NOTE ON THE THEORY OF IDEALS

The following is a brief explanation of the theory of ideals of algebraic numbers* and functions and the relation in which the theory given in the preceding pages stands with respect to it.

Gauss (*Disquisitiones Arithmeticae* (1801)) was the first to consider the laws of factorisation in a domain of whole numbers other than that of rational whole numbers $0, \pm 1, \pm 2, \ldots$. He proved that two given complex whole numbers $a+b\sqrt{-1}$, $c+d\sqrt{-1}$ (a, b, c, d rational integers) have always an H.C.F. and that any such number is a unique product of prime factors. Kummer (*J. reine angew. Math.* 35 (1847), 40 (1850), 53 (1857)) in extending the research to a larger class of whole numbers found that these properties were no longer absolutely true. Nevertheless he succeeded in making such numbers amenable to all the simpler laws of rational integers by introducing certain *ideal numbers* not existing in the domain considered; and thus laid the foundation of the theory of factorisation of whole algebraic numbers. Finally Dedekind (D), by using *ideals* instead of ideal numbers, extended the theory to the whole numbers of any algebraic corpus and to whole algebraic functions of one variable (DW); while Kronecker (Kr) extended the same theory of factorisation to algebraic functions in general. Kronecker went still further; he gave the first steps of a *general* theory of ideals of algebraic functions (Kr, p. 77) under the name of *modular systems*. In this general theory factorisation plays only a subsidiary part, since an ideal which is not prime is not in general a product of prime ideals.

Modules of whole rational functions (as defined pp. 1, 2 above) are ideals and modules in the sense of Dedekind; and the theory of such modules is the necessary starting point of the general theory of ideals.

An *algebraic number* is any root α of an algebraic equation

$$a_0 x^m + a_1 x^{m-1} + \ldots + a_m = 0$$

* The following are notable general accounts of the theory of algebraic numbers:

D. Hilbert. "Bericht über die Theorie der algebraischen Zahlkörper" (*Jahresb. d. deutschen Math.-Verein.*, Berlin (1897), Bd. IV).

H. Weber. *Lehrbuch der Algebra* (Brunswick, 2nd ed. (1899), Bd. II, p. 553).

G. B. Mathews. "Number" (*Ency. Brit.*, Cambridge, 11th ed. (1911), Vol. 19, p. 847).

For other references to the arithmetic theory of algebraic numbers and functions see (D), (DW), (K), and (Kr), p. xiii.

in which the coefficients $a_0, a_1, \ldots, a_m$ are rational integers. We may suppose that a_0 is positive, and that $a_0, a_1, \ldots, a_m$ have no common factor other than 1, and that the equation is irreducible in the rational domain. There is only one set of values of $a_0, a_1, \ldots, a_m$ satisfying these conditions for an assigned α.

α is called a *whole* (algebraic) number if $a_0=1$, and is called a *fractional* number if $a_0 \neq 1$. Thus an algebraic (as well as a rational) number is integral or fractional, but cannot be both. In any case $a_0\alpha$ is a whole number β, and $\alpha=\beta/a_0$, i.e. the denominator of any fractional algebraic number α can be rationalized, while the numerator remains a whole algebraic number β.

All roots of any equation $x^m+c_1x^{m-1}+\ldots+c_n=0$ (whether reducible or not) in which $c_1, c_2, \ldots, c_n$ are rational integers are whole algebraic numbers. For all irreducible factors of the left-hand side are of the type

$$x^m+a_1x^{m-1}+\ldots+a_m.$$

We omit the proof of this as of most other properties to be stated. Hence any number is whole if it satisfies any equation of this type.

If $\alpha, \beta, \gamma, \ldots$ are whole numbers $\alpha\pm\beta$ and $\alpha\beta$ are also whole numbers (D, p. 145); and so also is any whole rational function of $\alpha, \beta, \gamma, \ldots$ with rational integral coefficients.

A whole number α is said to have another β as a factor, or to be divisible by β, if $\alpha=\beta\gamma$, where γ is a whole number.

A whole number ϵ is called a *unit* if it is a factor of 1; or ϵ is a unit if ϵ and $1/\epsilon$ are both whole numbers. Thus if in the above equation $a_0=\pm a_m=1$ all its roots are units.

Two whole numbers α, β are said to be *equivalent* (as regards divisibility) if $\alpha=\epsilon\beta$ where ϵ is a unit; for then any whole number which divides either α or β divides the other. Such equivalence of α, β is denoted by $\alpha\sim\beta$.

A *corpus* of algebraic numbers is the aggregate of all rational functions (with rational coefficients) of any finite set of given algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_k$. All numbers of the corpus are rational functions of a single element

$$\alpha=c_1\alpha_1+c_2\alpha_2+\ldots+c_k\alpha_k,$$

where $c_1, c_2, \ldots, c_k$ are rational integers so chosen as not to be connected by special relations.

The corpus generated by α is denoted by $\Omega(\alpha)$ and the aggregate of algebraic integers included in the corpus by $\omega(\alpha)$. The *order* of the corpus and of α is the degree of the irreducible equation of which α is a root.

Thus $\Omega(1)$ is the corpus of rational numbers and $\omega(1)$ the aggregate of rational integers.

Any rational function of any finite number of elements of $\Omega(\alpha)$ is an element of $\Omega(\alpha)$, and any whole rational function with rational integral coefficients of any finite number of elements of $\omega(\alpha)$ is an element of $\omega(\alpha)$.

Any corpus $\Omega(\alpha)$ includes $\Omega(1)$, for $\alpha/\alpha=1$.

If $a_0x^m+a_1x^{m-1}+\ldots+a_m=0$ is the irreducible equation of which the element α of the corpus $\Omega(\alpha)$ is a root, the other roots $\alpha', \alpha'', \ldots, \alpha^{(m-1)}$ are

called the *conjugates* of a, and $\Omega(a'), \ldots, \Omega(a^{(m-1)})$ the conjugates of $\Omega(a)$. If a' is an element of $\Omega(a)$ then $\Omega(a')$ is the same as $\Omega(a)$, and if not, not. The corpus generated by $a, a', \ldots, a^{(m-1)}$ is called the Galoisian domain corresponding to $\Omega(a)$. The conjugates of any number $\beta = f(a)$ of $\Omega(a)$ are

$$\beta' = f(a'), \ldots, \beta^{(m-1)} = f(a^{(m-1)}).$$

The product $\beta\beta' \ldots \beta^{(m-1)}$ is a rational number (being a symmetric function of $a, a', \ldots, a^{(m-1)}$) and is called the *norm* of β and written norm β.

Since β and norm β are both numbers in $\Omega(a)$, norm β/β is a number in $\Omega(a)$. Moreover if β is a number in $\omega(a)$, then $\beta', \ldots, \beta^{(m-1)}$ are whole algebraic numbers, and norm β/β is a number in $\omega(a)$. If β is a unit, $\beta', \beta'', \ldots, \beta^{(m-1)}$ are all algebraic units, and norm $\beta = \pm 1$. Conversely, if β is a number in $\omega(a)$ such that norm $\beta = \pm 1$, β is a unit in $\omega(a)$. Norm $(au + \beta v + \ldots)$ is defined as $\prod_{i=0}^{m-1} (a^{(i)}u + \beta^{(i)}v + \ldots)$, $u, v, \ldots$ being indeterminates.

$\Omega(a)$ is a domain of rationality. $\omega(a)$ is called a *proper holoid* domain (König), that is, a domain in which every sum, difference and product, but not every quotient, of two elements is an element of the domain. A proper holoid domain in which every pair of elements a, β have an H. C. F. in the domain (defined as a factor δ of a and of β such that every common factor of a, β is a factor of δ) is called a *complete* holoid domain. $\omega(a)$ is not necessarily *complete*.

The simplest example of this last statement is the domain $\omega(\sqrt{-5})$ which is fully discussed by Dedekind (D, p. 73). If $x = a + b\sqrt{-5}$ (a, b rational) then $(x-a)^2 + 5b^2 = 0$, and in order that x may be whole $2a$ and $a^2 + 5b^2$ must be rational integers, i.e. a and b must be integers. Consider the two whole numbers $9, 3(1+\sqrt{-5})$. If these have an H. C. F. in $\omega(\sqrt{-5})$ it must be 3δ, where δ is a whole number in $\omega(\sqrt{-5})$ which divides 3 and $1+\sqrt{-5}$. But 3 and $1+\sqrt{-5}$ are non-factorisable in $\omega(\sqrt{-5})$; hence $\delta = 1$. Hence the H. C. F. (if any) of $9, 3(1+\sqrt{-5})$ is 3; but $2-\sqrt{-5}$ is a factor of 9 and $3(1+\sqrt{-5})$ and is not a factor of 3. Hence there is no H. C. F., and $\omega(\sqrt{-5})$ is not *complete*. That 3 is not factorisable in $\omega(\sqrt{-5})$ is shown by putting $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ from which it follows that

$$9 = (a^2+5b^2)(c^2+5d^2)$$

and that one of a^2+5b^2, c^2+5d^2 is 9 and the other 1, since neither can be 3. Also if $a^2+5b^2 = 9$ the only solutions are $a = \pm 3$, $b = 0$ and $a = \pm 2$, $b = \pm 1$ of which the latter must be rejected since $\pm 2 \pm \sqrt{-5}$ does not divide 3. Similarly for $1+\sqrt{-5}$. The numbers $3, 1+\sqrt{-5}$ have however a common factor $(1+\sqrt{-5})/\sqrt{2}$ or $\sqrt{-2+\sqrt{-5}}$ not in $\omega(\sqrt{-5})$.

Another point requiring notice is the distinction between a non-factorisable number and a prime number. A non-factorisable number in $\omega(a)$ is one which has no other factors in $\omega(a)$ than such as are equivalent to

itself or 1. A prime number is one which cannot be a factor of a product $\beta\gamma$ without being a factor of β or of γ. Thus 3 and $1+\sqrt{-5}$ are both non-factorisable in $\omega(\sqrt{-5})$, but neither of them is prime; 3 is a factor of $(1+\sqrt{-5})(1-\sqrt{-5})$ but not a factor of $1+\sqrt{-5}$ or $1-\sqrt{-5}$; and $1+\sqrt{-5}$ is a factor of 6 but not a factor of 2 or 3.

In a complete holoid domain every non-factorisable element is prime and every prime element is non-factorisable (K, p. 15).

Let π be any element of the domain which is non-factorisable, and let $\alpha\beta$ be divisible by π and β not divisible by π. Then the H.C.F. of β, π ~ 1; H.C.F. of $\alpha\beta$, $\alpha\pi \sim \alpha$; H.C.F. of $\alpha\beta$, $\pi \sim$ H.C.F. of $\alpha\beta$, $\alpha\pi$, $\pi \sim$ H.C.F. of α, π; i.e. H.C.F. of α, $\pi \sim \pi$, or α is divisible by π; hence π is prime. Again if π is prime and equal to $\pi_1\pi_2$, one of π_1, π_2 is divisible by π and the other is a unit; hence π is non-factorisable.

It is to be noticed that the proof depends only on the notions of product, quotient, and H.C.F., and is therefore applicable to any domain in which each pair of elements α, β has a product $\alpha\beta$, and an H.C.F. δ (defined as above), and may or may not have a quotient γ, defined by $\alpha=\beta\gamma$.

In a complete holoid domain any element which is not an infinite product of factors (not counting unit factors) is a unique product of prime factors if equivalent factors are regarded as the same factor.

For any element which is not prime is a product of two factors neither of which is a unit; each of these again if not prime is a product of two factors, and so on. Hence any element which is not an infinite product is a product of prime factors $p_1^{l_1}p_2^{l_2}\dots p_r^{l_r}$. This resolution into factors is unique in the sense of equivalence; for if $p_1^{l_1}\dots p_r^{l_r} \sim q_1^{m_1}\dots q_s^{m_s}$, where $q_1, q_2, \dots, q_s$ are primes and none of them units, p_1 must be a factor of q_1 or q_2 ... or q_s, and if a factor of q_1, then $p_1 \sim q_1$; from which the rest follows.

The domain of all algebraic integers is a complete holoid domain (D, p. 247) but contains no prime numbers, since any number α has an infinite number of factors, e.g. $\sqrt[n]{\alpha}$. This property of completeness is peculiar to numbers; it does not hold for functions, not even for relatively whole algebraic functions of a single variable.

No number in $\omega(\alpha)$ can be an infinite product, for otherwise its norm, which is a rational integer, would be an infinite product of rational integers. Hence if $\omega(\alpha)$ is complete each number in it is a unique product of prime factors.

All the above remarks concerning algebraic numbers (with the exception noted) apply *mutatis mutandis* to algebraic functions. The only difference is that there are two kinds of whole algebraic functions, relative and absolute.

An *algebraic function* is any quantity α which satisfies an algebraic equation

$$A_0 z^m + A_1 z^{m-1} + \dots + A_m = 0$$

in which the coefficients $A_0, A_1, \dots, A_m$ are whole rational functions of n variables $x_1, x_2, \dots, x_n$.

a is called a *relatively whole* (algebraic) function if A_0 does not involve the variables. In this case the numerical coefficients of $A_1, A_2, \ldots, A_m$ may be any real or complex numbers, whether algebraic or not. Moreover z is whole relatively to $x_1, x_2, \ldots, x_r$ if A_0 involves $x_{r+1}, \ldots, x_n$ only.

a is called an *absolutely whole* (algebraic) function if $A_0=1$ and the numerical coefficients of $A_1, A_2, \ldots, A_m$ are rational integers.

In the case of functions $\Omega(1)$ is the corpus of rational functions, and $\omega(1)$ the aggregate of whole rational functions.

In still continuing to speak of algebraic numbers it will be understood that what is said applies equally to algebraic functions. In considering the properties of algebraic numbers we naturally regard the numbers of a corpus $\Omega(a)$ and the domain $\omega(a)$ included in it as the principal subject of investigation, since these answer the most nearly to the numbers of $\Omega(1)$ and $\omega(1)$.

$\Omega(a)$ and more especially $\omega(a)$ are further subdivided. Dedekind defines a *module* in $\Omega(a)$ to be the aggregate of all numbers (or functions)

$$a_1\alpha_1+a_2\alpha_2+a_3\alpha_3+\ldots,$$

where $a_1, a_2, \ldots$ are fixed elements of $\Omega(a)$ and $\alpha_1, \alpha_2, \ldots$ any elements of $\omega(1)$, that is, rational integers in the case of number modules and whole rational functions (relative or absolute) in the case of function modules. If $\alpha_1, \alpha_2, \ldots$ are whole numbers, that is, elements of $\omega(a)$ instead of $\Omega(a)$, the module is a module of whole numbers. Any module of whole numbers (or functions) has a finite basis $(\mu_1, \mu_2, \ldots, \mu_k)$; and any module of fractions with a finite basis $(a_1, a_2, \ldots, a_k)$ is practically the same thing as a module of whole numbers, since $a_1, a_2, \ldots, a_k$ can be multiplied by a rational integer a so as to become whole numbers $\mu_1, \mu_2, \ldots, \mu_k$, and then any element of the module $(a_1, a_2, \ldots, a_k)$ is equal to the corresponding element of the module $(\mu_1, \mu_2, \ldots, \mu_k)$ divided by a. There are modules of fractions with infinite bases; but they seem to be unimportant, and it would be simpler to restrict the meaning of the term module to a module of whole numbers or functions. A *module* would then be defined as any aggregate of elements of $\omega(a)$ such that if a_1, a_2 are any two elements of the module, a_1+a_2 and αa_1 are also elements of the module, where α is any element of $\omega(1)$.

An *involution* of whole functions is any aggregate of elements of $\omega(a)$ such that if a_1, a_2 are any two elements of the involution, a_1+a_2 and ca_1 are also elements of the involution, where c is any constant. In the absolute theory the elements of $\omega(a)$ are absolutely whole functions and c a rational integer.

Dedekind's definition of an *ideal* is similar but still more fundamental. An ideal is any aggregate of elements of $\omega(a)$ such that if a_1, a_2 are any two elements of the ideal, a_1+a_2 and μa_1 are also elements of the ideal, where μ is any element of $\omega(a)$. Every ideal has a finite basis $(a_1, a_2, \ldots, a_k)$ and is a finite module $(a_1, a_2, \ldots, a_l)$; but not every module of whole numbers or functions is an ideal. In the domain of whole rational functions an ideal and a module are identical.

Kummer had found that the integers of a corpus did not necessarily satisfy all the simple laws of rational integers, or in other words they need not form a complete holoid domain. It occurred to Dedekind (and apparently independently to Kronecker) to consider in this case not the individual integers of a corpus only but sets of integers. For this purpose Dedekind made use of the ideals already defined. We shall in the first place consider ideals from a rather abstract point of view. The remarks apply also to some extent to modules and involutions.

The aggregate of elements of an ideal $(a_1, a_2, \ldots, a_k)$ constitutes an image of the properties possessed in common by all the elements of the aggregate, and especially of properties of divisibility (if any) common to $a_1, a_2, \ldots, a_k$. The term *ideal* should strictly be applied to these properties common to all the elements, whatever they may be; but it is more convenient and concise to define the ideal as the aggregate of elements itself. This point of view, viz. that the ideal is a set of properties rather than a set of numbers or functions, is the justification for saying that each element of the ideal contains or is divisible by the ideal, since it possesses all the properties in question. Kronecker makes use of another image, in some respects simpler, viz., $a_1u_1 + a_2u_2 + \ldots + a_ku_k$ or $a_1 + a_2u + \ldots + a_ku^{k-1}$, where $u, u_1, u_2, \ldots, u_k$ are indeterminates. This is not called an *ideal* because the term had already been appropriated by Dedekind with a different meaning, but it takes the place of Dedekind's ideal.

Thus at the outset we can form a natural conception of what should be meant by saying that an ideal $(a_1, a_2, \ldots, a_k)$ contains or is divisible by another $(\beta_1, \beta_2, \ldots, \beta_l)$. The conditions should be that each of $a_1, a_2, \ldots, a_k$ is an element of $(\beta_1, \beta_2, \ldots, \beta_l)$; for all elements of $(a_1, a_2, \ldots, a_k)$ will then possess all the properties possessed in common by all the elements of $(\beta_1, \beta_2, \ldots, \beta_l)$, and this apart from the fact that we may be unable to state explicitly what these properties are.

Again we can give a natural meaning to the G.C.M. and the L.C.M. of two ideals. The G.C.M. or H.C.F. of $(a_1, a_2, \ldots, a_k)$ and $(\beta_1, \beta_2, \ldots, \beta_l)$ should be an ideal $(\gamma_1, \gamma_2, \ldots)$ contained in both such that every ideal contained in both is contained in $(\gamma_1, \gamma_2, \ldots)$. There is one and only one such ideal, viz. the ideal $(a_1, a_2, \ldots, a_k, \beta_1, \beta_2, \ldots, \beta_l)$, cf. § 23. The L.C.M. should be an ideal $(\gamma_1, \gamma_2, \ldots)$ which contains both and such that every ideal which contains both contains $(\gamma_1, \gamma_2, \ldots)$. Again there is one and only one such ideal, viz. the ideal whose elements consist of all elements of $\omega(a)$ containing both $(a_1, a_2, \ldots, a_k)$ and $(\beta_1, \beta_2, \ldots, \beta_l)$. These elements constitute an ideal by definition.

But the crux lies in the difficulty of attaching a natural meaning to the term *product*. The product of two ideals should be an ideal whose properties consist of the product of the properties of the two ideals, and to this *product of properties* we cannot attach a meaning *a priori* from the definition of an ideal. Moreover the aggregate of the products of any element of $(a_1, a_2, \ldots, a_k)$ and any element of $(\beta_1, \beta_2, \ldots, \beta_l)$ does not constitute an ideal. The best that can be done is therefore to define the product of these two ideals to be the

ideal $(\ldots, a_i\beta_j, \ldots)$, $i=1, 2, \ldots, k$, $j=1, 2, \ldots, l$. This ideal includes all products $a\beta$ of elements of the two ideals, and in addition all sums of such products. It could not be told beforehand to what a theory based on so tentative a definition might lead.

We may say that the fact of an ideal containing another is a case of true divisibility if it always follows as a necessary consequence that the first is the product of the second and a third ideal (the converse being true by definition). This is exactly what Dedekind proved to be the case for all ideals of algebraic numbers and relatively whole algebraic functions of one variable, but only by means of a long series of subsidiary theorems. It followed that any such ideal could be uniquely expressed as a product of prime ideals. We know however that this is not true for ideals of functions of more than one variable, since it is not true for modules of rational functions. Also it is not true for ideals of absolutely whole algebraic functions of one variable; e.g. (x) contains $(x, 2)$* but is not the product of $(x, 2)$ and a third ideal; for the residual $(x)/(x, 2)$ is (x), and (x) is not the product of $(x, 2)$ and (x).

Kronecker's theory (Kr) concerns whole algebraic functions in general, and one of its remarkable features is that it applies to absolutely whole as well as to relatively whole functions. The absolute theory is based on the following fundamental theorem, which is proved by König (K, p. 78):

If $f_1, f_2, \ldots, f_k$ are any k polynomials in $u_1, u_2, \ldots$, Π any product of coefficients of $f_1, f_2, \ldots, f_k$ taken one from each, and $\Pi_1, \Pi_2, \ldots$ the coefficients of the polynomial $f_1 f_2 \ldots f_k$; then Π satisfies identically an equation of the type

$$\Pi^\rho + \Pi^{(1)}\Pi^{\rho-1} + \Pi^{(2)}\Pi^{\rho-2} + \ldots + \Pi^{(\rho)} = 0,$$

where $\Pi^{(i)}$ is a homogeneous polynomial of degree i $(i=1, 2, \ldots, \rho)$ in $\Pi_1, \Pi_2, \ldots$ with rational integral coefficients.

Kronecker gives the theorem in the second of the two memoirs referred to in (Kr), having discovered it after the first memoir was written. He states it for two polynomials f_1, f_2 in a single letter u or x. König gives the theorem in the more general form above. It is not generally necessary to introduce more than one letter or indeterminate u. If we suppose $f_1, f_2, \ldots, f_k$ to be polynomials of degrees $l_1, l_2, \ldots, l_k$ in a single letter u the number of the quantities Π is $(l_1+1)(l_2+1)\ldots(l_k+1)$, while the number of the quantities $\Pi_1, \Pi_2, \ldots$ (which are sums of the quantities Π) is only $l_1+l_2+\ldots+l_k+1$; and†

$$\rho = \frac{(l_1+l_2+\ldots+l_k)!}{l_1!\, l_2!\ldots l_k!}.$$

* In the relative theory $(x, 2)=(1)$, but not in the absolute theory. In the absolute theory a module in n variables can be of rank $n+1$ (cf. § 47); such in fact is any module which has some rational integer (but not unity) as a member, or any module which has no spread and is not (1). In both the absolute and relative theories the non-proper module (1) is without rank.

† The value found for ρ by König for the case $k=2$ is $(l_1+l_2+1)!/l_1!(l_2+1)!$, which is not symmetrical in l_1, l_2. It can be proved that ρ need not be greater

Let the coefficients of $f_1, f_2, \ldots, f_k$ be absolutely or relatively whole algebraic functions of n variables $x_1, x_2, \ldots, x_n$. These all belong to and determine a corpus of functions. Let $M_1, M_2, \ldots, M_k$ be the ideals determined by the coefficients of $f_1, f_2, \ldots, f_k$ respectively, and M the ideal $(\Pi_1, \Pi_2, \ldots)$ determined by the coefficients of $f_1 f_2 \ldots f_k$. Then Π is any element of the basis of the ideal $M_1 M_2 \ldots M_k$, and $\Pi^{(i)}$ is an element of the ideal M^i (and of the involution M^i).

Kronecker says that a quantity Π which identically satisfies an equation of the above type (where $\Pi^{(i)}$ is any element of the i^{th} power of a given ideal M) *contains M in the wider sense* of the word. Π contains *M in the strict sense* if it is an element of M, i.e. if it satisfies a *linear* identity of the above type. One ideal contains another (in the wider sense) if each element of (the basis of) the first contains the second (in the wider sense); and if each of two ideals M, M' contains the other (in the wider sense) M, M' are said to be equivalent in the wider sense. We denote such equivalence by $M \sim M'$, having already denoted strict equivalence by $M = M'$. Kronecker also remarks that (in the wider sense) if M contains M' and M' contains M'' then M contains M''. Consequently if $M \sim M'$ and $M \sim M''$ then $M' \sim M''$. *If $M, M_1, M_2, \ldots, M_k$ have the meanings given to them above we have $M \sim M_1 M_2 \ldots M_k$.*

This conception of wider equivalence is of considerable importance, and is specially applicable to Kronecker's theory. To any ideal M of a given corpus of functions there corresponds a unique *closed* equivalent ideal M_0 within the corpus. The elements of M_0 consist of all whole functions Π of the corpus which satisfy identically an equation of the type

$$\Pi^\rho + \Pi^{(1)} \Pi^{\rho-1} + \Pi^{(2)} \Pi^{\rho-2} + \ldots + \Pi^{(\rho)} = 0,$$

where $\Pi^{(i)}$ is an element of M^i. Any Π which satisfies identically an equation

$$\Pi^\sigma + \Pi_0^{(1)} \Pi^{\sigma-1} + \Pi_0^{(2)} \Pi^{\sigma-2} + \ldots + \Pi_0^{(\sigma)} = 0,$$

where $\Pi_0^{(i)}$ is an element of M_0^i, satisfies a linear identity of the same type and is an element of M_0. All ideals in the corpus equivalent to M are equivalent to M_0. A closed ideal may have relevant imbedded spreads; the closed module $(x_1^2, x_1 x_2)$ is an example.

If (speaking in the wider sense) M' contains M'' then MM' contains MM'', and conversely if MM' contains MM'' then M' contains M''; consequently if $MM' \sim MM''$ then $M' \sim M''$.

This theorem is not true for strict (or linear) equivalence, i.e. if $MM' = MM''$ it does not follow that $M' = M''$ (see § 24, Ex. i) unless M is an unmixed ideal of rank 1 (defined below).

than the smaller value given above, while for some of the products Π the value of ρ is less. In the cases of the first and last product Π it is evident that $\rho = 1$. If $l_1 = l_2 = 2$, ρ is 3 for the middle product Π, and 6 for the others, except the first and last.

Let $M=(a_1, a_2, \ldots, a_k)$, $M'=(a_1', a_2', \ldots, a'k')$, $M''=(a_1'', a_2'', \ldots, a''k'')$.

Then if M' contains M'' each element a' of the basis of M' satisfies an identity

$$a'^{\rho}+a^{(1)}a'^{\rho-1}+a^{(2)}a'^{\rho-2}+\ldots+a^{(\rho)}=0,$$

where $a^{(i)}$ is an element of M''^i, i.e. a homogeneous polynomial in $a_1'', a_2'', \ldots, a''_{k''}$ of degree i with whole functions of the corpus for coefficients. Putting $a'a_j=a$ we have

$$a^{\rho}+a^{(1)}a_j a^{\rho-1}+a^{(2)}a_j^2 a^{\rho-2}+\ldots+a^{(\rho)}a_j^{\rho}=0,$$

where $a^{(i)}a_j^i$ is an element of $(MM'')^i$; hence a contains MM'', i.e. MM' contains MM''. Conversely, given that MM' contains MM'', $a'a_j$ contains MM'' where a' is any element of M', i.e. we have an identity

$$(a'a_j)^{\rho_j}+\beta_j^{(1)}(a'a_j)^{\rho_j-1}+\beta_j^{(2)}(a'a_j)^{\rho_j-2}+\ldots+\beta_j^{(\rho_j)}=0,$$

where $\beta_j^{(i)}$ is an element of $(MM'')^i=(a_1, a_2, \ldots, a_k)^i\,(a_1'', a_2'', \ldots, a''_{k''})^i$. Hence this identity is homogeneous and of degree ρ_j in $a_1, a_2, \ldots, a_k$, and arranging it in power products of these, each coefficient is homogeneous and of degree ρ_j in $a', a_1'', a_2'', \ldots, a''_{k''}$. There are k such equations for the same a', viz. when $j=1, 2, \ldots, k$. The resultant of the k equations with respect to $a_1, a_2, \ldots, a_k$ is a homogeneous equation in $a', a_1'', a_2'', \ldots, a''_{k''}$ of degree $k\rho_1\rho_2\ldots\rho_k$, since it is homogeneous and of degree $\rho_1\rho_2\ldots\rho_k/\rho_j$ in the coefficients of the j^{th} equation. Also since the resultant is homogeneous in $a', a_1'', a_2'', \ldots, a''_{k''}$, and is found by a purely algebraical process, we can find the coefficient of $a'^{k\rho_1\rho_2\ldots\rho_k}$ in it by supposing all of $a_1'', a_2'', \ldots, a''_{k''}$ to be zeros. The resultant then becomes the resultant of $(a'a_1)^{\rho_1}, (a'a_2)^{\rho_2}, \ldots, (a'a_k)^{\rho_k}$, viz. $a'^{k\rho_1\rho_2\ldots\rho_k}$. The coefficient of this term is therefore 1. Hence a' contains M'', i.e. M' contains M''.

The above properties are true not only for ideals but also for modules and for involutions whether of absolutely whole or relatively whole algebraic functions.

Kronecker's way of considering a set of whole algebraic quantities $a_0, a_1, \ldots, a_l$ (numbers or functions) is more direct than Dedekind's. He sets them in a frame or form*

$$a_u=a_0+a_1u+a_2u^2+\ldots+a_lu^l,$$

where u is an indeterminate. Instead of power products of one indeterminate u we could use l indeterminates $u_1, u_2, \ldots, u_l$ or power products of any less

* We use the term *form* here and later as meaning a *representation* which is not a function but is subject to algebraic laws and operations. The form becomes a function of u if u is regarded as a variable or parameter.

The notation a_u for a form is copied from König; and the notation for an ideal $M=(a_0, a_1, \ldots, a_l)$ is the same as that used in the text for a module. Kronecker's notation is quite different; e.g. he uses M for an element which is denoted above by a, and the term modular system as equivalent to divisor system or basis.

number. The indeterminates serve merely to separate the quantities $a_0, a_1, \ldots, a_l$. Kronecker then expands norm a_u in powers of u, viz.

$$\begin{aligned}\text{norm } a_u &= (a_0 + a_1 u + \ldots + a_l u^l)(a_0' + a_1' u + \ldots + a_l' u^l)\ldots \\ &\qquad \ldots (a_0^{(m-1)} + a_1^{(m-1)} u + \ldots + a_l^{(m-1)} u^l) \\ &= F_0 + F_1 u + F_2 u^2 + \ldots + F_k u^k \qquad (k = lm),\end{aligned}$$

where $F_0, F_1, \ldots, F_k$ are whole rational functions of $x_1, x_2, \ldots, x_n$.

If $F_0, F_1, \ldots, F_k$ have an H.C.F. D, which may be a rational integer only, or a whole rational function of $x_1, x_2, \ldots, x_n$, then, having regard to the fact that norm a_u is the product of the above factors, we may say that $a_0, a_1, \ldots, a_l$ have something in common of the nature of a factor, which may be called their ideal common factor, and may be represented by the form a_u. So long as this factor D, which is the complete partial resolvent of rank 1 of the module $(F_0, F_1, \ldots, F_k)$, is only taken into account, while the partial resolvents of higher rank are neglected, Kronecker's theory is a theory of factorisation only.

Dedekind had established a theory of factorisation of whole algebraic numbers, which he subsequently extended to relatively whole algebraic functions of one variable. Considering that the factorisation of whole rational functions is exactly parallel to that of whole rational numbers the question naturally arises whether the factorisation of whole algebraic functions is parallel to that of whole algebraic numbers. Kronecker proved that it was absolutely parallel.

Kronecker says that a_u and norm a_u are *primitive* or *unit* forms if $D=1$. This is legitimate in a theory of factorisation. Later he says that they are properly primitive only if the module* $(F_0, F_1, \ldots, F_k)=(1)$. If $D \neq 1$ then norm a_u/D is a unit form. Kronecker names $a_u/(\text{norm } a_u/D)$ an "algebraic modulus or divisor," which may be interpreted, an "equivalent of a_u" in respect to divisibility and factorisation. König names a_u/ϵ_u, where ϵ_u is any unit form in $\omega(a)$, an *ideal whole quantity* of $\omega(a)$; and accepts the rather absurd paradox that the sum of two such quantities is their H.C.F. It would be preferable to name a_u/ϵ_u an *ideal whole form*. He proves that such ideal forms can be uniquely resolved (in the sense of equivalence) into products of prime ideal forms, and shows how for a given form the prime factors can be actually found.

To compare two forms a_u and a_u' Kronecker considers the fraction a_u'/a_u and rationalizes the denominator by multiplying numerator and denominator by norm a_u/a_u, which is a (strictly) whole form in $\omega(a)$. If the new numerator a_u' norm a_u/a_u is divisible by the D of the new denominator norm a_u then the form a_u' is said to be divisible by the form a_u. If further the quotient of

* The module $(F_0, F_1, \ldots, F_k)$ is the aggregate of all whole rational functions $A_0F_0 + A_1F_1 + \ldots + A_kF_k$, and the ideal $(F_0, F_1, \ldots, F_k)$ in the domain $\omega(a)$ is the aggregate of all functions $\beta_0F_0 + \beta_1F_1 + \ldots + \beta_kF_k$, where $\beta_0, \beta_1, \ldots, \beta_k$ are elements of $\omega(a)$.

a_u' norm a_u/a_u by D is a unit form, then $a_u'/a_u=\epsilon_u'/\epsilon_u$, where ϵ_u, ϵ_u' are both unit forms, and the ideal forms a_u, a_u' are equivalent as regards divisibility. The divisibility of a_u' by a_u is the same thing as the divisibility of the ideal $(a_0', a_1', \ldots, a_{l'}')$ by the ideal $(a_0, a_1, \ldots, a_l)$ in the case of algebraic numbers and relatively whole algebraic functions of one variable; but not in other cases. This, as we show below, is a consequence of the fact that in these two cases $(F_0, F_1, \ldots, F_k)=(D)$.

Let M be the ideal $(a_0, a_1, \ldots, a_l)$, and, as before, let

$$\text{norm } a_u=F_0+F_1u+\ldots+F_ku^k \qquad (k=lm).$$

Then, in the Galoisian domain $\Omega(a, a', \ldots, a^{(m-1)})$, the ideal $(F_0, F_1, \ldots, F_k)$ is equivalent to the product of M and its conjugates M', M'', $\ldots$, $M^{(m-1)}$, by the fundamental theorem; and another ideal $(F_0', F_1', \ldots, F'_{k'})$ obtained in a similar way from any other basis of M is equivalent to $(F_0, F_1, \ldots, F_k)$, i.e. a homogeneous equation of degree ρ exists between F_i', F_0, F_1, $\ldots$, F_k, in which the coefficient of $F_i'^{\rho}$ is 1, and the other coefficients are whole elements of the Galoisian domain. By rationalizing the equation it follows that the *modules* $(F_0, F_1, \ldots, F_k)$, $(F_0', F_1', \ldots, F'_{k'})$ are equivalent. Hence we may define the rank of the ideal M and of the form a_u to be the rank of the module $(F_0, F_1, \ldots, F_k)$. We may also say that the ideal M is unmixed in the wider sense if the closed module equivalent to $(F_0, F_1, \ldots, F_k)$ is unmixed.

A *principal ideal* is an ideal (β) having a basis consisting of a single element β.

It can be proved without difficulty that *the only ideal in a given corpus* $\Omega(a)$ *equivalent to a principal ideal* (β) *is the ideal* (β) *itself.*

The ideal M above is called an *unmixed ideal of rank* 1 if $(F_0, F_1, \ldots, F_k)$ is a principal ideal, i.e. if $(F_0, F_1, \ldots, F_k)=(D)+(1)$.

Suppose now that $M=(a_0, a_1, \ldots, a_l)$ is an unmixed ideal of rank 1, and that the form a_u' is divisible by a_u in the sense defined above. Then, putting

$$\frac{\text{norm } a_u}{a_u}=\beta_0+\beta_1u+\ldots+\beta_{k-l}u^{k-l},$$

we are given that $(a_0'+a_1'u+\ldots+a_{l'}'u^{l'})(\beta_0+\beta_1u+\ldots+\beta_{k-l}u^{k-l})$ is divisible by D. Hence $a_i'\beta_j$ is divisible by D, i.e. $a_i'\beta_j=D\beta_{ij}$. Hence

$$a_i'(\beta_0+\beta_1u+\ldots+\beta_{k-l}u^{k-l})=D(\beta_{i0}+\beta_{i1}u+\ldots+\beta_{i,\,k-l}u^{k-l}).$$

Multiplying by a_u, and putting $F_i=D\phi_i$, we have

$$a_i'(\phi_0+\phi_1u+\ldots+\phi_ku^l)=(\beta_{i0}+\beta_{i1}u+\ldots+\beta_{i,\,k-l}u^{k-l})(a_0+a_1u+\ldots+a_lu^l).$$

Hence $(\beta_{i0}, \beta_{i1}, \ldots, \beta_{i,\,k-l})(a_0, a_1, \ldots, a_l)\sim(a_i')(\phi_0, \phi_1, \ldots, \phi_k)=(a_i')$, since $(\phi_0, \phi_1, \ldots, \phi_k)=(1)$, and (a_i') is a principal ideal. Hence

$$(a_0', a_1', \ldots, a_{l'}')=(\ldots, \beta_{ij}, \ldots)(a_0, a_1, \ldots, a_l) \quad (i=0, 1, \ldots, l', j=0, 1, \ldots, k-l).$$

Conversely, if an ideal $(a_0', a_1', \ldots, a_{l'}')$ contains an ideal $(a_0, a_1, \ldots, a_l)$ the form a_u' is divisible by the form a_u, since a_i norm a_u/a_u, and therefore also a_j' norm a_u/a_u, is divisible by D.

Hence an ideal $(a_0', a_1', \ldots, a_{l'}')$ *which contains an unmixed ideal* $(a_0, a_1, \ldots, a_l)$ *of rank* 1 *is the product of* $(a_0, a_1, \ldots, a_l)$ *and a third ideal* $(\ldots, \beta_{ij}, \ldots)$, *i.e. it has* $(a_0, a_1, \ldots, a_l)$ *as a true factor.* This includes Dedekind's principal result, since all ideals considered by him are unmixed ideals of rank 1. If the ideal $(a_0', a_1', \ldots, a_{l'}')$ is also unmixed the quotient $(\ldots, \beta_{ij}, \ldots)$ is also unmixed. Hence there exists a theory of factorisation for the whole aggregate of unmixed ideals of rank 1 in a corpus $\Omega(a)$.

It follows that an unmixed ideal $(a_0, a_1, \ldots, a_l)$ *of rank* 1 *can be multiplied by a second unmixed ideal of rank* 1 *so as to become the principal ideal* (β), *where* β *is any element of* $(a_0, a_1, \ldots, a_l)$.

If it be true that any ideal of rank 1 must contain an unmixed ideal of rank 1, which is obvious in the two cases considered by Dedekind, but has not been proved in general so far as I know, then *any unmixed ideal of rank* 1 *is a unique product of unmixed prime ideals of rank* 1. For, assuming the truth of the hypothesis, it can be shown that any two given unmixed ideals M, M' of rank 1 which have a common factor must have an H.C.F., viz. the unmixed ideal M'' of rank 1 such that $(M, M') = M''M'''$, where M''' is either (1) or of rank > 1. It can be easily proved that the ideals M'', M''' thus defined are unique, and that any unmixed ideal of rank 1 which is a factor of M and of M' is a factor of M''; hence M'' is the H.C.F. of M and M'. In the cases considered by Dedekind (M, M') is itself an unmixed ideal of rank 1, and $M'' = (M, M')$. I cannot say whether this resolution into prime factors is exactly what is meant by Kronecker in his statement XIII, p. 89; and I cannot attach any true meaning to the parallel statement XIII°, p. 92, regarded as an extension of XIII.

Kronecker also considers another kind of divisibility of a form a_u' by a form a_u, which is more adaptable to the *general* theory of ideals. A form a_u' might be defined as divisible by a_u if the ideal $M' = (a_0', a_1', \ldots, a_{l'}')$ contains the ideal $M = (a_0, a_1, \ldots, a_l)$ in the strict sense. This definition is open to the objection that $a_u'\beta_u$ could be divisible by $a_u\beta_u$ without a_u' being divisible by a_u. The objection disappears when a wider definition is taken, viz. that a_u' is divisible by a_u if M' contains M in the wider sense.

The necessary and sufficient condition that any given ideal

$$M' = (a_0', a_1', \ldots, a_{l'}')$$

may contain any other given ideal $M = (a_0, a_1, \ldots, a_l)$ in the wider sense is that the ideal corresponding to a_u' norm a_u/a_u contains the ideal $(F_0, F_1, \ldots, F_k)$ corresponding to norm a_u in the wider sense, *which is the same thing* as containing the module $(F_0, F_1, \ldots, F_k)$ in the wider sense. In other words, it is necessary and sufficient that each of the $k - l + l' + 1$ coefficients a'' of the form a_u' norm a_u/a_u should satisfy identically an equation of some degree ρ which is homogeneous in $a'', F_0, F_1, \ldots, F_k$, the coefficient of a''^{ρ} being 1, and the other coefficients whole rational functions.

CAMBRIDGE: PRINTED BY J. B. PEACE, M.A. AT THE UNIVERSITY PRESS