GENERAL THEORY OF MODULAR INVARIANTS*

BY

LEONARD EUGENE DICKSON

Introduction.

The discovery of the fundamental theorems, established in the first part of the present paper, on the invariants of a general system of s forms under linear transformations in a finite field was the outcome of a new standpoint for the consideration of modular invariants. In former papers on the subject (cited later), the test for the invariance of a polynomial consisted in a more or less direct verification that it remained unaltered, up to a power of the determinant of the transformation, under the general linear group G in the field; instead of certain generators of the latter, the corresponding annihilators were employed. In the present paper, the transformation concept is employed only to furnish a complete set of non-equivalent classes $C_0, \cdots, C_{f-1}$ of systems of s forms under the group G. Thus the test for the absolute invariance of a polynomial P is that P shall take the same value for all systems of s forms in a class. It is shown in § 4 that the number of linearly independent absolute invariants equals the number f of classes under the total group G. In § 6 it is shown that the number of linearly independent invariants, including both absolute and relative, equals the number of classes under the group G_1 of transformations of determinant unity; it is furthermore specified which of the invariants under G_1 are invariants of the s forms.

The general theory is applied in §§ 8, 9, 16–19 to the determination of all the invariants of the general m-ary quadratic form in the Galois field of order p^n and in §§ 22–26 to the construction of all invariants of the binary cubic form† in the $GF[p^n]$. For the practical construction of the invariants, there is developed a uniform process, of function-theoretic nature, for the conversion of non-invariantive characterizations of the classes into invariantive characterizations. The intervening sections are devoted to the determination and characterization of the classes of the forms under investigation. A mere list of canonical types of forms is not sufficient. For m-ary quadratic forms in the $GF[2^n]$ such a list has been given‡ by the author; to obtain necessary and

* Presented to the Society (Chicago), January 1, 1909.

† Results for higher binary forms and for a pair of m-ary quadratic forms are to be published soon.

‡ American Journal of Mathematics, vol. 21 (1899), p. 222.

sufficient criteria for each class, a new theory for such forms has been constructed in §§ 10–15. Also for binary cubic forms, the case (§ 26) in which the modulus p equals 2 is more intricate than the general case $p > 2$. The nature of the invariants is quite different in the two cases, a result to be anticipated for quadratic forms, but rather surprising for cubic forms. The consequent assignment of such a large part of the present paper to the special case $p = 2$ was made not merely for the sake of completeness, but rather on account of the very prominent rôle which the linear groups with modulus 2 play in the applications * to geometry and in the general theory of linear groups.

Invariantive properties are often expressed in the algebraic theory by the vanishing of a covariant, or by means of an integer such as the rank of the matrix of a quadratic form. In the modular theory, every such property can be expressed by means of an explicit invariantive function of the coefficients. For quadratic forms illustrations of this point occur below. For a covariant K with the coefficients A_i,

$$I = \Pi(1 - A_i^{p^n-1})$$

is a modular invariant of the initial forms, in view of formula (1). We have $K \equiv 0$ or $K \not\equiv 0$ according as $I = 1$ or $I = 0$.

The method of the present paper for constructing modular invariants affords immediately important interpretations of these invariants.

It seems probable that modular invariants are destined to play a rôle in the theory of numbers comparable to that played by algebraic and differential invariants in higher algebra and geometry.

For a given set of forms, the theory of its modular invariants presents a doubly infinite number of problems, in view of the order p^n of the finite field. As compared with the use of annihilators employed in the earlier papers, the power of the present method may be inferred from the ease with which the various fields are now considered simultaneously. Hitherto the completeness of a proposed system of modular invariants for an infinitude of fields had not been established, even in so apparently simple a case as that of the binary quadratic form.

Existence theorems on modular invariants, §§ 1–5.

1. We shall make use of the following general theorem on interpolation in any finite field. *Within the $GF[p^n]$, there exists one and but one polynomial $\phi(x_1, \cdots, x_k)$ which has each exponent $\leqq p^n - 1$ and which takes prescribed values $v_{x_1,\ldots,x_k}$ for every set of elements $x_1, \cdots, x_k$ in the field.*

To proceed by induction, let the theorem be true for $k-1$ variables $x_2, \cdots, x_k$. Denote the elements of the field by $e_0, e_1, \cdots, e_\nu$, where $\nu = p^n - 1$. Then, for each value of i, there exists an unique polynomial $\phi(e_i, x_2, \cdots, x_k)$ with expo-

* JORDAN, *Traité des substitutions*, p. 313, p. 329; DICKSON, Annals of Mathematics, ser. II, vol. 6 (1905), pp. 141–150.

nents $\leqq \nu$, which takes the values $v_{e_0, e_1, \cdots, e_k}$ when $x_2, \cdots, x_k$ range over the field. We may now determine uniquely polynomials ψ_i in $x_2, \cdots, x_k$ such that

$$\psi_0 + \psi_1 x_1 + \cdots + \psi_\nu x_1^\nu \equiv \phi(x_1, x_2, \cdots, x_k)$$

will take the prescribed values $v_{x_1, \cdots, x_k}$. Indeed, the equations obtained by setting $x_1 = e_0, \cdots, e_\nu$ uniquely determine $\psi_0, \cdots, \psi_\nu$ as linear functions of the known polynomials $\phi(e_i, x_2, \cdots, x_k)$, since

$$\begin{vmatrix} 1 & e_0 & e_0^2 & \cdots & e_0^\nu \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & e_\nu & e_\nu^2 & \cdots & e_\nu^\nu \end{vmatrix} = \prod_{i<j} (e_i - e_j) \neq 0.$$

The argument applies also when $k = 1$, the ψ_i being parameters in the field. Hence the induction is complete.

Corollary. If two polynomials, with each exponent $\leqq p^n - 1$, are equal in $GF[p^n]$ for all sets of values of the variables, they are identical.

2. Consider a system of forms $F_1, \cdots, F_s$, where F_i is the general polynomial of degree d_i in m variables having as coefficients arbitrary parameters in the $GF[p^n]$. Assigning particular values to these parameters, we obtain a particular system S_1 of s forms. The distinct systems that can be obtained from S_1 by applying the various transformations of a given m-ary linear homogeneous group* L in the $GF[p^n]$ constitute the *class* C_1 of systems of forms conjugate, under L, with the given system S_1. Since the field is of finite order p^n, the order of L is finite, the number of systems in one class is finite, and there is a finite number of classes $C_0, C_1, \cdots, C_{f-1}$.

Selecting arbitrarily a system S_i from the class C_i, we shall say that $S_0, \cdots, S_{f-1}$ constitute a complete set of non-equivalent systems, under L, of s forms of degrees $d_1, \cdots, d_s$. When the S_i are relatively simple representatives of their classes, they are said to form a complete set of canonical types under L.

We shall expressly include the class, henceforth designated by C_0, which is composed of the system of forms all of whose coefficients are zero (see end of §4).

3. THEOREM. *Under a given linear homogeneous group L in the $GF[p^n]$, a system of forms has one and but one invariant† which takes prescribed values $v_0, \cdots, v_{f-1}$ for the various classes $C_0, \cdots, C_{f-1}$.*

By §1, there exists one and but one polynomial P which takes the prescribed values. If any chosen transformation of L replaces P by P', then P' takes the same values, so that $P' \equiv P$.

*The replacement of a group by any set of transformations is only an apparent generalization.

†A polynomial in the coefficients a_j of the forms, each a entering to a power $\leqq p^n - 1$, as may be assumed in view of $a^{p^n} = a$.

4. Denote by I_k the uniquely determined invariant which has the value unity for the class C_k and the value zero for every class $C_i (i \neq k)$. Since I_k completely characterizes the class C_k, it will be called the *characteristic invariant of the system of forms for the class C_k under the group L.*

Let $\sum c_i I_i \equiv 0$ be a linear homogeneous relation between the invariants I_i, with constant coefficients c_i in the $GF[p^n]$. Assign to the coefficients a_j of the given system of forms the values which they have in a particular system of forms belonging to the class C_k. Then $I_k = 1$, $I_i = 0$ $(i \neq k)$. Hence $c_k = 0$. Thus *the characteristic invariants are linearly independent in the field.*

Consider any invariant I of the system of forms under the group L. Let I have the value v_i for the class C_i. Then, by the corollary in § 1, $I \equiv \sum v_i I_i$. *Any invariant is a linear homogeneous function of the characteristic invariants with constant coefficients in the field.*

The essential part of the preceding results is contained in the

THEOREM. *The number of linearly independent invariants of a given system of s forms under a given linear homogeneous group L in the $GF[p^n]$ equals the number of non-equivalent classes under L.*

We note the non-homogeneous relation $\sum I_i = 1$. To compensate for the inclusion of the trivial invariant unity in counting the number of linearly independent invariants, we note that we have also included the trivial class C_0 of identically vanishing forms. For the latter,

$$I_0 = \prod_{i=1}^{\sigma} (1 - a_i^{p^n - 1}), \tag{1}$$

where $a_1, \cdots, a_\sigma$ is the aggregate of the coefficients of the s forms.

5. THEOREM. *Any set of $f - 1$ of the f characteristic invariants are independent, in the sense that no invariant of such a set equals a rational integral function of the remaining invariants of that set.*

Let the given set contain the $I_j (j \neq g)$, and assume that I_k equals a polynomial P in the $I_j (j \neq g, k)$. Since $I_i^2 = I_i$, $I_i I_j = 0$ $(i \neq j)$, $I_k = P$ may be given the form $I_k = c + \sum c_j I_j$ $(j \neq g, k)$. Replace c by $c \sum I_i$. The resulting homogeneous relation must be an identity. But, by the coefficients of I_k and I_g, $c = 1$, $c = 0$, respectively.

To give a second proof, consider representatives S_k and S_g of the classes C_k and C_g $(k \neq g)$. For the particular values of the coefficients in S_k and those in S_g, the invariant I_k takes different values (1 and 0), whereas each invariant $I_i (i \neq k, i \neq g)$ takes the same value zero. Hence I_k cannot equal a polynomial in the $I_i (i \neq k, g)$.

Absolute and relative invariants of a system of forms.

6. When L is the group G of all m-ary linear homogeneous transformations in the $GF[p^n]$, the invariants defined in §§ 3, 4 are called the *absolute invariants* of the s forms. When L is the group G_1 of all transformations of determinant unity, those invariants of G_1 which are multiplied by Δ^w under every transformation of determinant Δ are called the *relative invariants of weight w* of the s forms. A knowledge of the classes of forms under G_1 will be shown to be sufficient for the construction of all relative invariants.

Each class C_i under G separates into certain classes $C_{i1}, C_{i2}, \cdots, C_{ig_i}$ under G_1, which are transformed amongst themselves by all transformations of the $p^n - 1$ possible determinants. Hence $e_i = (p^n - 1)/g_i$ is the number of distinct determinants of the automorphs of a class C_{ij}. These e_i distinct values may be expressed as powers $\rho^\mu, \rho^{\mu'}, \cdots$ of a primitive root ρ of the field, where each exponent is $\geqq 0$. Let μ be the minimum positive exponent. Then $\mu' = k\mu + \nu (0 \leqq \nu < \mu)$. Let T and M be automorphs of determinants $\rho^{\mu'}$ and ρ^μ, respectively. The determinant of TM^{-k} is ρ^ν. Hence $\nu = 0$, so that every exponent is a multiple of μ. There are $(p^n - 1)/\mu$ distinct powers of ρ^μ. Hence $\mu = g_i$ and the e_i distinct determinants of the automorphs of C_{ij} are the distinct powers of a primitive root ρ^{g_i} of $x^{e_i} = 1$.

Under a linear transformation R of determinant ρ, the classes $C_{i1}, \cdots, C_{ig_i}$ undergo a permutation P. Since the determinant of R^{g_i} is a root of $x^{e_i} = 1$, P^{g_i} is the identity. Since ρ^{g_i} is the least positive power of ρ which gives a root of $x^{e_i} = 1$, P^{g_i} is the least positive power of P which leaves a class C_{ij} unaltered. Hence P permutes $C_{i1}, \cdots, C_{ig_i}$ in a single cycle. By assigning a suitable sequence to the $C_{ij} (j = 1, \cdots, g_i)$, we may set

$$P = \prod_i (C_{i1} C_{i2} \cdots C_{ig_i}).$$

Let a_t be the general coefficient of the given system of forms, a'_t the corresponding coefficient of the forms obtained by applying the transformation R. Thus R transforms a function $V(a)$ of the coefficients a_t into $V(a') = V'(a)$. Let V be an invariant under the group G_1, so that $V(a)$ has the same value for all systems of forms in a class C_{ij}. Now R transforms the class C_{ij} into the class C_{ij+1}, which is to be identified with C_{i1} when $j = g_i$. Hence the value of V for the class C_{ij+1} equals the value of the transformed function V' for the class C_{ij}. Let V be the characteristic invariant I_{ij+1}, so that I_{ij+1} has the value unity for the class C_{ij+1} and the value zero for all the remaining classes under G_1. Hence I'_{ij+1} equals unity for C_{ij} and zero for the remaining classes. Thus I'_{ij+1} equals the characteristic invariant I_{ij} for the class C_{ij}. Hence

$$R \sim \prod_i (I_{ig_i} \cdots I_{ij+1} I_{ij} \cdots I_{i2} I_{i1}).$$

Now $\gamma_i = \rho^{e_i}$ belongs to the exponent g_i. The g_i functions

$$\Sigma_{ik} = I_{i1} + \gamma_i^k I_{i2} + \gamma_i^{2k} I_{i3} + \cdots + \gamma_i^{(g_i-1)k} I_{ig_i} \quad (k = 0, 1, \cdots, g_i - 1) \tag{2}$$

are linearly independent functions of $I_{i1}, \cdots, I_{ig_i}$. The

$$g = g_0 + g_1 + \cdots + g_{f-1}$$

characteristic invariants $I_{ij} (j = 1, \cdots, g_i;\ i = 0, 1, \cdots, f-1)$ are linearly independent (§ 4). Hence the g invariants Σ_{ik} are linearly independent. Now R replaces Σ_{ik} by $\gamma_i^k \Sigma_{ik}$. Thus R^t, of determinant ρ^t, multiplies Σ_{ik} by

$$\gamma_i^{kt} = (\rho^t)^{ke_i}.$$

Hence Σ_{ik} is a relative invariant of weight ke_i.

Let $K = \sum c_{ij} I_{ij}$ be any relative invariant of weight w. Under the transformation R, of determinant ρ, K becomes $\rho^w K$, while I_{ij} becomes I_{ij-1} or I_{ig_i} according as $j > 1$ or $j = 1$. Hence for every $i, j\ (j > 1)$,

$$c_{ij} = \rho^w c_{ij-1}, \qquad c_{i1} = \rho^w c_{ig_i}.$$

Unless every $c_{ij} = 0$, we must have $\rho^{wg_i} = 1$, so that wg_i is a multiple of $p^n - 1 = e_i g_i$, whence $w = ke_i$. In the latter case, $\rho^w = \gamma_i^k$,

$$\sum_{j=1}^{g_i} c_{ij} I_{ij} = c_{i1} \sum_{j=1}^{g_i} \gamma_i^{k(j-1)} I_{ij} = c_{i1} \Sigma_{ik}.$$

Hence K is a linear function of those Σ_{ik} which are of weight w.

We have now established the following

THEOREM. *For a system of s general forms of given degrees in m variables, with arbitrary coefficients in the $GF[p^n]$, the number of linearly independent invariants, absolute and relative, equals the number g of the classes of the systems of forms under the group G_1 of m-ary linear transformations of determinant unity.*

Of the f classes C_i under the total m-ary linear group G, let the class C_i separate into g_i classes C_{ij} under G_1. Let k be any integer such that $0 \leqq k < g_i$. Then, for each i, there exist g_i invariants Σ_{ik}, given by (2), of weights ke_i, where $e_i = (p^n - 1)/g_i$. The $g = g_0 + \cdots + g_{f-1}$ invariants Σ_{ik} are linearly independent. Any invariant of weight w of G is a linear homogeneous function of those of the invariants Σ_{ik} which are of weight w.*

* By introducing notations to indicate which of the numbers e_i are equal, we may readily give an explicit formula for the total number of invariants, as well as the number of relative invariants of each weight. For example, the number of absolute invariants is $p^{n'}$.

The classes of quadratic forms q_m in the $GF[p^n]$, $p>2$.

7. First, let the field be the $GF[p^n]$, $p>2$, and consider the form

$$q_m=\sum_{i,j=1}^{m}\beta_{ij}x_ix_j \qquad (\beta_{ji}=\beta_{ij}), \tag{3}$$

whose coefficients are arbitrary parameters in the field. Then

$$D=|\beta_{ij}| \tag{3'}$$

is called the determinant or discriminant of q_m. For particular values in the field for the coefficients, q_m is said to be of rank zero if every $\beta_{ij}=0$, and of rank $r>0$ if at least one minor of order r of D is not zero, while every minor of order greater than r vanishes.

Of various methods leading to a classification of quadratic forms that due to KRONECKER * is best suited for the present application; his theory is seen to hold for any field not having modulus 2. It is based on two theorems. First, in a symmetrical matrix (β_{ij}) of rank $r>0$, not every principal minor of order r vanishes. Next, if the principal minor

$$D_{k_1,\cdots,k_r}\equiv|\beta_{k_sk_t}| \qquad (s,t=1,\cdots,r) \tag{4}$$

is not zero, while every minor of order $>r$ vanishes, there exists a linear transformation of determinant unity which replaces q_m by

$$\sum_{s,t=1}^{r}\beta_{k_sk_t}x_{k_s}x_{k_t}. \tag{5}$$

A proof of the last statement will be given in a form convenient for comparison with the treatment in § 14 of the case in which the modulus is 2. After rearranging the variables, we may assume that, instead of (4),

$$|\beta_{ij}|\neq 0 \qquad (i,j=1,\cdots,r). \tag{4'}$$

To q_m we apply the transformation, of determinant unity,

$$x_i=x_i'+c_ix_m' \ (i\leqq r), \qquad x_i=x_i' \ (i>r),$$

and obtain the form

$$\sum_{i,j=1}^{m-1}\beta_{ij}x_i'x_j'+2\sum_{j=1}^{m-1}B_{jm}x_j'x_m'+Ax_m'^2,$$

$$B_{jm}\equiv\sum_{i=1}^{r}\beta_{ij}c_i+\beta_{jm}, \qquad A\equiv\sum_{j=1}^{r}B_{jm}c_j+B_{mm}.$$

In view of (4'), $c_1,\cdots,c_r$ can be uniquely determined so that $B_{jm}=0$ $(j\leqq r)$. In the latter and B_{km} $(r<k\leqq m)$, the determinant of the coefficients of $c_1,\cdots,c_r,1$ is the minor of β_{km} in

$$|\beta_{ij}| \qquad (i,j=1,\cdots,r,k,m).$$

* *Werke*, vol. 1, p. 166, p. 357. Cf. BÔCHER, *Introduction to Higher Algebra*, p. 58, p. 139; GUNDELFINGER, Journal für reine u. angewandte Mathematik, vol. 91 (1881), p. 221.

This minor of order $r+1$ is zero by hypothesis. Hence $B_{km}=0\,(k>r)$, $A=0$.

Repetitions of the process lead to the form

$$\sum_{i,j=1}^{r}\beta_{ij}x_ix_j. \tag{5}$$

By a linear transformation of determinant unity, form (5) or (5′), of non-vanishing determinant ρ, can be transformed into *

$$\sum_{i=1}^{r-1}x_i^2+\rho x_r^2; \tag{6}$$

while a linear transformation of determinant Δ replaces (5′) by a form of determinant $\Delta^2\rho$. Hence two forms (6_1) and (6_2) are equivalent under the group G_1 of all r-ary linear transformations of determinant unity only when $\rho_1=\rho_2$; but are equivalent under the total group G if, and only if, ρ_1/ρ_2 is a square in the field.

Under the total group G, the class to which the form (6), with $\rho\neq 0$, belongs will be designated by $C_{r,1}$ or $C_{r,-1}$ according as ρ is a square or a not-square. Thus a complete set of non-equivalent classes of m-ary quadratic forms in the $GF[p^n]$, $p>2$, is given by

$$C_0,\ C_{r,\pm 1} \qquad (r=1,\cdots,m). \tag{7}$$

Hence a particular form q_m of rank $r>0$ belongs to the class $C_{r,\delta}$, where $\delta=D^{\mu}_{k_1,\ldots,k_r}$, $D_{k_1,\ldots,k_r}$ being a non-vanishing principal minor of order r of $|q_m|$, and $\mu=\frac{1}{2}(p^n-1)$.

The invariants of a quadratic form in the $GF[p^n]$, $p>2$.

8. We proceed to construct the characteristic absolute invariants I_0, $I_{r,\pm 1}$ of the general quadratic form q_m in the $GF[p^n]$, $p>2$, which correspond to the classes (7). By (1),

$$I_0=\Pi(1-\beta_{ij}^{2\mu}) \qquad (i,j=1,\cdots,m;\ i\leqq j). \tag{8}$$

Instead of dealing initially with the $I_{r,\pm 1}$, we first construct an absolute invariant A_r which takes the value $+1$ for the class $C_{r,+1}$, the value -1 for the class $C_{r,-1}$, and the value 0 for the remaining classes C_0, $C_{s,\pm 1}$ $(s\neq r)$. Then

$$I_{r,+1}=\tfrac{1}{2}(A_r^2+A_r),\qquad I_{r,-1}=\tfrac{1}{2}(A_r^2-A_r). \tag{9}$$

For $r=m$, we evidently have

$$A_m=D^{\mu} \qquad [\mu=\tfrac{1}{2}(p^n-1)]. \tag{10}$$

For $0<r<m$, the results of § 7 show (*a*) that $A_r=0$ if any principal minor of order $>r$ is not zero; (*b*) that $A_r=0$ if every principal minor of order $\geqq r$ vanishes; and (*c*) that $A_r=M^{\mu}$ if a particular principal minor M of order r is not zero, while every principal minor of order $>r$ vanishes. In view of the

* DICKSON, *Linear Groups*, pp. 157–158.

first statement (a), we have the identity

$$A_r \equiv \alpha_r \Pi (1 - d^{2\mu}), \tag{11}$$

where d ranges over the principal minors of order $> r$, while α_r is a polynomial in the β_{ij} to be determined. Let $M_1, \cdots, M_\rho$ denote the $\rho = C_r^m$ principal minors of order r, arranged in some definite sequence. In view of the third statement (c),

$$\alpha_r = M_i^\mu \qquad (\text{for every } d = 0,\ M_i \neq 0). \tag{12}$$

For $i = 1$, the latter yields the identity

$$\alpha_r \equiv M_1^\mu + K_1(1 - M_1^{2\mu}) \qquad (\text{for every } d = 0). \tag{13}$$

To determine K_1, consider any set of values of the β_{ij} which make each $d = 0$, $M_1 = 0$, $M_2 \neq 0$. Then by (12) for $i = 2$, and (13), $M_2^\mu = K_1$. Thus

$$K_1 \equiv M_2^\mu + K_2(1 - M_2^{2\mu}) \qquad (\text{for every } d = 0,\ M_1 = 0).$$

Then (13) yields* (14) for the case $j = 2$:

$$\begin{aligned} \alpha_r \equiv\ & M_1^\mu + M_2^\mu(1 - M_1^{2\mu}) + M_3^\mu(1 - M_1^{2\mu})(1 - M_2^{2\mu}) + \cdots \\ & + M_j^\mu(1 - M_1^{2\mu}) \cdots (1 - M_{j-1}^{2\mu}) + K_j(1 - M_1^{2\mu}) \cdots (1 - M_j^{2\mu}), \end{aligned} \tag{14}$$

for every set β_{ij} such that each $d = 0$. For the general step in the derivation of (14), we proceed by induction from $j = t$ to $j = t + 1$, assuming that (14) holds for $j = t$. We consider any set β_{ij} for which each $d = 0$, $M_i = 0\,(i \leqq t)$, $M_{t+1} \neq 0$. Then by (12) for $i = t + 1$, and (14) for $j = t$, $M_{t+1}^\mu = K_t$. Thus

$$K_t \equiv M_{t+1}^\mu + K_{t+1}(1 - M_{t+1}^{2\mu}).$$

for all sets β_{ij} such that each $d = 0$, $M_i = 0\,(i \leqq t)$. Upon substituting this value of K_t in (14), for $j = t$, we obtain (14), for $j = t + 1$.

Having established (14) for every $j \leqq \rho$, where ρ is the total number of the minors M, we consider (14) for $j = \rho$. Let the β_{ij} have any values such that $M_i = 0\,(i \leqq \rho)$ and every $d = 0$. By the second statement (b) preceding (11), $A_r = 0$. Thus, by (14) for $j = \rho$, $0 = K_\rho$. Independently of the restriction that every $d = 0$, (11) and (14) now lead to the result that *the explicit expression for the absolute invariant* A_r *is*

$$A_r = \{M_1^\mu + M_2^\mu(1 - M_1^{2\mu}) + \cdots + M_\rho^\mu(1 - M_1^{2\mu}) \cdots (1 - M_{\rho-1}^{2\mu})\} \Pi (1 - d^{2\mu}), \tag{15}$$

where d *ranges over the principal minors of orders* $> r$, *while* $M_1, \cdots, M_\rho$ *denote the principal minors of order* r *taken in any sequence.*

The range of d may be restricted to the principal minors of orders $r + 1, r + 2$.

* The restriction $M_1 = 0$ or K_1 is suppressed in (14) in view of $(1 - M_1^{2\mu})M_1 = 0$.

We note several forms of invariant (15) when $m=2, r=1$. In that case,

$$(16)\quad A_1=(\beta_{22}^{\mu}+\beta_{11}^{\mu}-\beta_{22}^{2\mu}\beta_{11}^{\mu})(1-D^{2\mu})=(\beta_{11}^{\mu}+\beta_{22}^{\mu}-\beta_{11}^{2\mu}\beta_{22}^{\mu})(1-D^{2\mu}),$$

$$(17)\qquad A_1=\tfrac{1}{2}(2-\beta_{11}^{\mu}\beta_{22}^{\mu})(\beta_{11}^{\mu}+\beta_{22}^{\mu})(1-D^{2\mu}).$$

Applying the useful congruence

$$(18)\quad (a-b)^{2\mu}\equiv\sum_{i=0}^{2\mu}a^i b^{2\mu-i}=(a^{\mu}+b^{\mu})\sum_{i=0}^{\mu}a^i b^{\mu-i}-a^{\mu}b^{\mu}\pmod p,$$

for $a=\beta_{11}\beta_{22}$, $b=\beta_{12}^2$, we get

$$D^{2\mu}-1=(\beta_{11}^{\mu}\beta_{22}^{\mu}+1+\beta_{12}^{2\mu}-1)\sum_{i=1}^{\mu}\beta_{11}^{i}\beta_{22}^{i}\beta_{12}^{2\mu-2i}-\beta_{11}^{\mu}\beta_{22}^{\mu}\beta_{12}^{2\mu}-1$$

$$=(\beta_{11}^{\mu}\beta_{22}^{\mu}+1)(-1+\Sigma),$$

since $(\beta_{12}^{2\mu}-1)\Sigma=(\beta_{12}^{2\mu}-1)\beta_{11}^{\mu}\beta_{22}^{\mu}$. Hence (16_1) gives*

$$(19)\qquad A_1=(\beta_{11}^{\mu}+\beta_{22}^{\mu})\left(1-\sum_{i=0}^{\mu}\beta_{11}^{i}\beta_{22}^{i}\beta_{12}^{2\mu-2i}\right).$$

9. Under the group G_1 of all m-ary linear transformations of determinant unity in the $GF[p^n]$, $p>2$, a complete set of non-equivalent classes of m-ary quadratic forms is given by

$$(20)\qquad C_0,\ C_{r,\pm 1}(r=1,\cdots,m-1),\ C_{m,\rho}\ (\rho\text{ arbitrary}\neq 0),$$

where $C_{m,\rho}$ is the class containing (6) for $r=m$. In that case, different ρ's give non-equivalent forms under G_1 (§ 7). But for $r<m$, (6) is transformed into a like form, with the parameter ρa^2, by the transformation

$$x_r=ax_r',\qquad x_m=a^{-1}x_m',\qquad x_i=x_i'\qquad (i\neq r,m)$$

of determinant unity. Let ϕ be a relative invariant of weight w of q_m, so that ϕ becomes $\Delta^w\phi$ under a transformation of determinant Δ. But each class is transformed into itself by every transformation of determinant ± 1 (in particular, by the one changing the sign of x_1). Hence w is even (cf. § 6).

Of the classes (7) under the total group G, classes $C_{m,\pm 1}$ alone separate into subclasses $C_{m,\rho}$ under G_1. If ϕ has the value v for a class $C_{m,\rho}$, then ϕ has the value $\Delta^w v$ for the class $C_{m,\rho\Delta^2}$ obtained from $C_{m,\rho}$ by a transformation of determinant Δ. Hence, if ρ'/ρ is a square, the value of ϕ for $C_{m,\rho'}$ equals $(\rho'/\rho)^{w/2}$ times its value for $C_{m,\rho}$. Thus arbitrary values can be assigned to ϕ for just one of the $\mu=\frac{1}{2}(p^n-1)$ classes $C_{m,\rho}$ in which ρ is a square, and for just one of the μ classes $C_{m,\rho}$ in which ρ is a not-square. When these two assigned values are zero, the invariant is absolute and has been constructed in § 8. The

* Invariant (19) is the negative of Q, these Transactions, vol. 8 (1907), pp. 211, 217, 218.

same is true if a non-vanishing value be assigned to ϕ for one of the classes C_0, $C_{r,\pm 1}$ $(r<m)$. Hence to obtain a non-absolute invariant ϕ of weight 2δ, where $0<2\delta<p^n-1$, we must assign to ϕ the value zero for C_0, $C_{r,\pm 1}$ $(r<m)$, and values not both zero for two classes $C_{m,\rho}$, in one of which ρ is a particular square, in the other ρ is a particular not-square. Since the values of ϕ for every class are then uniquely determined, an unique polynomial ϕ can be constructed (§ 1). Hence there are exactly two linearly independent invariants of weight 2δ. But, if D is the determinant of q_m, then D^δ and $D^{\delta+\mu}$ are linearly independent invariants of weight 2δ.

Combining the present results with those in § 8, we obtain the

THEOREM. *A complete set of linearly independent invariants of the m-ary quadratic form in the GF*$[p^n]$, $p>2$, *is given by the* $2m+1$ *characteristic absolute invariants* I_0, $I_{r,\pm 1}$ $(r=1,\cdots,m)$, *and the* p^n-3 *relative invariants* D^δ, $D^{\delta+\mu}$ $(\delta=1,\cdots,\mu-1)$, *where* $\mu=\frac{1}{2}(p^n-1)$. *As an alternative set, we may take*

$$(21)\qquad I_0,\ A_r,\ A_r^2\ (r=1,\cdots,m-1),\qquad D^k\ (k=1,\cdots,p^n-1).$$

The invariants mentioned are defined by (3'), (8), (9), (10), (15).

The product of any two invariants of the first set can be reduced to a linear combination of those in the first set by means of the relations*

$$(22)\qquad \begin{gathered} D^{2\mu+1}=D,\quad I_0D=I_{r,\pm 1}D=0\,(r<m),\quad I_{m,\pm 1}D=\tfrac{1}{2}(D\pm D^{\mu+1}),\\ I^{\frac{1}{2}}=I,\qquad II'=0\,(I \text{ and } I' \text{ any pair of the } I_0,\ I_{r,\pm 1}).\end{gathered}$$

For the set (21), the following relations suffice:

$$(23)\quad D^{2\mu+1}=D,\ I_0^2=I_0,\ A_r^3=A_r,\ I_0A_r=I_0D=A_rD=A_rA_s=0\,(r\neq s).$$

Reduction of quadratic forms in the GF$[2^n]$, §§ 10–15.

10. In view of the application to be made for fields having the modulus 2, we consider some algebraic properties of the quadratic form

$$(24)\qquad Q_m=\sum\beta_{ij}x_ix_j+\sum b_jx_j^2\qquad (i,j=1,\cdots,m\,;\ i<j).$$

Its discriminant D and a related skew-symmetric determinant d are

$$D=\begin{vmatrix} 2b_1 & \beta_{12} & \cdots & \beta_{1m}\\ \beta_{12} & 2b_2 & \cdots & \beta_{2m}\\ \cdot & \cdot & \cdot & \cdot\\ \beta_{1m} & \beta_{2m} & \cdots & 2b_m\end{vmatrix},\qquad d=\begin{vmatrix} 0 & \beta_{12} & \cdots & \beta_{1m}\\ -\beta_{12} & 0 & \cdots & \beta_{2m}\\ \cdot & \cdot & \cdot & \cdot\\ -\beta_{1m} & -\beta_{2m} & \cdots & 0\end{vmatrix}.$$

Now $d\equiv 0$ for m odd; while, for m even, d equals the square of the pfaffian †

* These follow at once from the values of the invariants for the various classes.

† We consider pfaffians in the β_{ij} exclusively. Note that [12] denotes β_{12}.

$[12\cdots m]$. Since corresponding elements of D and d differ by multiples of 2,

$$(25)\qquad D = 2S_m \quad (m \text{ odd}), \qquad D = [12\cdots m]^2 + 2R \quad (m \text{ even}).$$

If Q_m becomes Q'_m under a linear homogeneous transformation of determinant Δ, the discriminant D' of Q'_m equals $\Delta^2 D$. Hence, for m odd, S_m is invariant up to the factor Δ^2; while, for m even,

$$[12\cdots m]_{\beta'} = \Delta\,[12\cdots m]_\beta + 2\rho,$$

since the β'_{ij} involve only even multiples of the b_k.

11. Let the coefficients of Q_m belong to the $GF[2^n]$. If any coefficient be increased by a multiple of 2, D is increased by a multiple of 4; thus S_m and $[12\cdots m]$ are increased by multiples of 2. It will prove convenient to employ the notation $\{12\cdots m\}$ for S_m. *According as m is even or odd,* $[12\cdots m]$ *or* $\{12\cdots m\}$ *is an invariant* of* (24) *in the* $GF[2^n]$.

We shall consider two methods of normalizing Q_m under linear transformation in the $GF[2^n]$, each possessing certain advantages. The contrast between the two methods is analogous to that between the methods of LAGRANGE and KRONECKER in the algebraic theory. The present theory is essentially different from the algebraic theory; this is due partly to the fact that the terms involving the squares of the variables hold themselves aloof under transformation.

12. If every $\beta_{ij} = 0$, Q_m is the square of $\sum b_j^{\frac{1}{2}} x_j$ in the $GF[2^n]$ and either vanishes identically or can be transformed into x_1^2. If not every β_{ij} vanishes, let $\beta_{12} \neq 0$, $m > 2$. Under the transformation

$$(26)\quad x'_1 = x_1 + \sum_{i=3}^{m} \beta_{2i} x_i, \qquad x'_2 = x_2 + \sum_{i=3}^{m} \beta_{1i} x_i, \qquad x'_j = \beta_{12} x_j \quad (j = 3, \cdots, m),$$

of determinant β_{12}^{m-2}, $Q_m(x')$ becomes †

$$(27)\quad \beta_{12} x_1 x_2 + \beta_{12} \sum [12ij] x_i x_j + b_1 x_1^2 + b_2 x_2^2 + \sum \{12i\} x_i^2 \quad (i, j = 3, \cdots, m;\ i < j),$$

where $[12ij]$ is a pfaffian, while

$$\{12i\} = \beta_{12}\beta_{1i}\beta_{2i} + b_1\beta_{2i}^2 + b_2\beta_{1i}^2 + b_i\beta_{12}^2,$$

so that $\{123\}$ is the semi-discriminant of Q_3. Hence, for $m = 3$ or 4, the vanishing of the invariant $\{123\}$ or $\{1234\}$ is a necessary and sufficient condition that Q_3 or Q_4, with $\beta_{12} \neq 0$, shall be tranformable into a binary or ternary form, respectively.

Next, let $m > 4$. If every $[12ij] = 0$, (27) can be transformed into a ternary form. In the contrary case, let $[1234] \neq 0$ and apply the following discussion for $l = 2$, with $[1\cdots 0]$ replaced by unity, $\{1\cdots 0k\}$ replaced by b_k.

*American Journal of Mathematics, vol. 30 (1908), p. 265.

† Ibid., p. 264, formula (2), with x_3 replaced by $c_{12}x_3$.

The general step in the reduction process will be made by induction. Let l be an integer $\leqq m/2$ such that not every pfaffian of order $2l$ vanishes; in particular, let

$$[12] \neq 0,\ [1234] \neq 0,\ \cdots,\ [1\cdots 2l] \neq 0. \tag{28}$$

We assume that, after $l-1$ steps, Q_m has been transformed into

$$\begin{aligned}&[12]x_1x_2+[12][1234]x_3x_4+[1234][1\cdots 6]x_5x_6+\cdots\\&+[1\cdots 2l-4][1\cdots 2l-2]x_{2l-3}x_{2l-2}+[1\cdots 2l-2]\textstyle\sum[1\cdots 2l-2\,ij]x_ix_j\\&+b_1x_1^2+b_2x_2^2+\{123\}x_3^2+\{124\}x_4^2+\cdots+\{1\cdots 2l-4\,2l-3\}x_{2l-3}^2\\&+\{1\cdots 2l-4\,2l-2\}x_{2l-2}^2+\textstyle\sum\{1\cdots 2l-2\,i\}x_i^2\quad(i,j=2l-1,\cdots,m;\ i<j),\end{aligned} \tag{29}$$

by a transformation of determinant

$$[12]^2[1234]^2\cdots[1\cdots 2l-4]^2[1\cdots 2l-2]^{m-2l+2}. \tag{30}$$

To (29), with each x accented, we apply the transformation

$$\begin{aligned}x'_{2l-1}=x_{2l-1}+t\sum_{i=2l+1}^{m}[1\cdots 2l-2\,2li]x_i,\quad x'_{2l}=x_{2l}+t\sum_{i=2l+1}^{m}[1\cdots 2l-2\,2l-1i]x_i,\\ x'_j=t[1\cdots 2l]x_j\qquad(j=2l+1,\cdots,m),\end{aligned} \tag{31}$$

where $t=[1\cdots 2l-2]^{-1}$. This alters only the terms of (29) under the two summation signs. These terms are replaced by

$$\begin{aligned}&[1\cdots 2l-2][1\cdots 2l]x_{2l-1}x_{2l}+[1\cdots 2l]\textstyle\sum\sigma_{ij}x_ix_j\\&+\{1\cdots 2l-2\,2l-1\}x_{2l-1}^2+\{1\cdots 2l-2\,2l\}x_{2l}^2+\textstyle\sum f_ix_i^2\\&\qquad(i,j=2l+1,\cdots,m;\ i<j),\end{aligned}$$

where

$$\begin{aligned}\sigma_{ij}=t\{&[1\cdots 2l-2\,2li][1\cdots 2l-2\,2l-1j]\\&+[1\cdots 2l-2\,2lj][1\cdots 2l-2\,2l-1i]+[1\cdots 2l][1\cdots 2l-2\,ij]\},\end{aligned} \tag{32}$$

$$\begin{aligned}f_i=t^2\big(&[1\cdots 2l-2\,2li]^2\{1\cdots 2l-2\,2l-1\}\\&+[1\cdots 2l-2\,2l-1i]^2\{1\cdots 2l-2\,2l\}+[1\cdots 2l]^2\{1\cdots 2l-2\,i\}\\&+[1\cdots 2l-2][1\cdots 2l][1\cdots 2l-2\,2l-1i][1\cdots 2l-2\,2li]\big).\end{aligned} \tag{33}$$

Hence the induction will be complete if it is shown that

$$\sigma_{ij}=[1\cdots 2l\,ij],\qquad f_i=\{1\cdots 2l\,i\}. \tag{34}$$

The product of the determinant of (31) by (30) is clearly

$$[12]^2[1234]^2\cdots[1\cdots 2l-2]^2[1\cdots 2l]^{m-2l}. \tag{35}$$

Although (34_1) may be established by means of the algebraic theory of

pfaffians, we shall prove both parts of (34) by applying the invariance of the discriminant or semi-discriminant, up to a factor Δ^2, under a transformation of determinant Δ in the $GF[2^n]$. We note that the preceding development is valid for any $m \geqq 2l$. First, we take $m = 2l+2$. Then the discriminant of the final quadratic form is seen to equal $B^2\sigma^2_{2l+1\,2l+2}$, where B is the product (35), the final exponent being 2. But the discriminant of Q_{2l+2} is $[1 \cdots 2l+2]^2$. Hence (34_1) is true for $i = 2l+1$, $j = 2l+2$, and therefore for any i, j exceeding $2l$. Next for $m = 2l+1$, the semi-discriminant of the final form equals $P^2 f_{2l+1}$, where P is the product (35) with the last exponent unity. But the semi-discriminant of Q_{2l+1} is $\{1 \cdots 2l+1\}$. Hence (34_2) holds for $i = 2l+1$, and therefore for every $i > 2l$.

We make the further assumption that every pfaffian of order $> 2l$ vanishes. The form reached above thus becomes

$$(36)\qquad \sum_{s=1}^{l}[1\cdots 2s-2][1\cdots 2s]x_{2s-1}x_{2s}+\sum_{i=2l+1}^{m}\{1\cdots 2l\,i\}x_i^2 + \sum_{s=1}^{l}\{1\cdots 2s-2\;2s-1\}x_{2s-1}^2+\sum_{s=1}^{l}\{1\cdots 2s-2\;2s\}x_{2s}^2.$$

To this form we apply the transformation

$$x_{2s}=[1\cdots 2s]^{-1}x'_{2s},\quad x_{2s-1}=[1\cdots 2s-2]^{-1}x'_{2s-1}\,(s\leqq l),\quad x_i=x'_i\,(i>2l),$$

and then drop the accents on the x'. We get

$$(37)\qquad \sum_{s=1}^{l}x_{2s-1}x_{2s}+\sum_{i=1}^{2l}\delta_i x_i^2+\sum_{i=2l+1}^{m}\{1\cdots 2l\,i\}x_i^2,$$

$$(38)\qquad \begin{aligned}\delta_{2s-1}&=[1\cdots 2s-2]^{-2}\{1\cdots 2s-2\;2s-1\},\\ \delta_{2s}&=[1\cdots 2s]^{-2}\{1\cdots 2s-2\;2s\}\end{aligned}\qquad (s=1,\cdots,l)$$

The product of the determinant of this transformation by (35) is

$$(39)\qquad [1\cdots 2l]^{m-2l-1}$$

Hence Q_m is transformed into (37) by a transformation of determinant (39).

First, let at least one of the $\{1\cdots 2l\,i\}$ be not zero, where $i > 2l$, thus implying that $m > 2l$. Then, by (37), Q_m can be transformed into

$$(40)\qquad \sum_{s=1}^{l}x_{2s-1}x_{2s}+cx_{2l+1}^2\quad (c=1 \text{ if } m>2l+1,\ c=\{1\cdots 2l+1\} \text{ if } m=2l+1),$$

by a transformation of determinant unity. Under the group of transformations of all determinants, (40) with $m = 2l+1$ is equivalent to a like form with $c = 1$. In view of the invariance of the semi-discriminant, (40) can not be transformed into a form on fewer than $2l+1$ variables. Now $\{1\cdots 2l\,i\} \neq 0$

implies, in view of (33) and (34), that not every pfaffian of order $2l$ is zero.

Hence necessary and sufficient conditions that Q_m shall be transformable into a form on $2l+1$ variables, but not into a form on $2l$ variables, are that every pfaffian of order $>2l$ vanishes and that not every principal semi-minor $\{i_1 i_2 \cdots i_{2l+1}\}$ of order $2l+1$ vanishes.

Next, let every $\{1 \cdots 2l\, i\} = 0$. Then by a linear transformation of determinant unity, (37) can be transformed * into

$$\sum_{s=1}^{l} x_{2s-1}x_{2s} + x_1^2 + \delta x_2^2, \qquad \delta \equiv \sum_{s=1}^{l} \delta_{2s-1}\delta_{2s}. \tag{41}$$

Now $x_1x_2 + x_1^2 + \delta x_2^2$ is reducible or irreducible in the $GF[2^n]$ according as $\chi(\delta) = 0$ or 1, where

$$\chi(\delta) = \sum_{i=0}^{n-1} \delta^{2^i} \qquad \chi^2 \equiv \chi. \tag{42}$$

The forms (41) with $\chi(\delta) = 0$ are all equivalent to

$$\sum_{s=1}^{l} x_{2s-1}x_{2s} \tag{43}$$

under the group G_1 of linear transformations of determinant unity. The forms (41) with $\chi(\delta) = 1$ are equivalent under G_1, but no one of them can be transformed into (43). The reduction of Q_m to (37) was effected by a transformation of determinant (39). If $m > 2l$, Q_m can be transformed into (41) within G_1; but if $m = 2l$, the canonical form within G_1 may be taken to be (41) with one of the variables multiplied by $[1 \cdots 2l]$. Among the results established, we mention the following:

Necessary and sufficient conditions that Q_m shall be transformable into a form on $2l$ variables, but not into a form on $2l-1$ variables, are that every pfaffian of order $>2l$ and every $\{i_1 \cdots i_{2l+1}\}$ shall vanish, but not every pfaffian of order $2l$.

13. A quadratic form in the $GF[2^n]$ may be said to be of *rank r* if, of the principal minors of even order and the algebraic halves of the principal minors of odd order, those of order $>r$ vanish, but not all of order r vanish. As an equivalent definition we may say that Q_m is of odd rank $2l+1$ if every † $[i_1 \cdots i_{2l+2}]$ but not every $\{i_1 \cdots i_{2l+1}\}$ vanishes; that Q_m is of even rank $2l$ if every $[i_1 \cdots i_{2l+2}]$ and every ‡ $\{i_1 \cdots i_{2l+1}\}$ but not every $[i_1 \cdots i_{2l}]$ vanishes.

In comparing these definitions with the algebraic definition of the rank of a quadratic form or symmetrical matrix, we note that a principal minor of odd

* American Journal of Mathematics, vol. 30 (1908), p. 266, § 6.

† Then every pfaffian of order $>2l$ vanishes, also every $\{i_1 \cdots i_t\}$, $t > 2l+2$, by (33), (34).

‡ The vanishing of these does not imply that of the pfaffians of order $\geqq 2l+2$, as shown by the example $x_1x_2 + x_3x_4 + \cdots + x_{2l+1}x_{2l+2}$.

order vanishes identically modulo 2, so that we have introduced their algebraic halves; furthermore, when a principal minor M of even order vanishes in the $GF[2^n]$, all the first minors * M_{ij} of M also vanish, since $M_{ii}M_{jj} - M_{ij}^2$ is a multiple of M and since M_{ii} is multiple of 2.

From the results stated in italics in § 12 we have the

THEOREM. *A quadratic form in the $GF[2^n]$ can be transformed into a form on r variables, but not into one on $r-1$ variables, if and only if its rank is r.*

Second method of reduction of a quadratic form.

14. We consider a second method † of normalizing a quadratic form (24) in the $GF[2^n]$. If $[1\cdots m] \neq 0$, so that m is an even number $2l$, Q_m is already of the form (50). In the contrary case there is some integer $l < m/2$ such that every pfaffian of order $> 2l$, but not every pfaffian of order $2l$, vanishes. We assume that $l > 0$, thus excluding the rather trivial case in which every $\beta_{ij} = 0$. After rearranging the variables, we may set $[1\cdots 2l] \neq 0$. To Q_m we apply the transformation

$$x_i = x_i' + c_i x_m' \ (i = 1, \cdots, 2l), \qquad x_i = x_i' \ (i = 2l+1, \cdots, m).$$

Let $\beta_{ii} = \beta_{ij}$, $\beta_{ii} = 0$. Then the resulting form is

$$(44) \qquad \sum_{i<j}^{1,\cdots,m-1} \beta_{ij} x_i' x_j' + \sum_{j=1}^{m-1} B_{jm} x_j' x_m' + \sum_{i=1}^{m-1} b_i x_i'^2 + E_m x_m'^2,$$

$$(45) \quad B_{jm} = \sum_{i=1}^{2l} \beta_{ij} c_i + \beta_{jm}, \qquad E_m = \sum_{j=1}^{2l} \beta_{jm} c_j + \sum_{i<j}^{1,\cdots,2l} \beta_{ij} c_i c_j + \sum_{i=1}^{2l} b_i c_i^2 + b_m.$$

By choice of the c_i, we may make $B_{jm} = 0$ $(j = 1, \cdots, 2l)$. In fact, $[1\cdots 2l]^2 c_i$ equals the minor of β_{im} in the skew-symmetric determinant giving the square of $[1\cdots 2lm]$. Apart from sign, this minor equals ‡

$$[1\cdots i-1\ i+1\cdots 2lm][1\cdots 2l].$$

Hence

$$(46) \qquad c_i = [1\cdots 2l]^{-1}[1\cdots i-1\ i+1\cdots 2lm] \qquad (i = 1, \cdots, 2l).$$

For these values of the c_i, we have $B_{jm} = 0$ for any j, as may be shown from (46) or without computation as follows. The determinant of the coefficients of

* As shown earlier, the introduction of the $\frac{1}{2}M_{ii}$ serves to define the rank. Contrary to the suggestions in my earlier papers I now prefer to avoid the use of semi-minors other than principal, since $\frac{1}{2}M_{ij}$ $(i \neq j)$ is defined in the field only when $M = 0$, and even then in a very artificial manner.

† Having points of resemblance and points of contrast with KRONECKER'S algebraic method (§ 7).

‡ SCOTT, *Theory of Determinants*, 1880, p. 75, § 15.

$c_1, \cdots, c_{2l}, 1$ in B_{jm} $(j = 1, \cdots, 2l, k)$ is the minor M_{km} of the element β_{km} in the last row of

$$D_{2l+2} = |\beta_{st}| \qquad (s, t = 1, \cdots, 2l, k, m).$$

The latter equals $[1 \cdots 2l\, k\, m]^2$ and is zero by hypothesis. Let M_{ii} denote the minor of β_{ii}, so that $M_{ii} = 0$. But $M_{kk}M_{mm} - M_{km}^2$ equals the product of D_{2l+2} by the minor $|\beta_{st}|$, $s, t = 1, \cdots, 2l$. Hence $M_{km} = 0$.

To evaluate E_m, we note that the preceding discussion is valid for any m. For $m = 2l + 1$, the semi-discriminant of (44), with each $B_{jm} = 0$, equals $[1 \cdots 2l]^2 E_{2l+1}$, while that of Q_{2l+1} is $\{1 \cdots 2l + 1\}$. Now the first sum in E_m, given by (45), becomes a multiple of 2 when β_{jm} is eliminated by means of $B_{jm} = 0$. Hence

$$\{1 \cdots 2l+1\} = [1 \cdots 2l]^2 \left\{ \sum_{i<j}^{1,\cdots,2l} \beta_{ij} c_i c_j + \sum_{i=1}^{2l} b_i c_i^2 + b_{2l+1} \right\} \tag{47}$$

becomes an identity when the values (46), with $m = 2l + 1$, are inserted:

$$\begin{aligned} \{1 \cdots 2l+1\} \equiv & \sum_{i<j}^{1,\cdots,2l} \beta_{ij} [1 \cdots i-1\, i+1 \cdots 2l+1] \\ & \times [1 \cdots j-1\, j+1 \cdots 2l+1] + \sum_{i=1}^{2l+1} b_i [1 \cdots i-1\, i+1 \cdots 2l+1]^2. \end{aligned} \tag{48}$$

Replacing the subscript $2l + 1$ by m, we derive the identity

$$\{1 \cdots 2l\, m\} \equiv [1 \cdots 2l]^2 E_m. \tag{49}$$

For the next step, we add suitable multiples of x_{m-1} to $x_1, \cdots, x_{2l}$. After $m - 2l$ such steps, we find that Q_m has been reduced, by a transformation of determinant unity, to

$$\sum_{i<j}^{1,\cdots,2l} \beta_{ij} x_i x_j + \sum_{i=1}^{2l} b_i x_i^2 + [1 \cdots 2l]^{-2} \sum_{i=2l+1}^{m} \{1 \cdots 2l\, i\} x_i^2. \tag{50}$$

The first two sums define Q_{2l}, viz., (24) for $m = 2l$.

15. For the further normalization of (50) we shall apply transformations involving only the variables $x_1, \cdots, x_{2l}$. In particular, the final sum in (50) will not be altered. The present problem is therefore the normalization of Q_{2l} of discriminant $[1 \cdots 2l]^2 \neq 0$. Thus not every pfaffian of order $2l - 2$ vanishes; let $[1 \cdots 2l - 2] \neq 0$. We may proceed as in § 14 (with m replaced by $2l$, and l by $l - 1$) with a certain essential modification.* The transformation

$$x_i = x_i' + [1 \cdots 2l-2]^{-1} [1 \cdots i-1\, i+1 \cdots 2l-2\, 2l]\, x_{2l}' \quad (i = 1, \cdots, 2l-2),$$

$$x_{2l-1} = x_{2l-1}', \qquad x_{2l} = x_{2l}',$$

* In the proof that $B_{jm} = 0\,(j > 2l)$ by means of the vanishing of the pfaffians of order $2l + 2$. The latter correspond to pfaffians of order $2l$ in the present case, and these are not all zero. Instead of the B_{jm} we now have B_i, which does not vanish.

of determinant unity, replaces Q_{2l} by

$$(51)\quad \sum_{i<j}^{1,\cdots,2l-1}\beta_{ij}x_i'x_j'+B_lx_{2l-1}'x_{2l}'+\sum_{i=1}^{2l-1}b_ix_i'^2+[1\cdots 2l-2]^{-2}\{1\cdots 2l-2\ 2l\}x_{2l}'^2,$$

where

$$B_l\equiv\sum_{i=1}^{2l-2}\beta_{i\,2l-1}[1\cdots 2l-2]^{-1}[1\cdots i-1\ i+1\cdots 2l-2\ 2l]-\beta_{2l-1\,2l}$$
$$=[1\cdots 2l-2]^{-1}[1\cdots 2l].$$

The last equality follows from the expansion of $[1\cdots 2l]$ with respect to the elements $\beta_{i\,2l-1}$, or by the identity of the discriminants of Q_{2l} and (51).

Similarly, to (51) we apply the transformation

$$x_i'=x_i''+[1\cdots 2l-2]^{-1}[1\cdots i-1\ i+1\cdots 2l-2\ 2l-1]x_{2l-1}''\quad(i=1,\cdots,2l-2),$$
$$x_{2l-1}'=x_{2l-1}'',\qquad x_{2l}'=x_{2l}'',$$

suppress the accents on x'', and obtain the form

$$(52)\quad \sum_{i<j}^{1,\cdots,2l-2}\beta_{ij}x_ix_j+[1\cdots 2l-2]^{-1}[1\cdots 2l]x_{2l-1}x_{2l}+\sum_{i=1}^{2l-2}b_ix_i^2$$
$$+[1\cdots 2l-2]^{-2}\{1\cdots 2l-2\ 2l-1\}x_{2l-1}^2+[1\cdots 2l-2]^{-2}\{1\cdots 2l-2\ 2l\}x_{2l}^2.$$

The first and third sums define Q_{2l-2}. The double step by which Q_{2l} has been reduced to (52) by a transformation of determinant unity may now be repeated. By rearranging the variables $x_1,\cdots,x_{2l-2}$, we may assume that (28) holds. We arrive ultimately at the following conclusion: If every pfaffian of order $>2l$, but not every pfaffian of order $2l$, vanishes, the pfaffians $[12]$, $[1234],\cdots,[1\cdots 2l]$ may be assumed not to vanish; then Q_m may be reduced by a linear transformation of determinant unity to

$$(53)\quad \sum_{s=1}^{l}[1\cdots 2s-2]^{-1}[1\cdots 2s]x_{2s-1}x_{2s}+\sum_{s=1}^{l}[1\cdots 2s-2]^{-2}(\{1\cdots 2s-2\ 2s-1\}x_{2s-1}^2$$
$$+\{1\cdots 2s-2\ 2s\}x_{2s}^2)+[1\cdots 2l]^{-2}\sum_{i=2l+1}^{m}\{1\cdots 2l\,i\}x_i^2.$$

If we multiply x_{2s-1} and x_{2s} by $[1\cdots 2s-2]$, for $s=1,\cdots,l$; and x_i by $[1\cdots 2l]$, for $i=2l+1,\cdots,m$, we see that Q_m can be reduced by a linear transformation of determinant (35) to the form (36).

Hence the present method of reduction has led us to the same normal form as that obtained by the former method.

Definition and construction of the invariant χ_l.

16. It remains to investigate a problem of decided importance both for the general theory of the reduction of quadratic forms in the $GF[2^n]$ and for the

subsequent determination of the invariants. Under the assumption (28) that no one of the pfaffians $[12]$, $[1234]$, $\cdots$, $[1\cdots 2l]$ vanishes, the form Q_{2l} was transformed into the normal form (41), in which

$$(54)\quad \delta=\sum_{s=1}^{l}[1\cdots 2s-2]^{-2}[1\cdots 2s]^{-2}\{1\cdots 2s-2\,2s-1\}\{1\cdots 2s-2\,2s\}.$$

Of the forms (41), there are two non-equivalent canonical forms distinguished by the value 0 or 1 of $\chi(\delta)$, where χ is the function (42). Given a form Q_{2l} having $[1\cdots 2l]\neq 0$, we readily obtain by a suitable rearrangement of the variables a form Q'_{2l} for which the assumption (28) holds, so that the criterion $\chi(\delta)=0$ or 1 is applicable. What we desire, however, is a criterion which will apply directly to Q_{2l} itself. Moreover, we prefer to accomplish this result by means of an absolute invariant* of Q_{2l}, which must therefore be defined for all values of the coefficients including those making $[1\cdots 2l]=0$. Hence we seek a polynominal χ_l in the coefficients of Q_{2l} such that $\chi_l=1$ when Q_{2l} is transformable into (41) with $\chi(\delta)=1$, while $\chi_l=0$ for all remaining forms Q_{2l}. Such a polynominal χ_l is clearly an absolute invariant of Q_{2l}.

For $l=1$, $\beta_{12}\neq 0$, (54) gives $\delta=b_1b_2\beta_{12}^{-2}$. Hence we have

$$(55)\qquad \chi_1=\chi(b_1b_2\beta_{12}^{2^n-3}),$$

where (and below) an exponent 2^n-3 is to be replaced by unity when $n=1$.

Next, let $l=2$. For $\beta_{12}\neq 0$, $P\equiv[1234]\neq 0$, (54) gives

$$\delta=\beta_{12}^{-2}b_1b_2+\beta_{12}^{-2}P^{-2}\{123\}\{124\}.$$

Thus $\delta=\delta_{12}$, where

$$(56)\qquad \delta_{ij}=(b_ib_jP^2+\{ijk\}\{ijt\})(\beta_{ij}P)^{2^n-3},$$

i,j,k,t being a permutation of 1, 2, 3, 4. Hence

$$(57)\qquad \chi_2=\chi(\delta_{ij})$$

for every set of values of the 10 coefficients of Q_4 for which $\beta_{ij}\neq 0$ (whether or not $P\neq 0$). In particular, we deduce the identity

$$(58)\qquad \chi_2\equiv\chi(\delta_{12})+M(\beta_{12}^{\nu}-1)\qquad(\nu=2^n-1).$$

Consider any set with $\beta_{12}=0$, $\beta_{13}\neq 0$. By (58), and (57) for $i,j=1,3$,

$$[\chi(\delta_{13})]_{\beta_{12}=0}=M\qquad(\text{for }\beta_{13}\neq 0)$$
$$\equiv M+M_1(\beta_{13}^{\nu}-1),$$

where M_1 is free of β_{12}, β_{13}. Then (58) becomes

$$(59)\qquad \chi_2\equiv\chi(\delta_{12})+(\beta_{12}^{\nu}-1)\chi(\delta_{13})+M_1(\beta_{12}^{\nu}-1)(\beta_{13}^{\nu}-1).$$

* For the $GF[p^n]$, $p>2$, we used the power $\frac{1}{2}(p^n-1)$ of the discriminant.

Consider any set with $\beta_{12}=\beta_{13}=0$, $\beta_{14}\neq 0$. By (59) and (57) for $i,j=1,4$,

$$[\chi(\delta_{14})]_{\beta_{12}=\beta_{13}=0}\equiv M_1+M_2(\beta_{14}^{\nu}-1),$$

$$\chi_2\equiv\chi(\delta_{12})+(\beta_{12}^{\nu}-1)\chi(\delta_{13})+(\beta_{12}^{\nu}-1)(\beta_{13}^{\nu}-1)\chi(\delta_{14}) \tag{60}$$
$$+M_2(\beta_{12}^{\nu}-1)(\beta_{13}^{\nu}-1)(\beta_{14}^{\nu}-1),$$

where M_2 is free of β_{12}, β_{13}, β_{14}. If these β's vanish, $P=0$, so that $\chi_2=0$ by definition. Hence (60) gives $M_2=0$. Thus

$$\chi_2=\chi(e),\qquad e=\delta_{12}+(\beta_{12}^{\nu}-1)\delta_{13}+(\beta_{12}^{\nu}-1)(\beta_{13}^{\nu}-1)\delta_{14}. \tag{61}$$

The terms independent of the b's in χ_2 are

$$\chi(\beta_{12}^{\nu}\beta_{13}\beta_{14}\beta_{23}\beta_{24}P^{2^n-3})\equiv\chi\{(\beta_{13}\beta_{14}\beta_{23}\beta_{24}+\beta_{12}\beta_{13}\beta_{24}\beta_{34}+\beta_{12}\beta_{14}\beta_{23}\beta_{34})P^{2^n-3}\}.$$

For $\beta_{12}\neq 0$, this identity may be written

$$\chi\{t(P-t)P^{2^n-3}\}=0,\qquad t\equiv\beta_{12}\beta_{34},$$

and is true since the square of tP^{2^n-2} equals $t^2P^{2^n-3}$. For $\beta_{12}=0$, the identity reduces to

$$\chi\{\alpha\beta(\alpha+\beta)^{2^n-3}\}=0,\qquad \alpha\equiv\beta_{13}\beta_{24},\qquad \beta\equiv\beta_{14}\beta_{23}.$$

In view of (55), it expresses the condition that the quadratic form

$$x^2+(\alpha+\beta)xy+\alpha\beta y^2\equiv(x+\alpha y)(x+\beta y)$$

shall be reducible in the field.

In e the coefficients of b_3b_4, b_4, b_4^2 are the products of P^{2^n-3} by β_{12}^2, $\beta_{12}\beta_{13}\beta_{23}$, 0, respectively. Hence, by the symmetry of an invariant, we have*

$$\chi_2=\chi\{(\sum_{(3)}\beta_{13}\beta_{14}\beta_{23}\beta_{24}+\sum_{(4)}\beta_{12}\beta_{13}\beta_{23}b_4+\sum_{(6)}\beta_{12}^2b_3b_4)P^{2^n-3}\}. \tag{62}$$

For a general value of l, we shall express χ_l in terms of χ_{l-1}. We develop an auxiliary formula for the case $[1\cdots 2l-2]\neq 0$, $P\equiv[1\cdots 2l]\neq 0$. Then, by §15, Q_{2l} can be transformed into (52). Multiplying x_{2l-1} by $[1\cdots 2l-2]$ and x_{2l} by P^{-1}, we get

$$Q_{2l-2}+x_{2l-1}x_{2l}+\{1\cdots 2l-2\,2l-1\}x_{2l-1}^2+[1\cdots 2l-2]^{-2}P^{-2}\{1\cdots 2l-2\,2l\}x_{2l}^2.$$

First, let $\chi_{l-1}=0$. Then, by the proof leading to (43), Q_{2l-2} can be transformed into $\sum_{s=1}^{s=l-1}x_{2s-1}x_{2s}$. Hence $\chi_l=\chi(\delta)$, where δ equals

$$\delta_{1,\ldots,2l-2}=\{1\cdots 2l-2\,2l-1\}\{1\cdots 2l-2\,2l\}[1\cdots 2l-2]^{2^n-3}P^{2^n-3}. \tag{63'}$$

Next, let $\chi_{l-1}=1$. Then Q_{2l-2} can be transformed into

$$\sum_{s=1}^{l-1}x_{2s-1}x_{2s}+x_1^2+dx_2^2,\qquad \chi(d)=1.$$

Hence $\chi_l=\chi(d+\delta)=1+\chi(\delta)$, where δ is defined by (63').

*American Journal of Mathematics, loc. cit., p. 267, §7, for the special case $P=1$.

Thus, in either case, $\chi_l = \chi_{l-1} + \chi(\delta)$. Hence for any P,

$$\chi_l = \chi_{l-1} + \chi(\delta) + \mu(P^\nu - 1) \qquad \text{when} \qquad [1 \cdots 2l-2] \neq 0.$$

Let $P = 0$. Then $\chi_l = 0$ by definition. Thus $\mu = \chi_{l-1}$, and

$$(64') \qquad \chi_l = P^\nu \chi_{l-1} + \chi(\delta_{1,\ldots,2l-2}) \qquad \text{when} \qquad [1 \cdots 2l-2] \neq 0.$$

Let $i_1, \cdots, i_{2l}$ give any permutation of $1, \cdots, 2l$. Then

$$(64) \qquad \chi_l = P^\nu \chi_{l-1} + \chi(\delta_{i_1,\ldots,i_{2l-2}}) \qquad \text{when} \qquad [i_1 \cdots i_{2l-2}] \neq 0,$$

$$(63) \qquad \delta_{i_1,\ldots,i_{2l-2}} = \{i_1 \cdots i_{2l-2} i_{2l-1}\}\{i_1 \cdots i_{2l-2} i_{2l}\}[i_1 \cdots i_{2l-2}]^{2^n-3} P^{2^n-3}.$$

By our usual synthesis, we obtain *

$$(65) \quad \begin{aligned} \chi_l = {} & P^\nu \chi_{l-1} + \chi(d_1) + (P_1^\nu - 1)\chi(d_2) \\ & + (P_1^\nu - 1)(P_2^\nu - 1)\chi(d_3) + \cdots + (P_1^\nu - 1)\cdots(P_{\lambda-1}^\nu - 1)\chi(d_\lambda), \end{aligned}$$

where P_j denotes the pfaffian $[i_1 \cdots i_{2l-2}]$, d_j the corresponding function (63), λ the number $l(2l-1)$ of such pfaffians, and $P_1, \cdots, P_\lambda$ these pfaffians in any sequence.

For $l = 3$, set $P_1 = [1234]$, $P_2 = [1235]$, $P_3 = [1236]$. Now

$$\pi = (P_1^\nu - 1)(P_2^\nu - 1)(P_3^\nu - 1)P$$

is a factor of the terms of (65) after the fourth. But

$$(66) \qquad P_1[1256] - P_2[1246] + P_3[1245] \equiv \beta_{12} P,$$

algebraically. Hence $\pi = 0$ if $\beta_{12} \neq 0$. Interchanging 2 and 3, or 1 and 3 in (66), we find that $\pi = 0$ unless $\beta_{12} = \beta_{13} = \beta_{23} = 0$. In the latter case, $P_1 = P_2 = P_3 = 0$. Then let $P_4, \cdots, P_{12}$ denote the pfaffians $[ijkt]$ in which i, j are chosen from 1, 2, 3, and k, t from 4, 5, 6. Then each d_j $(j = 4, \cdots, 12)$ has the factor $\{123kt\}$, which is a linear homogeneous function of b_1, b_2, b_3. Among the P_j $(j \leqq 12)$ occurs every $[1r3s]$. Interchanging 2 with r in (66) we conclude, as above, that the terms of (65) with the factor $P\Pi(P_j^\nu - 1)$, $j = 1, \cdots, 12$, are zero; this is evident if each $\beta_{1r} = 0$, whence $P = 0$. Hence $\chi_3 = P^\nu \chi_2 + \chi(E)$, where

$$E = \delta_{1234} + (P_1^\nu - 1)\delta_{1235} + (P_1^\nu - 1)(P_2^\nu - 1)\delta_{1236} + L,$$

every term of L containing b_1, b_2, or b_3. In E the coefficients of $b_5 b_6, b_6^2, b_6$ are the products of P^{2^n-3} by

$$[1234]^2, \qquad 0, \qquad V \equiv P_1^\nu \psi + (P_1^\nu - 1)P_2^\nu \psi,$$

* The argument initially gives an additional term πM, where π is the product of the $P_j^\nu - 1$ for $j = 1, \cdots, \lambda$. But if we set every $P_j = 0$, we have $P = 0$, so that $\chi_l = 0$, by definition. Thus $0 = M$.

respectively, where ψ denotes the aggregate ψ_{12345} of the terms free of the b's in $\{12345\}$. Evidently $V=\psi$ if either $P_1 \neq 0$ or $P_2 \neq 0$. Since χ_3 is an absolute invariant, V is symmetrical in $1, \cdots, 5$. Hence $V=\psi$ unless every $[i_1 i_2 i_3 i_4]=0$, where $i, \cdots, i_4$ are chosen from $1, \cdots, 5$. But in the latter case, $\psi=0$, by (48), while V obviously vanishes. Hence

$$\chi_3 = \chi\{(F_3 + \Sigma \psi_{12345} b_6 + \Sigma [1234]^2 b_5 b_6) P^{2^n-3}\}, \tag{67}$$

where F_3 may be taken to be

$$F_3 = \sum_{(45)} \beta_{13}\beta_{14}\beta_{23}\beta_{24}\beta_{56}^2 + \sum_{(10)} \beta_{12}\beta_{13}\beta_{23}\beta_{45}\beta_{46}\beta_{56}.$$

An inspection of the expressions (55), (62), (67) for χ_l, for $l=1, 2, 3$, indicates that, in the formula, given by (65) and (63),

$$\chi_l = \chi(CP^{2^n-3}), \tag{68}$$

C has the following simple relation to the algebraic discriminant D of the quadratic form Q_{2l} (§ 10). The coefficients of $4b_{2l-1}b_{2l}$ in $4C$ and D are congruent modulo 2, likewise the coefficients* of $4b_{2l}$; while the terms independent of the b's in $D-(-1)^l P^2$ and $4C$ are multiples of 4, congruent modulo 8. In the last statement and in the proofs below, P is the expression obtained from the algebraic pfaffian $[1 \cdots 2l]$ by giving the various terms any desired signs. For such a function P, the congruence

$$D-(-1)^l P^2 \equiv 4C \pmod 8 \tag{69}$$

uniquely determines $C \pmod 2$. The resulting function (68) will be shown to be an absolute invariant of Q_{2l} in the $GF[2^n]$. Under any linear transformation of determinant Δ, D becomes $\Delta^2 D$ and P becomes $\Delta P + 2\rho$ (§ 10). Hence $d=D-(-1)^l P^2$ becomes $\Delta^2 d - (-1)^l(4\Delta P\rho + 4\rho^2)$. But, by (69), d is a multiple of 4. Hence dP^{2^n-3} takes the increment

$$(\Delta P)^{2^n-3}(4\Delta P\rho + 4\rho^2) + 8S.$$

Hence in the $GF[2^n]$, the function (68) takes the increment

$$\chi[(\Delta P)^{2^n-2}\rho] + \chi[(\Delta P)^{2^n-3}\rho^2] \equiv 0,$$

since the quantity in the second brackets is the square of that in the first.

For the canonical form (41), $D=(-1)^l(1-4\delta)$, $P^2=1$. Hence

$$C \equiv \delta, \qquad \chi_l \equiv \chi(\delta) \pmod 2,$$

so that (68) is the desired absolute invariant of Q_{2l}.

*Such terms, containing a single b, occur when $l>1$.

The invariants of a quadratic form Q_m in the $GF[2^n]$, §§ 17–20.

17. Under the group G of all m-ary linear homogeneous transformations in the $GF[2^n]$, we define C_0 to be the class to which the identically vanishing form Q_m belongs, C_{2l+1} the class for (40) with $c=1$, $C_{2l,1}$ the class for (41) with $\chi(\delta)=1$, $C_{2l,0}$ the class for (41) with $\chi(\delta)=0$.

We seek the characteristic absolute invariants I_0, I_{2l+1}, $I_{2l,1}$, $I_{2l,0}$ of the general Q_m for the respective classes. By (1),

$$I_0=\prod_{i<j}(\beta_{ij}^{\nu}-1)\prod(b_i^{\nu}-1) \qquad (\nu=2^n-1). \tag{70}$$

We shall employ the abbreviations

$$\pi_{2l}=\Pi(P^{\nu}-1), \qquad \sigma_{2l+1}=\Pi(S^{\nu}-1), \tag{71}$$

where P ranges over the pfaffians $[i_1\cdots i_{2l}]$ of order $2l$, while S ranges over the principal semi-minors $\{i_1\cdots i_{2l+1}\}$ of order $2l+1$. In particular,

$$\pi_2=\prod_{i<j}(\beta_{ij}^{\nu}-1), \qquad \sigma_1=\prod(b_i^{\nu}-1), \tag{71'}$$

$$I_0=\pi_2\sigma_1. \tag{70'}$$

Since $I_{2l+1}=1$ if every pfaffian of order $2l+2$ vanishes, but not every principal semi-minor $\{i_1\cdots i_{2l+1}\}$, while $I=0$ in the remaining cases, we have

$$I_{2l+1}=\pi_{2l+2}(1+\sigma_{2l+1}), \tag{72}$$

$$I_1=\pi_2+I_0. \tag{72'}$$

We readily determine the absolute invariant

$$R_{2l}=I_{2l,1}+I_{2l,0}, \tag{73}$$

which has the value 1 or 0 according as Q_m is or is not of rank $2l$. By the result at the end of § 12, we have

$$R_{2l}=\pi_{2l+2}\sigma_{2l+1}(1+\pi_{2l}), \tag{74}$$

the first two factors being absent if $2l=m$, so that

$$R_m=[1\cdots m]^{\nu} \qquad (m \text{ even}). \tag{74'}$$

By the same reference, we have

$$I_{2l,1}=\pi_{2l+2}\sigma_{2l+1}L, \tag{75}$$

where L is to be determined. Henceforth we consider only sets of coefficients for which every pfaffian of order $2l+2$ and every $\{i\cdots i_{2l+1}\}$ vanishes; then $I_{2l,1}=L$. Consider such a set with $[1\cdots 2l]\neq 0$; then Q_m can be transformed into the corresponding form Q_{2l} on $x_1,\cdots,x_{2l}$ (§ 14), and L has the

value χ_i defined by (68). Let the various pfaffians of order $2l$ be designated by $P_1, \cdots, P_t$. When $1, \cdots, 2l$ are replaced by $i_1, \cdots, i_{2l}$, $P = [1 \cdots 2l]$ becomes $P_i = [i_1 \cdots i_{2l}]$; let the function C become C_i. Then for any one of the above sets for which $P_i \neq 0$, L has the value

$$L_i = \chi(C_i P_i^{2^n-3}). \tag{76}$$

By the usual synthesis of these relations,

$$L = L_1 + (P_1^\nu - 1)L_2 + (P_1^\nu - 1)(P_2^\nu - 1)L_3 + \cdots + (P_1^\nu - 1)\cdots(P_{t-1}^\nu - 1)L_t, \tag{77}$$

with initially an addition term $M\Pi(P_i^\nu - 1)$, $i = 1, \cdots, t$. But for every $P_i = 0$, $I_{2l,1}$ is zero, by definition, so that $M = 0$. Similarly,

$$I_{2l,0} = \pi_{2l+2}\sigma_{2l+1}K.$$

For the sets with every $[i_1 \cdots i_{2l+2}] = \{i_1 \cdots i_{2l+1}\} = 0$, we have $I_{2l,0} = K$. If also $P_i \neq 0$, then $K = 1 + L_i$. A synthesis of the latter relations gives

$$K = 1 + L + \mu \prod_{i=1}^{t} (P_i^\nu - 1).$$

If every $P_i = 0$, then $I_{2l,0} = 0$, by definition. Hence $\mu = 1$. Thus

$$I_{2l,0} = \pi_{2l+2}\sigma_{2l+1}(L + 1 + \pi_{2l}). \tag{78}$$

As a check, we note that (74) follows at once from (75) and (78); also that for $m = 3$, $I_{2,1}$ is the invariant F given for $n \leqq 4$ in the American Journal of Mathematics, l. c.

18. The preceding determination of the invariant $I_{2l,1}$ was based upon the second method (§ 14) of reducing quadratic forms in the $GF[2^n]$. For $l > 1$, a determination based upon the first method (§ 12) appears to be more complicated. We shall treat briefly the case $l = 1$, $m = 4$, from the latter standpoint; we are thereby led naturally to a noteworthy modification of the earlier formula for $I_{2,1}$. If $\beta_{12} \neq 0$, Q_4 is transformable into an irreducible binary form $B = x_1x_2 + x_1^2 + cx_2^2$ if and only if $P \equiv [1234] = 0$, $\{123\} = 0$, $\{124\} = 0$, and (55) is unity. In general, if $\beta_{ij} \neq 0$, $I_{2,1} = 1$ if and only if $P = 0$, $\{ijk\} = 0$, $\{ijt\} = 0$, $L_{ij} = 1$, where i, j, k, t form a permutation of 1, 2, 3, 4, and

$$L_{ij} = \chi(b_i b_j \beta_{ij}^{2^n-3}), \qquad G_{ij} = (\{ijk\}^\nu - 1)(\{ijt\}^\nu - 1)L_{ij}. \tag{79}$$

Hence, if $\beta_{ij} \neq 0$, $I_{2,1} = (P^\nu - 1)G_{ij}$. By the usual synthesis,

$$\begin{aligned} I_{2,1} = (P^\nu - 1)\{G_{12} + (\beta_{12}^\nu - 1)G_{13} + (\beta_{12}^\nu - 1)(\beta_{13}^\nu - 1)G_{14} \\ + \cdots + (\beta_{12}^\nu - 1)\cdots(\beta_{24}^\nu - 1)G_{34}\}. \end{aligned} \tag{80}$$

A comparison of (80) with (75) and (77) indicates that

$$(P^\nu-1)G_{ij}=(P^\nu-1)\sigma_3 L_{ij}, \qquad \sigma_3 \equiv \prod_{(4)}(\{ijk\}^\nu-1).$$

This equality is obvious except in the case $P=0$, $\{ijk\}=0$, $\{ijt\}=0$, $L_{ij}=1$. But then Q_4 is transformable into B, so that $\{ikt\}=0$, $\{jkt\}=0$.

19. To determine the relative invariants of Q_m in the $GF[2^n]$, we note that (end of § 12) the only classes under the total group G which separate into sub-classes under the group G_1 of determinant unity are $C_{m,1}$ and $C_{m,0}$ for m even, while the only such class is C_m for m odd. In the latter case, the sub-classes may be designated by $K_{m,c}$, a representative form being (40) for $m=2l+1$. Here c is the non-vanishing semi-discriminant of Q_m. As in § 9, there exists a single invariant of a given weight w, $0<w<\nu$, since it must vanish for all the classes other than the $K_{m,c}$, and since its value for $K_{m,c}$ must be $c^{w/2}$ times its value $\neq 0$ for $K_{m,1}$. But such an invariant is $S^{w/2}$ for w even and $S^{(w+\nu)/2}$ for w odd, where S is the semi-discriminant of the general form Q_m. *Hence for m odd, the only relative invariants are powers of the semi-discriminant.*

Next let m be even. The sub-classes mentioned above may be designated $K_{m,\chi,P}$, where $\chi=1$ or 0, and $P=[1\cdots m]\neq 0$, representative forms being

$$(41') \qquad \sum_{s=2}^{\frac{1}{2}m} x_{2s-1}x_{2s}+Px_1x_2+P^2x_1^2+\delta x_2^2 \qquad [\chi(\delta)=\chi].$$

To obtain an invariant ϕ of weight w, $0<w<\nu$, we must assign to ϕ the value 0 for all the classes other than the $K_{m,\chi,P}$, and for the latter P^w times the value of ϕ for $K_{m,\chi,1}$. Hence the two values for the last two classes ($\chi=1$ or 0) alone are arbitrary, so that there are just two linearly independent invariants of the given weight w. But P^w and $P^w\chi_{m/2}$ have these properties, $\chi_{m/2}=I_{m,1}$ being the absolute invariant determined in § 16. *For m even, the only relative invariants are*

$$[1\cdots m]^w(c_1+c_2\chi_{m/2}) \qquad (0<w<2^n-1, \ c_1 \text{ and } c_2 \text{ constants}).$$

20. A simple method of obtaining a smaller number of independent invariants of Q_m in the $GF[2^n]$, in terms of which all the above invariants can be expressed rationally, will be illustrated by the case $m=4$. Let

$$(81) \qquad F_4=I_{4,1}+I_3, \qquad J_4=I_{2,1}+I_0, \qquad P=[1234].$$

By (72) for $l=1$, and (75) for $l=2$,

$$(82) \quad I_3=(P^\nu-1)(1+\sigma_3), \qquad I_{4,1}=L\equiv\chi_2, \qquad \sigma_3\equiv\prod_{(4)}(S^\nu-1).$$

Since χ_2, given by (62), is a multiple of P, $(P^\nu - 1)I_{4,1} = 0$. Hence *

$$(83)\quad \chi_2 = I_{4,1} = P^\nu F_4, \qquad I_3 = (P^\nu - 1)F_4, \qquad I_{4,0} = P^\nu(F_4 + 1),$$

the last following from $I_{4,1} + I_{4,0} = P^\nu$, given by (73) and (74′) for $l = 2$. By (73) and (74) for $l = 1$,

$$I_{2,1} + I_{2,0} = (P^\nu - 1)\sigma_3(1 + \pi_2) = (P^\nu - 1)\sigma_3 + \pi_2,$$

since each $\pi_2 S = 0$, $\pi_2 P = 0$, in view of the form $(71_1')$ of π_2. But by (82_1) and (83_2),

$$(P^\nu - 1)\sigma_3 = I_3 + P^\nu - 1 = (P^\nu - 1)(F_4 + 1).$$

Hence we have†

$$(84)\qquad I_{2,1} + I_{2,0} = (P^\nu - 1)(F_4 + 1) + \pi_2.$$

Now each term of (80) has a factor β_{ij}, in view of the L_{ij}. Thus

$$\pi_2 I_{2,1} = 0, \qquad \pi_2 I_0 = I_0,$$

the latter following from (70′). Hence by (81_2)

$$(85)\qquad I_0 = \pi_2 J_4, \qquad I_{2,1} = J_4(\pi_2 + 1).$$

Then by (72′) and (84),

$$(86)\quad I_1 = \pi_2(J_4 + 1), \qquad I_{2,0} = (P^\nu - 1)(F_4 + 1) + J_4(\pi_2 + 1) + \pi_2.$$

Hence formulæ (83), (85), (86) express all the absolute invariants of Q_4 in terms of F_4, J_4, P, π_2. Incorporating the result at the end of § 19, we have the

THEOREM.‡ *Every invariant of Q_4 in the $GF[2^n]$ is an integral function of the invariants F_4, J_4, P, π_2; in fact, a linear homogeneous function of*

$$(87)\qquad J_4,\ \pi_2,\ \pi_2 J_4,\ P^e,\ P^e F_4 \qquad (e = 0, 1, \cdots, 2^n - 1).$$

The values of these invariants for the various classes are here shown.

	$K_{4,0,P}$	$K_{4,1,P}$	C_3	$C_{2,0}$	$C_{2,1}$	C_1	C_0
F_4	0	1	1	0	0	0	0
J_4	0	0	0	0	1	0	1
P	P	P	0	0	0	0	0
π_2	0	0	0	0	0	1	1

* Another proof of (83_1) results from the fact that $P^\nu F_4$ has the value 1 for class $C_{4,1}$ and the value 0 for the remaining classes.

† Another proof follows from the fact that the second member of (84) has the value 1 for classes $C_{2,1}$ and $C_{2,0}$, the value 0 for the remaining classes.

‡ For $n = 1$, Proceedings of the London Mathematical Society, vol. 5 (1907), pp. 303–311. The invariants A_4, I_4 are the π_2, I_0 of the present paper. The explicit expressions for J_4 and F_4 are given on p. 308 and p. 310.

To prove (end of § 5) the independence of F_4, we employ C_3 and $C_{2,0}$; for J_4, C_1 and C_0; for P, $K_{4,1,P}$ and C_3; for π_2, $C_{2,0}$ and C_1. *Hence the four invariants are independent.* It follows from the table that

$$(88)\quad F_4J_4=F_4\pi_2=PJ_4=P\pi_2=0, \qquad P^{2^n}=P, \qquad I^2=I\,(I=F_4, J_4 \text{ or } \pi_2).$$

Any product of two invariants (87) *reduces to one of the set by means of* (88).

Reduction of binary cubic forms in the $GF[p^n]$.

21. If $p^n = 3l + 2$ or 3^n, every element $\neq 0$ of the $GF[p^n]$ is a cube:

$$e = e^{-3l} \qquad \text{or} \qquad e^{3\cdot 3^{n-1}},$$

respectively; hence every element has an unique cube root in the field. But if $p^n = 3l + 1$, just one-third of the elements $\neq 0$ are cubes. If ϵ is a primitive root in the field, the cubes are $\epsilon^{3i}\,(i = 1, \cdots, l)$; while the not-cubes are the products of the preceding by ϵ, ϵ^2. We shall set

$$(89)\quad \beta = 1 \text{ if } p^n = 3l + 2 \text{ or } p^n = 3^n; \qquad \beta = 1,\ \epsilon \text{ or } \epsilon^2 \text{ if } p^n = 3l + 1.$$

Consider the binary cubic with coefficients in the $GF[p^n]$,

$$(90)\qquad f(x, y) \equiv a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3.$$

If ρ_1, ρ_2, ρ_3 are the roots of $f(x, 1) = 0$, the discriminant of (90) is

$$(91)\quad D = a_0^4\,\Pi\,(\rho_i - \rho_j)^2 = 18a_0a_1a_2a_3 - 4a_0a_2^3 - 4a_1^3a_3 + a_1^2a_2^2 - 27a_0^2a_3^2.$$

When $p^n = 2$ the special form $f_1 = xy(x + y)$ is unaltered under every linear transformation in the field; it is a special case of the canonical form (93). Except when $f \equiv 0$, or when $p^n = 2$ and $f = f_1$, we can transform f into a form f' with $a_0' \neq 0$. If $a_0 = 0$, $a_3 \neq 0$, we apply $(y, -x)$. If $a_0 = a_3 = 0$, we apply $(x, \lambda x + y)$ and have $a_0' = a_1\lambda + a_2\lambda^2$.

In the normalization of a form f with $a_0 \neq 0$, we consider several cases.

(i) In case there is a triple root ρ, we apply the transformation

$$x - \rho y = \alpha x', \qquad y = \alpha^{-1}y',$$

of determinant unity. We obtain $a_0\alpha^3x'^3$, and hence βx^3.

(ii) In case there is a double root ρ_1 and a simple root ρ_2, we apply the transformation of determinant unity

$$(92)\qquad x - \rho_1 y = \alpha x', \qquad x - \rho_2 y = \alpha^{-1}(\rho_1 - \rho_2)y'.$$

We obtain cx'^2y', where $c = a_0\alpha(\rho_1 - \rho_2)$ may be made unity by choice of α.

(iii) Let $f(x, 1) = 0$ have three distinct roots ρ_i in the field. Applying the

transformation (92) to $f(x, y)$, we obtain $kx'y'(x' + ry')$, where

$$k = a_0\alpha(\rho_3 - \rho_2), \qquad r = \alpha^{-2}(\rho_1 - \rho_2)(\rho_3 - \rho_1)/(\rho_2 - \rho_3).$$

We make $k = 1$ by choice of α. Then $r^2 = D$, by (91). In

$$xy(x + ry), \qquad r^2 = D, \tag{93}$$

we may change the sign of r by applying $(ry, -r^{-1}x)$. Under the group G_1 of binary transformations of determinant unity, the canonical form is (93), where r is a particular square root of D.

Under the total group G, a canonical form is

$$\beta xy(x + y) \quad \text{or} \quad xy(x + \beta y). \tag{93'}$$

Indeed, $(sx, r^{-1}sy)$ replaces (93) by $cxy(x + y)$, $c = r^{-1}s^3$.

(iv) Let f be the product of an irreducible quadratic factor and a linear factor. The latter may be taken to be a multiple of x.

If $p \neq 2$, we apply $(x, y + ax)$ and obtain

$$dx(y^2 - \mu x^2), \qquad \mu \text{ a not-square.}$$

Applying $(dx, d^{-1}y)$, we obtain the canonical form under G_1

$$x(y^2 - \sigma x^2), \qquad \sigma \text{ a not-square, } \sigma = \tfrac{1}{4}D. \tag{94}$$

As the canonical form under the total group G, we may take *

$$x(y^2 - \nu\beta^2 x^2), \qquad \nu \text{ a particular not-square.} \tag{94'}$$

The latter is obtained from (94) with $\sigma = \nu t^2$ by applying $(s^{-2}x, sy)$, where s is chosen to make ts^{-3} take one of the values β.

If $p = 2$, $f = dx(xy + ax^2 + by^2)$, $dab \neq 0$. Applying $(b^{\frac{1}{2}}x, b^{-\frac{1}{2}}y)$, we obtain a form $mx(xy + y^2 + \delta x^2)$. Applying $(x, y + tx)$, we find that δ is replaced by $c = \delta + t + t^2$. This equation is solvable for t in the $GF[2^n]$ if and only if $\chi(c) = \chi(\delta)$, where

$$\chi(c) = \sum_{i=0}^{n-1} c^{2^i}, \qquad \chi^2 \equiv \chi, \qquad \chi \equiv 0 \text{ or } 1. \tag{95}$$

If $\chi(\delta) = 0$, the quadratic factor would be reducible. Hence

$$mx(xy + y^2 + cx^2), \quad c \text{ a particular root of } \chi(c) = 1, \tag{96}$$

are the canonical forms under G_1. If we multiply x and y by a suitably chosen element, we obtain as the canonical form under the total group G

$$\beta x(xy + y^2 + cx^2). \tag{96'}$$

* We may take $\beta x(s^2 - \nu y^2)$, obtained from (94) with $\sigma = \nu t^2$ by applying $(ax, vaty)$, where a is chosen to make $-a^2\nu t^2 = \beta$.

(v) Finally, let f be irreducible in the $GF[p^n]$. Then $f(x, 1) = 0$ has a root ρ in the $GF[p^{3n}]$, the remaining roots being ρ^{p^n}, $\rho^{p^{2n}}$. For

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y' \qquad (\Delta = \alpha\delta - \beta\gamma \neq 0), \tag{97}$$

we have

$$x - \rho y = (\alpha - \rho\gamma)(x' - \lambda y'), \qquad \lambda \equiv \frac{\delta\rho - \beta}{-\gamma\rho + \alpha} \tag{98}$$

so that ρ is transformed by the inverse of the linear fractional form of (97). Hence when $\alpha, \beta, \gamma, \delta$ take all values in the $GF[p^n]$ for which $\Delta \neq 0$, the fraction λ takes $p^n(p^{2n} - 1)$ distinct values in the $GF[p^{3n}]$, no one belonging to the $GF[p^n]$. Hence λ can be made equal to any assigned element of the $GF[p^{3n}]$, not occurring in the $GF[p^n]$; the ratios of the coefficients in (97) are thereby uniquely determined. The canonical forms under the total group G of all transformations (97) are therefore βC, where C is a particular irreducible cubic $x^3 + \cdots$. We may take

$$C = x^3 - xy^2 + \tau y^3,$$

where τ is suitably chosen. For, if $z^3 - z + \tau = 0$ were reducible for every τ in the $GF[p^n]$, $z^3 - z$ would take p^n distinct values when z does, whereas $z^3 - z$ vanishes for $z = 0, \pm 1$.

It remains to discuss the normalization of f under the group G_1 of the $(p^{2n} - 1)p^n$ transformations (97) with $\Delta = 1$. Then, in (98), $\lambda = \rho$ only when

$$\alpha = \delta = \pm 1, \qquad \beta = \gamma = 0.$$

For $p = 2$, the corresponding transformation (97) is the identity, and λ takes $p^n(p^{2n} - 1)$ distinct values; the $2^n - 1$ canonical forms are therefore mC. Henceforth, let $p > 2$. Then λ takes only $\frac{1}{2}p^n(p^{2n} - 1)$ values. Hence the roots of the various irreducible cubic equations fall into two types. Since $\Delta = 1$,

$$\lambda = -\delta\gamma^{-1} + \gamma^{-1}(\alpha - \gamma\rho)^{-1}, \qquad \lambda - \lambda^{p^n} = (\rho - \rho^{p^n})(\alpha - \gamma\rho)^{-1}(\alpha - \gamma\rho^{p^n})^{-1},$$

when $\gamma \neq 0$. But the second equation is true also when $\gamma = 0$. Thus

$$\phi(\lambda) = \phi(\rho) \div a_0^{-2} f^2(\alpha, \gamma), \qquad \phi(\rho) \equiv (\rho - \rho^{p^n})(\rho^{p^n} - \rho^{p^{2n}})(\rho^{p^{2n}} - \rho). \tag{99}$$

Since $\phi^{p^n} = \phi$, $\phi(\rho)$ is an element of the $GF[p^n]$; in particular, it is unaltered when ρ is replaced by another root ρ^{p^n} or $\rho^{p^{2n}}$ of the same cubic. Hence if ρ and λ are roots of two irreducible cubic equations such that λ is a linear fractional function of ρ of determinant a square (which may evidently be made unity), the ratio of $\phi(\lambda)$ to $\phi(\rho)$ is a non-vanishing square in the field. But if this determinant is a not-square, the ratio of the ϕ's is a not-square. It suffices to prove the latter for a particular linear fractional transformation of determinant a not-square ν, for example, $\lambda = \nu\rho$, whence $\phi(\lambda) = \nu^3\phi(\rho)$. Further, it was

shown above that there exists a linear fractional transformation replacing ρ by any root of any irreducible cubic. Hence if ρ and λ are roots of the equations corresponding to two irreducible cubic forms C and C', then C is equivalent to a multiple of C' under the group G_1 if and only if the ratio of $\phi(\lambda)$ to $\phi(\rho)$ is a square.

Since there are $\frac{1}{6}(p^{2n}-1)p^n$ distinct cubic equations of each type, there are exactly 6 binary transformations of determinant unity which multiply a given C by a constant, necessarily ± 1 by (99_1).

Under G_1 the non-equivalent canonical forms may be taken to be mC_1 and mC_2, where C_1 and C_2 are particular irreducible cubic forms $x^3+\cdots$, such that the equation corresponding to C_1 has a root ρ with $\phi(\rho)=1$, that corresponding to C_2 a root ρ with $\phi(\rho)=\nu$, where ν is a fixed not-square. Further, m takes only one of each pair of non-vanishing values $\pm M$. A cubic form, for which the invariant E (§ 22) is not zero, can be transformed into mC_1 or mC_2 according as $E=m^2$ or $m^2\nu$.

The invariants of the binary cubic form in the $GF[p^n]$, § 22–26.

22. The results under case (v) of § 21 lead us quite naturally to an important invariant E of the binary cubic $f(x, y)$ under the group G_1 of transformations of determinant unity. According to our general standpoint, there exists an invariant which takes prescribed values for each class under G_1. Let E be zero for all reducible cubics, $E=m^2$ for the cubic mC_1, $E=m^2\nu$ for mC_2. Thus E has the value $E_i=m^2\phi(\rho)$ for mC_i ($i=1$ or 2). We readily deduce the value of E for any irreducible cubic $f(x, y)$. One of the cubics mC_i can be transformed with G_1 into f. If λ is a root of $f(x, 1)=0$, (99_1) gives $\phi(\lambda)=\phi(\rho)m^2/a_0^2$, since the coefficient a_0 of $f(x, y)$ is the value of mC_i for $x=\alpha$, $y=\gamma$. Hence $a_0^2\phi(\lambda)=E_i$. Thus, for any irreducible cubic $f(x, y)$, E has the value $a_0^2\phi(\lambda)$. For a reducible cubic, $E=0$ by definition. Hence* for an arbitrary cubic $f(x, y)$, $E=a_0^2R$, where R is the resultant of $x^{p^n}=x$ and $f(x, 1)=0$, the constant factor being determined so that

$$R=\prod_{i=1}^{3}(x_i-x_i^{p^n}), \tag{100}$$

where the x_i are the roots $f(x, 1)=0$. Under the transformation $(x, \delta y)$, each root is multiplied by the determinant δ; then R is multiplied by δ^3, while a_0 is unaltered. *Hence E is a relative invariant of weight* 3.

23. We seek absolute characteristic invariants of the d classes represented by βx^3, where d is the greatest common divisor of $\mu=p^n-1$ and 3, and β is de-

* For a different, but equivalent, definition of E, see these Transactions, loc. cit., p. 307. For the explicit expressions for E for various values of p^n, see pp. 208, 212, 229, 230, 231.

fined by (89). To this end we construct a polynomial Q in the a_i which has the value $\beta^{\mu/d}$ for the class βx^3 (for each of the d values of β) and the value zero for all classes other than these d; then Q will be an absolute invariant of the cubic form. If $d=1$, Q itself is the desired characteristic invariant. If $d=3$, $\omega=\epsilon^{\mu/3}$ is a cube root of unity in the field, and

$$(101)\quad \tfrac{1}{3}(Q+Q^2+Q^3),\qquad \tfrac{1}{3}(\omega^2 Q+\omega Q^2+Q^3),\qquad \tfrac{1}{3}(\omega Q+\omega^2 Q^2+Q^3)$$

are characteristic absolute invariants for the classes x^3, ϵx^3, $\epsilon^2 x^3$, respectively.

The cubic form $f(x, y)$, given by (90), has a triple root if and only if

$$(102)\quad A=a_1^2-3a_0a_2,\qquad B=a_2^2-3a_1a_3,\qquad C=a_1a_2-9a_0a_3$$

all vanish in the field, a result valid for any p. Let

$$(103)\qquad \pi=(1-A^\mu)(1-B^\mu)(1-C^\mu).$$

Evidently $Q\equiv\pi q$. To determine q, we consider the sets a_i for which A, B, C all vanish, so that $Q=q$. For the sets with $a_0\neq 0$, f can be transformed into a_0x^3, so that $Q=a_0^{\mu/d}$. Hence

$$Q\equiv a_0^{\mu/d}+c(1-a_0^\mu),$$

for all the sets. For the sets with $a_0=0$, $a_3\neq 0$, $f\equiv a_3y^3$, so that

$$Q=a_3^{\mu/d}=c,\qquad c\equiv a_3^{\mu/d}+k(1-a_3^\mu).$$

Then for the sets with $a_0=a_3=0$, $f\equiv 0$, $Q=0$, whence $k=0$. Thus

$$(104)\qquad Q=\pi\,[a_0^{\mu/d}+a_3^{\mu/d}(1-a_0^\mu)].$$

For $d=1$, the second factor of Q equals $1-t$, where

$$t=(a_0^\mu-1)(a_3^\mu-1).$$

Since $a(a^\mu-1)=0$, we have $\pi t=I_0$,

$$(105)\qquad I_0=\prod_{i=0}^{3}(a_i^\mu-1),\qquad P=(a_1^\mu-1)(a_2^\mu-1),$$

$$(106)\qquad Q=\pi-I_0 \qquad (\text{if } d=1).$$

In particular, if $p=3$ (whence $d=1$), $\pi=P$.

For $d=3$, the cube of the final factor in (104) is $1-t$. Hence

$$(107)\qquad Q^3\equiv\pi-I_0,\qquad Q^4=Q \qquad (\text{for any } d).$$

24. Let J be the characteristic absolute invariant of the class represented by x^2y. Then $J=(1-D^\mu)L$. Consider the sets a_i with $D=0$, $A\neq 0$, and then the sets with $D=A=0$, $B\neq 0$. We find that

$$L=1+m(A^\mu-1)(B^\mu-1).$$

Consider the sets with $D = A = B = 0$. Then $C = 0$, since

$$-3D \equiv C^2 - 4AB, \tag{108}$$

so that $0 = 1 + m$. Hence

$$J = (1 - D^\mu)\{1 - (1 - A^\mu)(1 - B^\mu)\}. \tag{109}$$

We may give J a more symmetrical form. If $p \neq 3$,

$$D^\mu = (C^2 - 4AB)^\mu,$$

by (108). Also $A(A^\mu - 1) = 0$. Hence, by (103),

$$J = 1 - D^\mu - \pi. \tag{110}$$

This result is true also if $p = 3$, since then $DP = 0$, $\pi = P$.

In view of (110), π is an absolute invariant of the cubic.

25. We can now prove that every invariant of the binary form in the $GF[p^n]$, $p > 2$, is a rational integral function of D, E, Q, I_0. Under the group G_1 of transformations of determinant unity, a complete set of non-equivalent classes are defined by the representative forms $f \equiv 0$, βx^3, $x^2 y$, (93), (94), mC_1, mC_2, in which r and m each take $\frac{1}{2}\mu$ values $\neq 0$, no one value being the negative of another. Here $\mu = p^n - 1$. Hence, for $p > 2$, the number of classes is

$$1 + d + 1 + \tfrac{1}{2}\mu + \tfrac{1}{2}\mu + \tfrac{1}{2}\mu + \tfrac{1}{2}\mu = d + 2 + 2\mu.$$

Hence by § 4 there are exactly $d + 2 + 2\mu$ linearly independent invariants under G_1. These may be taken to be

$$I_0\ Q^\delta\ (\delta = 1, \cdots, d),\ J,\ D^i,\ E^i\ (i = 1, \cdots, \mu). \tag{111}$$

We note that I_0 and J are characteristic invariants of the classes $f \equiv 0$, $x^2 y$; likewise Q for x^3 if $d = 1$, and the linear combinations (101) for the βx^3 if $d = 3$. Suitable linear combinations of the E^i give the characteristic invariants of the classes mC_j, while linear combinations of the $(E^\mu - 1)D^i$ give those for the classes (93) and (94). For an irreducible cubic, $D = E^2$ by (91) and (100). Hence for every cubic,

$$DE = E^3, \qquad D^i E^k = E^{k+2i}, \qquad (E^\mu - 1)D^i = E^{2i} - D^i.$$

Hence, as in § 4, the invariants (111) are linearly independent.* Of these,

* If N is the number of sets of solutions $x : y$ of $f(x, y) = 0$ in the $GF[p^n]$, there exists an absolute invariant K for which $K \equiv N - 1 \pmod p$, with $K = 0$ if f is identically zero, Bulletin of the American Mathematical Society, vol. 14 (1908), p. 316. For $p > 2$, we may give to K the compact expression

$$K = J - E^\mu + (1 - E^\mu)(D^\mu + D^{\frac{1}{2}\mu}).$$

I_0, Q and J are absolute invariants, while the powers of D and E are relative invariants under the total group G.

THEOREM. *The $d + 2p^n$ invariants* (111) *give a complete set of linearly independent invariants of the binary cubic form in the $GF[p^n]$, $p > 2$.*

We may suppress J and introduce 1, in view of (107), (110). We may suppress Q^d and introduce π, etc. Any product of D, E, π, Q, I_0 can be reduced to a linear homogeneous function of the invariants (111), by means of the relations (valid for any p):

$$\begin{gathered} DE = E^3, \qquad D\pi = DQ = DI_0 = E\pi = EQ = EI_0 = QI_0 = 0, \\ \pi Q = Q, \quad \pi I_0 = I_0, \quad I_0^2 = I_0, \quad Q^4 = Q, \quad D^{\mu+1} = D, \quad E^{\mu+1} = E. \end{gathered} \tag{112}$$

Additional invariants of a cubic in the $GF[2^n]$.

26. For $p = 2$, there are $d + 2 + 3\mu$ classes represented by $f \equiv 0$, βx^3, $x^2 y$, (93), (96), and in mC, with $\mu = 2^n - 1$ forms in each of the last three sets. Hence we require μ invariants in addition to (111). These additional invariants together with the powers of D should enable us to differentiate the 2μ classes represented by (93) and (96), and hence to distinguish between the types of reducible cubics having no double root.

We seek the necessary and sufficient conditions that $f(x, y)$ shall be the product of a linear and an irreducible quadratic factor in the $GF[2^n]$. If $a_0 = 0$, $a_1 x^2 + a_2 xy + a_3 y^2$ must be irreducible, so that, by (42), (55),

$$\chi(a_1 a_3 a_2^{2^n-3}) = 1. \tag{113}$$

Next, let $a_0 \neq 0$. Let $a_0 x + a_1 y = \xi$, $y = \eta$. Then

$$a_0^2 f(x, y) = \xi^3 + e\xi\eta^2 + g\eta^3, \qquad e = a_1^2 + a_0 a_2, \qquad g = a_0 D^4. \tag{114}$$

If $e = 0$, the conditions require that there exist one and but one cube root of g; hence there must be a single root of $\omega^3 = 1$, so that $2^n - 1$ must be prime to 3. When the latter condition is satisfied, every element is a cube (§ 21). Hence if $e = 0$, the desired necessary and sufficient conditions are that n be odd and that $g \neq 0$. Finally, let $e \neq 0$. Let $X = e^{-\frac{1}{2}}\xi$, $Y = \eta$. Then

$$e^{-\frac{3}{2}} a_0^2 f(x, y) = X^3 + XY^2 + tY^3 \qquad (t = ge^{-\frac{3}{2}}). \tag{115}$$

If $t = 0$, we obtain $X(X + Y)^2$. Hence must $t \neq 0$. Our problem thus reduces to the characterization of the values $\neq 0$ of t for which there is one and but one root in the $GF[2^n]$ of the equation

$$z^3 = z + t. \tag{116}$$

We shall investigate the relations between the α's and β's in

$$z^{2^k} - z = \alpha_k^2 z^2 + \beta_k z. \tag{117}$$

We have the initial sets of values

$$(118)\qquad \alpha_1=\beta_1=1,\qquad \alpha_2=1,\qquad \beta_2=t+1,\qquad \alpha_3=\beta_3=t+1.$$

Squaring (117) and eliminating z^4, we find that

$$(119)\qquad \alpha_{k+1}=\alpha_k^2+\beta_k+1,\qquad \beta_{k+1}=t\alpha_k^4+1.$$

As k increases, the expressions for the α_k, β_k in terms of t increase rapidly in complexity. We shall prove by induction that

$$(120)\qquad \beta_k=\alpha_k^2+t\alpha_k\alpha_{k-1}^2.$$

The expression for β_{k+1} analogous to (120) will equal (119_2) if

$$t\alpha_k^2[(t\alpha_{k-1}^4+1)+(\alpha_k^2+t\alpha_k\alpha_{k-1}^2)]=0,$$

as seen by eliminating α_{k+1} by means of (119). But the quantity in brackets reduces to $\beta_k+\beta_k\equiv 0$ by (119) with k replaced by $k-1$, and (120). In view of (118), relation (120) holds for $k=2$ and $k=3$. Hence the induction is complete. Thus

$$(121)\qquad \alpha_{k+1}=1+t\alpha_k\alpha_{k-1}^2,\qquad \alpha_{k+1}=\alpha_k^2+t\alpha_{k-1}^4.$$

Upon equating the second members, we obtain an equation designated (121′).

We next prove the following relation between two α's:

$$(122)\qquad \alpha_{k+1}+t\alpha_{k+1}^2\alpha_k^2+\alpha_k^2=t^{2^k-1}.$$

It holds for $k=1$ and $k=2$ by (118). Assume it true as far as $k-1$. Then

$$\alpha_k+t\alpha_k^2\alpha_{k-1}^2+\alpha_{k-1}^2=t^{2^{k-1}-1}.$$

Multiplying the square of the latter by t, we see that (122) is true if

$$(\alpha_{k+1}+\alpha_k^2+t\alpha_{k-1}^4)+t\alpha_k^2(\alpha_{k+1}^2+1+t^2\alpha_k^2\alpha_{k-1}^4)=0.$$

The first part vanishes by (121_2), the second by the square of (121_1).

By (117) for $k=n$, a root of (116) belongs to the $GF[2^n]$ if and only if it satisfies also $\alpha_n^2z+\beta_n=0$; in fact, $z\neq 0$ since $t\neq 0$. If $\alpha_n=0$, then $\beta_n=0$ by (120) for $k=n$, and the cubic has three distinct roots in the field. Hence $\alpha_n\neq 0$ is a necessary condition that the cubic shall have a single root in the field. By (120),

$$(123)\qquad z=1+t\alpha_{n-1}^2\alpha_n^{-1}.$$

This uniquely determined value is actually a root of (116) if and only if $R_n=0$, where

$$(124)\qquad R_k=\alpha_k^3+t\alpha_k\alpha_{k-1}^4+t^2\alpha_{k-1}^6.$$

Multiply (121′) by α_k, (121_2) by $t\alpha_{k-1}^2$, and add. Thus

$$(124')\qquad R_k=\alpha_k+t\alpha_{k+1}\alpha_{k-1}^2.$$

In R_{k+1}, obtained from (124'), we replace α_{k+2} by its value from (121_1). Then

$$R_k^2 + R_{k+1} = (1+t)\alpha_k^2 + \alpha_{k+1} S, \qquad S = 1 + t^2\alpha_k^4 + t^2\alpha_{k+1}\alpha_{k-1}^4.$$

In S we replace α_{k+1} by its value (121_2), and then add the square of (121'):

$$S = (1+t)\{t\alpha_k^4 + (\alpha_k^4 + t^2\alpha_{k-1}^8)\}.$$

The quantity in the last parenthesis equals α_{k+1}^2 by (121_2). Hence

$$R_k^2 + R_{k+1} = (1+t)(\alpha_k^2 + t\alpha_k^4\alpha_{k+1} + \alpha_{k+1}^3).$$

To the last factor add the product of α_{k+1} by (121') with k replaced by $k+1$; there results the left member of (122). Hence

$$R_k^2 + R_{k+1} = t^{2^k} + t^{2^k-1}. \tag{125}$$

Raise to the power 2^i the equation (125) for $k = n-i-1$. Then

$$R_{n-i}^{2^i} + R_{n-i-1}^{2^{i+1}} = t^{2^{n-1}} + t^{2^{n-1}-2^i}.$$

Forming the sum of the latter for $i = 0, 1, \cdots, n-3$, we get

$$R_n = (n-1)t^{2^{n-1}} + \sum_{i=0}^{n-1} t^{2^{n-1}-2^i}, \tag{126}$$

upon replacing R_2 by its value $t^2 + t + 1$. Hence, finally,

$$R_n = t^{2^{n-1}}\{n - 1 + \chi(t^{-1})\}, \tag{127}$$

where χ is the function (42). We note that for $R_n = 0$, $t \neq 0$, then α_n can not vanish; for, if so, (124), with $k = n$, would give $\alpha_{n-1} = 0$, in contradiction with (121_1) for $k = n-1$. Hence we have the

THEOREM. *The cubic $z^3 = z + t$, with $t \neq 0$, has one and but one root in the $GF[2^n]$ if and only if $\chi(t^{-1}) = n - 1$.*

The unique root $z = \rho$ is given by (123), in which the α's are defined by the recursion formulae (121) with the initial values (118). Removing the factor $z - \rho$ from (116), we obtain $z^2 + \rho z + \rho^2 + 1$. Since the latter is irreducible, $\chi(1 + \rho^{-2}) = 1$, whence $\chi(\rho^{-1}) = n - 1$. *When t ranges over the elements $\neq 0$ of the $GF[2^n]$ for which $z^3 = z + t$ has an unique root ρ_t, the latter ranges over the same elements; the function $z^3 - z$ represents a substitution on these elements.*

27. The condition on t becomes $\chi(1 + t^{-2}) = 1$ upon applying

$$\chi(1+s) = n + \chi(s), \qquad \chi(s) = \chi(s^2).$$

We insert the value of t from (115). Hence the condition is

$$\chi(1 + g^{-2}e^3) = 1$$

if $eg \neq 0$. For $e = 0$, $g \neq 0$, this is equivalent to the condition, obtained

above for this case, that n is odd. Hence for $g \neq 0$, e arbitrary, the condition is

$$\chi(\epsilon) = 1, \qquad \epsilon = (g^2 + e^3)g^{2^n-3}, \tag{128}$$

where (and below) $2^n - 3$ is to be replaced by unity if $n = 1$.

Let H be the characteristic absolute invariant for the class of cubic forms having a linear and an irreducible quadratic factor, so that $H = 1$ for such a cubic, while $H = 0$ for all others. If $a_0 \neq 0$, we have $H = \chi(\epsilon)$, ϵ being defined by (128). For, if $g = 0$, then $D = 0$, so that $H = 0$ by definition. Hence in every case

$$H = \chi(\epsilon) + m(a_0^\mu - 1) \qquad (\mu = 2^n - 1).$$

Let $a_0 = 0$; then m equals the left member of (113). Without altering H, we may add $\chi(a_0 a_3^2 a_2^{2^n-4})$ to m. Inserting the values (114) of e, g, we get

$$H = \chi(\lambda), \quad \lambda = \Delta\{(a_1^6 + a_1^4 a_0 a_2 + a_0^3 a_2^3 + a_0^4 a_3^2) a_0 a_0^\nu \Delta^\nu + a_3 a_2^\nu (a_0^\mu - 1)\}, \tag{129}$$

where $\mu = 2^n - 1$, $\nu = 2^n - 4$, the latter being replaced by zero if $n = 1$: while

$$\Delta = a_0 a_3 + a_1 a_2 = D^{\frac{1}{2}} = D^{2^{n-1}}.$$

For $n = 1$ and $n = 2$, λ becomes

$$a_0 a_3 + a_0 a_1 a_2 + a_0 a_1 a_3 + a_0 a_2 a_3 + a_1 a_2 a_3 + a_0 a_1 a_2 a_3,$$

$$a_0 a_1 a_2 + a_0 a_1^3 a_3^2 + a_0 a_2^3 a_3^2 + a_1 a_2 a_3 + a_0 a_1^2 a_2^2 a_3,$$

and $H = \Delta(1 + R + K)$, ΔR, respectively, where R and K are invariants given in these Transactions, vol. 8 (1907), p. 222, p. 230.

For general n, linear combinations of the $D^i H$ $(i = 0, \cdots, \mu - 1)$ give characteristic invariants under G_1 for the classes defined by (96), whose discriminant D is m^4.

THEOREM. *The $d + 2 + 3\mu$ invariants* (111) *and $D^i H$ $(i = 0, \cdots, \mu - 1)$ give a complete set of linearly independent invariants of the binary cubic form in the $GF[2^n]$.*

The product of any two of these invariants can be reduced to a linear combination of them by means of relations (112) and

$$H^2 = H, \qquad D^\mu H = H, \qquad HI_0 = HQ = HJ = H\pi = HE = 0. \tag{130}$$

THE UNIVERSITY OF CHICAGO,
December 1, 1908.