$\sigma_2 = 5^4 \cdot 18$. $\tau_1^5 + \tau_4^5 = -5^4 \cdot 6$, $\tau_1^5\tau_4^5 = 3^5 \cdot 5^5$, $\tau_1^5 = -1875 + 525\sqrt{10}$, $\tau_4^5 = -1875 - 525\sqrt{10}$. $\tau_2^5 + \tau_3^5 = 5^4 \cdot 18$, $\tau_2^5\tau_3^5 = -3^5 \cdot 5^5$, $\tau_2^5 = 5625 + 1800\sqrt{10}$, $\tau_3^5 = 5625 - 1800\sqrt{10}$. $5x = \tau_1 + \tau_2 + \tau_3 + \tau_4$.

The connection with Runge's resolvent is effected by the relation

$$\rho = -5\beta\frac{v - 5\alpha}{v - \alpha},$$

by which equation (1) may be verified. The relation

$$\sigma = \frac{-5^4\beta}{2(v - \alpha)}(v - 5\alpha + \sqrt{v^2 - 6\alpha v + 25\alpha^2}),$$

which includes the preceding and gives the key to equations (2) and (3), was worked out by Lagrange's theorem.

COLUMBIA UNIVERSITY,
April 6, 1915.

THE MADISON COLLOQUIUM LECTURES ON MATHEMATICS.

Part I: On Invariants and the Theory of Numbers. By LEONARD EUGENE DICKSON. New York, American Mathematical Society, 1914.

THE number of new mathematical systems which may be characterized as distinct mutations, whose discovery or development is to be credited to American research, has shown a marked increase within a few decades. The reviewer of Professor Dickson's Lectures of the Madison Colloquium volume has the satisfaction of recording one of these great discoveries, his theory of classes in invariant theory, and of observing how as a result of this discovery, number theory, which long had little contact with the theory of invariants, now has very much in common with it. Dickson's technical memoirs in which the theory of classes and the invariant theory of modular forms were first expounded appeared in 1909. And while the material and indeed much of the method also of the Colloquium Lectures are new, they are dominated by the theory of classes and may, therefore, be regarded as a superstructure of the system founded in his 1909 papers. Lecture I may be regarded also, as introductory to the theory as a whole.

The theory of classes is a general invariant theory, applicable, and applied by the lecturer, to three types of invariants. We now define these. Ordinary invariant theory of algebraical quantics, which we may call the *algebraic* theory, is one in which the coefficients of the linear transformations as well as the coefficients of the transformed quantics themselves are perfectly arbitrary variables. If both of these sets of coefficients are parameters representing residues of a prime number p (or, generally, marks of a Galois field), we have the invariant theory called *modular* invariant theory, due to Dickson. Again if the coefficients of the quantics are variables while the coefficients of the transformations are modular the invariant formations are called *formal modular*. This type of invariant was first defined by A. Hurwitz.

Suppose that S is a system of modular forms, and to follow the inductive plan of the Lectures, suppose that the modulus is p and that S consists of one modular quadratic form q_m in m variables. The coefficients β_{ij} of q_m are parameters to which may be assigned in turn particular sets of residues modulo p, giving the particular forms q_m', q_m'', $\cdots$. Now if the totality of forms $q_m^{(k)}$ be transformed by all of the transformations of the linear group L (mod p) on the variables, the $q_m^{(k)}$ are separated into classes C_i such that two particular forms belong to the same class if and only if they are equivalent under L.

The definition of an invariant now becomes a function-theoretic matter. A single-valued function φ of the undetermined coefficients β_{ij} is an invariant of q_m if φ has the same value for all sets β_{ij}', β_{ij}'', $\cdots$ of coefficients of forms q_m', q_m'', $\cdots$ belonging to the same class.

To determine the value of an invariant φ for a given class C_i we need only assign to the β_{ij} in φ the particular coefficients in a canonical form of q_m which belongs to C_i. In consequence invariants may here be determined from their values by an interpolation formula, or by some particular method whose use would be equivalent to the determination of a function by the interpolation process. And to determine a fundamental system of invariants we need only to determine a set which completely characterizes the classes C_i. Specifically a set of invariants $\varphi_1, \varphi_2, \cdots$ is said to characterize completely the classes when each φ_k has the same value for two classes only when the latter are identical, and the following theorem

proved in Lecture I, taken with the interpolation idea, furnishes not only a powerful construction method, but also an advantageous means of proving that a system which has been constructed forms a fundamental system: If the modular invariants $A, B, \cdots, J$ completely characterize the classes, they form a fundamental system of modular invariants.

The particular problems treated in Lecture I are, first, the reduction of the algebraic quadratic form

$$q_m = \sum_{i,j=1}^{m} \beta_{ij} x_i x_j \qquad (\beta_{ij} = \beta_{ji})$$

to the canonical form

$$x_1^2 + \cdots + x_{m-1}^2 + D x_m^2 \qquad (D = |\beta_{ij}|), \tag{1}$$

or to

$$x_1^2 + \cdots + x_r^2, \tag{2}$$

according as the rank r of D is $= m$ or $< m$. This can be done by linear transformations with complex coefficients of determinant unity, and thus all algebraic quadratic forms may be separated into the classes

$$C_{m,D},\ C_r \quad (D \neq 0,\ r = 0, 1, \cdots, m-1),$$

where, for a particular value of D, $C_{m,D}$ is composed of all forms q_m of determinant D, each being transformable into (1), and so on. Every single-valued algebraic invariant of q_m is a single-valued function of D and r which completely characterize the classes.

Secondly, the corresponding canonical reduction of the modular q_m is made; the forms are (1), (2) and

$$x_1^2 + \cdots + x_{r-1}^2 + \rho x_r^2 \qquad (0 < r < m), \tag{3}$$

and the classes

$$C_{m,D},\ C_{r,+1},\ C_{r,-1},\ C_0 \quad (D=1, \cdots, p-1;\ r=1, \cdots, m-1),$$

where, for instance, $C_{r,-1}$ is composed of all forms transformable into (3). A fundamental system of rational integral modular invariants of q_m is then

$$D, A_1, \cdots, A_{m-1}, I_0,$$

where if $M_1, M_2, \cdots, M_n$ denote the principal minors of order r of D, and d ranges over the principal minors of orders $> r$,

$$A_r = \{M_1^{(p-1)/2} + M_2^{(p-1)/2}(1 - M_1^{p-1}) + \cdots$$

$$+ M_n^{(p-1)/2}(1 - M_1^{p-1}) \cdots (1 - M_{n-1}^{p-1})\} \times \Pi(1 - d^{p-1}).$$

This invariant has the value + 1 for any form of class $C_{r,1}$, for example. Also $I_0 = \Pi(1 - \beta_{ij}^{p-1})$.

In the opening paragraphs of Lecture II the algebraic binary quartic forms f are separated into classes by transformations of the type (algebraic) $T: x = x' + ty', y = y'$. Since invariants under T are seminvariants of f we arrive at a determination of five seminvariants of f from the point of view of the classes, and a proof that they form a fundamental system of rational integral seminvariants. This set does not completely characterize the classes, i. e., is not a fundamental system of *single-valued* seminvariants of f. If f is modular and $p > 3$ eight determinate seminvariants characterize the classes.

Professor Dickson next establishes an inductive method of constructing all of the members of a fundamental system of modular seminvariants of a form of order n from the system for a form of order $n - 1$. For instance if n is divisible by p $(n = pq)$, and $F_n = A_0x^n + A_1x^{n-1}y + \cdots$, the set consisting of A_0 and the fundamental system for

$$\bar{F}_{n-1} = \frac{1}{y}(F_n - \varphi) \qquad [\varphi = A_0(x^p - xy^{p-1})^q] \tag{4}$$

completely characterize the classes of F_n.

By this and similar processes an explicit fundamental system of modular seminvariants of F_n $(p > n)$ is constructed and for particular low orders some explicit systems for $p \not> n$. Invariants are then treated as seminvariants which possess the right type of symmetry, and the subject of linearly independent sets claims attention.

Lecture III is devoted to concomitants of the formal modular type. The first problem solved is that of the determination of a set of rational integral invariant functions of the variables of the modular transformations L, alone, such that any other such function is a rational integral function of those determined, with integral coefficients; i. e., the determination of a fundamental system of universal covariants of the group L. The first such determination was made by Dickson in a paper published in 1911. But for the case of two variables the work is here simplified by the introduction of geometrical concepts.

The transformations being

$$(5)\quad G\colon\ x' \equiv bx + dy,\quad y' \equiv cx + ey,\quad be - cd \equiv 1 \pmod{p},$$

and a point being defined as a pair of homogeneous coordinates $(x, y) = (kx, ky)$, we say that a point is a special point if it is invariant under at least one transformation which is not identity. For it

$$x' \equiv \rho x,\quad y' \equiv \rho y,$$

and ρ is a root of the characteristic congruence

$$(6)\qquad \rho^2 - (b + e)\rho + 1 \equiv 0 \pmod{p}.$$

Only real special points are invariant when (6) has an integral root, and all real points are conjugate under G. It follows that if an invariant of G vanishes for one of the real points it vanishes for all and has the factor

$$L = y\prod_{a=0}^{p-1}(x - ay) \equiv x^p y - xy^p \pmod{p}.$$

If (6) has Galois imaginary roots, the corresponding invariant, representing the conjugate set of imaginary special points, is

$$Q = (x^{p^2}y - xy^{p^2}) \div L,$$

and L, Q is the system sought.

The details of the proof here contain the two principal elements in the author's main method of constructing formal modular invariants and showing what ones are reducible. For with $p = 2$ and $f = ax^2 + bxy + cy^2$ the transformation $x = x' + y'$, $y = y'$ induces the transformation

$$a' \equiv a,\quad b' \equiv b,\quad c' \equiv a + b + c \pmod{2}.$$

This latter may be identified with a special case of (5), and the two universal covariants of this special group become formal modular seminvariants of f. As to reducibility, in view of the theory of conjugate points, we need only show that a covariant has the factor y in order to know that it has the factor L.

Fundamental systems of formal modular seminvariants and invariants of the binary quadratic form modulo p are completely determined in this Lecture, as well as sets for the cubic, and some simpler modular covariant systems modulo 2.

Brief mention is given to the total binary group's form problem, and the invariantive classification of forms.

We now come to the two lectures on modular geometry, and in Lecture IV, the modular geometry and covariantive theory of a quadratic form in m variables modulo 2. Modular geometry is not a new term, but Dickson's formulation of a new theory under the old name marks a notable advance. In modular theories such as G. Arnoux's Essai de Géométrie analytique modulaire (1911), a " curve " is a finite aggregate of real points. Thus an analytic representative of this curve, its quantic, is not determinate in any sense from its points. Dickson assumes at the beginning that the curve, represented for instance by the modular form

$$q_m(x) = \Sigma c_{ij}x_ix_j + \Sigma b_ix_i^2 \quad (i, j = 1, \cdots, m; i < j),$$

modulo 2, shall contain an infinitude of points. That is, he defines a point as a set of m ordered elements $(x_1, \cdots, x_m)$, not all zero, of the infinite field F_2 composed of the roots of all congruences modulo 2 with integral coefficients. The point $(x) = (x_1, \cdots, x_m)$ is called real if the ratios of the x's are congruent to integers modulo 2, otherwise it is imaginary. Then the aggregate of points (x) for which $q_m(x) \equiv 0 \pmod 2$ is called a quadric locus, a conic if $m = 3$. The quadric is thus composed of an infinitude of points, only a finite number of which are real. The investigation of the modular invariant theory of this locus is carried out as a purely arithmetical theory, without any geometrical representation of the locus, although the terminology and to some extent the methods of analytic projective geometry are employed. The lack of any mode of geometrical representation leaves the reader with a feeling of conjecture as to just what kind of geometry in the concrete he is here concerned with, and as to whether something similar, perhaps, to isometric projection could be invented to give a picture of the infinite point cluster constituting the modular curve.

The first invariant formation treated in this lecture is the polar locus

$$P(y, z) \equiv \Sigma c_{ij}(y_iz_j + y_jz_i) \pmod 2.$$

For an odd m the polars of all points (y) have at least one point in common. A determinate common point, whose coordinates happen to be cogredient to the variables, is called the apex of the quadric. Any line through the apex is tangent to the

quadric, and conversely. Thus the quadric has a linear tangential equation. If (C) is the apex, $q_m(C)$ is a formal modular invariant. If it vanishes, the apex is on the locus, which is then a cone. In the case of a conic, reducible to

$$\varphi \equiv X_1X_2 + X_3^2,$$

the only real points on the locus are (1, 1, 1), (1, 0, 0), (0, 1, 0). The apex is (0, 0, 1). The only other real points, three in number, lie on the covariant line

$$X_1 + X_2 + X_3 \equiv 0 \pmod 2. \tag{7}$$

A like configuration on the real points defined by the quinary surface, of great beauty, is constructed, and a similar theory for the case of an even m is given.

The latter half of this chapter, the most technical part of the Lectures, is devoted to a determination, from the standpoint of the classes, of a fundamental system of modular covariants of the ternary quadratic form F with integral coefficients modulo 2.

With a modular analytic projective geometry defined and its covariant theory established Professor Dickson proceeds in Lecture V to a particular curve and a particular feature of the geometry on that curve. This is a theory of plane cubic curves with a real inflexion point which holds true both in ordinary and in modular geometry. After reducing the cubic to the normal form

$$C = x^2y + gy^3 + hy^2z + \delta z^3 \qquad (\delta \neq 0),$$

the author develops the theory of the inflexions. A prominent part is played by the invariants

$$s = -3\delta h, \quad t = -108\delta^2 g.$$

A cubic with integral coefficients taken modulo p, a prime > 3, with at least one real inflexion point and with invariant $s = 0$, and $t \neq 0$, has nine real inflexion points if p is of the form $3j + 1$ and $-t$ is a sixth power modulo p, a single real inflexion point if $p = 3j + 1$ and $-t$ is a quadratic nonresidue of p, and exactly three real inflexion points in all other cases. The author proves a series of similar theorems.

As a whole these Lectures are indeed a most meritorious contribution, suggesting many new problems of many new kinds.

O. E. GLENN.