9. Professor Bowden gave an elementary proof by mathematical induction of the formula

$$C_r^{m+n} = \sum_{k=1}^{k=r+1} C_{r-k+1}^m C_{k-1}^n.$$

F. N. Cole,
Secretary.

ON TRIPLE ALGEBRAS AND TERNARY CUBIC FORMS.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society, October 26, 1907.)

1. For any field F in which there is an irreducible cubic equation $f(\rho) = 0$, the norm of $x + y\rho + z\rho^2$ is a ternary cubic form C which vanishes for no set of values x, y, z in F, other than $x = y = z = 0$. The conditions under which the general ternary form has the last property are here determined for the case of finite fields. One formulation of the result is as follows:

Theorem. *The necessary and sufficient conditions that a ternary cubic form C shall vanish for no set of values x, y, z in the $GF[p^n]$, $p > 2$, other than $x = y = z = 0$, are that its Hessian shall equal mC, where m is a constant different from zero, and that the binary form obtained from C by setting $z = 0$ shall be irreducible in the field.*

Although I have not hitherto published a proof of this theorem, I have applied it to effect a determination * of all finite triple linear algebras in which multiplication is commutative and distributive, but not necessarily associative, while division is always uniquely possible. I shall here (§ 11) determine these algebras by applying directly the more fundamental conditions from which the preceding theorem is derived.

These ternary cubic forms arise in various other problems; for instance, in the normalization of families of ternary quadratic forms containing three linearly independent forms.

---

* *Amer. Math. Monthly*, vol. 13 (1906), pp. 201–205. References are there given to my earlier papers on the subject.

All such ternary cubic forms in a finite field are equivalent under linear transformation in the field (§ 9).

2. Let a ternary form,* with coefficients in the $GF[p^n]$,

$$(1) \qquad C \equiv ax^3 + bx^2y + cx^2z + dxy^2 + exz^2 + fxyz + gy^3 + hy^2z + kyz^2 + lz^3,$$

vanish in the field only for $x = y = z = 0$. Then for any assigned values, not both zero, of y and z in the field, the cubic in x is irreducible; hence it has three roots in the $GF[p^{3n}]$, whose product is $K \equiv -a^{-1}(gy^3 + \cdots + lz^3)$. Now K is irreducible in the $GF[p^n]$. In the $GF[p^{3n}]$ every set of three factors of K, conjugate with respect to the $GF[p^n]$, may be given the form $\gamma(y - \rho z)$, $\gamma^{p^n}(y - \rho^{p^n}z)$, $\gamma^{p^{2n}}(y - \rho^{p^{2n}}z)$, where γ is a root of

$$\gamma^{p^{2n}+p^n+1} = -a^{-1}g.$$

It follows that (1) vanishes for $x = \gamma(y-\rho z)$. In other words, C must have a linear factor, in the $GF[p^{3n}]$,

$$(2) \qquad x - \lambda y - \mu z.$$

For $x = \lambda y + \mu z$, let C become

$$R_0y^3 + R_1y^2z + R_2yz^2 + R_3z^3.$$

Then for y and z arbitrary in the $GF[p^n]$, this sum must vanish for suitably chosen values of λ and μ in the $GF[p^{3n}]$. Hence the four equations $R_i = 0$ must be solvable simultaneously in the $GF[p^{3n}]$.

The conditions $R_i = 0$ are seen to be

$$(3)\ R_0 \equiv a\lambda^3 + b\lambda^2 + d\lambda + g = 0, \quad (4)\ R_3 \equiv a\mu^3 + c\mu^2 + e\mu + l = 0,$$

$$(5)\ R_1 \equiv R_0'\mu + c\lambda^2 + f\lambda + h = 0, \quad (6)\ R_2 \equiv R_3'\lambda + b\mu^2 + f\mu + k = 0,$$

where the accents denote differentiation. If (3) had a root in the $GF[p^n]$, C would vanish for $x = \lambda$, $y = 1$, $z = 0$. Hence (3) and (4) must be irreducible in the $GF[p^n]$. Thus $R_0' \neq 0$, $R_3' \neq 0$.

For λ a root of (3) and for μ defined by (5), we seek the condition under which (2) vanishes for a set of elements x, y, z, not all zero, in the $GF[p^n]$. Eliminating μ between

* To include the cases $p = 2$, $p = 3$, we do not prefix binomial coefficients.

$$x-\lambda y-\mu z=0$$

and (5), and then eliminating λ^3 by (3), we obtain

(7) $\lambda^2(3ax+by+cz)+\lambda(2bx+2dy+fz)+dx+3gy+hz=0,$

Hence such elements x, y, z do not exist if, and only if,

$$(8) \qquad \begin{vmatrix} 3a & b & c \\ 2b & 2d & f \\ d & 3g & h \end{vmatrix} \neq 0.$$

THEOREM. *The necessary and sufficient conditions that C shall vanish for no set of values x, y, z in the $GF[p^n]$, other than $x=y=z=0$, are that C shall have a linear factor* (2) *in the $GF[p^{3n}]$, that* (3) *shall be irreducible in the $GF[p^n]$, and that* (8) *shall hold.*

3. We readily deduce the theorem of § 1 from the preceding theorem. When the conditions of the latter theorem are satisfied, C has three distinct linear factors in the $GF[p^{3n}]$ and hence can be transformed into $\xi\eta\zeta$. The Hessian of the latter is $2\xi\eta\zeta$. In view of the covariance of the Hessian, we conclude that the Hessian of C is of the form mC, m an element $\neq 0$ of the $GF[p^n]$, $p>2$. Conversely when the Hessian has this property, C has three distinct linear factors.* Each factor is of the form (2), where λ is a root of the irreducible equation (3) and μ is uniquely determined by (5), so that λ and μ belong to the $GF[p^{3n}]$. Further, (8) is satisfied when $m \neq 0$. Indeed, the coefficients of (7) equal $\frac{1}{2}C_{xx}$, C_{xy}, $\frac{1}{2}C_{yy}$, respectively; if they all vanished, the Hessian would vanish.

4. Although the conditions on the coefficients of C may be obtained from the Hessian, we deduce them in convenient form directly from the conditions for the simultaneity of the four equations $R_i=0$ in the $GF[p^{3n}]$.

For any field we may make $b=0$ in (1) by an obvious transformation on y and z. Moreover the case $b=0$ is sufficient for the applications to linear algebras.

---

* For a direct proof for finite fields, see §§ 5, 6. In the algebraic theory of ternary cubic forms, this property follows from the canonical types (cf. Gordan, *Transactions*, vol. 1, p. 403). We note that if the Hessian of $x^3+y^3+z^3+6mxyz$ is a multiple of the form, then $m=-\frac{1}{2}\omega$, where $\omega^3=1$. Replacing ωz by Z, we obtain the factors $x+y+Z$, $x+\omega y+\omega^2 Z$, $x+\omega^2 y+\omega Z$.

Eliminating μ between (5) and (6) and then eliminating the higher powers of λ by means of (3), we obtain a quadratic function of λ, which must vanish identically, in view of the irreducibility of (3). Hence

$$(9) \qquad 3aJ = 0, \quad dJ = 0, \quad 3aK + dL = 0,$$

where

$$J = afh - adk - 3aeg + c^2g,$$

$$(10) \qquad K = ah^2 - 3agk + cfg - cdh,$$

$$L = ach + 4ade - af^2 - c^2d.$$

But for $b = 0$, (8) becomes

$$(11) \qquad 6adh - 9afg - 2cd^2 \neq 0.$$

Thus $3a$ and d do not both vanish. Hence

$$(12) \qquad J = 0.$$

Eliminating λ between (5) and (6), and dividing by R_3, we obtain the quotient

$$(13) \quad Q \equiv 9a^2d\mu^2 + (3acd + 9a^2h)\mu + c^2d + 3ach - 3ade,$$

and a remainder of degree two, which must vanish identically, in view of the irreducibility of $R_3 = 0$. Hence

$$(14) \quad cL - 3aM = 0, \quad eL + 3aN = 0, \quad eM + cN = 0,$$

where

$$(15) \quad M = 3adl - afk + aeh, \quad N = ak^2 - 3ahl - cdl.$$

We proceed to prove that, if Q is not identically zero, and if conditions (9), (11), (14) are satisfied, and if (3) is irreducible in the $GF[p^n]$, then the four equations $R_i = 0$ are simultaneous in the $GF[p^{3n}]$. Let λ be a root of (3) and μ be defined by (5). In view of the origin of (9), μ satisfies (6). In view of the origin of (14), μ satisfies $QR_3 = 0$. It remains only to show that $Q \neq 0$. First, μ is not an element of the $GF[p^n]$. For, if so, equation (5) and the irreducibility of (3) would give

$$3a\mu + c = 0, \quad f = 0, \quad d\mu + h = 0,$$

and determinant (8) would vanish, having proportional elements in the first and third columns. Next, a mark μ of the $GF[p^{3n}]$, not in the $GF[p^n]$, cannot belong to the $GF[p^{2n}]$. Hence $Q \neq 0$.

5. Finally, let Q be identically zero. The case $p = 3$ is excluded, since then $cd \neq 0$ by (11). Hence $d = h = 0$. Then $fg \neq 0$ by (11). By (9),

$$c^2 = 3ae, \quad cf = 3ak. \tag{16}$$

Then (14) are satisfied, viz., the result of eliminating λ between (5) and (6) now vanishes identically. Removing the factor λ in (5), we now have

$$\mu = (-c\lambda - f)/3a\lambda. \tag{17}$$

Substituting this value in (4), eliminating λ^3 by means of (3), and e by means of (16), we get

$$27a^2gl = c^3g - af^3. \tag{18}$$

In the resulting form C satisfying (16), (18) and

$$b = d = h = 0, \quad fg \neq 0 \qquad (p \neq 3), \tag{19}$$

we replace x by $X - \frac{1}{3}ca^{-1}z$ and obtain

$$aX^3 + gy^3 - \tfrac{1}{27}a^{-1}g^{-1}f^3z^3 + fXyz. \tag{20}$$

Its Hessian is seen to equal $-6f^2C$. Let

$$g = -a\nu, \quad y = -Y, \qquad fz = 3a\nu Z.$$

Then by (20) and (3),

$$C = a(X^3 + \nu Y^3 + \nu^2 Z^3 - 3\nu XYZ), \tag{21}$$

where $\lambda^3 = \nu$ is irreducible in the $GF[p^n]$, whence $p^n = 3m + 1$. After the present change of notation is made, (2) becomes, in view of (17),

$$X + \lambda Y + \lambda^2 Z. \tag{22}$$

This is indeed a factor of (21) for $\lambda^3 = \nu$. Connected with this form (21) is a remarkable non-linear algebra in three units in which division is always uniquely possible.*

* Dickson, *Göttinger Nachrichten*, 1905, p. 359, p. 373.

6. Returning to the case in which Q is not identically zero, we treat first the case in which the modulus exceeds 3. Then we may transform * (1) into a form having $b = c = f = 0$. Condititions (9)–(15) then reduce to $dh \neq 0$ and

$$(23) \qquad \begin{aligned} dk + 3eg = 0, \quad 4de^2 + 3ak^2 - 9ahl = 0, \\ eh + 3dl = 0, \quad 4d^2e + 3ah^2 - 9agk = 0. \end{aligned}$$

The second may be derived from the other three. In view of these conditions the Hessian of C reduces to $3deC$. Evidently $e \neq 0$.

Conversely, if the Hessian $3adex^3 + \cdots$ of a form C, having $b = c = f = 0$, is a non-vanishing multiple of C, then conditions (23) follow. Also $h \neq 0$. For, if $h = 0$, conditions (23) give

$$l = 0, \quad d = \frac{-3ak^2}{4e^2}, \quad g = \frac{ak^3}{4e^3},$$

and (3) would vanish for $\lambda = -k/e$.

7. We may readily enumerate the resulting forms C. We consider first the case $p > 3$, and set $\epsilon = 1$ if $p^n = 3m + 1$, $\epsilon = 0$ if $p^n = 3m + 2$. We set $b = c = 0$, thus considering one of p^{2n} coordinate cases. Let first $Q \equiv 0$, so that d, h, e, k all vanish (§ 5). There are $\frac{2}{3}\epsilon(p^n - 1)^2$ sets a, g for which $a\lambda^3 + g = 0$ is irreducible in the $GF[p^n]$. Now f may have any value $\neq 0$; while l is determined by (18). Hence there are

$$\tfrac{2}{3}\epsilon(p^n - 1)^3 p^{2n} \text{ forms with } Q \equiv 0.$$

For $Q \not\equiv 0$, d and h are not both zero. Let first $d = 0$. For each of the $\frac{2}{3}\epsilon(p^n - 1)^2$ sets a, g, the coefficients h and e may have any values not zero, f being not zero by (11). Then $f = 3egh^{-1}$, $k = \frac{1}{3}g^{-1}h^2$ by $J = K = 0$, and M is then zero. Finally, $eL + 3aN = 0$ determines l. Next, for $d \neq 0$, we make $f = 0$ and apply § 6. The number of irreducible cubics $a\lambda^3 + d\lambda + g$ with $d \neq 0$ is †

$$\kappa \equiv \tfrac{1}{3}(p^{2n} - 1)(p^n - 1) - \tfrac{2}{3}\epsilon(p^n - 1)^2.$$

---

* First by $x' = x + \rho y + \sigma z$ we make $b = c = 0$. The coefficient of x is a binary quadratic form, so that the term fyz may be deleted.

† BULLETIN, October, 1906, p. 4.

For each set a, d, g, and for any $h \neq 0$, (23) give

$$l = \frac{-eh}{3d}, \quad k = \frac{-3eg}{d}, \quad e(4d^3 + 27ag^2) = -3adh^2,$$

the coefficient of e being the discriminant of the irreducible cubic. In view of b, c, f, we have the factor p^{3n}. Hence there are

$$\tfrac{2}{3}\epsilon(p^n - 1)^4 p^{2n} + \kappa(p^n - 1)p^{2n} \text{ forms with } Q \not\equiv 0.$$

THEOREM.* *The total number of ternary cubic forms in the* $GF[p^n]$ *which vanish in the field only for* $x = y = z = 0$ *is*

$$(24) \qquad \tfrac{1}{3}(p^{2n} - 1)(p^n - 1)^2 p^{3n}.$$

8. Consider the automorphs of one of our ternary forms C. In view of (3) and (5), we find that $\mu = r\lambda^2 + s\lambda + t$, where $r \neq 0$. Now $C = L_1 L_2 L_3$, where

$$(25) \quad L_1 = x - \lambda y - \mu z, \quad L_2 = x - \lambda^{p^n} y - \mu^{p^n} z, \quad L_3 = x - \lambda^{p^{2n}} y - \mu^{p^{2n}} z.$$

The determinant D of the coefficients in the L's is a mark $\neq 0$ of the $GF[p^n]$, since $D^{p^n} = D$. Let $L_1' = x' - \lambda y' - \mu z'$, etc. The transformation

$$(26) \qquad L_1' = \tau L_1, \quad L_2' = \tau^{p^n} L_2, \quad L_3' = \tau^{p^{2n}} L_3,$$

yields x', y', z' as functions of x, y, z with coefficients in the $GF[p^n]$. Hence there are $p^{2n} + p^n + 1$ automorphs (26) of C. Further,

$$(27) \qquad L_1' = L_2, \quad L_2' = L_3, \quad L_3' = L_1$$

and its square are automorphs of C. Evidently every automorph is generated by (26) and (27).

THEOREM. *The number of automorphs of* C *is* $3(p^{2n}+p^n+1)$.

9. In view of the order of the general ternary linear homogeneous group in the $GF[p^n]$ and the preceding theorem, it follows that a form C is one of

$$\frac{(p^{3n} - 1)(p^{3n} - p^n)(p^{3n} - p^{2n})}{3(p^{2n} + p^n + 1)} = \tfrac{1}{3}(p^{2n} - 1)(p^n - 1)^2 p^{3n}$$

conjugates. But this number is the same as (24).

* Another proof results from an enumeration of the distinct products of three linear forms in the $GF[p^{3n}]$ conjugate with respect to the $GF[p^n]$.

THEOREM. *In the* $GF[p^n]$, *all ternary cubic forms which vanish only for* $x = y = z = 0$ *are equivalent under linear transformation.*

10. We consider briefly the case* $p = 2$, the Hessian of C being then identically zero. By an obvious transformation we may make $b = c = h = 0$. Then $afg \neq 0$ by (11). Since it remains only to treat the case in which (18) does not vanish identically, we may set $d \neq 0$. Conditions (9)–(14) then reduce to

$$dk = eg, \quad agk = df^2, \quad dl = fk, \quad ef^2 = ak^2,$$

the last being superfluous. We may determine ρ so that $d\rho^2 = a$. We set

$$x = X, \quad y = \rho Y, \quad z = \frac{ga}{fd} Z, \quad \gamma = \frac{g\rho}{d}.$$

Then C has the factor a, which may be made unity by applying a transformation (26). The complementary factor is

$$(28) \quad X^3 + XY^2 + XZ^2 + \gamma XYZ + \gamma Y^3 + \gamma YZ^2 + \gamma^2 Z^3.$$

Multiplying (5) by λ and applying (3), we get

$$g\mu = f\lambda^2.$$

Let $\tau = \rho\lambda$. Then (3) becomes

$$(29) \qquad \tau^3 + \tau + \gamma = 0.$$

The factor (2) of C is seen to equal

$$(30) \qquad X + \tau Y + \tau^2 Z.$$

By a preliminary transformation on x and y, the irreducible cubic (29) may be transformed into any particular one.

THEOREM. *In the* $GF[2^n]$, *every ternary cubic form which vanishes only for* $x = y = z = 0$ *may be transformed into* (28), *where* γ *is a particular mark for which* (29) *is irreducible.*

11. We proceed to determine all finite triple linear algebras in which multiplication is commutative and distributive, but

* For $p = 3$, I have determined canonical types of all ternary cubic forms. The results are to appear shortly in the *American Journal.*

not necessarily associative, while division is always uniquely possible. We may assume (*Göttinger Nachrichten*, l. c.) that the units are 1, i, j, where

$$(31)\qquad i^2 = j, \quad ij = ji = g - di, \quad j^2 = h + \delta i + Dj,$$

$x^3 + dx - g$ being irreducible in the $GF[p^n]$. In

$$(x + yi + zj)(\xi + \eta i + \zeta j) = P + Qi + Rj,$$

the determinant of the coefficients of ξ, η, ζ in P, Q, R is of the form (1) with

$$(32)\qquad \begin{aligned} &a = 1, \quad b = 0, \quad c = D - d, \quad e = -h - dD, \\ &f = -\delta - 2g, \quad k = -gD, \quad l = \delta g + dh, \end{aligned}$$

the coefficients g, d, h being the same in the two forms. Let λ be a root, in the $GF[p^{3n}]$, of (3), viz.,

$$(3')\qquad \lambda^3 + d\lambda + g = 0.$$

Thus $-\lambda$ plays a rôle analogous to the unit i of the algebra. We may regard $\lambda, d, g, h, \delta, D$ to be of dimensions 1, 2, 3, 4, 3, 2 respectively. Hence we shall set*

$$(33)\qquad h = \epsilon d^2, \quad \delta = \tau g, \quad D = \kappa d,$$

ϵ, τ, κ being of dimension zero. Then, by (5),

$$-\mu = [(\kappa - 1)d\lambda^2 - (\tau + 2)g\lambda + \epsilon d^2] \div (3\lambda^2 + d).$$

The numerator is of dimension 4, the denominator 2. Hence

$$(5')\qquad -\mu = \rho\lambda^2 + \sigma d,$$

where ρ, σ are of dimension zero. Equating the two values and reducing by (3′), we obtain

$$(34)\qquad \kappa - 1 = 3\sigma - 2\rho, \quad \tau + 2 = 3\rho, \quad \epsilon = \sigma.$$

Next, (6) becomes

$$[3\mu^2 + 2(\kappa - 1)d\mu - (\kappa + \epsilon)d^2]\lambda - (\tau + 2)g\mu - \kappa dg = 0.$$

Eliminating μ by (5′), reducing by (3′), and applying (34), we get

* The case $d = 0$ may be avoided by a transformation of units.

$$(35)\qquad \begin{aligned} 4\rho\sigma - \rho^2 - 3\sigma^2 - 4\sigma + 2\rho - 1 = 0,\\ (\rho - 1)(\rho - 1 - 3\sigma) = 0, \end{aligned}$$

the coefficient of λ^2 being zero. For $\rho = 1$, $\sigma = 0$, and the algebra is a field. For $\rho = 1 + 3\sigma$, (35_1) is satisfied; then $\kappa = -\rho$. Substituting (5′) in (4) and reducing by (3′), we find that the coefficients of λ^2 and λ vanish, and that the constant term is

$$-\sigma^2(\sigma + 1)(4d^3 + 27g^2) = 0.$$

But the second factor is not zero in view of the irreducibility of (3′). For $\sigma = 0$, the algebra is a field. For $\sigma = -1$, $\rho = -2$, and we obtain the non-field algebra

$$(36)\quad i^2 = j,\quad ij = ji = g - di,\quad j^2 = -d^2 - 8gi + 2dj.$$

THE UNIVERSITY OF CHICAGO,
September, 1907.

ISOTHERMAL SYSTEMS IN DYNAMICS.

BY PROFESSOR EDWARD KASNER.

(Read before the American Mathematical Society, October 26, 1907.)

CONSIDER any simply infinite system of plane curves defined by its differential equation

$$(1)\qquad y' = f(x, y).$$

The ∞^2 isogonal trajectories satisfy the equation *

$$(2)\qquad y'' = (F_x + y'F_y)(1 + y'^2),$$

where

$$F = \tan^{-1} f.$$

The theorem of Cesàro-Scheffers states that the trajectories passing through a given point have circles of curvature forming a pencil. We inquire whether any hyperosculating circles exist.

* Primes are employed to denote derivatives with respect to x, and literal subscripts to denote partial derivatives.