7. As in § 210, $p^{2n} + 4p^n - 1$, being relatively prime to p, must divide $(p^{3n} - 1)$ $(p^{2n} - 1)$ and thus also $4p^n(p^{3n} - 1)$ and hence* $4(17p^n - 5)$ and hence divides

$$20(p^{2n} + 4p^n - 1) - (68p^n - 20) = p^n(20p^n + 12)$$

Hence $(p^n + 2)^2 - 5$ must divide 304, since

$$3(68p^n - 20) + 5(20p^n + 12) = 304p^n.$$

Thus $$p^n + 2 < 18 > \sqrt{309}.$$

But $p^n = 13, 11, 9, 5, 3$ are readily excluded; while $p^n = 7$ yields 76 a divisor of 304 and indeed of $(7^3 - 1)$ $(7^2 - 1)$, but is excluded since -1 is a non-residue of 7.

8. With the hypothesis of Jordan § 211, that $a^2 + b^2 + c^2 = 0$, etc., we have $a^2 = b^2 = \cdots$. Hence $3a^2 = 3b^2 = \cdots = 0$ and $ma^2 = 1$. Thus either $a^2 = b^2 = \cdots = 1$ or $2a^2 = 2b^2 = \cdots = 1$, when $1 - a^2 = a^2 =$ square.

UNIVERSITY OF CALIFORNIA,
November 20, 1897.

WEBER'S ALGEBRA.

Lehrbuch der Algebra. By HEINRICH WEBER, Professor of Mathematics in the University of Strassburg. Braunschweig, Friedrich Vieweg und Sohn. 1895–96. 8vo. Vol. I., pp. 653; Vol. II., pp. 796.

For some years the need of a thoroughly modern textbook on algebra has been seriously felt. The great strides that algebra has taken during the last twenty-five years, in almost all directions, have made Serret's classical work more and more antiquated, while modern books like Petersen's and Carnoy's make no claims to give a large and comprehensive survey of the subject. The appearance of any book modelled on the same broad plan as Serret's Algèbre Supérieure would thus be greeted with a hearty welcome, but when written by such a master as Heinrich Weber, we greet it with expressions of sincerest joy and satisfaction.

As Weber himself tells us, he has cherished for years the plan of this great undertaking; but before deciding to execute it he has traversed in his university lectures many times this vast domain as a whole, and has treated various parts separately with greater detail. No wonder, then, that

* Jordan has $68p - 12$, thus losing the divisor 76.

we find everywhere in perusing the pages of his work, evidence of mature judgment in the choice of the matter treated, in the amount of space devoted to each subject according to its relative importance, in the harmonious grouping of the parts, in the manner of presenting the different theories. Our admiration is no less excited by its pedagogic excellencies; Weber's German is simple and concise, the demonstrations are clear and rigorous, and many of them are of extreme elegance. After a point of view has been gained, the author disposes of one problem after the other as they are met in his path, and, as these are always clearly stated, the reader has the pleasure of knowing in advance the goal in view. The typography, which does so much to make a book readable, is excellent; not only the theorems, but also the more important results are made prominent by italics. We should have been glad to see more illustrative examples given, but the great size the work has already taken on, probably forbade this; perhaps the employment of a third kind of type, quite small, as for example in the works of Lie, would have been useful here.

Now in regard to the plan of the work: Weber's idea has been to write a work which shall lead the reader by easy steps from the most elementary notions to the most advanced and modern theories. Various auxiliary notions and theories are developed with great skill as found necessary, so that the reader nowhere needs to consult other works for information in order to continue his reading with pleasure and profit. As was to be expected, the chief interest of the work centers in the distinctly modern theories of Galois and Klein, of finite groups and algebraic numbers, while the older invariant theory as developed in the Higher Algebra of Salmon, for example, is scarcely touched. Referring the reader to the latter parts of this review for more detail we wish to note here that, in our opinion, the author's presentation of Galois's theory, with its many excellent examples, is beyond all comparison the most satisfactory yet given, whether in a work on algebra or one devoted exclusively to this theory; we recommend it most heartily for all who wish to acquaint themselves with this difficult but essential part of modern algebra. No less heartily can we praise the section devoted to explain Kronecker's theories applied to algebraic numbers. This certainly is the most novel part of the whole work, and Weber has earned by it the thanks of the whole mathematical community. We do not doubt that many will find Kronecker's algebraic methods more congenial than the purely arithmetical but more abstract methods of Dedekind.

We turn now to a review of its contents. We must remark, however, at the outset that it is impossible to give more than an imperfect account of them; the wealth of material is so great that even a passing notice would be beyond the limits of the space at our disposal; we shall thus have to content ourself with signaling what is most novel and important. The whole work contains over 1,400 pages. It is divided into two volumes, of which the first contains the more elementary theories and can serve by itself as an excellent introduction to algebra. Each volume is divided into books which mark the great theories to be treated; the first volume contains three, the second four such books. They treat the following topics: The Foundations, The Roots, The Theory of Galois, Abstract Groups, Linear Groups, Application of the Theory of Groups, Algebraic Numbers.

VOLUME I.

BOOK I. THE FOUNDATIONS.

As one of the features of the work is to develop all necessary auxiliaries it will not surprise us that an introductory chapter is devoted to the development of the number concept. Indeed, an analytical demonstration of the fundamental theorem of algebra that every equation has a root cannot be rigorously given without basing our reasoning on the notions of maxima and minima, of limits, and continuity, all of which rest on the notion of irrational numbers. Weber goes to work in a very abstract and general manner. Multiplicities are defined and these are subdivided as ordered, discrete, dense, and measurable. The irrational numbers are introduced by means of Dedekind's *Schnitte* or *partitions*, and his definition of continuity is also followed. The ordinary definition of addition and subtraction is given; but the treatment of multiplication and division, based on the broad Euclidian notion of ratio, is original and beautiful in the extreme. Negative numbers and zero are now introduced and so the continuous system of the real numbers is completed. The principle all along employed may be stated thus: A multiplicity being given, some of its elements are selected to form a new thing. These at first are endowed with no properties; they are mere symbols. We proceed now to give them one property after another, such as greater and less, etc., taking care that no new property conflicts with those already given. This process ended, we have a definite concept which possesses reality in the

same sense as the abstract number one or two does. Let us illustrate this by showing how the complex numbers $x + iy$ are created. From the multiplicity of the real numbers any two a, b are taken to form a new thing which we can denote by the symbol (a, b). Their totality forms a new multiplicity. We proceed to give them the character of real numbers. Two of them (a, b) and (α, β) are equal only when $a = \alpha$, $b = \beta$. The operations of addition and multiplication are defined thus

$$(a, b) + (\alpha, \beta) = (a + \alpha, b + \beta),$$

$$(a, b) \cdot (\alpha, \beta) = (a\alpha - b\beta, a\beta + b\alpha).$$

Subtraction and division are defined as the inverse operations and their result is unique. When $b = 0$ in (a, b) we say $(a, 0) = a$, and for simplicity we denote $(0, 1)$ by the symbol i. Then

$$(a, 0)\ (0, 1) = (0, a) = ai,$$

while $$(a, 0) + (0, b) = (a, b) = a + ib,$$

and $$(0, 1)\ (0, 1) = i^2 = -1.$$

In so small a space as this the complex number and the four arithmetical operations upon it are defined. Of the mystery that once surrounded this number not an atom is left by such a treatment; fractions and irrational numbers, negative and complex numbers, all stand on the same footing; all are equally real or unreal.

This remarkable chapter closes with a few properties of complex numbers and Gauss', or, as I suppose we now should say, Wessel's, representation of (a, b) by a point in the plane.*

The next two chapters are devoted to the theory of rational functions and determinants; in the first of these the notion of divisibility is extended to integral functions of x and important conclusions drawn, such for example as Gauss' theorem on the nature of the coefficients in $f = f_1 f_2$; while in the second all the more fundamental theorems of determinants and their minors are given, together with an application to systems of linear equations.

* It is a fact not yet generally known that a Norwegian mathematician, a surveyor by profession, Caspar Wessel, brother of the poet John Herman Wessel, has the honor of having first invented the representation usually accredited to Gauss or Argand. Cf. Sophus Lie, edition of Wessel's paper (1797) in the Danish Academy, entitled Om Directionens Analytiske Betegning, etc. Kristiania, A. Cammermeyers Forlag.

Chapter III. contains two demonstrations of the fundamental theorem of algebra. The first rests on d' Alembert's proof improved by Legendre and Cauchy. The leading idea is that if $f(x)$ does not vanish at the point x, another point $x + h$ can be found so that

$$|f(x + h)| < |f(x)|.$$

From this Cauchy inferred that for some value of x, say ξ, $f(\xi)$ actually vanishes and here he has been followed in English by such a careful writer as Chrystal.* This is all the more remarkable as Gauss already, in the fourth paragraph of his *Dissertation*,† observed that this conclusion must be separately proved. It is a pleasure to see a perfectly rigorous and simple demonstration such as Weber gives; the objection just made to Cauchy's proof is removed by showing that if g is a lower limit of $|f(x)|$ then some value of x exists where $|f(x)|$ actually takes on the value g. The reasoning rests on the notion of Dedekind's partitions. In the course of the demonstration the fact is made use of that every binomial equation has at least one root, and for this a purely algebraical demonstration is given depending also on the use of partitions. The solution of these equations by exponentials, although already given, is not employed in this connection, since from Weber's standpoint the great and fundamental theorems of algebra must be proved as far as possible by algebraic means. A source of dissatisfaction with the preceding demonstration lies in the fact that, although the existence of a root is established, no indication is given how it may be found; to remove this a second demonstration, a modification of Lipschitz's, is given.‡ This chapter also contains the solution of the equations of second, third and fourth degrees; in regard to the cubic, a very elegant form, due to Cayley,§ is given, which has the great advantage that in giving the radicals all their possible values only three values result, instead of nine as usual. In passing, we may remark that in the second volume (p. 319) an analogous form for the biquadratic is given; we hope they will find their way into our American text-books.

Chapter IV. is devoted to symmetric functions; application to discriminants, resultants, and theory of elimination is made. In connection with the last subject Tschirn-

* Algebra, vol. 1, p. 244.
† Werke, vol. 1, p. 10.
‡ Lehrbuch der Analysis, vol. 1, p. 248 seq.
§ Mathematical Papers, vol. 5, p. 54.

haus's transformation is introduced and its application to the cubic, biquadratic, and quintic is shown. The most remarkable feature of the chapter is the proof that the decomposition of integral rational functions of n variables into their irreducible factors for a natural domain of rationality is unique. In the introductory chapter the analogous theorem for integers was established. The demonstration rested on the fundamental theorem that if $\alpha\beta$ is divisible by γ, and if α is relative prime to γ, then β must be divisible by γ. This, in turn, rests on the fact established by Euclid's algorithm of the greatest common divisor that, if α and β be relative prime, then two integers ξ, η can be found so that $\xi\alpha + \eta\beta = 1$. Precisely the same path is followed here and the perfect parallelism of the reasoning affords the reader a deep satisfaction. Our only regret is that the author has not thought it worth while to indicate a method whereby the decomposition could be actually performed. As Kronecker has shown in the *Festschrift*,* this may be effected by using Lagrange's formula of interpolation which Weber has already developed in the second chapter. Thus only a few extra words would have been necessary, which a notion so fundamental as reducibility and irreducibility might surely justify, all the more when we find that five pages are devoted to considering Lipschitz's algorithm for finding the roots of an equation.

Chapter V. considers the theory of linear transformation. This is first applied to represent a quadratic form as the sum of squares and then to prove Sylvester's law of inertia. Application is now made to forms of nth degree which leads us naturally to consider their invariance. General methods for generating invariants and covariants are given, and the theory is applied with great beauty to cubic and biquadratic binary forms and equations.

Chapter VI. takes up Hermite's well-known modification of Tschirnhaus's transformation so as to employ the theory of invariants. The quadratic form Sylvester has called the Bezoutian is discussed ; the important theorem that the determinant of the Bezoutian is the nth part of the discriminant of $f(x)$ is proved and a convenient method for calculating the Bezoutian is given. The theory is applied to the cubic and to Klein's principal form of the quintic

$$x^5 + ax^2 + bx + c = 0. \tag{1}$$

* *Crelle*, vol. 92, p. 11. Other methods have been indicated by Mertens, Runge and Mandl.

In regard to the latter it is shown that if we take Hermite's transformation in the form

$$y = t_3 F_0 + t_2(F_1 a_2 + F_2 a_1 + F_3 a_0)$$

where the F's have the usual significance, the a's can be so chosen that the resulting equation in y is a principal equation for all values of t_2, t_3, the only irrationality necessary to introduce being $\sqrt{5D}$ where D is the discriminant of (1). This result is useful later. Another remarkable result, due to Gordan, is proved, namely, that making use only of the same irrationality, the equation (1) may be given the form

$$z^5 + 15z^4 - 10\gamma z^2 + 3\gamma^2 = 0$$

which involves but a single parameter. As the Bring-Jerrard normal form which contains also but a single parameter requires a cubic irrationality, a decided gain is hereby made.

Book II. The Roots.

The first four chapters of this book deal with the questions concerning the reality of the roots of real equations, their number in a given interval, their superior and inferior limits, and methods for their numerical approximation. The fundamental significance of the Bezoutian in questions regarding the reality of the roots is due to the fact that if it is the sum of p positive and n negative irreducible squares, then $p + n + 1$ is the total number of roots of the equation; there are n conjugate pairs and $p - n + 1$ real roots. The determination of p and n is now effected. We should mention in passing the application of Kronecker's discriminantal surface* to the discussion of the reality of the roots of the biquadratic. Another theory of Kronecker is here discussed with admirable clearness; we mean his theory of characteristics applied to determining the number of roots of $F = 0$ in a given contour. We cannot pass this by without a short sketch.

Let $\varphi(x, y) = 0$ be a closed curve; space within φ we call positive, without φ negative. Let the same be true for $\psi = 0$. Certain parts of the plane will thus lie within one and without the other; for such areas $\varphi.\psi$ is negative, they are called *Binnenraüme* or polar spaces. Let $f = 0$ be a third closed curve not passing through the points of intersection of

* Kronecker discusses this particular case of his general theory, in the Berlin *Monatsberichte*, 1878, p. 119.

φ and ψ. Passing around f in the positive sense, a point of intersection with φ is called a point of entrance if we pass into the polar space of φ, ψ and a point of exit if we pass out of such a space; they are denoted respectively by

$$I(f; \varphi, \psi), \quad O(f; \varphi, \psi).$$

If $i(f; \varphi, \psi)$ denote the number of points of the first kind for the whole circuit about f and $o(f; \varphi, \psi)$ that of the second, the characteristic of f, φ, ψ is

$$k = \tfrac{1}{2}[\, i(f; \varphi, \psi) - o(f; \varphi, \psi)\,],$$

and this number remains unchanged for all 6 permutations of f, φ, ψ. We apply these notions to the equation

$$\begin{aligned} F(z) &= z^n + a_1 z^{n-1} + \cdots + a_n = 0 \\ &= \varphi(x, y) + i\psi(x, y), \end{aligned}$$

the coefficients being real or complex.

Let $f(x, y) = 0$ be any arbitrary closed curve: as $\varphi = 0$, $\psi = 0$ are not closed, we close them anyway by curves lying however wholly outside $f = 0$. The theorem is established that the characteristic of this system is equal to the number of intersections of $\varphi = 0$, $\psi = 0$ inside $f = 0$; that is, k is the number of times $F(z)$ vanishes inside the contour $f = 0$. To determine k we take the coördinates of $f = 0$ as functions of a parameter t which passes from $-\infty$ to $+\infty$ as we pass around f. Sturm's theorem permits us to divide the contour of f into segments which contain each but a single intersection with φ or ψ, say φ; this will be a point of entrance or exit according as $\varphi\psi$ is positive or negative at the beginning of the interval. A simple application of this theory gives us a third demonstration of the fundamental theorem which is essentially that given by Gauss in his dissertation.

Chapter XI. deals with continued fractions and their well-known application to quadratic irrationalities and the Pellian equation.

In the next chapter, the last in the second book, we touch for the first time one of the great subjects of the present work, the theory of the roots of unity. Only the elements are here given. The irreducibility of the equation whose roots are here the $\varphi(n)$ primitive nth roots of unity is proven not only for the natural domain, but for that containing roots whose degrees are relatively prime to n. A slight oversight which crept in here is corrected in the appendix of the second volume. The connection of

the primitive nth roots of unity with the primitive congruence roots of n affords Weber a splendid opportunity to make an excursus on congruences, where important facts are established for later use. But Weber does not stop here. The determination of the nth roots of unity, or, what is the same thing, the problem of dividing the circumference of a circle into n equal parts is but a particular case of the division of an arbitrary arc into n equal parts, or, analytically, the division by n of the argument of the circular functions. The equations for $\sin \frac{x}{n}$ and $\cos \frac{x}{n}$ are thus considered, and the absolute term of the latter gives us the well-known identities:

$$2^{\frac{n-1}{2}} \prod \cos \frac{2\nu m\pi}{n} = \pm 1 \qquad n \text{ odd}$$

$$2^{\frac{n-1}{2}} \prod \sin \frac{2\nu m\pi}{n} = \pm \sqrt{n} \qquad \nu = 1, 2 \cdots \frac{n-1}{2}$$

The determination of the proper signs of the right-hand sides affords an opportunity to introduce the Legendre-Jacobian symbol $\left(\frac{m}{n}\right)$, and prove the law of quadratic reciprocity. The present chapter illustrates how admirably the author understands to weave in those auxiliary theories which will be needed later.

Book III. Galois' Theory.

One of the characteristic features of modern algebra is the prominent part the theory of Galois plays. This theory, dealing with the most subtle and hidden properties of algebraic equations, is unusually difficult to present simply and correctly. The algebra of Serret has the honorable distinction of being the first to give an account of it. Appearing for the first time in the third edition (1866), it has come down to us substantially unchanged in the succeeding editions. The fundamental ideas are well and carefully exposed by Serret and this work has probably introduced more mathematicians to Galois' ideas than all others together. But two objections are open to Serret's treatment; firstly, thanks to the labors of later mathematicians, the theory may now be presented more simply and comprehensively; secondly, and chiefly, we are disappointed by finding that Galois' ideas which pour such a flood of light on all ques-

tions concerning the solution of equations, are not applied to anything except the single problem treated by Galois himself, namely, equations of prime degrees. The treatment of the equations of second, third and fourth degrees, the demonstration of the algebraic insolubility of general equations of higher degrees, the solution of Abelian equations and the equations upon which the determination of the points of inflection of a cubic curve depends, all this is done by the antiquated pre-Galoisian methods. Besides the Algèbre Supérieure, we Americans are probably best acquainted with the presentation given in the English translation of Netto's work. But, although the part of this work devoted to the theory of substitution groups is unquestionably of great merit, the part devoted to exposing Galois' ideas is universally regarded as unfortunate.

All Americans will thus welcome most heartily the account given by Weber in this third and last book. In the second volume the more advanced parts of the theory are given; here only the most important and fundamental notions are treated. This is done with the utmost care and simplicity; the reader is led along by easy steps to consider the notion of domain of rationality, *Körper* or body, reducibility, adjunction, and so comes to normal bodies and the Galoisian resolvent. At this stage he is introduced to substitution groups. Now this method of approaching the theory of these groups in connection with the Galoisian theory is original and admirable. Usually the student has to wade through chapters on this driest of theories before their application, which gives them life and interest, comes into sight. Here, on the contrary, he meets them in the midst of his progress, their significance is clear, their application immediate and continuous. Another excellent feature of Weber's treatment is the care taken to keep in mind exactly what is in the domain of rationality, and in particular to avoid surreptitiously introducing roots of unity without studying the effect of their adjunction on the group of the equation. This is constantly done by many writers. For equations whose domains naturally contain variable parameters, no reduction in general takes place; but even this is not always true; witness the equations for the division of the argument of the elliptic functions. For equations however with constant coefficients, and above all when considering the solution of the equations which define the roots of unity themselves, this is an unpardonable sin. Netto, for example, on page 181 does precisely this. The group is determined for the absolute domain; Lagrange's resolvent is

introduced as a *rational* function which of course requires that *now* a unit $(p-1)$th root has been adjoined, and the group is tacitly assumed to be unaltered. This is indeed the fact by virtue of Kronecker's theorem we mentioned in speaking of the 12th chapter; but this theorem is nowhere even mentioned by Netto. We cannot stop to detail all the beauties of Weber's treatment of Galois' theory; we must, however, mention one more before continuing our analysis. We refer precisely to that feature whose absence we criticised so severely in Serret's work; in Weber's hand Galois' theory is not a pretty theory too delicate for much use, but a powerful instrument for research, a torch for illuminating the difficulties and complexities which surround the solution of algebraic equations, and this is true whether he is considering the solution of the biquadratic, or the equation for finding the 28 bitangents of a quartic curve, whether he is studying the nature of the roots of metacyclic equations of prime degrees, or the abstruse questions regarding the nature of relative normal bodies.

We return to our analysis. The first two chapters, or about 70 pages, suffice to give the broad outlines of the theory; while the remaining four chapters are devoted to its applications. The first of these is of course the solution of the cubic and biquadratic equations; the variety of subgroups which the symmetric groups of four elements affords being employed with good effect. Abelian equations are now taken up; a simple reasoning shows how their solution may be made to depend upon cyclic equations. Thus we are lead to consider with more than usual detail the properties of Lagrange's resolvent

$$(\varepsilon, x) = x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \cdots + \varepsilon^{m-1} x_{m-1}$$

where ε is any mth root of unity, and the x's for the moment independent variables. This done, we proceed with the solution of cyclic equations. In passing we observe the care the author takes to consider the case when his resolving functions vanish. This, as far as we know, is invariably neglected; and so the solutions given are illusory for even such a simple Abelian equation as $x^4 + 1 = 0$. As an interesting forerunner to the equations met in the theory of elliptic functions, the equations for the division of the argument of the circular functions are considered. The next application of the Galoisian theory is the solution of the equations upon which the division of the circle depends, or the cyclotomic equations; we thus return once more to the roots of unity and the theory is considerably advanced.

Two methods of solution are given, both due to Gauss; the first makes use of the fact that the rational function of the roots (the periods of Gauss)

$$\eta = r + r_e + r_{2e} + \cdots + r_{(f-1)e},\ n - 1 = ef,\ n = \text{a prime},\ \alpha^e = 1$$

belongs to a subgroup of index e, and so gives rise to a resolvent of eth degree; the second uses the resolving function $(\alpha, \eta)^e$ which leads to a binomial equation. The intimate relation between the roots of unity and the theory of numbers is again employed to deduce many important results. The Gaussian periods of $\frac{n-1}{2}$, $\frac{n-1}{3}$, and $\frac{n-1}{4}$ terms are considered. The first gives us the sums of Gauss, which are evaluated very elegantly; the second and third afford theorems on the representation of primes of the form $3m + 1$ and $4m + 1$. At this point we are given a first taste of the great theory of algebraic numbers which is to occupy our attention so much in the next volume. The Körper or bodies considered are those generated by the cube and fourth roots of unity, which we shall denote in the future by $R(\rho)$ and $R(i)$. As an algorithm for finding the greatest common divisor analogous to that of Euclid's exists for these numbers, it follows at once that their decomposition into prime factors is unique, aside of course from unit factors. For this purpose the representation won a moment ago for primes of the form $3m + 1$ and $4m + 1$ is employed.

Chapter XVII. carries the general Galoisian theory quite a way farther. The well-known criterion, due to Jordan for the algebraic solvability is deduced; and on showing that the alternate group is simple for $n > 4$ we have a proof of Abel's great theorem that general equations of degree greater than four cannot be solved by the extraction of roots. To be quite satisfactory it is necessary to complete this theorem by one due to Hilbert, which states that in order to have an affectless equation it is not necessary to restrict the coefficients to independent variables, since there even exists an infinite number of equations with integral coefficients of this character. Weber gives his elegant demonstration of this for equations of prime degrees. Another beautiful application of Galois' theory is made to settle the old question whether the *Casus Irreducibilis* is indeed such; that is effected by means of the general theorem that normal equations of odd degree cannot become reducible on adjoining real radicals. Galois' theorems regarding algebraic soluble equations are now deduced and the

chapter closes with an application to a class of soluble quintics due to Runge, *Acta Mathematica*, vol. 7. Runge's equation (2) on p. 177, is given by Weber with a wrong sign* which goes through all succeeding equations affecting in particular the final values of the parameters α and β.

The last chapter of the volume is devoted to the form of the roots of metacyclic equations of prime degrees. Abel having shown that the general equations of degree greater than four cannot be solved algebraically, the problem naturally presented itself to him to find all equations which could be. This he takes up in his customary bold way in the "Mémoire sur la résolution algébrique des équations," left unfinished by his premature death. Kronecker, following in Abel's footsteps, arrived at results which were published in the *Monatsberichte* of the Berlin Academy for 1853. He completely solves the problem for equations of prime degrees, and in studying the forms of the roots in connection with Kummer's ideal theory, arrives at the theorem that the roots of all Abelian equations in the domain of rational numbers are rational functions of unit roots. Kronecker goes even farther, and asserts a similar relation exists between the roots of Abelian equations whose coefficients lie in $R(i)$ and the equations connected with the division of the Lemniscate. As the Lemniscate affords the simplest case of complex multiplication, this remark opened a wide field of research. We should not have allowed ourselves to go into these details if precisely this mémoire were not of determining influence for the present work. Indeed, here, at the outset of his career, as unfortunately so often later, Kronecker contented himself with sketching the analysis which led him to the root forms

$$A + \Sigma K_\nu \tau_\nu^{r_{\nu-2}} \tau_{\nu+1}^{r_{\nu-3}} \cdots \tau_{\nu+n-2}^{r_0}, \quad \nu = 0, 1 \cdots n-2,$$

while in regard to the theorem of Abelian bodies no hint is given at all except that just mentioned. For more than thirty years this last theorem remained undemonstrated and unappreciated until Weber in the eighth volume of the *Acta Mathematica* gave a proof and called the attention of mathematicians to it as one of the most promising in modern algebra since it points the way which must be pursued if we are to obtain a deeper insight into the nature of algebraic numbers. A considerable part of the second volume is spent in developing the foundation upon which it rests and theories intimately related to it. As the preface tells

* The slip was kindly pointed out to me by Dr. McClintock.

us, Weber hopes to continue the present work, giving in a third volume the analogous theories relating to the complex multiplication of the elliptic functions. But to return to the first part of the mémoire, as remarked, Kronecker merely sketches the reasoning which led him to the above form of the roots. Enough. however, is given to fill it out and this has been done in various places, but a fact has been overlooked which seriously limits the validity of these expressions. Certain quantities which enter the reasoning may vanish, certain others may be equal. How to avoid this was first shown by Weber in a paper which appeared in the *Berichte* of the Marburg Society in 1892. The reasoning rests on the employment of rational integral functions of the roots of the equation with indeterminate coefficients which are considered in the double light of a Tschirnhausian substitution and a linear substitution with non-vanishing determinant. The chapter terminates in finding the explicit form of the roots of algebraically solvable quintics for an arbitrary domain. A slightly more general form is given than the familiar form found by Abel for integral coefficients.

VOLUME II.

BOOK I. GROUPS.

We turn now to the review of the second volume. What strikes us at first sight is the novelty of the subjects treated, which, with a few unimportant exceptions, appear here for the first time in a treatise on algebra; the 790 pages which the volume possesses may fairly represent the progress algebra has made in the last twenty-five years. The volume appropriately begins with an account of abstract groups, which, together with the theory of functions, dominate so large a part of the mathematics of to-day. The origin of the theory of groups goes back to the theory of numbers on the one hand and algebra on the other. But we must allow that it is in the algebraical papers of Lagrange, Ruffini, Abel, and in particular Galois that the theory received its first vigorous impulse and not in the few scattered remarks of Gauss; so that after all we may permit algebra to enjoy the enviable distinction of giving birth to this great modern theory.

The definition Weber gives for abstract groups is the familiar one employed in his various papers in the *Annalen* and the *Acta Mathematica* and, indeed, much that is in the first chapters is taken from these mémoires. Many of the theorems established in the first volume for substitution

groups are now demonstrated afresh for abstract groups. The nature of a series of composition is studied; Jordan's theorem on the invariance of the factors of composition is proved following Netto's modification of Hölder's demonstration. We regret that Hölder's theorem on the invariance of the factor groups is not given. This not only contains Jordan's theorem but, as Hölder has pointed out, has an algebraical significance which is fundamental for the solution of equations. In fact, these factor groups must appear among the groups of a chain of simple resolvents in in whose roots the roots of the given equation can be rationally expressed, and this is true whether we employ natural or accessory irrationalities. At the same time, a lower limit is given to the number of equations in any chain, and we have as an important consequence that, when this limit is reached, the irrationalities employed are natural. The invariance of the factor groups asserts therefore the invariance of the *character* of the resolvents, rational or not, which *must* be employed sooner or later in the solution of the given equation. In passing, we wish to observe that, contrary to the prevailing impression, these factor groups were first employed by Jordan in his paper "Sur la limite de transitivité des groupes non alternés," *Bulletin de la Société Mathématique de France*, vol. 1 (1873), and not in Hölder's paper in the *Annalen*, vol. 34, sixteen years later. The notation G/H is also due to Jordan.

These generalities disposed of, Weber now considers finite Abelian groups; their structure is the simplest of all groups, their importance perhaps the greatest. The fundamental theorem that every Abelian group can be represented by a basis is established, and a method is given to determine all its subgroups. This last leads us to consider the invariants and characters of an Abelian group. Defining the former differently than usual as the prime powers which enter the orders of the elements of a basis, it is shown that they serve completely to determine the group, since all groups having the same invariants are simply isomorphic and conversely. The most important example of Abelian groups is the group formed by throwing all numbers into classes so that all those congruent to a given number *modulo* m are in one class. The classes whose elements are relatively prime to m form the group in question; its order is of course $\varphi(m)$. An illustration of one of the results which flow immediately from this is Euler's theorem

$$a^{\phi(m)} \equiv 1 \ mod \ m$$

since the order of any element of a group is a divisor of the order of the group. The basis of these numerical class groups is now determined and the results at once used to solve the problem of representing all cyclotomic bodies without repetition. This was first done by Weber in the eighth volume of the *Acta Mathematica;* the presentation here given being considerably amplified. The success of the method depends upon a proper generalization of the periods of Gauss. To illustrate the rather intricate details an application to cubic and biquadratic bodies is given. These bodies have a heightened interest due to the fact that they also form all cubic and biquadratic Abelian bodies in the absolute domain of rationality by virtue of Kronecker's great theorem; but as this theorem is proved only in the last chapters of the volume after an elaborate chain of reasoning, it is a real pleasure to see how easily the demonstration can be effected for these simple cases. This is due to the fact that in the domains $R(\rho)$ and $R(i)$ the decomposition of numbers follows the same laws as in the absolute domain. The proof rests on the decomposition of Lagrange's resolvent into its prime factors, which for the general case requires the introduction of ideals. We leave now for the present the theory of cyclotomic bodies and return to the general theory of finite groups. One of the problems which presents itself here is the determination of all possible groups in the same way as a moment ago we determined all possible cyclotomic bodies; but a problem of this great extent is to-day utterly beyond our reach, and mathematicians have been obliged to search for the groups satisfying some simple conditions, for example, all groups whose orders are less than a certain number or whose orders contain only certain prime factors, etc. Fundamental here are a number of theorems due to Sylow; for example, Sylow's generalization of Cauchy's theorem that if p^k be the highest power of the prime p, which is contained in the order n of a group P, then P contains a subgroup Q of order p^k; of these groups Q, $pa+1$ exist, they are conjugate and $n = p^k r(pa+1)$. Two remarkable facts result from these investigations on possible groups; first, that the number of groups whose orders satisfy one of the above conditions is relatively very small, and, secondly, that the character of the order of a group in regard to its prime factors serves to determine the nature of the group in many cases beyond expectation. Thus Sylow has shown that all groups of order p^k are solvable, or, as Weber says, metacyclic; the same is true of groups whose orders are of the

form $p^{\alpha}q$ or the product of any number of different primes, as Frobenius has proved. These investigations bring to light also the surprising result that the number of simple groups of low order is extremely small. Galois enunciated the first theorem we had on this subject; he stated that the order of the smallest simple group which is not a prime is 60. Hölder, carrying the investigation to order 200, found only one other simple group, which is Kronecker's group of order 168. Cole, Moore and Burnside have carried the investigation to order 1,092. A good introduction to the methods employed in these researches is given by our author, who takes up the simpler cases. The book closes with the consideration of the limits of the index of a subgroup of the symmetric group, a problem which has its origin in the attempts of Lagrange and Vandermonde to find a resolvent of the third or fourth degree of the general equation of the fifth degree.

BOOK II. GROUPS OF LINEAR SUBSTITUTIONS.

The special groups studied up to the present have all been finite; in the theory of linear substitutions we are led to consider infinite groups. We must remark, however, that it is only their finite divisors which will be studied in detail. After the first properties of these groups have been exposed the notion of the invariants of a finite linear group is introduced. Particular examples of invariants we have already met; in fact, as every permutation group G is a particular case of a linear group, the rational functions of the n variables which in the Galoisian theory are said to belong to G, are here the absolute invariants of G while those functions which take on a unit root as factor after an operation of G are the relative invariants. Thus, for the alternate group the square root of the discriminant is an absolute invariant; for the symmetric group it is only a relative invariant. If $\varphi(x_1, x_2, \cdots, x_n)$ is a relative invariant of G, those substitutions of G which leave φ absolutely unchanged form an invariant subgroup H of G. The covariants which can be formed from any invariant belonging to a group G, are also invariants of G. The fundamental theorem is now proved that only a finite number of indedendent invariants belong to any finite group of linear substitutions; the demonstration rests on a very general lemma of Hilbert's and is due to Hurwitz. The first chapter of this book closes with an account of Klein's *Formenproblem*, but as no application is made of it till several chapters later we postpone speaking of it till then.

The next two chapters are devoted to the polyhedral groups and their invariants. The way Weber arrives at them is very interesting. First the orthogonal substitutions are considered as a subgroup of the linear group and it is shown how in particular every ternary orthogonal group may be considered as a group of rotations of a solid about a fixed point. When this group is finite it corresponds to the group of rotations which bring a certain body into coincidence with itself, for example a cube or an octahedron. On the other hand, it is shown that these finite ternary orthogonal groups are isomorphic with the group of linear fractional substitutions

$$G; \qquad x, \theta_1(x), \theta_2(x), \cdots, \theta_{n-1}(x),$$

where $\theta(x)$ stands for

$$\frac{\alpha x + \beta}{\gamma x + \delta} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

The problem is taken up of finding all finite groups of this type. This, as is well known, was first effected by Klein; his methods were considerably simplified by Gordan, and Weber's treatment is a simplification of Gordan's. The method rests on the notion of a pole of a substitution, that is, the two roots a, b of

$$x = \theta(x).$$

The pole a is ν-fold if $\nu - 1$ substitutions $\theta_1, \theta_2, \cdots, \theta_{\nu-1}$ have this as a pole. These, together with the identical element, form a group of order ν, so that ν must be a divisor of n; it is further shown that these ν elements have the form $1, \theta, \theta^2, \cdots, \theta^{\nu-1}$, that is, they form a cyclic group Q of order ν. If $\psi_1 = 1, \psi_2, \cdots, \psi_\mu$ are such that

$$G = \psi_1 Q + \psi_2 Q + \cdots + \psi_\mu Q$$

then $\qquad a_1 = \psi_1(a) = a, \quad a_2 = \psi_2(a) \cdots a_\mu = \psi_\mu(a)$

are called the conjugate poles to a; they are all distinct and ν-fold. Different conjugate systems have no poles in common. As every element of G except the identical element has two poles the total number is $2(n-1)$, hence

$$2(n-1) = \mu(\nu - 1) + \mu'(\nu' - 1) + \ldots,$$

or calling h the number of systems of conjugate poles

$$2n - 2 = nh - \mu - \mu' - \cdots$$

which shows that h must be either 2 or 3. A simple reasoning shows further that only five cases are possible, and it remains only to show that these cases all exist and to determine the form of the elements of each group. To effect this Weber writes the substitutions in their homogeneous form and shows that if $a_1, a_2, \cdots, a_\mu$ be a system of conjugate poles and

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_\mu),$$

then

$$f(x_1, x_2) = x_2^{\mu} f\left(\frac{x_1}{x_2}\right)$$

is an invariant of G of degree μ. These various forms corresponding to the different systems of poles are called the fundamental forms of the group. The following theorem is of importance here: If $F(x_1, x_2)$ is an invariant of G of lower degree than the order of G, then $F = 0$ identically if it is not the product of fundamental forms. Also the theorem that if G contains only one system of ν-fold poles, it may be so transformed that the substitutions $\theta(x) = \varepsilon x$ and $\psi(x) = \frac{c}{x}$ occur, ε being a primitive νth root and c an arbitrary constant. With these general principles it is an easy matter actually to build the groups corresponding to the five cases above and to construct their fundamental forms. Because these groups are isomorphic with the groups of rotations of the corresponding bodies they are called the cyclic, dihedral, tetrahedral, octahedral and icosahedral. The last of these has the most interest for us on account of its relation to the solution of the quintic. The group contains 60 elements which may be generated by

$$\theta(x) = \varepsilon x, \quad \psi(x) = -\frac{1}{x}, \quad \chi(x) = \frac{\omega x + 1}{x - \omega}$$

where

$$\varepsilon = e^{\frac{2\pi i}{5}}$$

and

$$\omega = \varepsilon + \varepsilon^{-1}.$$

The three fundamental forms of the group are

$$f = x_1 x_2 (x_1^{10} + 11 x_1^5 x_2^5 - x_2^{10}),$$

its Hessian H, and the functional determinant T of f and H. Between them exists the identical relation

$$T^2 + H^3 = 1728 f^5.$$

The quotients $\frac{T^2}{f^5}$, $\frac{H^3}{f^5}$ are homogeneous forms of zero de-

gree; we may consider them as functions of $\frac{x_1}{x_2} = x$ alone. The second of them set equal to z gives us an equation for x of 60th degree

$$H^3 - zf^5 = 0$$

or writing out in full

$$(x^{30} + 522\,x^{25} - 10005\,x^{20} - 10005\,x^{10} - 522\,x^5 + 1)^2$$
$$- z\,(x^{10} + 11\,x^5 - 1)^5 = 0.$$

This is called the icosahedral equation; another form of it is obviously $T^2 - (1728 - z)f^5 = 0$ got from the identity above.

Chapter IX. treats of linear congruence groups introduced by Galois in connection with the modular equations. The theory becomes clearer and broader if we consider the numbers entering these substitutions $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to lie in the congruence body defined by the congruence $P(x) \equiv 0$ *mod.* p where p is a prime and $P(x)$ is an irreducible polynomial *modulo* p of degree n. The p^n numbers of this body will be of the form $a_0 + a_1\varepsilon + \cdots + a_{n-1}\varepsilon^{n-1}$; where the a's are ordinary integers taken *mod.* p and ε is an ideal number which Galois has introduced to satisfy the above congruence. The resulting groups are called congruence groups. An immediate application of these groups lies in the fact that they afford us a whole class of simple groups, since they are all simple except for the two cases $n = 1$, $p = 2, 3$. For $n = 3$, $p = 2$ we have the simple group discovered by Cole of order 504, which for a long time had been overlooked. The general theory of these groups was given for the first time by Moore. The subgroups of the ordinary modular groups corresponding to $n = 1$ are now investigated; great assistance is gained by considering them in connection with congruence groups corresponding to $n = 2$. The Galoisian imaginary here employed is defined by $\varepsilon^2 \equiv N$ *mod.* p and N is a certain fixed quadratic nonresidue of p. Almost the same reasoning as employed in finding the possible polyhedral groups applies here and we find besides the well-known cyclic and metacyclic groups studied by Serret, that there are only three other kinds of groups; tetrahedral for every p, octahedral for $p \equiv \pm 1$ *mod.* 8, and icosahedral for $p \equiv \pm 1$ *mod.* 5. These results were first obtained by Gierster (1881) and are generalizations of a theorem due to Galois.

BOOK III. APPLICATION OF THE THEORY OF GROUPS.

The first chapter of this book, the 10th, deals principally with metacyclic irreducible primitive equations whose degrees are powers of a prime p^κ. The group P of these equations is shown to be of the form TQ where the substitutions of Q are

$$\begin{pmatrix} z_1 & \cdots\cdots & z_\kappa \\ z_1+a_1 & \cdots\cdots & z_\kappa+a_\kappa \end{pmatrix} \quad mod\ p$$

and T is a metacyclic subgroup of the homogeneous linear congruence group S. These results are applied to equations of the 8th and 9th degrees. For the latter the elegant result is obtained that the whole group S is metacyclic so that every equation of the 9th degree whose group is a linear congruence group is algebraically solvable. For equations of the 8th degree the result is obtained that the roots have the form

$$A \sum_{z=0}^{6} \sqrt{\varphi_z}\ \sqrt{\varphi_{z+1}}\ \sqrt{\varphi_{z+2}}\ \sqrt{\varphi_{z+3}} + B$$

where A, B are rational quantities and the φ's are roots of a metacyclic equation of degree 7.

The next two chapters are applications of Galois' theory to geometry, the 9 points of inflection on a cubic and the 28 bitangents of a quartic being the subjects considered. True to his plan that all necessary auxiliary notions and theories be developed in the course of the work whenever needed, the author supposes only the merest elements of analytical geometry to be known. Starting, therefore, *de novo*, an admirably compact and clear treatment of the geometrical aspect of these problems is given. The equation upon which the determination of the points of inflection depends is a triple equation; that is if x_1, x_2 be any two of its roots a third is completely determined by a rational relation $x_3 = \theta(x_1, x_2)$. If ξ, η be taken *mod* 3 the nine roots of a triple equations can be represented by the symbol (ξ, η) and three of them form a triple when $\xi_1+\xi_2+\xi_3 \equiv 0$ $\eta_1+\eta_2+\eta_3 \equiv 0$ *mod* 3. The group of these triple equations of 9th degree lies in the complete linear congruence group Γ *mod* 3; conversely an equation of 9th degree is triple if it lies in Γ and is doubly transitive. The question of the reality of the roots of triple equations of 9th degree for a real domain is also disposed of.

In considering the geometry of the 28 bitangents of a quartic without singularities the 288 asyzygetic systems of 7 bitangents first studied by Aronhold are of fundamental

importance, because when one of these Aronhold systems is given the 21 remaining bitangents can be rationally determined. Another fact of importance in determining the group G of our equation is this; any three of its roots corresponding to a syzygetic triple satisfy a rational equation which still holds true when this triple is replaced by any other syzygetic triple, but does not subsist if they are replaced by an asyzygetic triple. We can now conclude that no substitution of G replaces a syzygetic by an asyzygetic triple or conversely; and therefore the elements of an Aronhold system are never torn asunder by a substitution of G. It is shown that G contains the $288.7!$ substitutions which permute the 7 elements of an Aronhold system among themselves or replace it by another system, the effect on the other tangents being completely determined as already observed. The structure of G is examined; it is simple, twofold transitive and contains a divisor of index 36 which is transitive and simply isomorphic with the symmetric group of 8 things. Thus the adjunction of a root of an equation of the 36th degree reduces the group to that of the general equation of the 8th degree. Finally an interesting discussion of the reality of the tangents is given; it is shown that either 4, 8, 16, or all are real and their syzygetic relations are noticed.

It is now our agreeable task to give an account how Weber has used the ideas of Klein to treat the solution of the general equation of 5th degree and the equation of 7th degree with a group isomorphic to that of the modular equations of degree 8. The fact that Weber has been very independent in his treatment of these problems will make the account only more interesting. A few words on the history of the term *solution of an equation* may not be amiss. The fundamental problem of algebra is the solution of equations. Prior to Abel's time this meant: Express the roots by radicals. After Abel had shown this to be in general impossible it was necessary to change the problem to this: What equations can be solved by radicals; what are the forms of their roots? As the majority of equations do not admit an algebraic solution, the question also presented itself: In what shall the solution of these equations consist? This remained a long time unanswered. Then all at once, in 1858, the memorable solutions of the general quintic by Hermite, Brioschi, and Kronecker appeared. Their results opened a new path which was transformed into a broad highway as the ideas of Galois became better known. From the standpoint of the Galoisian theory the solution of

an equation $f(x) = 0$ consists in finding a chain of resolvents of the nature Hölder has described whose groups shall contain the factor groups of $f = 0$; resolvents are chosen which possess some peculiar and desirable properties. This being largely personal, different mathematicians will select different resolvents. For example, Kronecker would admit only *rational* resolvents in his system, a position not approved of by many others. But the above standpoint gives us little hold on affectless equations of higher degrees, since on adjoining the square root of the discriminant their groups are simple. To advance a step in the solution of these equations Klein has formulated the problem in an entirely new and original manner. The foundation is Klein's *Formenproblem*, which we may state as follows: Being given a group S of linear substitutions of the variables $x_1, x_2, \cdots, x_n$, express these last as algebraic functions of the invariants of the group. If we take a rational function of the x's as θ, chosen so that its value is altered for every substitution of the group, it is shown just as in the Galoisian theory that the x's can be expressed rationally in terms of the invariants of S and the numbers of some body. Let the values θ takes on for S be

$$\theta, \theta_1, \theta_2, \cdots;$$

the equation

$$\Phi(t) = (t - \theta)(t - \theta_1)(t - \theta_2) \cdots = 0$$

is the Galoisian resolvent, its group is the Galoisian group of the *Formenproblem* belonging to S. The *Formenproblem* contains thus the Galoisian theory of the solution of the general equation of degree n as a special case; here the group S is the symmetric group of permutations while the invariants of the group are the symmetric functions of the roots. But the number of variables entering the *Formenproblem* may often be reduced; for example, the solutions of the equations of the first four degrees depend upon *Formenprobleme* involving only a single variable; the general quintic depends on one involving only two variables while the general equations of 6th and 7th degrees depend on *Formenprobleme* with 4 variables. This leads Klein to propose the following as the general solution of algebraic equations: Among the problems having isomorphic groups that one is considered as the simplest which has the least number of variables. This is called the normal problem and the solution of the others is to be effected by reducing them to this. How the normal problem is to be solved is a matter by it-

self. Let us see how Weber applies these ideas to the quintic. The first step taken is to prove Kronecker's theorem that no rational resolvent of the general quintic exists involving but a single parameter. Suppose the quintic transformed to Klein's principal form:

$$y^5 + 5ay^3 + 5by + c = 0 ; \tag{1}$$

this equation is no longer general, but it possesses a rational resolvent with a single parameter $\Phi(\vartheta, z) = 0$. This we may take to be the icosahedral equation already mentioned,

$$(\vartheta^{30} + 522\vartheta^{25} - 10005\vartheta^{20} - 10005\vartheta^{10} - 522\vartheta^5 + 1)^2 = z\,\vartheta^5(\vartheta^{10} + 11\vartheta^5 - 1)^5.$$

The question is now asked what equations can be solved by means of the icosahedral irrationality ϑ. To this end we need to find the resolvents corresponding to the different divisors of the icosahedral group. The most important are of course the resolvents of the 5th and 6th degrees corresponding to the tetrahedral and dihedral groups. In regard to the resolvent of 5th degree it is shown how it may be made identical with any given principal equation without employing any irrationality besides the square root of the discriminant. The importance of the sextic resolvent is due to its intimate relation with equations of transformations of the elliptic functions. For example, using the notation employed by Weber in his book on elliptic functions, the sextic resolvent of the icosahedron

$$y^6 - 10zy^3 + z^2y + 5z^2$$

is identical with the equation of transformation

$$v^6 + 10v^3 - \gamma_2(\omega)v + 5 = 0$$

whose roots are

$$v_\infty = 5\,\frac{\eta^2(5\omega)}{\eta^2(\omega)} \qquad v_\xi = \frac{\eta^2\left(\dfrac{-24\xi + \omega}{5}\right)}{\eta^2(\omega)} \qquad \xi = 0, 1, \cdots 4$$

if we only set

$$z = \gamma_2^{\,3} \text{ and } y = -\gamma_2 v.$$

If we compare this presentation of the solution of the quintic with that given by Klein in the *Ikosœder* we observe that, whereas Kronecker's theorem, that no rational resolvent of the quintic exists having a single parameter, appears

in the *Ikosœder* as a final result, it is here made the foundation on which the whole theory rests. In this way the explicit expression of ϑ as a rational function of the roots is made unnecessary and yet a relation is established between the quintic and the icosahedral equation in a natural and easy manner.

The last two chapters of this book, the 14th and 15th, are devoted to the *Formenproblem* belonging to the group G_{168} of 168 ternary linear substitutions which is isomorphic to the group of the modular equations of 8th degree, and the relation of this *Problem* to the equations of 7th degree. The first thing after showing the existence of G_{168} is to find its invariants. To affect this x_1, x_2, x_3 are regarded as trilinear coördinates of a point in the plane and the substitutions of G thus transform the plane into itself in 168 ways. By these transformations certain points and right lines (the poles and axes) remain invariant, and these form the configuration of the group. Any invariant of the group $\varphi(x_1, x_2, x_3)$ set $= 0$ represents a curve which is invariant for G. Of these

$$f = x_1^3 x_3 + x_2^3 x_1 + x_3^3 x_2$$

is the simplest. Other invariants may be formed by taking its covariants. Two of these Δ and C are respectively of 6th and 14th degree. These, together with an invariant K of 21st degree, form the complete system of the group. The next problem in order is the determination of x_1, x_2, x_3 as algebraic functions of the invariants. Now G_{168} is simple, hence x_1, x_2, x_3 are rational in the roots of any rational resolvent. Such a one is that generated by

$$x_1^2 + x_2^2 + x_3^2 - \frac{1 - \sqrt{-7}}{2}(x_2 x_3 + x_3 x_1 + x_1 x_2).$$

A special form of this resolvent arises when x lies on the fundamental curve $f = 0$ viz:

$$z^7 - 7 \cdot \frac{1 - \sqrt{-7}}{2} \Delta z^4 - 7 \frac{5 + \sqrt{-7}}{2} \Delta^2 z - C = 0.$$

This resolvent is of interest on account of its relation to the transformation equations of the elliptic functions; the general resolvent for which f is not 0 can be reduced to this by introducing an accessory biquadratic irrationality, as Klein has remarked. It is now shown how the equation of the 7th degree $F = 0$ whose group P_{168} is isomorph to G_{168} may be

reduced to the above *Formenproblem*. Obviously it is only necessary to show that three rational functions X_1, X_2, X_3 of the roots of $F = 0$, can be found such that when the substitutions of P_{168} are applied they form the group of linear substitutions G_{168}.

Book IV. Algebraic Numbers.

The theory of numbers until the epoch making paper of Gauss on *Biquadratic Residues* was restricted to integers. But in passing from the theory of quadratic residues to those of higher order, he found it was necessary to enlarge the field of number if we were to arrive at a simple and comprehensive theory. For cubic residues the new numbers to introduce were those formed by the cube root of unity ρ, for biquadratic residues those formed of the fourth root i. Now in the preceding chapters we saw that the integral numbers in $R(\rho)$ and $R(i)$ like ordinary rational numbers can be resolved into prime factors in but one way, and hence all the theorems resting on this fundamental one will subsist too. Like integers, these numbers can also be thrown into a certain number of incongruent classes, so that a linear congruence with prime modulus, for example, has one root only if it has any. Similarly Fermat's theorem and the law of reciprocity have their analogues. Thus Gauss's paper opened up a vista of unlimited expanse; for, while before we had but one class of numbers, the integers, to investigate, now an endless number presented themselves, offering abundant rewards not only in investigating their own peculiar properties, but promising to shed a flood of light on the most hidden properties of the natural integers. At the very outset, however, the first hardy explorers met a barrier which threatened to prevent them from penetrating very far into this virgin territory. It was observed in fact that the bodies $R(\rho)$ and $R(i)$ were rather the exception; that the theorem which asserts the uniqueness of decomcomposition of a number into its prime factors did not hold true in general.* It is an immortal achievement of Kummer's to have overcome this obstacle for cyclotomic bodies by the introduction of his *ideals*. What Kummer has done for the numbers formed of the roots of unity Dedekind and Kro-

* The algebraic body $R(\sqrt{-5})$ affords a simple illustration. In this body 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ are primes in the ordinary sense that they cannot be further decomposed in R; nevertheless we have

$$6 = 2.3 = (1+\sqrt{-5})\ (1-\sqrt{-5}),$$

that is, 6 can be resolved in more than one way into prime facors.

necker have done for numbers formed of the roots of any algebraic equation with rational coefficients. The theory of these numbers is the subject of the present book. Until now the only orderly presentation we have had was that Dedekind has given of his theories in the supplements of Dirichlet's *Zahlentheorie*. But Kronecker has sketched a theory of these numbers from an entirely different standpoint in his *Festschrift;* unfortunately, as there presented, it forms only a special case of a general theory of algebraic quantities; at the same time, according to his usual custom, only the bold features of the theory are outlined. We welcome, therefore, most heartily Weber's attempt to present some of Kronecker's notions and methods relating to algebraic numbers in an elementary and simple manner, and we do not doubt that it will be considered the most important and successful part of the whole treatise. Certainly the wide circulation this work is destined to enjoy will give a powerful impulse to the study of Kronecker's ideas, as Serret's algebra did a generation ago for the ideas of his great countryman Galois. In passing, we remark that we are fortunate in possessing still a third work on the theory of algebraic numbers; this is Hilbert's splendid *Bericht* for the Deutsche Mathematische Vereinigung on *Algebraische Zahlkörper* which has appeared since the second volume of Weber's Algebra came out. The great interest attached to these speculations is shown by the rapidly increasing literature on the subject; we mention in particular Minkowski's Geometrie der Zahlen and Klein's last autographed lectures, Ausgewählte Kapitel der Zahlenlehre.

We turn now to Weber's presentation of Kronecker's theory. A characteristic feature of this we mention at the start; we mean the systematic employment of variables or indeterminates as a vehicle for reasoning on the numbers of an algebraic body. The introduction of these variables may at first sight seem foreign to the theory of numbers, but a simple reflection will do much to remove this and show that Kronecker is merely carrying still further the ideas of Gauss. Indeed, as Kronecker himself remarks,* before Gauss only the quadratic forms of numbers were known; the narrow point of view then prevalent which considered only the various representations of numbers he discarded and introduced forms with real indeterminates. We may thus consider Gauss' whole theory of binary quadratic forms $ax^2 + 2bxy + cy^2$ after the theory of equivalence has been established, as a theory of a system of three

* Festschrift zu Kummer's Doctor Jubiläum, *Crelle* vol. 92, p. 95.

numbers (a, b, c); while if we should remove the indeterminates x, y, which act as the vehicle of our reckoning, not only would it be more difficult to oversee the operations and results but also fundamental theoretical points of view would be lost. It is precisely by the aid of these indeterminates together with the notion of units that the unique decomposition of algebraic numbers is reëstablished. But the usefulness of these indeterminates goes much further; indeed, it is in their systematic employment that the secret of the great power of Kronecker's methods lies.

The first chapter is devoted to the most elementary ideas and theorems. A rational function of the indeterminates $x, y, z, \cdots$ whose coefficients lie in a numerical body Ω is called a *Functionale* or *Form* in Ω. These forms behave in many respects precisely like algebraic numbers; indeed, we may consider these last as particular cases of forms. If the coefficients of a form ω are rational numbers, the form is said to be rational; every such form is the product of a positive rational number a and the quotient of two rational integral functions of the variables $x, y, z, \cdots$ whose coefficients have no common factor; a is called the absolute value of ω; if it is an integer, ω is said to be integral. If the coefficients of ω are not rational numbers, the forms which arise when these coefficients are replaced by their conjugates are called conjugate forms; their product $N\omega$ is called the norm of a; the absolute value of $N\omega$ is the absolute norm $N_a\omega$ of ω. Every form ω is root of an algebraic equation $N(t - \omega) = 0$ where t is a variable not in ω; if the coefficients are integral ω is said to be integral. Next to the notion of *Functionale* the most important new idea is the *Einheiten* or units. Any form ω for which $N_a\omega = 1$ is a unit. Two forms whose quotient is a unit are *associated*. A third fundamental element in the theory is the expression of the greatest common divisor of a number of integral forms $\alpha, \beta, \gamma, \cdots$; this is simply the form

$$\delta = x\alpha + y\beta + z\gamma + \cdots$$

where $x, y, z \cdots$ are new indeterminates. Equipped with these we are ready to raise with ease the first great pillar on which the theory of algebraic numbers rests, we mean the uniqueness of the decomposition of algebraic numbers into their prime factors. This is done generally for *Functionale* following precisely the same path employed before on two similar occasions. The next subject treated relates to the bases of a body Ω, and its discriminant; then we pass

to the consideration of congruences in respect to a form μ. Here the first step is to show that all integral numbers can be thrown into a certain number of classes, each class containing only congruent numbers. To effect this the notion of a basis of a form is introduced and with this we can show that the number of incongruent classes is $N_a(\mu)$. We now have the foundation to develop a theory of congruences analogous to that for integers. For example, the linear congruence

$$\alpha x + \beta \equiv 0 \qquad mod\ \mu$$

has one solution and one only when α is relative prime to μ; while the general congruence of nth degree

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n \equiv 0$$

for a prime form modulus π has at most n roots. Fermat's theorem, which in the ordinary theory is of such fundamental importance, plays here an equally important *rôle*, and reads thus:

$$\alpha^{p^f-1} - 1 \equiv 0 \qquad mod\ \pi$$

where $p^f = N_a(\pi)$ is called the degree of π.

The relation between Dedekind's *ideals* and Kronecker's *forms* is discussed; it is shown that a perfect correspondence is established as soon as all associated forms are regarded as forming a new concept to which, as it behaves like Dedekinds *ideals*, we may attach the same name. Then all forms associated with an integral algebraic number form a *principal ideal.*

By means of the notion of equivalence all forms are thrown into classes whose number h is shown to be finite dependent only on the nature of the body Ω. The composition of these classes is defined, giving rise to an Abelian group of order h. An immediate consequence of the general properties of groups is that, φ being any form in Ω, there exists a number k a divisor of h such that φ^k is associated with a number in Ω. The importance of this simple conclusion will be manifest when we come to establish Kronecker's theorem on Abelian bodies. We observe in passing that when $h = 1$ the theory of the integral numbers in the corresponding body is essentially the same as that of integers; such bodies, for example, are $R(\rho)$ and $R(i)$.

A theorem of fundamental importance regarding the discriminant of a body asserts that it contains at least one prime. Stated by Kronecker* in the Festschrift but with-

* *Crelle*, vol. 92, p. 21.

out proof, its demonstration is a signal achievement of Minkowski. A brief sketch of the geometrical ideas on which it rests we wish to give here. A simple analysis shows that the demonstration rests on the fact that a certain quadratic form $f(x_1, x_2, \cdots, x_n)$, which by means of a real linear substitution

$$(1) \qquad \xi_i = a_{i,1}\, x_1 + \cdots + a_{i,n}\, x_n \quad i = 1, 2, \cdots n,$$

can be thrown into the sum of n squares, is always less than a certain number. Minkowski's geometrical notions make the proof of this very easy. Let $x_1, x_2, \cdots, x_n$ be the coördinates of a point in space R_x; if they take on only integral values their ensemble forms a point system called a *Gitter*. Applying the transformation (1), this *Gitter* goes over into another in the space R_ξ. If

$$V_x = \int dx_1\, dx_2 \cdots dx_n = \lim_{\Delta x = 0} \Sigma \Delta x_1\, \Delta x_2 \cdots \Delta x_n$$

be the volume of some figure G_x in R_x, and V_ξ be that of the corresponding figure G_ξ in R_ξ we have

$$V_\xi = \sqrt{D}\, V_x.$$

Take now $\Delta x = t^{-1/n}$; we have

$$V_x = \lim_{t=\infty} \frac{Z_t}{t}$$

where Z_t is the number of elements of volume in G_x; but this number is that of the number of points in the figure $G_x^{\,t}$ got from G_x by increasing each coördinate in the ratio of $t^{1/n}$ to 1, or also the number in the corresponding figure $G_\xi^{(t)}$ in R_ξ. Calling this number γ and the determinant of f, D, we have

$$V_\xi = \sqrt{D} \lim_{t=\infty} \frac{\gamma}{t}.$$

Now since

$$f = \xi_1^{\,2} + \xi_2^{\,2} + \cdots + \xi_n^{\,2}$$

and the points of the *Gitter* in R_ξ are similarly situated, the least value that f takes on for a point in the *Gitter* R_x is the least distance between any two points in the *Gitter* R_ξ. Denoting this by λ, describe about each point in $G_\xi^{(t)}$ an n-dimensional sphere of radius $\frac{\lambda}{2}$; the volume of all these spheres is less than that of $G_\xi^{\,t}$, that is, less than tV_ξ; and so we find

$$\sqrt{D} > \frac{v\,\lambda^{n/2}}{2^n}$$

where v is the volume of a sphere of unit radius. Using instead of these spheres their inscribed cubes, we find

$$\lambda < n \sqrt[n]{D}$$

which affords a much lower limit than obtained by Hermite, *Crelle*, vol. 40 (1850). A closer approximation using inscribed cylinders is

$$\lambda < n \sqrt[n]{0.404\,D}.$$

Minkowski has obtained still closer ones. Leaving this subject we come to Dedekind's important theorem on the discriminant Δ of a body, which asserts that Δ contains all and only those natural primes as factors which contain the square of a prime ideal. A method due to Hensel is also given to decompose the natural primes into their prime factors; this affords a means of obtaining representatives of all prime ideals of a given body.

Up to the present the properties of algebraic numbers have been studied only with reference to the absolute domain; Hilbert and Dedekind have shown that many important facts are brought to light when we take a different domain. This leads up to relative norms, relative fundamental ideals, etc. In regard to this last it is proved that the fundamental ideal of a body Ω containing R is the product of the relative fundamental ideal of Ω in respect to R and the fundamental ideal of R. The extension of this to a body having a succession of divisors is obvious. Bodies are now considered which are normal in regard to R and an account of some of Hilbert's investigations is given. The *Zerlegungs-* *Trägheits-* and *Verzweigungsgruppen* are studied and an application is made to determine the prime ideals which enter the relative fundamental ideal. The theory is also applied to determine the ideals lying in a divisor of one of these bodies.

The general theory is now left and two delightful chapters follow, containing applications to quadratic and cyclotomic bodies. Both these chapters might be read with great advantage in connection with the preceding 110 pages. They will aid to clear up many difficult points which, up to the present, have been without a single illustrative example. We pass at once to the consideration of the second,

which is of great interest because the facts here established will be of use later in proving Kronecker's theorem. The body in question Ω is formed of the mth roots of unity; m is taken to be the power of a prime q^k, which is quite sufficient for later purposes. The first problem taken up is to determine all the prime ideals in Ω; these arise from the prime q and from other primes. The decomposition of q is at once effected; it is the $\mu = \varphi(m)$ power of a prime ideal of first degree. To decompose the other primes p we apply Hilbert's theory taking here for R the absolute domain. The *Zerlegungs-* and *Trägheitsgruppen* are determined; as the latter is here the identical group, p is not divisible by the square of a prime ideal. The *Zerlegungsgruppe* is of order f, the exponent of p in regard to the modulus m, thus p is the product of $e = \mu/f$ conjugate ideals of degree f. The nature of these ideals is examined, making use of the fact that the *Zerlegungsgruppe* is isomorphic with a subgroup of the class groups for the modulus m. The investigation culminates in a generalization of Kummer's theorem on the decomposition of Lagrange's resolvent, which we shall have occasion to cite later. Connected with Ω is a real body H embracing all the real numbers of Ω. In this body q is the $\frac{1}{2}\mu$ power of a prime ideal of first degree; the other primes p fall into two classes, for one class the prime ideals of H are also prime in Ω, for the other they split into two factors in Ω. In regard to the numerical units in Ω it is shown that they are all the product of a real unit lying in H and a unit root in Ω; these last are powers of a primitive mth root of unity r multiplied by ± 1. The next three chapters, which also terminate the account given of algebraic numbers, are devoted to the demonstration of Kronecker's great theorem that all Abelian bodies in the domain of rational numbers are cyclotomic bodies. The demonstration here given rests upon three main supports: the decomposition of Lagrange's resolvent into prime ideals, the determination of an expression of h, the *Classenzahl* or class number of Ω, and finally an intimate knowledge of the numerical units of Ω. Considered merely as a demonstration of Kronecker's theorem we should be obliged to criticise its great length and prefer in its stead the one due to Hilbert,* which besides being very short, avoids the transcendental methods of Dirichlet introduced

*"Ein neuerer Beweis, etc.," *Göettinger Nachrichtne*, January, 1896. Hilbert's proof is purely arithmetical and rests on his theory of a Galoisian numerical body which Weber sketches in Chapter 19. A prominent feature of the demonstration is Minkowski's theorem that the discriminant of every body contains at least one prime.

by the *Classenzahl.* But if we consider it as a delightful stroll through some of the more abstruse parts of the general theory of algebraic numbers, stimulated by the knowledge that the facts picked up on the way not only enable us to prove Kronecker's theorem but are among the most important in the whole theory, we shall surely thank our guide for choosing precisely the route taken. We give now a sketch of the principal steps in the demonstration. A simple reasoning shows we need only to prove the theorem for Abelian bodies whose degree is the power of a prime $m = q^k$ and whose group is cyclic. Lagrange's resolvent

$$(r^s, x) = x_0 + r^s x_1 + r^{2s} x_2 + \cdots + r^{(m-1)s} x_{m-1}$$

is considered ; here $x_0, x_1, \cdots, x_{m-1}$ are the roots of a rational irreducible cyclic equation of degree m, and r is a primitive mth root of unity which generates Ω.

The above resolvent gives us

$$mx_0 = \Sigma(r^s, x_0) \qquad s = 0, 1, \cdots, m-1$$

and as $(r^s, x_0)^{-1}\ (r, x_0)$ lies in it, it remains to show that (r, x_0) is cyclotomic or what is the same that $\omega = (r, x_0)^m$ is the mth power of a cyclotomic number. To effect this ω is decomposed into its ideal primes in Ω and now the determination of all the prime ideals in Ω, together with Kummer's theorem, are needed. It is found that ω is the product of a unit form ε, the mth power of a form φ and the mth power of certain cyclotomic numbers K lying in a higher body but such that K^m lies in Ω. We can thus write

$$\omega = \varepsilon\, \varphi^m K_1^m K_2^m \cdots \tag{1}$$

This shows that the conjugate forms φ_n^m belong to the principal class. Suppose now that we can show

(*A*) *that the forms φ_n belong to the principal class ;*

then (1) shows that ω_n has the form

$$\omega_n = e_n a_n^m K_1^m K_2^m \cdots \tag{2}$$

where e_n are now numerical units. Suppose secondly that we can show

(*B*) *that the numerical units e_n are mth powers of a unit β in Ω multiplied by a power of r ;*

then (2) shows that

$$(r, x_0) = \rho\beta K_1 \ K_2 \cdots \tag{3}$$

where ρ is a unit root; as the right hand side of (3) is a cyclotomic number, Kronecker's theorem is proved. There remains thus the demonstration of (A) and (B); this is very different according as q is odd and even. The former case can be easily disposed of. (A) is proved by using Weber's generalization of Kummer's theorem while (B) is demonstrated at once using the fact already established that all numerical units in Ω are, aside from their sign, the product of a unit in H and a power of r. The case when q is even, that is when m is a power of 2, presents the most serious difficulties as Kronecker remarked in his paper in the *Monatsberichte* of 1853 already referred to. The demonstration of (A) for this case Weber makes depend on the oddness of the *Classenzahl* h by remarking that if φ^k belongs to the principal class and k is not divisible by 2, φ also does. Concerning (B) a simple reasoning shows that this is proved if it can be shown that when a real unit e in Ω together with its conjugates are all positive, then e is the square of a real unit in Ω. In the reasoning which follows we mention two theorems as fundamental. Dirichlet's theorem on the numerical units of *any* algebraic body Ω we may state thus: If among the m conjugate bodies

$\Omega, \Omega_1, \Omega_2, \cdots \Omega_{m-1}$, m_1 are real and $m_2 = \frac{m-m_1}{2}$ form conjugate pairs, then there exists in Ω a system of $\mu = m_1 + m_2 - 1$ units $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_\mu$ such that every unit in Ω is represented once only by

$$\rho \varepsilon_1^{\xi_1} \varepsilon_2^{\xi_2} \cdots \varepsilon^{\xi_\mu}$$

where $\xi_1\ \xi_2 \cdots$ are integers and ρ is a unit root in Ω.

The second is Dedekind's expression for the *Classnumber*

$$\lim_{s=1} (s-1)\, \Phi(s) = gh$$

where $\Phi(s)$ is the series

$$\Sigma \frac{1}{N_a(a)^s}$$

the sum extending over all the ideals a in Ω, and g being a number depending on Ω only. The series Φ converges for all $s > 1$.

The last chapter is devoted to transcendental numbers; as it has been admirably translated by Professor Beman* for the BULLETIN we do not need to give an account of it.

* BULLETIN, 1897, p. 174.

We will close now our review regretting its inadequacy to give but a faint idea of the merits of this great work. A classic from the day of its publication, it is destined to a long and useful career, a monument of honor to its genial author.

JAMES PIERPONT.

YALE UNIVERSITY,
December, 1897.

SHORTER NOTICES.

Analytic Geometry for Technical Schools and Colleges. By P. A. LAMBERT, M.A., Instructor in Mathematics, Lehigh University. New York, The Macmillan Co., 1897. 8vo, 216 pp. Price, $1.50.

The volume before us differs greatly in the choice and arrangement of material from the standard English textbooks on analytic geometry, and clearly shows the influence of Briot and Bouquet's "Géométrie Analytique." In the first few pages Cartesian coördinates are defined, and exemplified by curves plotted from tables of statistics. In the second chapter the straight line, the circle, the conic sections, the ellipse, the hyperbola, and the parabola are allotted a paragraph each, and the student is hurried on in Chapter III. to the plotting of algebraic equations, and in Chapter IV. to the plotting of transcendental equations.

The discussion, at this early stage, of the curves represented by the exponential, logarithmic and circular functions, the cycloids, etc., should be of interest to the beginner, and shows the reaction against the undue prominence frequently given to the conic sections in works on elementary geometry. It would be absurd to expect a thorough treatment of the theory of curve-tracing in such limited space, but one or two unnecessarily misleading statements might have been avoided. The tangent is defined as a secant having two points of intersection with the curve "coincident," instead of consecutive, and a similar misuse of terms occurs in defining a point of inflection. The point of inflection is the only singularity discussed, therefore the distinction between the analytical conditions for a point of inflection and a double-point, often a question of some difficulty to the young student, is not touched on.