DEFINITE FORMS IN A FINITE FIELD*

BY

LEONARD EUGENE DICKSON

§ 1. *Introduction; summary of results.*

THE character of the present investigation may be indicated by the following special case of a theorem proved below:

Let p be an odd prime number and $Q(x, y)$ a binary quartic form with integral coefficients. If, for each pair of integers x', y', not both divisible by p, $Q(x', y')$ is a quadratic residue of p, then $Q(x, y)$ is formally congruent, modulo p, to the square of a binary quadratic form.

In other words, there exists an algebraic identity

$$Q(x, y) = (ax^2 + bxy + cy^2)^2 + pQ_1(x, y),$$

in which a, b, c and the coefficients of the quartic Q_1 are integers.

In the proof of the preceding result, it is convenient to introduce Galois imaginaries, i. e., to extend the initial field of integers modulo p to a larger Galois field.† As it adds to the clearness and generality of the question and does not increase the difficulties of the analysis, the investigation will be made from the outset for forms in the general Galois field of order p^n, designated $GF[p^n]$. The latter is composed of the p^n elements $a_0 + a_1\rho + \cdots + a_{n-1}\rho^{n-1}$, in which the a_i are integers taken modulo p, and ρ is a root of a congruence of degree n irreducible modulo p. An element, not zero, is called a square or a not-square according as it equals or does not equal the square of some element of the $GF[p^n]$. We here exclude the case $p = 2$, since then every element $\neq 0$ is a square.

A form $F(x_1, \cdots, x_m)$ will be said to be definite in the $GF[p^n]$, if, for each set of elements $x_1', \cdots, x_m'$, not all zero, in the field, $F(x_1', \cdots, x_m')$ is a square in the field. To obtain the forms which represent not-squares exclusively, we have only to multiply the definite forms by a particular not-square.

The result stated above is thus a special case of the following:

THEOREM I. *Every definite binary quartic in the $GF[p^n]$, $p > 2$, is formally a perfect square in the field.*

---

* Presented to the Society at the Summer Meeting at Champaign, September 10, 1908.

† Cf. the writer's *Linear Groups*, pp. 5–14.

From the latter we deduce, in § 3,

THEOREM II. *There exists no definite quartic form in the* $GF[p^n]$, $p > 2$, *on* m *variables when* $m > 2$.

There is no definite form of odd degree d in a finite field. Indeed, for $a \neq 0$, ax^d may be made a square or a not-square by choice of x in the field. For $r > 1$, any r-ary quadratic form in the $GF[p^n]$, $p > 2$, represents both squares and not-squares * and hence is not definite.

THEOREM III. *For* $p^n \geqq 13$, *every definite binary sextic in the* $GF[p^n]$ *is formally a perfect square. For* $p^n < 13$, *there exists at least one additional type of definite binary sextics* (§ 4).

It is probable that every definite binary form of degree $2r$ ($r > 1$) in the $GF[p^n]$ is formally a perfect square whenever p^n exceeds a certain limit N_r. If this conjecture should prove to be correct, it would not be particularly difficult to establish for forms of degree $2r$ on m variables a general theorem including as special cases Theorem II and the following:

THEOREM IV. *For* $p^n \geqq 11$, *every definite ternary sextic in the* $GF[p^n]$ *is formally a perfect square; there exists no definite sextic in the* $GF[p^n]$, $p > 2$, *on* m *variables when* $m > 3$.

The simplicity † of the preceding existence theorems on definite forms enhances their value for applications in number-theoretic investigations. Immediate application may be made to the determinant of a net of quadratic forms in a finite field.

A method of deriving definite forms from a given one is explained in § 7.

Some general arithmetical properties of definite binary forms are obtained in § 8 by restricting the range of the variables to the elements of the finite field.

§ 2. *Definite binary quartic forms.*

Let $q = c_0x^4 + c_1x^3y + \cdots$ be a binary quartic with coefficients in the $GF[p^n]$, $p > 2$, and let q equal a square for each pair of elements x, y, not both zero, in the field. Taking $x = 1$, $y = 0$, we see that c_0 must be a square. Set $Q = q/c_0$. Then for every x, y, not both zero, in the $GF[p^n]$,

$$Q(x, y) = x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4$$

equals a square. In particular, Q has no linear factor and hence is either irreducible or is the product of two irreducible quadratic factors in the field.

First, we assume that Q is irreducible in the $GF[p^n]$. Hence a root ρ of $Q(x, 1) = 0$ defines the $GF[p^{4n}]$; thus

$$Q = \prod_{i=0}^{3}(x - \rho^{p^{ni}}y) = (x - \rho y)^{(p^{4n}-1)/(p^n-1)}.$$

* *Linear Groups*, pp. 46–48.

† In contrast to the algebraic theory. Cf. HILBERT, Acta Mathematica, vol. 17 (1893), p. 169, where references to other papers are given.

By hypothesis, $Q^{(p^n-1)/2}=1$ for x and y not both zero. Hence

$$(x-\rho y)^{(p^{4n}-1)/2}=1,$$

so that $x-\rho y$ is a square in the $GF[p^{4n}]$ for each pair of elements x, y, not both zero, in the $GF[p^n]$. Thus, for x_i in the latter field,

$$(1)\quad f_x=\frac{(x_1-\rho)(x_2-\rho)}{x_3-\rho},\qquad g_x=\frac{x_1-\rho}{x_3-\rho},\qquad h_x=(x_1-\rho)(x_2-\rho)$$

are squares in the $GF[p^{4n}]$; likewise their products by any non-vanishing element of the $GF[p^n]$. We next show that the products

$$(2)\qquad af_x,\qquad a'g_{x'},\qquad a''h_{x''}$$

take only distinct values when the a's range independently over the elements $\neq 0$ of the $GF[p^n]$, x_1 and x_2 take equal values or one of the two sets defined by a pair of unequal values, while x_3 has any value distinct from x_1 and x_2 in the field. Of the three types (2), no function of one type equals one of another type, in view of the difference of their degrees in ρ, a root of an irreducible quartic. If $ag_x=bg_y$, then $a=b$, $y_1=x_1$, $y_3=x_3$, and the functions are identical. Similarly, ah_x and bh_y are equal only when identical. If $af_x=bf_y$, then $a=b$ and x_1, x_2, y_3 form a permutation of y_1, y_2, x_3; but x_3 is distinct from x_1, x_2; hence $x_3=y_3, f_x\equiv f_y$. In counting the number of values (1), we separate the cases $x_1=x_2$, $x_1\neq x_2$; the resulting number is

$$\{p^n(p^n-1)+\tfrac{1}{2}p^n(p^n-1)(p^n-2)\}+p^n(p^n-1)+\{p^n+\tfrac{1}{2}p^n(p^n-1)\}.$$

Since a has p^n-1 values, the number of distinct values (2) is

$$\tfrac{1}{2}p^n(p^{2n}+2p^n-1)(p^n-1).$$

This exceeds $\frac{1}{2}(p^{4n}-1)$, the total number of squares in the $GF[p^{4n}]$. In fact, for $p^n\geqq 3$, we have

$$(p^{2n}-2p^n-1)(p^n-1)>0.$$

Hence Q cannot be irreducible in the field.

Let therefore Q be the product of two quadratic factors, each irreducible in the $GF[p^n]$, $p>2$. One factor may be transformed linearly into $x^2-\nu y^2$, where ν is a fixed not-square in the $GF[p^n]$. Let the second factor become

$$x^2+2axy+by^2=(x+ay)^2-(a^2-b)y^2.$$

Hence a^2-b is a not-square νc^2. Thus

$$(3)\qquad Q=(x^2-\nu y^2)[(x+ay)^2-\nu c^2y^2]\quad (c\neq 0,\ \nu \text{ a not-square}).$$

Consider the values of x and y, $y\neq 0$, for which the first factor is a square s^2. Set $x-s=t$, so that $t\neq 0$. Then $x+s=\nu y^2/t$ and

$$2x=t+\nu y^2/t.$$

The second factor of Q must also be a square, so that

$$(t + \nu y^2/t + 2ay)^2 - 4\nu c^2 y^2$$

must be a square. Set $t = zy$. Then*

$$q = (z^2 + 2az + \nu)^2 - 4\nu c^2 z^2 \tag{4}$$

must be a square for every z in the $GF[p^n]$.

We may define the $GF[p^{2n}]$ by means of the equation $J^2 = \nu$, which is irreducible in the $GF[p^n]$. Then $J^{p^n} = -J$, and

$$q = F_z^{p^n+1}, \qquad F_z \equiv z^2 + 2az + \nu - 2czJ. \tag{5}$$

By hypothesis $q^{(p^n-1)/2} = 1$. Hence $F_z^{(p^{2n}-1)/2} = 1$, so that F_z is a square in the $GF[p^{2n}]$ for every z in the $GF[p^n]$. If

$$kF_z = \kappa F_\zeta \qquad (k \neq 0, \kappa \neq 0),$$

then

$$kz = \kappa\zeta, \qquad k(z^2 + \nu) = \kappa(\zeta^2 + \nu).$$

Eliminating k and κ, we get

$$(\zeta - z)(\zeta z - \nu) = 0.$$

If $z = 0$, then $\zeta = 0$. If $z \neq 0$, then $\zeta = z$ or ν/z. The latter values are distinct, one being a square and the other a not-square. Hence the distinct values of the functions kF_z are obtained† by allowing z to range over the elements 0 and the $\frac{1}{2}(p^n - 1)$ squares of the $GF[p^n]$, while k ranges over all the elements $\neq 0$. The resulting $\frac{1}{2}(p^n + 1)(p^n - 1)$ values kF_z account for all the $\frac{1}{2}(p^{2n} - 1)$ squares of the $GF[p^{2n}]$. Hence every square in the $GF[p^{2n}]$ may be given the form kF_z.

We have shown that, for arbitrary elements l and λ, each $\neq 0$, of the $GF[p^n]$, $l(\lambda - J)^2 = l(\lambda^2 + \nu - 2\lambda J)$ may be given the form kF_z, in which k and z are elements, each $\neq 0$, of that field, and conversely. Hence

$$\frac{\lambda^2 + \nu}{\lambda}, \qquad \frac{z^2 + 2az + \nu}{cz} \tag{6}$$

must take the same set of values when λ and z range over the marks $\neq 0$ of the $GF[p^n]$, viz., over the roots of

$$w^{p^n-1} - 1 = 0. \tag{7}$$

The sum of the roots of (7) is zero; likewise the sum of their reciprocals.

* This form is better adapted to the later discussion that the forms of Q,

$$(x^2 + axy \mp \nu cy^2)^2 - \nu\{xy(1 \mp c) + ay^2\}^2,$$

derived from (3) by the usual process or by the use of the irrationality $\nu^{\frac{1}{2}}$.

† Also by the formulæ k, $s^2 F_z$ (z taking all values $\neq 0$).

Taking the sums of the values of each function (6), we have

$$0 = \frac{2a}{c}(p^n - 1),$$

whence $a = 0$. If $p^n = 3$, we have $c = \pm 1$, since $c \neq 0$. Next, if $p^n > 3$, the sum of the squares of the roots of (7) equals zero; likewise the sum of the reciprocals of their squares. Taking the sums of the squares of the values of each function (6), we have, since $a = 0$,

$$2\nu(p^n - 1) = c^{-2} \cdot 2\nu(p^n - 1),$$

whence $c^2 = 1$. Hence, for $p^n \geqq 3$, the two factors (3) are identical. Theorem I is therefore proved.

§ 3. *Definite quartic forms on m variables.*

Consider a ternary quartic which represents only squares in the $GF[p^n]$, $p > 2$. The coefficient a_0 of x^4 must be a square; dividing the form by a_0, we obtain a definite ternary form $x^4 + \cdots$. Applying a transformation

$$x = x' + ry' + sz', \qquad y = y' + tz', \qquad z = z',$$

we obtain a definite ternary form Q lacking the terms x^3y, x^3z, y^3z. By § 2, the terms free of z are $(x^2 - \nu y^2)^2$, those free of y are $(x^2 - \nu s^2 z^2)^2$. Replacing sz by a new variable z, we have $s = 1$. The terms free of x are therefore $\nu^2(y^2 \pm z^2)^2$. But Q vanishes only when $x = y = z = 0$. Hence the upper sign holds and -1 must be a not-square. We may therefore set $\nu = -1$. Hence

$$Q = (x^2 + y^2 + z^2)^2 + xyz(ax + by + cz).$$

Now Q must represent a square for every x, y, z, not all zero, in the field and hence for $x = \lambda y$, λ arbitrary in the field. Then Q becomes

$$Q' = (\lambda^2 + 1)^2 y^4 + (a\lambda^2 + b\lambda) y^3 z + (2\lambda^2 + 2 + \lambda c) y^2 z^2 + z^4.$$

By § 2, Q' must be formally a perfect square. Hence Q' must be the square of $(\lambda^2 + 1)y^2 \pm z^2$, for every λ in the $GF[p^n]$ and for arbitrary variables y, z. Hence, since $p^n \geqq 3$, $a = b = c = 0$. But * $x^2 + y^2 + z^2$ vanishes for $p^{2n} - 1$ sets of values x, y, z, each $\neq 0$, in the $GF[p^n]$, $p > 2$. Hence there exists no definite ternary quartic in a finite field. Theorem II therefore follows.

§ 4. *Definite binary sextic forms.*

By a rather intricate analysis, which I omit in the hope that a more direct method may be invented, I find that every definite binary sextic in the $GF[p^n]$, $p^n > 11$, is formally a perfect square.

* *Linear Groups*, p. 48.

Of the exceptional cases $p^n \leqq 11$, I first give the results for $p^n = 5$ and 7, in which cases we may at once remove the term x^5y.

For $p^n = 5$, I multiply the variables by suitable constants and get

$$x^6 + bx^4y^2 \pm cx^3y^3 + dx^2y^4 \pm exy^5 + y^6. \tag{8}$$

After fixing the sign, I find that the definite forms (8) are

$$\begin{gathered}(x^2-2y^2)(x^4+x^2y^2+2y^4), \quad (x^3+2x^2y+xy^2-2y^3)(x^3-2x^2y+xy^2+2y^3), \\ (x^3+xy^2+y^3)^2, \qquad x^6+2x^4y^2+x^3y^3+2x^2y^4-xy^5+y^6,\end{gathered} \tag{9}$$

$$\begin{gathered}(x^3+2xy^2-y^3)^2, \qquad x^6+x^4y^2+2x^3y^3+2x^2y^4+2xy^5+y^6, \\ (x^2+xy+2y^2)(x^4-x^3y-2xy^3-2y^4), \quad (x^2+xy+2y^2)(x^4-x^3y-2x^2y^2-2y^4),\end{gathered} \tag{10}$$

and those derived from (9_1) and (9_2) by interchanging x with y. To (9_3) and (9_4) I apply the respective transformations

$$x \equiv -2Y,\ y \equiv X-Y; \qquad x \equiv -X,\ y \equiv X+Y \pmod 5$$

and obtain (10_1) and (10_2), written in X, Y. Forms (10_3) and (10_4) are transformed into (9_1), written in X, Y, by the respective transformations

$$x \equiv -2Y,\ y \equiv -X-2Y; \qquad x \equiv 3X-Y,\ y \equiv X+Y \pmod 5.$$

Every definite binary sextic modulo 5 *may be linearly transformed into one of the four types* (9), *in which the fourth form and the indicated factors are irreducible modulo* 5.

For $p^n = 7$, a definite sextic may be given the form $\alpha^2 S$, where

$$S = x^6 + bx^4y^2 + cx^3y^3 + dx^2y^4 + exy^5 + \sigma y^6, \tag{11}$$

where $\sigma \equiv 1, 2, 4$; $b \equiv 0, 1, -1$. Set

$$\begin{aligned} m_1 &= 1+\sigma+b+d, & n_1 &= c+e, \\ m_2 &= 1+\sigma+2b+4d, & n_2 &= c+2e, \\ m_3 &= 1+\sigma+4b+2d, & n_3 &= -c+3e. \end{aligned}$$

Then S is definite if, and only if, each $m_i + n_i$ and each $m_i - n_i$ is a square. Hence the cube of each is $\equiv 1 \pmod 7$, so that $n_i \equiv 0$, $m_i^3 \equiv 1$, or else

$$n_i^2 \equiv 4m_i^2, \qquad m_i^3 = -1 \qquad (m^i = \text{not-square}). \tag{12}$$

Now the n_i are linearly independent modulo 7, so that two vanish only when $c \equiv e \equiv 0$. In the latter case, each m_i is a square and the four sextics S are seen to be (13_1), (13_2), (14_1), (14_2). Next, if no one of the n_i vanishes, then (12) holds for $i = 1, 2, 3$, and the resulting forms S are (13_3), (14_3), (15_1), and those with the sign of x changed. There remains the case in which just one of the n_i vanishes. First, let $n_1 \equiv 0$, $e \not\equiv 0$. Then

$$n_2^2 \equiv e^2 \equiv 4m_2^2, \qquad n_3^2 \equiv 2e^2 \equiv 4m_3^2, \qquad m_3^2 \equiv 2m_2^2.$$

Hence $m_3 \equiv \pm 3m_2$. But m_2 and m_3 are not-squares, so that $m_3 \equiv -3m_2$, $b \equiv 1+\sigma$. Hence this case is excluded. Next, if $n_2 \equiv 0$, $e \not\equiv 0$, we find similarly that $2b \equiv 1+\sigma$, whence $\sigma \equiv b \equiv 1$ or $\sigma \equiv 4$, $b \equiv -1$. After changing the sign of x, we get (15_2), (15_3), (16_1). Finally, if $n_3 \equiv 0$, $e \not\equiv 0$, then $4b \equiv 1+\sigma$, $\sigma \equiv 2$, $b \equiv -1$, and we get (16_2) after changing the sign of x.

(13) $x^6+y^6 \equiv (x^2+y^2)(x^2+2y^2)(x^2+4y^2)$, $x^6-x^4y^2-x^2y^4+2y^6$, $(x^3-2y^3)^2$,

(14) $x^6+x^4y^2+x^2y^4+y^6$, $x^6-x^4y^2-2x^2y^4+4y^6$, $(x^3-3xy^2+y^3)^2$,

(15) $(x^3+3y^3)^2$, $x^6+x^4y^2-2x^3y^3+xy^5+y^6$, $(x^3+3xy^2-2y^3)^2$,

(16) $x^6+x^4y^2+3x^3y^3+3x^2y^4+2xy^5+y^6$, $x^6-x^4y^2-x^3y^3+x^2y^4+2xy^5+2y^6$.

Now $x=X+Y$, $y=X-Y$ transforms (13_1) into the double of (14_1); while $x=3Y$, $y=X$ transforms (13_2) into the double of (14_2). In (15_2) we replace y by $y+x$ (to cancel xy^5) and then interchange x, y; we obtain (13_2). In the latter we set $x=-X+Y$, $y=3X+2Y$, and get 4 times (16_1). In the latter we set $x=Y$, $y=2Y-X$, and obtain (16_2).

If C and C' are two binary cubic forms, each irreducible in the $GF[p^n]$, there exists a linear transformation in that field which transforms C into a multiple of C'.

Hence *every definite binary sextic modulo* 7 *may be linearly transformed into* $\alpha^2 S$, *where* $\alpha^2 = 1, 2, 4$, *while* S *is one of the three forms* (13), *the second being irreducible modulo* 7.

THEOREM. *Within the* $GF[3^n]$, $n>1$, *any binary sextic*

$$S = x^6+ax^5y+bx^4y^2+cx^3y^3+dx^2y^4+exy^5+fy^6, \tag{17}$$

not an exact cube, may be linearly transformed into a sextic (17) *with* $a=1$, $b=0$.

We first show that S may be transformed into a sextic with $a \neq 0$. It suffices to treat the case $a=e=0$. Under the transformation

$$x=\alpha\xi+\beta\eta, \qquad y=\gamma\xi+\delta\eta \qquad (\Delta=\alpha\delta-\beta\gamma\neq 0), \tag{18}$$

S becomes S', in which the coefficient of $\xi^5\eta$ is

$$\alpha\gamma\Delta(d\gamma^2-b\alpha^2).$$

If $b=d=0$, S is the cube of

$$x^2+c'xy+f'y^2 \qquad (t=3^{n-1}),$$

contrary to hypothesis. If $b=0$, $d\neq 0$, or if $b\neq 0$, $d=0$, it suffices to take $\alpha\neq 0$, $\gamma\neq 0$. Finally, let $b\neq 0$, $d\neq 0$. If d/b is a not-square, it suffices to take $\alpha\gamma\neq 0$. If $d/b=\sigma^2$, it suffices to take $\alpha\gamma\neq 0$, $\alpha/\gamma\neq\pm\sigma$; for example, we may take $\beta=\gamma=1$, $\delta=0$, α any element except 0, σ, $-\sigma$, a possible choice since $p^n>3$.

To the resulting form (17) with $a \neq 0$, we apply the transformation $x = \xi$, $y = a^{-1}\eta$, and obtain a sextic with $a = 1$. To the latter, we apply the transformation $x = \xi + b$, $y = \eta$, and obtain a sextic with $a = 1, b = 0$.

THEOREM. *A definite binary sextic S in the $GF[3^n]$ can be linearly transformed into a sextic* (17) *with $a = 1, b = 0$, except for the case in which $n = 1$ and S is the product*

$$(19) \quad (x^2 + y^2)(x^2 + xy - y^2)(x^2 - xy - y^2) \equiv x^6 + x^4y^2 + x^2y^4 + y^6$$

of all the irreducible quadratic forms modulo 3.

The coefficient of x^6 must be a square α^2. Replace x by $\alpha^k X$, where $k = -3^{n-1}$. The coefficient of X^6 is now unity. For $n > 1$, the theorem follows from the preceding one, since the case in which S is a cube is now excluded by the fact that a binary quadratic form represents both squares and not-squares. For $n = 1$, the same proof holds except when $a = e = 0$, $d/b = 1$, $f = 1$. Then, if $b = 1$, the case $c \neq 0$ is excluded since S would vanish for $x = -cy$, while $c = 0$ gives (19). If $b = -1$, S vanishes for $x = y$, when $c = 0$; while S is the not-square -1 for $x = -c$, $y = 1$, when $c \neq 0$.

It remains to discuss (17) for $a = 1, b = 0, y \neq 0$. Set $x = zy$. Then

$$(20) \qquad S_1 = z^6 + z^5 + cz^3 + dz^2 + ez + f$$

must be a square for every z in the $GF[3^n]$.

First let $n = 1$. Then must $S_1 \equiv 1 \pmod 3$ for every z. But

$$S_1 \equiv z^2(1 + d) + z(1 + c + e) + f \pmod 3.$$

Hence $d \equiv -1, e \equiv -1 - c, f \equiv 1$. For $c \equiv 0, 1, -1$, S_1 becomes

$$(z^3 - z^2 + z + 1)^2, \qquad (z^2 - z - 1)(z^4 - z^3 - 1), \qquad z^6 + z^5 - z^3 - z^2 + 1,$$

respectively. *Hence every definite binary sextic modulo* 3 *may be linearly transformed into one of the four types* (19) *and*

$$(21) \quad (x^3 - x^2y + xy^2 + y^3)^2, \quad (x^2 - xy - y^2)(x^4 - x^3y - y^4), \quad x^6 + x^5y - x^3y^3 - x^2y^4 + y^6,$$

the last being irreducible; (19) *is invariant under every linear transformation.*

A similar argument shows that the general sextic (17) is definite modulo 3 if, and only if, $b + d \equiv -1, a + c + e \equiv 0, f \equiv 1$. There are just three irreducible quadratics and eight irreducible cubics modulo 3. Sextic (17) has the factor $x^2 + 1$ if, and only if, $c \equiv 0, b \equiv 1$; the factor $x^2 \pm x - 1$ if, and only if, $b \equiv 1 \pm c, a \equiv c$. Thus (17) is the product of $x^2 + 1$ by an irreducible quartic if, and only if, $c \equiv 0, b \equiv 1, a \equiv \pm 1$.

Of the 27 *definite sextics* (17) *modulo* 3, 8 *are equivalent to* (21_1), 6 *to* (21_2), 1 *to* (19), *and the remaining* 12 *to* (21_3).

For the $GF[3^n]$, $n = 2$, we require that (20) shall represent only squares. Hence must $S_1 S_1^3 = 1$ for every root of $z^9 = z$. Now

$$S_1^3 = z^7 + d^3z^6 + e^3z^3 + z^2 + c^3z + f^3,$$

$$S_1^4 = Ax^8 + B^3x^7 + C^3x^6 + Bx^5 + Dx^4 + Ex^3 + Cx^2 + E^3x + f^4,$$

$$A = 1 + e + e^3 + d^4, \qquad B = 1 + c + f^3 + de^3, \qquad C = c + c^3e + df^3 + f,$$

$$D = 1 + d + d^3 + c^4 + e^4, \qquad E = e + d^3 + cf^3 + c^3d + e^3f.$$

Hence the last five functions must vanish, and $f^4 = 1$. These equations were discussed in two distinct ways and found to have exactly three sets of solutions in the $GF[9]$:

$$(c, d, e, f) = (1 + i, 1 - i, i, -1), \quad (0, -1, -1, 1), \quad (1, 0, 1, 1),$$

where $i^2 \equiv -1 \pmod 3$. The resulting functions (20) are

$$(z^3 - z^2 + z - i)^2, \ (z^3 - z^2 + z + 1)^2,$$

$$z^6 + z^5 + z^3 + z + 1 = [z^3 + (i-1)z^2 + (i-1)z - i][z^3 - (i+1)z^2 - (i+1)z + i].$$

Applying suitable linear transformations we find that *every definite binary sextic in the* $GF[3^2]$ *may be linearly transformed into one of two:*

$$(22) \qquad (x^3 - xy^2 - y^3)^2, \ (x^3 - xy^2 - y^3)(x^3 - xy^2 + y^3).$$

For $p^n = 11$, the general discussion showed that every definite binary sextic not a perfect square is the product of three quadratic factors. Since every integer is a cube modulo 11 the general sextic may be reduced to the form (8) by removing the term x^5y and multiplying the variables by suitable integers. The only definite form (8), not a perfect square, is

$$(23) \quad (x^2 + y^2)(x^2 + 2xy - y^2)(x^2 - 2xy - y^2) \equiv x^6 - 5x^4y^2 - 5x^2y^4 + y^6.$$

§ 5. *Definite ternary sextic forms.*

For $p > 3$, we may assume that the ternary sextic T lacks the terms x^5y, x^5z, y^5z, and has unity as the coefficient of x^6. For $p^n > 11$, the terms of T free of one variable form a perfect square (§ 4). Hence the terms free of z, y, x may be taken to be respectively

$$(24) \quad (x^3 + axy^2 + by^3)^2, \qquad (x^3 + cxz^2 + dz^3)^2, \qquad (by^3 + eyz^2 \pm dz^3)^2.$$

The remaining terms of T are of the form

$$(25) \quad xyz(Ax^3 + By^3 + Cz^3 + Dx^2y + Ex^2z + Fxy^2 + Gxz^2 + Ky^2z + Lyz^2 + Mxyz).$$

For * $x = \lambda y$, let T become S. Then S must be a perfect square in y, z for

* As pointed out to me by Professor H. S. WHITE, the algebraic proof in the text has the following geometric analogue: If on each ray of a pencil a sextic curve has three double points, the sextic is a cubic curve counted twice. This helpful analogy was not proposed as a substitute for the algebraic proof. On the one hand, a definite form vanishes for no sets of values x, y, z in the field and one may speak only roughly of a curve. On the other hand, considerations based upon continuity obviously fail in the present modular problem.

every λ in the field. We find that

$$(26)\quad S = P^2y^6 + P_1y^5z + P_2y^4z^2 + P_3y^3z^3 + P_4y^2z^4 + P_5yz^5 + d^2z^6,$$

where

$$P_1 = A\lambda^4 + D\lambda^3 + F\lambda^2 + B\lambda, \qquad P_2 = 2c\lambda^4 + E\lambda^3 + M\lambda^2 + K\lambda + 2be,$$
$$P_3 = 2d\lambda^3 + G\lambda^2 + L\lambda \pm 2bd, \qquad P_4 = c^2\lambda^2 + C\lambda + e^2,$$
$$P_5 = 2cd\lambda \pm 2ed, \qquad P = \lambda^3 + a\lambda + b.$$

In view of the first and last three terms of S, we must have

$$S = \left\{ \epsilon Py^3 + \frac{1}{2d}(C \mp 2ce)\lambda y^2z + (c\lambda \pm e)yz^2 + dz^3 \right\}^2, \qquad \epsilon^2 = 1.$$

Comparing the terms y^3z^3 in the two expressions for S, we find from the coefficients of λ^3 and the constant terms that $\epsilon = +1$ and that the upper signs hold; then from the coefficients of λ^2 and λ,

$$dG = c(C - 2ce), \qquad dL = e(C - 2ce) + 2ad^2.$$

Comparing the terms y^4z^2 and the terms y^5z, we find that

$$E = 2e, \qquad M = 2ac + (C - 2ce)^2/4d^2, \qquad K = 2ae + 2bc,$$
$$D = 0, \qquad dA = C - 2ce, \qquad dF = a(C - 2ce), \qquad dB = b(C - 2ce).$$

Replacing $C - 2ce$ by dA, we get

$$B = bA, \quad C = dA + 2ce, \quad D = 0, \quad E = 2e, \quad F = aA, \quad G = cA,$$
$$K = 2ae + 2bc, \qquad L = eA + 2ad, \qquad M = 2ac + \tfrac{1}{4}A^2.$$

Now T is composed of (25) and the distinct terms (24). Inserting the preceding values of $B, \cdots, M$, we see that T is the square of

$$x^3 + axy^2 + cxz^2 + by^3 + eyz^2 + dz^3 + \tfrac{1}{2}Axyz.$$

Hence the first part of Theorem IV is proved when $p \neq 3$, $p^n > 11$.

For $p^n = 11$, the following instructive proof shows that every definite ternary sextic T is a perfect square. As shown at the end of § 4, every definite binary sextic is either a perfect square S or a product π of three quadratic forms; it will be said to be of type S or π. The terms free of x in T will be designated by B_{yz}, those free of y by B_{xz}, etc. Without disturbing the character of B_{xy} and B_{xz}, we may delete the terms x^5y, x^5z and take the coefficients of x^6, y^6, z^6 to be unity by replacing x by $x + ry + sz$ and then multiplying x, y, z by constants (note that every integer is a cube modulo 11).

Suppose that one of the B's, say B_{xz}, is of type π. Then by (23) and the preceding remark, we may set

$$B_{xz} = x^6 - 5x^4z^2 - 5x^2z^4 + z^6, \qquad B_{xy} = x^6 - 5x^4y^2 - 5x^2y^4 + y^6 \text{ or } (x^3 + axy^2 + y^3)^2.$$

If $a = 0$, T would vanish for $z = 0, x = -y$. Hence in either case,

$$B_{xy} = x^6 + bx^4y^2 + \cdots \qquad (b \neq 0).$$

Upon replacing y by $y + \rho z$, let T become T'. In T', $B'_{xy} = B_{xy}$,

$$B'_{xz} = x^6 + 0x^5z + mx^4z^2 + \cdots, \qquad m = b\rho^2 + A\rho - 5,$$

where A is the coefficient of x^4yz in T. We may choose ρ so that $m \neq -5$; then B'_{xz} is not of type π, and hence is of type S.

Thus in any case one of the B's may be assumed to be a perfect square. With B_{xy} a square, the preceding discussion shows that, without disturbing B_{xy}, we may make also B_{xz} a perfect square.

We now have two of the B's perfect squares. These will be denoted by B_{xy}, B_{xz}, so that we may apply the transformation given above and delete x^5y, etc. Changing if necessary the sign of y or that of z, we may set

$$(27)\quad B_{xy}=(x^3+bxy^2+y^3)^2,\quad B_{xz}=(x^3+axz^2+z^3)^2,\quad B_{yz}=y^6+c_1y^5z+\cdots+c_5yz^5+z^6.$$

The remaining terms of T are of the form (25). Set $x = \lambda y$. Then

$$(28)\quad T=(\lambda^3+b\lambda+1)^2y^6+\cdots+(a^2\lambda^2+C\lambda+c_4)y^2z^4+\alpha yz^5+z^6,$$

where $\alpha = 2a\lambda + c_5$. To remove the term yz^5, set $y = Y$, $z = Z - 2\alpha Y$. Then

$$(29)\qquad T= Z^6 + rZ^4Y^2 + \rho Z^3Y^3 + sZ^2Y^4 + \sigma ZY^5 + tY^6,$$

where

$$r = 3a^2\lambda^2 + 2ac_5\lambda + C\lambda + c_4 + 6c_5^2, \qquad s = 5a^4\lambda^4 + \cdots.$$

But (end of §4) (29) is a product π of three quadratic forms if, and only if,

$$(30)\qquad s \equiv 2r^2, \qquad t \equiv -3r^3, \qquad \rho \equiv 0, \qquad \sigma \equiv 0 \pmod{11},$$

and is a perfect square if, and only if,

$$(31)\qquad s \equiv 3r^2, \qquad \sigma \equiv 6r\rho, \qquad t \equiv 3\rho^2 \pmod{11}.$$

For each λ either (30) or (31) must hold. In particular

$$(32)\qquad (s - 2r^2)(s - 3r^2) \equiv 0 \qquad \text{(for every } \lambda\text{)}.$$

Each factor is of degree four in λ. In $s - 2r^2$ the coefficient of λ^4 is $9a^4$. Now $a \neq 0$. Hence $s - 3r^2 \equiv 0$, for every λ. But r vanishes for at most two values of λ. Hence (30_1) holds for at most two values of λ. Hence the set (31) must hold for at least nine values of λ, and hence, in view of the degree in λ, for every value of λ. Hence (29), and therefore also (28), must be formally a square for every λ. This property was seen to require that the ternary sextic be a perfect square.

I have not examined the cases $3 < p^n < 11$. But for $p^n = 3$, the general definite ternary sextic must be congruent to unity (modulo 3) for every set of

integers x, y, z, not all congruent to zero, and is readily seen to have the form:

$$
\begin{aligned}
&x^6 + ax^5y + bx^5z + cx^4y^2 + dx^4yz + ex^4z^2 + fx^3y^3 + gx^3y^2z + hx^3yz \\
&+ jx^3z^3 - (c+1)x^2y^4 + mx^2y^3z + x^2y^2z^2 - (d+m)x^2yz^3 - (e+1)x^2z^4 \\
&- (a+f)xy^5 + txy^4z + vxy^3z^2 - (g+t)xy^2z^3 - (h+v)xyz^4 - (b+j)xz^5 \\
&+ y^6 + Dy^5z + Ey^4z^2 + Fy^3z^3 - (E+1)y^2z^4 - (D+F)yz^5 + z^6,
\end{aligned} \tag{33}
$$

containing 15 independent parameters. It is in general not a perfect square; the terms free of z may give any one of the 27 forms mentioned in § 4. A more symmetrical formula results from the substitution $E = \epsilon + 1, \cdots$.

§ 6. *Definite sextic forms in m variables, $m > 3$.*

Consider a definite sextic form in x, y, z, w in the $GF[p^n]$, $p^n \geqq 11$, $p > 3$. We may take the coefficient of x^6 to be unity and remove the terms x^5y, x^5z, x^5w, y^5z, y^5w, z^5w. By § 5, the terms free of w, z, y or x are, respectively,

$$
\begin{gathered}
(x^3 + axy^2 + bxz^2 + cy^3 + dyz^2 + ez^3 + hxyz)^2, \\
(x^3 + axy^2 + Bxw^2 + cy^3 + Dyw^2 + Ew^3 + Hxyw)^2, \\
(x^3 + bxz^2 + Bxw^2 + ez^3 + fzw^2 + Ew^3 + jxzw)^2, \\
(cy^3 + dyz^2 + Dyw^2 + ez^3 + fzw^2 + Ew^3 + Jyzw)^2.
\end{gathered}
$$

The remaining terms of the sextic S_4 are

$$2xyzw(\alpha x^2 + \beta y^2 + \gamma z^2 + \delta w^2 + lxy + qxz + rxw + syz + tyw + kzw).$$

The sextic S_3 obtained from S_4 by setting $x = \rho y$ must be the square of a ternary cubic T in y, z, w. The terms of S_3 involving only z and w must be the same as in S_4. From the terms $y^6, y^5z, y^5w, yz^5, yz^4w, yw^5$ of S_3 we determine at once the first six terms of T:

$$
\begin{aligned}
T = \pm(\rho^3 + a\rho + c)y^3 \pm h\rho y^2z \pm H\rho y^2w + (b\rho + d)yz^2 \\
+ (j\rho + J)yzw + (B\rho + D)yw^2 + ez^3 + fzw^2 + Ew^3.
\end{aligned}
$$

The identity $S_3 = T^2$ requires that the upper signs hold (in view of the terms in y^3w^3 or y^3z^3) and that

$$
\begin{gathered}
\alpha = J, \quad \beta = cj + aJ, \quad \gamma = bJ + dj + eH, \quad \delta = BJ + jD + hE + fH, \\
l = aj + hH, \quad q = hj + bH, \quad r = hB + jH, \quad s = hJ + dH, \\
t = af + hD + HJ, \quad k = jJ + dB + bD + hf.
\end{gathered}
$$

Hence the initial quaternary sextic S_4 is the square of

$$x^3 + axy^2 + bxz^2 + hxyz + Bxw^2 + Hxyw + jxzw$$
$$+ cy^3 + dyz^2 + Dyw^2 + ez^3 + fzw^2 + Ew^3 + Jyzw,$$

composed of the distinct terms appearing in the above four functions squared.

But every quaternary cubic form in the $GF[p^n]$ vanishes* for values, not all zero, of the four variables in the field. Hence a quaternary sextic in the $GF[p^n]$, $p^n \geqq 11$, cannot be definite. The second part of Theorem IV is therefore proved.

§ 7. *Derivation of definite forms from those of lower degrees.*

If we have a definite binary form B in the $GF[p^n]$, $p > 2$, such that B is the product QF of a quadratic form Q and a form F of degree f, we may derive from B a definite binary form G of degree $2f$. The method is that employed in deriving the form preceding (4) from (3). We assume the variables have been so transformed that Q has the normal form $x^2 - \nu y^2$. In F we replace $2x$ by $t + \nu y^2/t$ and multiply the resulting function by t^f. We obtain a homogeneous function G of t and y of degree $2f$. By the proof in § 2, G is definite when B is definite.

For example let $p^n = 11$, $\nu = -1$. From the definite sextic (23) we deduce the octic $G = A_+ A_-$, where the

$$A_\pm = t^4 + 5t^2y^2 + y^4 \pm 4ty(t^2 - y^2)$$

are irreducible modulo 11. Then, writing x for t, we get

$$G = x^8 + 5x^6y^2 + 4x^4y^4 + 5x^2y^6 + y^8. \tag{34}$$

A definite octic containing only even powers may be reduced to

$$x^8 + bx^6y^2 + dx^4y^4 + fx^2y^6 + y^8. \tag{35}$$

I have determined the definite forms (35) having $b = 0, 1$, or 2. Omitting those which are perfect squares, I get the products $B_+ B_-$, where

$$B_\pm = x^4 - 5x^2y^2 \pm 4xy^3 - y^4, \qquad x^4 \pm 4x^3y + 3x^2y^2 \mp 4xy^3 + y^4,$$
$$x^4 \pm 4x^3y - 2x^2y^2 \pm xy^3 - y^4,$$

each irreducible modulo 11, and

$$x^8 + 2x^6y^2 - x^4y^4 + 2x^2y^6 + y^6 = (x^2 - 2y^2)(x^2 - 6y^2)(x^2 + 5xy + y^2)(x^2 - 5xy + y^2).$$

From the latter we obtain by the above method, setting $Q = x^2 - 2y^2$, the following definite form modulo 11:

$$(x^4 + 2x^2y^2 + 4y^4)(x^4 - x^3y - 3x^2y^2 - 2xy^3 + 4y^4)(x^4 + x^3y - 3x^2y^2 + 2xy^3 + 4y^4). \tag{36}$$

*The proof will be given in a paper to appear in the Bulletin of the American Mathematical Society. It is based on an earlier paper, ibid., vol. 14 (1908), pp. 160–169.

§ 8. *Some arithmetical properties of binary forms.*

Let m be a fixed integer and let F denote the $GF[p^n]$. Consider a polynomial $f(z)$ of degree $\leqq p^n - 1$, with coefficients in F, and having the property that, for each element z of F, $f(z)$ equals an mth power in F:

$$f(z) = v_z = t_z^m \qquad \text{(for each } z \text{ in } F\text{)}. \tag{37}$$

Let δ be the greatest common divisor of m and $p^n - 1$. Then for $v_z \neq 0$, there are δ elements t_z of F which give the same value v_z for t_z^m. For each z, we select arbitrarily one of these δ values of t_z and build by* an interpolation formula a polynomial $\phi(z)$, of degree $\leqq p^n - 1$, such that $\phi(z) = t_z$ for each particular element z in F. Then, by (37), $\phi^m(z) = f(z)$ for each z in F.

THEOREM. *If a polynomial $f(z)$, with coefficients in a finite field F, represents exclusively mth powers in F, then $f(z)$ is (arithmetically in F) equal to the mth power of a polynomial $\phi(z)$ with coefficients in F.*

Not all of the values v_z are zero. If k of the values are not zero, so that $p^n - k$ are zero, any one of the k non-vanishing elements t_z may be chosen in δ ways. Hence *there are δ^k polynomials ϕ determined by the given f.* If we construct one ϕ and multiply each t by the same root r of $x^\delta = 1$, we obtain $r\phi$. For example, if $m = 2$, $p = 3$, $f = (z+1)^2$, then $\phi \equiv \pm(z+1)$ or $\pm(z+1)^2$.

The most important case is that in which $f(z)$ represents exclusively non-vanishing mth powers in the $GF[p^n]$. Then there are δ^{p^n} polynomials $\phi(z)$ and the quotient $q(x)$ of any two ϕ's is such that $[q(x)]^m = 1$ for every x in the field. In particular, for $m = 2$, $p > 2$, there are 2^{p^n} polynomials $q(x)$ whose square equals unity for every x in the $GF[p^n]$. For $p^n = 3$, these are 1, $x^2 + 1$, $x^2 \pm x - 1$, and their negatives. For $p^n = 5$, they are

$$1,\ -2x^4 + 1,\ -x^4 \pm x^2 + 1,\ 2x^4 \pm x^3 - 2x^2 \mp x + 1,\ x^4 \pm x^3 + 2x^2 \mp x + 1,$$

$$-x^4 \pm x^3 \mp 2x + 1,\ -x^4 \pm 2x^3 \mp x + 1,\ 2x^4 \pm 2x^3 + 2x^2 \pm 2x + 1,$$

$$x^4 \pm 2x^3 - 2x^2 \pm 2x + 1,$$

and their negatives. For $p^n = 7$, I have verified that if $q^2 = 1$ for every x, where q is a function of degree < 6, then $q = \pm 1$. At least for $p^n = 3, 5, 7$, it follows that, *in any function (other than ± 1) whose square is unity, the coefficient of x^{p^n-1} is not zero.* We note that, for any p^n, the square of $-2x^{p^n-1} + 1$ is unity for every x in the field.

THE UNIVERSITY OF CHICAGO,
July, 1908.

* Or by undetermined coefficients, noting that $|z^i| \neq 0$, z ranging over F.