LINEAR ALGEBRAS IN WHICH DIVISION IS ALWAYS UNIQUELY POSSIBLE*

BY

LEONARD EUGENE DICKSON

§ 1. *Introduction; summary of results.*

Let the elements of an algebra be $A = \sum_{i=1}^{m} a_i e_i$, where the coördinates a_i range over a given field F, while the units e_i are linearly independent with respect to F and have a multiplication table,

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

Given two elements A and B with the a_i not all zero, we can determine an unique element X_r such that $AX_r = B$ and an unique element X_l such that $X_l A = B$ if and only if each of the determinants

$$\Delta_r \equiv \left| \sum_{i=1}^{m} \gamma_{ijk} a_i \right|, \qquad \Delta_l \equiv \left| \sum_{i=1}^{m} \gamma_{jik} a_i \right| \qquad (j, k = 1, \cdots, m)$$

does not vanish. Hence the condition that right hand [left hand] division shall always be uniquely possible is that Δ_r [Δ_l] shall vanish only when every a_i vanishes. Now either of these conditions is satisfied when the other is, since either is equivalent to the condition that a product shall vanish only when one factor vanishes. We consider algebras in which these conditions are satisfied and in which there is a modulus, i. e., an element 1 such that $1A = A1 = A$ for every element A. We shall henceforth set $e_1 = 1$.

For $m = 2$, the algebra is the field $F(e_2)$. Indeed, $e_2^2 - e_2\gamma_{222} - \gamma_{221} = 0$ is irreducible in F since $\Delta_r = a_1^2 + a_1 a_2 \gamma_{222} - a_2^2 \gamma_{221}$.

In § 2 I consider the general transformation of algebras with three units, exhibiting families of algebras invariant under every linear transformation and determining the algebras which admit more than one transformation into itself (and hence exactly three transformations). From each standpoint I am led to the same remarkable set of families of algebras, each set characterized by a parameter μ. For $\mu = 1$, the family consists of all fields of rank three with respect to F. For $\mu = 0$, the commutative algebras have the property that division is always possible.

* Presented to the Society (Chicago), April 14, 1906. Received for publication March 19, 1906.

In § 3 there is indicated a method of deducing an algebra of mk units from one of m units. In §§ 4, 5, there is indicated a method of constructing a remarkable algebra in m units, where m is any even integer greater than two, such that division is always possible. An important point in the theory is established in § 6 by the exhibition of two non-equivalent, non-field, commutative algebras in six units with coördinates in the same general field.

Throughout the paper I exclude fields with modulus 2.

§ 2. *Algebras with three units*, $1, i, j$.

Suppose first that, for every element e, e^2 is a linear function of e. Then $i^2 = ai + A$, $j^2 = bi + B$. Set $I = i - a/2$, $J = j - b/2$. Hence

$$I^2 = \alpha, \qquad J^2 = \beta, \qquad IJ = r + sI + tJ, \qquad JI = R + SI + TJ.$$

Applying the assumption to $e = I + lJ$ for $l = 1$ and -1 in turn, we find that $IJ + JI$ must be a constant. Hence $S = -s$, $T = -t$. We may assume that s and t are not both zero, since otherwise $(RI - \alpha J)I = 0$. We show that division by $E \equiv sI + tJ$ is not possible in general. If we express $(x + yI + zJ)E$ in the form $K + LI + MJ$, we find that $tL \equiv sM$. Hence arbitrary values cannot be given to both L and M.

Hence there exists an element e for which e^2 is linearly independent of e. We may therefore set $i = e, j = e^2$. Then

$$\text{(I)} \qquad i^2 = j, \qquad ij = b + \beta i + Bj, \qquad ji = a + \alpha i + Aj, \qquad j^2 = d + \delta i + Dj.$$

If $a = 0$ or $b = 0$ there exists no solution of $Xi = 1$ or $iX = 1$, respectively. Hence $a \neq 0, b \neq 0$. Suppose that $x^3 - b - \beta x - Bx^2 = 0$ has a root $x = -w$ in the field, and set $I = i + w$, $J = j + 2iw + w^2$. Then

$$I^2 = J, \qquad IJ = b - \beta w + Bw^2 + w^3 + (\beta - 2Bw - 3w^2)I + (B + 3w)J.$$

The constant term in IJ thus vanishes and the algebra is excluded. Similarly, the constant term in JI is $a - \alpha w + Aw^2 + w^3$ and hence would vanish if $-w$ is a root of $x^3 - a - \alpha x - Ax^2 = 0$. *Hence any triple algebra in a field F not having modulus 2 may be given the form* (I) *with $x^3 - b - \beta x - Bx^2$ and $x^3 - a - \alpha x - Ax^2$ irreducible in F.*

To algebra (I) we apply the transformation of units,

$$\text{(1)} \quad I = r + si + tj, \quad J = I^2 = \omega + \kappa i + \rho j \quad \left(\begin{matrix} \omega = r^2 + st(a+b) + t^2 d, \\ \kappa = 2rs + st(\alpha + \beta) + t^2 \delta, \\ \rho = s^2 + 2rt + st(A + B) + t^2 D \end{matrix} \right).$$

This transformation is valid when r, s, t are any marks such that s and t are not both zero.. In fact, we show that

$$C \equiv s\rho - t\kappa \equiv s^3 + s^2 t(A + B) + st^2(D - \alpha - \beta) - t^3 \delta$$

vanishes only when $s=t=0$. Replacing a_1, a_2, a_3 by r, s, t, respectively, we get

$$\Delta_r = \begin{vmatrix} r & ta & sb+td \\ s & r+t\alpha & s\beta+t\delta \\ t & s+tA & r+sB+tD \end{vmatrix}$$

Denote the minors of the elements of the first row in Δ_r by $\Delta', \Delta'', \Delta'''$. The latter, and hence also Δ_r, can be made to vanish if there exists a set of solutions s and t, not both zero, of $C=0$. Indeed, we then have $t \neq 0$ and we can determine r uniquely to satisfy $\Delta'''=0$. But upon substituting this value of r in $t\Delta''=0$ and $t^2\Delta'=0$, we get $C=0$ and $(s+At)C=0$, respectively.

Under the transformation (1) algebra (I) becomes.*

$$I^2=J, \qquad IJ=b'+\beta' I+B'J, \qquad JI=a'+\alpha' I+A'J, \qquad J^2=d'+\delta' I+D'J,$$

$$B'=3r+sB+t(\alpha+D), \qquad A'=3r+sA+t(\beta+D),$$

$$\beta'=-3r^2-2rt(\alpha+D)-2rsB+s^2\beta+st(a+b+\delta+\beta A-\alpha B)+t^2(d+\delta A-\alpha D),$$

$$\alpha'=-3r^2-2rt(\beta+D)-2rsA+s^2\alpha+st(a+b+\delta+\alpha B-\beta A)+t^2(d+\delta B-\beta D),$$

$$b'=r^3+r^2t(\alpha+D)+r^2sB-rs^2\beta-rst(\alpha+b+\delta+\beta A-\alpha B)-rt^2(d+\delta A-aD)+s^3b+s^2t(d+bA-aB)+st^2(dA-aD+a\beta-b\alpha)+t^3(a\delta-ad),$$

$$a'=r^3+r^2t(\beta+D)+r^2sA-rs^2\alpha-rst(a+b+\delta+\alpha B-\beta A)-rt^2(d+\delta B-\beta D)+s^3a+s^2t(d+aB-bA)+st^2(dB-bD+b\alpha-a\beta)+t^3(b\delta-d\beta),$$

$$D'=6r^2+2rs(A+B)+2rt(\alpha+\beta+2D)+s^2D+st[2a+2b-\delta+(A+B)(\alpha+\beta+D)]+t^2(D^2+2d+D\alpha+D\beta),$$

$$\delta'=-8r^3-4r^2s(A+B)-4r^2t(\alpha+\beta+2D)+2rs^2(\alpha+\beta-D)+rst[6\delta-2(A+B)(\alpha+\beta+D)]+rt^2[2\delta(A+B)-4D(\alpha+\beta)-2D^2]+s^3\delta+s^2t[2\delta(A+B)+(\alpha+\beta)(\alpha+\beta-D)]+st^2[\delta D+2\delta(\alpha+\beta)+\delta(A+B)^2-D(\alpha+\beta)(A+B)]+t^3[\delta^2+\delta D(A+B)-D^2(\alpha+\beta)],$$

$$d'=3r^4+2r^3s(A+B)+2r^3t(\alpha+\beta+2D)+r^2s^2(D-2\alpha-2\beta)+r^2t^2[D^2+3D(\alpha+\beta)-2d-2\delta(A+B)]+r^2st[(A+B)(\alpha+\beta+D)-2a-2b-5\delta]$$

* The simplest method of performing this computation is to identify the linear expressions in i, j for IJ and $b'+\beta' I+B'J$, etc. Then α', β' and D may be found by a single division by C; while a', b', d' follow without such a division. The computation was checked in various ways.

$$
\begin{aligned}
&- rs^2t\,[(\alpha+\beta)(\alpha+\beta-D)+2\delta(A+B)-4d]+rs^3(2a+2b-\delta)\\
&- rst^2\,[\delta D+2\delta(\alpha+\beta)+\delta(A+B)^2-2d(A+B)+2D(a+b)\\
&- D(\alpha+\beta)(A+B)]-rt^3\,[\delta^2+\delta D(A+B)-D^2(\alpha+\beta)\\
&+2d(\alpha+\beta)-2\delta(a+b)]-t^4\,[d^2+dD(\alpha+\beta)-\delta D(a+b)]\\
&+st^3\,[\delta(a+b)(A+B)-2d(a+b)-D^2(a+b)+\delta d+dD(A+B)\\
&- d(\alpha+\beta)(A+B)]+s^2t^2\,[dD+d(A+B)^2-(a+b)^2+2\delta(a+b)\\
&- D(a+b)(A+B)]+s^3t\,[2d(A+B)+(a+b)(\alpha+\beta-D)]+s^4d.
\end{aligned}
$$

The set of all algebras (I) in which division is uniquely possible is invariant under every transformation (1) with r and s not both zero. This property evidently holds for the set of commutative algebras. It holds for the larger set of all algebras (I) with $A=B$, $\alpha=\beta$, since then $A'=B'$, $\alpha'=\beta'$. Within the latter set of algebras there exist sub-sets such that each is invariant under the transformations (1) and such that d, δ and D are fixed rational integral functions of a, b, β, B. The totality of all fields (I_1) obviously forms such a sub-set. We proceed to determine all such sub-sets. Under the assumption that $A=B$, $\alpha=\beta$, we require that d', δ', D' shall be expressible as rational integral functions of a', b', β', B', with coefficients independent of r, s, t, a, b, β, B. Thus must $D'=\lambda\beta'+\mu B'^2$, whence

$$
\begin{gathered}
9\mu-3\lambda-6=0,\quad (\beta+D)(6\mu-2\lambda-4)=0,\quad B(6\mu-2\lambda-4)=0,\\
D=\lambda\beta+\mu B^2,\quad (\lambda-2)(a+b)+(\lambda+1)\delta+2\mu B(\beta+D)-2B(2\beta+D)=0,\\
(\lambda-2)d+\lambda(\delta B-\beta D)+(\mu-1)(D+\beta)^2+\beta^2=0.
\end{gathered}
$$

In case F has modulus 3 we assume * here and also below that F is the $GF[3^n]$. Then if $\beta+D=0$ and $B=0$, $C\equiv s^3-t^3\delta$ would be reducible. Hence, in every case,

$$
(2)\quad \begin{cases}
D=(3\mu-2)\beta+\mu B^2,\\
(a+b)(3\mu-4)+\delta(3\mu-1)+2\beta B\mu(3\mu-4)+2B^3\mu(\mu-1)=0,\\
d(3\mu-4)+\delta B(3\mu-2)+B^4\mu^2(\mu-1)\\
\qquad +B^2\beta\mu(3\mu-4)(2\mu-1)+\beta^2(\mu-1)(3\mu-1)(3\mu-4)=0.
\end{cases}
$$

Now it may be verified that also the last two relations hold true for the transformed algebra. For each value of μ, *the set of all the algebras* (I) *in which* $A=B$, $\alpha=\beta$, *and relations* (2) *hold is invariant under every transformation* (1) *with* r *and* s *not both zero.* Within each set, the sub-set of algebras

* Note that there exist infinite fields having modulus 3 such that there is an irreducible function of the form x^3-z, e. g., the totality of rational functions of a parameter z, with integral coefficients taken modulo 3.

with $a=b$ is invariant. The sub-sets given by $\mu=0$ and $\mu=1$ are respectively

$$(I_0) \qquad i^2=j,\ ij=ji=b+\beta i+Bj,\ j^2=4bB-\beta^2-8bi-2\beta j;$$

$$(I_1) \quad i^2=j,\ ij=ji=b+\beta i+Bj,\ j^2=bB+(b+\beta B)i+(\beta+B^2)j.$$

Let F be any field (not having modulus 2) for which

$$f(x)\equiv x^3-b-\beta x-Bx^2$$

is irreducible. Then algebra (I_1) is the *field* $F(i)$. We proceed to prove that the non-field * algebra (I_0) has the property that division is always uniquely possible. For (I_0) and (I_1), Δ_r is, respectively,

$$\begin{vmatrix} r & tb & sb+t(4bB-\beta^2) \\ s & r+t\beta & s\beta+t(-8b) \\ t & s+tB & r+sB+t(-2\beta) \end{vmatrix}, \qquad \begin{vmatrix} r & tb & sb+tbB \\ s & r+t\beta & s\beta+t(b+\beta B) \\ t & s+tB & r+sB+t(\beta+B^2) \end{vmatrix}.$$

Now the latter is transformed into the former by the replacement of r, s, t by $r+\beta t, s+2Bt, -2t$, respectively, the transformation being valid since F does not have modulus 2. But for a field, Δ vanishes only when $r=t=s=0$. *Division is always uniquely possible in the non-field algebra* (I_0), *where* b, β, B *are any marks of any field* (*not having modulus* 2) *for which* $x^3-b-\beta x-Bx^2$ *is irreducible.* †

Another remarkable family of algebras invariant under every transformation (1) is the set of all algebras (I) for which

$$A=B, \qquad \alpha=\beta=-\tfrac{1}{3}B^2, \qquad a+b+\delta+\tfrac{2}{3}B(D+\beta)=0,$$

$$d+\delta B-\beta D+\tfrac{1}{3}(D+\beta)^2=0.$$

The last two equations may be given the form

$$\delta=-a-b-\tfrac{2}{3}B(D-\tfrac{1}{3}B^2), \qquad d=B(a+b)-\tfrac{1}{3}D^2+\tfrac{5}{9}DB^2-\tfrac{7}{27}B^4,$$

so that $A, \alpha, \beta, \delta, d$ are given functions of a, b, B, D. But in this algebra division is not uniquely possible for an *arbitrary* field F. Indeed, for $x=y+\frac{1}{3}B$,

$$f(x)\equiv x^3-b+\tfrac{1}{3}B^2x-Bx^2=y^3+\tfrac{1}{27}B^3-b.$$

But if F is the $GF[p^n]$, and p^n is of the form $3l+2$, every mark is a cube, so that $f(x)$ is reducible for every b and B.

* Suppose, indeed, that algebras (I_0) and (I_1) are identical. Then, if F does not have modulus 3, $\beta=-\frac{1}{3}B^2$, $b=\frac{1}{27}B^3$, so that $f(x)$ vanishes for $x=\frac{1}{3}B$. If F has modulus 3, then $\beta=B=0$, and x^3-b is reducible in the $GF[3^n]$.

† For the case $B=0$, this algebra was given in my memoir on finite algebras, Göttingen Nachrichten, 1905, pp. 358-393.

We next discuss the equivalence (under a linear transformation of units) of algebras (I). Suppose first that F does not have modulus 2 or 3. Then we can so determine r, s, t (s and t not both zero) as to make $A' = B' = 0$. Hence we consider (I) for $A = B = 0$. The algebra obtained by applying transformation (1) will have $A' = B' = 0$ if and only if

$$r = -\tfrac{1}{3}t(\alpha + D) = -\tfrac{1}{3}t(\beta + D).$$

Let first $\alpha \neq \beta$. Then must $r = t = 0$. Hence $I = si$, $J = s^2 j$, and

$$b' = s^3 b,\ \beta' = s^2\beta,\ a' = s^3 a,\ \alpha' = s^2\alpha,\ D' = s^2 D,\ \delta' = s^3\delta,\ d' = s^4 d.$$

Now $\delta \neq 0$, in view of the irreducibility of C. Further α and β are not both zero, since $\alpha \neq \beta$. Hence s^3 and s^2 are uniquely determined. *There is at most one transformation converting an algebra* (I) *with* $A = B = 0$, $\alpha \neq \beta$, *into a similar algebra.* Moreover, the conditions for equivalence are obvious.

Let next $\alpha = \beta$. Then for $A = B = 0$, $r = -(\beta + D)t/3$, we have

$$\alpha' = \beta' = \beta s^2 + st(a + b + \delta) + t^2[d + \tfrac{1}{3}(\beta^2 - \beta D + D^2)],$$

$$a' = as^3 + s^2 t[d + \tfrac{1}{3}\beta(\beta + D)] + \tfrac{1}{3}st^2[\delta(\beta + D) + a(D - 2\beta) + b(4\beta - 2D)]$$
$$+ t^3[b\delta + \tfrac{1}{3}d(D - 2\beta) + \tfrac{1}{27}(\beta + D)(\beta - 2D)(2\beta - D)],$$

$$D' = Ds^2 + st(2a + 2b - \delta) + \tfrac{1}{3}t^2(6d + D^2 + 2\beta D - 2\beta^2),$$

$$\delta' = \delta s^3 + \tfrac{2}{3}s^2 t(2\beta - D)^2 + st^2\delta(2\beta - D) + t^3[\delta^2 - \tfrac{2}{27}(2\beta - D)^3],$$

the value of b' being derived from a' by interchanging a with b, while the long expression for d' will not be required. Set $\rho = D - 2\beta$. Then

$$\rho' = \rho s^2 - 3\delta st - \tfrac{1}{3}\rho^2 t^2,\ a' - b' = (a - b)\,C,\ C \equiv s^3 + \rho st^2 - \delta t^3.$$

Since $\delta \neq 0$, we may apply a preliminary transformation and make $\rho \neq 0$. We proceed to determine all the transformations of the algeba into itself. For $t = 0$, the transformation is the identity. Let $t \neq 0$ henceforth. For a non-commutative algebra a very simple treatment is possible. Since $a \neq b$, we have $C = 1$. Hence $\delta' - \delta C = 0$, viz.,

$$s^2\rho^2 - 3st\delta\rho + t^2(3\delta^2 + \rho^3/9) = 0.$$

Combining this equation with $\rho' = \rho$, we get $t\sqrt{R} = \mp 3\rho$, where

$$R = -27\delta^2 - 4\rho^3 = \text{discriminant of } C;\ R \neq 0.$$

Note that, if F is the $GF[p^n]$, R is a square. Indeed, the roots of the irreducible equation $x^3 + \rho x - \delta = 0$ are λ, λ^{p^n}, $\lambda^{p^{2n}}$, where $\lambda^{p^{3n}} = \lambda$. Hence

$$R = P^2, \qquad P \equiv (\lambda - \lambda^{p^n})(\lambda - \lambda^{p^{2n}})(\lambda^{p^n} - \lambda^{p^{2n}}), \qquad P^{p^n} = P.$$

The preceding quadratic equation now gives $(\mp s\sqrt{R} - \tfrac{1}{2}9\delta)^2 = \tfrac{1}{4}R$. The

quantity in parenthesis must equal $\pm \frac{1}{2}\sqrt{R}$, this determination of sign being necessary in view of $C = 1$. Hence

$$t = \mp 3\rho/\sqrt{R}, \qquad s = -\tfrac{1}{2} \mp \tfrac{1}{2}9\delta/\sqrt{R}.$$

For this result we proceed to give a proof valid for both commutative and non-commutative algebras. Set $\rho = kl^2$, $\delta = kl^3$, $s = ylt$. Then the equations $\delta' = \delta$ and $\rho' = \rho$ become

$$1 = t^3 l^3(y^3 + \tfrac{2}{3}ky^2 - ky + k + \tfrac{2}{27}k^2), \qquad 1 = t^2 l^2(y^2 - 3y - \tfrac{1}{3}k).$$

Squaring the first, cubing the second, and eliminating tl, we get a quintic equation $Q = 0$ in y. It becomes simpler if we set $k = -9w - \frac{27}{4}$. Thus

$$l = \delta/\rho, \qquad k = \rho^3/\delta^2, \qquad w = R/36\delta^2.$$

Hence $w \neq 0$. Removing the factor $3w$ from $Q = 0$, we get

$$4y^5 - 3(4w + 7)y^4 + (32w + 36)y^3 + 3(w + \tfrac{3}{4})(8w - 6)y^2$$
$$- 36(w + \tfrac{3}{4})^2 y - 3(w + \tfrac{3}{4})^2(4w - 9) = 0.$$

The left member is seen to factor. Hence

$$4UV = 0, \quad U \equiv y^2 - 3y - w + \tfrac{9}{4}, \quad V \equiv y^3 - 3(w + \tfrac{3}{4})y^2 + 3(w + \tfrac{3}{4})^2.$$

Since the cubic function C is irreducible in the field F, the same is true of V. Indeed, if we make the above substitutions in C, using capital Y to avoid confusion, we get

$$C = l^3 t^3 [\, Y^3 - 9(w + \tfrac{3}{4})\, Y + 9(w + \tfrac{3}{4})\,].$$

For $Y = 3(w + \frac{3}{4})/y$, the quantity in brackets becomes $9(w + \frac{3}{4})\, V/y^3$. Hence $V \neq 0$. Then $U = 0$ gives $y = \frac{3}{2} \pm \frac{1}{6}\sqrt{R}/\delta$. From the two above equations whose first members are unity, we get t uniquely. The resulting values of s and t are those given above.

The two transformations (1) given by these two sets of values of s and t are inverse operators. Hence an algebra invariant under one is invariant under the other. We find that the conditions that β' shall equal β for *both* sets of values of s and t are equivalent to the following:

$$(3) \qquad (a + b)(D - 2\beta) + \delta(D + \beta) = 0, \qquad 3d = \beta^2 - D^2.$$

But these relations are equivalent to relations (2) for $B = 0$. Hence the family of algebras (I) with $A = B = 0$, $\alpha = \beta$, and satisfying conditions (3), is invariant under every transformation (1), so that relations (3) hold true when written in the accented letters. Hence from the fact that the two sets of values of s and t satisfy the relations $\beta' = \beta$, $\delta' = \delta$, $D' - 2\beta' = D - 2\beta$, $a' - b' = a - b$, it follows without computation that they satisfy relations $D' = D$, $d' = d$, $a' = a$, $b' = b$. We have now proved the

THEOREM. *Let F be any field not having modulus 2 or 3. Consider the algebras* (I) *for which the cubic function C is irreducible in F. By a preliminary transformation of units we may make $A = B = 0$. Then the only algebras which admit more than one transformation (and hence three transformations) into themselves are the algebras with $\alpha = \beta$ and satisfying conditions** (3) *and having the discriminant R of C a square in F. When F is a finite field, R is always a square.*

It remains to treat the case when F is the $GF[3^n]$. Then every mark is a cube. Applying a preliminary transformation, we may set $B = 0$. Since $x^3 - b - \beta x$ shall be irreducible, β is not zero. In view of B', every transformation of the algebra into itself must have $t(\alpha + D) = 0$.

Let first $\alpha + D \neq 0$. Then $t = 0$. Hence $\beta' = s^2\beta$, $b' = r^3 - rs^2\beta + s^3 b$. For a transformation of the algebra into itself, $s^2 = 1$, $b = r^3 - r\beta + sb$. The case $s = -1$ is excluded since $r^3 - r\beta + b$ is irreducible. Hence $s = 1$, $r^3 = r\beta$. It was shown above that the discriminant $-27b^2 + 4\beta^3$ of an irreducible cubic $x^3 - \beta x - b$ is a square. Hence β is a square in the $GF[3^n]$. Now the algebra is transformed into itself by $I = i + \beta^{\frac{1}{2}}$ if and only if

$$A = 0,\ \alpha = \beta,\ D = \beta,\ a + b + \delta = 0.$$

There remains the case $B = 0$, $\alpha + D = 0$. Then $B' \equiv 0$, $\alpha' + D' \equiv 0$. By a preliminary transformation we can make also $A = 0$. In view of A', every transformation of the algebra into itself must have $t(\beta + D) = 0$. Since C shall be irreducible, $D - \alpha - \beta \neq 0$. Hence $t = 0$. As above, $s = 1$, $r^3 = r\beta$, $\alpha = \beta$. Hence $D - \alpha - \beta = 0$, so that this case is excluded.

Noting that for modulus 3 the conditions on the algebra cited in the above theorem require that $\alpha + D \neq 0$ in view of the irreducibility of C, we may state that the theorem holds true when F is the $GF[3^n]$.

THEOREM. *When F is the $GF[p^n]$, $p > 2$, all the algebras* (I_0) *for which $x^3 - b - \beta x - Bx^2$ is irreducible in F are equivalent.*

For this algebra we have

$$C = s^3 + 2s^2tB - 4\beta st^2 + 8bt^3.$$

We prove that C vanishes only when $s = t = 0$. For $t \neq 0$, set $s = -2\sigma t$. Then $C = -8t^3(\sigma^3 - b - \beta\sigma - B\sigma^2)$. Hence $C \neq 0$. In view of our earlier results, the family of algebras (I_0) is invariant under the $p^n(p^{2n} - 1)$ transformations (1) with s and t not both zero; while each algebra is transformed into itself by exactly three transformations. The theorem will now follow if we show that there are exactly $\frac{1}{3}p^n(p^{2n} - 1)$ irreducible cubic functions in the

* That these conditions are necessary may be shown without computation. For $\beta \neq 0$, $D \neq 0$, there is more than one transformation only when the quadratic functions β' and D' are identical, apart from a constant factor, the conditions for which are (3). Otherwise $\beta'/D' = \beta/D$ would uniquely determine s/t. The same argument applies to the cases $\beta = 0$, $\beta' \neq 0$; $D = 0$, $D' \neq 0$. When $D \equiv 0$ we have a special case of (3). The case $\beta' \equiv 0$ requires separate treatment.

$GF[p^n]$. But we readily enumerate the reducible cubic functions. Of those with three linear factors, p^n have three equal factors, $p^n(p^n-1)$ have just two equal factors, and $\frac{1}{6}p^n(p^n-1)(p^n-2)$ have distinct factors. Finally, there are $\frac{1}{2}p^{2n}(p^n-1)$ cubic functions with a linear and an irreducible quadratic factor.

The theorem is readily extended to other sets of commutative algebras satisfying relations (2). In particular, it is true for (I_1).

As an illustration of the use of the above transformation theory, we determine the non-equivalent algebras in the $GF[3]$ such that division is always uniquely possible. As above, we may set $B=0$. Then $x^3-b-\beta x$ must be irreducible, so that $b^2=1$, $\beta=1$. By the transformation which merely changes the sign of i, β is unaltered, while b is replaced by $-b$. Hence we may set $b=\beta=1$. Now $\phi\equiv x^3-a-\alpha x-Ax^2$ and $C\equiv s^3+s^2tA+st^2(D-\alpha-1)-t^3\delta$ must be irreducible. Under the transformation $I=i-1$, $J=j+i+1$, the algebra becomes a similar algebra with

$$\alpha'=a+\alpha+A-1, \qquad \alpha'=\alpha-A, \qquad A'=A,$$

$$D'=A+D, \qquad \delta'=\alpha+\delta-A-D, \qquad d'=a+\alpha+A+d+\delta+D-1.$$

Let first $A=0$. Then $a^2=1$, $a=1$ by ϕ; $\delta^2=1$, $-D+\alpha+1=1$ by C, whence $D=1$. The transformed algebra differs from the original only in d' and $d'=d+a+\delta+1$. If $a+\delta+1\neq 0$, we can make d' arbitrary (by a repetition of the transformation) and hence make $d=\delta$. Then $(j-\delta i-D)j=0$. Hence $a+\delta+1=0$, so that $a=\delta=1$, $d\neq 1$. For $d=0$, the algebra is the $GF[3^3]$. For $d=-1$, it is a case of algebra (I_0).

Let next $A\neq 0$. By a repetition of the above transformation, we can make $\alpha=0$. Then $a+A=0$ by ϕ; either $D=0$, $A\neq\delta$, or $D\neq 0$, $A=\delta$, by C. For the first case, $\alpha=D=0$, $a=\delta$, $A=-\delta$, $\delta\neq 0$, $d\neq\delta$; then if $d=0$, Δ_r vanishes for $r=t=1$, $s=0$; if $d=-\delta$, the first row of Δ_r is δ times the third row for $r=\delta$, $s=\delta+1$, $t=1$. Hence must $D\neq 0$, $A=\delta$, $a=-\delta$, $\alpha=0$, $\delta\neq 0$, $d\neq\delta$. Then Δ_r for $t=1$, $s=0$, becomes $r^2D-rd-1$. Hence either $D=-1$, $d=0$, or else $D=1$, $d\neq 0$, whence $d=-\delta$. In either case Δ_r vanishes only when $r=s=t=0$. For example, if $t=1$, $s=-1$, $\Delta_r=\mp(r^2-\delta r-1)$. The resulting algebras are*

$$i^2=j,\ ij=1+i,\ ji=\mp 1\pm j,\ j^2=\pm i-j;$$

$$i^2=j,\ ij=1+i,\ ji=\mp 1\pm j,\ j^2=\mp 1\pm i+j.$$

No two of these algebras are equivalent under a transformation (1). Since $B=\alpha=0$, $D\neq 0$, $B'=tD$. Hence $B'=0$ requires that $t=0$. Then $s\neq 0$, $\alpha'=rsA$. Hence $\alpha'=0$ requires that $r=0$. But the transformation which merely changes the sign of i does not preserve the relation $ij=1+i$.

* If in Δ for the field $i^2=j$, $ij=1+i$, $j^2=i+j$, we replace r and s by $r-t$ and $s+t$; r by $r+t$; s and t by $s+t$ and $-t$; t by $-t$, we obtain the determinant Δ_r of the four algebras, respectively.

THEOREM. *When F is the $GF[3]$ there are exactly six non-equivalent algebras in which division is always uniquely possible. The two commutative algebras fall under* (I_0) *and* (I_1).

Finally, I give a representative of each of the 36 non-equivalent sets of non-commutative algebras in the $GF[5]$ in which division is always uniquely possible. The two existing types of commutative algebras are given by (I_0) and (I_1), and are not listed. The tables relate to formula (I) with $A = B = 0$.

$b = 2, \beta = 1$

α	a	d	δ	D
1	-2	0	± 1	-1
-1	1	1	1	1
-1	1	0	± 1	2
-1	-1	1	2	-1
-1	-1	0	± 2	-2
2	± 2	-1	± 1	0
2	∓ 2	2	± 2	1
-2	± 1	1	1	0
-2	± 1	-2	± 2	2
-2	± 1	-2	-2	-2

$b = 2, \beta = 2$

α	a	d	δ	D
1	± 2	-1	1	0
1	∓ 2	2	± 1	-1
1	± 2	2	-2	1
-1	∓ 1	1	± 2	0
-1	± 1	-2	∓ 1	2
-1	± 1	-2	-1	-2
-2	1	-1	1	2
-2	1	0	± 2	-1
-2	-1	-1	2	-2
-2	-1	0	± 1	1

§ 3. *Derivation of an mk-tuple algebra from an m-tuple algebra.*

From an m-tuple algebra in a general field F, we readily deduce an mk-tuple algebra. We take as F the field $f(\rho)$ obtained from the field f by the adjunction of a root ρ of an equation of degree k, irreducible in f. Then if $e_1, \cdots, e_m$ are the units of the given algebra in F, we take the products $e_r\rho^s (r = 1, \cdots, m;\ s = 0, 1, \cdots, k-1)$ as the mk units of the desired algebra.

By way of illustration, we construct from (I_0) a 6-tuple algebra, which will be employed later. Let F be the field $f(\rho)$, where $\rho^2 = \nu$, ν being a not-square in f. Set $b = a + c\rho$, $\beta = \alpha + \gamma\rho$, $B = A + C\rho$, $\rho i = k$, $\rho j = l$. We obtain the 6-tuple algebra in f:

$$(II)\quad \begin{cases} \rho^2 = \nu,\ \rho i = k,\ \rho j = l,\ \rho k = \nu i,\ \rho l = \nu j,\ i^2 = j,\ ik = l,\ k^2 = \nu j, \\ ij = a + c\rho + \alpha i + \gamma k + Aj + Cl,\ il = kj = \nu c + a\rho + \nu\gamma i + \alpha k + \nu Cj + Al, \\ j^2 = 4aA + 4\nu cC - \alpha^2 - \nu\gamma^2 + (4aC + 4Ac - 2\alpha\gamma)\rho - 8ai - 8ck - 2\alpha j - 2\gamma l, \\ l^2 = \nu j^2,\ jl = \rho j^2,\ kl = \nu a + \nu c\rho + \nu\alpha i + \nu\gamma k + \nu Aj + \nu Cl; \end{cases}$$

the value of j^2 to be inserted in l^2 and jl. Similarly, from (I′) we deduce a field (II′) whose multiplication-table differs from (II) only in the values of j^2, l^2, jl. It may be shown that the determinant $\Delta(a)$ of (II′) can be transformed into that of (II). Since the algebras (I_0), and hence the algebras (II), are all equivalent, it suffices to make the proof for the case $A = C = c = \gamma = 0$. With the notation $a_1 + a_2 i + a_3 j + a_4 \rho + a_5 k + a_6 l$ for the general element, the determinant $\Delta(a)$ of (II′) becomes $\Delta(a)$ of (II) upon replacing a_1 by $a_1 + \alpha a_3$, a_4 by $a_4 + \alpha a_6$, a_3 by $-2a_3$, a_6 by $-2a_6$.

§ 4. *Commutative algebras with four units*, $1, i, j, k$.

Let F be a field not having modulus 2. By a transformation of units we may make * $i^2 = j$. Indeed there is some element e such that e^2 is not a linear function of e and we may set $i = e$, $j = e^2$. For, suppose that for every element e, e^2 is of the form $re + s$. Then $i^2 = ai + A$. Let $I = i - a/2$. Hence $I^2 = A + a^2/4$. Proceeding similarly with j we may set $i^2 = \alpha$, $j^2 = \beta$. Let $ij = r_1 + r_2 i + r_3 j + r_4 k$. Then, for arbitrary l,

$$(i + lj)^2 \equiv \alpha + l^2\beta + 2lr_1 + 2lr_2(i + lj) + 2lj(r_3 - lr_2) + 2lr_4 k$$

must be a linear function of $i + lj$. Hence $r_2 = r_3 = r_4 = 0$. Hence

$$i^2 = \alpha, \qquad ij = r_1, \qquad i(r_1 i - \alpha j) = 0.$$

In a 4-tuple algebra with $i^2 = j$, we may set $ij = k$. For, suppose that $ij = a + bi + cj$ with no term in k and that $ik = c_1 + c_2 i + c_3 j + c_4 k$. In

$$(l_1 + l_2 i)(x_1 + x_2 i + x_3 j + x_4 k),$$

the coefficient of k is $(l_1 + l_2 c_4)x_4$ and hence may be made zero by choice of l_1 and l_2, not both zero. The above product could not then be made equal to k, so that division by $l_1 + l_2 i$ would not always be possible.

Consider a 4-tuple algebra of the form

$$\text{(III)} \quad \begin{cases} i^2 = j, \ ik = ki = c_1 + c_2 i + c_3 j + c_4 k, \ j^2 = d_1 + d_2 i + d_3 j + d_4 k, \\ ij = ji = k, \ jk = kj = k_1 + k_2 i + k_3 j + k_4 k, \ k^2 = s_1 + s_2 i + s_3 j + s_4 k. \end{cases}$$

Suppose that $d_1 = 0$. Then the constant term in the product

$$(l_2 i + l_3 j)(x_1 + x_2 i + x_3 j + x_4 k)$$

is $(c_1 l_2 + k_1 l_3)x_4$ and hence may be made zero by choice of l_2 and l_3, not both zero. The product is then never 1, so that $l_2 i + l_3 j$ would have no inverse. Hence $d_1 \neq 0$.

We can now prove † that there is no root in the field F of

$$E \equiv x^4 - d_1 - d_2 x - d_3 x^2 - d_4 x^3 = 0.$$

* The same argument applies to algebras with m units, $m > 2$.

† The analogous theorem on algebras with m units is proved similarly.

Suppose that $E = 0$ has in F the root $x = -w$. Let

$$I = i + w, \qquad J = j + 2wi + w^2, \qquad K = k + 3wj + 3w^2 i + w^3.$$

Then $I^2 = J$, $IJ = K$, while the constant term in J^2, expressed as a linear function of I, J, K, is $d_1 - d_2 w + d_3 w^2 - d_4 w^3 - w^4$, and hence is zero. Hence the algebra is equivalent to one of the form (III) with $d_1 = 0$, contrary to the above result.

Next, the function E is not the product of two quadratic factors with coefficients in F. Indeed, if $E = (x^2 - px - q)(x^2 - rx - s)$, then

$$(j - pi - q)(j - ri - s) = 0.$$

The preceding results lead to the following

THEOREM. *In a field F not having modulus 2, a quaternary linear algebra in which multiplication is commutative and division is always uniquely possible is equivalent in F to an algebra of the form* (III) *in which $E \equiv x^4 - d_1 - d_2 x - d_3 x^2 - d_4 x^3$ is irreducible in F.*

For algebra (III) the determinant $\Delta(l)$ is

$$(4) \qquad \begin{vmatrix} l_1 & c_1 l_4 & d_1 l_3 + k_1 l_4 & c_1 l_2 + k_1 l_3 + s_1 l_4 \\ l_2 & l_1 + c_2 l_4 & d_2 l_3 + k_2 l_4 & c_2 l_2 + k_2 l_3 + s_2 l_4 \\ l_3 & l_2 + c_3 l_4 & l_1 + d_3 l_3 + k_3 l_4 & c_3 l_2 + k_3 l_3 + s_3 l_4 \\ l_4 & l_3 + c_4 l_4 & l_2 + d_4 l_3 + k_4 l_4 & l_1 + c_4 l_2 + k_4 l_3 + s_4 l_4 \end{vmatrix}$$

The problem is to determine c_i, d_i, k_i, s_i $(i = 1, 2, 3, 4)$ in F so that $\Delta(l)$ vanishes only when each l_i vanishes. We apply the principle * that any algebra (III) is equivalent to one of like form in which the d_i are given marks for which E is irreducible in F.

First, let F be the field of order 3. Since $x^4 - x - 1$ is irreducible modulo 3, we set $d_1 = d_2 = 1$, $d_3 = d_4 = 0$. For $l_3 = l_4 = 0$, (4) becomes

$$l_1^4 + c_4 l_1^3 l_2 - c_3 l_1^2 l_2^2 + c_2 l_1 l_2^3 - c_1 l_2^4.$$

Since it shall vanish only when $l_1 = l_2 = 0$, the c_i must satisfy one of the four sets of conditions in the $GF[3]$:

$$(5) \qquad \begin{cases} c_1 = 1, \ c_3 = 0, \ c_2 + c_4 \neq 0; & c_1 = 1, \ c_3 \neq 0, \ c_2 + c_4 = 0; \\ c_1 = -1, \ c_3 = -1, \ c_2 + c_4 \neq 0; & c_1 = -1, \ c_3 \neq -1, \ c_2 + c_4 = 0. \end{cases}$$

For $l_4 = 0$, $l_3 \neq 0$, we may set $l_1 = x l_3$, $l_2 = y l_3$, and remove the factor l_3^4 from (4). In the resulting function we give to x, y in turn the 9 pairs of values 0,

* See p. 30 of my memoir, cited above. Compare next to the last theorem of § 2; also the verification of the principle for algebra (IV) below.

$0; 1, 0; \cdots; -1, -1$. Hence no one of the nine resulting expressions is to vanish:

$$(6)\quad \begin{cases} k_2-k_1, \quad k_3-k_1, \quad c_1+c_2-c_3+c_4+k_1+k_2-k_3+k_4, \\ \qquad\qquad -k_3-k_1, \quad -c_2-c_3-c_4+k_2+k_3+k_4, \\ c_2-c_3+k_2-k_3, \quad -1-c_1-c_2+c_4+k_1+k_2-k_4, \\ \qquad 1-c_1-c_2-c_4-k_1-k_2-k_4, \quad c_1+c_2-c_3-k_1-k_2+k_3. \end{cases}$$

For each set of c's given by (5), one readily determines the sets of k's satisfying (6). For example, if $c_1=1$, $c_2=0$, $c_3=0$, $c_4=1$, we must have $k_1=1$, $k_2=-1$, $k_3=0$, $k_4=0$. It remains to examine (4) for $l_4 \neq 0$. In view of the homogeneity, we may set $l_4=1$. For $(l_1, l_2)=(1, -1)$ and $(0, 0)$, (4) becomes respectively

$$(l_3-s_2)(l_3^2+1)-s_3(l_3^2+l_3-1)-s_4, \quad (l_3-s_2)(l_3^2+l_3)-s_3(l_3-1)+s_4(l_3^2-l_3).$$

Neither is to vanish for any value of l_3. Hence no one of the expressions

$$s_2-s_3+s_4, \quad 1+s_2+s_3-s_4, \quad -1+s_2-s_3-s_4, \quad s_3, \quad s_2-1, \quad s_3+s_4$$

is to vanish. Hence $s_2=0$, $s_3=1$, $s_4=0$. Then (4) vanishes for $l_1=0$, $l_2=1$, $l_3=-1$. In the same manner are excluded all cases in which $c_1=1$, $c_3=0$, except the $GF[3^4]$. If $c_1=1$, $c_2=0$, $c_3=1$, $c_4=0$, then $(k_1, k_2, k_3, k_4)=(0, 1, -1, 0)$, $(1, 0, 0, 0)$, or $(-1, 0, 0, -1)$; the first is excluded, while for the second we must have $s_1=1$, $s_2=1$, $s_3=0$, $s_4=-1$, and therefore

$$(\text{IV})\quad \begin{gathered} i^2=j, \quad ij=ji=k, \quad ik=ki=1+j, \quad jk=kj=1, \\ j^2=1+i, \quad k^2=1+i-k. \end{gathered}$$

A computation showed that, for algebra (IV), $\Delta(l)$ vanishes only when every $l_i=0$. An immediate proof will be given below. In (IV), set

$$(7)\qquad I=\alpha+\beta i+\gamma j+\delta k, \quad J=I^2, \quad K=IJ.$$

Then condition that $1, I, J, K$ shall be independent units reduces to

$$\begin{vmatrix} \beta & \gamma & \delta \\ \delta^2+\gamma^2 & \beta^2-\beta\delta & -\delta^2-\beta\gamma \\ -\delta^3 & \delta^3-\beta^2\gamma & \beta^3-\beta^2\delta+\gamma^3+\delta^3 \end{vmatrix} \not\equiv 0 \pmod 3.$$

But this determinant vanishes only when $\beta \equiv \gamma \equiv -\delta \pmod 3$. Hence there are exactly $3(27-3)=72$ valid transformations (7). Exactly four of these transform algebra (IV) into itself, viz.,

$$T: \quad I=i-j, \quad J=1+i+j+k, \quad K=-1+\imath,$$

and T^2, T^3, $T^4 =$ identity. Hence there are exactly 18 algebras with $I^2 = J$ and $IJ = K$, which are equivalent to (IV). To obtain them, we apply transformation (7) with $(\beta, \gamma, \delta) = (0, 0, \pm 1), (\pm 1, 0, 0), (0, 1, 1), (1, 1, 0)$, and replace α by $\alpha \pm 1$ in the first case, α by $\alpha + 1$ in the third. The resulting algebras are

IK	J^2	JK	K^2
$1-\alpha I+J+\alpha K$	$\alpha^2 \mp \alpha - 1 \pm I - J + \alpha K$	$\alpha \pm 1 - \alpha^2 I + (\alpha^2 - 1)K$	$\alpha^2 - 1 - (\alpha \mp 1)I - J - (\alpha \pm 1)K$
$1-\alpha I+J+\alpha K$	$-\alpha^2 \mp \alpha + 1 + (\alpha \pm 1)I + \alpha K$	$\pm 1 - \alpha^2 I + \alpha^2 K$	$1 - \alpha^2 \pm I - (\alpha \pm 1)K$
$-1-\alpha^2+\alpha I+\alpha K$	$\alpha^2 + 1 - J + \alpha K$	$I + \alpha J + (\alpha^2 - 1)K$	$1 + \alpha I + J - \alpha K$
$-1-\alpha^2+\alpha I+\alpha K$	$1 - \alpha I + J + \alpha K$	$\alpha + I + \alpha J + (\alpha^2 + 1)K$	$-1 + \alpha I + J - \alpha K$

If we add $-x^4$ to the various functions in the second column, after replacing I, J, K by x, x^2, x^3, respectively, we obtain the 18 existing irreducible functions of the fourth degree modulo 3. We have therefore verified the principle cited above.

Special attention should be given to the algebra in the third line of the table for the case $\alpha = 0$, viz.,

(V) $I^2 = J$, $IJ = K$, $J^2 = 1 - J$, $IK = -1$, $JK = I - K$, $K^2 = 1 + J$.

Its determinant $\Delta(l)$ equals $F_{1,3} + F_{2,4}$, where

$$F_{x,y} \equiv x^4 - 2x^3y - x^2y^2 + 2xy^3 + y^4.$$

Since $F_{x,y} \equiv (x^2 + y^2)^2 \pmod 3$, $\Delta(l)$ vanishes only when each $l_i = 0$.

Next, let F be the field of order 5. Since $x^4 - 2$ is irreducible modulo 5, we set $d_1 = 2$, $d_2 = d_3 = d_4 = 0$ in (III). Then, for $l_2 = l_4 = 0$, (4) equals

$$(l_1^2 - 2l_3^2)(l_1^2 + k_4 l_1 l_3 - k_2 l_3^2).$$

Hence the second factor must be irreducible modulo 5, so that $k_4^2 - k_2$ must be a not-square, viz., 2 or -2. Thus

(8) $(k_4, k_2) = (0, \pm 2)$, $(\pm 1, 3)$, $(\pm 1, 4)$, $(\pm 2, 1)$, or $(\pm 2, 2)$.

If we set $I = 2i$, $J = -j$, $K = -2k$, we get

$$I^2 = J, \qquad IJ = K, \qquad J^2 = 2, \qquad IK = c_1 - 2c_2 I - c_3 J + 2c_4 K,$$
$$JK = 2k_1 + k_2 I - 2k_3 J - k_4 K.$$

Hence we may change the sign of k_4 without altering k_2. Hence we need retain only the upper signs in the last four cases of (8). Consider the case $k_4 = 0$, $k_2 = 2$. By repetitions of the above transformation we can multiply c_4 (or c_2) by any power of 2; hence there are three sub-cases: $c_4 = 1$; $c_4 = 0$, $c_2 = 0$; $c_4 = 0$, $c_2 = 1$. By an investigation entirely analogous to that employed above for the case modulus 3, but here much more laborious, I found that the cases

$c_1 = 0$ and $c_1 = \pm 1$ are to be excluded, while for $c_1 = 2$ the only algebra is the $GF[5^4]$. For $c_1 = -2$, I examined only one of the three sub-cases cited above, viz., that for which $c_4 = 0$, $c_2 = 0$, and found that we must have $c_3 = 0$, $k_1 = k_3 = 0$, $s_1 = s_2 = s_4 = 0$, $s_3 = 2$. The resulting algebra is

(VI) $$i^2 = j,\ ij = k,\ j^2 = 2,\ ik = -2,\ jk = 2i,\ k^2 = 2j.$$

For it $\Delta(l)$ is seen to equal $(l_1^2 - 2l_3^2)^2 + 2(l_2^2 - 2l_4^2)^2$. Since 2 and -2 are not squares, $\Delta(l)$ vanishes only when each l_i vanishes.

Let F be any field for which -1 is a square and ν is a not-square. Replacing 2 by ν in (VI) we obtain the algebra

(VII) $$i^2 = j,\ ij = k,\ j^2 = \nu,\ ik = -\nu,\ jk = \nu i,\ k^2 = \nu j,$$
$$\Delta(l) = (l_1^2 - \nu l_3^2)^2 + \nu(l_2^2 - \nu l_4^2)^2.$$

Seeking a generalization of algebras (V) and (VII), we set

(III′) $$i^2 = j,\ ij = k,\ j^2 = d_1 + d_3 j,\ ik = c_1,\ jk = k_2 i + k_4 k,\ k^2 = s_1 + s_3 j.$$

The simplicity of our proofs that division is always uniquely possible in algebras (V) and (VII) is due to the fact that for each $\Delta(l)$ equals the sum of a function of l_1, l_3 and a function of l_2, l_4. We now require that (III′) shall have the same property.* The conditions for this are found to be

$$s_1 + s_3 k_4 = 0,\ k_2 + 2c_1 + s_3 = 0,\ 2s_1 - 2c_1 d_3 = 0,\ d_1 + k_2 + 2c_1 = 0,$$
$$2c_1 k_2 + s_3 k_2 + s_3 d_1 - s_1 d_3 + s_1 k_4 = 0,\ k_2 c_1 d_3 - k_2 s_1 = 0,$$
$$k_4 d_1 + c_1 d_3 = 0,\ d_3 s_1 - k_4 c_1 d_3 - s_3 d_1 - 2k_2 c_1 - k_2 d_1 = 0.$$

The coefficient $-s_3 c_1 k_2$ of l_4^4 in $\Delta(l)$ cannot vanish. Hence the above conditions are satisfied if and only if

* Note added May 25, 1906. It may be shown that, if the general algebra (III) has this property, d_2, d_4, k_1, k_3, s_2 and s_4 all vanish, so that (III) reduces to (III′). As at the beginning of § 5, we must have $c_2 = c_3 = c_4 = 0$, $c_1 \neq 0$. Also $s_4 = -k_3$, since the coefficient of $l_1^3 l_4$ in (4) must vanish. I expanded determinant (4) with these values inserted. Since the coefficients of $l_2^3 l_3$, $l_2^2 l_2 l_3$, $l_1 l_2^2 l_4$, $l_1 l_2^2 l_3$, $l_1^2 l_2 l_4$, $l_2 l_3^3$, $l_1 l_2 l_4^2$, $l_2^2 l_3 l_4$, $l_1^2 l_3 l_4$, $l_1 l_4^3$, $l_1 l_2 l_3 l_4$ must vanish, we have respectively,

$$k_1 = -c_1 d_4,\quad k_3 = -d_2,\quad s_2 = c_1 d_4,\quad k_2 = -d_1 - 2c_1,\quad s_3 = d_1,$$
$$d_1 d_2 - c_1 d_2 - c_1 d_3 c_4 = 0,\quad d_1 d_2 + 3c_1 d_2 + c_1 d_4 k_4 = 0,\quad d_1 d_2 - c_1 d_2 - s_1 d_4 = 0,$$
$$c_1 d_4 + d_2 d_3 - d_1 d_4 + 0,\quad c_1^2 d_4 - c_1 d_1 d_4 + s_1 d_2 = 0,\quad 2s_1 + c_1 d_4^2 - d_2^2 - 2c_1 d_3 = 0.$$

Since the terms involving l_1 and l_2 alone are $l_1^4 - c_1 l_2^4$, c_1 must be a not-square.

The conditions arising from other coefficients are not needed for the argument. From the two conditions preceding the last, we derive $s_1 d_2 = c_1 d_2 d_3$. If $d_2 \neq 0$, the last condition now becomes $c_1 d_4^2 - d_2^2 = 0$, which is impossible, c_1 being a not-square. Hence $d_2 = 0$. The above conditions are seen to require that $d_4 = 0$.

$s_1 = c_1 d_3,\ s_3 = d_1,\ k_2 = -d_1 - 2c_1,\ k_4 = -c_1 d_3 d_1^{-1},\ (4d_1 + d_3^2)(c_1 + d_1) = 0.$

The two sets of solutions are

$$(9) \qquad d_1 = -c_1,\ s_3 = -c_1,\ s_1 = c_1 d_3,\ k_2 = -c_1,\ k_4 = d_3;$$

$$(9') \qquad d_1 = s_3 = -\tfrac{1}{4}d_3^2,\ s_1 = c_1 d_3,\ k_2 = \tfrac{1}{4}d_3^2 - 2c_1,\ k_4 = 4c_1 d_3^{-1}.$$

For these respective sets of values

$$(10) \qquad \Delta(l) = F_{l_1, l_3} - c_1 F_{l_2, l_4}, \qquad F_{x,y} \equiv (x^2 + d_3 xy + c_1 y^2)^2;$$

$$(10') \qquad F_{x,y} \equiv [x + \tfrac{1}{2}d_3 y]^2 [x^2 + 4c_1 d_3^{-1} xy + (2c_1 - \tfrac{1}{4}d_3^2) y^2].$$

In the latter case $\Delta(l)$ vanishes when $l_1 = l_2 = d_3$, $l_3 = l_4 = -2$. Hence the set (9′) is excluded. In order that $\Delta(l)$, given by (10), shall vanish only when each l_i vanishes, it is necessary and sufficient that c_1 be a not-square and that $z^2 + d_3 z + c_1$ be irreducible in the field F. We obtain the algebra

$$(\text{VIII}) \quad \begin{cases} i^2 = j,\ ij = k,\ ik = c,\ j^2 = -c + dj,\ jk = -ci + dk,\ k^2 = cd - cj, \\ c \text{ and } d^2 - 4c \text{ each a not-square in the field } F. \end{cases}$$

Note that $kj = (ij)j = i(j^2)$, $k^2 = i(jk)$; also that the sub-algebra defined by the units 1 and j is a field. When F is the Galois field of order p^n, there exists an algebra (VIII). For, take as c any fixed not-square; then when d ranges over the p^n marks, $d^2 - 4c$ takes $1 + \frac{1}{2}(p^n - 1)$ distinct values each not zero. But only $\frac{1}{2}(p^n - 1)$ of the marks are squares. Hence there is some value of d for which $d^2 - 4c$ is a not-square.

A noteworthy generalization of algebra (VIII) may be obtained by making the transformation

$$I = i + t, \qquad J = j + 2it + t^2, \qquad K = k + 3jt + 3it^2 + t^3.$$

Simplifications arise if we set $\delta = d - 2t^2$, $\gamma = c - t^2 d + t^4$. Then

$$(\text{IX}) \quad \begin{cases} I^2 = J, \qquad IJ = K, \qquad IK = \gamma + t^2\delta + 4t^3 I - 6t^2 J + 4tK, \\ J^2 = -\gamma - 2t\delta I + (\delta - 4t^2) J + 4tK, \\ JK = 2\delta t^3 + (8t^4 - 4t^2\delta - \gamma) I - 20t^3 J + (\delta + 12t^2) K, \\ K^2 = \gamma\delta + t^2\delta^2 + 4t^2\gamma + 8t^4\delta + (32t^5 - 4t^3\delta - 4t\gamma) I \\ \qquad\qquad + (-\gamma - 10t^2\delta - 64t^4) J + (6t\delta + 32t^3) K, \\ \delta^2 - 4\gamma \text{ and } \gamma + t^2\delta + t^4 \text{ each a not-square in the field.} \end{cases}$$

§ 5. *Commutative algebras with* 6 *units.*

We seek an algebra such that, if the general element be given the notation $r_1 + r_2 i + r_3 j + r_4 k + r_5 l + r_6 m$, the determinant $\Delta(r)$ shall equal the sum of a function of r_1, r_3, r_5 and a function of r_2, r_4, r_6. Set

(11) $i^2=j,\ ij=k,\ ik=l,\ il=m,\ im=c_1+c_2i+c_3j+c_4k+c_5l+c_6m.$

For $r_3=r_4=r_5=r_6=0$, $\Delta(r)$ equals

$$r_1^6+r_1^5r_2c_6-r_1^4r_2^2c_5+r_1^3r_2^3c_4-r_1^2r_2^4c_3+r_1r_2^5c_2-r_2^6c_1.$$

Hence must $c_2=c_3=c_4=c_5=c_6=0$, $c_1\neq 0$.

We are seeking the algebra in 6 units which corresponds to algebra (VIII) in 4 units. For the latter, the first and third units, 1 and j, form a sub-algebra, while the rest of the multiplication-table of the units may be deduced by the associative law, viz., $jk=i(j^2)$, $k^2=i(jk)$. For the 6-tuple algebra we therefore assume that the units $1, j, l$ form a sub-algebra and that

(12) $jk=i(j^2),\ k^2=i(jk),\ lm=i(l^2),\ m^2=i(lm),\ kl=jm=i(jl),\ km=i(jm).$

Hence the algebra must be of the form *

$$\text{(X)}\quad\begin{cases} i^2=j,\ ij=k,\ ik=l,\ il=m,\ im=c, \\ j^2=d_1+d_3j+d_5l, \quad l^2=m_1+m_3j+m_5l, \quad jl=f_1+f_3j+f_5l, \\ jk=d_1i+d_3k+d_5m,\ lm=m_1i+m_3k+m_5m,\ kl=jm=f_1i+f_3k+f_5m, \\ k^2=d_1j+d_3l+d_5c,\ m^2=m_1j+m_3l+m_5c,\ km=f_1j+f_3l+f_5c, \end{cases}$$

it being understood that multiplication is commutative, $ij=ji$, etc.

The determinant $\Delta(r)$ of (X) with certain rows and columns interchanged is

$$\text{(13)}\quad \begin{vmatrix} r_1 & A_1 & B_1 & r_6c & E_3c & D_3c \\ r_3 & A_2 & B_2 & r_2 & E_1 & D_1 \\ r_5 & A_3 & B_3 & r_4 & E_2 & D_2 \\ r_2 & E_1 & D_1 & r_1 & A_1 & B_1 \\ r_4 & E_2 & D_2 & r_3 & A_2 & B_2 \\ r_6 & E_3 & D_3 & r_5 & A_3 & B_3 \end{vmatrix},$$

$$A_1=r_3d_1+r_5f_1,\ B_1=r_3f_1+r_5m_1,\ E_1=r_4d_1+r_6f_1,\ D_1=r_4f_1+r_6m_1$$

$$A_2=r_1+r_3d_3+r_5f_3,\ B_2=r_3f_3+r_5m_3,\ E_2=r_2+r_4d_3+r_6f_3,\ D_2=r_4f_3+r_6m_3,$$

$$A_3=r_3d_5+r_5f_5,\ B_3=r_1+r_3f_5+r_5m_5,\ E_3=r_4d_5+r_6f_5,\ D_3=r_2+r_4f_5+r_6m_5.$$

We desire that (13) shall equal

* I was first led to this algebra by postulating (11), giving to $1, i, j, k, l, m$ the weights 0, 1, 2, 3, 4, 5; assuming that, if the sum of the weights of two units is even (odd) their product is a linear function of the units of even (odd) weight; finally requiring that the matrix of the determinant $\Delta(r)$ shall take the form (13), viz., $\begin{pmatrix} A & B' \\ B & A \end{pmatrix}$, where the rows of matrix B' form a cyclic permutation of the rows of B, aside from the factor c. These properties correspond to those of algebra (VIII).

$$(14)\qquad \begin{vmatrix} r_1 & A_1 & B_1 \\ r_3 & A_2 & B_2 \\ r_5 & A_3 & B_3 \end{vmatrix}^2 - c \begin{vmatrix} r_2 & E_1 & D_1 \\ r_4 & E_2 & D_2 \\ r_6 & E_3 & D_3 \end{vmatrix}^2,$$

and hence that the remaining terms in the Laplace development of (13) shall vanish identically. The conditions for this all follow from

$$m_1 = -cf_5,\ m_3 = cd_5,\ f_1 = -c - cd_5,\ f_3 = -d_1,\ d_1^2 - cd_3d_5 - cd_3 + cf_5 = 0,$$

$$c + cd_5 + cd_5^2 + d_1f_5 = 0,\ f_1m_5 + cf_5^2 - cd_1 = 0,\ d_1m_5 + cd_3 + cd_5f_5.$$

From these we derive

$$cm_5 = (-cd_5 - cd_5^2 - d_1f_5)m_5 = cd_5(f_5^2 - m_5 - m_5d_5) + f_5(-d_1m_5 - cd_5f_5),$$

and hence $cm_5 = cd_5d_1 + cf_5d_3$. But $c \neq 0$. We may now readily verify that the above set of conditions is equivalent to the following:

$$(15)\qquad \begin{cases} m_1 = -cf_5,\ m_3 = cd_5,\ m_5 = d_1d_5 + d_3f_5, \\ f_1 = -c - cd_5,\ f_3 = -d_1,\ f_5 = d_3 + d_3d_5 - c^{-1}d_1^2, \end{cases}$$

$$(16)\qquad c^2 + c^2d_5 + c^2d_5^2 + cd_1d_3 + cd_1d_3d_5 - d_1^3 = 0.$$

It remains to impose the condition that (14) shall vanish only when every r_i vanishes. Now the second determinant in (14) is the same function of r_2, r_4, r_6 that the first is of r_1, r_3, r_5. Hence we must take c to be a not-square and require that

$$(17)\qquad \begin{vmatrix} r_1 & A_1 & B_1 \\ r_3 & A_2 & B_2 \\ r_5 & A_3 & B_3 \end{vmatrix}$$

shall vanish only when r_1, r_3, r_5 all vanish. Now (17) is the determinant $\Delta(r)$ of the subalgebra $(1, j, l)$. We proceed to determine the conditions under which the latter is a field. Now d_5 is not zero.* For, if $d_5 = 0$, then $m_3 = 0$, and the elements of the fifth row of (13) would all vanish for $r_3 = r_4 = 0$, $r_1 = -r_5f_3$, $r_2 = -r_6f_3$. Hence we may take as the units of the subalgebra $1, j, L = d_1 + d_3j + d_5l$. Then

$$(18)\qquad \begin{cases} j^2 = L, \qquad jL = (f_5 + d_3)L + (d_1 + d_5f_3 - d_3f_5)j + d_5f_1 - f_5d_1, \\ L^2 = (d_3^2 + d_5m_5 + 2d_1 + 2d_3f_5)L + (d_5^2m_3 + 2d_3d_5f_3 - d_3d_5m_5 - 2d_3^2f_5)j \\ \qquad\qquad + d_5^2m_1 + 2d_3d_5f_1 - d_1^2 - d_1d_5m_5 - 2d_1d_3f_5. \end{cases}$$

* We do not retain the condition $d_5 \neq 0$ in the final theorem. For, if $d_5 = 0$, we multiply (19) by d_1^3 and set $z = d_1y$. After eliminating d_3, we get $(z + c^2)^2(z - d_1^3) = 0$. Hence the cubic is reducible if $d_5 = 0$.

The three conditions for the identity $j(jL) = L^2$ are seen to follow from relations (15) and (16). Hence the subalgebra (18) is a field if

$$x^3 - (f_5 + d_3)x^2 - (d_1 + d_5 f_3 - d_3 f_5)x + f_5 d_1 - d_5 f_1 = 0$$

is irreducible in F. Multiplying the left member by c^3, setting $y = cx$, and applying (15), we get

$$(19) \quad y^3 - (2cd_3 + cd_3 d_5 - d_1^2)y^2 - (cd_1 - cd_1 d_5 - cd_3^2 - cd_3^2 d_5 + d_1^2 d_3)cy - c^4 = 0.$$

THEOREM. *For any not-square c and any marks d_1, d_2, d_3 such that the cubic* (19) *is irreducible in the field F, and such that condition* (16) *holds, formulæ* (X) *with the amplification* (15) *define a non-field algebra in which division is always uniquely possible.*

We proceed to prove the existence of an algebra (X) for any Galois field of order p^n, $p > 2$. It suffices to take $d_5 = -1$. Then (16) becomes $c^2 - d_1^3 = 0$. We take $c = \rho^{3r}$, $d_1 = \rho^{2r}$, where r is any odd integer and ρ is a primitive root of the $GF[p^n]$. Hence c is a not-square and (16) is satisfied. In the simplified form of (19), we set

$$y = d_1^2 z, \qquad cd_3 = d_1^2(\tau + 1).$$

The factor d_1^6 may be removed. The resulting equation is

$$(20) \quad z^3 - \tau z^2 - (\tau + 3)z - 1 = 0.$$

Now d_3 and hence also τ may be chosen arbitrarily. But there exist values of τ for which (20) is irreducible in the $GF[p^n]$. Indeed, if a cubic is reducible it must have a root in the field. But (20) does not have a root 0 or -1, whatever be the value of τ. Hence, since τ enters linearly, there are at most $p^n - 2$ values of τ for which the cubic has a root in the $GF[p^n]$. Hence there are at least two irreducible cubics.*

§ 6. *Non-equivalence of the* 6*-tuple algebras* (II) *and* (X).

LEMMA. *Consider the field $F(\rho)$ derived from a field F by the adjunction of a root of an equation, irreducible in F,*

$$(21) \quad \rho^m = \alpha_0 + \alpha_1 \rho + \cdots + \alpha_{m-1}\rho^{m-1}.$$

The determinant $\Delta(r)$ of the algebra $F(\rho)$ has the factor

$$r_0 + r_1 \rho + \cdots + r_{m-1}\rho^{m-1}.$$

*The cubic is irreducible when $p^n = 3$, $\tau \neq 0$; $p^n = 5$, $\tau \neq 1$; $p^n = 7$, $\tau \neq 2, -2, -1$. For $p^n = 3$, there exist exactly six algebras (X); they are given by $d_5 = -1$, $d_1 = 1$, $d_3 = 0$ or 1. $d_5 = 1$, $d_1 = 0$, $d_3 = \pm 1$; $d_5 = 1$, $d_1 = \pm 1$, $d_3 = 1$.

By applying (21), we obtain relations of the form

$$\rho^{m+1} = \beta_0 + \beta_1\rho + \cdots + \beta_{m-1}\rho^{m-1}, \qquad \rho^{m+2} = \gamma_0 + \gamma_1\rho + \cdots + \gamma_{m-1}\rho^{m-1}, \cdots.$$

If $L \equiv r_0 + r_1\rho + \cdots + r_{m-1}\rho^{m-1}$ is the general element of $F(\rho)$, $\Delta(r)$ is

$$\begin{vmatrix} r_0 & r_{m-1}\alpha_0 & r_{m-2}\alpha_0 + r_{m-1}\beta_0 & r_{m-3}\alpha_0 + r_{m-2}\beta_0 + r_{m-1}\gamma_0 \cdots \\ r_1 & r_0 + r_{m-1}\alpha_1 & r_{m-2}\alpha_1 + r_{m-2}\beta_1 & r_{m-3}\alpha_1 + r_{m-2}\beta_1 + r_{m-1}\gamma_1 \cdots \\ r_2 & r_1 + r_{m-1}\alpha_2 & r_0 + r_{m-2}\alpha_2 + r_{m-1}\beta_2 & r_{m-3}\alpha_2 + r_{m-2}\beta_2 + r_{m-1}\gamma_2 \cdots \\ r_3 & r_2 + r_{m-1}\alpha_3 & r_1 + r_{m-2}\alpha_3 + r_{m-1}\beta_3 & r_0 + r_{m-3}\alpha_3 + r_{m-2}\beta_3 + r_{m-1}\gamma_3 \cdots \\ \cdot & \cdot & \cdot & \cdot \end{vmatrix}.$$

Multiply the 2d row by ρ, the 3d by $\rho^2, \cdots$, the mth by ρ^{m-1}; add the products to the first row. Then the new first row is $L, \rho L, \rho^2 L, \rho^3 L, \cdots$.

THEOREM. *Let F be the $GF[p^n]$, so that $F(\rho)$ is the $GF[p^{nm}]$. When all possible sets of values in the $GF[p^n]$ are assigned to $r_0, r_1, \cdots r_{m-1}$, the determinant $\Delta(r)$ equals any chosen mark, not zero, of the $GF[p^n]$ exactly $(p^{nm}-1)/(p^n-1)$ times, and equals zero once.*

Equations (21) has the roots $\rho, \rho^{p^n}, \cdots, \rho^{p^{n(m-1)}}$. Since $\Delta(r)$ has the factor $L(\rho)$, it has the factors $L(\rho^{p^n}) = L^{p^n}, \cdots, L^{p^{n(m-1)}}$. Hence

$$\Delta(r) = L^s, \qquad s \equiv 1 + p^n + p^{2n} + \cdots + p^{n(m-1)}.$$

If a is any chosen mark, not zero, of the $GF[p^{nm}]$, the equation $L^s = a$ has exactly s roots in the $GF[p^{nm}]$, each determining one set of marks r_i of the $GF[p^n]$.

As in § 5, let F_{135} denote the determinant of a triple algebra which may be identified with the $GF[p^{3n}]$. We shall prove the

THEOREM. *If b and c are marks of the $GF[p^n]$, $p > 2$, c being a not-square and b not zero, the number of sets of solutions $r_1, \cdots, r_6$ in the $GF[p^n]$ of $F_{135}^2 - cF_{246}^2 = b$ is*

$(p^{6n}-1)/(p^n-1)$ *if* -1 *is a square;*

$(p^n+1)(p^{2n}+p^n+1)^2$ *if* -1 *and* b *are not-squares;*

$(p^n+1)(p^{2n}+p^n+1)(p^{2n}-3p^n+1)$ *if* -1 *is a not-square,* b *a square.*

There are p^n+1 sets of solutions x, y in the $GF[p^n]$ of

$$b = x^2 - cy^2 \equiv (x + Jy)^{p^n+1} \qquad (J^2 = c).$$

If -1 is a square, there are exactly two sets of solutions in which x or y vanishes, and $p^n - 1$ sets in which neither vanishes. Applying the preceding theorem for $m = 3$, we find that the number of sets of solutions $r_1, \cdots, r_6$ is

$$2(p^{2n}+p^n+1)+(p^n-1)(p^{2n}+p^n+1)^2=(p^{6n}-1)/(p^n-1).$$

If -1 is a not-square, set $-c=\gamma^2$. If b is the square of a mark β, then $x=0$, $y=\pm\beta/\gamma$ and $x=\pm\beta$, $y=0$ are solutions. Hence the number of sets r_i is

$$4(p^{2n}+p^n+1)+(p^n-3)(p^{2n}+p^n+1)^2.$$

But if b is a not-square, all p^n+1 sets of solutions have $x\neq 0$, $y\neq 0$, so that the number of sets r_i is $(p^n+1)(p^{2n}+p^n+1)^2$.

THEOREM. *When F is the $GF[p^n]$, $p>2$, no 6-tuple algebra* (X) *is equivalent to a 6-tuple algebra* (II).

When -1 is a not-square the statement follows from the preceding two theorems, since (§ 3) the determinant $\Delta(a)$ of (II) can be linearly transformed into that of the $GF[p^{6n}]$.

When -1 is the square of a mark η of the $GF[p^n]$, the proof will be restricted, for brevity, to an algebra (X) for which

$$c=\nu^3,\quad d_1=\nu^2,\quad d_3=\nu(2\eta-1),\quad d_5=-1 \qquad (\nu \text{ a not-square}). \tag{22}$$

Then (16) is satisfied. In (19) set $y=\nu^4 z$. Then

$$z^3-(2\eta-2)z^2-(2\eta+1)z-1=0. \tag{23}$$

This is irreducible for $p^n=5$, $\eta=\pm 2$; $p^n=13$, $\eta=5$ (but not for $\eta=-5$); $p^n=17$, $\eta=4$; $p^n=29$, $\eta=-12$ (but not for $\eta=12$). These are the earliest cases and are the only cases examined. We consider the fields for which (23) is irreducible. The only elements of the algebra (22) whose square equals ν are seen to be $\pm\rho$, where $\rho=\nu^{-2}m-\nu^{-1}\eta k$. Now $\rho(\rho i)=k+\nu^{-1}m-\nu\eta i$. Hence $\rho(\rho A)$ does not equal νA for every element A. The algebra is therefore not equivalent to (II).

The same method of pooof may be applied to other cases. Thus for $p^n=3$, $d_1=1$, $d_3=1$, $d_5=-1$, the only elements ρ of algebra (X) for which $\rho^2=-1$ are $\rho=\pm(i+k-m)$. But $\rho(\rho j)\neq -j$.

THE UNIVERSITY OF CHICAGO.