AN INTRODUCTORY ACCOUNT OF THE ARITHMETICAL THEORY OF ALGEBRAIC NUMBERS AND ITS RECENT DEVELOPMENTS *

BY L. J. MORDELL

1. *Introduction.* In dealing with the subject of my lecture, I might have considered it from a purely logical point of view, and developed it in all its beauty in this manner. I think, however, it will be of more interest to you if I introduce it from the historical standpoint. Its beginnings date from Euler, who attempted to prove Fermat's statement, that the only integer solutions of the equation $y^2 + 2 = x^3$ were $x = 3$, $y = \pm 5$, by putting $x = a^2 + 2b^2$ and taking

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3.$$

By equating irrational parts, he found

$$1 = b(3a^2 - 2b^2),$$

whence $b = 1$, $a = \pm 1$; but it is neither obvious nor true in general that all the integer solutions can be found in this way, —one used by Euler and Lagrange for some related questions. Then, about 1800, much interest was shown in the so-called law of quadratic reciprocity, first rigorously proved by Gauss; namely, that if p and q are two odd positive primes

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

The symbol (p/q) denotes $+1$ or -1, according as the congruence $x^2 \equiv p \pmod{q}$ is possible or impossible, and then p is called a quadratic or non-quadratic residue respectively of q. With certain extensions, this law is really equivalent to a reduction formula enabling us to calculate the value of the symbol (p/q), and forms the foundation of the theory of numbers.

* Lecture read before the London Mathematical Society on January 18, 1923, and, by request of the program committee, before the American Mathematical Society, on September 6, 1923.

Obvious generalizations are suggested for other congruences, such as

$$x^3 \equiv p \pmod{q}, \qquad x^4 \equiv p \pmod{q}.$$

Taking the latter, it was found that the result appeared in a very complicated form, which, however, simplified remarkably if, instead of primes p and q, we considered their decompositions (when possible) in the form

$$p = a^2 + b^2,$$

or into complex factors $(a + ib)(a - ib)$. This led Gauss to the study of the arithmetic properties of complex numbers of the form $z = a + ib$, where a and b are integers. He proved that they did not differ essentially from those of ordinary integers, and showed that it was a very simple matter to define primes so that complex numbers could be factored uniquely, that if a product $z_1 z_2$ were divisible by a complex prime z, then either z_1 or z_2 was divisible by z, etc.

Gauss also showed that if p was a prime of the form $4n + 1$, then the value of a (odd say) was given by the absolutely least residue satisfying the congruence

$$a \equiv (-1)^{n+1} \tfrac{1}{2} \frac{2n!}{(n!)^2} \pmod{p}.$$

This result was extended by Stern, Cauchy, Jacobi, and Eisenstein. The proofs depended upon complex numbers formed from other roots of unity than the fourth root i and applications were made to laws of reciprocity.

The most important facts concerning these numbers were discovered in connection with Fermat's last theorem on the insolubility in non-zero integers of the equation

$$x^p + y^p = z^p.$$

The left-hand side can be factored in the form

$$(x + y)(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^{p-1} y) = z^p,$$

where ζ is a complex pth root of unity; and it appeared to be a natural assumption, by analogy with elementary arithmetic, to put

$$x + \zeta y = (A + B\zeta + C\zeta^2 + \cdots)^p,$$

or perhaps to some multiple of the right-hand side, where $A, B, C, \cdots$ are ordinary integers. This involved the assumption that these algebraic numbers could be factored in a unique manner, an assumption which was, however, in general erroneous. This can be seen from a far more simple case:

$$21 = 3 \cdot 7$$
$$= (4 + \sqrt{-5})(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}),$$

and it is easily verified that none of $3, 7, 4 \pm \sqrt{-5}, 1 \pm 2\sqrt{-5}$ can be split up into factors of the form $a + b\sqrt{-5}$ with a and b integers. Again

$$3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

and $2 \pm \sqrt{-5}$ are not squares, and neither have a common factor of the form $a + b\sqrt{-5}$, nor can be split into factors of this form.

The primary object of the theory was to re-establish order in the chaos produced by the breakdown of the fundamental theorem upon which depends all the higher arithmetic. This was accomplished by Kummer in the special case of the algebraic numbers arising from the roots of unity, and more generally by several other writers. We shall give an account of Dedekind's method, since the main idea is not only easily explained, but is also very characteristic of mathematics, in generalizing a concept or a function by including it in a wider one. This idea is familar to all, e.g., $n!$ initially defined by $1 \cdot 2 \cdot 3 \cdots n$ when n is an integer, is generalized to

$$\Gamma_{(n)} = \int_0^\infty e^{-x} x^{n-1} dx,$$

when n has its real part positive; and for all values of n by the well known infinite product. Again the chord of contact of the tangents from a point P to a conic can be generalized as the polar of P, giving from one point of view a simpler interpretation when the tangents are imaginary. Dedekind's idea was to consider groups of numbers which he called ideals, and with the obvious method of multiplying and dividing such groups as suggested by their definition, he showed that a

unique factor law existed for his ideals, and that his results included as particular cases the fundamental laws of arithmetic and the correct arithmetical deductions to be drawn from relations involving algebraic numbers.

2. *Algebraic Numbers.* We must now define an algebraic number. The number θ is called an *algebraic number* if it is the root of an equation of the form

$$a\theta^n + b\theta^{n-1} + \cdots + l = 0,$$

where $a, b, \cdots, l$ are ordinary integers. If $a = 1$, θ is called an *algebraic integer,* and it is easy to show that this generalization is consistent, e.g., the sum, difference, product of integers are integers, and that if an algebraic integer is rational, it must be an ordinary integer. We may suppose that the equation in θ is irreducible in the field of rationality R defined by the ordinary integers, and that it has r_1 real roots and r_2 pairs of imaginary roots.

Any rational function of θ with rational coefficients, i.e., coefficients in R, can be reduced to the form

$$f = A_0 + A_1\theta + \cdots + A_{n-1}\theta^{n-1},$$

where $A_0, A_1, \cdots, A_{n-1}$ are rational numbers; and the assemblage of all such functions is referred to as the *field* or *Körper* $K(\theta)$. If f is an algebraic integer, the numbers conjugate to f are also algebraic integers, and by writing down the conjugate equations and solving, we find that $d(\theta)A_0$, $d(\theta)A_1$, $\cdots$ are rational integers where $d(\theta)$ is the discriminant of the equation in θ. Hence any algebraic integer in the field $K(\theta)$ can be written as

$$f = \frac{1}{d(\theta)}(a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}),$$

where $a_0, a_1, \cdots, a_{n-1}$ are integers. From this it follows that we can find n algebraic integers $\omega_1, \omega_2, \cdots, \omega_n$ called the base of the field, such that any algebraic integer f can be written in the form

$$f = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n,$$

where $x_1, x_2, \cdots, x_n$ are rational integers. For example, in the field $K(\sqrt[3]{2})$, all integers are of the form $x_1 + x_2\sqrt[3]{2} + x_3\sqrt[3]{4}$, while in the field $K(\sqrt{5})$ they are of the form $x_1 + x_2(1 + \sqrt{5})/2$.

The base can be chosen in an infinite number of ways, but any one base can be derived from any other by a linear substitution in the ω's with integer coefficients and with a determinant unity. Hence the square of the determinant formed from the ω's and their conjugates, that is,

$$d = \begin{vmatrix} \omega_1^{(1)}, \omega_2^{(1)}, \cdots, \omega_n^{(1)} \\ \omega_1^{(2)}, \omega_2^{(2)}, \cdots, \omega_n^{(2)} \\ \cdots\cdots\cdots \end{vmatrix}^2,$$

where $\omega_1^{(2)}$, etc., are the conjugates of $\omega_1^{(1)} = \omega_1$, etc., is an invariant of the bases, and is a rational integer called the discriminant d of the field. It is always greater than unity, and there are only a finite number of algebraic fields with a given discriminant d, as follows from an asymptotic formula given by Minkowski (as an example of his result stated further on), namely

$$d \sim \frac{1}{2\pi n}\left(\frac{\pi}{4}\right)^{2r_2} e^{2n - \frac{1}{6n}}.$$

3. *Units.* Among algebraic integers the most important are the units, i.e., the divisors of unity. For example, in the field $K(i)$, $\pm 1, \pm i$ are divisors of unity, while in the field $K(\sqrt{2})$, $t + u\sqrt{2}$ is a unit if the integers t, u satisfy the equation $t^2 - 2u^2 = \pm 1$. It is well known that all the units are given by $\pm(1 + \sqrt{2})^n$, where n is any integer.

A similar theory holds in the general case, since it was proved by Dirichlet that any unit can be represented in the form $e_1^p e_2^q, \cdots$ for a finite number of values of $e_1, e_2, \cdots$, where $p, q, \cdots$ are any integers. For example, in the field $K(\sqrt[3]{2})$, the units are of the form $x + y\sqrt[3]{2} + z\sqrt[3]{4}$, where x, y, z are integers satisfying the equation

$$x^3 + 2y^3 + 4z^3 - 6xyz = \pm 1,$$

where the left-hand side is the norm of $x + y\sqrt[3]{2} + z\sqrt[3]{4}$,

so that the theory gives the complete solution of this equation in x, y, z. It has lately been announced that it can be shown in this way that the equation $x^3 - ay^3 = 1$ never has more than one integer solution when a is given.

4. *Minkowski's Theorem.* It is Minkowski's theorem on linear forms, however, which is fundamental in the theory and has contributed greatly to its simplicity and elegance, namely, that integer values of x and y, not both zero, can be found so that

$$|ax + by| \leqq p, \qquad |cx + dy| < q,$$

where a, b, c, d are any real numbers, and $p, q > 0$, satisfy the equation

$$pq = \begin{vmatrix} a, & b \\ c, & d \end{vmatrix}.$$

There is of course the obvious extension to any number of variables $x, y, z, \cdots$.

No less than four distinct proofs have been given. The original proof by Minkowski is equivalent to the geometric theorem that any parallelogram in the x, y plane with one vertex at the origin and area $\geqq 1$ contains at least one lattice point on its sides or within its interior and is really a particular case of a far more general one. This proof, as well as the latest one just given by Siegel, which is analytic in character and depends upon trigonometric series, applies directly regardless of whether the coefficients are rational or not. The other proofs are arithmetic in character, first establishing the theorem for rational coefficients. Hilbert's proof depends upon Dirichlet's idea that if $n + 1$ objects are arranged in n groups, then one group will contain at least two objects. The proof by Hurwitz is a beautiful piece of arithmetic work, very characteristic of the author, showing that there are

$$\begin{vmatrix} a, & b \\ c, & d \end{vmatrix}$$

forms of the type $\lambda x + \mu y$, such that all forms $Ax + By$, with A, B integers, can be written in the form

$$\lambda x + \mu y + p(ax + by) + q(cx + dy),$$

where all coefficients, etc., are integers, and where a, b, c, d are given.

5. *Test for Algebraic Numbers.* I may say here a few words regarding the conditions that a given number θ should be an algebraic number of the nth degree, i.e., the root of an equation of the nth degree irreducible in R. Of the two kinds known, one states that a number θ cannot be an algebraic number of the nth degree if we can find an infinity of rational approximations p/q, such that

$$\left|\frac{p}{q} - \theta\right| < \frac{c}{q^{\lambda}},$$

where c is a given number, and where $\lambda > n$ according to Liouville, $\lambda \geqq n$ according to Thue in 1908, or finally $\lambda > 2\sqrt{n}$ according to Siegel in 1921. From this flow such results as that the equation $f(x, y) = c$ has only a finite number of integer solutions if f is an irreducible binary quantic in x, y of degree greater than 2. The proofs are very complicated, but very remarkable, depending only on elementary algebra.

The other types of results are due to Minkowski and Furtwängler and depend upon the investigation of the minima of the form

$$x_0 + x_1\theta + \cdots + x_{n-1}\theta^{n-1}$$

for integer values of $x_0, x_1, \cdots, x_{n-1}$, all numerically less than some number t. If now t takes the values $1, 2, \cdots$, we have a series of minima $m_1, m_2, m_3, \cdots$, which are such that the ratios $m_2/m_1, m_3/m_2, \cdots$ have only a finite number of values for all values of t.

6. *Ideals.* The algebraic integers in the field $K(\theta)$ form the foundation of all that follows, just as ordinary rational integers do in arithmetic, and the word *integer* hereafter refers to the integers in the field $K(\theta)$.

Let $\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_p$ be any given integers; then the *ideal* A is the group of integers defined by $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots$, where $\lambda_1, \lambda_2, \lambda_3, \cdots$ are any integers, a fact expressed by the notation

$$A = [\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_p].$$

The ideals A and $B = [\beta_1, \beta_2, \beta_3, \cdots, \beta_q]$ are equal, written $A = B$ if every number of A is included in B and conversely; i.e., if integers λ, μ can be found so that

$$\beta_1 = \lambda_{11}\alpha_1 + \lambda_{12}\alpha_2 + \cdots, \qquad \beta_2 = \lambda_{21}\alpha_1 + \lambda_{22}\alpha_2 + \cdots,$$

and

$$\alpha_1 = \mu_{11}\beta_1 + \mu_{12}\beta_2 + \cdots, \qquad \alpha_2 = \mu_{21}\beta_1 + \mu_{22}\beta_2 + \cdots.$$

An ideal is called a *principal ideal* if it can be written in the form $[\alpha]$, so that it consists of all the integers divisible by α. Further the principal ideals $[\alpha]$ and $[\beta]$ are equal if and only if α and β are associated integers, i.e., $\alpha = \beta e$, where e is a unit.

In particular, if $\alpha = 1$, we have as the unit ideal [1] all the integers in $K(\theta)$.

We can now extend many arithmetic concepts to ideals. Thus the product AB of the ideals A and B is defined as the ideal C formed from the numbers obtained by multiplying every number of A by every number of B; and we write $C = AB$. The commutative law is obviously satisfied, so that we can write $A \times A = A^2$, $A \times A \times A = A^3$, etc., while A^0 stands for the unit ideal [1].

Division is defined as the inverse of multiplication, so that the ideal C is divisible by the ideal A if an ideal B can be found so that $C = AB$. An ideal P is called a *prime ideal* if it is divisible by only itself and [1], the unit ideal. Finally, two ideals are called *prime to each other* if they have no common divisor except [1].

The fundamental theorem in the theory of ideals states that an ideal can be factored in only one way, apart of course from the order of the factors. Many important consequences follow just as in elementary number theory. The proof can be presented in several different ways, requiring in any case a long chain of subsidiary propositions. In Hurwitz' method the important steps are as follows:

(1) Corresponding to any ideal A we can find an ideal B so that AB is a principal ideal $[\alpha]$ where α is a positive rational integer.

(2) From the equality $[\gamma]A = [\gamma]B$, we have $A = B$, and hence from $CA = CB$, also $A = B$. From these we show that if C is divisible by A, every number of C is included in A, and conversely.

It is then shown that an ideal A has only a finite number of divisors, since a given rational integer α is a member of only a finite number of ideals.

The next step is to show that if an ideal P is a divisor of AB, then either A or B is divisible by P. This depends upon the fact that the greatest common divisor of the ideals A, B is given by $[\alpha_1,\alpha_2, \cdots, \alpha_p, \beta_1, \beta_2, \cdots, \beta_q]$. The result follows immediately.

An ideal can be factored by a definite and direct process. We can then factor any algebraic integer I by factoring the principal ideal $[I]$. Suppose we find

$$[I] = A^\lambda B^\mu C^\nu \cdots,$$

where $A, B, C, \cdots$ are different prime ideals. Then if $A, B, C, \cdots$ are principal ideals $[\alpha]$, $[\beta]$, $[\gamma]$, $\cdots$, we have the result that

$$I = \epsilon \alpha^\lambda \beta^\mu \gamma^\nu \cdots,$$

where ϵ is a unit. If, however, one at least of the ideals $A, B, C, \cdots$ is not a principal ideal, the integer I cannot be factored in the ordinary sense, though the ideal $[I]$ can be. It is for this reason that I cannot be considered as a prime, and that a unique factorization law that would naturally suggest itself does not hold in the theory of algebraic numbers.

7. *Congruences and Norms.* We can now consider congruences with respect to ideals. A number μ is said to be divisible by the ideal A if μ is one of the numbers forming the ideal A, or, what amounts to the same thing, if the principal ideal $[\mu]$ is divisible by A; and we write

$$\mu \equiv 0 \pmod{A}.$$

Hence we mean by the congruence

$$\mu \equiv \nu \pmod{A}$$

that $[\mu - \nu]$ is divisible by A, or that $\mu - \nu$ belongs to the ideal A. The ideal A is only a part of the integers of $K(\theta)$, and the number of incongruent integers (mod A) is finite and is denoted by $N(A)$. In particular, if A is a principal ideal $[\mu]$, $N(A)$ is the absolute value of the product of μ by its conjugates. For example, in the field $K(i)$, if ω is a prime of the form $a + ib$, where $p = a^2 + b^2$ is a rational prime $\equiv 1 \pmod 4$ and where a, b are rational integers, the number of incongruent integers (mod ω) is

$$(a + ib)(a - ib) = p.$$

If μ is a rational integer, the number $N(\mu)$ becomes $|\mu^n|$.

The norm satisfies the law

$$N(A)N(B) = N(AB).$$

To find a simple formula for the norm of an ideal, we first prove that an ideal has a base, i.e., n integers $\alpha_1, \alpha_2, \cdots, \alpha_n$ can be found so that all the numbers of A can be written in the form

$$\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n,$$

where $\lambda_1, \lambda_2, \cdots, \lambda_n$ are rational integers, and further that the determinant

$$\begin{vmatrix} \alpha_1^{(1)}, \alpha_2^{(1)}, \cdots, \alpha_n^{(1)} \\ \alpha_1^{(2)}, \alpha_2^{(2)}, \cdots, \alpha_n^{(2)} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{vmatrix}$$

formed from the base and its conjugates is an invariant of the ideal. The numbers $\alpha_1, \alpha_2, \cdots, \alpha_n$ of the base can be expressed in terms of the base $\omega_1, \omega_2, \cdots, \omega_n$ of the field by means of the equations

$$\begin{aligned} \alpha_1 &= c_{11}\omega_1 + c_{12}\omega_2 + \cdots, \\ \alpha_2 &= c_{21}\omega_1 + c_{22}\omega_2 + \cdots, \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{aligned}$$

where the c's are rational integers. The determinant $|c_{kl}|$ is the norm of the ideal A. We can also write

$$|\alpha_{kl}|^2 = dN^2(A),$$

a most useful equation.

The norm of a prime ideal P takes a very simple form. For P must be a divisor of a rational prime p which is the smallest rational integer divisible by P. Hence we have

$$N(P) = p^f, \quad \text{where} \quad 1 \leqq f \leqq n.$$

The integer f is called the *grade* of the ideal. It should be noted that only a finite number of ideals have a given norm.

There are of course an infinite number of ideals, but they can be divided into a finite number of classes. Thus an ideal A will be called equivalent to B, i.e., they are in the same class, if integers α, β can be found so that

$$[\alpha]A = [\beta]B,$$

a fact expressed by writing $A \sim B$.

All the principal ideals are equivalent, and they constitute the principal class. Further, there are only a finite number of classes, as follows from the fact that every class contains an ideal whose norm $\leqq \sqrt{d}$. This is a simple deduction from the fact, depending upon Minkowski's theorem, that every ideal A contains a number a such that

$$|N(a)| \leqq N(A)\sqrt{d}.$$

We could also in this way actually calculate H, the number of ideal classes. The classes of ideals form an ordinary abelian group.

The whole theory can be developed by proving that H is finite, and then deducing the unique factorization law.

8. *Application to Indeterminate Equations.* This number H, and the fact that it is finite, are of the greatest importance in the applications to indeterminate equations. For if A is any ideal, then A^H belongs to the principal class, i.e., $A^H \sim [1]$. Conversely, if $A^n \sim [1]$, and n is prime to H, it follows that A is a principal ideal. Hence, if we wish to draw any conclusion from the equality $ab = c^n$ in algebraic integers, we must first write it as an equation in ideals $[a][b] = [c]^n$. Therefore, if the ideals $[a]$, $[b]$ have a common factor, say a principal ideal $[d]$, we must have, say,

$$[a] = [d]A^n, \qquad [b] = [d]^{n-1}B^n,$$

where $[c] = AB$; and the ideals A and B will be principal ideals only if n is prime to H. We then have

$$A = [x], \qquad B = [y],$$
$$[a] = [d][x]^n, \qquad [b] = [d]^{n-1}[y]^n,$$

whence $a = dx^n e$, where e is some unit.

For example, in Fermat's equation in rational integers,

$$x^p + y^p = z^p,$$

or

$$(x + y)(x + \zeta y)(x + \zeta^2 y) \cdots = z^p,$$

where $\zeta = e^{2\pi i/p}$, we consider first the case when x, y, z are all prime to p, that is, the greatest common factor of the ideals $[x + \zeta y], [x + \zeta^2 y], \cdots$, is unity. Hence, if p is prime to the number of ideal classes in the field $K(\zeta)$, we have

$$x + \zeta y = e a^p,$$

where e is a unit and a is an algebraic integer. It is not very difficult to prove from this equation that Fermat's equation is impossible. Similarly, when one of x, y, z is divisible by p, all, of course, on the assumption that p is prime to H.

Another illustration is given by the classical indeterminate equation

$$az^2 = x^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4,$$

where a, b, c, d, e are given rational integers and x, y, z are unknown rational integers. If θ is a root of the equation

$$\theta^4 + b\theta^3 + c\theta^2 + d\theta + e = 0,$$

az^2 has a factor $x - \theta y$, so that we have the equation in ideals

$$[x - \theta y] = \mu\tau^2,$$

where μ is one of a finite number of ideals and τ is an unknown ideal. Since the number of ideal classes is finite we can put $\tau = \alpha v/\beta$, where α, β are integers, and v is one of a finite number of ideals. Then μv^2 must be one of a finite number of principal ideals, say $[\gamma]$, so that

$$[x - \theta y] = \alpha^2[\gamma]/\beta^2,$$

whence

$$x - \theta y = \epsilon\alpha^2\gamma/\beta^2,$$

where e is a unit. Since all units can be expressed in the form $\epsilon_1 \epsilon_2^2$ for a finite number of values of ϵ_1, we deduce an equation

of the form

$$x - \theta y = \nu\alpha^2,$$

where ν is one of a finite number of integers and α is an unknown integer. If this has an infinite number of solutions, we have for a particular solution

$$x_0 - \theta y_0 = \nu\alpha_0^2,$$

whence, by multiplication, we can deduce an equation of the form

$$(x - \theta y)(x_0 - \theta y_0) = M^2(a + b\theta + c\theta^2 + d\theta^3),$$

where x, y, a, b, c, d are unknown rational integers and x_0, y_0, M are given rational integers. It was from an equation of this form (e.g., with $x_0 = 1$, $y_0 = 0$) that I showed that the method of infinite descent applied to the original equation, and hence to the homogeneous ternary cubic

$$f(x, y, z) = 0,$$

i.e., that all its rational solutions could be derived from a finite number by the classic method.*

9. *The Class Number.* The problem of finding the number H of ideal classes is a very interesting and difficult one. Analytically H is a multiple of the residue at $s = 1$ of the function defined when the real part of s is greater than one, by

$$f(s) = \sum \frac{1}{N[A]^s},$$

where the summation refers to all the ideals of the field $K(\theta)$. This is deduced from the series

$$f_L(s) = \sum_A \frac{1}{N(A)^s},$$

the summation referring to all the ideals in the class L, and the residue at $s = 1$ being independent of the class L. We may also write

$$f_L(s) = N(B)^s \sum_\mu \frac{1}{N(\mu)^s},$$

where the summation refers to all non-associated integers μ divisible by the ideal B, and B is an ideal in the class L^{-1}.

*The same method shows that $Ey^2 = Ax^3 + Bx^2 + Cx + D$ has only a finite number of integer solutions if the right side has no squared factor in x.

The function $f(s)$ is the analog of the ordinary Riemann zeta function. Its chief properties remained unknown for many years, and their investigation was one of the problems proposed by Hilbert in his address in 1900 to the International Mathematical Congress at Paris.

In 1916, it was shown by Hecke that $f(s)$ represented a function of s which can be continued throughout the s plane, whose only singularity is a simple pole at $s = 1$, and which also satisfies a very simple functional relation. His method can be illustrated by considering the ordinary ζ function

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots.$$

By using the gamma function, we can express this as a definite integral

$$\int_0^\infty \xi^{\frac{s}{2}-1}\theta(\xi)d\xi,$$

where $\theta(\xi)$ is practically a theta function. The range of integration is split into $\int_1^\xi + \int_0^1$. In the former, ξ is changed into $1/\xi$ and the classical transformation formula for $\theta(1/\xi)$ is applied. The result at once follows. Moreover, a simple functional equation between $\zeta(s)$ and $\zeta(1 - s)$ is apparent.

The same method applies to $f_L(s)$ by noting that

$$N(\mu) = \mu_1\mu_2 \cdots \mu_n,$$

so that $f_L(s)$ can be transformed into a multiple integral with limits ∞, 0 by writing

$$\Gamma_{(s)}k^{-s} = \int_0^\infty e^{-kt}t^{s-1}dt$$

if k is real and positive, $R(s) > 0$. The great difficulty was to express the fact that the summation refers to the non-associated integer μs, i.e., that only one number of the group $e_1^p e_2^q \cdots \mu$ arising from any integer values of p, q appears in the summation. By writing the limits of integration as

$$\int_0^1 + \int_1^2 + \int_2^3 + \cdots,$$

Hecke transformed the integral into a theta series with n vari-

ables associated with the ideal, where the summation now refers to all the integers μ (not merely the non-associated one). Moreover, since the multiple theta series also had a simple transformation formula, he was able to find a simple functional relation between $f(s)$ and $f(1-s)$, to show that $f(s)$ exists all over the s plane, and has a simple pole at $s=1$. Siegel has lately shown that these results can be found in another way, wherein the units make no appearance. The same method applies to many functions associated with or derived from the Dedekind zeta function, such as the series

$$\sum_A \frac{\chi(A)}{[N(A)]^s},$$

where now $\chi(A)$ is a root of unity associated with the ideal A, and many results in the ordinary theory of prime numbers can be extended to the case of prime ideals. For example, the prime number theorem, which states that the number of primes less than x is asymptotically equal to $x/\log x$, is equivalent to the fact that the Riemann zeta function has only a simple pole at $s=1$ and no zeros in a contour whose right-hand boundary is say $z=2$, and whose left-hand boundary approaches $z=1$ from the left according to the law

$$y = 1 - \frac{a}{\log x},$$

where a is a constant. The Dedekind zeta function has practically the same properties as the Riemann function whence results the same asymptotic formula for ideals as for ordinary primes, e.g., the number of prime ideals whose norm $\leqq x$ is asymptotically equal to $x/\log x$. Further Hecke was able to prove results such as that the indefinite form $ax^2+bxy+cy^2$ represents an infinite number of primes in any given sector of the xy plane whose center is at 0 and whose radius is infinite. The θ functions dealt with by Hecke are associated with ideals and algebraic numbers in a very simple and elegant manner. A simple case is that in which we have

$$\theta(t,A) = \sum_{\mu \equiv 0 \pmod{A}} e^{-c|\mu_1|^2 t_1 - c|\mu_2|^2 t_2 - \cdots - c|\mu_n|^2 t_n},$$

where the summation refers to all the numbers $\mu = \mu_1$ of an ideal A, and $\mu_2, \mu_3, \cdots$ are the conjugates of μ, and c is a constant depending on the ideal A. Then we may write

$$\theta(t, A) = \frac{1}{\sqrt{t_1 t_2 \cdots t_n}} \theta\left(\frac{1}{t}, B\right),$$

where B is an ideal derived very simply from A, namely $AB = 1/D$, where D is the *grund* ideal, really an ideal whose norm is the discriminant d.

These θ functions led Hecke to the consideration of Gauss' sums in any algebraic field, for which they are as important as are the ordinary Gauss' sums in the elementary theory of numbers. He showed that the reciprocity formula for them follows from the functional equation for the zeta function, and that the law of quadratic reciprocity for any algebraic field is a simple consequence of his general methods. His functional equations have enabled him to prove a number of striking results, both arithmetic and analytic. One of the latter is that if $R(x)$ is the fractional part of x so that $0 \leqq R(x) < 1$, while $x - R(x)$ is an ordinary integer, then the Dirichlet series

$$\sum_{m=1}^{\infty} \frac{R(ma) - 1/2}{m^s},$$

where $a = \sqrt{d}$ or $1/\sqrt{d}$, represents a meromorphic function of s, analytic for $R(s) > 0$, while if $R(s) \leqq 0$, it has simple poles at the points represented by the formula

$$s = -2k \pm \frac{2n\pi i}{\log \eta}, \quad (n, k = 0, 1, 2, \cdots),$$

where η is the fundamental unit or its square in the field $K(\sqrt{d})$.

10. *Representations as Sums of Squares.* Siegel has shown that the methods introduced by Hardy and Littlewood into the analytic theory of numbers can also be extended to similar questions involving algebraic numbers. Thus the question of finding approximate formulas for the number of representations of a given rational integer n as a sum of say 5 squares is equivalent to finding the coefficient of x^n in the expansion

of $f(x) = (1 + 2x + 2x^4 + \cdots)^5$. This is given by a contour integral around a circle whose radius is taken to be very nearly one, say $1 - 1/n$. The range of integration 2π and 0, or say 1, 0, is split up into arcs according to the Farey method of division of order, say $[\sqrt{n}]$. If the fraction p/q is associated with one of these arcs, the integrand is evaluated approximately at $x = e^{2\pi ip/q}$ and the sum of the resulting integrals is proved to be a genuine approximation. Siegel has shown that if we seek the number of representations of an algebraic integer as a sum of squares of algebraic integers (when the field and its conjugates are real), the θ function $1 + 2x + 2x^4 + \cdots$ can be replaced by the θ series considered by Hecke. For example, in a quadratic field, the coefficient involves a double integral over the unit square. This square can be subdivided in a method similar to the ordinary Farey method into a number of small regions, and in each of these regions an approximate value is taken for the integrand, and the resulting integral again gives a genuine approximation.

11. *Laws of Reciprocity.* Finally the general laws of reciprocity in any field, i.e., the investigation of the congruence

$$x^n \equiv p \pmod{Q},$$

where Q is a given ideal, p a given algebraic integer, x an unknown algebraic integer, and n a given rational integer, are some of the most successful, abstruse, and far reaching results of the ideal theory, giving one a glimpse of regions so remote that apparently many years will elapse before our efforts will bring us within measurable distance.

First consider the congruence $x^2 \equiv q \pmod{p}$ in rational numbers, where p and q are odd primes. As factorization of $x^2 - q$ suggests $\sqrt{q}$, let us examine the meaning of this congruence in the field $K(\sqrt{q})$. If it is possible, it is equivalent to saying that the prime p factors in the field $K(\sqrt{q})$. By associating with any ideal a certain number of roots of unity, say $e_1, e_2, \cdots, e_k$, we can divide the ideal classes into genera; and conversely, if these units are given and satisfy an equation of consistency $e_1e_2 \cdots e_k = 1$, we can find a class of ideals

associated with the given units. Not only can we prove the law of quadratic reciprocity in this way, as was done by Kummer, but the ideas involved are so general that they have been extended by Hilbert and Furtwängler to the law of reciprocity in any field. Many new ideas, however, are involved in the proof, e.g., if $x^2 \equiv q \pmod{p}$ where now x, q are integers, and p is an ideal in the field $K(\theta)$, we have to investigate the properties of the algebraic field $K(\sqrt{q})$. It is of course obvious that $\sqrt{q}$ satisfies an equation of degree $2n$, but it is more convenient to consider it as a number satisfying a quadratic equation, the coefficients being integers in $K(\theta)$, so that $\sqrt{q}$ generates a quadratic field relative to the field $K(\theta)$. So it is more convenient to consider the ideals in the field $K(\sqrt{q})$ as quadratic ideals relative to the field $K(\theta)$. If the field $K(\theta)$ satisfies certain very special conditions, the study of the relative field $\sqrt{q}$ leads to the law of quadratic reciprocity in the field. All the laws of reciprocity, quadratic, cubic, etc., can be deduced when the proper relative field is known. This is a question of great difficulty and importance.

Great progress has been made arithmetically as far as the laws of reciprocity are concerned. In particular, the relative discriminant of these fields is unity and the relative Galois group is isomorphic with the group of the ideal classes in $K(\theta)$. Analytically, however, it has only been done in a few cases. The problem is equivalent to questions such as the following. Take the equation $x^p = 1$ where p is a prime. This is an abelian equation, i.e., all its roots are rationally represented in terms of one of them, e.g., ζ, ζ^2, ζ^3, ζ^4, $\cdots$, or, say, $f_1(\zeta)$, $f_2(\zeta), f_3(\zeta), \cdots$, and it is obvious that

$$f_a[f_b(\zeta)] = f_b[f_a(\zeta)].$$

Then there is a theorem which states that the root of any abelian equation whose coefficients are rational integers, can be expressed rationally with ordinary rational coefficients in terms of roots of unity. The next stage is that the roots of any abelian equation whose coefficients are imaginary quadratic integers in the field $K(\omega)$ can be expressed rationally in

terms of $j(\omega)$, where $j(\omega)$ is the well known modular function, that is, by means of the complex multiplication of elliptic functions.

Beyond this, however, we at present cannot go. But it is obvious what a field of research is suggested for the future.

Some of the relative fields are given by the equations in elliptic functions dealing with the subdivision of the periods, and also by the modular functions of several variables, an idea due to Hilbert, and developed by Blumenthal and Hecke and intimately connected with the θ function in the Riemann theory of algebraic functions.

The final law of reciprocity can be stated in all its generality in a remarkably simple form. For example, the law of quadratic reciprocity in any field $K(\theta)$ is equivalent to the theorem that the equation

$$ax^2 + by^2 + cz^2 = 0,$$

where a, b, c are given and x, y, z are unknown coprime integers in the field, is possible if and only if the congruence

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{P}$$

can be satisfied if P is any ideal in the field. A simple proof of this would of course lead to an easy arithmetical proof of the laws of reciprocity, and it is well worth the attention of mathematicians.

Finally, we may state that Siegel has made recently an interesting application of the law by showing that every algebraic integer can be expressed as the sum of 4 squares of algebraic numbers provided it is totally positive, that is, those of the conjugates that are real must be positive. Waring's theorem also has been extended to algebraic numbers.*

THE UNIVERSITY OF MANCHESTER, ENGLAND

* For references on this and other topics mentioned above, see the *Report on Algebraic Numbers*, BULLETIN OF THE NATIONAL RESEARCH COUNCIL, February, 1923; H. Bohr and H. Cramer, *Die neuere Entwickelung der analytischen Zahlentheorie*, ENCYKLOPÄDIE, II C 8; Hecke, *Vorlesungen über die Theorie der Algebraischen Zahlen*; Mordell, *Indeterminate equations of the third degree*, SCIENCE PROGRESS, July, 1923.