LINEAR ASSOCIATIVE ALGEBRAS AND ABELIAN EQUATIONS*

BY

L. E. DICKSON

1. In the recent development of the theory of linear associative algebras the coördinates of whose numbers range over the field of ordinary complex numbers, an important rôle is played by the so-called simple algebras, the only ones being the matric algebras with r^2 units. For the more general case of algebras the coördinates of whose numbers range over any field (Körper) K of finite or infinite order, a corresponding importance is to be attached to simple algebras; an algebra is simple † if and only if it is the direct product of a matric algebra and a primitive algebra (one in which every element has an inverse). The problem of primitive algebras is the chief outstanding problem in the theory of algebras over a field K. Aside from real quaternions the only known primitive linear associative algebras are fields. We proceed to exhibit a primitive algebra L with r^2 units over K.

Let $\kappa(x) = 0$ be a uniserial abelian equation of degree r with respect to the field K, i. e., let the equation have as its coefficients numbers in K, be irreducible in K, and have as its roots

$$(1)\quad i,\ \theta(i),\ \theta^2(i)\equiv\theta[\theta(i)],\ \cdots,\ \theta^{s+1}(i)\equiv\theta^s[\theta(i)],\ \cdots,\ \theta^{r-1}(i),$$

where $\theta(x)$ is a polynomial with coefficients in K, while

$$(2)\qquad \theta^r(i) = i.$$

Then the algebra in question is the linear associative algebra L over K (i. e., the coördinates of its numbers are arbitrary elements of K) with the r^2 units

$$(3)\qquad i^s j^k \qquad (s, k = 0, 1, \cdots, r-1),$$

where

$$(4)\qquad ji = \theta(i)\, j,$$

$$(5)\qquad j^r = g \qquad (g \text{ in } K).$$

* Presented to the Society, April 14, 1906. Cf. the abstract in the Bulletin of the American Mathematical Society, vol. 12 (1905–6), p. 442. But §§ 9–22 were added March, 1913.

† J. H. M. Wedderburn, Proceedings of the London Mathematical Society, ser. 2, vol. 6 (1907), p. 99.

Using the associative law, we readily deduce (7) and hence

$$(6) \qquad l(i)\,j^s \cdot f(i)\,j^k = l(i)\,f[\theta^s(i)] \begin{cases} \cdot\, j^{s+k} & (\text{if } s+k<r) \\ \cdot\, g j^{s+k-r} & (\text{if } s+k \geqq r), \end{cases}$$

where $l(i)$ and $f(i)$ are any polynomials in i of degree $< r$ with coefficients in K. Conversely, it is readily verified that the associative law holds when multiplication is defined by the preceding relation and the supplementary law that the product of two polynomials in i is found as in ordinary algebra with a subsequent reduction of the degree to $r-1$ by use of the equation $\kappa(i)=0$ of degree r. We may of course write i_s for i^s and j_k for j^k in our formulæ. Hence to any uniserial abelian equation* of degree r with respect to K there corresponds a linear associative algebra L over K with r^2 units.

For $r=2$, L is a generalization of quaternions discussed in § 9; we may take $i^2=c$; then† L is primitive if and only if g is not the norm x^2-cy^2 of any number $x+yi$ in the field $K(i)$.

As stated in the abstract of 1906 (see the first reference above), an algebra L with r^2 units is primitive when g and the coefficients of $\kappa(x)$ are suitably chosen numbers of the field K. The argument in my manuscript of that date is as follows: Take $r=3$ and denote the general number of the algebra by $M=R+Sj+Tj^2$, where R, S, T are numbers of $K(i)$. For $M\neq 0$, the equation $XM=M'$ uniquely determines a number X of the algebra if and only if

$$\Delta \equiv \begin{vmatrix} R & gT_1 & gS_2 \\ S & R_1 & gT_2 \\ T & S_1 & R_2 \end{vmatrix}$$

vanishes only when $R=S=T=0$, where $R_1=R(\theta)$, $R_2=R(\theta^2)$,

$$S_1=S(\theta),\ S_2=S[\theta^2(i)], \qquad T_1=T(\theta),\ T_2=T[\theta^2(i)].$$

If $T=0$, $S\neq 0$, then $\Delta=0$ implies that $g=n(-R/S)$, where the norm SS_1S_2 of S is denoted by $n(S)$. If $T\neq 0$, T has an inverse in $K(i)$, so that it suffices to consider numbers M with $T=1$. Then

$$\Delta = g^2+g(SS_1S_2-RS_1-R_1S_2-R_2S)+RR_1R_2.$$

* Note the special case of a binomial equation $x^r-h=0$. If a primitive rth root ϵ of unity occurs in the field K, and h is not the rth power of an element of K, and if r is a prime, x^r-h is known to be irreducible in K. The algebra is then defined by

$$i^r=h,\quad j^r=g,\quad ji=\epsilon ij.$$

If we set $h=g=1$, we lose the irreducibility property, but obtain the algebra ($i=e_2$, $j=e_1$) considered by Wedderburn, Proceedings of the Royal Society of Edinburgh, vol. 26 (1906), pt. 1, p. 48.

† Dickson, these Transactions, vol. 13 (1912), p. 66.

If $S = 0$, then $\Delta = 0$ implies that $g = 0$ or $n(-g/R)$, according as $R = 0$, or $R \neq 0$. Henceforth, let $S \neq 0$. To simplify Δ, set

$$R = SS_2 Q, \qquad g = Gn(S).$$

Then Δ has the factor $n^2(S)$ and $\Delta = 0$ implies that

$$G^2 + G(1 - Q - Q_1 - Q_2) + QQ_1Q_2 = 0.$$

The product of this by $G - 1$ may be written in the form

$$Gn(Q - 1) = n(Q - G).$$

Thus, if $Q \neq 1$, G (and hence g) is the norm of a number of $K(i)$. If $Q=1$, then $(G - 1)^2 = 0$. Hence *if g is not the norm of any number of $K(i)$, the algebra L is primitive.*

For a general value of r the last theorem was found in November, 1913, by Professor Wedderburn; his brief and elegant proof will appear in an early number of these Transactions.

It will be proved that any linear associative algebra having the properties specified in § 2 contains a subalgebra of type L. It is later proved that there exist such algebras, not identical with their subalgebras L. Some remarkable algebras are obtained in this way.

2. Let A be any linear associative algebra the coördinates of whose numbers range over any given field F and for which the following three properties hold:

(*a*) There exists in A a number i satisfying an equation $\phi(x) = 0$ of degree n with coefficients in F and irreducible in F.

(*b*) Any number of A which is commutative with i is in the field $F(i)$.

(*c*) There exists in A a number j, not in $F(i)$, such that $ji = \theta j + \sigma$, where θ and σ are in $F(i)$.

Note that the field $F(i)$ is composed of the totality of polynomials in i with coefficients in F. Indeed, in view of the associative law, any two powers of i are commutative; hence any two polynomials in i are commutative. That the quotient of two polynomials in i can be expressed as a polynomial in i is proved as in the theory of algebraic numbers.*

Conditions (*a*)–(*c*) hold when A is the system of quaternions with coördinates in the field of real numbers. Conditions (*a*) and (*b*) are satisfied for any linear associative algebra D over F in which each right-hand and left-hand division is always possible and unique. In fact, any number i of D satisfies an equation with coefficients in F and irreducible in F. Choose i so that the degree n of the equation is a maximum. If a number v of D is

* Cf. Bachmann, *Allgemeine Arithmetik der Zahlenkörper*, 1905, p. 15.

commutative with i, it is in the field $F(i)$. For if not, a standard theorem on algebraic numbers shows that the field $F(i, v)$ would contain a number satisfying an equation of degree exceeding n and irreducible in F.

For a linear associative algebra over F satisfying condition (a), the number of units is a multiple of n; they may be taken to be

$$i^s,\ i^s j,\ i^s j_1,\ \cdots \qquad (s = 0, 1, \cdots, n-1).$$

In case the number of units is $2n$, ji is necessarily a linear combination of the i^s, $i^s j$ and hence is of the form $\theta j + \sigma$ in (c).

These remarks serve to indicate the origin of conditions (a)-(c). All three conditions are satisfied by any algebra of type L (§ 8).

3. From the relation in (c), we find by induction that

$$ji^s = \theta^s j + (\theta^{s-1} + \theta^{s-2} i + \cdots + \theta i^{s-2} + i^{s-1})\,\sigma,$$

for $s > 1$. We are here using ordinary powers of θ and not symbolical powers as in (1). Multiply the members of the equation by c_s and sum, where

$$\phi(x) = \sum_{s=0}^{n} c_s x^s$$

is the function in (a) with the root i. Thus

$$0 = \phi(\theta) j + c_1 \sigma + \sum_{s=2}^{n} (\theta^{s-1} + \theta^{s-2} i + \cdots + \theta i^{s-2} + i^{s-1})\, c_s \sigma.$$

But j is not in the field $F(i)$. Hence $\phi(\theta) = 0$. Suppose first that $\theta = i$. If $\sigma = 0$, then $ji = ij$, j not in $F(i)$, contrary to (b). Hence $\sigma \neq 0$. The preceding relation thus gives

$$0 = c_1 + \sum_{s=2}^{n} s i^{s-1} c_s = \phi'(i).$$

Thus i would be a double root of $\phi(x) = 0$, contrary to its irreducibility. Hence $\theta \neq i$. Thus $Ji = \theta J$ if

$$J = j + \frac{\sigma}{(\theta - i)}.$$

Hence after a suitable choice of j we have relation (4) and

$$ji^s = [\theta(i)]^s j \qquad (s = 1, \cdots, n).$$

If $f(x)$ is any polynomial with coefficients in F,

$$(7) \qquad jf(i) = f(\theta) j, \quad \cdots, \quad j^s f(i) = f[\theta^s(i)]\, j^s,$$

the last relation following by induction and the use of the notation defined in (1). In particular, if $f(x)$ is the function $\phi(x)$ which vanishes for $x = i$,

we see from the first relation that $\theta(i)$ is a root of $\phi(x) = 0$. Hence $\phi[\theta(x)] = 0$ has the root i in common with the irreducible equation $\phi(x)=0$ and therefore the root $\theta(i)$. Thus $\theta^2(i)$ is a root of $\phi(x) = 0$. We see in this way that each of the numbers (1) is a root of $\phi(x) = 0$. Hence there must be an equality

$$\theta^{k+r}(i) = \theta^k(i) \qquad (r > 0).$$

If $k = 0$, (2) holds. If $k > 0$, $x = \theta(i)$ is a root of

$$\theta^{k+r-1}(x) = \theta^{k-1}(x). \tag{8}$$

Since this equation with coefficients in the field F has a root in common with the equation $\phi(x) = 0$, irreducible in F, it has also the root $x = i$. Then (8) for $x = i$ gives a relation like the initial equality but with lower symbolic powers. Proceeding in this manner, we ultimately obtain relation (2).

Let r be the least positive integer for which (2) holds. If $r = 1$, (4) would be in contradiction with (*b*). The argument just used shows that the numbers (1) are all distinct.

Theorem 1. *The algebra A contains a number j not in the field $F(i)$ and satisfying relation* (4). *Among the roots of $\phi(x) = 0$ occur the r ($r > 1$) distinct numbers* (1); *they form a closed cycle since relation* (2) *holds.*

4. In the last equation (7) take $s = r, f(x) = x$. By (2),

$$j^r i = \theta^r(i) j^r = ij^r.$$

Hence, by (*b*), j^r is in the field $F(i)$:

$$j^r = g(i), \tag{9}$$

where $g(i)$ is a polynomial with coefficients in F. Henceforth we shall assume that $g(i) \neq 0$.

For $\rho = 1$ and $\rho = 2$ we know that the numbers

$$i^s, \quad i^s j, \quad i^s j^2, \quad \cdots, \quad i^s j^{\rho-1} \qquad (s = 0, 1, \cdots, n-1;\ 0 < \rho < r) \tag{10}$$

are linearly independent with respect to the field F. Assume that the ρn numbers (10) are linearly independent. Then these and the n numbers $i^s j^\rho$ are linearly independent. For, if not, there is a polynomial $\tau(i) \neq 0$ such that τj^ρ is a linear function of the numbers (10) with coefficients in F. Since τ has an inverse in the field $F(i)$,

$$j^\rho = R_0 + R_1 j + \cdots + R_{\rho-1} j^{\rho-1}, \tag{11}$$

where each R_k is in $F(i)$. Multiply each term of (11) by i on the right and apply (7). We get

$$\theta^\rho(i) j^\rho = R_0 i + R_1 \theta(i) j + \cdots + R_{\rho-1} \theta^{\rho-1}(i) j^{\rho-1}.$$

Eliminating j^ρ by means of (11) and noting that the numbers (10) are linearly independent with respect to F, we see that

$$\theta^\rho(i) R_k = R_k \theta^k(i) \quad [k = 0, 1, \cdots, \rho - 1; \ \theta^0(i) \equiv i].$$

Since $k < \rho < r$, $\theta^\rho(i) \neq \theta^k(i)$ by Theorem I. Hence each $R_k = 0$. Then $j^\rho = 0$ by (11), so that $j^r = 0$, contrary to the assumption on (9).

Theorem 2. *The algebra A contains a linear associative subalgebra S over F with the rn units*

$$i^s, \quad i^s j, \quad i^s j^2, \quad \cdots, \quad i^s j^{r-1} \quad (s = 0, 1, \cdots, n-1) \tag{12}$$

linearly independent with respect to the field F. The product of any two of these units can be expressed as a linear function of the units by means of $\phi(i) = 0$ and relations (4) *and* (9).

5. In view of the first relation (7),

$$\begin{gathered} ji = \theta(i) j, \qquad j\theta(i) = \theta^2(i) j, \\ j\theta^2(i) = \theta^3(i) j, \quad \cdots, \qquad j\theta^{r-1}(i) = ij, \end{gathered} \tag{13}$$

where the final equation has been simplified by use of (2). Hence if s_k is an elementary symmetric function of the numbers (1),

$$js_k = s_k j. \tag{14}$$

Let K be the field composed of all rational functions with coefficients in F of these elementary symmetric functions:

$$K = F(s_1, s_2, \cdots, s_r). \tag{15}$$

Hence any number of K is commutative with j and, being a polynomial in i, also with i. Thus any number of K is commutative with every number of the algebra S.

If a number N of S is commutative with every number of S, then N is in the field K. For, by (*b*), N is in the field $F(i)$. Next, if $0 \leqq s < r$, $Nj^s = j^s N$ requires, by (7), that

$$N(i) j^s = N[\theta^s(i)] j^s.$$

Multiply each member by j^{r-s} on the right. Since the terms of (9) are not zero, we get

$$N(i) = N[\theta^s(i)] \qquad (s = 0, \cdots, r-1).$$

If we exclude the case of fields F having a modulus dividing r, we obtain, by addition and division by r, $N(i)$ expressed as a symmetric function of the numbers (1) and hence as a number of K. But we can easily give a proof valid for all fields F. By means of the equation of degree r having the roots

(1), we can express $N(i)$ as a polynomial in i of degree $r-1$ with coefficients in K. Thus

$$N(x) = a_0 + a_1 x + \cdots + a_{r-1} x^{r-1} \qquad (a\text{'s in } K)$$

holds for $x = i$. But the left member is unaltered when x is replaced by any one of the r numbers (1). Since an equation of degree $r-1$ with r distinct roots is an identity, $N(i) = a_0, a_1 = 0, \cdots$.

Theorem 3. *A number of the subalgebra S over F with the units* (12) *is commutative with every number of S if and only if it is in the field K defined by* (15).

Corollary. The right member of (9) is in the field K.

6. Let $\psi(x) = 0$ be the equation with coefficients in K and irreducible in K which has the root i. Since j is commutative with every number of K, in view of (14), relations (7) hold for any polynomial $f(x)$ with coefficients in K. Taking $\psi(x)$ as $f(x)$, we conclude that every $\theta^s(i)$ is a root of $\psi(x) = 0$. Thus the latter has the r distinct roots (1). But these r numbers are the roots of an equation $\kappa(x) = 0$ with coefficients in K, in view of the definition of K. Hence $\kappa(x)$ is irreducible in K.

Theorem 4. *The r numbers* (1) *are the roots of an equation $\kappa(x) = 0$ of degree r with coefficients in the field K and irreducible in K.*

7. Any number of algebra S, i. e., any linear function of its units (12) with coefficients in F, can be expressed by means of the equation $\kappa(i) = 0$ of degree r as a linear function of the r^2 numbers (3) with coefficients in the field K. These r^2 numbers are linearly independent with respect to K; the proof is as in § 4 with n replaced by r, F by K, $F(i)$ by $K(i) \equiv F(i)$. Hence the algebra S over F can be exhibited as the algebra L over K defined in § 1.

Theorem 5. *Any linear associative algebra A over the field F with the properties (a), (b), (c), and such that $g(i) \neq 0$ in* (9), *has a subalgebra S over F which can be exhibited as the algebra L over K with r^2 units* (3) *linearly independent with respect to K.*

8. If N is a number of the algebra L which is commutative with i, then N is a polynomial in i with coefficients in the field K. Indeed,

$$N = R_0 + R_1 j + \cdots + R_{r-1} j^{r-1},$$

where each R_s is a polynomial in i with coefficients in K. By (7),

$$j^s i = \theta^s(i)\, j^s,$$

$$Ni = R_0 i + R_1 \theta(i)\, j + \cdots + R_{r-1} \theta^{r-1}(i)\, j^{r-1}.$$

Equating the latter to iN and noting that the units (3) are linearly independent with respect to K, and that the numbers (1) are distinct, we find that R_1, $R_2, \cdots, R_{r-1}$ are zero.

Theorem 6. *Any algebra of type L has the properties (a), (b), (c), with n replaced by r and F by K.*

ALGEBRAS A WITH $r = 2$.

9. For $r = 2$, the irreducible equation satisfied by i may be given the form* $i^2 = c$ by applying a linear transformation on i. The algebra L then has the units $1, i, j, k$, where

$$\begin{aligned} &i^2 = c, \quad j^2 = g, \quad ij = k = -ji, \\ &k^2 = -cg, \quad jk = -gi = -kj, \quad ki = -cj = -ik. \end{aligned} \tag{16}$$

The relations in the second line were derived from those in the first line by use of the associative law. Right-hand and left-hand division† is always possible and unique in this algebra L if and only if c is not the square of a number in K and g is not expressible in the form $x^2 - cy^2$, with x and y in K. We shall assume henceforth that these conditions are satisfied. Then L is a generalized‡ quaternion algebra over K.

Consider an algebra A related to this L as in Theorem 5. Then K is of rank $n/2$ with respect to its subfield F. When K is so related to F, algebra L can evidently be exhibited as an algebra S of $2n$ units over F. We seek algebras A with such a subalgebra S but distinct from S. Since right- and left-hand division is always possible in S, the number of units m of A is a multiple of $2n$.

10. For the simplest case $n = 2$, $K \equiv F$ and A has L as a subalgebra. Let A have the least possible number 8 of units:

$$1, \quad i, \quad j, \quad k, \quad f, \quad if, \quad jf, \quad kf.$$

Then $fi = Q + Rf$, where Q and R are in L. Multiply by i on the right. Thus $R^2 = c$, $Qi + RQ = 0$. Hence $R = \pm i$. If $R = i$, then $Q = ej + lk$, and i is commutative with $f + jl/2 + ke/(2c)$, contrary to (b). Hence $R = -i$, $Qi = iQ$, $Q = e + li$. Taking $f - l/2 - ie/(2c)$ as a new unit f, we have

$$fi = -if. \tag{17}$$

Next, $fj = v + wf$, where v and w are in L. Multiply by j on the right. Thus $w^2 = g$, $w = \pm j$, $vj \pm jv = 0$.

* We exclude fields having modulus 2.

† These Transactions, vol. 13 (1912), p. 66. Division is always uniquely possible in the more general algebra (9), p. 67, since $\Delta(X) = \Delta'(X) = \sigma^2$.

‡ The ordinary quaternion algebra if $c = g = -1$ and if K is the field of all real numbers.

For the upper signs, $v = ri + sk$. Taking $f - kr/(2g)$ as a new f, we see that (17) remains true and that

$$fj = sk + jf. \tag{18}$$

Multiply (17) on the right by j. Thus $fk = -scj - kf$. Multiply (17) on the left by f. Thus f^2 is commutative with i. Hence, by (b),

$$f^2 = a + bi \qquad (a, b \text{ in } F). \tag{19}$$

Multiply (18) on the left by f. Thus $bk = -s^2 cj - bk$, $b = s = 0$,

$$fi = -if, \quad fj = jf, \quad fk = -kf, \quad f^2 = a. \tag{20}$$

The general element is $Q + Rf$, Q and R in L. We have

$$(Q + Rf)(q + rf) = Qq + Rr^* a + (Qr + Rq^*)f, \tag{20'}$$

where r^* is derived from r by changing the signs of the coefficients of i and k. Since $fr = r^* f$, $(r\rho)^* = r^* \rho^*$, the algebra with the multiplication table (20′) is associative. It is not an algebra A over F since every element is commutative with jf. Indeed, $Qj = jQ^*$.

For the lower signs, $v = e + lj$, so that

$$fj = e + lj - jf.$$

Multiply (17) on the right by j. We get

$$fk = -ei - lk + kf. \tag{21}$$

Now the multiplication table (16) for L is unaltered in form if we set

$$j = k_1, \qquad k = cj_1, \qquad g = -cg_1.$$

Then, by (21),

$$fj_1 = -\frac{e}{c}i - lj_1 + j_1 f.$$

Dropping the subscripts, we have the former case $fj = v + jf$.

Theorem 7. *There does not exist an algebra of type A with 8 units.*

Nor is there any algebra $A > L$ in which every number satisfies a quadratic equation with coefficients in F. For, if so, we may set $f^2 =$ constant. Then $(f \pm i)^2$ is a linear function of $f \pm i$, so that $fi + if$ is a linear function of $f + i$ and also of $f - i$ and hence is a constant:

$$fi + if = c_1, \qquad fj + jf = c_2, \qquad fk + kf = c_3,$$

$$fk = fij = (-if + c_1)j = i(jf - c_2) + c_1 j = kf - c_2 i + c_1 j.$$

Hence $2fk$ and thus f is in L. Thus* $A \equiv L$.

* We may thus give a remarkably simple proof of the famous theorem that a linear associative algebra (over the field of reals) in which division is always possible and unique is either the field of reals, the field of ordinary complex numbers or the system of real quaternions. Indeed, it is very easily shown that if there be more than two units, the algebra has a subalgebra of the quaternion type [making use of these Transactions, vol: 13 (1912), p. 64, first lines of § 6]. See § 11 of *Linear Algebras* (in press), Cambridge Tracts.

Algebras A With 16 *Units.*

11. For the next case $n = 4$, there exist algebras A with the minimum number 16 of units. We may take K to be the field $F(\xi)$, where

$$\xi^2 = \nu \qquad (\nu \text{ not a square in } F). \tag{22}$$

As the 8 units of algebra S we may take

$$1, \quad \xi, \quad i, \quad \xi i = i\xi, \quad j, \quad \xi j = j\xi, \quad k, \quad \xi k = k\xi. \tag{23}$$

The products of these by f on the right may be taken as the remaining 8 units of algebra A. Then $f\xi = Q + Rf$, where Q and R are in S. Multiplying by ξ on the right, we see that

$$R^2 = \nu \equiv \xi^2, \qquad (\xi + R)\, Q = 0.$$

If $\xi + R \neq 0$, then $Q = 0$, $R = \xi$, $f\xi = \xi f$, so that A is an algebra of 8 units over the field $F(\xi)$ and hence, if existent, is a quaternary algebra L over a larger field (§ 10). We therefore take $R = -\xi$. Taking $f - Q/(2\xi)$ as a new f, we have

$$f\xi = -\xi f. \tag{24}$$

Thus ξ is commutative with $q + rf$, where q and r are in S, if and only if $r = 0$. But ξ is commutative with f^2. Hence

$$f^2 = \lambda + \mu j \qquad [\lambda, \mu \text{ in } F(i)]. \tag{25}$$

12. The following notations will be employed. If $u = a + b\xi$, where a and b are in the field F, write $u' = a - b\xi$. If $\alpha = r + si$, where r and s are in the field $F(\xi)$, write $\bar{\alpha} = r - si$. Hence

$$fu = u'f, \qquad j\alpha = \bar{\alpha}j, \qquad k\alpha = \bar{\alpha}k \quad [u \text{ in } F(\xi),\ \alpha \text{ in } F(i)]. \tag{26}$$

13. We must have

$$fi = Q + Rf, \qquad Q = \alpha + \beta j, \qquad R = \gamma + \delta j \quad [\alpha, \cdots, \delta \text{ in } F(i)].$$

Then

$$fi^2 = c'f = Qi + RQ + R^2 f, \qquad c' = R^2, \qquad Qi + RQ = 0,$$

$$c' = \gamma^2 + \delta\bar{\delta}g, \qquad \delta(\gamma + \bar{\gamma}) = 0, \tag{27}$$

$$g\bar{\beta}\delta = -\alpha(i + \gamma), \qquad \bar{\alpha}\delta = \beta(i - \gamma). \tag{28}$$

First, let $\delta = 0$. If either α or β is not zero, then

$$\gamma = \pm i, \qquad c' = \gamma^2 = c,$$

and i satisfies the equation $i^2 = c$, with c in F, contrary to $n = 4$. Hence $\alpha = \beta = 0, fi = \gamma f$. Now $\gamma = x + yi$, x, y, and c' being in $F(\xi)$. Thus $c' = \gamma^2$ gives $xy = 0$. If $y = 0$, then $i^2 = c = x'^2$, and $i = \pm x'$ would be n $F(\xi)$. Hence $x = 0$,

$$(\mathrm{I}) \qquad fi = yif, \qquad c' = y^2 c \qquad [y \text{ in } F(\xi)].$$

If a number of A is commutative with i it is easily seen (see § 19) to be in $F(i)$, so that property (b) holds.

Next, let $\delta \neq 0$. Then by (27_2), $\gamma = \sigma i$, σ in $F(\xi)$. If $\beta \neq 0$, we find by eliminating α from (28), and using (27_1), that $c' = c$. Hence $\beta = 0$, $\alpha = 0$, and

$$(\mathrm{I}') \qquad fi = (\sigma i + \delta j) f, \qquad c' = c\sigma^2 + g\delta\bar{\delta} \quad [\sigma \text{ in } F(\xi),\ \delta \neq 0 \text{ in } F(i)].$$

14. We must have $fj = q + rf$, q and r in S. Then

$$(29) \qquad fj^2 = g'f = qj + rq + r^2 f, \qquad g' = r^2, \qquad qj = -rq.$$

Set $q = B + Cj$, $r = D + Ej$, where $B, \cdots, E$ are in $F(i)$. Then

$$(30) \qquad g' = D^2 + gE\bar{E}, \qquad E(D + \bar{D}) = 0,$$

$$(31) \qquad gC + DB + gE\bar{C} = 0, \qquad B + DC + E\bar{B} = 0.$$

First, let $E = 0$. Set $D = w + zi$, w and z in $F(\xi)$. Since $D^2 = g'$ is in $F(\xi)$, $wz = 0$. If $z = 0$, then $j^2 = g = w'^2$, and $j = \pm w'$ would be in $F(\xi)$. Hence $z \neq 0$, $D = zi$. Eliminating B from (31), we get $C(g - D^2) = 0$. If $C \neq 0$, then $j = \pm zi$. Hence $C = 0$, $B = 0$, and

$$(\mathrm{II}) \qquad fj = zif, \qquad g' = z^2 c \qquad [z \text{ in } F(\xi)].$$

Next, let $E \neq 0$. Then, by (30), $D = \omega i$, ω in $F(\xi)$, and

$$(32) \qquad g' = c\omega^2 + gE\bar{E}.$$

Multiply (31_1) by i and substitute the resulting value of $c\omega B$ into the product of (31_2) by ωc. By use of (32), we get

$$iC(g' - g) = 0.$$

If $g' \neq g$, then $C = 0$ and, by (31), $B = 0$, since the case $E\bar{E} = 1, \omega = 0$, is excluded by (32). Hence

$$(\mathrm{II}') \qquad fj = (\omega i + Ej) f, \qquad g' \neq g, \qquad E \neq 0 \ [\text{subject to } (32)].$$

For $g' = g$, it is simpler to employ conditions (29). Then $r^2 = j^2$, $r = \pm j$.

If $r = j$, set $f_1 = if$. Then (I) and (I′) hold with f replaced by f_1 and δ by $-\delta$. Also

$$f_1 j = i(q + rf) = iq - jif = iq - jf_1.$$

Hence it suffices to treat the case $r = -j$. Then $fj + jf = q$ is commutative with ξ. But, by (24), $(fj + jf)\xi = -\xi(fj + jf)$. Hence

$$(II'') \qquad fj = -jf, \qquad g' = g.$$

15. It remains to combine one of the cases (I), (I′) with one of the cases (II), (II′), (II″). The combination (I) and (II) is readily excluded. Multiply (I) on the right by j and apply (II). We get

$$fk = yi \cdot zif = yzcf = fy'z'c', \qquad k = y'z'c',$$

whereas k is not in $F(\xi)$.

16. Let (I) and (II″) hold. By the latter, $f^2 j = jf^2$. Hence by (25) and (26_2), $\lambda = \bar{\lambda}$, $\mu = \bar{\mu}$, so that λ and μ are in $F(\xi)$. By (I),

$$f^2 i = yy' if^2, \qquad y^2 y'^2 = 1.$$

Using (25), we see that $\mu = 0$ or $\lambda = 0$, according as $yy' = +1$ or -1. For the present, let the first alternative hold:

$$(33) \qquad yy' = +1, \qquad f^2 = \lambda,$$

where λ is in $F(\xi)$. Then f is commutative with λ. Hence by (26_1), λ is in F.

Writing* f_1, f_2, f_3 for if, jf, kf, we may express any number of the algebra as a linear combination of $1, i, j, k, f, f_1, f_2, f_3$, with coefficients in the field $F(\xi)$. The associative law then uniquely determines the multiplication table for these eight units:

	i	j	k	f	f_1	f_2	f_3
i	c	k	cj	f_1	cf	f_3	cf_2
j	$-k$	g	$-gi$	f_2	$-f_3$	gf	$-gf_1$
k	$-cj$	gi	$-gc$	f_3	$-cf_2$	gf_1	$-gcf$
f	yf_1	$-f_2$	$-yf_3$	λ	$y\lambda i$	$-\lambda j$	$-y\lambda k$
f_1	ycf	$-f_3$	$-ycf_2$	λi	$c\lambda y$	$-\lambda k$	$-yc\lambda j$
f_2	$-yf_3$	$-gf$	gyf_1	λj	$-y\lambda k$	$-g\lambda$	$gy\lambda i$
f_3	$-ycf_2$	$-gf_1$	$ygcf$	λk	$-yc\lambda j$	$-g\lambda i$	$gyc\lambda$

* The rest of this section and § 17 are not essential in the later work.

Let N be unity or one of the seven numbers $i, \cdots, f_3$ at the head of the table. Let N_1 be one of the same eight numbers. Let x and u be any numbers in $F(\xi)$. Then

$$(34) \qquad (xN)(uN_1) = (xU)(NN_1) \quad \begin{pmatrix} U = u \text{ if } N = 1, i, j, k; \\ U = u' \text{ if } N = f, f_1, f_2, f_3 \end{pmatrix}.$$

By means of the table and (34), we can express the product of any two linear functions of $1, i, \cdots, f_3$ with coefficients in $F(\xi)$ as a third such function. Multiplication thus uniquely defined is associative; it is far simpler to prove this fact by means of the condensed notations of § 18.

17. The preceding algebra can be given a simpler form by using a functional notation in addition to the notations in § 12. If $A = u + vi$, where u and v are in $F(\xi)$, write $A^* = u' + yv'i$. Then by (26), (I), (II''),

$$(35) \qquad fA = A^*f, \qquad jA = \bar{A}j, \qquad \phi A = \bar{A}^*\phi,$$

where $\phi = jf$. Any number of the algebra is of the form

$$N = X + Yj + Zf + W\phi \qquad [X, \cdots, W \text{ in } F(i)].$$

Then

$$(36) \qquad N(A + Bj + Cf + D\phi) = P + Qj + Rf + S\phi,$$

where

$$(37) \qquad \begin{aligned} P &= XA + Y\bar{B}g + ZC^*\lambda - W\bar{D}^*\lambda g, \\ Q &= XB + Y\bar{A} - ZD^*\lambda + W\bar{C}^*\lambda, \\ R &= XC + Y\bar{D}g + ZA^* - W\bar{B}^*g, \\ S &= XD + Y\bar{C} - ZB^* + W\bar{A}^*. \end{aligned}$$

18. A further simplification is effected by writing the general number of the algebra in the form $U + Vf$, where U and V are in S (i. e., are generalized quaternions), on writing $U\dagger = X^* - Y^*j$ if $U = X + Yj$, X and Y being in $F(i)$. Then $fU = U\dagger f$. The law of multiplication is now

$$(38) \qquad (U + Vf)(G + Hf) = UG + VH\dagger\lambda + (UH + VG\dagger)f.$$

This multiplication is seen at once to be associative since the element $f^2 = \lambda$ of F is commutative with every U and since

$$(39) \qquad (UV)\dagger = U\dagger V\dagger, \qquad (U\dagger)\dagger = U.$$

The latter relations follow at once from

$$(40) \quad (X+Y)^*=X^*+Y^*, \quad (XY)^*=X^*Y^*, \quad (X^*)^*=X, \quad (\bar{X})^*=\bar{X}^*,$$

where X, Y are any numbers in $F(i)$. Relations (40) are easily verified, use being made of (I), (33), $(u')' = u$, $(uv)' = u'v'$.

19. Let i be commutative with $U + Vf$. Then $Ui = iU$, so that U is in $F(i)$, and $yVi = iV$. Multiply the latter by i on the left. Then

$$cV = i^2 V = yiVi = y(yVi)i = y^2 cV.$$

If $y^2 = 1$, then $c' = c$ by (I) and i is a root of the equation $i^2 = c$ with coefficients in F, contrary to $n = 4$. Hence $V = 0$. Thus any number of the algebra commutative with i is in the field $F(i)$.

20. Since $yy' = 1$, the condition in (I) may be written $c'y' = cy$. Hence cy is in the field F, so that $c = dy'$, d in F. Set $y = a - b\xi$, a and b being in F. Then $yy' = 1$ gives

$$a^2 - \nu b^2 = 1. \tag{41}$$

Now i is a root of $x^2 = c$ and hence of

$$x^2 = d(a + b\xi), \qquad (x^2 - da)^2 = d^2 b^2 \nu.$$

By using (41), we see that i is a root of

$$x^4 - 2dax^2 + d^2 = 0. \tag{42}$$

Theorem 8. *If a, b, d, λ, g, ν are numbers in the field F such that* (41) *holds and such that equations* (42) *and $\xi^2 = \nu$ are irreducible in F, and if we set $y = a - b\xi$, $c = dy'$, the linear algebra over F with the* 16 *units* $1, i, j, k, f, f_1, f_2, f_3$ *and their products by ξ on the left, with multiplication defined by* (34) *and the table in* § 16, *or more compactly by* (38), *is a linear associative algebra with the properties* (a), (b), (c) *of* § 2.

The conditions on a, b, d are easily discussed. For example, let F be the field of all rational numbers. Take $\nu = -1$, $d = \pm 1$, $a = 0$, $b = 1$. Then (41) holds and (42) becomes the equation $x^4 + 1 = 0$ for the primitive eighth roots of unity and is known to be irreducible in the field of rational numbers.

Then $y = -\xi$, $c = \pm\xi$, and K is the field of the numbers $r + s\xi$, where r and s are rational and $\xi^2 = -1$. While it is not an essential condition on our algebra, we may choose g so that division* is unique in the algebra L.

21. We have treated the first one (33) of two alternatives. Next, let

$$yy' = -1, \qquad f^2 = \mu j.$$

* Evidently c is not the square of $r + s\xi$, since then $2s^2 = +1$ or -1. Next, there is a rational number g not of the form $x^2 - cy^2$, where $x = r + s\xi$, $y = l + m\xi$. Indeed, $x^2 - \xi y^2 = A + B\xi$, $A = r^2 - s^2 + 2lm$, $B = 2rs - l^2 + m^2$. Take $B = 0$. If $r = 0$, then $A = \pm 2l^2 - s^2$. If $r \neq 0$, we eliminate s and get $4r^2 A = \{2r^2 + (l + m)^2\}\{2r^2 - (l - m)^2\}$. If $2r^2 - v^2$ is divisible by the prime p, but not by p^2, then $p = 8k \pm 1$. For $2r^2 + v^2$ the condition is $p = 8k + 1$ or $8k + 3$. The primes not in either set are $p = 8k + 5$. Hence we may take as g a number divisible by an odd power of a prime $8k + 5$.

By $ff^2 = f^2 f$, we get $\mu' = -\mu$. Thus $\mu = t\xi$,

$$yy' = -1, \qquad f^2 = t\xi j \qquad (t \text{ in } F). \tag{43}$$

Define A^* as in § 17, and $U\dagger$ as in § 18. As before,

$$fA = A^* f, \qquad fU = U\dagger f, \qquad (AB)^* = A^* B^*, \qquad (UV)\dagger = U\dagger V\dagger, \tag{44}$$

but we now have

$$(A^*)^* = \bar{A}, \qquad (U\dagger)\dagger j = jU, \qquad [(X + Yj)\dagger]\dagger = \bar{X} + \bar{Y}j, \tag{45}$$

of which the last two equations are equivalent. Multiplication

$$(U + Vf)(G + Hf) = UG + VH\dagger t\xi j + (UH + VG\dagger)f \tag{46}$$

is easily verified to be associative. Also § 19 holds here. By (I),

$$c'y'\xi' = cy\xi, \qquad c = dy'\xi \qquad (d \text{ in } F)$$

As in § 20, $a^2 - \nu b^2 = -1$, while i is a root of

$$x^4 - 2bd\nu x^2 + \nu d^2 = 0. \tag{47}$$

The first condition is satisfied if $a = b = 1$, $\nu = 2$, and for $d = 1$ equation (47) becomes $x^4 - 4x^2 + 2 = 0$, which is irreducible in the field of rational numbers. *Hence we have an algebra for which* (*a*), (*b*), (*c*) *hold.*

Theorem 9. *If* a, b, d, t, g, ν *are numbers in the field* F *such that* $a^2 - \nu b^2 = -1$ *and such that* (47) *and* $\xi^2 = \nu$ *are irreducible in* F, *if* $y = a - b\xi$, $c = dy'\xi$, *and if* U *and* V *are numbers of the algebra* (16) *over* $F(\xi)$, *then the numbers* $U + Vf$, *subject to the law of multiplication* (46), *define a linear associative algebra with* 16 *units and having the properties* (*a*), (*b*), (*c*) *of* § 2.

22. Finally, let (I) and (II′) hold. Multiply (I) by j on the right and replace the fj introduced by its value in (II′). Thus

$$fk = y\omega c + yEkf.$$

Multiply this by k and eliminate the fk introduced. Then

$$-c'g'f = y^2(Ek)^2 f + y\omega c(1 + yE)k.$$

If $\omega \neq 0$, then $yE = -1$ and, by the coefficients of f, $cg = c'g'$. Now y and hence E is in $F(\xi)$, so that $\bar{E} = E$. Hence $y^2 E\bar{E} = 1$. Multiply this by c and apply (I). Thus $c'E\bar{E} = c$. But (32) then gives $\omega = 0$.

Hence $\omega = 0$. Consider the case $yE = -1$. By (I), $yy' = \mp 1$. Thus $E = \mp y'$, $g' = gy'^2$. Let $J = k$, $K = cj$. Then

$$fi = yif, \quad fJ = -Jf, \quad iJ = K, \quad J^2 = G, \quad K^2 = -cG,$$

where $G = -cg = G'$. Hence the algebra is equivalent to that in § 16.

As it is not our purpose to enumerate all the algebras A with 16 units, we do not consider the remaining values of E, nor an algebra in which (I′) holds.

Theorems 8 and 9 show that there exist linear associative algebras A with the properties (a), (b), (c), and distinct from their sub-algebras S. Hence the class of algebras A is more extensive than the class of primitive algebras L.