LINEAR ALGEBRAS*

BY

LEONARD EUGENE DICKSON

We consider linear algebras of which neither the associative nor the commutative law of multiplication is assumed, but which contain a modulus. It is shown in § 2 that every element X satisfies an equation whose degree is the number of units and which is derived from the well-known characteristic equation of a linear associative algebra by replacing X^3 by $X(XX)$, etc.. In § 3 there is developed a very simple theory of polynomials in these quasi powers XX, $X(XX)$, etc.

Linear algebras in which every element satisfies a quadratic equation are treated in §§ 5–7. By making either of two sets of further assumptions, we obtain algebras of the quaternion type.

While in §§ 1–7 the coördinates range over the elements of a general field (domain of rationality), we restrict attention in § 8 to commutative linear algebras in the field of real numbers with division always possible and unique.† It is shown that the numbers of units is at least six, and that if there be only six units the characteristic sextic is the equation of lowest degree which is satisfied by the general element of the algebra. Of linear algebras with a modulus, with real coördinates and with division uniquely possible, multiplication is associative but not commutative in the quaternion system, whereas multiplication is commutative but not associative in no algebra with fewer than six units.

In § 9 we exhibit commutative linear algebras with six units in which every element is a root of a quartic, but not of a quadratic or cubic, equation.

In § 10 it is shown ‡ that division is always possible and unique in CAYLEY's non-associative linear algebras in eight units with real coördinates.

1. **Definitions and notations.**—Given a field (domain of rationality) F and n elements $e_1, \cdots, e_n$, linearly independent with respect to F, and such that

$$e_i e_j = \sum_{k=1}^{n} \gamma_{ijk} e_k \qquad (i, j = 1, \ldots, n;\ \gamma\text{'s in } F), \tag{1}$$

* Presented to the Society at Minneapolis, December 28, 1910.

† For an extensive class of fields, not including the field of reals, commutative linear algebras in which division is uniquely possible are given in my papers in these Transactions, vol. 7 (1906), pp. 370–390, 514–522.

‡ Added November, 1911; presented to the Society at Chicago, December 29, 1911.

we shall say that the set of elements $\Sigma x_k e_k$, in which the x_k range over F, form a *linear algebra.* The sum, difference and product of two elements $X = \Sigma x_i e_i$ and $X' = \Sigma x'_i e_i$ are defined by

$$X \pm X' = \sum_{i=1}^{n} (x_i \pm x'_i) e_i, \qquad XX' = \sum_{i,j=1}^{n} x_i x'_j e_i e_j = \sum_{i,j,k} x_i x'_j \gamma_{ijk} e_k.$$

ultiplication is not assumed to be associative or commutative.

Given two elements X and Y of the algebra, $X \neq 0$, we can determine an e ement X' such that $XX' = Y$ if

$$\Delta(X) = \left| \sum_{i=1}^{n} x_i \gamma_{ijk} \right| = \begin{vmatrix} \Sigma x_i \gamma_{i11} & \cdots & \Sigma x_i \gamma_{in1} \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ \Sigma x_i \gamma_{i1n} & \cdots & \Sigma x_i \gamma_{inn} \end{vmatrix}$$

is not zero; we can determine X' such that $X'X = Y$ if

$$\Delta'(X) = \left| \sum_{i=1}^{n} x_i \gamma_{jik} \right|$$

is not zero. We call $\Delta(X)$ the *right hand determinant* of X, and $\Delta'(X)$ the *left hand determinant* of X.

We shall assume that e_1 is a modulus, viz., that $e_1 X = X e_1 = X$ for every element X We shall write 1 for e_1. Then, by (1) for $i = 1$ and $j = 1$ in turn,

$$\gamma_{1jj} = \gamma_{j1j} = 1, \qquad \gamma_{1jk} = \gamma_{j1k} = 0 \qquad (j \neq k). \tag{2}$$

Thus x_1 occurs only in the terms of Δ and Δ' lying in the main diagonal. Hence if we replace x_1 by $x_1 - \rho$, where ρ is an element of F, we obtain

$$\Delta(X - \rho) = \sum_{i=0}^{n} r_i \rho^i, \qquad \Delta'(X - \rho) = \sum_{i=0}^{n} l_i \rho^i,$$

called the *right and left hand characteristic determinants* of X. Equating them to zero, we obtain the *right and left hand characteristic equations.*

Avoiding the ambiguous symbol X^i, we shall set

$$X_0 = {}_0X = 1, \qquad X_1 = X, \qquad X_{i+1} = X_i X, \qquad {}_1X = X, \qquad {}_{i+1}X = X({}_iX).$$

If $\Sigma t_i X_i = 0$, X is called a *right hand root* of the equation $\Sigma t_i \rho^i = 0$; if $\Sigma t_i ({}_iX) = 0$, X is a *left hand root.*

2. **Theorem.** *Every element of a linear algebra is a left hand root of the right and characteristic equation and a right hand root of the left hand characteristic equation; namely, for any element* X,

$$\sum_{i=0}^{n} r_i ({}_iX) = 0, \qquad \sum_{i=0}^{n} l_i X_i = 0. \tag{3}$$

Denote by $x_1', \cdots, x_n'$ the co-factors of the elements in the first row of the determinant $\Delta(X)$. Multiply them by the corresponding elements of the kth row of $\Delta(X)$ and add the products. We obtain the coefficient y_k of e_k in $Y = XX'$. Hence $y_1 = \Delta$, $y_k = 0\ (k > 1)$. Thus $XX' = \Delta$. Replace x_1 by $x_1 - \rho$ and let X' become $F = \Sigma_{i=0}^{n-1} F_i \rho^i$, where the F_i are elements of the algebra. Then

$$(X - \rho) F = \sum_{i=0}^{n} r_i \rho^i .$$

Equating coefficients of like powers of ρ, we get

$$XF_0 = r_0,\ XF_1 - F_0 = r_1,\ \cdots,\ XF_{n-1} - F_{n-2} = r_{n-1},\ -F_{n-1} = r_n .$$

Multiply on the left the second equation by X, the third by X twice, the fourth by X three times, etc. By adding we get $\Sigma r_i ({}_iX) = 0$.

The proof* of $\Sigma l_i X_i = 0$ is similar.

3. Linear combinations of the right hand† powers X_i of an element X of a linear algebra have certain properties analogous to those of polynomials in a scalar variable. Set

$$B_0 = \sum_{j=0}^{\beta} b_j X_j, \qquad B_k = B_{k-1} X = \sum_{j=0}^{\beta} b_j X_{j+k} .$$

Lemma. If $a = bc + d$, where

$$a = \sum_{i=0}^{\alpha} a_i \rho^i, \qquad b = \sum_{i=0}^{\beta} b_i \rho^i, \qquad c = \sum_{i=0}^{\gamma} c_i \rho^i, \qquad d = \sum_{i=0}^{\delta} d_i \rho^i,$$

then, for every element X of a linear algebra,

$$\sum_{i=0}^{\alpha} a_i X_i = \sum_{k=0}^{\gamma} c_k B_k + \sum_{i=0}^{\delta} d_i X_i .$$

For proof, set $a_i' = a_i - d_i$, $a' = a - d$. From $a' = bc$, we have

$$a_i' = \sum_{k=g}^{s} c_k b_{i-k} \quad (g = \text{greater of } 0,\ i - \beta;\ s = \text{smaller of } \gamma$$

For $0 \leqq k \leqq \gamma$, the coefficients of X_i in B_k is b_{i-k} or zero according as $i - \beta \leqq k \leqq i$ or not.

Corollary I. If X is a root of

$$B_0 = \sum_{j=0}^{\beta} b_j X_j = 0$$

---

* Bulletin of the American Mathematical Society, vol. 17 (1911), p. 294. Under the assumption that multiplication is associative, the proof becomes essentially that by Frobenius, Berliner Sitzungsberichte, 1896, p. 601.

† Throughout the section we may replace right hand by left hand powers.

and if

$$\sum_{j=0}^{\beta} b_j \rho^j$$

is a factor of

$$\sum_{i=0}^{\alpha} a_i \rho^i,$$

then

$$\sum_{i=0}^{\alpha} a_i X_i = 0.$$

Corollary II. If X is a root of $\Sigma b_j X_j = 0$, but of no similar equation of lower degree, then $\Sigma a_i X_i = 0$ implies that $\Sigma a_i \rho^i$ has the factor $\Sigma b_j \rho^j$.

Theorem. *If $a = \Sigma a_i \rho^i$ and $b = \Sigma b_i \rho^i$ have the greatest common divisor $g = \Sigma g_i \rho^i$, and we set $G_0 = \Sigma g_i X_i$, $G_s = G_{s-1} X$, etc., then*

$$A_0 = \Sigma m_s G_s, \qquad B_0 = \Sigma n_t G_t, \qquad G_0 = \Sigma p_s A_s + \Sigma q_t B_t,$$

where the m, n, p, q are elements of F. In particular, A_0 and B_0 both vanish if and only if G_0 vanishes.

To simplify the notation, let Euclid's process to determine g terminate in three steps, so that

$$a = bc + d, \qquad b = de + f, \qquad d = fk + g, \qquad f = g.$$

In view of the above Lemma, we have

$$A_0 = \sum_{k=0}^{\gamma} c_k B_k + D_0, \qquad B_0 = \sum_{k=0}^{\epsilon} e_k D_k + F_0,$$

$$D_0 = \sum_{k=0}^{\kappa} k_k F_k + G_0, \qquad F_0 = \sum_{k=0}^{\lambda} l_k G_k.$$

By the last two equations, $D_0 = \Sigma v_j G_j$; by the second, $B_0 = \Sigma n_t G_t$; by the first, $A_0 = \Sigma m_s G_s$. Next, the second equation gives

$$B_k = \sum_{j=0}^{\epsilon} e_j D_{j+k} + F_k.$$

Replacing D_{j+k} by its value from the first equation, we see that the third equation gives G_0 as a linear element of the A_s and B_t.

4. Suppose that the general element X is a root of

$${}_mX = b_1({}_{m-1}X) + \cdots + b_{m-1}X + b_m,$$

but of no similar equation of lower degree. By the preceding Cor. II, b_m is a factor of the right hand characteristic determinant $\Delta(X)$. Set

$$\Delta = b_m Q, \qquad C = {}_{m-1}X - b_1({}_{m-2}X) - \cdots - b_{m-1} = \sum_{i=1}^{n} c_i e_i.$$

Then $XC = b_m$. Let $m_1, \cdots, m_n$ be the co-factors of the elements of the first row of $\Delta(X)$ and set $M = \Sigma m_i e_i$. By § 2, $XM = \Delta$. Since Q is a scalar,

$$X(QC) = (XC)Q = b_m Q = \Delta = XM, \qquad X(M - QC) = 0.$$

Then $XX' = 0$ for every X, where $X' = M - QC$. The coördinates x_j' of X' are polynomials in $x_1, \cdots, x_n$. Then $x_j' \Delta(x)$ is identically zero in $x_1, \cdots, x_n$, while $\Delta(x)$ is not (§ 1). Thus $x_j' = 0, X' = 0$. Hence $M = QC$, $m_i = Qc_i$.

*Linear algebras in which every element satisfies a quadratic equation.**

5. Let the square of every element be a linear function of that element with coefficients in a field F not having modulus 2. Since $e^2 = a + be$, $(e - b/2)^2$ is an element of F. Hence we take the fundamental units to be $1, e_1, \cdots, e_m$, where $e_i^2 = s_{ii}$, an element of F. We shall introduce new units $1, E_1, \cdots, E_m$ such that

(4) $$E_k^2 = c_k, \qquad E_k E_l + E_l E_k = 0 \quad (l, k = 1, \ldots, m;\ l \neq k),$$

where the c_k are elements of F. The case $m = 1$ requires no attention. For $m > 1$, $i \neq j$, $(e_i \pm e_j)^2$ is a linear function of $e_i \pm e_j$. Hence $e_i e_j + e_j e_i$ is a linear function of $e_i + e_j$, also a linear function of $e_i - e_j$, and hence is an element of F:

$$e_i e_j + e_j e_i = 2s_{ij} = 2s_{ji} \qquad (i, j = 1, \ldots, m).$$

Let $u_1, \cdots, u_m$ be arbitrary elements of F and set $U = \Sigma u_k e_k$. Then

$$U^2 = Q \equiv \sum_{k,\,l=1}^{m} s_{kl} u_k u_l.$$

By a linear transformation with coefficients in F,

$$u_k = \sum_{l=1}^{m} a_{kl} v_l \qquad (k = 1, \ldots, l;\ |a| \neq 0)$$

Q can be reduced to the form $\Sigma c_i v_i^2$. Set

$$E_l = \sum_{k=1}^{m} a_{kl} e_k \qquad (l = 1, \ldots, m).$$

* Sections 5–7 were read before the Mathematical Club of the University of Chicago, May 18, 1906.

Then $1, E_1, \cdots, E_m$ are linearly independent with respect to F and may be taken as new units. Now

$$U = \sum_{k,l} a_{kl} v_l e_k = \sum_l v_l E_l, \qquad U^2 = \sum_{k,l} v_k v_l E_k E_l = \Sigma c_i v_i^2.$$

Hence relations (4) hold.

Conversely, when these relations hold, every element

$$X = x_0 + \sum_{k=1}^{m} x_k E_k \tag{5}$$

of the algebra satisfies a quadratic equation:*

$$X^2 - 2x_0 X + \sigma = 0, \qquad \sigma \equiv x_0^2 - \sum_{k=1}^{m} c_k x_k^2. \tag{6}$$

This quadratic is the equation of lowest degree with coefficients in F satisfied by an element X not in F. Thus, by § 4, σ is a factor of $\Delta(X)$ and the cofactors of the elements of the first row of Δ are $qx_0, -qx_1, \cdots, -qx_m$, where $q = \Delta/\sigma$.

If X is a root of a quadratic, all products of n factors each X are equal and may be designated by X^n.

6. Consider algebras (4) for which a product vanishes only when one factor vanishes. Then each c_k is a not-square in F. Further, $E_i E_j$ is linearly independent of $1, E_i, E_j$. For, if

$$E_i E_j = a + bE_i + cE_j,$$

then

$$(E_i - c)(E_j + sE_i + t) = 0, \qquad s = \frac{a + bc}{c^2 - c_i}, \qquad t = \frac{bc_i + ac}{c^2 - c_i}.$$

Hence $m \geqq 3$ and, by interchanging $E_3, \cdots, E_m$, we may assume that $\gamma_{123} \neq 0$. Thus we may introduce the new units

$$E_1' = E_1, \qquad E_2' = E_2, \qquad E_3' = \sum_{k=3}^{m} \gamma_{12k} E_k, \qquad E_i' = E_i + \rho_i E_3' \quad (i \geqq 4).$$

Then $E_3'^2$ is the constant $\Sigma \gamma_{1k}^2 c_k$, not zero, which we shall designate by c_3'. Taking $\rho_i = -c_i \gamma_{12i}/c_3'$, we find that

$$E_3' E_i' + E_i' E_3' = 0, \qquad E_j' E_3' + E_3' E_j' = 0, \qquad E_j' E_i' + E_i' E_j' = 0 \quad (i \geqq 4, j = 1, 2).$$

These relations obviously remain true when any E_i' $(i \geqq 4)$ is replaced by a linear homogeneous function E_i'' of $E_4', \cdots, E_m'$. By the argument leading to

* For the field of all real members we may take $c_k = -1$. Then σ vanishes only if each $x_i = 0$. Thus every element $X \neq 0$ has an inverse $(2x_0 - X)/\sigma = X_1$. If multiplication is associative, $XY = Z$ has the solution $Y = X_1 Z$.

(4), we can choose linearly independent functions $E_4'', \cdots, E_m''$ such that

$$E_k''^2 = c_k'', \qquad E_k''E_l'' + E_l''E_k'' = 0 \quad (k, l = 4, \ldots, m;\ l \neq k).$$

Hence, dropping accents, we obtain a set of independent units satisfying relations (4) and also

$$(7) \qquad E_1E_2 = \gamma_{12} + \gamma_{121}E_1 + \gamma_{122}E_2 + E_3, \qquad E_iE_j = \gamma_{ij} + \sum_{k=1}^{m} \gamma_{ijk}E_k.$$

We now add the hypothesis that multiplication is associative. Thus

$$E_i(E_iE_j) = c_iE_j, \qquad (E_jE_i)E_i = c_iE_j,$$

$$0 = E_i(E_iE_j) + (E_iE_j)E_i = 2\gamma_{ij}E_i + 2c_i\gamma_{iji} + \sum_{k \neq i} \gamma_{ijk}(E_iE_k + E_kE_i).$$

Hence $\gamma_{ij} = 0$, $\gamma_{iji} = 0$. By (4), $\gamma_{ijk} = -\gamma_{jik}$. Hence $\gamma_{ijj} = 0$. Thus (7) gives $E_1E_2 = E_3$. Hence

$$E_3^2 = E_1E_2 \cdot E_1E_2 = -E_1^2E_2^2, \qquad c_3 = -c_1c_2.$$

If $m \geqq 4$, $E_1(E_2E_4) = E_3E_4$. But

$$(E_3E_4)^2 = -c_3c_4, \quad (E_1E_2E_4)^2 = -E_1E_2E_1E_4E_2E_4 = E_1^2(E_2E_4)^2 = -c_1c_2c_4.$$

Thus $c_3 = c_1c_2$, in contradiction with $c_3 = -c_1c_2$. Hence $m = 3$. Now

$$E_1E_3 = E_1(E_1E_2) = c_1E_2, \qquad E_3E_2 = (E_1E_2)E_2 = c_2E_1.$$

Hence, by (4), we have

$$(8) \qquad \begin{aligned} &E_1^2 = c_1, \quad E_2^2 = c_2, \quad E_3^2 = -c_1c_2, \quad E_1E_2 = E_3 = -E_2E_1, \\ &E_1E_3 = c_1E_2 = -E_3E_1, \quad E_3E_2 = c_2E_1 = -E_2E_3. \end{aligned}$$

For this algebra we readily determine the conditions on c_1 and c_2 under which right and left hand division is always possible and unique. The general element may be written in the form $R + SE_2$, where $R = r + \rho E_1$ and $S = s + \sigma E_1$ belong to the field $F(E_1)$. Set $\bar{R} = r - \rho E_1$. Then $E_2R = \bar{R}E_2$. Hence

$$(X + YE_2)(R + SE_2) = XR + Y\bar{S}c_2 + (XS + Y\bar{R})E_2.$$

For R and S not both zero, we require that this product shall equal an arbitrarily assigned element of the algebra. A necessary and sufficient condition is that

$$\Delta = \begin{vmatrix} R & \bar{S}c_2 \\ S & \bar{R} \end{vmatrix} = R\bar{R} - c_2S\bar{S}$$

shall vanish only when $R = S = 0$. For $S = 0$, the condition requires that

$r^2 - \rho^2 c_1$ shall vanish only for $r = \rho = 0$, namely, that c_1 be a not-square. For $S \neq 0$, R/S is an element T of $F(E_1)$, and the condition requires that c_2 shall not be of the form $T\bar{T}$. Similarly,

$$(R + SE_2)(X + YE_2) = A + BE_2, \qquad A = RX + S\bar{Y}c_2, \qquad \bar{B} = \bar{S}X + \bar{R}\bar{Y},$$

the determinant of the coefficients of X and $\bar{Y}$ being Δ. Hence *right and left hand division is always possible and unique in algebra* (8) *if and only if c_1 is a not-square in the field F and c_2 is not expressible in the form $x^2 - c_1 y^2$, x and y in F.*

We have now determined the linear associative algebras with coördinates in a field F such that every element of the algebra satisfies a quadratic equation in F and such that right and left hand division is always possible and unique. The algebra is either F itself, a field $F(E_1)$ quadratic with respect to F, or one of type (8).

If F is the field of all real numbers, c_1 and c_2 may be taken to be -1 and (8) is then the quaternion system. Since a real polynomial in ρ is a product of real linear and quadratic factors, every element of an algebra satisfies a real quadratic equation. Hence the linear associative algebras in which division is unique and in which the coördinates range over the real numbers are the real, the complex and the quaternion number systems. This result is due to FROBENIUS* and C. S. PEIRCE.†

7. Consider algebra (4) for $m = 3$. Employing the notations (5) and (7_2), we find that the minor of the first element of the first row of $\Delta(X)$ is

$$M_0 = \begin{vmatrix} x_0 + x_2\gamma_{211} + x_3\gamma_{311} & x_1\gamma_{121} + x_3\gamma_{321} & x_1\gamma_{131} + x_2\gamma_{231} \\ x_2\gamma_{212} + x_3\gamma_{312} & x_0 + x_1\gamma_{122} + x_3\gamma_{322} & x_1\gamma_{132} + x_2\gamma_{232} \\ x_2\gamma_{213} + x_3\gamma_{313} & x_1\gamma_{123} + x_3\gamma_{323} & x_0 + x_1\gamma_{133} + x_2\gamma_{233} \end{vmatrix}.$$

From $M_0 = Qx_0$, we find by inspection that

$$Q = x_0^2 + x_0\sum_{i,j} x_i\gamma_{ijj} + \sum_{i,j} x_i x_j \begin{vmatrix} \gamma_{ijj} & \gamma_{jkj} \\ \gamma_{ijk} & \gamma_{jkk} \end{vmatrix} + \sum_i x_i^2 \begin{vmatrix} \gamma_{ijj} & \gamma_{ikj} \\ \gamma_{ijk} & \gamma_{ikk} \end{vmatrix},$$

where i, j, k form a permutation of $1, 2, 3$, while in the final sum $j < k$.

We discuss the algebras for which $Q \equiv \sigma$. By the coefficients of x_0,

$$\gamma_{133} = -\gamma_{122}, \qquad \gamma_{232} = -\gamma_{131}, \qquad \gamma_{233} = \gamma_{121}.$$

Then the conditions from the terms quadratic in x_1, x_2, x_3 become

$$\gamma_{122}\gamma_{121} + \gamma_{131}\gamma_{123} = 0, \qquad \gamma_{131}\gamma_{122} - \gamma_{132}\gamma_{121} = 0, \qquad \gamma_{121}\gamma_{131} + \gamma_{231}\gamma_{122} = 0,$$

$$\gamma_{122}^2 + \gamma_{123}\gamma_{132} = c_1, \qquad \gamma_{121}^2 - \gamma_{123}\gamma_{231} = c_2, \qquad \gamma_{131}^2 + \gamma_{132}\gamma_{231} = c_3.$$

---

* Journal für reine und angewandte Mathematik, vol. 84 (1878), p. 59.

† American Journal of Mathematics, vol. 4 (1881), p. 225.

Let each $c_i \neq 0$. In the second and third equations, the determinant of the coefficients of γ_{121}, γ_{122} is $-c_3$. Hence $\gamma_{121} = \gamma_{122} = 0$. By the first equation, $\gamma_{131} = 0$. Then

$$\gamma_{132} = c_1/\gamma, \qquad \gamma_{231} = -c_2/\gamma, \qquad c_1c_2 = -c_3\gamma^2, \qquad \gamma \equiv \gamma_{123}.$$

Replacing E_3 by $\gamma^{-1}E_3$, we have

$$(9) \qquad \begin{gathered} E_1^2 = c_1, \qquad E_2^2 = c_2, \qquad E_3^2 = -c_1c_2, \qquad E_1E_2 = E_3 + \delta_{12}, \\ E_1E_3 = c_1E_2 + \delta_{13}, \qquad E_2E_3 = -c_2E_1 + \delta_{23}. \end{gathered}$$

If the associative law holds, each $\delta_{ij} = 0$ and the algebra becomes (8).

We may specialize the δ_{ij} by applying to the E_i the transformation $(I + Z)^{-1}(I - Z)$, an automorph of $q = c_1v_1^2 + c_2v_2^2 + c_3v_3^2$, where I is the unit matrix, $Z = M^{-1}Y$, M being the matrix of q and Y being any skew symmetric matrix. Here $c_3 = -c_1c_2$. We find that $c_1E_2E_3$, $-c_2E_1E_3$, $c_3E_1E_2$ are transformed cogrediently with E_1, E_2, E_3; likewise, $c_1\delta_{23}$, $-c_2\delta_{13}$, $c_3\delta_{12}$. In particular, $c_1\delta_{23}^2 + c_2\delta_{13}^2 + c_3\delta_{12}^2$ is an absolute invariant.

Commutative linear algebras in the field of real numbers, with division always possible and unique.

8. The association law is not assumed. Let

$$X_m + a_1X_{m-1} + \cdots + a_m = 0$$

be the equation of lowest degree with real coefficients satisfied by a given element X of the algebra (cf. § 2). If X is not in the field of reals, we have $m > 1$. Then m must be even. For, if m were odd, then

$$\rho^m + a_1\rho^{m-1} + \cdots + a_m = (\rho + r)(\rho^{m-1} + b_1\rho^{m-2} + \cdots + b_{m-1}),$$
$$0 = X_m + a_1X_{m-1} + \cdots + a_m = (X + r)(X_{m-1} + \cdots + b_{m-1}),$$

whereas each factor is of degree $< m$ and hence not zero. Let n be the number of units. If $n = 2$, the algebra is the complex number system. Henceforth, let $n > 2$. Since algebra (4) is not commutative, not every element satisfies a quadratic equation. Hence three of our units may be taken to be 1, e_1, $e_2 = e_1^2$, where e_1 does not satisfy a cubic equation. Thus e_1e_2 is linearly independent of e_1 and e_2. Hence we may take as the fourth unit $e_3 = e_1e_2$.

Suppose that $e_2 + a + be_1 + ce_2 + de_3 = 0$. In the field of reals let

$$x^4 + a + bx + cx^2 + dx^3 = (x^2 + ex + f)(x^2 + gx + h).$$

Then

$$a = fh, \qquad f = eh + fg, \qquad c = f + h + eg, \qquad d = e + g.$$

Thus

$$0 = e_2^2 + a + be_1 + ce_2 + de_3 = (e_2 + ee_1 + f)(e_2 + ge_1 + h),$$

whereas neither factor is zero. Hence $n \geqq 5$ and we may take $e_4 = e_2^2$ as the fifth unit.

For $n = 5$, the general element X satisfies an equation of degree m, where m is even and $2 < m \leqq 5$; hence $m = 4$. For $n \geqq 6$, we make the assumption that $m = 4$. Thus

$$X \cdot X^3 = A + BX + CX^2 + DX^3. \tag{10}$$

In particular, $e_1 e_3 = A + \cdots + De_3$. Set $E_1 = e_1 + k$, $E_2 = E_1^2, \cdots$. Then

$$E_1 E_3 = \alpha + \beta E_1 + \gamma E_2 + (D + 4k) E_3.$$

Hence we may set $D = 0$ and

$$e_1 e_3 = be_2 + ce_1 + d.$$

Then $t^4 = bt^2 + ct + d$ has no real root. For, if so,

$$(e_1 - t)[e_3 + te_2 + (t^2 - b) e_1 + t^3 - tb - c] = 0.$$

Lemma. If e is linearly independent of $1, e_1, e_2, e_3$, then $e_1 e$ is linearly independent of $1, e_1, e_2, e_3, e$.

For, if $e_1 e = \alpha e + \beta e_3 + \gamma e_2 + \delta e_1 + \epsilon$, then

$$(e_1 - \alpha)(e + ye_3 + ze_2 + we_1 + \lambda)$$

vanishes when

$$z = \alpha y - \beta, \qquad w = (\alpha^2 - b) y - \alpha\beta - \gamma, \qquad \lambda = (\alpha^3 - \alpha b - c)y - \alpha^2\beta - \alpha\gamma - \delta,$$

$$(\alpha^4 - \alpha^2 b - \alpha c - d) y = \alpha^3\beta + \alpha^2\gamma + \alpha\delta + \epsilon.$$

Since α is real, the coefficient of y is not zero.

Taking $e = e_4$, we see that $n > 5$ and that the sixth unit may be chosen to be $e_5 = e_1 e_4$.

Let the algebra have only 6 units, $e_0 = 1, e_1, \cdots, e_5$. Then

$$e_1^2 = e_2, \qquad e_1 e_2 = e_3, \qquad e_2^2 = e_4, \qquad e_1 e_3 = be_2 + ce_1 + d, \qquad e_1 e_4 = e_5, \tag{11}$$

$$e_1 e_5 = \Sigma m_i e_i, \qquad e_2 e_3 = \Sigma f_i e_i, \qquad e_2 e_4 = \Sigma g_i e_i, \qquad e_2 e_5 = \Sigma h_i e_i. \tag{12}$$

Applying the Lemma for $e = xe_4 + ye_5$, where x and y are not both zero, we see that $xe_5 + y(m_4 e_4 + m_5 e_5)$ is not a multiple of $xe_4 + ye_5$. Hence

$$\begin{vmatrix} ym_4 & x + ym_5 \\ x & y \end{vmatrix} \neq 0, \qquad m_5^2 + 4m_4 < 0.$$

Thus $m_4 < 0$ and we may set $m_4 = -1/r^2$. For $E_i = r^i e_i$,

$$E_2 = E_1^2, \quad E_3 = E_1 E_2, \quad E_4 = E_2^2, \quad E_5 = E_1 E_4, \quad E_1 E_5 = \sum_{i<4} m_i' E_i - E_4 + rm_5 E_5.$$

Hence we may set $m_4 = -1$, $0 \leqq m_5 < 2$ in the initial formulas.

The characteristic determinant for $X = x_0 + x_1e_1 + x_2e_2$ is

$$\Delta = \begin{vmatrix} x_0 & 0 & 0 & x_1 d + x_2 f_0 & x_2 g_0 & x_1 m_0 + x_2 h_0 \\ x_1 & x_0 & 0 & x_1 c + x_2 f_1 & x_2 g_1 & x_1 m_1 + x_2 h_1 \\ x_2 & x_1 & x_0 & x_1 b + x_2 f_2 & x_2 g_2 & x_1 m_2 + x_2 h_2 \\ 0 & x_2 & x_1 & x_0 \quad + x_2 f_3 & x_2 g_3 & x_1 m_3 + x_2 h_3 \\ 0 & 0 & x_2 & x_2 f_4 & x_0 + x_2 g_4 & - x_1 \quad + x_2 h_4 \\ 0 & 0 & 0 & x_2 f_5 & x_1 + x_2 g_5 & x_0 + x_1 m_5 + x_2 h_5 \end{vmatrix}.$$

Set

$$X^3 - B - CX - DX^2 = \Sigma c_i e_i .$$

Then, by (10) and §4, the co-factor F_i of the ith element of the first row of Δ equals Qc_i, where $Q = \Delta / A$. Now

$$c_5 = x_1 x_2^2 (1 + 2f_5) + x_2^3 g_5, \qquad c_4 = x_1^2 x_2 + x_2^2 l, \qquad l \equiv 3x_0 + g_4 x_2 - D.$$

Thus F_5 has the factor x_2^2. But

$$F_5 = x_1^3 x_2 \{ x_0 (1 + f_5) - x_1 f_4 \} + x_2^2 (\ ).$$

Hence $f_4 = 0$, $f_5 = -1$, $c_5 = x_2^2 (g_5 x_2 - x_1)$. Then F_5 is divisible by c_5 if and only if

$$g_3 = g_5^3 + 2g_5(g_4 - f_3), \quad g_1 = g_2 g_5 - 2f_1 g_5 + (2f_2 - g_3 - 2c) g_5^2 + (g_4 + 2b - 2f_3) g_5^3,$$

the quotient being

$$Q = - x_0^2 - g_5 x_0 x_1 + x_0 x_2 (f_3 - 2g_4 - g_5^2) + x_1^2 (b + g_4 - f_3) + x_1 x_2 Y + x_2^2 Z,$$

$$Y \equiv f_2 - g_3 - c + (g_4 + 2b - 2f_3) g_5,$$

$$Z \equiv g_2 - f_1 + (2f_2 - g_3 - 2c) g_5 + (g_4 + 2b - 2f_3) g_5^2 .$$

The conditions for $F_4 = Qc_4$ reduce to $l = - x_0 - (b + 1) x_2$ and*

$$m_5 = g_5, \quad f_3 = g_4 + b + 1, \quad h_5 = g_5^2 - b - 1, \quad h_4 = f_2 - c - g_5, \quad m_3 = g_3,$$

$$h_3 = 2f_1 - g_2 - 2f_2 g_5 + 2cg_5 + g_3 g_5 + 2g_5^2 + 2g_4 (b + 1),$$

$$m_2 = f_1 - f_2 g_5 + cg_5 + g_5^2 + g_4 (b + 1),$$

$$h_2 = m_1 + g_5 m_2 + bg_3, \qquad h_1 = Z (b + 1) - h_5 f_1 .$$

Giving notations to $e_3^2, \cdots, e_4 e_5$, we set

(13) $X = \Sigma x_i e_i, \quad X^2 = \Sigma L_i e_i, \quad X^3 = \Sigma G_i e_i, \quad X \cdot X^3 = \Sigma M_i e_i \quad (i = 0, 1, \ldots, 5).$

* These and the earlier relations are together equivalent to those obtained by requiring that $e_2 + xe_1$ shall satisfy an equation (10).

Then, by (10),

$$M_i = Bx_i + CL_i + DG_i \qquad (i = 1, \ldots, 5). \tag{14}$$

First, set $x_0 = x_4 = x_5 = 0$. Eliminating B, and then C, D we have

$$\Delta_{ij} = \begin{vmatrix} M_i x_j - M_j x_i & L_i x_j - L_j x_i & G_i x_j - G_j x_i \\ M_4 & L_4 & G_4 \\ M_5 & L_5 & G_5 \end{vmatrix} = 0 \quad (i, j = 1, 2, 3).$$

The terms with the factor x_1^6 in Δ_{23} and Δ_{13} were obtained and the resulting conditions on the constants derived. Also $L_4 M_5 - L_5 M_4$ must be divisible by $L_4 G_5 - L_5 G_4$, the quotient being D. Finally, $M_5 - DG_5$ must be divisible by L_5, the quotient being C. Similarly, for $x_0 = x_2 = x_3 = 0$, the analogous determinants Δ_{15} and Δ_{45} were examined; by the terms of highest degree in x_1, we get

$$g_4 = 3 + 3b - 4g_5^2, \qquad f_2 = c + 4g_5 - 2g_5^3.$$

For $x_0 = x_5 = 0$, the terms in $x_1^2 x_4^2$, $x_1 x_2^2 x_4$, $x_1 x_2 x_3 x_4$ of $M_5 - DG_5 - CL_5 = 0$ yield

$$m_2 = g_2 + 4 + 8b + 4b^2 - 8bg_5^2 - 4g_5^2 + 3g_5^4.$$

Hence, writing $g = g_5$,

$$Q = -x_0^2 - gx_0x_1 + (3g^2 - 2 - 2b)\,x_0x_2 - x_1^2 + (g + g^3 - bg)\,x_1x_2 + (2g^2 - 2g^4 + 3bg^2 - b^2 - 2b - 1)x_2^2,$$

$$-4Q = [2x_0 + gx_1 + (2 + 2b - 3g^2)\,x_2]^2 + (4 - g^2)\,(x_1 - gx_2)^2,$$

the additional term in x_2^2 having the coefficient zero. Hence Q and therefore Δ vanishes for values of the x_i not all zero, so that division is not always uniquely possible.

Theorem. *If division is always possible and unique in a commutative linear algebra with coördinates ranging over all real numbērs, the number of units is at least six. If there are only six units, the characteristic sextic is the equation of lowest degree satisfied by the general element of the algebra.*

Commutative linear algebras with six units in which every element is a root of a quartic equation.

9. Consider a commutative algebra of type (11)–(12), in which every element satisfies a quartic equation, and $m_4 = -1$, as before. Replacing e_1 by $e_1 + k$, we may take $c = 0$. To s'mplify the formulas and computation set $b = -1$,

$g_2 = g_5 = m_1 = 0$. The only such algebras may be shown to be those satisfying (11) and

$$(15)\quad \begin{gathered} e_1e_5 = m - e_4, \quad e_2e_3 = f - e_5, \quad e_2e_4 = g, \quad e_2e_5 = h, \\ e_3^2 = \alpha - e_4, \quad e_3e_4 = \delta, \quad e_3e_5 = E, \quad e_4^2 = \beta, \quad e_4e_5 = K, \quad e_5^2 = \gamma. \end{gathered}$$

We shall prove that in a commutative algebra defined by (11) and (15), every element $\Sigma x_i e_i$ satisfies a quartic equation. It suffices to treat the elements with $x_0 = 0$. Then, in (13),

$$L_0 = 2dx_1x_3 + 2mx_1x_5 + 2fx_2x_3 + 2gx_2x_4 + 2hx_2x_5 + \alpha x_3^2 + 2\delta x_3x_4 + 2Ex_3x_5 + \beta x_4^2 + 2Kx_4x_5 + \gamma x_5^2,$$

$$L_1 = 0, \qquad L_2 = x_1^2 - 2x_1x_3, \qquad L_3 = 2x_1x_2,$$

$$L_4 = -2x_1x_5 + x_2^2 - x_3^2, \qquad L_5 = 2x_1x_4 - 2x_2x_3,$$

$$G_0 = f(L_2x_3 + L_3x_2) + g(L_2x_4 + L_4x_2) + h(L_2x_5 + L_5x_2) + dL_3x_1 + \alpha L_3x_3 + \delta(L_3x_4 + L_4x_3) + E(L_3x_5 + L_5x_3) + \beta L_4x_4 + K(L_4x_5 + L_5x_4) + mL_5x_1 + xL_5x_5,$$

$$G_1 = L_0x_1, \qquad G_2 = L_0x_2 - L_3x_1, \qquad G_3 = L_0x_3 + L_2x_1,$$

$$G_4 = L_0x_4 + L_2x_2 - L_3x_3 - L_5x_1, \qquad G_5 = L_0x_5 - L_2x_3 - L_3x_2 + L_4x_1,$$

$$M_1 = G_0x_1, \quad M_2 = G_0x_2 + G_1x_1 - G_1x_3 - G_3x_1, \quad M_3 = G_0x_3 + G_1x_2 + G_2x_1,$$

$$M_4 = G_0x_4 - G_1x_5 + G_2x_2 - G_3x_3 - G_5x_1,$$

$$M_5 = G_0x_5 + G_1x_4 - G_2x_3 - G_3x_2 + G_4x_1.$$

We obtain M_0 from G_0 by replacing L_i by G_i and adding $dG_1x_3 + mG_1x_5$.

We may now show that X satisfies a quartic equation (10) with $D = 0$. Consider the conditions (14). For $i = 1$, we get $M_1 = Bx_1$, whence $B = G_0$. Then for $i = 3$,

$$G_1x_2 + G_2x_1 = 2x_1x_2C, \qquad 2x_1x_2(L_0 - x_1^2 - C) = 0, \qquad C = L_0 - x_1^2.$$

For these values of B, C, D, conditions (14), with $i = 2, 4, 5$, are seen at once to become identities when the G's are expressed in terms of the L's and L_i in the one term L_0L_i is expressed in terms of the x's. Finally, there remains only the condition $M_0 = A + CL_0$. Hence $X = x_1e_1 + \cdots + x_5e_5$ is a root of

$$(16)\qquad X \cdot X^3 = M_0 - L_0(L_0 - x_1^2) + G_0X + (L_0 - x_1^2)X^2.$$

In particular, when $d, m, \cdots, \gamma$ are zero, we have

$$(17)\quad \begin{aligned} &e_1^2 = e_2, \quad e_1 e_2 = e_3, \quad e_1 e_3 = -e_2, \quad e_1 e_4 = e_5, \quad e_1 e_5 = e_3^2 = -e_4, \quad e_2^2 = e_4, \\ &e_2 e_3 = -e_5, \quad e_2 e_4 = e_2 e_5 = e_3 e_4 = e_3 e_5 = e_4^2 = e_4 e_5 = e_5^2 = 0. \end{aligned}$$

In a commutative algebra of this type, $x_1 e_1 + \cdots + x_5 e_5$ is a root of

$$(18)\qquad X \cdot X^3 + x_1^2 X^2 = 0,$$

but not of a cubic or quadratic equation. The general element $x = X + x_0$ is therefore a root of

$$(19)\quad x \cdot x^3 - 4x_0 x^3 + (x_1^2 + 6x_0^2)\,x^2 - (2x_0 x_1^2 + 4x_0^3)x + x_0^2 x_1^2 + x_0^4 = 0.$$

Uniqueness of division in Cayley's algebras with eight units.

10. CAYLEY * gave, as a direct generalization of quaternions, a linear algebra with eight units in which the modulus of a product equals the product of the moduli of the factors, each modulus being a sum of eight squares. By changing the sign of the final unit we obtain one of the two algebras obtained by CAYLEY † in his complete enumeration of certain types of algebras which possess this property of eight squares. Either of these two algebras may be obtained by changing the signs of $e_2, \cdots, e_7$ in the other. The algebra are distinguished by the sign of $\epsilon_7 = \pm 1$; that with $\epsilon_7 = +1$ has the units $1, e_1, \cdots, e_7$, where

$$e_i^2 = -1, \qquad e_i e_j = -e_j e_i \qquad (i, j = 1, \cdots, 7;\ i \neq j),$$

$$e_1 e_2 = e_3, \quad e_1 e_4 = e_5, \quad e_1 e_6 = e_7, \quad e_2 e_5 = e_7, \quad e_3 e_4 = e_7, \quad e_3 e_5 = e_6, \quad e_4 e_2 = e_6,$$

with fourteen equations obtained by permuting the subscripts cyclically

Since the modulus of any element is the sum of the squares of its coördinates, any element except zero has an inverse, the coördinates being assumed real. Since the associative law does not hold, the existence of an inverse does not imply uniqueness of division. To prove the latter, we note that every element may be expressed as a linear function of e_2, e_4, e_6, with coefficients linear in e_1. For $B = r + se_1$, set $\bar{B} = r - se_1$. Let also C be linear in e_1. Then

$$e_j B = \bar{B} e_j, \qquad (Be_j)(Ce_j) = (B\bar{C}) e_j^2, \qquad (Be_j)(Ce_k) = (\bar{B}\bar{C})(e_j e_k) \qquad (j, k = 2, 4, 6;\ j \neq k).$$

Hence if the coefficients are linear in e_1, we have

$$(A + Be_2 + Ce_4 + De_6)(\alpha + \beta e_2 + \gamma e_4 + \delta e_6) = P + Qe_2 + Re_4 + Se_6,$$

$$P = A\alpha - B\bar{\beta} - C\bar{\gamma} - D\bar{\delta}, \qquad Q = A\beta + B\bar{\alpha} - \bar{C}\bar{\delta} + \bar{D}\bar{\gamma},$$

$$R = A\gamma + \bar{B}\bar{\delta} + C\bar{\alpha} - \bar{D}\bar{\beta}, \qquad S = A\delta - \bar{B}\bar{\gamma} + \bar{C}\bar{\beta} + D\bar{\alpha}.$$

* Philosophical Magazine, London, (3), vol. 26, (1845), p. 210.

† American Journal of Mathematics, vol. 4 (1881), pp. 293–296.

By multiplication and addition we derive

$$\sigma A = \bar{\alpha} P + \bar{\beta} Q + \bar{\gamma} R + \bar{\delta} S, \qquad \sigma B = -\beta P + \alpha Q + \bar{\delta} \bar{R} - \bar{\gamma} \bar{S},$$

$$\sigma C = -\gamma P - \bar{\delta} \bar{Q} + \alpha R + \bar{\beta} \bar{S}, \qquad \sigma D = -\delta P + \bar{\gamma} \bar{Q} - \bar{\beta} \bar{R} + \alpha S,$$

$$s\alpha = \bar{A} P + B \bar{Q} + C \bar{R} + D \bar{S}, \qquad s\beta = -B \bar{P} + \bar{A} Q - \bar{D} \bar{R} + \bar{C} \bar{S},$$

$$s\gamma = -C \bar{P} + \bar{D} \bar{Q} + \bar{A} R - \bar{B} \bar{S}, \qquad s\delta = -D \bar{P} - \bar{C} \bar{Q} + \bar{B} \bar{R} + \bar{A} S,$$

$$\sigma = \alpha \bar{\alpha} + \beta \bar{\beta} + \gamma \bar{\gamma} + \delta \bar{\delta}, \qquad s = A \bar{A} + B \bar{B} + C \bar{C} + D \bar{D}.$$

Hence if G and H are any given elements, $G \neq 0$, there is an unique solution X or Y of $XG = H$ or $GY = H$. *Right and left hand division except by zero is always possible and unique in these Cayley algebras.*