THE THEORY OF SUBSTITUTIONS.

The Theory of Substitutions and its Applications to Algebra. By Dr. EUGEN NETTO, Professor of Mathematics in the University of Giessen. Revised by the Author and translated with his permission by F. N. COLE, Ph.D., Assistant Professor of Mathematics in the University of Michigan. Ann Arbor, Mich., The Register Publishing Company, 1892. 8vo, pp. xii. + 301.

NETTO'S "Substitutionentheorie und ihre Anwendungen auf die Algebra" appeared for the first time in 1882; it was followed, in 1885, by an Italian edition, and now we have the pleasure of welcoming an English edition, revised by the author and translated into English by Dr. Cole.

The mathematical public at large, and the English-speaking part of it in particular, are greatly indebted to Dr. Cole for his careful and expert translation. Mastering the subject as well as both languages in full extent, Dr. Cole has transformed the sometimes rather tough material into clear and fluent English. We are especially obliged to him for the fortunate choice of many technical terms, alien so far to the English mathematical language.

We are equally indebted to the author for the numerous valuable additions by which this new edition has been enlarged and improved.

The great merit of Netto's book consists in the skilful and highly pedagogical presentation of the theory of substitutions, given in the first part of the book. The reader is gradually led from the most elementary considerations on symmetric and alternating functions to the general theory of unsymmetric functions of n independent elements, out of which the theory of substitutions is step by step evolved, the unsymmetric functions serving all the while as a concrete substratum for the abstract conclusions of the theory of substitutions. By this means an easy and attractive entrance into the theory of substitutions is gained, accessible even to the beginner, and it may fairly be said that Netto's book has largely contributed to spread the knowledge of this important branch of mathematics.

While thus fully acknowledging the high and lasting merits of the first part of Netto's book, we cannot withhold our opinion that the author has not been equally successful in his attempt to simplify Galois' theory of the algebraic solution of equations, which forms the principal subject of the second part. The great difficulties which are contained in Galois' theory, are, it seems to us, not sufficiently considered, and the comparative simplicity of the deductions is only obtained at the cost of rigor.

The following review* will be divided into four sections :
I. The first part of Netto's book.
II. Excursus on the principal difficulties of Galois' theory.
III. Analysis of Netto's exposition of the theory of the group of an equation.
IV. The remaining chapters of the second part.

I.

The first part is devoted to the theory of substitutions and of integral functions. It opens in chapter I., with an exposition of the principal properties of *symmetric functions* of n independent quantities $x_1, x_2, \ldots x_n$. A symmetric function remains unchanged in form, and consequently also in value, when the x's are permuted in any way, and is therefore, at the same time, a *single-valued* function ; conversely every single-valued function of n independent elements is symmetric in these elements. The simplest symmetric functions are the elementary symmetric functions :

$$\begin{aligned} c_1 &= x_1 + x_2 + \ldots + x_n \\ c_2 &= x_1 x_2 + x_1 x_3 + \ldots + x_{n-1} x_n \\ &\vdots \\ c_n &= x_1 x_2 \ldots x_n. \end{aligned}$$

Every integral symmetric function of $x_1, x_2, \ldots x_n$ can be expressed as an integral function of the elementary symmetric functions $c_1, c_2, \ldots c_n$.

If a function is not symmetric, it will be changed in form, and consequently, if the x's are independent, also in value, by some of the possible interchanges of the x's. We shall have two-valued, three-valued, m-valued functions, according to the number of different values they take when the x's are permuted in all possible ways. The simplest unsymmetric functions are the *two-valued functions*. The square root of the discriminant

$$\sqrt{\Delta} = \prod_{\lambda,\mu} (x_\lambda - x_\mu)$$

offers a first example of a two-valued function ; it is, moreover, an *alternating* function, because its two values differ only in sign. Every integral alternating function is the product of $\sqrt{\Delta}$ into an integral symmetric function. Every integral

* Reviews of the first edition will be found in : *Fortschritte der Mathematik*, 1882, p. 90. *Zeitschrift für Mathematik*, 1883, part II., p. 181. *Bulletin des Sciences Mathématiques*, 1883, p. 57.

two-valued function is of the form $S_1 + S_2\sqrt{\Delta}$, (where S_1 and S_2 are integral symmetric functions) and satisfies an equation of the second degree whose coefficients are integral functions of $c_1, c_2, \ldots c_n$.

If we pass to functions of a greater number of values, we soon perceive that the knowledge of the number of its values is not sufficient to characterize an unsymmetric function; we must go a step further and turn our attention from the functions to the interchanges of the x's, and in doing so, we enter the peculiar domain of the *theory of substitutions*.

After a few necessary explanations concerning notation, terminology, and some elementary properties of substitutions, the most important conception of the whole theory is introduced, that of a *group of substitutions*, a group being defined as a system of substitutions which reproduces itself by multiplication of its individual members. Those substitutions which leave a function $\varphi(x_1, x_2, \ldots x_n)$ unchanged, constitute a group called the group of φ. And *vice versa*: for every group of substitutions there are functions which are unchanged by all the substitutions of the group and by no others. This theorem contains the basis of a classification of functions of n elements: each class ("family"*) contains all the functions which belong to the same group.

Here arises the problem: To determine all the possible groups of substitutions of n elements.

The general solution† of this problem, however, presents difficulties as yet insuperable. Still, a great number of theorems concerning the construction of groups are known, and a first series of them are given in the remaining sections of chap. II. They refer to the symmetric group, the alternating group, the cyclic groups, and others of a more special nature.

Chapter III. is devoted to the different values of a multiple-valued function. Here we have first the theorem: The order r of a substitution-group G is always a divisor of $n!$; and every function φ which belongs to G, takes

$$\rho = \frac{n!}{r}$$

different values ("conjugate values") when operated upon by all the $n!$ substitutions. These results concerning the relation of the symmetric group and one of its subgroups can

* The term is only introduced in chap. V.

† That is for an indeterminate n. For a numerically given value of n, the problem can always be solved by a finite number of trials: the solution has been pushed as far as $n = 9$: compare several papers by ASKWITH and CAYLEY, *Quarterly Journal of Mathematics*, 1890, 1891, 1892.

be extended to the relation between any group and one of its subgroups.

Every one of the ρ conjugate values of a ρ-valued function belongs itself to a certain group; thus we obtain, corresponding to the ρ values, ρ *conjugate groups*. They are found to be "similar," and can be derived from the group G by the process of "transformation."

If it happens that these ρ groups coincide, or in other words, that the ρ conjugate values all belong to the same group, then G is called—to anticipate a term introduced only in the following chapter—a *self-conjugate subgroup* of the symmetric group. The alternating group is always a self-conjugate subgroup of the symmetric group, and (excepting the case $n = 4$) it is, beside the trivial group 1, the only self-conjugate subgroup of the symmetric group. On the other hand, the ρ conjugate values of our integral function φ are the roots of an equation of degree ρ whose coefficients are integral functions of the elementary symmetric functions $c_1, c_2, \ldots c_n$. And if now we ask under what circumstances this equation becomes binomial, it is easily shown that the group of the function φ must be a self-conjugate subgroup of the symmetric group. Combining this with the above result, we are led to the theorem:

The only unsymmetric functions of which a power can be symmetric, are the alternating functions.

Three different proofs of this important theorem are given; one of them is based on the properties of the *discriminant* of φ:

$$\Delta_\phi = \prod_{\alpha,\beta} (\varphi_\alpha - \varphi_\beta)^2$$

Along with these developments, we find, in chap. III. other investigations of a different nature. The problem of the *construction of groups* is again taken up, and a new and simplified proof of Cauchy-Sylow's theorem is given. As a new addition, a very interesting theorem due to Netto deserves special notice:

Suppose a group H of order h contains in one of its substitutions a cycle of order k, say $\omega_1 = (x_1, x_2, \ldots x_k)$. If h' is the order of that subgroup of H whose substitutions do not affect the k letters $x_1, x_2, \ldots x_k$, then h is divisible by the product $h'k$. And if now we transform the cycle ω_1 with respect to all the substitutions of H, we obtain $h/h'k$ distinct "conjugate cycles." Every one of these $h/h'k$ cycles occurs h' times in the group H; hence, the cycle ω_1 and its conjugates with respect to H occur h/k times in the group H. The number of letters in all these cycles is therefore equal to the order h of the group H. The special case $k = 1$ leads to a theorem previously given by Frobenius.

The fourth chapter treats of four properties of groups which are, each in its peculiar way, of fundamental importance for the algebraic solution of equations: transitivity, primitivity, composition and isomorphism.

a) A group is called *transitive* if its substitutions permit any selected element to be replaced by every other element; otherwise intransitive. Extending this definition to a set of k elements, we obtain the idea of a k-fold transitive group. The alternating group is $(n-2)$-fold transitive. The principal problem concerning transitive groups is the determination of an upper limit for the degree of transitivity for a group of degree n, which is neither the symmetric nor the alternating group. A series of special theorems due to Mathieu, Jordan and Netto, are given.* A new term is introduced, the *class of a substitution:* a substitution is of the k^{th} class if it affects exactly k letters.

b) Closely connected with the idea of transitivity is that of *primitivity* and *non-primitivity*. A simply transitive group is called non-primitive when its elements can be divided into systems, each including the same number, such that every substitution of the group replaces all the elements of any system either by the elements of the same system or by those of another system. This section is entirely rearranged in the new edition and numerous new researches are added. We call particular attention to §§ 66, 67, where the relation between a non-primitive group and the corresponding group of substitutions of the systems is explained.

c) The fundamental idea of the *decomposition* of a group, due to Galois, has been touched a first time in the preceding chapter. Here the entire theory is developed.

A subgroup H of a group G is called *self-conjugate,* if it is commutative with all the substitutions of G, in symbols, if

$$t^{-1}Ht = H,$$

for every substitution t of G. A group which contains a self-conjugate subgroup, different from 1, is called a *compound group,* otherwise a *simple* group. If G contains no other self-conjugate subgroup K which includes H, then H is a *maximal* self-conjugate subgroup. The *series of composition* of a group G is a series of groups, beginning with G, ending with 1, such that each group is a maximal self-conjugate subgroup of the group immediately preceding it. The quotients of the orders of two consecutive groups are called the *factors* of composition of G. A compound group may admit of dif-

*For a further development of this theory we refer to two papers by BOCHERT, *Mathematische Annalen*, vols. 29 and 33.

ferent series of composition; in this case the factors of composition in the different series are identical, apart from their order. The series of composition of the symmetric group of n elements consists, if $n \gtrless 4$, of the alternating group and the group 1; for $n \gtrless 4$ the alternating group is simple.

d) *Isomorphism* is, in the simplest case, a one-to-one relation between the substitutions of two groups of the same order of such a nature that to the product of any two substitutions of the one corresponds the product of the two corresponding substitutions of the other group. The definition can be extended so as to apply also to a one-to-q-correspondence, and even to a p-to-q-correspondence: p-q-fold isomorphism. Isomorphic groups have a certain class of properties in common: for instance, in two simply isomorphic groups corresponding substitutions are of the same order; to a (self-conjugate) subgroup in the one corresponds a (self-conjugate) subgroup in the other, and so on.*

A very welcome addition is the introduction of the *quotient-group*, which plays such an important part in numerous recent researches. The easiest, though not best, way of defining it is perhaps the following: Let G be a group of order mk, H a self-conjugate subgroup of G of order m, $\varphi(x_1, x_2, \ldots x_n)$ a function belonging to H. The function φ, on being operated upon by all the substitutions of G, takes k values, $\varphi_1 = \varphi$, $\varphi_2, \ldots \varphi_k$. If now we apply to these k functions simultaneously all the substitutions of G, the φ's undergo a transitive substitution-group T of order k, which is 1-m-fold isomorphic with G. This group T is called, according to Hölder, the quotient of G and H, and is denoted by

$$T = G : H.$$

Netto adopts Hölder's definition, which is more abstract and independent of the function φ.† Likewise Hölder's *factor-groups* (the quotients of two consecutive groups in a series of composition) are mentioned.

In chapter v. Netto returns to the discussion of rational functions of n independent quantities, continuing and generalizing the investigations of chapter iii.

The fundamental problem is: Given (a) a group G and one of its subgroups, H; (b) a rational function φ belonging to G and a rational function ψ belonging to H. What algebraic relation exists between φ and ψ? The answer is given in two theorems due to Lagrange:

---

*See below the remarks on groups of operations.

† Another very elegant definition is given by Dyck, *Math. Annalen*, vol. 20, pp. 11–15.

I.) φ is expressible as a rational function of ψ and of the elementary symmetric functions $c_1, c_2, \ldots c_n$ of $x_1, x_2, \ldots x_n$.
This rational function is of the form :

$$\varphi = \frac{g(\psi ; c_1, c_2 \ldots c_n)}{\Delta_\psi}$$

where g is an integral function of $\psi, c_1, c_2, \ldots c_n$, whereas Δ_ψ denotes the discriminant of ψ.
Two special cases of this theorem are particularly important :
1) Two functions belonging to the same group can be rationally expressed one in terms of the other. Hence the totality of all rational functions belonging to the same group form indeed a "family" (*Gattung*) in the sense in which Kronecker uses the word.
2) Every rational function of n independent elements can be rationally expressed in terms of every $n!$-valued function ; for instance in terms of

$$\xi = \alpha_1 x_1 + \alpha_2 x_2 + \ldots \alpha_n x_n,$$

where the α's are arbitrary parameters.
II.) If the order of G is m times that of H, ψ satisfies an algebraic equation of degree m whose coefficients are rational functions of φ and $c_1, c_2, \ldots c_n$.
Here again the important question arises : Under what circumstances can this equation become binomial ? The answer is : H must be a self-conjugate subgroup of G ; conversely, if H is a self-conjugate subgroup of G, and if moreover m is a prime number, then there exist always, in the family of ψ, functions for which the equation becomes binomial. These results furnish a complete insight into the mechanism of the solution of the general equations of the second, third, and fourth degrees. Anticipating developments of chap. x., the general principle of their solution may be exhibited as follows : Let

$$G - H - I - \ldots - 1$$

be the series of composition of a group G ; and suppose that all the factors of composition of G are prime numbers. On the strength of the last proposition, it is then possible to determine a series of functions $\varphi, \psi, \chi \ldots \xi$, belonging to the groups $G, H, I, \ldots 1$ respectively, and such that each function can be obtained from the function immediately preceding it by solving a binomial equation.
Now for $n = 2, 3, 4$, all the factors of composition of the symmetric group are prime numbers ; we may therefore apply

this principle to the symmetric groups of 2, 3, 4 elements and thus obtain the solution of the general equations of the degrees 2, 3, 4 by means of a chain of binomial equations. For the details, see §§148 to 150.

The remaining three chapters of the first part are devoted to special investigations concerning the existence or construction of substitution-groups between a given number of elements. We must confine ourselves to a short enumeration of the principal problems.

We have seen that the *number ρ of values of a multiple-valued function* of n elements is always a divisor of $n!$ This is a first strong restriction upon the possible values of ρ. Further restrictions are given in a series of theorems due to Bertrand, Cauchy, Serret, and Jordan.*

Every substitution-group is simply isomorphic with a *regular group*, that is, a transitive group whose order equals the number of elements; hence the importance of regular groups. Netto determines all regular groups whose order is either a prime number or the product of two prime numbers.

The circular substitution $(x_0, x_1, \ldots x_{p-1})$ may be written in an *abbreviated form*

$$\binom{x_z}{x_{z+1}}, \quad (z = 0, 1, 2, \ldots p-1),$$

or still shorter

$$| \, z \quad z+1 \, | \pmod p,$$

if we agree to consider two indices as identical when they are congruent (mod p). In a similar way, the more general symbol

$$| \, z \quad \beta z + \alpha \, | \pmod p$$

in which α, β are two integers and β not $\equiv 0 \pmod p$, represents a substitution if p is a prime number. The aggregate of all substitutions which are obtained by giving α, β all admissible values, form a group of order $p(p-1)$, called the *metacyclic group*. These results may be generalized in several directions: Either we may pass to *fractional* linear substitutions

$$\left| \, z \quad \frac{\alpha z + \beta}{\gamma z + \delta} \right| \pmod p, \quad (z = 0, 1, \ldots p-1, \infty);$$

they form a group of order $(p+1)\,p\,(p-1)$ which is of great importance in the theory of modular equations.

---

* For a further development of this difficult part of the theory we refer to two papers by BOCHERT, *Math. Annalen*, vols. 33 and 40.

Or we may introduce, instead of a single index z, a system of indices $z_1, z_2, \ldots z_k$; this leads to the theory of "*arithmetic*" and "*geometric*" substitutions, which plays an important part in the theory of solvable equations.

Or we may pass to the general theory of the *analytical representation* of substitutions (Hermite).

All these problems are studied in detail.

A particular interest attaches to the last subject which we have to mention, Kronecker's investigations on groups of *commutative substitutions*, not only on account of their importance for the theory of Abelian equations, but because, transgressing the limits of the theory of substitutions, they point to a more general field of research, the theory of *groups of operations* in general. With this one exception, Netto, true to his programme clearly expressed in the preface, strictly confines himself to groups of substitutions proper. Yet the general theory of groups throws such a new light backwards on the theory of substitution-groups out of which it has developed, that a few additional remarks on this important extension of the theory of substitutions may not be out of place.

It seems that Cayley * was the first to conceive the idea of extending the conception of a group, originally restricted to substitutions, to any operations which admit of repetition and combination. From this standpoint, two groups are considered as identical if the laws of combination of their operations are the same for both, no matter what the particular nature of the operations may be, whether they are substitutions, or rotations, or quaternions, or linear transformations, etc. Using the modern terminology, we may express the same idea in another form: Simply isomorphic groups are considered as identical. A systematic exposition of such a general theory of groups has first been given by Dyck.†

Now all possible properties of substitution-groups may be divided into two classes:

I.) Properties which are independent of the peculiar nature of the operations and are therefore properties of groups of operations in general. Such are the theorems on the relations between a group and its subgroups, on cyclic groups, Cauchy-Sylow's theorem,‡ and those on self-conjugate subgroups, on the construction of groups of a given order, on isomorphism, etc. Their common characteristic is that they are not destroyed by a transition to any simply isomorphic group.

---

* On the theory of groups, *Phil. Mag.*, 4th series, vols. 7 and 18, and *American Journal of Mathematics*, vols. 1 and 11.

† *Math. Annalen*, vols. 20 and 22; besides, we refer to KLEIN, "Vorlesungen über das Ikosaeder," pp. 5–8, and HÖLDER, *Math. Annalen*, vol. 34, pp. 28–39.

‡ See FROBENIUS's proof, *Journal für Mathematik*, vol. 100, p. 179.

II.) Properties which depend on the peculiar nature of the operations, as the theorems on the symmetric and alternating groups, on transitivity and primitivity, on the construction of groups of a given degree, on the analytical representation of substitutions, etc.

An analogon, familiar to all, may serve to illustrate this classification: In the theory of algebraic curves, we distinguish between those properties of a curve which are not destroyed by projection and those which are destroyed. To the transition from one curve to another curve, projective with the first, corresponds in our case the transition from one group to another group, simply isomorphic with the first.

II.

Throughout the first part of Netto's book, the elements $x_1, x_2, \ldots x_n$ are regarded as entirely independent quantities.* We may therefore consider them as the roots of the *general equation* of the nth degree

$$(x - x_1)(x - x_2) \ldots (x - x_n) \equiv x^n - c_1 x^{n-1} + c_2 x^{n-2} \ldots \pm c_n = 0,$$

whose coefficients are themselves independent quantities. And all our theorems on rational functions of n independent quantities may be interpreted as theorems on rational functions of the roots of the general equation of the nth degree.

At first sight nothing seems simpler than the transition from the general equation to any *special equation*, that is, an equation whose coefficients are no longer independent quantities, but have either numerically given values or else are functions of one or more independent parameters. And yet, in this transition there are difficulties hidden which, it seems to us, can scarcely be too much emphasized. Before entering into a discussion of the second part of Netto's book, it will therefore be well to premise some remarks concerning the transition from general to special equations.

1) *First difficulty: domain of rationality.*

The peculiar difficulty of the theory of special equations faces us right at the outset when we try to define what we mean by saying an equation is *algebraically solvable.* The problem may be considered from two entirely different standpoints; it may either be regarded as a problem of the theory of functions or of pure algebra. Accordingly, we obtain two different definitions. We may say

* With the exception of a few special investigations, such as §§ 32, 111.

either (*theory of functions*): | or (*algebra*):

An equation is algebraically solvable, if its roots can be derived from the coefficients

and a number of constant quantities | *and the numerical unity* 1*

by means of the five elementary algebraic operations, viz.: addition, subtraction, multiplication, division, extraction of roots of prime index, applied a finite number of times.

The difference between the two definitions is precisely the characteristic difference between theory of functions and algebra: in the theory of functions the fundamental distinction refers to variable quantities and constant quantities; our whole attention is directed toward the variables, and the arithmetical nature of the constants is left out of consideration. In algebra, on the contrary, the principal distinction refers to rational quantities and irrational quantities, and the chief interest concentrates upon the arithmetical nature of the constants.

The theory-of-functions-definition is applicable only to equations whose coefficients contain at least one variable parameter; if applied to numerical equations it would, combined with Gauss's theorem on the existence of the roots of an algebraic equation, lead to the result that every numerical equation is algebraically solvable.

The algebraic definition, with which we are here exclusively concerned, is applicable to all algebraic equations, whether the coefficients contain variable parameters or not. It admits, however, of a generalization which is essential for our further developments: The coefficients may themselves be derived from other quantities, regarded as known, by means of rational operations. Denoting the latter quantities by

$$\Re', \Re'', \Re''' \ldots,$$

an equation whose coefficients are expressible as rational functions *with integral coefficients* of $\Re', \Re'', \Re''' \ldots$, will be said to be algebraically solvable, if its roots can be derived from the quantities $\Re', \Re'', \Re''' \ldots$, by means of the above-named five elementary algebraic operations, applied a finite number of times. We expressly include in this definition the case in which some of the $\Re$'s do not explicitly appear in the coefficients; thus the coefficients of the equation

$$x^4 + x^3 + x^2 + x + 1 = 0$$

* The words "and the numerical unity 1" may be omitted since $1 = \frac{c}{c}$.

may be said to be rationally expressible in terms of the quantity $\Re' = \sqrt{5}$. It is therefore partly a matter of free choice from what quantities we regard the coefficients as being rationally derived. And the question whether a given equation is algebraically solvable admits of an answer only with respect to a definite choice of the $\Re$'s, or, to use Kronecker's terminology, it depends on the *domain of rationality* in which we are operating.

The domain of rationality $(\Re', \Re'', \Re''' \ldots)$ consists of all quantities which are expressible as rational functions with integral coefficients of $\Re', \Re'', \Re''' \ldots$. The simplest domain of rationality consists of all rational numbers, and is characterized by a single quantity $\Re$, viz.: $\Re' = 1$.*

The conception of domain of rationality is of the most fundamental importance for Galois' theory; there is not a proposition in the whole theory in which it is not implicitly contained. And it should always be borne in mind that terms like "algebraically solvable," "irreducible," "group of an equation," "Abelian equation," and the like, have a meaning only if referred to some definite domain of rationality.

Again, if we say, a quantity, ξ, is a rational function † of the roots $x_1, x_2 \ldots x_n$ of our equation, say

$$\xi = \varphi(x_1, x_2 \ldots x_n),$$

we always mean a rational function whose coefficients belong to our domain of rationality. Without some restriction concerning the nature of the coefficients of $\varphi(x_1, x_2 \ldots x_n)$, the above statement would be meaningless, at least in the case of a numerical equation; and the idea of a rational function with any constant coefficients, as used in the theory of functions, should carefully be kept out of all purely algebraic investigations.

2) *Second difficulty: formal and numerical invariance.*

As long as the x's are undetermined quantities, two rational functions of $x_1, x_2, \ldots x_n$ are considered as equal only if they are identical, that is, equal for all sets of values of $x_1, x_2 \ldots x_n$. But if the x's are the roots of a special equation, it may hap-

---

* Compare ABEL, Œuvres, II., pp. 219, 220; GALOIS, Œuvres, p. 34 (*Journal de Mathématiques*, vol. 11, 1846); KRONECKER, *Journal für Mathematik*, vol. 92, pp. 3–10.

† There seems, however, to be something unsatisfactory in the use of the word rational function in this connection, particularly in the case of a numerical equation. "Function" always implies the idea of a variable quantity dependent on some other variable quantities, whereas in the present case all quantities involved are constant. We should prefer to say: ξ is rationally expressible in terms of $x_1, x_2, \ldots x_n$, or shorter ξ is rational in $x_1, x_2 \ldots x_n$. See HÖLDER, *Math. Ann.*, vol. 34, p. 41.

pen that two rational functions of $x_1, x_2, \ldots x_n$, though different in form are equal in numerical value.

Example: The roots of the equation

$$x^4 + 1 = 0$$

are, if we put $e^{\frac{\pi i}{4}} = \varepsilon$,

$$x_1 = \varepsilon,\ x_2 = i\varepsilon,\ x_3 = -\varepsilon,\ x_4 = -i\varepsilon.$$

The two functions

$$\varphi = x_1^2 \quad \text{and} \quad \psi = x_2 x_4,$$

though different in form, are numerically equal, viz. $= i$.

In particular, it may happen, that two conjugate values of a rational function become equal, in which case we have to distinguish between formal and numerical invariance. In the above example the function $\varphi = x_1^2$ remains *formally* unchanged by the substitutions: 1; (234); (243); (34); (42); (23), whereas it remains *numerically* unchanged not only by these substitutions, but besides by the substitutions: (13); (42) (13); (413); (4213); (4132); (213), which replace x_1 by x_3 (notice $x_1^2 = x_3^2 = i$).

a) *Formal invariance:* Those substitutions which leave a rational function $\varphi(x_1, x_2 \ldots x_n)$ formally unchanged form, of course, a group, as before. It must, however, be remembered that one and the same quantity, rational in the roots, may admit of different expressions in terms of the roots, in which case it may at the same time belong to several groups, according to its different expressions in terms of the roots. It seems therefore advisable to avoid in this connection the term "group of a rational function," or "group of a quantity rational in the roots," and only to speak of the group of a given "expression of a rational function."* Thus we would say, in the above example, the "expression" x_1^2 belongs to the group [1; (234); (243); (34); (42); 23], the "expression" x_2x_4 to the group [1; (24); (13); (13) (24)], whereas the "quantity" $i = x_1^2 = x_2x_4$ may be said to belong to both groups at the same time.

b) *Numerical invariance:* Those substitutions which leave a rational function $\varphi(x_1, x_2 \ldots x_n)$ *numerically* unchanged *do not in general form a group.*† In the above example the 12 substitutions which leave x_1^2 numerically unchanged do not form a group.

---

* This is, however, only intended as a temporary terminology; the proper way of modifying the definition of the group of a rational function of the roots will be pointed out later: see p. 100, footnote.

† See HÖLDER, *Math. Annalen*, vol. 34, p. 41.

3) *Third difficulty: Lagrange's theorem.*

If some of the conjugate values of a rational function $\psi(x_1, x_2 \ldots x_n)$ are equal in numerical value, the discriminant of ψ, Δ_ψ, vanishes, and Lagrange's theorem can no longer be applied to the function ψ.* Along with Lagrange's theorem all its consequences cease to hold.

It is to *Galois'* genius that we owe a way out of these difficulties which seem to endanger most of our theorems on unsymmetric functions the moment we pass from the general equation to a special equation.†

III.

Netto's exposition of Galois' theory of the *group of an equation*, which is given in chaps. IX. and XIV., seems to us to be open to a number of objections all derived from the fact that the difficulties explained in the preceding section are not sufficiently considered. The term "rational function" is used without an explanation concerning the nature of the coefficients; no distinction is made between formal and numerical invariance; and Lagrange's theorem is used without a previous examination of the discriminant. All this gives to the deductions a certain vagueness and ambiguity. Moreover some of the most important theorems are omitted, others left without a proof. We think it therefore necessary to enter into a detailed analysis and to add such explanations as we believe indispensable to complete Netto's developments.

1) *Definition of the group of an equation.*

Netto gives, in the present edition, a new definition of the group of an equation, which takes a position intermediate between Jordan's and Kronecker's definitions. It is based on the following considerations: Let

$$(1) \qquad f(x) \equiv x^n - c_1 x^{n-1} + c_2 x^{n-2} - \ldots \pm c_n = 0$$

be an equation of the nth degree whose roots $x_1, x_2, \ldots x_n$ are all distinct. The $n!$-valued function

$$(2) \qquad \xi = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$$

where the α's are arbitrary constants,‡ satisfies a resolvent equation of degree $n!$:

---

* See NETTO-COLE, § 111.

† See the remarks at the end of the following section.

‡ This is too vague. The α's must be either rational functions with integral coefficients of $c_1, c_2, \ldots c_n$, so chosen that the $n!$ values of ξ are numerically distinct (GALOIS), or else undetermined quantities (KRONECKER). The developments would, however, have gained in clearness as well as in generality if the general idea of domain of rationality had been introduced from the outset, instead of only in chap. XIII.

$$(3) \quad F(\xi) \equiv \xi^{n!} - A_1\xi^{n!-1} + \ldots \pm A_{n!} \equiv \Pi\,[\xi - (\alpha_1 x_{h_1} + \alpha_2 x_{h_2} + \ldots + \alpha_n x_{h_n})],$$

where the product extends over all the $n!$ permutations $h_1, h_2, \ldots h_n$ of the indices $1, 2, \ldots n$, and the coefficients A are rational integral functions* of those of (1) and of $\alpha_1, \alpha_2, \ldots \alpha_n$.

If the coefficients $c_1, c_2, \ldots c_n$ of (1) are entirely independent, $F(\xi)$ cannot break up into rational factors. But for particular values of the coefficients c, $F(\xi)$ may break up into *irreducible* factors with rational coefficients

$$(4) \quad F(\xi) = F_1(\xi)F_2(\xi) \ldots F_n(\xi).$$

Consider any one of these irreducible factors, say $F_i(\xi)$. It may be written in two different forms: either decomposed into its linear factors

$$(5) \quad F_i(\xi) = \Pi\,[\xi - (\alpha_1 x_{i_1} + \alpha_2 x_{i_2} + \ldots + \alpha_n x_{i_n})],$$

where the product extends over certain permutations $i_1, i_2, \ldots i_n$ of the indices $1, 2, \ldots n$; or arranged according to powers of ξ

$$(6) \quad F_i(\xi) = \xi^r - B_1\xi^{r-1} + \ldots \pm B_r.$$

Since $F_i(\xi)$ is supposed to be a rational divisor of $F(\xi)$, the coefficients $B_1, B_2, \ldots B_r$ are expressible as rational functions of $c_1, c_2, \ldots c_n$ and $\alpha_1, \alpha_2, \ldots \alpha_n$.

The "expression" (5) of $F_i(\xi)$ is an *unsymmetric* function of $x_1, x_2, \ldots x_n$, and belongs to a certain group G_i; the "expression" (6) of $F_i(\xi)$ is a *symmetric* function of $x_1, x_2, \ldots x_n$, belongs to the symmetric group and is rationally known.†

From this double expression of $F_i(\xi)$, it follows that every function belonging to G_i is rationally known, being a rational function of $F_i(\xi)$.‡

Netto next shows that the groups G_i all coincide:

$$(7) \quad G_1 = G_2 = \ldots = G_\nu,$$

---

* With integral coefficients. Rational function is here always understood in this sense.

† This is an illustration of the remark 2, a) of the last Section, and shows again that the term "group of the function F_i" is not unambiguous.

‡ This conclusion supposes $\Delta_{F_i} \neq 0$; it is, however, not difficult to prove that this condition is always satisfied, owing to the undetermined quantity ξ, which is contained in F_i.

say $= G$. And it is this group G which Netto defines as *the group of the equation* (1). It is interesting to compare this definition with Jordan's definition on the one hand, and with Kronecker's definition on the other hand.

a) *Jordan's definition.*

Let $F_1(\xi)$ denote that irreducible factor of $F(\xi)$ which admits the root

$$\xi_1 = \alpha_1 x_1 + \alpha_2 x_2 + \ldots . \alpha_n x_n ;$$

all the roots of $F_1(\xi)$ are derived from ξ_1 by the application of certain substitutions

$$(8) \qquad 1, a, b, \ldots l$$

between the letters $x_1, x_2, \ldots x_n$, and $F_1(\xi)$ may be written

$$F_1(\xi) = (\xi - \xi_1)(\xi - \xi_a)(\xi - \xi_b) \ldots (\xi - \xi_l).$$

Jordan proves* the theorem :

The substitutions (8) *form a group, say* G'.

This group G' is the group of the given equation. Starting from this definition, it is easy to show † that Netto's group G is identical with G'. Netto himself uses later on (§229) the identity of both groups,‡ but he omits to prove that the substitutions (8) form a group.

b) *Kronecker's definition.*

Kronecker § considers the irreducible factor $F_1(\xi)$ not as a function of the roots but *as a function of the parameters* $\alpha_1, \alpha_2, \ldots \alpha_n$, which he regards as undetermined quantities. By this ingenious device, he avoids the ambiguity which attaches to the term "group of a function" in the case of non-independent quantities. No matter in which form we may express the function $F_1(\xi)$ it always belongs to one and the same group, say Γ, between $\alpha_1, \alpha_2, \ldots \alpha_n$.

If now we replace, in the group Γ, the letter α by the letter x, we obtain precisely the group G of the equation (1).‖ Netto touches Kronecker's definition in §226, page 267, but without showing its identity with his own definition.

---

* JORDAN, l. c. No. 354, and SERRET, l. c. No. 584, Corollaire.

† JORDAN, l. c. No. 351.

‡ There is a similar silent assumption in the proof of (7).

§ "Grundzüge einer arithmetischen Theorie der algebraischen Grössen," §11; *Journal für Mathematik*, vol. 92.

‖ For a direct proof of this statement, I refer to my note "Ueber Kronecker's Definition der Gruppe einer Gleichung," in one of the forthcoming numbers of the *Mathematische Annalen*.

2) *Properties of the group of an equation.*

Netto formulates Galois' fundamental theorem as follows: "*Every function belonging to G is rationally known; and, conversely, every rationally known function belongs to G.*"

We object to the use of the word "belonging to G" without an additional explanation whether it refers to formal or to numerical invariance; the more so, as from all that precedes it seems more likely that it is used in the former sense. And yet, in this case, the above formulation would not give the full meaning of Galois' theorem; the first part would state too little, the second too much.

Illustration: The group of the equation

$$x^4 + 1 = 0$$

with respect to the domain $\Re = 1$ is

$$G = [1\,;\ (12)\ (34)\,;\ (13)\ (24)\,;\ (14)\ (23)].$$

Using the same notation as on page 95 we have

$$x_1x_2^2 + x_3x_4^2 = 0.$$

Hence the expression $x_1x_2^2 + x_3x_4^2$ is rationally known; nevertheless it is not formally unchanged by G.

Galois himself expressly states in a footnote to his proposition I., that he means *numerical* invariance; and, in fact, the whole emphasis of the theorem lies on the numerical invariance.

To complete Netto's proof of the first part of the theorem, the following lemma must be added: "Every function which is numerically unchanged by the substitutions of a group, can always be thrown into such a form that it is also formally unchanged." For if $1, a, b, \ldots l$ are the substitutions of the group, and r their number, then it follows from $\varphi_1 = \varphi_a = \varphi_b = \ldots = \varphi_l$ that

$$\varphi_1 = \frac{1}{r}[\varphi_1 + \varphi_a + \varphi_b + \ldots + \varphi_l].$$

As to the second part of Galois' theorem, Netto gives no proof of it either in §153 or in §226. And yet the second part is just as important as the first and by no means self-evident.

In this connection we must mention a statement in §154: "It is clear that every unsymmetric equation $\varphi(x_1, x_2, \ldots x_n) = 0$ between the roots produces an affect." This is only true if $\Delta_\varphi \neq 0$.

Illustration: $x^3 - 2 = 0$. Its roots

$$x_1 = \sqrt[3]{2},\ x_2 = \omega\sqrt[3]{2},\ x_3 = \omega^2\sqrt[3]{2},\ \left(\omega = e^{\frac{2\pi i}{3}}\right)$$

satisfy the unsymmetric relations

$$x_1^2 - x_2x_3 = 0,\ x_2^2 - x_3x_1 = 0,\ x_3^2 - x_1x_2 = 0.$$

Nevertheless it is easily shown that the group of the equation with respect to the domain $\mathfrak{R} = 1$, is the symmetric group; that is, the equation has no affect.

We regret that Netto omits to point out one feature of Galois' theory which seems to us one of the most important, the *reconstruction* of the theorems on rational functions of the roots*, alluded to at the end of the preceding section. This reconstruction may be condensed in a simple practical rule: To pass from a theorem on rational functions of n independent quantities to the corresponding theorem in the case of a special equation, replace "symmetric group" by "group G of the equation" and "formally unchanged" by "numerically unchanged."

Thus the theorem (§29): "Those substitutions (viz., of the symmetric group) which leave a rational function of n independent quantities (formally) unchanged form a group," now takes the form:

Those substitutions *of the group G* which leave a rational function (φ) of the roots *numerically* unchanged form a group (H).†

Example: The group of the equation

$$x^4 + 1 = 0$$

with respect to the domain of rationality $\mathfrak{R} = 1$, is the group

$$G = [1 : (12)(34);\ (13)(24);\ (14)(23)].$$

Those substitutions of G which leave the function $\varphi = x_1^2 = x_3^2 = x_2x_4$ numerically unchanged, are: 1; (13)(24); they form indeed a group.

Similarly, the propositions of §41 and §53 have to be replaced by the following: If the order of G is ν times the

---

* See KLEIN, "Vorlesungen über das Ikosaeder," pp. 85, 86; HÖLDER, l. c. §15-20; and my paper, "On the theory of substitution groups" etc. §13, *American Journal of Mathematics*, vol. 13.

† JORDAN, l. c. No. 362. It seems natural to call this group H "the group of φ."

order of H, then the function φ, on being operated upon by all the substitutions of G, takes exactly ν *numerically distinct values*

$$\varphi_1, \varphi_2, \ldots \varphi_\nu .$$

They are the roots of an equation of degree ν, whose coefficients are rationally known, and which, moreover, is *irreducible* in the domain of rationality under consideration.*

Again, Lagrange's theorem takes the form :

If a rational function φ of the roots remains numerically unchanged by all those substitutions of the group G which leave another function ψ numerically unchanged, then φ is rationally expressible in terms of ψ ; and the theorem is true without any exception.†

These propositions contain the complete solution of the difficulties of the preceding section.

3) *Reduction of the group by adjunction.*

Suppose we had found, by solving an auxiliary equation $g(z) = 0$, an irrational function z of the known quantities $\mathfrak{R}', \mathfrak{R}'', \ldots$; we may then, henceforth, consider also z as a known quantity, or, in the language of Galois and Kronecker, *adjoin it to our domain of rationality.*

It may happen that the factors $F_1(\xi)$, $F_2(\xi)$, ... of $F(\xi)$, irreducible in the original domain $(\mathfrak{R}', \mathfrak{R}'', \ldots)$, are reducible in the new domain $(z ; \mathfrak{R}', \mathfrak{R}'', \ldots)$. In this case the group G *of* $f(x) = 0$ *is reduced to a subgroup of* G by the adjunction of z. And the solution of an equation by a chain of auxiliary equations consists, from Galois' point of view, in the successive reduction of its group until the group finally only contains the one substitution 1.

Two cases have to be distinguished according as z is rationally expressible in terms of the roots of the given equation ("natural irrationality") or not ("accessory irrationality," Klein).

The principal theorem concerning the *adjunction of natural irrationalities* is Galois' proposition IV.‡: "By the adjunction of the numerical value of a rational function φ of the roots, the group G of the equation is reduced precisely to that subgroup H of G which leaves φ numerically unchanged." This proposition, which is omitted in Netto's exposition, would have simplified the developments of §§ 230–234 concerning the group Γ of the auxiliary equation $g(\varphi) = 0$, satisfied by the rational function φ. If, in particular, H is a self-conjugate subgroup of G, the group Γ is the quotient-group $G : H$.

* See JORDAN, l. c. No. 366.

† See JORDAN, l. c. No. 362, Cor. II., and KLEIN, l. c.

‡ GALOIS, l. c. p. 41, SERRET, l. c. No. 583, and JORDAN, l. c. No. 362.

Further, if H is a maximal self-conjugate subgroup, the group Γ is simple. Hence the solution of a composite * equation can be reduced, by the successive adjunction of a series of rational functions of the roots, to the solution of a chain of simple regular * equations.†

The *adjunction of accessory irrationalities* is treated in §§236–238. Galois' proposition III., concerning the adjunction of all the roots of an auxiliary equation, is given, and Jordan's theorem concerning the mutual adjunction of all the roots of $g(z) = 0$ to the equation $f(x) = 0$ and of all the roots of $f(x) = 0$ to the equation $g(z) = 0$, with the corollary: "If the group of $f(x) = 0$ is reduced by the solution of a simple equation $g(z) = 0$, then the roots of the latter equation are rational functions of the roots of $f(x) = 0$."

This corollary contains, as Netto points out, a proof and an extension of Abel's celebrated theorem concerning the irrationalities which enter into the solution of an algebraically solvable equation.

IV.

The three following chapters are devoted to three important classes of special equations: cyclotomic equations, Abelian equations, and equations with rational relations between three roots.

The *cyclotomic equation*

$$\frac{x^p - 1}{x - 1} \equiv x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

for a prime number p is irreducible in the domain $\mathfrak{R} = 1$; if ω denotes one of its roots, all the roots may be written

$$\omega^g,\ \omega^{g^2},\ \cdots\ \omega^{g^{p-1}}$$

g denoting a primitive root (mod p). Hence it follows by applying the second part of Galois' fundamental theorem, that the group G of the equation is the cyclic group consisting of the p powers of the substitution

$$\left(\omega^g,\ \omega^{g^2},\ \cdots\ \omega^{g^{p-1}}\right).$$

---

* An equation is called simple, composite, regular, etc., if its group is simple, composite, regular, etc.

† Compare JORDAN, l. c. No. 362, 366–372, and HÖLDER, l. c. §§18–20.

The $(p-1)$th power of Lagrange's expression

$$(\alpha, \omega) = \omega + \alpha\omega^{g} + \alpha^{2}\omega^{g^{2}} + \cdots \alpha^{p-2}\omega^{g^{p-2}},$$

where α denotes a primitive root of the equation $z^{p-1} - 1 = 0$, is unchanged by the substitutions of G and therefore rationally expressible in terms of α. Hence the solution of the cyclotomic equation for the prime number p requires only the determination of a primitive root of the equation $z^{p-1} - 1 = 0$, and the extraction of the $(p-1)$th root of an expression which is then rationally known.

If $p_1, p_2, \ldots$ are the prime factors of $p-1$, the solution can be decomposed into a chain of binomial equations of degrees $p_1, p_2, \ldots$ Hence Gauss's celebrated theorem: If $2^m + 1$ is a prime number, the regular polygon of $2^m + 1$ sides can be constructed by means of ruler and compass. The constructions for $p = 5$ and $p = 17$ are given in full detail.

The chapter on *Abelian equations* begins with a reproduction of Abel's researches on irreducible equations of which one root x'_1 is a rational function of another root x_1: $x'_1 = \theta(x_1)$. The group of such an equation is determined and found to be non-primitive. If in particular all the roots can be arranged in one cycle

$$x_1, \theta(x_1), \theta^2(x_1), \ldots \theta^{m-1}(x_1); \quad \theta^m(x_1) = x_1,$$

the group is cyclic, and we have the immediate generalization of the cyclotomic equations ("simplest Abelian equations"), and the equation is solvable by radicals. Two examples of this type of equations are discussed; in the one case

$$\theta(x) = \frac{\alpha x + \beta}{\gamma x + \delta};$$

in the other, which is a new addition of the English edition, $\theta(x)$ is an integral function.

Then follows the general definition of Abelian equations in accordance with Jordan: an equation is called Abelian if all its roots are rational functions of one of them

$$x_1, \theta_1(x_1), \theta_2(x_1), \ldots \theta_{n-1}(x_1)$$

and besides the operations θ are commutative:

$$\theta_\alpha\theta_\beta(x_1) = \theta_\beta\theta_\alpha(x_1).$$

The substitutions of the group of an Abelian equation are all *commutative;* conversely, if the substitutions of the group

of an equation are all commutative, the equation is an Abelian equation.

Kronecker's as well as Jordan's treatment of Abelian equations are developed ; both methods lead to the theorem due to Abel : *Every Abelian equation is solvable by radicals.* As an illustration the equation for $\cos \frac{2\pi}{n}$ is discussed.

In chap. XII. irreducible equations are considered all the roots of which are rational functions of two among them. If, in particular, the degree is a prime number p, the equation is a *Galois equation ;* its group is the metacyclical group or one of its transitive subgroups. The solution of a Galois equation reduces to that of two Abelian equations. The binomial equation of prime degree $x^p - A = 0$ is the simplest example of a Galois equation.

An allied class of equations are Nöther's *triad equations,* the theory of which is developed in the second part of the chapter ; a well-known example of a triad equation is the equation of the 9th degree for the determination of the nine points of inflection of a plane curve of the third order. An interesting investigation on triad equations of degree 7 has been added in the new edition. The group of the most general irreducible triad equation of degree 7 is the "Kronecker group" of order 168 defined by

$$| z \; az + b |, | z \; a\theta(z + b) + c |$$

$$[a = 1, 2, 4 ; \; b, c = 0, 1, \ldots 6 ; \; \theta(z) = -z^2(z^3 + 1)].$$

The two remaining chapters are devoted to the general theory of *algebraically solvable equations,* treating, however, the problem by two entirely different methods, which may be characterized as *Abel's* and *Galois'*.

1) *Abel's Method* (chap. XIII.).

The first part of the chapter reproduces Abel's proof, simplified by Kronecker, of the fundamental theorem that the solution of an algebraically solvable equation can always be performed by a chain of binomial equations of prime degrees whose roots are rationally expressible in terms of the roots of the given equation and of certain roots of unity.*

Combining this proposition with the results of chap. III. concerning the existence of rational functions of n undeter-

* The shorter form in which the above theorem is given in Art. 85 of my paper "On the theory of substitution groups, etc.," *American Journal,* vol. 13, viz.: "The radicals which enter into the solution of a solvable equation are always rationally expressible in terms of the roots and of certain roots of unity," is not exact.

mined quantities, a power of which is symmetric or two-valued, it follows at once that *the general equations of a degree higher than the fourth are not algebraically solvable.*

The latter part of the chapter is devoted to the difficult problem of the *explicit expression of the roots of a solvable equation.* Abel had obtained in his memoir "Sur la résolution algébrique des équations," of which, unfortunately, we possess but fragments, two expressions for a root of an algebraically solvable equation of prime degree p: The first is

$$g_0 + \sqrt[p]{R} + \sqrt[p]{R_2} + \ldots \sqrt[p]{R_{p-1}}, \qquad (1)$$

where g_0 is a rational quantity * and $R_1, R_2, \ldots R_{p-1}$ are the roots of an equation of degree $p-1$ whose coefficients are rational quantities. The second is

$$g_0 + s^{\frac{1}{p}} + \varphi_2(s)\, s^{\frac{2}{p}} + \ldots + \varphi_{p-1}(s)\, s^{\frac{p-1}{p}}, \qquad (2)$$

where $\varphi_2, \ldots \varphi_{p-1}$ are rational functions whose coefficients are rational quantities. These two forms are necessary but not sufficient for a root of a solvable irreducible equation of prime degree.

Kronecker, completing Abel's researches and generalizing a result obtained by Abel, for $p = 5$, gave,†—yet without a proof,—the further conditions which must be satisfied by the quantities $R_1, R_2, \ldots R_{p-1}$, in order that the expression (1) may actually satisfy an irreducible solvable equation of degree p.

Netto not only proves Abel's results, but—and this is one of the most important additions of the new edition—he also gives a proof and further development of Kronecker's propositions.

2) *Galois' Method* (chap. XV.).

Galois' method consists in the successive reduction of the group of the given equation by the successive adjunction of the various radicals which enter into the expression of the roots. By means of his propositions III. and IV., mentioned in section III., Galois establishes the fundamental theorem:

In order that an equation may be algebraically solvable, it is necessary and sufficient that all the factors of composition of its group be prime numbers.

Hence arises the problem: To determine all groups of sub-

---

* That is, rationally expressible in terms of $\mathfrak{R}', \mathfrak{R}'', \ldots$

† *Monatsberichte der Berliner Akad.* 1853, translated in SERRET, Cours d'Algèbre supérieure, 4me édition, No. 599.

stitutions between n letters whose factors of composition are all of them prime numbers.

The problem can be reduced to the case of transitive groups. A further reduction results from the following propositions:

Every equation the group of which is non-primitive, is the result of the elimination of an auxiliary quantity y from two irreducible equations,

$$y^\nu - A_1 y^{\nu-1} + \ldots \pm A_\nu = 0,$$

$$x^m - S_1(y)x^{m-1} + \ldots \pm S_m(y) = 0,$$

(the A's being rational quantities and the $S(y)$'s rational functions of y); and

If the degree of a solvable irreducible equation is divisible by two different prime numbers, its group is non-primitive.

We may therefore confine ourselves to the consideration of primitive equations whose degree is a power of a prime, $n = p^k$; for these the following theorem holds:

The group of every solvable primitive equation of degree p^k consists of the group of the arithmetic substitutions of the degree p^k,

$$\left| z_1, z_2, \ldots z_k \quad z_1 + \alpha_1, z_2 + \alpha_2, \ldots z_k + \alpha_k \right| (\mathrm{mod}\, p),$$

combined with geometric substitutions of the same degree,

$$\left| z_1, z_2, \ldots z_k \quad a_1 z_1 + b_1 z_2 + \ldots + c_1 z_k, \right.$$
$$\left. a_2 z_1 + b_2 z_2 + \ldots + c_2 z_k, \quad \ldots \right| (\mathrm{mod}\, p).$$

If $k = 1$, the converse of this theorem is also true; hence Galois' theorem:

The group of a solvable irreducible equation of prime degree is the metacyclic group (or one of its transitive subgroups); and conversely, every metacyclic equation is algebraically solvable.

If, on the contrary, $k > 1$, not every group of the above form belongs to a solvable equation; and the determination of all solvable groups is, in this case, as yet an unsolved problem.

These are the principal subjects treated in the last chapter of Netto's book.

O. BOLZA.

UNIVERSITY OF CHICAGO, *January*, 1893.