We must rejoice, however, in proof of the wide circulation of Hilbert's ideas, that both a French and an English translation have actually been published. A widely diffused knowledge of the principles involved will do much for the logical treatment of all science and for clear thinking and clear writing in general.

E. R. HEDRICK.

YALE UNIVERSITY,
September, 1902.

DICKSON'S LINEAR GROUPS.

Linear Groups with an Exposition of the Galois Field Theory. By L. E. DICKSON, Assistant Professor of Mathematics in the University of Chicago. Teubner's Sammlung von Lehrbüchern auf dem Gebiete der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen, Volume VI. Leipzig, B. G. Teubner, 1901. 8vo, x + 312 pp.

SHORTLY after the appearance of the first few numbers of the Encyclopädie der Mathematischen Wissenschaften the publishers announced a series of text-books on advanced mathematics to be issued in connection with the Encyclopädie. While the authors of articles in the Encyclopädie were especially requested to take advantage of this series to develop their subjects more fully and thus make them more accessible to the student, other writers were asked to assist to make the series as complete as possible. More than fifty different volumes of this series have already been announced, by almost as many different writers of various countries.

Never before has there been such extensive collaboration to bring the developments in the various parts of our subject within the reach of the student. It is hoped that this series will do much towards increasing the number of well-equipped investigators and thus exert a strong influence towards more substantial progress in various directions. The fact that the authors belong to so many different countries emphasizes the cosmopolitan element in mathematical work and the absence of national prejudices among its devotees.

The present work is the sixth volume of the series and is devoted to a subject which has been developed principally on French and American soil. The fundamental ideas are due to Galois and were published by him at the early age of eighteen

in a memoir entitled "Sur la théorie des nombres." * In this brief memoir Galois introduced a new kind of imaginaries and studied their classification and reduction to the least possible number.

Let $F(x)$ represent an integral function with integral coefficients. If it is possible to find three other integral functions with integral coefficients $F_1(x)$, $F_2(x)$, $F_3(x)$ such that the degrees of $F_1(x)$ and $F_2(x)$ are less than the degree of $F(x)$ and that

$$F(x) = F_1(x)F_2(x) + pF_3(x)$$

then $F(x)$ is said to be reducible modulo p. Otherwise it is said to be irreducible. In the latter case Galois represents a root of the congruence $F(x) \equiv 0 \bmod p$ by i and considers the general expression

$$a + a_1 i + a_2 i^2 + \cdots + a_{n-1} i^{n-1},$$

where $a, a_1, a_2, \cdots, a_{n-1}$ represent integers and n is the degree of $F(x)$. He observes that the $p^n - 1$ values of this general expression, when the coefficients assume separately all the least positive residues modulo p such that not all are simultaneously equal to zero, are powers of a single one of them. Hence all the algebraic quantities which enter into the theory of these imaginaries are roots of the equations of the form $x^{p^n} = x$ and are therefore independent of the form of the special irreducible congruence of degree n.†

From these results it is evident that the p^n values of the general expression of the preceding paragraph constitute a finite domain of rationality, endlicher Körper, or finite field. The interest in this theory has been greatly enhanced by Moore's proof of the fact that the elements of every finite field may be put in a (1, 1) correspondence with those of such a Galois field. ‡ The great simplicity of this field appears perhaps more remarkable when compared with the difficulties which are met in the study of other finite systems, such as Kronecker's modular systems and the theory of groups of finite order.

The first part (pages 3–71) of the present work is devoted to an exposition of the Galois field theory, chiefly in its abstract

* *Bulletin des Sciences de M. Férussac*, vol. 13 (1830), p. 428. Reprinted in *Liouville* vol. 11 (1846), p. 398.

† Oeuvres de Galois, *Liouville*, vol. 11 (1846), p. 400.

‡ This term seems to have been first used by Moore, BULLETIN, vol 3 (1893), p. 73.

form. Beginning with the simplest example, classes of residues with respect to a prime modulus, the author points out the characteristic properties of a Galois field. The greater part of the first chapter is devoted to the proof that no other finite field can exist and that there is only one such field of a given order p^n. The notation and general method of proof are practically the same as those employed by Moore in his paper entitled "A doubly infinite system of simple groups." *

The second chapter is devoted to a proof of the existence of a Galois field of order p^m, $GF[p^m]$, for every prime p and every integer m. This existence follows directly from the fact that there is at least one congruence of degree m which is irreducible modulo p. Instead of proving the latter fact directly as Serret has done,† the author assumes the existence of a $GF[p^n]$ and proves that there are irreducible functions of *every* degree in this field. Since the field of integers modulo p is known to exist, this not only proves the point in question but also exhibits some important properties of the $GF[p^{mn}]$ with respect to the included $GF[p^n]$. A somewhat different method of proof is indicated in the "exercises" which close the chapter.

The determination and classification of irreducible quantics forms the subject matter of the third chapter. Just as in the study of least residues with respect to a prime modulus, it is convenient to make prominent use of the law of exponents in the study of the irreducible quantics. A quantic $F[x]$ of degree m and irreducible in the field of order p^n is denoted by $IQ[m, p^n]$. It is said to belong to the exponent e provided e is the least positive integer for which $F(x)$ divides $x^e - 1$ in the $GF[p^n]$. When $e = p^{nm} - 1$ then $F(x)$ is said to be a primitive irreducible quantic of degree m in $GF[p^n]$. The determination of such quantics forms one of the most difficult problems in the Galois field theory. The latter part of the chapter is devoted to special methods of solving this problem.

Chapter IV is devoted to miscellaneous properties of Galois fields and begins with the study of squares, not-squares, and mth powers in a Galois field. To some readers this part would doubtless have been clearer if they were told explicitly that they were concerned with operators of a cyclic group C. The statement that "every mark has one and only one square root in the $GF[2^n]$" would thus appear as a special case of the theorem

* Moore, Published Papers of the Am. Math. Soc., vol. 1 (1896), p. 208.
† Serret, Algèbre supérieure, vol. 2 (1885), p. 137.

that in an abelian group of odd order every operator is the square of one and only one operator. It is true the zero element of $GF[2^n]$ is not contained in C but the theorem evidently applies to it. Moreover, it may be observed that 0 and 1 are the only two marks of $GF[2^n]$ which coincide with their square roots.

Similarly, Section 62 is equivalent to saying that all the operators of a subgroup of even index are squares of operators of C. The theorem of Section 63 is clearly true for any abelian group and is a direct consequence of the facts that in an abelian group there is a subgroup whose order is any arbitrary divisor $[(p^n - 1)/d]$ of the order of the group and if each operator of an abelian group is raised to a power prime to the order of the group the resulting operators may be put in a (1, 1) correspondence with the original operators. In other words, every operator of an abelian group is the mth power of just one of its operators, where m is any number prime to the order of the group.

In such developments it is always a question what an author should presuppose. If a knowledge of the fundamental abstract properties of abelian groups had been assumed on the part of the reader it would have been possible at various places to indicate more clearly the contact with abstract group theory and also to bring out additional facts in the same amount of space notwithstanding the fact that the zero element in the Galois field requires separate treatment from this standpoint.

Sections 64–67 are devoted to generalizations of Jordan's results in regard to the solutions of certain quadratic equations in a Galois field. This is followed by a study of the additive groups and their multiplier Galois fields as employed by Moore. A set of m marks $\lambda_1, \lambda_2, \cdots, \lambda_m$ belonging to the $GF[p^n]$ and linearly independent with respect to the $GF[p]$ give rise to p^m distinct marks

$$c_1\lambda_1 + c_2\lambda_2 + \cdots + c_m\lambda_m \qquad (c_i = 0, 1, \cdots, p - 1)$$

with respect to the larger field. These are said to form an additive group of rank m with respect to the $GF[p]$. In particular, the $GF[p^n]$ may be regarded as an additive group of rank n. These conceptions are generalized and a condition for the linear independence of marks with respect to an included field is developed. The chapter closes with a consideration of

Newton's identities for sums of powers of the roots of an equation belonging to a Galois field.

In this chapter the term *group* is used for the first time but no definition is given. The statement "since the *sum* of any two of these p^m marks may be expressed as one of the set, they are said to form an additive group" cannot be regarded as a definition. Moreover, it is apt to mislead the reader since such incomplete definitions of group are not uncommon in the mathematical literature. On the other hand, if the reader is supposed to be familiar with the definition of the term it would have been of interest to contrast this additive group with the multiplicative group formed by the marks of a field, which differ from zero.

The fifth and last chapter of Part I is devoted to the analytic representation of substitutions on marks of a Galois field. This subject is treated quite fully in Part I of the author's dissertation * where extensive references are given. Beginning with the definition of a substitution quantic the author develops the analytic conditions which characterize such functions and gives a table of all such reduced quantics whose degree is less than 6. A study of the Betti-Mathieu group and six suggestive exercises furnish the close of these interesting and important developments of modern algebra.

The second part of the present volume (pages 75–310) is devoted to a study of the most important properties of linear groups in a Galois field. Some of these groups were investigated in the field of integers modulo p by Galois, Serret and Jordan. These results are here generalized for the larger field and new systems are investigated ab initio in this field. The work of Moore first emphasized the importance of employing the general Galois field in linear group problems as the investigations are generally not much more complicated and the results are more general. Jordan frequently indicated these generalizations without entering upon their complete development.

A great part of the text is taken directly from the author's numerous memoirs, but in other parts the method of presentation differs widely from that employed in the original papers. More stress seems to have been laid upon clearness in presentation and some of the longer calculations have been avoided. The work has thus gained considerable in attractiveness and

* Dickson, *Annals of Mathematics*, vol. 11 (1897), p. 65.

has become more suitable to serve its purpose as an introduction to the extensive subject of linear groups in a finite field.

The first chapter begins with two definitions of the general linear homogeneous group on m indices with coefficients in the $GF[p^n]$. The group is denoted by $GLH(m, p^n)$ while the symbol $GLH[m, p^n]$ is used to represent its order. The latter is proved to be

$$(p^{nm} - 1)(p^{nm} - p^n)(p^{nm} - p^{2n}) \cdots (p^{nm} - p^{n(m-1)}).$$

For $n = 1$ the factors of composition were determined by Jordan in his Traité des Substitutions. For the general value of n they were determined independently by the author and by Burnside. The general case is considered here, and from these factors it follows directly that the group of all linear fractional substitutions $LF(m, p^n)$ in the $GF[p^n]$ on $m - 1$ variables and having the determinant either unity or some mth power in the field, is simple except in the two special cases $(m, p^n) = (2, 2)$ or $(2, 3)$.

The abelian linear group and a generalization of this group form the subjects of Chapters II and III. The former has been investigated by Jordan in the field of integers, while the latter is mentioned by him but he did not investigate its properties. Both have been studied by Dickson in the general Galois field and are here presented in this general way. The term abelian was first applied to these groups by Jordan, although they are not, in general, commutative. To distinguish them from commutative groups they are called abelian *linear* groups.

The hyperabelian group consists of the totality of linear homogeneous substitutions in the $GF[p^{2n}]$ which leave absolutely invariant the function

$$\psi \equiv \sum_{l=1}^{m} \begin{vmatrix} \xi_{2l-1} & \xi_{2l} \\ \xi_{2l-1}^{p^n} & \xi_{2l}^{p^n} \end{vmatrix}.$$

It was first studied by the author in the *Proceedings of the London Mathematical Society*, volume 31, and forms the subject of Chapter IV of the present volume. It is distinct from the hypoabelian groups studied by Jordan in his Traité and by Dickson in the BULLETIN and elsewhere. Moreover, it must be distinguished from Picard's hyperabelian group of infinite order. The totality of its substitutions whose coefficients belong to the included $GF[p^n]$ constitute the special abelian

linear group $SA(2m, p^n)$. The latter is transformed into itself by a subgroup of the hyperabelian group whose order is $p^n + 1$ times the order of $SA(2m, p^n)$.

The greater part of Chapter V is taken directly from the author's article entitled "The structure of the linear homogeneous groups defined by the invariant $\lambda_1\xi_1^r + \lambda_2\xi_2^r + \cdots + \lambda_m\xi_m^r$." * Chapter VI is devoted to a new exposition of the theory of compounds of a linear homogeneous group. This theory is entirely due to the author, having been introduced by him in several papers published in 1898.† He also employed it in his new definition of the general abelian linear group, which was published in the first volume of the *Transactions* of the AMERICAN MATHEMATICAL SOCIETY.

In Chapters VII and VIII the linear homogeneous group in the $GF[p^n]$ defined by a quadratic invariant is investigated. The case when $p > 2$ is considered in the former and that when $p = 2$ in the latter of these chapters. By employing the theory of compounds, developed in the preceding chapter, the investigations, especially when $p > 2$, have been presented in a much simpler manner than in the original papers. Chapter VIII is followed by twelve exercises with a number of suggestions, covering the text of the first eight chapters of this part.

The next three Chapters (IX–XI) are devoted respectively to linear groups with certain invariants whose degree exceeds 2, canonical form and classification of linear substitutions, and operators and cyclic subgroups of the simple linear fractional group $LF(3, p^n)$. In Chapter XII the subgroups of the linear fractional group $LF(2, p^n)$ are studied. The first statement of the last paragraph of this chapter is evidently incorrect. For instance, the icosahedral group may be represented as a transitive substitution group of degree 12, but it does not contain a complete system of 12 conjugate subgroups. If a simple group is represented on the smallest possible number of letters it must be primitive, and a primitive group of degree N must always contain a complete system of N conjugate subgroups; but this is not necessarily true of imprimitive groups of degree N even if they are simple.

The developments of Chapters XIII and XIV are quite different from those which precede. In the former a number

* Dickson, *Math. Annalen*, vol. 52 (1899), p. 561.

† Dickson, BULLETIN, vol. 5 (1898), p. 120; *Proc. Lond. Math. Soc.*, vol. 30 (1898), p. 70.

of theorems in regard to abstract groups are developed. Beginning with the well known theorems of Moore with respect to the abstract definitions of the alternating and the symmetric groups and the classic theorem due to Hamilton and Dyck in regard to the abstract definition of the icosahedral group, the author develops a number of other theorems with respect to the generational relations of known groups. Some of these are employed in the study of the group of the equation for the 27 straight lines on a general surface of the third order, which is the subject of Chapter XIV. The treatment of this subject seems to be especially commendable.

The study of linear groups has thus far been the most fruitful in increasing our knowledge of simple groups. As in Jordan's Traité des Substitutions, so in the present work a great deal of attention is given to the factors of composition of the groups under consideration. In this way a number of systems of simple groups are established and the closing chapter is fittingly devoted to a summary of the known simple groups. With a few exceptions all of these groups are included in one or more known infinite systems. It may be observed that the simple group of order 7920 cannot be represented on less than 11 letters so that 9 should be replaced by 11 in the list on page 309.

The present work seems to be the first separate volume on the subject to which it is devoted. The treatment of the first part has much in common with Chapters III and IV of Serret's Algèbre supérieure, volume 2 (1885), while the second part seems to have been mostly influenced by Jordan's Traité des Substitutions (1870). The author's thorough acquaintance with his subject, and his experience as a writer, have enabled him to present a somewhat abstract subject in an unusually attractive manner. It may be hoped that the book will do much to create a wider interest in these fields of higher algebra. While the generality of treatment calls for considerable maturity on the part of the reader, yet not much special knowledge is presupposed.

G. A. MILLER.

STANFORD UNIVERSITY.