RUTHERFORD ON MODULAR INVARIANTS

Modular Invariants. By D. E. Rutherford. Cambridge Mathematical Tracts, Number 27. Cambridge, University Press, and New York, Macmillan, 1932. viii+84 pp.

This little tract brings together into small compass the principal results in the theory of modular invariants (both formal and otherwise) up to 1930, thus assembling under one cover both the results of what might be called the American school—Dickson, Glenn, Sanderson, Hazlett, and others—and also the work of E. Noether based on the abstract theory of ideals, as it appears in the research of Steinitz, Artin, and van der Waerden.

The subject had its rise in 1903 in a paper by Hurwitz on the solution of higher congruences, but lay dormant until rediscovered, in another connection, by Dickson in 1907. During the next seven years, the latter developed and finished the theory of modular invariants (here called residual covariants), based on the theory of classes, developed a theory of invariants of the general linear group defined over the Galois field, $GF[p^n]$, proved the finiteness theorem for modular covariants, and made the beginnings of a theory of formal modular covariants (here called formal covariants). In 1913 appeared that short but stimulating and suggestive paper by Miss Sanderson, giving her theorem that given a formal modular invariant, i, of a system of forms under a modular group, G, defined over $GF[p^n]$, we can construct a formal modular invariant, I, such that $I\,x$ is congruent to i in the field for all sets of values of coefficients in the field. In the Madison Colloquium Lectures (1914), Dickson gave a series of lectures on the theory to date. During the next eight years appeared many papers by American writers on the subject, giving treatments of special cases and proving various theorems that are more or less analogous to theorems in the classic theory of algebraic invariants. At the end of Miss Sanderson's paper, she expressed some of the formal invariants and covariants of the binary quadratic for $GF[p^n=3]$ in a symbolic form, and this small but suggestive beginning was now the source of inspiration of Miss Hazlett's paper (1921–22) on the symbolic theory of formal modular covariants of a binary form. This proved that a suitable positive, integral power of every formal modular invariant is congruent in the field to an algebraic invariant of $f(a;\,x)$ and certain related forms, $f(a^{p^n};\,x)$, $f(a^{p^{2n}};\,x)$, $\cdots$, $f(a;\,x^{p^n})$, $\cdots$. The same paper also proved the finiteness theorem for formal modular covariants of a system of binary forms. Then, in 1926, appeared a brief but important paper by E. Noether in which she proved the finiteness theorem for a system of n-ary forms, by using the theory of a ring of polynomials in any number of variables.

Rutherford takes all this theory—at least, all of any importance—and welds the various results and processes into a whole, putting the work of the American school into Part I (51 pages) and following this, in Part II (31 pages) by E. Noether's theorem together with as much of the theory of fields, both algebraic and transcendental, as is necessary for her proof.

Throughout the whole tract, Rutherford is very clear-cut in precisely those places where it is necessary. At the very beginning (§1), he introduces two

new notations, $||$ and $|||$, to denote respectively "is congruent to" and "is identically congruent to." After a couple of sections in which he defines a Galois field, $GF[p^n]$, of order p^n, he states Fermat's theorem for this field and summarizes the essentials of the theory of linear groups in this field. He devotes the fourth section to a clear-cut classification of concomitants of a system of n-ary forms into five essentially different types.

As this is the first time that such a classification has been made and as he changes the name for one type, it will, perhaps, be just as well to reproduce his classification. If the coefficients of the forms are denoted by a's and the coefficients of the linear transformation by $\mathbf{a}$'s, the concomitants have to be studied by essentially different methods according as both the a's and the $\mathbf{a}$'s are indeterminates in the field, CF, of complex numbers, or in the Galois field, $GF[p^n]$, or one in one field and the other in the other field. Type I: If both the a's and $\mathbf{a}$'s are in CF and reductions of the form $p||0$ are allowed, the concomitants are algebraic, which is the classic type and thus not treated here. Type II: If both a's and $\mathbf{a}$'s belong to CF but reductions $p||0$ are allowed in the numerical coefficients that arise as a result of multiplication and addition, the concomitants are called congruent concomitants by the author. Type III: If the a's belong to CF and the $\mathbf{a}$'s to $GF[p^n]$, so that the reductions $p||0$ in the numerical coefficients and $\mathbf{a}^{p^n}||\mathbf{a}$ are permitted, then the concomitant is called formal. (It used to be called a formal modular concomitant.) Type IV: If the a's belong to $GF[p^n]$ and the $\mathbf{a}$'s to CF, so that reductions $p||0$ and $a^{p^n}||a$ are allowed, then the concomitant is called a non-formal concomitant. (To date, these have not been studied.) Type V: If both the a's and the $\mathbf{a}$'s are in $GF[p^n]$, so that reductions $p||0$, $a^{p^n}||a$, and $\mathbf{a}^{p^n}||\mathbf{a}$ are permitted, then the concomitant is called a residual concomitant although formerly called a modular concomitant. Types II to V are grouped together and called modular by Rutherford to distinguish them from Type I, the non-modular or algebraic case. Throughout the rest of this review, we shall use Rutherford's terminology.

After a few other sections devoted to further preliminary notions, he first considers congruent concomitants, proving that a congruent concomitant is completely isobaric and that, if a formal concomitant is isobaric, it is a congruent concomitant. Then he proves that, in the binary case, every congruent concomitant is congruent to an algebraic concomitant of the same system of forms. To date, however, no one has proved in the general n-ary case that every congruent concomitant is congruent to an algebraic concomitant. This is both unfortunate and tantalizing, for the question as to whether a congruent concomitant is congruent to an algebraic concomitant is equivalent to the question as to whether a congruent concomitant is representable symbolically, so that the existence of congruent concomitants not congruent to algebraic concomitants would mean that the symbolical theory of formal modular concomitants developed about 1921 would not be of much use. So, until some one has proved that there exists no congruent concomitant that is not representable symbolically, it is necessary to divide all congruent concomitants into two classes: symbolic and non-symbolic. This phraseology, "until some one has proved that there exists no congruent concomitant" may seem to beg the question, but both the author and reviewer have the feeling that every congruent

concomitant is congruent to an algebraic one. If there exist any that is not algegraic, then such must be very different from those that are algebraic, and even peculiar.

Now follow a couple of sections on universal invariants (=invariants of the group), including Dickson's neat proof that a full system of universal invariants consists of the determinant, L, and various quotients of determinants, the Q's. This is followed by several sections on methods of forming a large number of invariants by using the results on universal invariants and various modular operators, due to Glenn. In his final section on this part of the theory, he proves Hazlett's theorem already quoted.

Next, he turns his attention to residual invariants (called by Dickson and others modular invariants) and he gives Dickson's very beautiful and altogether satisfying theory of classes and characteristic invariants and a new theory of syzygies of residual invariants due to Weitzenböck. In view of Sanderson's theorem, it is easily possible to obtain a full system of residual invariants from a full system of formal invariants by replacing each variable, a_i, by a general number of the field and reducing with respect to the moduli that determine the field. As her theorem has not yet been extended to covariants, there is at present no definitive method of deciding whether a given set of residual covariants form a full set. The next two sections give a method of finding characteristic invariants and a method of finding a smallest full system, of which the work seems to be largely new and due to the author, as the reviewer does not recall having seen it and there is no reference. Then follow several sections of Dickson's work on residual invariants for special cases and a very brief section on the kind of modular covariant that he calls non-formal residual covariant. The latter has not been studied up to the present, but seems to have no importance.

In Part II, he devotes about eleven pages to Steinitz's work on fields (Journal für Mathematik, vol. 137 (1909–10), pp. 167–309; published in book-form with title *Algebraische Theorie der Körper*, under the editorship of R. Baer and H. Hasse, 1930) reproducing his central theorems on algebraic and transcendental expansions and systems both reducible and irreducible. Then he gives the rational basis theorem of E. Noether which was first published in the Göttinger Nachrichten for 1926 (Heft 1, p. 28) which asserts that, if $\{f\}$ be a collection of rational functions $f(x_1, \cdots, x_n)$ of n indeterminates $x_1, \cdots, x_n$ with coefficients from a field K, then from $\{f\}$ it is possible to choose a finite number of functions $f_1, \cdots, f_m$ such that every f is a rational function of these f_i with coefficients from the field K. Such a system of forms $f_1, \cdots, f_m$ is called a rational basis. The proof depends essentially on a well known theorem about the dependence of $n+1$ polynomials in n independent variables and a theorem of Steinitz. Then follow several pages on perfect and imperfect fields, together with the definition of the fields $K^{p^{\pm f}}$ followed by a section on expansions of the first and second sort. Having thus prepared the way, the author is now ready to give van der Waerden's theorem on divisor chains. If R be a ring in which every ideal is finite, then every ideal of R has a finite basis if and only if there exist no chain of ideals $\mathbf{a}_1 < \mathbf{a}_2 < \cdots$, where $\mathbf{a}_{i+1}$ is an actual divisor of $\mathbf{a}_i$, which chain does not come to an end after a finite number of steps. After two more sections on R-modules and a theorem on

rings due to Artin and van der Waerden, he gives the finiteness criterion of E. Noether which asserts that a ring J of polynomials in $x_1, \cdots, x_n$ with coefficients from P, which has no divisors of zero, is finite with respect to P if and only if there exist within J a sub-ring R which is finite with respect to P, such that every element of J is R-entire. From this follows immediately, as a special case, the finiteness theorem for modular covariants.

There are three appendices, of which the first is devoted to a summary of all papers on modular covariants published since the third volume of Dickson's *History of the Theory of Numbers*, where (in Chapter 19) he gave a summary of all papers published up to that date. In the second, he gives a list of papers on the subject; and, in the third, a tabulation of those papers in which modular covariants of an m-ary l-ic are considered for particular cases of m and l.

The reviewer noticed only one misprint that might bother anyone. On page 30, in the footnote, the reference should be to volume 24 (1922) of the Transactions and not to volume 14 (1913).

In the amount of space at his disposal, the author seems to have done about the best possible in presenting his subject. Although the reviewer would most certainly not have followed the order of topics chosen by the author, yet she has to admit that the author has succeeded in giving practically all the widely differing points of view of the various writers. It is unfortunate that the second part of the tract is so radically different from the first; but this is a comment on the mathematics rather than on the author, at the present stage of development. Of course the finiteness theorem is, strictly speaking, a theorem of rings in general and not of modular invariants themselves, so that the sharp cleavage is natural. The author has certainly assimilated the theorems and processes of the theory of modular invariants and he is to be congratulated on his tract.

O. C. HAZLETT