ON COMMUTATIVE LINEAR ALGEBRAS IN WHICH DIVISION IS ALWAYS UNIQUELY POSSIBLE*

BY

L. E. DICKSON

1. We consider commutative linear algebras in $2n$ units, with coördinates in a general field F, such that n of the units define a sub-algebra forming a field $F(J)$. The elements of the algebra may be exhibited compactly in the form $A + BI$, where A and B range over $F(J)$. As multiplication is not associative in general, A and B do not play the rôle of coördinates, so that the algebra is not binary in the usual significance of the term.† Nevertheless, by the use of this binary notation, we may exhibit in a very luminous form the multiplication-tables of certain algebras in four and six units, given in an earlier paper.‡ Proof of the existence of the algebras and of the uniqueness of division now presents no difficulty. The form of the corresponding algebra in $2n$ units becomes obvious. After thus perfecting and extending known results, we attack the problem of the determination of all algebras with the prescribed properties. An extensive new class of algebras is obtained.

2. Consider first algebra (VIII) of the paper cited. Let $x^2 - dx + c$ be irreducible in F, c being a not-square. The units are $1, I, J, K$, with

$$I^2 = J, \qquad IJ = JI = K, \qquad IK = KI = c,$$

$$J^2 = dJ - c, \qquad JK = KJ = dK - cI, \qquad K^2 = cd - cJ.$$

The elements $Y = y + \eta J$, y and η ranging over F, form a field $F(J)$. In this field $x^2 - dx + c = 0$ has the roots J and $J' = c/J$. Set $Y' = y + \eta J'$. Then if B and Y are any two elements of $F(J)$, we readily find that

$$(1) \qquad B(YI) = (BY)I, \qquad (BI)(YI) = B'Y'J.$$

---

* Presented to the Society at the New Haven summer meeting, September 3, 1906. Received for publication July 2, 1906.

† A binary algebra in which division is always possible is a field.

‡ Transactions, vol. 7 (1906), pp. 370-390, algebras (VIII), (X).

The rule of multiplication of any two elements of the algebra is thus

$$(2)\quad (A+BI)(X+YI)=R+SI,\quad R\equiv AX+B'Y'J,\quad S\equiv BX+AY.$$

To show that division is always uniquely possible, we let A, B, R, S be any marks of $F(J)$ such that A and B are not both zero, and prove that marks X and Y can be uniquely determined so as to satisfy (2). Eliminating X, we get

$$(3)\qquad BB'Y'J-A^2Y=C,\qquad C\equiv BR-AS.$$

It suffices to show that Y can be found in $F(J)$ to satisfy (3) and

$$(3')\qquad -A'^2Y'+BB'YJ'=C'$$

This can be done since $cB^2B'^2-A^2A'^2\neq 0$, c being a not-square in F.

3. We next indicate the essential point in the proof that algebra (X) on six units, treated in § 5 of the paper cited, can be exhibited in the luminous form (2). Now j (our present J) is a root of

$$(4)\quad x^3-(2d_3+d_3d_5-c^{-1}d_1^2)x^2-(d_1-d_1d_5-d_3^2-d_3^2d_5+c^{-1}d_1^2d_3)x-c=0,$$

where

$$c^2+c^2d_5+c^2d_5^2+cd_1d_3+cd_1d_3d_5-d_1^3=0.$$

Equation (4) *is a normal cubic.* Indeed, it has a second root l/j, viz.,

$$(5)\qquad j'=d_5^{-1}(j-d_3-d_1j^{-1}).$$

It is now a simple matter to verify (1), with $B=b_1+b_2j+b_3l$, etc.

4. The generalization to $2n$ units is now obvious. Consider any uniserial abelian equation, with coefficients in F,

$$(6)\qquad x^n-c_1x^{n-1}+c_2x^{n-2}-\cdots\pm c_n=0\quad (c_n \text{ a not-square in } F),$$

viz., an equation irreducible in F and having the roots

$$(7)\qquad J,\ J'=\theta(J),\ J''=\theta^2(J),\ \cdots,\ J^{(n-1)}=\theta^{n-1}(J)\quad [\theta^n(J)\equiv J],$$

where θ is a polynomial with coefficients in F. If A is a polynomial in J with coefficients in F, we denote $A(J')$ by A', $A(J'')$ by A'', etc. Then J is a not-square in the field $F(J)$. For, if $J=f^2$, then $J'=f'^2$, etc., so that $c_n\equiv JJ'J''\cdots$ would be the square of $ff'f''\cdots$, which is a mark of F. Consider the algebra with the $2n$ units

$$(8)\qquad J^r,\qquad IJ^r\qquad (r=0,1,\cdots,n-1),$$

subject to the multiplication-table implied by (2). To show that division is always uniquely possible, it suffices to prove that there exists a solution Y in $F(J)$ of equation (3). Writing down the $n-1$ equations obtained from (3) by passing to the conjugates, and solving the systems of n linear equations, we get

$$\Delta Y = \sum_{s=0}^{n-1} C^{(s)} BB'J \cdot B'B''J' \cdots B^{(s-1)} B^{(s)} J^{(s-1)} [A^{(s+1)}]^2 \cdots [A^{(n-1)}]^2,$$

$$\Delta = c_n B^2 B'^2 \cdots [B^{(n-1)}]^2 - A^2 A'^2 \cdots [A^{(n-1)}]^2.$$

Since c_n is a not-square in F, while A and B are not both zero, we have $\Delta \neq 0$. The resulting value of Y is seen to satisfy (3).

In conclusion, we note that if F is the $GF[p^m]$, $p > 2$, the algebra exists, since there are irreducible equations (6) with c_n a not-square in F. Indeed, $c_n = J^t$, $t \equiv 1 + p^m + p^{2m} + \cdots + p^{m(n-1)}$, so that c_n is a not-square in F if (and only if) $J^{\frac{1}{2}(p^{nm}-1)} = -1$, i. e., if J is a not-square in the $GF[p^{nm}]$. It thus suffices to take as (6) a primitive irreducible equation in F.

5. We pass to the problem of the determination of all commutative algebras with $2n$ units (8), where J is a root of (6) and $I^2 = J$, while in place of (1) the law of multiplication is*

$$(9) \qquad B(YI) = lBY + mB'Y' + I(uBY + wB'Y'),$$

$$(10) \qquad (BI)(YI) = LBY + MB'Y' + I(UBY + WB'Y'),$$

$l, \cdots, W$ being fixed marks of $F(J)$, the same for every B, Y.

In (9) set $Y = 1$, $B = 1$; then $Y = 1$, $B = J$. Hence

$$l + m = 0, \quad u + w = 1; \qquad lJ + mJ' = 0, \quad uJ + wJ' = J.$$

But $J \neq J'$. Hence $l = m = w = 0$, $u = 1$. In (10) set $B = Y = 1$, and apply $I^2 = J$. Hence $L + M = J$, $U + W = 0$. Thus (9) and (10) become

$$B(YI) = (BY)I,$$

$$(BI)(YI) = LBY + (J - L)B'Y' + IU(BY - B'Y').$$

The rule of multiplication of any two elements of the algebra is thus

$$(A + BI)(X + YI) = R + SI,$$

$$(11) \qquad R \equiv AX + LBY + (J - L)B'Y',$$

$$S \equiv BX + AY + U(BY - B'Y').$$

* The writer conjectures that every commutative linear algebra in four units in which division is unique satisfies these assumptions. By a tedious computation, this was established for the case in which F is the $GF[3]$.

Let A, B, R, S be any given marks of $F(J)$ such that A and B are not both zero. We seek the conditions under which marks X and Y of $F(J)$ can be uniquely determined so that (11) shall hold. By eliminating X, we are led to the equivalent problem to determine the conditions under which there is an unique solution Y in $F(J)$ of

$$YG + Y'H = C,$$

$$G \equiv A^2 + UAB - LB^2, \tag{12}$$

$$H \equiv (L - J)BB' - AB'U,$$

where $C \equiv AS - BR$ is a given mark. In (12) and

$$Y'G' + Y''H' = C', \qquad Y''G'' + Y'''H'' = C'', \cdots$$

$$Y^{(n-1)}G^{(n-1)} + YH^{(n-1)} = C^{(n-1)},$$

the determinant of the coefficients of $Y, Y', \cdots, Y^{(n-1)}$ equals

$$\Delta \equiv GG'G'' \cdots G^{(n-1)} - (-1)^n HH'H'' \cdots H^{(n-1)}. \tag{13}$$

If $\Delta \neq 0$, the values of $Y, \cdots, Y^{(n-1)}$, obtained by solving these n equations as linear equations, are seen to be conjugate. *Hence division is always uniquely possible if and only if* $\Delta = 0$ *implies* $A = B = 0$.

It will be convenient to set

$$E = L + \tfrac{1}{4}U^2, \qquad \alpha = A + \tfrac{1}{2}UB. \tag{14}$$

Then

$$G = \alpha^2 - EB^2, \qquad H = (E + \tfrac{1}{4}U^2 - J)BB' - U\alpha B'. \tag{15}$$

We first show that if $G = H = 0$ then $\alpha = B = 0$. For, if $B \neq 0$, then $\alpha = \kappa B$, $\kappa^2 = E$, κ in $F(J)$. Then $H = BB'\{\kappa - \tfrac{1}{2}U)^2 - J\}$. The last factor does not vanish since J is a not-square in $F(J)$.

Next, let $\Delta = 0$, $G \neq 0$. Then $H = \tau G$, where

$$\tau\tau'\tau'' \cdots \tau^{(n-1)} = (-1)^n. \tag{16}$$

We may make an important normalization. Set

$$\alpha = \alpha_1 x, \qquad B = B_1 x, \qquad G_1 = \alpha_1^2 - EB_1^2,$$

$$H_1 = (E + \tfrac{1}{4}U^2 - J)B_1B_1' - U\alpha_1 B_1'.$$

Then $H = H_1 xx'$, $G = G_1 x^2$, so that $H_1 = G_1 \tau x/x'$. It can be shown that, in view of (16), x can be so chosen in $F(J)$ as to make $\tau x/x' = (-1)^n$.

After this normalization, we have $H=(-1)^nG$. For $D=\alpha+\frac{1}{2}(-1)^nUB'$, this becomes

$$(17)\quad D^2-[B+(-1)^nB'][EB+\tfrac{1}{4}(-1)^nU^2B']+(-1)^nJBB'=0.$$

Hence division is uniquely possible in the algebra if and only if $D=0$, $B=0$ *is the only set of solutions in the field* $F(J)$ *of equation* (17).

We have therefore reduced a problem on homogeneous forms of degree $2n$ in $2n$ variables to a problem on quadratic forms.

6. THEOREM. *For* $n=2$, *division is uniquely possible if*

$$(18)\quad E=\frac{1}{4c_2}J^2U'^2,$$

$$(19)\quad \epsilon^2-4c_2U^2U'^2=\begin{cases}a\ not\text{-}square^*\ in\ F(J)\\ or\ a\ square\ in\ F\end{cases}\qquad(\epsilon\equiv J'U^2+JU'^2-4c_2).$$

When F *is a finite field, division is uniquely possible in no further algebras* (11) *except the field-algebra defined by* $U=0$, $E=L=J$.

The first part of the theorem is readily proved. We may set $U\neq 0$, since the case $U=0$, $E=L=0$, has been treated in § 2. If we multiply the conjugate of (17) by J/J' and apply $JJ'=c_2$, we find that the final terms are the same as those in (17); hence $D^2=D'^2J/J'$. Thus $J'D^2$ is an element e of F. But $D^2=(d+\delta J)^2=Je/c_2$ gives $d^2-c_2\delta^2=0$, from which $d=\delta=0$. We next find the conditions under which (17), with $D=0$, has a root $B\neq 0$ in $F(J)$. Let $B=XB'$, so that $XX'=1$. Multiplying (17) by $-4c_2$, completing the square in X and applying (18), we get

$$(20)\quad (2XJU'^2+\epsilon)^2=\epsilon^2-4c_2U^2U'^2,$$

where ϵ, given by (19), is a mark of F. The second member must equal the square of a mark R of $F(J)$. Thus $X=(R-\epsilon)/2JU'^2$. Since $XX'=1$,

$$(R-\epsilon)(R'-\epsilon)=4c_2U^2U'^2\equiv(R-\epsilon)(-R-\epsilon).$$

Hence $R'=-R$, so that the second member of (20) is a not-square in F.

Inversely, if the second member of (20) is a square R^2 in $F(J)$, but a not-square in F, there exists a mark $X=x+yJ$ in $F(J)$ which satisfies (20) and $XX'=1$. Then $B=XB'$ is satisfied by a mark $B=b+\beta J\neq 0$ in $F(J)$. Indeed, the determinant of the coefficients of b and β in the equivalent two linear equations is $x^2+xyc_1+y^2c_2-1$, which is zero since $XX'=1$.

When (18) *holds,* $D=0$, $B=0$ *is the only set of solutions of* (17), *for* $n=2$, *if and only if condition* (19) *is satisfied.*

* The first alternative does not occur when F is a finite field.

To prove the second part of the theorem it now suffices to show that either $U=0$, $E=J$, or else that condition (18) holds. We show that in the remaining cases (17) has a set of solutions $D=d+\delta J$, $B=b+\beta J$, $b\neq 0$. If t is a mark of F, then tB, tD are solutions when B, D are; hence we set $b=1$. Set also

$$E=e+fJ, \qquad \tfrac{1}{4}U^2=r+sJ. \tag{21}$$

Hence (17) is equivalent to the two equations

$$d^2-\delta^2 c_2-(2+\beta c_1)(e+r+\beta r c_1-\beta f c_2+\beta s c_2)=0, \tag{22}$$

$$2d\delta+\delta^2 c_1-(2+\beta c_1)(f+s+\beta e+\beta f c_1-\beta r)+1+\beta c_1+\beta^2 c_2=0. \tag{23}$$

For brevity we treat in detail only the case in which F is the $GF[p^m]$, p^m of the form $4k+1$. Then if ν is a not-square, so is also $-\nu$. Then * we may set $c_1=0$, $c_2=-\nu$, so that $J^2=\nu$.

Let first $f=s$, so that β does not occur in (22). Set

$$\tau=\beta\nu+e-r, \qquad \gamma=2e+2r, \qquad \kappa=\nu-4\nu s+(e-r)^2. \tag{24}$$

Then (22) and (23) become

$$d^2+\nu\delta^2-\gamma=0, \qquad \tau^2-\kappa-2\nu d\delta=0. \tag{25}$$

If $d^2+\nu\delta^2=d_1^2+\nu\delta_1^2$ and $d\delta=d_1\delta_1$, we readily find that

$$(d^2,\ \delta^2)=(d_1^2,\ \delta_1^2) \qquad \text{or} \qquad (\nu\delta_1^2,\ \nu^{-1}d_1^2).$$

In the second case, $d=\delta=d_1=\delta_1=0$. Hence if $\gamma\neq 0$, then $d=\pm d_1$, $\delta=\pm\delta_1$. But there are exactly p^m+1 sets of solutions d, δ of $d^2+\nu\delta^2=\gamma$ $(\gamma\neq 0)$ in the $GF[p^m]$. Hence there are $\frac{1}{2}(p^m+1)$ distinct values of the product $d\delta$ of such solutions. But only $\frac{1}{2}(p^m-1)$ marks are not-squares. Hence there is at least one set of solutions d, δ of (25_1) for which $\kappa+2\nu d\delta$ is a square, so that (25_2) is solvable for τ. Hence if $f=s$ then $e=-r$ by (24), so that (18) holds.

Let next $f\neq s$ and set, for brevity,

$$\begin{aligned} &\sigma=s-f, \qquad g=e+r, \qquad t=-4f-2\sigma+1, \\ &h=2g-2\sigma(2r-g), \qquad l=-4\nu t-4(2r-g)^2. \end{aligned} \tag{26}$$

On eliminating β between equations (22) and (23) with $c_1=0$, we get

$$(d^2+\nu\delta^2-h)^2=\sigma^2(8\nu d\delta-l) \qquad (\sigma\neq 0). \tag{27}$$

* For remarks on the principle that any quaternary algebra of the kind considered is equivalent to one in which the irreducible quartic $x^4-c_1x^2+c_2=0$ is any chosen one, see paper cited in § 1.

We wish to prove that $h=0$, $l=4\nu\sigma^2$ is the only set of values of the parameters h, l for which (27) is not solvable for d, δ. It suffices to prove this for the case $\sigma^2=1$ in view of the normalization

$$d=d_1\sigma, \qquad \delta=\delta_1\sigma, \qquad h=h_1\sigma^2, \qquad l=l_1\sigma^2.$$

The normalized problem is thus to find the values of the parameters h, l for which there is no set of solutions ρ, d, δ in F of the simultaneous equations

$$d^2+\nu\delta^2-h=\rho, \qquad 8\nu d\delta-l=\rho^2. \tag{28}$$

Such a set of solutions exists if and only if

$$\phi\equiv\rho+h+\tfrac{1}{4}\nu^{-1}(\rho^2+l)J$$

is a square in $F(J)$, viz., the square of $d+\delta J$. Hence ϕ must be a not-square and therefore ϕJ a square in $F(J)$. Thus must

$$f_\rho\equiv\tfrac{1}{4}(\rho^2+l)+(\rho+h)J=\text{square in } F(J) \text{ for every } \rho \text{ in } F. \tag{29}$$

Hence $f_\rho f'_\rho$ must be a square in F, viz.,

$$(\rho^2+l)^2-16\nu(\rho+h)^2=\text{square in } F \text{ for every } \rho. \tag{30}$$

It can be shown that this condition requires that the left member be algebraically a perfect square in ρ, so that $h=0$, $l=4\nu$. Restoring σ, we have $h=0$, $l=4\nu\sigma^2$. Let first $\sigma=-1$. Then, by (26),

$$r=0, \qquad t=-1-\epsilon^2/\nu, \qquad f=1+\epsilon^2/4\nu, \qquad s=f-1=\epsilon^2/4\nu.$$

But $r^2-\nu s^2$ must be a square. Hence $s=0$, $U=0$, $E=L=J$, so that the algebra is a field. The case $\sigma\neq-1$ is excluded since then

$$\epsilon=\frac{2r\sigma}{\sigma+1}, \quad t=-\sigma^2-\frac{1}{\nu}\left(\frac{2r}{\sigma+1}\right)^2, \quad f=\frac{(\sigma-1)^2}{4}+\frac{r^2}{\nu(\sigma+1)^2}, \quad s=\sigma+f,$$

$$r^2-\nu s^2=r^2-\nu\left\{\frac{(\sigma+1)^2}{4}+\frac{r^2}{\nu(\sigma+1)^2}\right\}^2=-\nu\left\{\frac{(\sigma+1)^2}{4}-\frac{r^2}{\nu(\sigma+1)^2}\right\}^2.$$

If we proceed without the specialization $c_1=0$, we find that, unless the algebra is a field, $e=-r$, $f=s+rc_1/c_2$, from which (18) follows.

7. It remains to determine which of the quaternary algebras (11) satisfying (18) and (19) are equivalent under a linear transformation of the units $1, I, J, K=IJ$. Let $(1, i, j, k)$ be equivalent to $(1, I, J, K)$. Then j and J are roots of $x^2-c_1x+c_2=0$. If $j=J$, then $i^2=j=J=I^2$, so that the algebras are identical or differ only in the sign of the parameter U. Let next $j=J'$,

so that $i^2 = J'$. We prove that, if F is a finite field, there exists an element $X + YI$ whose square is J'. By (11), the conditions are

$$(31)\quad X^2 + L(Y^2 - Y'^2) + JY'^2 = J', \qquad 2XY + U(Y^2 - Y'^2) = 0.$$

Set $U^2 = \lambda + \mu J$. Then by (14) and (18),

$$(32)\qquad L = \tfrac{1}{4}\lambda J(J - J')/c_2.$$

Set $Y^2 = e + fJ$. Then (31_2) becomes $XY = \frac{1}{2}Uf(J' - J)$. Substituting its square in (31_1) multiplied by Y^2, and applying (32), we get

$$ec_1 + fc_2 = 0, \quad -e = \tfrac{1}{4}(c_1^2 - 4c_2)[f^2\mu + \lambda f(e + c_1 f)/c_2] + e^2 + efc_1 + f^2 c_2.$$

But $e \neq 0$, since $Y = 0$ requires $X^2 = J'$, while J is a not-square. Hence

$$(33)\quad f = -ec_1/c_2, \quad e\omega = -4c_2^3, \quad \omega \equiv (c_1^2 - 4c_2)\{\mu c_1^2 c_2 - \lambda c_1(c_2 - c_1^2)\} + 4c_2^3.$$

For $U^2 = \lambda + \mu J$, (19) becomes, on multiplication by the not-square $c_1^2 - 4c_2$,

$$(34)\quad \lambda^2(c_1^2 - 4c_2)^2 - 8\lambda c_1 c_2(c_1^2 - 4c_2) - 16c_2^2(c_1^2 - 4c_2)(\mu - 1) = \text{not-square}.$$

We may now show that $\omega \neq 0$. As this is obvious when $c_1 = 0$, we set $c_1 \neq 0$. Then if $\omega = 0$, we have $c_2(c_1^2 - 4c_2)\mu$ expressed as a linear function of λ. Substituting this value in (34), we obtain for the left member

$$\{\lambda(c_1^2 - 4c_2) - 4(2c_2^2/c_1 - c_1 c_2)\}^2.$$

Thus e and f are uniquely determined in F by (33). Then

$$(35)\qquad i = \tfrac{1}{2}UAc_1(J' - J)/J + AJI, \qquad A^2 \equiv -e/c_2.$$

If u is the parameter of the algebra $(1, i, j, k)$, $u(j - j') \equiv u(J' - J)$ is the coefficient of i in ik. We readily find that

$$(36)\qquad u = c_2 AU(c_1 J^{-2} - J^{-1}) = AUJ'^3/c_2.$$

We proceed to prove that, if $U \neq 0$, the new algebra, with the parameter u, is distinct from the earlier algebras, with the parameters U and $-U$. Suppose that $u(j) = \pm U(J)$. Set $u' = u(J') \equiv u(j)$. Then must $u' \equiv \pm U$, as functions of J. Hence, by (36), $A'U'J^3 = \pm c_2 U$. Then $AUJ'^3 = \pm c_2 U'$. Forming the product, we get $AA'c_2 = 1$, since $JJ' = c_2$ and $U \neq 0$. But $A^2 = A'^2 = -e/c_2$. Hence $e^2 = 1$. If $e = -1$, then $A' = -A$; for, if A be a mark of the field F, c_2 would be a square. Then $AA'c_2 = 1$ and $A^2 = 1/c_2$ are contradictory. Hence $e = 1$. Thus $U'^2 J^6 + c_2^3 U^2 = 0$. Express the left

member as a linear function of J by applying $U^2 = \lambda + \mu J$, $J^2 - c_1 J + c_2 = 0$. Aside from the non-vanishing factor $c_1^2 - c_2$, the coefficient of J is

$$\mu c_2 (c_1^2 - 2c_2) + \lambda c_1 (c_1^2 - 3c_2) = 0. \tag{37}$$

The constant term equals $-c_1 c_2$ times the preceding expression. By (33), $\omega = -4c_2^3$, and $c_1 \neq 0$. We thus have two linear equations in λ and μ. We get

$$\lambda = \frac{-4c_2(c_1^2 - 2c_2)}{c_1(c_1^2 - 4c_2)}, \qquad \mu = \frac{4(c_1^2 - 3c_2)}{c_1^2 - 4c_2}, \tag{38}$$

where $c_1^2 - 4c_2$ is a not-square, being the discriminant of (6) with $n = 2$. The expression (19) is now found to reduce to

$$64c_2^4 \div c_1^2(c_1^2 - 4c_2),$$

a not-square in F. We have now proved the following

THEOREM. *Consider the set of all quaternary algebras* (11) *satisfying conditions* (18) *and* (19), *where J is a root of a fixed quadratic equation irreducible in the field F. When F is a finite field, the algebras with $U \neq 0$ are equivalent in sets of four, and the identity is the only transformation of such an algebra into itself.*

The algebra (2), *given by $U = 0$, is not equivalent to an algebra with $U \neq 0$, and admits exactly four transformations into itself, viz.,*

$$i = \pm I; \qquad i = \rho I, \qquad \text{where} \qquad \rho^2 = J^2/c_2.$$

THE UNIVERSITY OF CHICAGO,
June, 1906.