INVARIANTS OF BINARY FORMS UNDER MODULAR TRANSFORMATIONS*

BY

LEONARD EUGENE DICKSON

For a non-modular field F and a binary form f with coefficients in F, the problem of the determination of functions of the coefficients and variables of f, invariant under all binary linear transformations in F, is formally identical with the corresponding problem of the ordinary algebraic invariant theory. But for a finite modular field the problem is essentially different; the terms of an invariant need not be of the same degree nor of constant weight; the annihilators are quite complicated, involving higher partial derivatives. Fortunately, the difficulty in the direct computation of the invariants is in marked contrast with the regularity observed in the actual form of the invariants and with the simplicity of the relations between the invariants, common to the algebraic and modular theories, and the additional invariants peculiar to the modular theory.

In the study of the invariants of a given quantic in the Galois field of order p^n, we have a doubly infinite system of problems, corresponding to a single problem in the algebraic theory. Interest naturally centers in a comparative study, rather than in the individual problems. The aim of the present paper is to give in correlation the results of a rather extensive comparative study. Formal proofs of the laws observed are given only in a few instances. It is hoped that proofs of the remaining properties observed will become more practicable when a satisfactory symbolic treatment is constructed.

Since there is evidently only a finite number of linearly independent invariants I of a given binary form of degree m in the $GF[p^n]$, each set of numbers m, n, p uniquely defines a commutative linear associative algebra, whose units are these invariants I.

In the final sections of the paper, application is made to the invariantive reduction of binary quantics to canonical forms.†

* Presented to the Society at the preliminary meeting of the Southwestern Section December 1, 1906. Received for publication December 19, 1906.

† The invariants of k-ary quadratic forms are treated in papers to appear in the Proceedings of the London Mathematical Society and the American Journal of Mathematics.

1. THEOREM. *The binary form* with coefficients in the* $GF[p^n]$,

$$f=\sum_{i=0}^{m} a_i x^{m-i} y^i, \tag{1}$$

has the absolute invariant

$$I=\prod_{i=0}^{m}(a_i^{\mu}-1), \qquad \mu \equiv p^n-1. \tag{2}$$

Here and below we employ the generators (t, λ any marks $\neq 0$)

$$x=x'+ty', \qquad y=y'; \tag{3}$$

$$x=x', \qquad y=\lambda y'; \tag{4}$$

$$x=y', \qquad y=-x'; \tag{5}$$

of the group of all binary linear transformations with coefficients in the $GF[p^n]$. Under (3) f becomes a form f' with the coefficients

$$a_0'=a_0, \quad a_1'=a_1+ma_0, \cdots, \quad a_i'=a_i+\sum_{j=0}^{i-1} C_{m-j,\,i-j}\, t^{i-j} a_j, \ \cdots. \tag{6}$$

Under transformations (4) and (5) we have, respectively,

$$a_i'=\lambda^i a_i \qquad (i=0, 1, \cdots, m), \tag{7}$$

$$a_i'=(-1)^{m-i} a_{m-i} \qquad (i=0, 1, \cdots, m). \tag{8}$$

Under the replacements (7) and (8) the function (2) is unaltered, since $\lambda^{\mu}=1$ for every mark $\lambda \neq 0$. Consider next the replacement (6). The first factor $a_0^{\mu}-1$ is unaltered. Then, since $(a_0^{\mu}-1)a_0=0$,

$$(a_0'^{\mu}-1)(a_1'^{\mu}-1)=(a_0^{\mu}-1)(a_1^{\mu}-1+Aa_0)=(a_0^{\mu}-1)(a_1^{\mu}-1).$$

The proof may be completed by induction from $i-1$ to i. Let

$$P_i=\prod_{j=0}^{i}(a_j^{\mu}-1).$$

Then

$$P_i'=P_{i-1}(a_i'^{\mu}-1)=P_{i-1}(a_i^{\mu}-1+B_0a_0+B_1a_1+\cdots+B_{i-1}a_{i-1})$$
$$=P_{i-1}(a_i^{\mu}-1)=P_i.$$

2. The absolute invariant (2) has a simple interpretation. According as $a \neq 0$ or $a=0$, we have $a^{\mu}-1=0$ or -1. *Hence the form f vanishes identically if and only if $I \neq 0$.*

* We do not at present introduce binomial coefficients C_{mi}, some of which are divisible by p for certain values of m and p.

Frequently a property expressible by a single invariant in the modular theory requires in the algebraic theory the use of a covariant or else an invariantive simultaneous system of equations. A less obvious instance relates to the minors of the determinant of a k-ary quadratic form.

3. THEOREM. *For m a power of p, the binary form* (1) *of degree m with coefficients in the $GF[p^n]$ has the absolute invariant*

$$P = \prod_{i=1}^{m-1} (a_i^{\mu} - 1), \qquad \mu \equiv p^n - 1. \tag{9}$$

The proof is similar to that in § 1. We now have

$$C_{mi} \equiv 0 \pmod{p} \qquad (i = 1, \cdots, m-1),$$

so that there is no term a_0 in a_i' $(i = 1, \cdots, m-1)$ in formulæ (6).

4. An obvious invariant of f is the eliminant E of

$$f = 0, \qquad x^{p^n} = x, \qquad y^{p^n} = y.$$

For example, let $m = 3$, $p^n = 3$. Multiply f by xy, x^2y^2 and x^2 in turn and reduce by means of $x^3 = x$, $y^3 = y$. The corresponding equations

$$a_0x + a_1x^2y + a_2xy^2 + a_3y = 0, \qquad (a_0 + a_2)x^2y + (a_1 + a_3)xy^2 = 0,$$

$$(a_1 + a_3)x^2y + (a_0 + a_2)xy^2 = 0, \qquad a_0x + (a_1 + a_3)x^2y + a_2xy^2 = 0,$$

have the eliminant, identical with (17) of § 9,

$$a_0a_3\{(a_1 + a_3)^2 - (a_0 + a_2)^2\}.$$

Evidently, $E = a_m R$, where R is the resultant of

$$f_1 \equiv a_0 + a_1y + \cdots + a_my^m = 0, \qquad y^{p^n} = y.$$

By the elimination of $1, y, y^2, \cdots, y^{p^n-1}$ by SYLVESTER'S dialytic method, we obtain for R a determinant of order p^n in which each element in the main diagonal is a_0. The numerical factor is thereby determined so that $R = a_0^{p^n} + \cdots$.

Except in the simplest cases, it is more convenient to have E expressed as the product of the linear functions obtained from f by giving to x, y the $p^n + 1$ sets of values $0, 1$; and $1, \rho$, where ρ ranges over the marks of the field:

$$E = a_m \Pi(a_0 + a_1\rho + \cdots + a_m\rho^m), \quad \rho \text{ ranging over the } GF[p^n].$$

For the case of quadratic forms $(m = 2)$ in the $GF[p^n]$, simple expressions may be given to E. For $p = 2$, $E = a_1^2\chi$, where χ is the absolute

invariant given by (20). For $p > 2$,

$$E = \tfrac{1}{2}(\Delta^{\frac{1}{2}(p^n+1)} - \Delta), \qquad \Delta = a_1^2 - 4a_0a_2.$$

Note, in verification of this result, that $f_1 = 0$ has a root in the field if, and only if, the discriminant Δ is zero or a square, so that $E = 0$ if, and only if,

$$\Delta(\Delta^{\frac{1}{2}(p^n-1)} - 1) = 0.$$

For cubic forms, consider first the case $p^n = 3^2$.

We define the $GF[9]$ by the primitive irreducible congruence $i^2 \equiv i + 1 \pmod 3$; then the marks $\neq 0$ are 1, i, i^2, i^3, and their negatives. Hence $E = a_0a_3\pi$, where

$$\pi = \Pi\{(a_0 + a_2\rho^2)^2 - (a_1\rho + a_3\rho^3)^2\} \qquad (\rho = 1, i, i^2, i^3)$$

$$= \Pi(a_0^2 - \alpha\rho^2 + \beta\rho^4 - a_3^2\rho^6) \quad (\alpha = a_1^2 + a_0a_2,\ \beta = a_2^2 + a_1a_3).$$

Forming the product of the factors given by $\rho = 1$, i^2, and those given by $\rho = i$, i^3, we get, since $i^4 = -1$,

$$\pi = \{(a_0^2 + \beta)^2 - (a_3^2 + \alpha)^2\}\{(a_0^2 - \beta)^2 + (a_3^2 - \alpha)^2\}$$

$$= (a_0^4 + a_3^2\alpha + \beta^2)^2 - (a_3^4 + a_0^2\beta + \alpha^2)^2.$$

Since $a_0a_3(a_0^8 - a_3^8) = 0$ in the field, are readily obtain the result:

$$E = a_0^3a_1a_3^6 - a_0a_1^4a_3^5 + (a_0^2a_1a_2^3 - a_0a_1^3a_2^2)a_3^4 - (a_0^2a_2^5 + a_0a_1^2a_2^4 + a_0^6a_2)a_3^3$$
$$+ (a_0a_1a_2^6 - a_0^4a_1^3a_2 + a_0^3a_1^5)a_3^2 + (a_0a_2^8 + a_0^5a_2^4 + a_0^4a_1^2a_2^3 + a_0^3a_1^4a_2^2 - a_0^2a_1^6a_2 - a_0a_1^8)a_3. \tag{10}$$

For $p \neq 3$, we shall employ the cubic form (40) with binomial coefficients. Then π is the product of the functions $a_0 + 3a_1\rho + 3a_2\rho^2 + a_3\rho^3$, ρ ranging over the marks $\neq 0$. For $p^n = 2$, 2^2, 2^3, the expressions for π and E are given in §23. For $p^n = 5$,

$$\pi = (a_0^2 - a_2^2 - a_1a_3)^2 - (a_1^2 - a_3^2 + a_0a_2)^2$$

$$= a_0^4 - a_1^4 + a_2^4 - a_3^4 + 2a_0^2a_2^2 - 2a_1^2a_3^2 + 2a_0a_2a_3^2 - 2a_0^2a_1a_3 + 2a_1a_2^2a_3 - 2a_0a_1^2a_2,$$

so that E is given by (90). For $p^n = 7$, it is convenient to set

$$\alpha = a_0^2 - a_3^2, \qquad \beta = a_1a_3 + 2a_2^2, \qquad \gamma = -a_0a_2 - 2a_1^2.$$

Forming the product of the factors by twos, viz., those with $\rho = \pm 1$, those with $\rho = \pm 2$, and those with $\rho = \pm 3$, we obtain the interesting result:

$$\pi \equiv (\alpha + \beta + \gamma)(\alpha + 2\beta + 4\gamma)(\alpha + 4\beta + 2\gamma) \equiv \alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma \pmod 7.$$

The resulting expression for E is given by (93).

5. THEOREM. *The weights* $\sigma = e_1 + 2e_2 + \cdots + me_m$ *of the various terms*

$$a_0^{e_0} a_1^{e_1} \cdots a_m^{e_m}$$

of an invariant ϕ *differ by multiples of* $\mu = p^n - 1$.

Here and in § 6, let ϕ become $\phi' = D^d \phi$ under every binary transformation of determinant D. Consider the special transformation (4) in which λ is a primitive root of the $GF[p^n]$. In view of (7), the above general term of ϕ is multiplied by λ^σ. Hence

$$\lambda^\sigma = \lambda^d, \qquad \sigma \equiv d \pmod{\mu}.$$

6. THEOREM. *The degrees* ρ *of the various terms of an invariant differ by multiples of* μ/δ, *where* δ *is the greatest common divisor of* m *and* $\mu = p^n - 1$. *Further,* $m\rho - 2\sigma$ *is a multiple of* μ.

For the transformation $x = \lambda x'$, $y = \lambda y'$, we have $a_i' = \lambda^m a_i$. Hence a term of degree ρ of ϕ is multiplied by $\lambda^{m\rho}$, so that $m\rho \equiv 2d \pmod{\mu}$.

7. The differential operators which annihilate an invariant are here more complicated than in the algebraic theory. This is due primarily to the fact that, in a series of powers of an arbitrary mark t of the $GF[p^n]$, certain terms now combine, viz., t^i, $t^{i+\mu}$, $t^{i+2\mu}$, $\cdots$, where $\mu = p^n - 1$. Since $a^{p^n} = a$ for every mark a, we may assume that the exponent of each a_i in an invariant does not exceed μ. Then, for the case $n = 1$, we can employ TAYLOR's theorem for the expansion of a polynomial of degree $\mu = p - 1$,

$$\psi(a + t) = \psi(a) + t\psi'(a) + \cdots + \frac{1}{i!} t^i \psi^{(i)}(a) + \cdots + \frac{1}{\mu!} t^\mu \psi^{(\mu)}(a),$$

since the denominator $i!$ is prime to the modulus p. The case $n > 1$ apparently (cf. § 10) offers a theoretical difficulty; it actually presents a difficulty from another source (§ 12). We therefore begin with examples illustrating the simpler case $n = 1$.

8. For the first illustrative example, consider the form

$$a_0 x^2 + a_1 xy + a_2 y^2, \tag{11}$$

in which the coefficients are integers taken modulo 3. Under the transformation (3), a_1 and a_2 receive, in view of (6), the respective increments

$$\alpha_1 = 2ta_0, \qquad \alpha_2 = ta_1 + t^2 a_0.$$

Let ϕ be a polynomial in a_0, a_1, a_2, with exponents $\leqq 2$. By TAYLOR's theorem,

$$\phi' - \phi = \alpha_1\phi_{a_1} + \alpha_2\phi_{a_2} + \tfrac{1}{2}\alpha_1^2\phi_{a_1^2} + \alpha_1\alpha_2\phi_{a_1a_2} + \tfrac{1}{2}\alpha_2^2\phi_{a_2a_2}$$
$$+ \tfrac{1}{2}\alpha_1^2\alpha_2\phi_{a_1^2a_2} + \tfrac{1}{2}\alpha_1\alpha_2^2\phi_{a_1a_2^2} + \tfrac{1}{4}\alpha_1^2\alpha_2^2\phi_{a_1^2a_2^2},$$

where $\phi_{a_1^2a_2}$ denotes $\partial^3\phi/\partial a_1^2\partial a_2$, etc. Then $\phi' - \phi = t\delta\phi + t^2\delta_1\phi$, where

$$\delta\phi \equiv 2a_0\phi_{a_1} + a_1\phi_{a_2} + 2a_0^2\phi_{a_1a_2} + a_0a_1\phi_{a_2^2} + 2a_0^2a_1\phi_{a_1^2a_2} + (a_0 + a_0a_1^2)\phi_{a_1a_2^2} + 2a_0a_1\phi_{a_1^2a_2^2},$$

$$\delta_1\phi \equiv a_0\phi_{a_2} + 2a_0^2\phi_{a_1^2} + 2a_0a_1\phi_{a_1a_2} - (a_0^2 + a_1^2)\phi_{a_2^2} + 2a_0\phi_{a_1^2a_2} + 2a_0^2a_1\phi_{a_1a_2^2}$$
$$+ (a_0^2 + a_0^2a_1^2)\phi_{a_1^2a_2^2}.$$

A necessary condition for $\phi' = \phi$ is $\delta\phi = 0$. This condition is also sufficient. Indeed, if $[\delta\phi]$ denotes $\delta\phi$ in reduced form, i. e., with every exponent $\leqq 2$ (in virtue of $a^3 \equiv a$), then $\delta[\delta\phi] \equiv \delta_1\phi$. To verify the latter, note that if ψ is a reduced function of a, viz., $\psi = ra^2 + sa + t$, then $[a\psi] \equiv ra + sa^2 + ta$, and $[a\psi]_a \equiv a\psi_a + \psi - \psi_{aa} \pmod 3$. Again, if $\chi = sa + t$, $[a^2\chi] \equiv sa + ta^2$, and

$$[a^2\chi]_a \equiv a^2\chi_a + (a^2)_a\chi + \chi_a \pmod 3.$$

Proceeding to the computation of the invariants, we may set

$$\phi = \sum_{i,j}^{0,1,2} A_{ij}a_1^ia_2^j \qquad (A_{ij} \text{ quadratic functions of } a_0).$$

Employing the annihilator δ and giving to $\delta\phi$ its reduced form $[\delta\phi]$ with exponents $\leqq 2$, we require that $[\delta\phi] \equiv 0$, identically in a_1, a_2. Among the resulting conditions occur

$$A_{11} \equiv 0, \qquad A_{12} \equiv 0, \qquad A_{10}a_0 \equiv 0, \qquad A_{22}a_0 \equiv 0 \pmod 3.$$

In view of these, the remaining conditions reduce to

$$A_{21}a_0 - A_{22} - A_{02} \equiv 0, \qquad A_{20}a_0 + A_{21} + A_{01} - A_{21}a_0^2 - A_{02}a_0 \equiv 0.$$

From $A_{22}a_0 \equiv 0$ we get $A_{22} \equiv r(a_0^2 - 1)$, where r is a constant. The term $ra_0^2a_1^2a_2^2$ is unaltered by transformation (4), so that $r = 0$ unless ϕ is an absolute invariant. In the latter case we replace ϕ by $\phi - rI$, where I is the invariant given by (2). In either case, it remains to consider ϕ with $A_{22} \equiv 0$. Under transformation (5),

$$(8') \qquad a_0' = a_2, \qquad a_1' = -a_1, \qquad a_2' = a_0.$$

This replacement must leave ϕ unaltered. But by $A_{22} \equiv 0$, $a_1^2a_2^2$ is a factor of no term of ϕ. Hence $a_1^2a_0^2$ is a factor of no term of ϕ. We may therefore set

$$A_{21} = \alpha + \beta a_0, \qquad A_{20} = \lambda + \mu a_0 \qquad (\alpha, \beta, \lambda, \mu \text{ constants}).$$

Similarly, by $A_{12} \equiv 0$, $a_1 a_0^2$ is a factor of no term, so that $A_{10} \equiv 0$. The above long conditions now give

$$A_{02} = \alpha a_0 + \beta a_0^2, \qquad A_{01} = -\alpha + (\beta - \lambda) a_0 - (\alpha + \mu) a_0^2.$$

The conditions that ϕ shall be unaltered by (8′) are $\mu = \alpha$, $A_{00} = k - \alpha a_0$, k a constant. Hence

$$\phi = \beta a_0^2 a_2^2 + (\beta - \lambda) a_0 a_2 + \lambda a_1^2 + \beta a_0 a_2 a_1^2 + \alpha Q + k,$$

where

$$Q = a_0 a_2^2 + a_0^2 a_2 + a_1^2 a_2 + a_1^2 a_0 - a_2 - a_0. \tag{12}$$

The coefficient of λ is the discriminant $\Delta = a_1^2 - a_0 a_2$, that of β is congruent to $\Delta^2 - \Delta$. *As the linearly independent invariants of the quadratic form* (11) *modulo* 3, *we may take* I, Q, Δ, Δ^2. *Now* $I \equiv Q^2 + \Delta^2 - 1$. *As the independent invariants we may take* Q *and* Δ.

9. Consider the binary cubic $(1)_{m=3}$ with integral coefficients modulo 3. The discriminant Δ and (9) give the absolute invariants

$$\Delta = a_1^2 a_2^2 - a_0 a_2 - a_1 a_3, \qquad P = (a_1^2 - 1)(a_2^2 - 1). \tag{13}$$

Hence there is an absolute invariant of the second degree:

$$K \equiv \Delta - P + 1 = a_1^2 + a_2^2 - a_0 a_2 - a_1 a_3. \tag{14}$$

In view of (6), a_0 and a_1 are unaltered by transformation (3), while a_2 and a_3 have the respective increments $2ta_1$ and $t(a_0 + a_2) + t^2 a_1$. The coefficient of t in $\phi' - \phi$ gives the annihilator

$$\begin{aligned} &2a_1 \phi_{a_2} + (a_0 + a_2)\phi_{a_3} - a_1^2 \phi_{a_2 a_3} + a_1 (a_0 + a_2)\phi_{a_3^2} - a_1^2 (a_0 + a_2)\phi_{a_2^2 a_3} \\ &\quad + \{a_1 + a_1 (a_0 + a_2)^2\}\phi_{a_2 a_3^2} - a_1 (a_0 + a_2)\phi_{a_2^2 a_3^2}. \end{aligned} \tag{15}$$

By §§ 5, 6, the terms of an invariant ϕ are all of even degrees, while all are of even or all of odd weights. Further, by (5) and (8), ϕ must be unaltered by the substitution

$$a_0' = -a_3, \qquad a_3' = a_0, \qquad a_1' = a_2, \qquad a_2' = -a_1. \tag{16}$$

Let first the weights be even, so that by § 5, $e_1 \equiv e_3 \pmod 2$ in every term of ϕ. Then, in view of (16), ϕ must have the form

$$\begin{aligned} &b(a_0^2 + a_3^2) + c(a_1^2 + a_2^2) + d(a_0 a_2 + a_1 a_3) + e a_0^2 a_3^2 + f a_1^2 a_2^2 + g(a_0^2 a_1^2 + a_2^2 a_3^2) \\ &\quad + h(a_0^2 a_2^2 + a_1^2 a_3^2) + j(a_0^2 a_1 a_3 + a_3^2 a_0 a_2) + k(a_1^2 a_0 a_2 + a_2^2 a_1 a_3) + l a_0 a_1 a_2 a_3 \\ &\quad + m(a_0^2 a_1^2 a_2^2 + a_1^2 a_2^2 a_3^2) + n(a_0^2 a_1^2 a_3^2 + a_0^2 a_2^2 a_3^2) + q(a_0^2 a_2^2 a_1 a_3 + a_1^2 a_3^2 a_0 a_2) \\ &\quad + r a_0^2 a_1^2 a_2^2 a_3^2. \end{aligned}$$

By subtracting from ϕ suitable multiples of P, K, Δ^2, and I, given by (2), we may set $c=d=k=r=0$. Then (15) vanishes if and only if

$$n=f=0, \qquad g=q=e=h=-m, \qquad b=j=l=m.$$

The coefficient of m is the absolute invariant

$$T=a_0^2+a_3^2-a_0^2a_3^2-a_0^2a_1^2-a_2^2a_3^2-a_0^2a_2^2-a_1^2a_3^2+a_0^2a_1a_3+a_0a_2a_3^2 \\ +a_0a_1a_2a_3+a_0^2a_1^2a_2^2+a_1^2a_2^2a_3^2-a_0^2a_1a_2^2a_3-a_0a_1^2a_2a_3^2.$$

Finally, when the weights are odd, the possible terms are

$$B(a_0a_1-a_2a_3)+G(a_0^2a_1a_2-a_3^2a_1a_2)+H(a_0^2a_2a_3-a_3^2a_0a_1) \\ +J(a_1^2a_0a_3-a_2^2a_0a_3)+K(a_1^2a_2a_3-a_2^2a_0a_1)+L(a_0^2a_1^2a_2a_3-a_3^2a_2^2a_0a_1).$$

The conditions that (15) shall vanish are $B=G=K=L=0$, $J=H$. Hence

$$E=a_1^2a_0a_3-a_2^2a_0a_3+a_0^2a_2a_3-a_3^2a_0a_1 \tag{17}$$

is the only invariant of odd weights. By §§ 4, 27, the cubic form is irreducible modulo 3 if, and only if, $E\neq 0$.

The relations between T and the remaining invariants are

$$IT=0, \qquad PT=P-I, \qquad \Delta T=I-P+T, \qquad ET=E, \qquad T^2=T.$$

We obtain the simpler relations * (19) by introducing $W\equiv I-P+T$, viz.,

$$W=a_3^2(a_0^2a_1^2a_2^2-a_0^2a_2^2-a_0a_1^2a_2+a_0a_2-a_0^2a_1^2)+a_3(-a_0^2a_1a_2^2+a_0a_1a_2+a_0^2a_1). \tag{18}$$

THEOREM. *As a complete set of linearly independent invariants of the cubic form modulo* 3, *we may take* I, P, Δ, Δ^2, E, W. *The product of any two invariants can be reduced to a linear function of these six by means of*

$$\begin{cases} I^2=I, \quad IP=I, \quad I\Delta=IE=IW=0, \quad P^2=P, \quad P\Delta=PE=PW=0, \\ \Delta^3=\Delta, \quad \Delta E=E, \quad \Delta W=W, \quad E^2=W, \quad EW=E, \quad W^2=W. \end{cases} \tag{19}$$

10. The next illustrative examples relate to the invariants of a quantic in the $GF[p^n]$, $n>1$. We require the expansion of $\psi(a+t)$ in powers of t, where $\psi(a)$ is a polynomial of degree at most $\mu=p^n-1$. This can be done by TAYLOR's theorem, the coefficient of t^i being the quotient obtained algebraically by dividing $\psi^{(i)}(a)$, all of whose coefficients are exact multiples of $i!$, by the number $i!$. Similar remarks apply to TAYLOR's theorem for two or more variables.

* Conforming with the relations (§ 21) between the invariants of the cubic form in the $GF[9]$. Note that $I-P+T$ and $-\Delta-\Delta^2$ are the only invariants W satisfying the relations (19) involving W. Hence there is a single invariant W which can replace T.

11. Consider the quadratic form (11) with coefficients in the $GF[2^n]$. Under the transformation (3), a_0 and a_1 are unaltered while the increment to a_2 is $ta_1 + t^2 a_0$. Let ϕ be a polynomial in a_0, a_1, a_2, with exponents $\leqq 2^n - 1$.

Let first $n = 2$. Then the coefficient of t in $\phi' - \phi$ equals

$$a_1 \phi_{a_2} + a_0^2 [\tfrac{1}{2} \phi_{a_2^2}] + a_0 a_1^2 [\tfrac{1}{6} \phi_{a_2^3}],$$

where the indicated divisions of the derivatives by 2 and 6 are to be performed algebraically and the quotients only are interpreted in the $GF[4]$. If we set

$$\phi = \sum_{i=0}^{3} B_i a_2^i \qquad (B\text{'s functions of } a_0, a_1),$$

the above expression for the coefficient of t becomes, in the $GF[4]$,

$$a_1(B_1 + B_3 a_2^2) + a_0^2(B_2 + B_3 a_2) + a_0 a_1^2 B_3.$$

This must vanish identically in a_2. From $a_1 B_3 = a_0 B_3 = 0$ we get

$$B_3 = r(a_0^3 - 1)(a_1^3 - 1) \qquad (r = \text{constant}).$$

The remaining condition * becomes $a_1 B_1 + a_0^2 B_2 = 0$. Replacing ϕ by $\phi - rI$, where I is the absolute invariant (2), we may set $B_3 = 0$. By (8), ϕ must be symmetrical in a_0 and a_2. Hence no term of ϕ contains the factor a_2^3 or the factor a_0^3. By §§ 5, 6, the degrees ρ (and likewise the weights σ) of the various terms of ϕ differ by multiples of 3, and $\rho \equiv \sigma \pmod 3$.

Let first $\rho \equiv \sigma \equiv 0$. Then ϕ involves only the terms a_1^3, $a_0 a_1 a_2$, $a_0^2 a_1^2 a_2^2$, so that

$$B_0 = l a_1^3, \qquad B_1 = m a_0 a_1, \qquad B_2 = k a_0^2 a_1^2.$$

Then $m = k$ by $a_1 B_1 + a_0^2 B_2 = 0$. The linearly independent invariants † are

$$I, \qquad a_1^3, \qquad J = a_0 a_1 a_2 + a_0^2 a_1^2 a_2^2.$$

For $\rho \equiv \sigma \equiv 1$, ϕ involves only the terms a_1, $a_0 a_1^2 a_2$, $a_0^2 a_2^2$, $a_0^2 a_1^3 a_2^2$, so that

$$B_0 = b a_1, \qquad B_1 = c a_0 a_1^2, \qquad B_2 = d a_0^2 + e a_0^2 a_1^3.$$

By $a_1 B_1 + a_0^2 B_2 = 0$, we get $d = 0$, $e = c$. The invariants † are a_1 and $a_1 J$.

The case $\rho \equiv \sigma \equiv 2$ may be reduced to the preceding by squaring, an operation here reversible. Hence the invariants are a_1^2 and $a_1^2 J$.

---

* The corresponding conditions from the coefficient of t^2 are $a_1 B_3 = a_0 B_3 = 0$, $a_0 B_1 + a_1^2 B_2 = 0$. Thus the vanishing of the coefficient of t does not imply the vanishing of that of t^2 (but does that of t^3, viz., $a_0^3 B_3 + a_1^3 B_3$). In this respect the case of invariants in the $GF[p^n]$, $n > 1$, appears to be in contrast to the case $n = 1$.

† The remaining conditions from t^2 (preceding foot-note) are satisfied.

For general n, we can prove (cf. §§ 4, 26) the following

THEOREM. *The independent invariants of the quadratic form* (11) *in the* $GF[2^n]$ *may be taken to be* a_1 (*which is multiplied by the determinant of the transformation*), I *and the absolute invariant*

$$(20) \qquad \chi(a_0 a_2 a_1^{2^n-3}), \qquad \textit{where} \qquad \chi(c) \equiv c + c^2 + c^4 + \cdots + c^{2^{n-1}},$$

the last invariant being replaced by $a_0 a_2 a_1$ *in the case* $n = 1$.

12. The illustrative examples employed thus far were chosen on account of their comparative simplicity. As the order of the $GF[p^n]$ increases, the complexity of the computation increases very rapidly. Certain remarks will be found to be very useful. While, for $n > 1$, certain divisions are called for in the definition of an annihilator δ (see §§ 10, 11), the actual performance of the divisions can be dispensed with in the computation of $\delta\phi$. For example, in the $GF[3^2]$ the result of operating on a term $a_0^e a_1^i a_2^j$ by $1/3!\ 1/2!\ \partial^5/\partial a_1^3 \partial a_2^2$ is zero unless $i \geqq 3, j \geqq 2$, while in the latter case the result is $C_{i3} C_{j2} a_0^e a_1^{i-3} a_2^{j-2}$. It thus suffices to have a table * of the residues modulo 3 of the binomial coefficients C_{rs} $(r, s \leqq 8)$. In view of this remark, the following permanent notations will be used for the terms of $\delta\phi$, the notations not exhibiting the numerical divisors. We shall set

$$(21) \qquad (1^i) = \frac{1}{i!} \frac{\partial^i \phi}{\partial a_1^i}, \qquad (1^i 2^j) = \frac{1}{i!\, j!} \frac{\partial^{i+j} \phi}{\partial a_1^i \partial a_2^j}, \quad \text{etc.}$$

In the algebraic theory ϕ is invariant under the special transformation (3) if, and only if, $\delta\phi = 0$, where $\delta\phi$ denotes the coefficient of t in $\phi' - \phi$. The same theorem appears to hold in the modular theory when $n = 1$. In a few cases (cf. § 8), I have made a direct proof of this statement; in very many cases I have secured indirect verification in showing that the computed functions are actually invariants. But for $n > 1$ such a theorem does not hold (cf. foot-notes to § 11). However, it appears to be true that the vanishing of the coefficients of $t, t^p, t^{p^2}, \cdots, t^{p^{n-1}}$ implies the vanishing of the coefficients of the remaining powers (the last one being $p^n - 1$). The importance of this conjecture as a guide in actual computations is obvious; its effect on the explicit form of the invariant is noted in § 17.

13. Consider the quadratic form (11) in the $GF[3^2]$. Under transformation (3), a_1 and a_2 receive the respective increments $\delta_1 = -ta_0$, $\delta_2 = ta_1 + t^2 a_0$. Expanding the powers $\delta_2^2, \cdots, \delta_2^8$, reducing the coefficients modulo 3 and the exponents by means of $x^9 = x$, we write down by inspection (in view of the

* The residues of multinomial coefficients modulo p, a prime, are obtained rapidly by means of two general theorems given in the writer's dissertation, Annals of Mathematics, ser. 1, vol. 11 (1896-7), pp. 75, 76.

simple form of δ_1) the coefficient (22) of t and the coefficient (23) of t^3 in $\phi' - \phi$, employing the notations (21).

$$
\begin{aligned}
&- a_0(1) + a_1(2) - a_0^8(1^7 2) + a_0^8 a_1(1^8 2) - a_0^7(1^5 2^2) - a_0^7 a_1(1^6 2^2)\\
&- a_0^7 a_1^2(1^7 2^2) - a_0^6(1^3 2^3) + a_0^6 a_1^3(1^6 2^3) - a_0^5(1^2 4) + a_0^5 a_1(1^2 2^4)\\
&+ a_0^5 a_1^3(1^4 2^4) - a_0^5 a_1^4(1^5 2^4) - a_0^4 a_1(2^5) - a_0^4 a_1^2(1^2 5) + a_0^4 a_1^3(1^2 2^5)\\
&+ a_0^4 a_1^4(1^3 2^5) + a_0^4 a_1^5(1^4 2^5) - a_0^4(1^7 2^5) - a_0^4 a_1(1^8 2^5) - a_0^3 a_1^3(2^6)\\
&- a_0^3 a_1^6(1^3 2^6) - a_0^3(1^5 2^6) - a_0^3 a_1^3(1^8 2^6) - a_0^2 a_1^6(1^2 7) + a_0^2 a_1^7(1^2 2^7)\\
&- a_0^2(1^3 2^7) + a_0^2 a_1(1^4 2^7) - a_0^2 a_1^3(1^6 2^7) + a_0^2 a_1^4(1^7 2^7) - a_0 a_1^7(2^8)\\
&- (a_0 + a_0 a_1^8)(1^2 8) - a_0 a_1(1^2 2^8) - a_0 a_1^2(1^3 2^8) - a_0 a_1^3(1^4 2^8)\\
&- a_0 a_1^4(1^5 2^8) - a_0 a_1^5(1^6 2^8) - a_0 a_1^6(1^7 2^8) - a_0 a_1^7(1^8 2^8).
\end{aligned}
\tag{22}
$$

$$
\begin{aligned}
&- a_0^3(1^3) - a_0^2(12) + a_0^2 a_1(1^2 2) - a_0 a_1(2^2) - a_0 a_1^2(1^2 2) - a_0(1^7 2^2)\\
&- a_0 a_1(1^8 2^2) + a_1^3(2^3) - a_0^8(1^5 2^3) + a_0^8 a_1^3(1^8 2^3) - a_0^7(1^3 2^4)\\
&+ a_0^7 a_1(1^4 2^4) + a_0^7 a_1^3(1^6 2^4) - a_0^7 a_1^4(1^7 2^4) - a_0^6(1^2 5) - a_0^6 a_1(1^2 2^5)\\
&- a_0^6 a_1^2(1^3 2^5) + a_0^6 a_1^3(1^4 2^5) + a_0^6 a_1^4(1^5 2^5) + a_0^6 a_1^5(1^6 2^5) - a_0^5 a_1^3(1^2 2^6)\\
&- a_0^5 a_1^6(1^5 2^6) - a_0^5(1^7 2^6) - a_0^4 a_1^3(2^7) + a_0^4 a_1^4(1^2 7) - a_0^4 a_1^6(1^3 2^7)\\
&+ a_0^4 a_1^7(1^4 2^7) - a_0^4(1^5 2^7) + a_0^4 a_1(1^6 2^7) - a_0^4 a_1^3(1^8 2^7) - a_0^3 a_1^5(2^8)\\
&- a_0^3 a_1^6(1^2 8) - a_0^3 a_1^7(1^2 2^8) - (a_0^3 + a_0^3 a_1^8)(1^3 2^8) - a_0^3 a_1(1^4 2^8)\\
&a_0^3 a_1^2(1^5 2^8) - a_0^3 a_1^3(1^6 2^8) - a_0^3 a_1^4(1^7 2^8) - a_0^3 a_1^5(1^8 2^8).
\end{aligned}
\tag{23}
$$

We may set

$$
\phi = \sum_{i,j}^{0,\cdots,8} A_{ij} a_1^i a_2^j \qquad (A\text{'s functions of } a_0). \tag{24}
$$

Since a_2^8 occurs only in the first term of (22) and (23), we get

$$
A_{i8} a_0 = 0 \qquad (i = 1, \cdots, 8).
$$

Employing these to simplify the coefficient of a_2^7 in the first four terms of (22) and that in the first three terms of (23), we get

$$
- a_0 \Sigma i A_{i7} a_1^{i-1} - a_1 \Sigma A_{i8} a_1^i, \qquad - a_0^3 \Sigma C_{i3} A_{i7} a_1^{i-3}.
$$

These must vanish identically in $a_1 = a_1^9$. Hence

$$
A_{i7} a_0 = 0 \ (i = 1, 3, \cdots, 8), \quad A_{i8} = 0 \ (i = 1, \cdots, 7), \quad A_{27} a_0 - A_{08} - A_{88} = 0.
$$

Before examining the further conditions we shall introduce a decided simplification. From $A_{88} a_0 = 0$, $A_{88} = k(a_0^8 - 1)$, k a constant. But the term

$ka_0^8a_1^8a_2^8$ of ϕ is unaltered by transformation (4). Hence k is zero unless ϕ is an absolute invariant. In the latter case, we replace ϕ by $\phi - kI$, where I is the absolute invariant (2). In either case we have $A_{88} = 0$. *Then* $A_{ij}a_0 = 0$ $(i \neq 0)$ *implies* $A_{ij} = 0$. For, then $A_{ij} = c(a_0^8 - 1)$, while $a_0^8a_1^ia_2^j$ is not a term of ϕ. If it were, then would $a_0^ja_1^ia_2^8$ occur in ϕ since ϕ must be unaltered by (5) and hence by (8′) of § 8, whereas $A_{i8} = 0$ $(i = 1, \cdots, 8)$.

We next examine the coefficients of a_2^6 in (22) and (23), then those of a_2^5, etc. At each step we utilize the conditions previously found. In view of the above result and the fact that the binomial coefficients C_{i2} $(i = 3, 4, 6, 7)$, C_{64}, C_{65}, C_{75} are multiples of the modulus 3, the determination of the coefficient of a_2^k may be done readily by inspection. The resulting conditions,* including the earlier ones, are:

$$\begin{aligned}
&A_{i8} = 0\,(i = 1, \cdots, 8),\ A_{i7} = 0(i = 1, 3, \cdots, 8),\ A_{i6} = 0(i = 1, 3, 5, 6, 7, 8),\\
&A_{i5} = 0\,(i = 1, 2, 3, 4, 5, 7, 8),\ A_{i4} = 0\,(i = 1, 3, 4, 5, 7),\\
&A_{i3} = 0\,(i = 1, 3, 5, 7),\ A_{i2} = 0\,(i = 1, 2, 3, 5, 7, 8),\\
&A_{i1} = 0\,(i = 1, 3, 5, 7),\ A_{i0} = 0\,(i = 1, 3, 5, 7);
\end{aligned} \tag{25}$$

$$\begin{aligned}
&A_{08} = A_{27}a_0,\ A_{27} = A_{46}a_0,\ A_{07} = -A_{26}a_0,\ A_{65} = A_{84}a_0,\ A_{27} = A_{84}a_0^3,\\
&A_{05} = A_{24}a_0,\ A_{07} = A_{64}a_0^3,\ A_{64} = -A_{83}a_0,\ A_{24} = A_{43}a_0,\ A_{26} = A_{83}a_0^3,\\
&A_{06} = A_{63}a_0^3,\ A_{46} = A_{84}a_0^2,\ A_{05} = -A_{62}a_0^3,\ A_{24} = -A_{81}a_0^3,\ A_{64} = A_{41}a_0^3,\\
&A_{42} = A_{84}a_0^6,\ A_{62} = A_{81}a_0,\ A_{02} = A_{21}a_0,\ A_{23}a_0 + A_{04} + A_{84} + A_{84}a_0^8 = 0,\\
&A_{61}a_0^3 = A_{23}a_0,\ A_{41} = -A_{83}a_0^6,\ A_{21} = A_{40}a_0 - A_{63}a_0^6,\ A_{61} + A_{80}a_0 + A_{27}a_0^2 = 0,\\
&A_{20}a_0 + A_{01} + A_{81} + A_{81}a_0^8 = 0,\ A_{63} = A_{40}a_0^3 - A_{21}a_0^2,\ A_{43} = -A_{81}a_0^2,\\
&A_{23} + A_{80}a_0^3 + A_{84}a_0^7,\ A_{03} + A_{83} + A_{60}a_0^3 - A_{07}a_0^4 = 0.
\end{aligned} \tag{26}$$

We note that each A_{ij} not in the set (25) has a non-vanishing value in at least one invariant given below.

In the notations of § 5, we have here

$$e_1 + 2e_2 \equiv 2e_0 + e_1 \equiv d \pmod 8. \tag{27}$$

Consider first the absolute invariants, so that $d \equiv 0$. For $e_1 = 8$, $e_2 = 0$ or 4, we have $e_0 = 0$, 4 or 8. The value $e_0 = 8$ is excluded, since (as shown above) $a_0^8a_1^8a_2^{e_2}$ is not a term of ϕ. Hence we may set

$$A_{84} = e + fa_0^4, \qquad A_{80} = l + ma_0^4, \qquad A_{00} = \lambda + \mu a_0^4 + \nu a_0^8.$$

* Those in set (25) and likewise the remaining ones occur approximately in the order of their determination. Obvious simplifications have been made in the latter conditions. Certain conditions have been omitted as being simple consequences of those retained.

By (27) the only further non-vanishing A_{ij} are the following, whose values are derived at once from the non-identical conditions (26):

$$A_{65} = ea_0 + fa_0^5, \quad A_{27} = ea_0^3 + fa_0^7, \quad A_{08} = ea_0^4 + fa_0^8, \quad A_{46} = ea_0^2 + fa_0^6,$$

$$A_{42} = ea_0^6 + fa_0^2, \quad A_{23} = -(f+l)a_0^3 - (e+m)a_0^7, \quad A_{61} = -(f+l)a_0 - (e+m)a_0^5,$$

$$A_{04} = -e + (l-f)a_0^4 + ma_0^8.$$

The necessary and sufficient conditions that the resulting function (24) shall be unaltered by (5) and hence by (8′) are $m = e$, $\mu = -e$, $\nu = 0$. The independent parameters are thus e, f, l. The coefficients of l and f are Δ^4 and $\Delta^8 - \Delta^4$, respectively, where

$$\Delta = a_1^2 - a_0 a_2 \tag{28}$$

is the discriminant of the quadratic form. The coefficient of e is

$$\begin{aligned} Q = {} & a_1^8 a_2^4 + a_0^4 a_1^8 - a_0^4 + a_0 a_1^6 a_2^5 + a_0^3 a_1^2 a_2^7 + a_0^4 a_2^8 \\ & + a_0^2 a_1^4 a_2^6 + a_0^6 a_1^4 a_2^2 + a_0^7 a_1^2 a_2^3 + a_0^5 a_1^6 a_2 - a_2^4 + a_0^8 a_2^4. \end{aligned} \tag{29}$$

By way of check we note here the important relations

$$Q^2 + \Delta^8 - 1 = I, \qquad Q\Delta = 0 \tag{30}$$

Next, there is no invariant with $d \equiv 1 \pmod 8$. Indeed, each of the nine $A_{e_1 e_2}$ for which $e_1 + 2e_2 \equiv 1 \pmod 8$ is zero by (25). There is no invariant with $d \equiv 3$; for, if so, its cube would be an invariant with $d \equiv 1$. Similarly, the cases $d \equiv 7$, $d \equiv 5$ are excluded.

In an invariant with $d \equiv 2 \pmod 8$, the possible non-vanishing A_{ij} are $A_{20}, A_{01}, A_{81}, A_{62}, A_{43}, A_{24}, A_{05}$. Now A_{81} is a linear function of a_0 and a_0^5 by (27). But $a_0^5 a_1^3 a_2$ is not a term of ϕ in view of (8′). Hence $A_{81} = la_0$. Similarly, $A_{20} = r + sa_0^4$. Then the seven non-vanishing conditions (26) give

$$A_{62} = la_0^2, \quad A_{05} = -la_0^5, \quad A_{24} = -la_0^4, \quad A_{43} = -la_0^3, \quad A_{01} = (l-r)a_0 - sa_0^5.$$

The resulting function ϕ must be unaltered by (8′); hence $s = 0$. The coefficients of r and l are Δ and $\Delta^5 - \Delta$, respectively. By cubing, we conclude that the only invariants with $d \equiv 6 \pmod 8$ are the linear functions of Δ^3 and Δ^7.

Finally, for $d \equiv 4$, every A_{ij} vanishes except $A_{40}, A_{21}, A_{02}, A_{63}, A_{06}$, while $A_{40} = c$, $A_{21} = ka_0$. The four non-vanishing conditions (26) give

$$A_{02} = ka_0^2, \qquad A_{63} = (c-k)a_0^3, \qquad A_{06} = (c-k)a_0^6.$$

For $c = k = 1$, $\phi = \Delta^2$; for $c = 1$, $k = 0$, $\phi = \Delta^6$.

THEOREM. *Every invariant of a quadratic form in the $GF[9]$ is a linear function of I, Q, $\Delta^i (i = 1, \cdots, 8)$. As independent invariants we may take Q and Δ.*

14. The results of §§ 8, 13 on the invariants of a quadratic form in the $GF[3^n]$, $n = 1, 2$, may be given a simpler form, better adapted to the extension to the case of general n. We set

$$(31) \quad J = Q + \Delta^2 - 1 \text{ (for } n = 1), \qquad J = Q + \Delta^8 - 1 \text{ (for } n = 2).$$

Then in each case

$$(32) \quad J\Delta = 0, \qquad J^2 - J = I,$$

as follows from (30) and the similar relations for $n = 1$. The importance of the introduction of the invariant J lies in the simplicity of relations (32) and in the factorizations

$$(33) \quad J = (a_0 + 1)(a_2 + 1)(a_1^2 + a_0 a_2 - 1) \qquad (\text{for } n = 1),$$

$$(34) \quad J = (a_0^4+1)(a_2^4+1)(a_1^8+a_0^4a_2^4+a_0a_2a_1^6+a_0^3a_2^3a_1^2+a_0^2a_2^2a_1^4-1) \qquad (\text{for } n = 2).$$

For general n, the corresponding function is

$$(35) \quad J = (a_0^\nu + 1)(a_2^\nu + 1)\left\{ \sum_{i=0}^{\nu} a_0^i a_2^i a_1^{2\nu-2i} - 1 \right\},$$

where $\nu = \frac{1}{2}(3^n - 1)$. The discussion in § 15 will apply here since (28) and (35) are unaltered modulo 3 when a_1 is multiplied by 2.

15. Consider the quadratic form* in the $GF[p^n]$, $p > 2$,

$$(36) \quad a_0 x^2 + 2a_1 xy + a_2 y^2.$$

We investigate the function J given by (35) for $\nu = \frac{1}{2}(p^n - 1)$. It is obviously unaltered by the substitutions (7) and (8), so that the proof of its absolute invariance† depends only upon the verification that it is unaltered by the transformation (3). Let J' denote the function (35) of the transformed coefficients a_0', a_1', a_2'. Here $a_0' = a_0$, $\Delta' = \Delta$. As shown below, $J\Delta = 0$, $J'\Delta' = 0$. Hence if $\Delta \neq 0$, $J = J' = 0$. Let next $\Delta = 0$, so that $a_1^2 = a_0 a_2$, $a_1'^2 = a_0' a_2'$. Then the sum in (35) equals $(\nu + 1) a_0^\nu a_2^\nu$. Now $\nu + 1 = \frac{1}{2}(p^n + 1)$ is the mark $\frac{1}{2}$ in the field. Hence the final factor of J equals $\frac{1}{2} a_0^\nu a_2^\nu - 1$. If a_0 is a not-square, $a_0^\nu = -1$, so that $J = 0$, $J' = 0$. If $a_0 = 0$, then $a_1 = 0$, while

* If we employ (11) instead of (36), we must introduce the factor 4^i under the summation sign in (35). For the essentially distinct case $p = 2$, here excluded, see § 11.

† The existence of an invariant independent of I and Δ follows from the canonical form theory (§ 26).

the form a_2y^2 is unaltered by transformation (3). Finally, let a_0 be a square $\neq 0$, so that $a_0^\nu = 1$. Then

$$J = (a_2^\nu + 1)(a_2^\nu - 2), \qquad J' = (a_2'^\nu + 1)(a_2'^\nu - 2).$$

Since $a_0 a_2$ is a square or zero, a_2 is a square or zero, so that $a_2^\nu = 1$ or 0; in either case $J = -2$. Likewise $J' = -2$. We have now proved the following

THEOREM. *The quadratic form* (36) *in the* $GF[p^n]$, $p < 2$, *has the absolute invariant* J *defined by* (35) *for* $\nu = \frac{1}{2}(p^n - 1)$.

We next prove the following relations, which reduce to (32) for $p = 3$:

$$J\Delta = 0, \qquad (J+1)^2 = I + 1, \tag{37}$$

so that, *for the functions obtained from* I *and* J *by deleting their constant terms* -1, *the one is the square of the other.* We here have

$$\Delta = a_1^2 - a_0 a_2, \qquad I = (a_0^{2\nu} - 1)(a_1^{2\nu} - 1)(a_2^{2\nu} - 1). \tag{38}$$

Since $a^{2\nu+1} = a$, a simple change of summation indices gives

$$J\Delta = P(a_0 a_2 - a_0^{\nu+1} a_2^{\nu+1}), \qquad P \equiv (a_0^\nu + 1)(a_2^\nu + 1).$$

Then $J\Delta = 0$ follows from

$$a_0^{\nu+k} a_2^{\nu+k} P = (a_0^{2\nu+k} + a_0^{\nu+k})(a_2^{2\nu+k} + a_2^{\nu+k}) = (a_0^k + a_0^{\nu+k})(a_2^k + a_2^{\nu+k}) = a_0^k a_2^k P \quad (k > 0). \tag{39}$$

To determine J^2, call σ the last factor, $\Sigma - 1$, in (35). Then

$$(a_2^\nu + 1)^2 \sigma^2 = \{a_2^{2\nu} - 1 + 2(a_2^\nu + 1)\}\sigma^2 = -(a_2^{2\nu} - 1)(a_1^{2\nu} - 1) + 2(a_2^\nu + 1)\sigma^2,$$

since $(a^{2\nu} - 1)a = 0$. Modifying $(a_0^\nu + 1)^2$ similarly, we get

$$J^2 = -I - 2(a_0^\nu + 1)(a_2^{2\nu} - 1)(a_1^{2\nu} - 1) + 2(a_2^\nu + 1)\{-(a_0^{2\nu} - 1)(a_1^{2\nu} - 1) + 2(a_0^\nu + 1)\sigma^2\}$$
$$= -I + 2P\{(a_1^{2\nu} - 1)(2 - a_0^\nu - a_2^\nu) + 2\sigma^2\}.$$

Now

$$\sigma = a_1^{2\nu} - 1 + a_0^\nu a_2^\nu + \Sigma, \qquad \Sigma \equiv \sum_{i=1}^{\nu-1} a_0^i a_2^i a_1^{2\nu-2i},$$

$$\sigma^2 = -(a_1^{2\nu} - 1) + 2(a_1^{2\nu} - 1) a_0^\nu a_2^\nu + a_0^{2\nu} a_2^{2\nu} + 2a_0^\nu a_2^\nu \Sigma + \Sigma^2.$$

Since $2J = 2P\sigma$, we have

$$J^2 + 2J = -I + 2P\{(a_1^{2\nu} - 1)(1 - a_0^\nu - a_2^\nu + a_0^\nu a_2^\nu) + L\} = I + 2PL,$$

$$L \equiv a_0^\nu a_2^\nu + 2a_0^{2\nu} a_2^{2\nu} + 3a_0^\nu a_2^\nu (a_1^{2\nu} - 1) + 4a_0^\nu a_2^\nu \Sigma + \Sigma + 2\Sigma^2.$$

Hence (37_2) will follow if we show that $PL = 0$. In view of (39),

$$PL = P(3a_0^\nu a_2^\nu a_1^{2\nu} + 5\Sigma + 2\Sigma^2).$$

The second member may be shown, by means of (39), to equal

$$P(2\nu+1)(a_0^\nu a_2^\nu a_1^{2\nu}+\Sigma),$$

and hence vanishes in the $GF[p^n]$, since $2\nu+1=p^n$.

16. This section and the four succeeding sections will be devoted primarily to the exhibition of a remarkable absolute invariant K of degree $\mu=p^n-1$ of the binary cubic form in the $GF[p^n]$, and to the simple relation between K and the discriminant Δ of the form. Except for the case $p=3$ (cf. § 9), we shall write the form with binomial coefficients

$$a_0x^3+3a_1x^2y+3a_2xy^2+a_3y^3. \tag{40}$$

Under transformation (3), a_1, a_2, a_3 take the respective increments

$$\delta_1=ta_0, \qquad \delta_2=2ta_1+t^2a_0, \qquad \delta_3=3ta_2+3t^2a_1+t^3a_0. \tag{41}$$

For each term (§ 5) of an absolute invariant ϕ we have

$$3e_0+2e_1+e_2=r\mu, \qquad e_1+2e_2+3e_3=s\mu \qquad (r, s \text{ integers}). \tag{42}$$

The condition that the term shall be of degree μ is $r+s=3$. For $r=3$ and $r=0$, we obtain the respective terms

$$a_0^\mu, \qquad a_3^\mu. \tag{43}$$

The general term with $r=1$ is

$$a_0^{e_0}a_1^{e_1}a_2^{e_2}a_3^{e_3}, \qquad 3e_0+2e_1+e_2=\mu, \qquad e_1+2e_2+3e_3=2\mu. \tag{44}$$

In view of (5), an invariant ϕ must be unaltered by the substitution

$$a_0'=-a_3, \qquad a_3'=a_0, \qquad a_1'=a_2, \qquad a_2'=-a_1. \tag{45}$$

For $p=2$, the signs may be taken positive. For $p>2$, μ is even, and hence e_0, e_2 are both even or both odd. Further, we cannot have $e_0=e_3$ and $e_1=e_2$ in a term (44). Hence each term (44) of ϕ is accompanied by another term, not of type (44), having the same coefficient as the former. These new terms give all the terms of ϕ for which $r=2$, $s=1$ in (42).

In all the cases, viz., for $p^n=2^n(n=1,\cdots,5)$, 3^n (n general), 5, 7, 11, 13, in which I have actually constructed an absolute *invariant* K of degree $\mu=p^n-1$, I find that the two terms (43) do not occur. Excluding those terms, we have the simpler* problem: *to construct an absolute invariant K whose terms are those given by* (44) *with suitable coefficients, and those derived by applying the substitution* $(a_0a_3)(a_1a_2)$.

* Since the exponent of a_3 is at most $\frac{2}{3}\mu$. By (41), the powers of δ_3 are complicated.

The results for the case $n = 1$ are very simple; all the terms just mentioned actually occur in K. *The cubic form with coefficients modulo p, a prime, has an absolute invariant K of degree $p-1$ containing $2k$ terms, where k is the number of partitions of $p-1$ into $3e_0 + 2e_1 + e_2$.* For $p = 3$, K is given by (14). For $p \neq 3$, the results relate to the notation (40) for the cubic form. Then, for $p = 2$, $K = a_1 + a_2$. For $p = 5, 7, 11, 13$, the expressions for K follow in that order. The first terms in the parentheses are the terms (44), arranged so that if two terms have different exponents to a_0, that with the lesser precedes, while, if the exponents of a_0 are equal the term with the lesser exponent to a_1 precedes. The second term in any parenthesis is derived from the first by the substitution $(a_0 a_3)(a_1 a_2)$.

$$(46)\quad (a_2^4+a_1^4)-(a_1a_2^2a_3+a_0a_1^2a_2)-(a_1^2a_3^2+a_0^2a_2^2)+(a_0a_2a_3^2+a_0^2a_1a_3),\ GF[5].$$

$$(47)\quad \begin{aligned}&(a_2^6+a_1^6)+3(a_1a_2^4a_3+a_0a_1^4a_2)+3(a_1^2a_2^2a_3^2+a_0^2a_1^2a_2^2)+(a_1^3a_3^3+a_0^3a_2^3)\\&+3(a_0a_2^3a_3^2+a_0^2a_1^3a_3)+2(a_0a_1a_2a_3^3+a_0^3a_1a_2a_3)+(a_0^2a_3^4+a_0^4a_2^2),\ GF[7].\end{aligned}$$

$$(48)\quad \begin{aligned}&(a_2^{10}+a_1^{10})-3(a_1a_2^8a_3+a_0a_1^8a_2)-3(a_1^2a_2^6a_3^2+a_0^2a_1^6a_2^2)+4(a_1^3a_2^4a_3^3+a_0^3a_1^4a_2^3)\\&+(a_1^4a_2^2a_3^4+a_0^4a_1^2a_2^4)-(a_1^5a_3^5+a_0^5a_2^5)+6(a_0a_2^7a_3^2+a_0^2a_1^7a_3)\\&+6(a_0a_1a_2^5a_3^3+a_0^3a_1^5a_2a_3)+5(a_0a_1^2a_2^3a_3^4+a_0^4a_1^3a_2^2a_3)-3(a_0a_1^3a_2a_3^5+a_0^5a_1a_2^3a_3)\\&+5(a_0^2a_2^4a_3^4+a_0^4a_1^4a_2^3)+4(a_0^2a_1a_2^2a_3^5+a_0^5a_1^2a_2a_3^2)-(a_0^2a_1^2a_3^6+a_0^6a_2^2a_3^2)\\&+(a_0^3a_2a_3^6+a_0^6a_1a_3^3),\qquad GF[11].\end{aligned}$$

$$(49)\quad \begin{aligned}&(a_2^{12}+a_1^{12})+5(a_1a_2^{10}a_3+a_0a_1^{10}a_2)+5(a_1^2a_2^8a_3^2+a_0^2a_1^8a_2^2)-6(a_1^3a_2^6a_3^3+a_0^3a_1^6a_2^3)\\&+6(a_1^4a_2^4a_3^4+a_0^4a_1^4a_2^4)+2(a_0^2a_2^6a_3^4+a_0^4a_1^6a_3^2)+2(a_1^5a_2^2a_3^5+a_0^5a_1^2a_2^5)+(a_1^6a_3^6+a_0^6a_2^6)\\&-3(a_0a_2^9a_3^2+a_0^2a_1^9a_3)+2(a_0a_1a_2^7a_3^3+a_0^3a_1^7a_2a_3)-3(a_0a_1^2a_2^5a_3^4+a_0^4a_1^5a_2^2a_3)\\&+3(a_0a_1^3a_2^3a_3^5+a_0^5a_1^3a_2^3a_3)-3(a_0a_1^4a_2a_3^6+a_0^6a_1a_2^4a_3)+4(a_0^2a_1a_2^4a_3^5+a_0^5a_1^4a_2a_3^2)\\&-3(a_0^2a_1^2a_2^2a_3^6+a_0^6a_1^2a_2^2a_3^2)+3(a_0^2a_1^3a_3^7+a_0^7a_2^3a_3^2)-6(a_0^3a_2^3a_3^6+a_0^6a_1^3a_3^3)\\&+2(a_0^3a_1a_2a_3^7+a_0^7a_1a_2a_3^3)+(a_0^4a_3^8+a_0^8a_3^4),\qquad GF[13].\end{aligned}$$

17. For a cubic form in the $GF[p^n]$, $n > 1$, the invariant K of degree $\mu = p^n - 1$ does not involve all the terms (44). Indeed, when the multiplicative constant is suitably chosen, K is identical* with K^p, so that a term (44) occurs in K only when

$$(50)\qquad [p^i e_0] + [p^i e_1] + [p^i e_2] + [p^i e_3] = \mu \cdot \ (i = 1, \cdots, n-1),$$

where $[x]$ denotes the least positive (or zero) residue of x modulo μ. Inversely, *K contains every term* (44) *satisfying conditions* (50). In exhibiting an invariant, we enclose within a parenthesis terms derived as follows: first a term (44); then in turn its pth, (p^2)th, $\cdots$, (p^{n-1})th powers, when they are distinct

* The explanation of this property appears to lie in the fact noted at the end of § 12.

from the first term; finally, the terms derived from the preceding by the substitution $(a_0a_3)(a_1a_2)$, when they are distinct from the preceding.

18. For a cubic form in the $GF[2^n]$, the absolute invariant K of degree 2^n-1 contains exactly 2^n terms. We exhibit K for $n \leqq 5$, arranging the terms as explained in §§ 16, 17.

$$(a_2+a_1), \qquad GF[2]. \tag{51}$$

$$(a_2^3+a_1^3)+(a_0a_3^2+a_0^2a_3), \qquad GF[4]. \tag{52}$$

$$(a_2^7+a_1^7)+(a_0a_2^4a_3^2+a_0^2a_2a_3^4+a_0^4a_2^2a_3+a_0^2a_1^4a_3+a_0^4a_1a_3^2+a_0a_1^2a_3^4), \quad GF[8]. \tag{53}$$

$$\begin{aligned}&(a_2^{15}+a_1^{15})+(a_0a_2^{12}a_3^2+a_0^2a_2^9a_3^4+a_0^4a_2^3a_3^8+a_0^8a_2^6a_3+a_0^2a_1^{12}a_3+a_0^4a_1^9a_3^2+a_0^8a_1^3a_3^4\\&+a_0a_1^6a_3^8)+(a_0a_1^2a_2^8a_3^4+a_0^2a_1^4a_2a_3^8+a_0^4a_1^8a_2^2a_3+a_0^8a_1a_2^4a_3^2)+(a_0^5a_3^{10}+a_0^{10}a_3^5),\end{aligned} \tag{54}$$
$GF[16]$.

$$\begin{aligned}&(a_2^{31}+a_1^{31})+(a_0a_2^{28}a_3^2+a_0^2a_2^{25}a_3^4+a_0^4a_2^{19}a_3^8+a_0^8a_2^7a_3^{16}+a_0^{16}a_2^{14}a_3+a_0^2a_1^{28}a_3\\&+a_0^4a_1^{25}a_3^2+a_0^8a_1^{19}a_3^4+a_0^{16}a_1^7a_3^8+a_0a_1^{14}a_3^{16})+(a_0a_1^2a_2^{24}a_3^4+a_0^2a_1^4a_2^{17}a_3^8+a_0^4a_1^8a_2^3a_3^{16}\\&+a_0^8a_1^{16}a_2^6a_3+a_0^{16}a_1a_2^{12}a_3^2+a_0^4a_1^{24}a_2^2a_3+a_0^8a_1^{17}a_2^4a_3^2+a_0^{16}a_1^3a_2^8a_3^4+a_0a_1^6a_2^{16}a_3^8\\&+a_0^2a_1^{12}a_2a_3^{16})+(a_0^5a_2^{16}a_3^{10}+a_0^{10}a_2a_3^{20}+a_0^{20}a_2^2a_3^9+a_0^9a_2^4a_3^{18}+a_0^{18}a_2^8a_3^5+a_0^{10}a_1^{16}a_3^5\\&+a_0^{20}a_1a_3^{10}+a_0^9a_1^2a_3^{20}+a_0^{18}a_1^4a_3^9+a_0^5a_1^8a_3^{18}),\end{aligned} \tag{55}$$
$GF[32]$.

19. For the cubic form, with coefficients in the $GF[3^n]$,

$$a_0x^3+a_1x^2y+a_2xy^2+a_3y^3, \tag{56}$$

we can determine immediately the absolute invariant K of degree 3^n-1 in terms of the absolute invariant P, given by (9), and the discriminant Δ of (56), viz.,

$$P=(a_1^{3^n-1}-1)(a_2^{3^n-1}-1), \qquad \Delta=a_1^2a_2^2-a_0a_2^3-a_1^3a_3. \tag{57}$$

In fact, the invariant K is simply the reduced form of

$$K=\Delta^{(3^n-1)/2}-P+1. \tag{58}$$

The reduced form of K depends upon the character of the product

$$\pi\cdot\Delta^{3^{n-1}}, \qquad \pi\equiv\prod_{i=0}^{n-2}\Delta^{3^i}. \tag{59}$$

But in the $GF[3^n]$, we have

$$\Delta^{3^i}=(a_1a_2)^{2\cdot3^i}-a_0^{3^i}a_2^{3^{i+1}}-a_3^{3^i}a_1^{3^{i+1}} (i<n-1), \quad \Delta^{3^{n-1}}=(a_1a_2)^{2\cdot3^{n-1}}-a_0^{3^{n-1}}a_2-a_3^{3^{n-1}}a_1.$$

Now every term of the expanded product π is of degree

$$4\sum_{i=0}^{n-2}3^i=2d, \qquad d\equiv3^{n-1}-1.$$

Further, $\pi = (a_1 a_2)^d + \sigma$, where each term of σ is of degree higher than d in one of the letters a_1, a_2. Indeed, if we employ either of the last two terms of $\Delta^{3^{n-2}}$ the resulting term of the product π is of degree $\geqq 3^{n-1}$ in a_1 or a_2. Hence the statement follows by induction from $n-1$ to n.

It now follows that, in the complete product (59), a term is exactly of degree $3^n - 1$ if one of its factors is chosen from the last two terms of $\Delta^{3^{n-1}}$. Finally, in

$$\pi \cdot (a_1 a_2)^{2 \cdot 3^{n-1}} = (a_1 a_2)^{3^n - 1} + \sigma (a_1 a_2)^{2 \cdot 3^{n-1}}$$

every term, except the first, is of degree higher than $d + 2 \cdot 3^{n-1} \equiv 3^n - 1$ in one of the letters a_1, a_2, and hence admits of a reduction in total degree (by means of the equation $a^{3^n} = a$, satisfied by every mark of the field) from $2d + 4\ 3^{n-1} = 2(3^n - 1)$ to $3^n - 1$. The exceptional first term cancels a term of $-P$. Hence *every term in the reduced form of the absolute* invariant* (58) *is of degree* $3^n - 1$.

In the expansion of (59) no two terms have the same set of exponents, so that there result 3^n distinct terms, no one identical with $a_j^{3^n-1}$ ($j = 1$ or 2). Hence *the reduced form of* (58) *contains exactly* $3^n + 1$ *terms*. For $n = 1$, they are given by (14); for $n = 2$ by (75). For $n \leqq 3$, I have verified that the terms of K obey the laws stated in § 17. As these (empirical) laws were formulated from another standpoint (and in fact prior to the investigation of the present case $p = 3$), we have independent evidence of the validity of the conjectures.

From (57) and (58) we deduce immediately the important relation

$$(\Delta^{(3^n+1)/2} - \Delta) K = 0. \tag{60}$$

Indeed, $\Delta P = 0$, so that

$$\Delta K = \Delta^{(3^n+1)/2} + \Delta, \qquad \Delta^{(3^n+1)/2} K = \Delta^{3^n} + \Delta^{(3^n+1)/2}, \qquad \Delta^{3^n} = \Delta.$$

20. The discriminant of the cubic form (40) in the $GF[p^n]$, $p \neq 3$, is

$$\Delta = -3a_1^2 a_2^2 + 4a_0 a_2^3 + 4a_1^3 a_3 - 6a_0 a_1 a_2 a_3 + a_0^2 a_3^2. \tag{61}$$

Now the invariants K, given by (46)-(49), satisfy the relation

$$(\Delta^{(p^n+1)/2} - \epsilon\Delta) K = 0, \qquad \epsilon = (-3)^{(p^n-1)/2}, \tag{62}$$

ϵ being $+1$ or -1 according as -3 is a square or a not-square in the $GF[p^n]$, $p > 3$. If we define Δ to be the function (61) multiplied by -3 (or by $-3\lambda^2$, λ any mark $\neq 0$), relation (62) is replaced by the simpler relation

$$(\Delta^{(p^n+1)/2} - \Delta) K = 0. \tag{63}$$

* Under a transformation of determinant D, the discriminant Δ is multiplied by D^6, so that $\Delta^{(3^n-1)/2}$ is an absolute invariant in the $GF[3^n]$.

THEOREM.* *If the indeterminate constant factor in the discriminant* Δ *of a cubic form in the* $GF[p^n]$, $p>2$, *be chosen so that the coefficient of* $a_1^2a_2^2$ *is a square in the field, then* Δ *and the absolute invariant* K *of degree* p^n-1 *satisfy the relation* (63).

21. Consider next invariants of the cubic form (56) in the $GF[3^n]$. Under transformation (3), the increments to a_2 and a_3 are $-ta_1$ and $ta_2+t^2a_1+t^3a_0$, respectively, while a_0 and a_1 are unaltered. The case $n=1$ was treated in § 9. Let here $n=2$. Then the coefficients of t and t^3 in $\phi'-\phi$ give the respective annihilators: †

$$
\begin{aligned}
&-a_1(2)+a_2(3)+a_0a_1^6(2^63)-a_1^8(2^73)+a_1^8a_2(2^83)-a_0^2a_1^3(2^33^2)\\
&-a_0a_1^5(2^43^2)+(a_0a_1^5a_2-a_1^7)(2^53^2)-a_1^7a_2(2^63^2)-a_1^7a_2^2(2^73^2)-a_0^3(3^3)\\
&-a_1^6(2^33^3)+a_1^6a_2^3(2^63^3)+a_0^3a_1^3(2^83^3)+a_0a_1^3(3^4)-a_1^5(23^4)+a_1^5a_2(2^23^4)\\
&-a_0a_1^3a_2^3(2^33^4)+a_1^5a_2^3(2^43^4)-a_1^5(a_0^4+a_2^4)(2^53^4)+a_0^3a_1^7(2^63^4)-a_0^3a_1^7a_2(2^73^4)\\
(64)\quad&+a_0a_1^3(2^83^4)+(a_0^2a_2^2-a_1^4a_2)(3^5)+(a_0a_1^2a_2^3-a_1^4a_2^2)(23^5)+(a_0^4a_1^4+a_1^4a_2^4)(2^33^5)\\
&+(a_0^3a_1^6a_2^2-a_0a_1^2)(2^63^5)-a_1^3a_2^3(3^6)-a_0^3a_1^5(2^23^6)-a_1^3a_2^6(2^33^6)\\
&+(a_0^3a_1^5a_2^3-a_1^3)(2^53^6)-a_0^6a_1^7(2^73^6)-a_1^3a_2^3(2^83^6)+(a_0a_2^6-a_0^3a_1^4)(3^7)\\
&+(a_0^3a_1^4a_2-a_1^2a_2^6)(23^7)+(a_1^2a_2^7-a_0^4a_1^2a_2^3+a_0a_1^8)(2^23^7)+(a_0^3a_1^4a_2^3-a_1^2)(2^33^7)\\
&+(a_0^4a_1a_2^3-a_0^3a_1^3a_2^2-a_0a_1^7-a_1a_2^7)(3^8)\cdot
\end{aligned}
$$

$$
\begin{aligned}
&-a_1^3(2^3)+a_0(3)-a_1^2(23)+a_1^2a_2(2^23)+a_0a_1^8(2^83)-a_1a_2(3^2)-a_1a_2^2(23^2)\\
&-a_0^2a_1^5(2^53^2)-a_0a_1^7(2^63^2)+(a_0a_1^7a_2-a_1)(2^73^2)-a_1a_2(2^83^2)+a_2^3(3^3)\\
(65)\quad&+a_0^3a_1^2(2^23^3)-a_1^8(2^53^3)+a_1^8a_2^3(2^83^3)+a_0^3a_1(3^4)-a_0^3a_1a_2(23^4)+a_0a_1^5(2^23^4)\\
&-a_1^7(2^33^4)+a_1^7a_2(2^43^4)-a_0a_1^5a_2^3(2^53^4)+a_1^7a_2^3(2^63^4)-(a_0^4a_1^7+a_1^7a_2^4)(2^73^4)\\
&+a_0^3a_1(2^83^4)+(a_0^3a_2^2-a_0a_1^4)(3^5)+(a_0a_1^4a_2-a_1^6)(23^5)+(a_0a_1^4a_2^3-a_1^6a_2^2)(2^33^5)
\end{aligned}
$$

* If, instead of the mere verification of this theorem for the computed invariants K, we had a direct proof, it would be of decided aid to the computation. We may compute K by means of (63) alone. For example, let $p^n=3^2$, and give K its necessary form (75) with the four parentheses multiplied by 1, m, s, r, respectively. In $(\Delta^5-\Delta)K$, we readily find that the factor of a_3^8 is $(s-r)a_0a_1^8a_2^3-(s+m)a_1^2a_2^3$, while the terms independent of a_1 and a_3 are $(s-1)(a_0^6a_2^7-a_0a_2^3)$. Hence $-m=r=s=1$.

In general, the labor of determining the high power of Δ would be great. We may, however, employ only the first two terms of (61) and so readily compute the terms of (63) independent of a_3. We thereby get the coefficients of the terms of ϕ independent of a_3. The coefficients of the terms involving a_3 to the first power are then either known or else occur in the terms involving a_3^e $(e\geqq 2)$, in view of (45). The work with the annihilators is now greatly simplified. It suffices to find the coefficients of a_3^r, $\cdots$, a_3^3, a_3^2, in turn, where r is the greatest integer in $2/3(p^n-1)$. We need only a part of the annihilators; for instance, the derivative with respect to a_3 need not be of order higher than $r-2$.

† We have omitted the terms (2^i3^8), $i\geqq 1$, (2^i3^7), $i\geqq 4$, (2^i3^5), $i=2, 4, 5, 7, 8$ (which have long coefficients), since they have no effect upon a function ϕ satisfying (67), the binomial coefficients C_{6i} $(i=2, 4, 5)$ being multiples of 3.

$$+(a_1^6a_2^5+a_0^3a_1^8-a_0^4a_1^6a_2)(2^63^5)-a_0^6a_1(23^6)-a_1^5a_2^3(2^23^6)-a_0^3a_1^7(2^43^6)$$
$$-a_1^5a_2^6(2^53^6)+(a_0^3a_1^7a_2^3-a_1^5)(2^73^6)+(a_0^6a_2-a_1^4a_2^3)(3^7)+(a_0^4a_1^4+a_1^4a_2^4)(23^7)$$
$$+(a_0a_1^2a_2^6-a_0^3a_1^6)(2^23^7)+(a_0^3a_1^6a_2-a_1^4a_2^6)(2^33^7)$$
$$+(a_0^4a_1^3a_2-a^3a_1^5-a_0a_1a_2^6-a_1^3a_2^5)(3^8).$$

We may set

$$\phi=\sum_{i,j}^{0,\cdots,8}B_{ij}a_2^ia_3^j \qquad (B\text{'s functions of } a_0,\ a_1). \tag{66}$$

Since a_3^8 occurs only the first term of (64) and of (65), we get

$$B_{i8}a_1=0 \qquad (i=1,\cdots,8).$$

In view of these relations, a_3^7 occurs only in the first two terms of (64) and the first two terms of (65). The resulting sets of conditions react on each other and give the first two conditions (69) and

$$B_{i8}=0\ (i=1,\cdots,7), \qquad B_{i7}a_1=0\ (i=1,4,5,6,7,8),$$

together with $B_{88}a_0=0$. From the latter and $B_{88}a_1=0$ follows

$$B_{88}=k\pi, \qquad \pi\equiv(a_0^8-1)(a_1^8-1).$$

Hence on replacing ϕ by $\phi-kI$, when I is the absolute invariant (2), we have $B_{88}=0$. If both $B_{ij}a_0$ and $B_{ij}a_1$ vanish, then $B_{ij}=c\pi$, and hence $B_{ij}=0$ in view of (16).

We consider in turn the coefficients of $a_3^6,\cdots,a_3$ in (64) and (65) and finally the terms * independent of a_3 in (65). The process of writing down the two coefficients of a_3^r is simplified by holding in mind those of the relations (67) and (68) which have been found in the earlier steps. The two resulting sets of conditions react on each other very considerably, and some further simplifications result from the earlier conditions. The final results are as follows:

$$B_{i8}=0\,(i=1,\cdots,8), \quad B_{i7}=0\,(i=1,4,\cdots,8), \quad B_{i5}=0\,(i=2,3,4,5,7,8); \tag{67}$$

$$B_{i6}a_1=0\,(i=1,7,8), \quad B_{i4}a_1=0\,(i=5,7), \quad B_{i2}a_1=0\,(i=3,5,8); \tag{68}$$

together with the set of conditions, referred to as (69):

$$B_{08}=P_{27}a_1,\ B_{08}a_0=-B_{37}a_1^3,\ B_{07}=-B_{26}a_1,\ B_{37}=-B_{56}a_1,\ B_{27}=B_{46}a_1,$$
$$B_{37}a_0=-B_{66}a_1^3,\ B_{27}a_0=B_{56}a_1^3,\ B_{07}a_0=B_{36}a_1^3,\ B_{15}a_1=-B_{08}a_0^3,\ B_{65}a_1^3=B_{08},$$

* Those in (64) are not required in computing the invariants; they were determined directly for each invariant and found to vanish, thus giving a check.

$B_{65}=B_{84}a_1$, $B_{15}=-B_{27}a_0^3$, $B_{05}=B_{24}a_1$, $B_{44}a_1=-B_{37}a_0^3$, $B_{65}a_0=-B_{37}$,
$B_{84}a_1^3=B_{27}$, $B_{14}a_1+B_{65}a_0a_1^6+B_{07}a_0^3=0$, $B_{44}a_1^3=-B_{15}a_0$, $B_{07}=B_{64}a_1^3$,
$B_{05}a_0=B_{15}a_1^2-B_{34}a_1^3$, $B_{74}=B_{86}a_0^3$, $B_{64}=B_{76}a_0^3-B_{83}a_1$, $B_{54}=B_{66}a_0^3+B_{73}a_1$,
$B_{44}=B_{56}a_0^3$, $B_{34}=B_{46}a_0^3-B_{53}a_1$, $B_{24}=B_{36}a_0^3+B_{43}a_1-B_{66}a_1^6$,
$B_{14}=B_{26}a_0^3-B_{84}a_0a_1^6$, $B_{04}+B_{84}+B_{23}a_1-B_{16}a_0^3+B_{46}a_1^6=0$,
$B_{64}a_0a_1^6=B_{13}a_1+B_{06}a_0^3$, $B_{56}=B_{84}a_0$, $B_{46}=B_{74}a_0+B_{84}a_1^2$, $B_{36}=B_{64}a_0$,
$B_{26}=B_{54}a_0+B_{83}a_1^3$, $B_{16}=B_{44}a_0+B_{73}a_1^3$, $B_{06}+B_{86}=B_{34}a_0-B_{44}a_1^2+B_{63}a_1^3$,
$B_{76}=B_{24}a_0-B_{53}a_1^3-B_{08}a_0^3$, $B_{66}=B_{14}a_0-B_{24}a_1^2-B_{43}a_1^3-B_{05}a_1$,
$B_{04}a_0=B_{33}a_1^3+B_{26}a_0^3a_1^2-B_{56}a_1^8$, $B_{12}a_1=B_{05}a_0^3$, $B_{22}a_1=-B_{15}a_0^3$,
$B_{42}a_1=-B_{65}a_1^6-B_{08}a_1^3$, $B_{15}=-B_{72}a_1^3$, $B_{05}=-B_{62}a_1^3$, $B_{65}=B_{42}a_1^3$,
$B_{72}=B_{84}a_0^3$, $B_{62}=B_{81}a_1+B_{74}a_0^3$, $B_{52}=B_{64}a_0^3+B_{37}a_1^3-B_{71}a_1$, $B_{42}=B_{54}a_0^3+B_{27}a_1^3$,
$B_{32}=B_{51}a_1+B_{44}a_0^3$, $B_{22}=B_{34}a_0^3+B_{07}a_1^3-B_{41}a_1$, $B_{12}=B_{24}a_0^3$,
$B_{02}+B_{82}=B_{21}a_1-B_{72}a_0a_1^6+B_{14}a_0^3$, $B_{62}a_0a_1^6=B_{04}a_0^3+B_{84}a_0^3a_1^8-B_{11}a_1$,
$B_{54}=B_{82}a_0$, $B_{44}=B_{72}a_0$, $B_{34}=B_{62}a_0-B_{84}a_0^3a_1^2$, $B_{24}=B_{52}a_0-B_{81}a_1^3$,
$B_{14}=B_{42}a_0-B_{71}a_1^3$, $B_{04}+B_{84}=B_{32}a_0-B_{61}a_1^3-B_{27}a_1^5$, $B_{74}=B_{22}a_0+B_{51}a_1^3$,
$B_{64}+B_{22}a_1^2=B_{12}a_0+B_{41}a_1^3$, $B_{12}a_1^2=B_{02}a_0+B_{31}a_1^3$, $B_{53}+B_{81}a_0+B_{72}a_1=0$,
$B_{43}+B_{71}a_0+B_{62}a_1=0$, $B_{33}+B_{61}a_0-B_{71}a_1^2=0$, $B_{23}+B_{51}a_0+B_{80}a_1^3+B_{84}a_1^7=0$,
$B_{13}+B_{41}a_0-B_{51}a_1^2+B_{70}a_1^3=0$, $B_{03}+B_{83}+B_{31}a_0-B_{41}a_1^2+B_{60}a_1^3=0$,
$B_{73}+B_{21}a_0+B_{12}a_1-B_{50}a_1^3=0$, $B_{63}+B_{11}a_0-B_{21}a_1^2-B_{02}a_1-B_{40}a_1^3=0$,
$B_{01}a_0-B_{11}a_1^2-B_{30}a_1^3+B_{23}a_0^3a_1^2-B_{53}a_1^8+B_{04}a_0^3a_1+B_{24}a_0a_1^5=0$.

The general term of ϕ, in the notations of § 5, is

(70) $a_0^{e_0}a_1^{e_1}a_2^{e_2}a_3^{e_3}$, $\quad 3e_0+2e_1+e_2\equiv d$, $\quad e_1+2e_2+3e_3\equiv d \pmod 8$.

For use in the later cases, we first determine the absolute invariants, viz., those with $d\equiv 0$. If $B_{e_2e_3}a_1=0$, then $e_1\equiv 0$, and hence $B=0$ unless $e_3\equiv 2e_2 \pmod 8$. Hence by (68),

(71) $B_{16}=B_{86}=B_{54}=B_{74}=B_{32}=B_{82}=0$, $B_{76}=ca_0^3(a_1^8-1)$, $B_{52}=ka_0(a_1^8-1)$.

For B_{27}, $e_1=7$, $e_0=0$ or 8; but $a_0^8a_1^7$ does not occur in view of (16) since $B_{78}=0$. Hence $B_{27}=ra_1^7$, r a constant. Then $B_{08}=ra_1^8$, $B_{37}=-ra_0a_1^5$,

etc., by (69). But Δ^4 and Δ^8 are absolute invariants, Δ being the discriminant (57), and

$$\Delta^8 = a_3^8 a_1^8 + a_3^7(a_1^7 a_2^2 - a_0 a_1^5 a_2^3) + \cdots. \tag{72}$$

Hence if we replace ϕ by $\phi - r\Delta^8$, we may set $r = 0$. Hence, by (69)

$$B_{08}, B_{27}, B_{37}, B_{56}, B_{46}, B_{66}, B_{15}, B_{65}, B_{84}, B_{44}, B_{73}, B_{22}, B_{42}, B_{72}, B_{51} \text{ all vanish.} \tag{73}$$

Now ϕ must be unaltered by substitution (16) and hence by $(a_0 a_3)(a_1 a_2)$, since e_0 and e_2 are both even or both odd, by (70). Thus, from (71), $B_{83} = c a_0^6 a_1^7$. Note that from $B_{07} = -c a_0^6 a_1^3$, we can conclude initially only that $B_{36} = -c a_0^7 + \rho a_0^7 a_1^8$, but subsequently that $\rho = 0$ since $B_{87} = 0$. In this way we readily find that conditions (69) are all satisfied if and only if, in addition to (71) and (73), the following relations hold:

$$B_{83} = c a_0^6 a_1^7,\ B_{03} = -c a_0^6 a_1^7,\ B_{81} = k a_0^2 a_1^5,\ B_{01} = -k a_0^2 a_1^5,\ B_{64} = -c a_0^6,$$

$$B_{06} = -c a_0^4 a_1^6,\ B_{07} = -c a_0^6 a_1^3,\ B_{36} = -c a_0^7,\ B_{14} = c a_0 a_1^2,\ B_{21} = c a_0^4 a_1,$$

$$B_{26} = c a_0^6 a_1^2,\ B_{24} = -k a_0^2,\ B_{02} = -k a_0^4 a_1^2,\ B_{05} = -k a_0^2 a_1,\ B_{12} = -k a_0^5,$$

$$B_{62} = k a_0^2 a_1^6,\ B_{71} = -k a_0 a_1^7,\ k = c,\ B_{41} = B_{31} = B_{43} = 0,\ B_{34} = c a_0^3 a_1^6,$$

$$B_{63} = c a_0^4 a_1^3,\ B_{53} = -c a_0^3 a_1^5,\ B_{23} = w a_1^3 \ (w \text{ new parameter}),\ B_{30} = w a_0^3 a_1^2,$$

$$B_{04} = -w a_1^4,\ B_{40} = -w a_0^4,\ B_{11} = -(k + w) a_0^3 a_1^3,\ B_{33} = -(k + w) a_0 a_1,$$

$$B_{61} = w a_1,\ B_{10} = w a_0 a_1^6,\ B_{20} = B_{50} = B_{60} = B_{70} = B_{13} = 0,$$

$$B_{80} = l(a_1^8 - 1) - w \ (l \text{ new parameter}),\ B_{00} = -(w + l) a_1^8 + \text{constant}.$$

For convenience, we take the constant in B_{00} (the absolute term of ϕ) to be l. Then there are three independent parameters w, l and $c = k$. The coefficient of the latter is the negative of the absolute invariant (of degrees 24, 16, 8):

$$\begin{aligned} W = {} & a_3^7 a_0^6 a_1^3 + a_3^6\{-a_0^3(a_1^8 - 1) a_2^7 + a_0^7 a_2^3 - a_0^6 a_1^2 a_2^2 + a_0^4 a_1^6\} + a_3^5 a_0^2 a_1 \\ & + a_3^4(a_0^6 a_2^6 - a_0^3 a_1^6 a_2^3 + a_0^2 a_2^2 - a_0 a_1^2 a_2) + a_3^3\{-a_0^6 a_1^7(a_2^8 - 1) - a_0^4 a_1^3 a_2^6 + a_0^3 a_1^5 a_2^5 + a_0 a_1 a_2^3\} \\ & + a_3^2\{-a_0^2 a_1^6 a_2^6 - a_0(a_1^8 - 1) a_2^5 + a_0^5 a_2 + a_0^4 a_1^2\} \\ & + a_3\{-a_0^2 a_1^5(a_2^8 - 1) + a_0 a_1^7 a_2^7 - a_0^4 a_1 a_2^2 + a_0^3 a_1^3 a_2\}. \end{aligned} \tag{74}$$

The coefficient of l is the invariant P, given by (57). The negative of the coefficient of w is the absolute invariant of degree 8 (see § 19):

$$K = a_3^4 a_1^4 + a_3^3(a_0 a_1 a_2^3 - a_1^3 a_2^2) + a_3(a_0^3 a_1^3 a_2 - a_1 a_2^6) + a_2^8 + a_0^4 a_2^4 - a_0^3 a_1^2 a_2^3 - a_0 a_1^6 a_2 + a_1^8. \tag{78}$$

Now $K = \Delta^4 - P + 1$, in agreement with (58). *Hence the absolute invariants are the linear functions of* $I, P, W, \Delta^4, \Delta^8$. The system should be closed also under multiplication. In verification, we note the relations

$$(76) \qquad \begin{gathered} I^2 = I,\ IP = I,\ IW = 0,\ I\Delta = 0,\ P^2 = P,\ PW = 0, \\ P\Delta = 0,\ W^2 = W,\ W\Delta^4 = W. \end{gathered}$$

Let next $d \equiv 1 \pmod 8$. Then $B_{e_2 e_3} a_1 = 0$ implies $B = 0$ unless $e_3 \equiv 2e_2 + 3 \pmod 8$. Hence the B_{ij} in (68) all vanish. For B_{27}, $e_1 = 0$ or 8, $e_0 = 5$; but $a_0^5 a_1^8$ does not occur in view of (16) since $B_{85} = 0$. Thus $B_{27} = ca_0^5$. Also $B_{84} = ra_0^5 a_1^5$. But one of relations (69) is $B_{84} a_1^3 = B_{27}$. Hence $B_{27} = B_{84} = 0$. In view of relations (69) and the invariance* of ϕ under (16), we readily find that the only non-vanishing B_{ij} are the sixteen for which i, j range over the exponents of a_2, a_3 in the following invariant, the value of B_{ij} being the product of a fixed parameter l by the coefficient of $a_2^i a_3^j$:

$$\begin{aligned} &a_3^7 a_0^3 a_1^4 + a_3^6 (a_0^4 a_1 a_2^3 - a_0^3 a_1^3 a_2^2 - a_0 a_1^7) + a_3^4 (a_0^3 a_1 a_2^2 - a_0^6 a_1^3 a_2) \\ &+ a_3^3 (- a_0^3 a_2^8 - a_0 a_1^4 a_2^6 - a_0^7 a_2^4 + a_0^6 a_1^2 a_2^3 - a_0^4 a_1^6 a_2 + a_0^3 a_1^8) + a_2^3 (- a_0 a_1^3) \\ &+ a_3 (a_0^6 a_2^7 + a_0^3 a_1^6 a_2^4 + a_0^2 a_2^3), \end{aligned} \tag{77}$$

which equals $-E^3$, E being given by (10). By (82), $E^3 = \Delta E$.

For $d \equiv 3 \pmod 8$, we conclude that E is the only invariant. Indeed, the operation of cubing is uniquely reversible in the $GF[9]$. Similarly, the case $d \equiv 2$ reduces to the case $d \equiv 8$, and $d \equiv 7$ to $d \equiv 5$.

For $d \equiv 6 \pmod 8$, we may set $B_{08} = ka_0^6 a_1^6$. Then $B_{27} = ka_0^6 a_1^5$, etc. If we replace ϕ by $\phi + k\Delta W$, where

$$\Delta W = a_3^8 (- a_0^6 a_1^6) + a_3^7 (a_0^7 a_1^3 a_2^3 - a_0^6 a_1^5 a_2^2 - a_0^4 a_1) + \cdots, \tag{78}$$

we may set $k = 0$. The resulting invariant is easily found to be a linear function of Δ and Δ^5. Hence for $d \equiv 2$, the invariants are the linear functions of Δ^3, Δ^7 and $\Delta^3 W^3 \equiv \Delta^3 W$.

For $d \equiv 4$, we have $B_{27} = da_0^4 a_1^3$, $B_{08} = da_0^4 a_1^4$, $B_{37} = - da_0^5 a_1$, $B_{07} = da_0^2 a_1^7$, etc. We replace ϕ by $\phi - d\Delta^2 W$, where

$$\Delta^2 W = a_3^8 a_0^4 a_1^4 + a_3^7 (- a_0^5 a_1 a_2^3 + a_0^4 a_1^3 a_2^2 + a_0^2 a_1^7) + \cdots, \tag{79}$$

and hence may set $d = 0$. The resulting invariant is readily found to be a linear function of Δ^2 and Δ^6.

* Here a more exacting condition than for $d \equiv 0$. Thus $B_{31} = ma_0 a_1^2$ yields $m = 0$.

For $d \equiv 5$, we have $B_{27} = ra_0a_1^4$, $B_{08} = ra_0a_1^5$, $B_{37} = -ra_0^2a_1^2$, etc. We replace ϕ by $\phi - r\Delta^3 E$, where

$$\Delta^3 E = a_3^8 a_0 a_1^5 + a_3^7(a_0 a_1^4 a_2^2 - a_0^2 a_1^2 a_2^3) + \cdots, \tag{80}$$

and easily find that the resulting invariant vanishes identically. Then for $d \equiv 7$, the only invariant is $(\Delta^3 E)^3 \equiv \Delta^2 E$, by (82).

THEOREM. *The cubic form* (57) *in the* $GF[9]$ *has exactly* 18 *linearly independent invariants. These may be taken to be*

$$I, P, \Delta^i\ (i = 1, \cdots, 8), \qquad \Delta^j W, \Delta^j E\ (j = 0, 1, 2, 3). \tag{81}$$

The product of any two invariants can be reduced to a linear function of these 18 *invariants by the application of relations* (76) *and*

$$IE = PE = 0, \quad WE = E, \quad E^2 = \Delta W, \quad \Delta^4 E = E, \quad \Delta^9 = \Delta. \tag{82}$$

22. The invariants I and P of the cubic form in the $GF[3^n]$ can be expressed in terms of a single invariant Γ. Thus

$$\Gamma = I + P, \qquad I = \Gamma - \Gamma^2, \qquad P = \Gamma^2. \tag{83}$$

For $n = 1$, $W = E^2$ by (19). For $n = 2$, we have, by (76), (82),

$$W = W\Delta^4 = E^2\Delta^3.$$

Hence we have proved, for $n = 1$ and $n = 2$, the following

THEOREM. *The invariants of the cubic form in the* $GF[3^n]$ *are all rational integral functions of the three fundamental invariants* $\Gamma = I + P$, E, *and the discriminant* Δ, *where* I, P, E, *are defined in* §§ 1, 3, 4.

23. For the cubic form in the $GF[2^n]$, the power 2^{n-1} of the discriminant $a_0^2a_3^2 + a_1^2a_2^2$ gives the invariant

$$D = a_0a_3 + a_1a_2. \tag{84}$$

The eliminant E (§ 4) is $a_0a_3\pi$, where for $n = 1, 2, 3$, respectively, π equals

$$\Sigma a_i, \qquad \Sigma a_i^3 + D(a_0 + a_3), \qquad \Sigma a_i^7 + \lambda + \mu,$$

λ being the expression in the second parenthesis of (53), and

$$\mu = a_1a_2^5a_3 + a_0a_1a_2^2a_3^3 + a_0^3a_1a_2^3 + a_0a_1^5a_2 + a_0^3a_1^2a_2a_3 + a_1^3a_2a_3^3.$$

Thus $a_0a_3\mu = a_1a_2\lambda$. Hence, in each case, $E = DK$, K being given in § 18.

For $n = 1$ *or* 2, *every invariant is an absolute invariant.* This is evident for $n = 1$. For $n = 2$, we add the congruences (70), the modulus now being

3; there results $0 \equiv d \pmod 3$. By use of the annihilators, I have found the invariants

$$(85) \qquad R_{n=1} = a_0 + a_3 + a_0a_1 + a_0a_2 + a_1a_2 + a_1a_3 + a_2a_3,$$

$$(86) \quad R_{n=2} = a_0 + a_3 + a_0a_1^3 + a_0a_2^3 + a_0a_3^3 + a_0^3a_3 + a_1^3a_3 + a_2^3a_3 + a_0^2a_1a_2 + a_1a_2a_3^2 + a_0a_1a_2a_3,$$

and have proved that, for $n = 1, 2$, every invariant is a rational integral function of D, K, R. In particular, an expression for (2) is

$$(87) \qquad I = (D^\mu - 1)(K^\mu - 1)(R^\mu - 1), \qquad \mu = 2^n - 1.$$

For $n = 1$, every invariant is a linear function of D, K, R, DK, DR. Any relation between these follows from $KR = 0, D^2 = D, K^2 = K, R^2 = R$.

For $n = 2$, the 13 linearly independent invariants may be taken to be

$$(88) \qquad K, \quad D^i, \quad R^i, \quad D^iR, \quad D^iK \qquad (i = 1, 2, 3).$$

Any relation between these (absolute) invariants follows from

$$(89) \quad KR = 0, \quad K^2 = K, \quad (DR)^2 = DR, \quad D^4 = D, \quad R^4 = R.$$

For a proof that D, R, K are independent, see §§ 27, 28.

24. For the cubic form (40) with the integral coefficients modulo 5, the only invariant with $d \equiv 3 \pmod 4$ is the eliminant, given by § 4,

$$(90) \quad E = a_3^3(2a_0^2a_2 - 2a_0a_1^2) + a_3^2(2a_0a_1a_2^2 - 2a_0^3a_1) + a_3(a_0a_2^4 + 2a_0^3a_2^2 - 2a_0^2a_1^2a_2 - a_0a_1^4);$$

while ΔE is the only invariant with $d \equiv 1$. The only (absolute) invariants with $d \equiv 0$ are the linear functions of $I, \Delta^2, \Delta^4, K, \Delta^2K$, where K is given by (46). The only invariants with $d \equiv 2$ are the linear functions of $\Delta, \Delta^3, \Delta K$.

The ten linearly independent invariants of the cubic form (40) in the $GF[5]$ may be taken to be

$$(91) \qquad I, \ E, \ \Delta E, \ K, \ \Delta K, \ \Delta^2K, \ \Delta, \ \Delta^2, \ \Delta^3, \ \Delta^4.$$

Any relation between these follows from

$$(92) \quad \begin{gathered} I^2 = I, \quad IE = I\Delta = IK = 0, \quad E^2 = \Delta - \Delta^3 - \Delta K, \quad \Delta^2E = -E, \\ KE = -E, \quad K^2 = K - \Delta^2 + \Delta^4, \quad \Delta^3K = -\Delta K, \quad \Delta^5 = \Delta. \end{gathered}$$

25. For the cubic form (40) with integral coefficients modulo 7, the non-absolute invariants have $d \equiv 3 \pmod 6$. Indeed, if we add the congruences $\pmod 6$, analogous to (70), we find that $0 \equiv d \pmod 3$.

The only invariants with $d \equiv 3 \pmod 6$ are the linear functions of E, ΔE, and $\Delta^2 E$, where the eliminant E is (end of § 4)

$$(93)\quad \begin{aligned} E = {} & a_3^5(3a_0^3) + a_3^4(2a_0a_1^3 - 3a_0^2a_1a_2) + a_3^3(a_0^2a_2^3 + a_0a_1^2a_2^2 - 3a_0^5) \\ & + a_3^2(5a_0a_1a_2^4 + 3a_0^4a_1a_2 - a_0^3a_1^3) + a_3(a_0a_2^6 - 2a_0^4a_2^3 - a_0^3a_1^2a_2^2 + 2a_0^2a_1^4a_2 - a_0a_1^6). \end{aligned}$$

The absolute invariants are functions of Δ, K, given by (47), and Q:

$$(94)\quad \begin{aligned} Q = {} & a_3^6(2a_0^2) + a_3^5(6a_0a_1a_2 + 3a_1^3) + a_3^4(a_0a_2^3 + a_1^2a_2^2) + a_3^3(2a_1a_2^4 + 3a_0^3a_1a_2 + 4a_0^2a_1^3) \\ & + a_3^2(2a_2^6 + 4a_0^3a_2^3 + 3a_0^2a_1^2a_2^2 + a_0a_1^4a_2 - a_1^6 + 2a_0^6 - 2) \\ & + a_3(a_0^2a_1a_2^4 - a_0a_1^3a_2^3 + 2a_1^5a_2^2 - a_0^5a_1a_2 + a_0^4a_1^3) \\ & - a_0^2a_2^6 + 2a_0a_1^2a_2^5 + 3a_0^5a_2^3 + a_0^4a_1^2a_2^2 + 2a_0^3a_1^4a_2 + 2a_0^2a_1^6 - 2a_0^2. \end{aligned}$$

The sixteen linearly independent invariants of the cubic form (40) *in the* $GF[7]$ *may be taken to be*

$$(95)\quad E,\ \Delta E,\ \Delta^2 E,\ Q,\ Q^2,\ Q^3,\ \Delta^i\ (i = 1, \cdots, 6),\ \Delta^j K\ (j = 0, 1, 2, 3).$$

Any relation between these follows from

$$(96)\quad \begin{aligned} & \Delta^3 E = E,\ EQ = 0,\ EK = -E,\ Q^4 = 3\Delta^5 - 3\Delta^2 - Q,\ QK = 0,\ \Delta^7 = \Delta, \\ & \Delta^4 K = \Delta K,\ \Delta Q = 2\Delta^3 - 2\Delta^6,\ K^2 = K + \Delta^6 + \Delta^3,\ E^2 = 2\Delta K - 2\Delta^4 - 2\Delta. \end{aligned}$$

The invariant (2) has the following expression:

$$(97)\quad I = Q^3 + \Delta^3 K - K + 2\Delta^6 - 3\Delta^3 + 1.$$

26. The following tables give a complete set of (non-equivalent) canonical forms of binary quadratic forms in the $GF[p^n]$ and the values of the independent invariants for each canonical form:

$p > 2$ (invariants, § 15).

Canonical.	Δ	J
$x^2 - \nu y^2$	ν	0
xy	1	0
x^2	0	-2
νx^2	0	0
Vanishing	0	-1

$p = 2$ (invariants, § 11).

Canonical.	a_1	I	K
$x^2 + xy + cy^2$	1	0	1
xy	1	0	0
x^2	0	0	0
Vanishing	0	1	0

Here ν denotes a particular not-square in the $GF[p^n]$, $p > 2$; while c is a particular solution of $c + c^2 + \cdots + c^{2^{n-1}} = 1$ in the $GF[2^n]$.

27. As a complete set of (non-equivalent) canonical cubic forms in the $GF[p^n]$, we may take

$$\beta C,\ \beta x Q,\ \beta xy(x+y),\ x^2y,\ \beta x^3,\ \text{vanishing form},$$

where C and Q are any particular irreducible cubic and quadratic forms, e. g., $C = x^3 - xy^2 + \tau y^3$, for a suitable value of τ, and (§ 26)

$$Q = x^2 - \nu y^2 \quad (p > 2), \qquad Q = x^2 + xy + cy^2 \quad (p = 2);$$

while $\beta = 1$ if $p^n = 3^n$ or $3l + 2$; $\beta = 1, \epsilon, \epsilon^2$, if $p^n = 3l + 1$, ϵ being a primitive root of the field.

$GF[2]$ (invariants, § 23).

Canonical.	D	R	K
$x^3 - xy^2 + y^3$	1	0	1
$x(x^2 + xy + y^2)$	1	0	0
$xy(x + y)$	1	1	0
x^2y	0	0	1
x^3	0	1	0
Vanishing	0	0	0

$GF[2^2]$, $i^2 \equiv i + 1 \pmod 2$ (§ 23).

Canonical.	D	R	K
$\beta(x^3 - xy^2 + y^3)$	β^2	0	β
$\beta x(x^2 + xy + iy^2)$	$i\beta^2$	$i^2\beta$	$i^2\beta$
$\beta xy(x + y)$	β^2	0	0
x^2y	0	0	1
βx^3	0	β	0
Vanishing	0	0	0

$GF[3^n]$, $n = 1, 2$ (§ 22).

Canonical.	Δ	E	Γ
$x^3 - xy^2 + y^3$	1	1	0
$x(x^2 - \nu y^2)$	ν^3	0	0
$xy(x + y)$	1	0	0
x^2y	0	0	0
x^3	0	0	1
Vanishing	0	0	-1

$GF[5]$ (§ 24).

Canonical.	Δ	K	I	E
$x^3 - xy^2 + 2y^3$	2	-1	0	1
$x(x^2 - 2y^2)$	-1	0	0	0
$xy(x + y)$	2	2	0	0
x^2y	0	1	0	0
x^3	0	0	0	0
Vanishing	0	0	1	0

28. An inspection of the tables §§ 26, 27 shows that all the invariants given are necessary to characterize the canonical forms (since if one invariant is omitted, the others have equal values for some two canonical forms), and that no invariant is a rational function of the others (since any one takes different values when the others are equal). The only exception to these statements is the case of invariant E of the cubic form in the $GF[5]$; the characterization is complete without E; but the independence of E follows from the weights d (§ 24).

THE UNIVERSITY OF CHICAGO,
November, 1906.