, Vol. XXVI. (1906), pp. 48–50.
10. T. Molien.—"Über Systeme höherer complexer Zahlen," *Math. Ann.*, Bd. XLI. (1893), pp. 83–156.
11. B. Peirce.—"Linear Associative Algebra" (1870), *Amer. Journ. of Math.*, Vol. IV. (1881), p. 97.
12. G. Scheffers.—"Zurückführung complexer Zahlen auf typische Formen," *Math. Ann.*, Bd. XXXIX. (1891), pp. 293–390.
13. G. Scheffers.—"Über die Reducibilität complexer Zahlensysteme," *Math. Ann.*, Bd. XLI. (1893), pp. 601–604.
14. J. B. Shaw.—"Theory of Linear Associative Algebra," *Amer. Math. Soc. Trans.*, Vol. IV. (1903), pp. 251–287.
15. J. J. Sylvester.—"Lectures on the Principles of Universal Algebra," *Amer. Journ. of Math.*, Vol. VI. (1884), p. 270.

CONTENTS.