Springer

The Genesis of Ideal Theory
Author(s): Harold M. Edwards
Source: *Archive for History of Exact Sciences*, Vol. 23, No. 4 (31.XII.1980), pp. 321-378
Published by: Springer
Stable URL: https://www.jstor.org/stable/41133600
Accessed: 27-07-2018 22:02 UTC

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

JSTOR

Springer is collaborating with JSTOR to digitize, preserve and extend access to *Archive for History of Exact Sciences*

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

The Genesis of Ideal Theory

HAROLD M. EDWARDS

Communicated by M. KLINE

1. Introduction

This paper deals with the development of the theory of ideal factorization of algebraic integers, from the first discovery of KUMMER that such a theory is necessary and possible in the case of the cyclotomic integers to the final general theories of DEDEKIND and KRONECKER. DEDEKIND's theory used what he called "ideals" while KRONECKER used "divisors"; the title of the paper could as well have been "The Genesis of Divisor Theory" – and in fact I would prefer to use this name – but the name "ideal theory" will probably be familiar to more readers. It is assumed that the reader has some general background in modern algebra – groups, rings, and fields – but not necessarily any knowledge of algebraic number theory.

As DEDEKIND said (see Section 14) the *goal* of the general theory was clear as soon as KUMMER gave his theory for the cyclotomic integers with prime exponent: the goal was to do for a general algebraic number field (that is, an algebraic extension of the rational field Q) what KUMMER had done in this special case. KRONECKER allegedly had achieved this by 1859, about 10 years after KUMMER's pioneering work, but he published nothing until 1882. DEDEKIND admitted to having struggled unsuccessfully for many years before he published the first version of his theory in 1871.

The paper advances the view that *Dedekind's first version was his best.* DEDEKIND had strong philosophical principles – which took shape about the same time as his ideal theory – and each time he revised his theory and tried to bring it into conformity with his principles it became less satisfactory. This happened because, at base, KUMMER's approach, which DEDEKIND was trying to get away from, is better than the one dictated by DEDEKIND's set-theoretic prejudices. In fact, the first explanation of DEDEKIND's theory in Section 6 avoids introducing "ideals" at all and describes the theory in KUMMER's terms. DEDEKIND's point of view is then explained in Section 7.

Sections 10–22 contain a complete description of KRONECKER's theory of divisors in the case of algebraic number fields. Although such eminent writers as WEYL [38] and EICHLER [17] have expressed a preference for KRONECKER's approach over DEDEKIND's, no explanation of KRONECKER's approach seems to exist except for KRONECKER's own rather crabbed exposition. WEYL [38] does develop a modern version of KRONECKER's theory (Chapter 2), but his version differs in essential ways from the original, and it will certainly not make the original accessible to a modern reader, which I hope the treatment here will do.

Archive for History of Exact Sciences, Volume 23, © *by Springer-Verlag 1980*

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

The approach to ideal theory adopted by HILBERT in his so-called *Zahlbericht* [20] is a hybrid that uses DEDEKIND's "ideals" but establishes their basic properties using a method that derives in essence from KRONECKER's approach. Ironically, the key theorem here is a theorem of DEDEKIND which he called his "Prague" theorem because he published it in the notices of the German Mathematical Society of Prague [8]. Needless to say, DEDEKIND saw clearly that the use of the Prague theorem violated his principles, and he himself did not use it in his definitive version [9] of the theory. This story is told in Section 13.

The concluding section, Section 14, deals with the personal relations between the two* founders, DEDEKIND and KRONECKER. This is followed by a brief appendix which describes KRONECKER's theory of divisors from a somewhat more modern point of view.

Short Chronology of Publications

1844 KUMMER [29] shows that unique factorization fails for cyclotomic integers with exponent 23 but seems to succeed for smaller prime exponents.
1846 KUMMER [30] announces theory of ideal factorization for cyclotomic integers with prime exponents.
1847 KUMMER [31] publishes details of his theory.
1856 KUMMER [33] generalizes his theory to cyclotomic integers with arbitrary exponents.
1857 KUMMER [34] plugs a serious gap in his theory (see [14]).
1859 KUMMER [35] proves his general reciprocity law using ideal factorization in "Kummer fields" (excepting some primes). He also announces that KRONECKER will "soon" publish a simple and fully developed theory for the "most general" case.
1871 DEDEKIND [3] presents a complete theory for general algebraic number fields in Supplement X to the 2nd edition of DIRICHLET's *Zahlentheorie*.
1877 DEDEKIND [4] revises his theory and gives an exposition of it.
1879 DEDEKIND [6] includes the new version as Supplement XI to the 3rd edition of *Zahlentheorie*.
1881 KRONECKER [26] finally publishes his theory of "divisors".
1892 DEDEKIND [8] proves a generalization of GAUSS's lemma, which he later called his "Prague theorem", and shows how it can be used as a foundation for the theory, especially for KRONECKER's version of the theory. MERTENS [36] publishes a similar theorem, also inspired by KRONECKER's work.
1894 DEDEKIND [9] gives yet another version, quite different from the previous two, in Supplement XI to the 4th edition of *Zahlentheorie*.
1894 HURWITZ [21] suggests another approach to the subject, essentially the same as DEDEKIND's based on the "Prague theorem", and DEDEKIND [10] replies.

* Some recent writers have included the Russian mathematician EGOR IVANOVICH ZOLOTAREV (1847–1878) as one of the founders of ideal theory. However, ZOLOTAREV's work was done after DEDEKIND's was published, and it seems to have had no influence on the development of the theory.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

2. The failure of unique factorization

A simple example of the failure of unique factorization for algebraic integers is given by the equation

$$3\cdot 7=(4+\sqrt{-5})\,(4-\sqrt{-5})=21. \tag{2.1}$$

Here one is dealing with the ring $Z[\sqrt{-5}]=\{a+b\sqrt{-5}\colon a,b \text{ integers}\}$. In this ring every element $a+b\sqrt{-5}$ has a norm $(a+b\sqrt{-5})\,(a-b\sqrt{-5})=a^2+5b^2$ and the norm of a product is the product of the norms. This simple fact about norms shows that 3 has no factorizations $3=(a+b\sqrt{-5})\,(c+d\sqrt{-5})$ other than the trivial ones $1\cdot 3$, $(-1)\cdot(-3)$, $3\cdot 1$, and $(-3)\cdot(-1)$, because the factors must have norm 1, 3, or 9 (the norm of 3 is 9) and no element has norm 3 ($3=a^2+5b^2$ is obviously impossible). For similar reasons, the other factors, 7 and $4\pm\sqrt{-5}$, in (2.1) have no factorizations. Thus (2.1) represents two essentially different ways of writing the same "integer" (element of $Z[\sqrt{-5}]$) as a product of factors that have no further decompositions.

Another way of describing the failure of unique factorization that sets it in a very clear light is to say that the *irreducible* elements, that is, the elements which have no factorizations other than trivial ones, are *not necessarily prime,* that is, may divide a product without dividing either factor. Thus (2.1) shows that 3, although it is irreducible, is not prime, because it divides the product $(4+\sqrt{-5})\,(4-\sqrt{-5})$ without dividing either factor. For ordinary integers, irreducible implies prime, as was already proved in EUCLID's *Elements* (Book VII, Proposition 30), and this is the crucial fact in the proof of unique factorization for integers.

The first mathematician to attempt to extend the techniques used in the arithmetic of ordinary integers to other sorts of numbers, for example to $Z[\sqrt{-5}]$, was LEONHARD EULER. Strangely, though, EULER *assumed* that these techniques could be applied in the more general case, and he used them to give very simple deductions of some number-theoretical facts. His conclusions were for the most part correct, even though his arguments based on unique factorization were fallacious. The fallacious arguments occur in his *Algebra* [18] (see, for example, §191 of the last part) which he wrote late in life, and perhaps they are a result of his age or of the fact that his blindness forced him to collaborate with a less talented scribe. The lapse is the more puzzling in view of the fact that the counterexample (2.1) was well known to EULER, and before him to FERMAT, in the form of the statement that a prime divisor of a number of the form x^2+5y^2 need not itself have this form.

(FERMAT had stated, and EULER and LAGRANGE had proved, that if p is an odd prime which divides a number of the form x^2+ny^2 nontrivially – that is, without dividing both x and y – then p must itself have the same form x^2+ny^2 in the cases $n=1,2,3$. This would be very easy to prove if one could assume unique factorization for $Z[\sqrt{-n}]$, but its failure in the case of $n=5$ shows that this is not a valid argument. It is a mystery how EULER could have overlooked this refutation of his argument.)

The first explicit observation of the fact that unique factorization into primes is not always valid for more general sorts of numbers was made by E.E. KUMMER

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

in 1844. In connection with his study of the higher reciprocity laws, KUMMER was doing extensive computations with the ring of cyclotomic integers for a prime exponent. For a given exponent λ, this is the ring $Z[\alpha]$ of all polynomials in α with integer coefficients, added and multiplied in the obvious way, where α is a primitive λ^{th} root of unity, that is, where α satisfies the relation $\alpha^{\lambda-1}+\alpha^{\lambda-2}+\cdots+\alpha+1\,(=(\alpha^{\lambda}-1)/(\alpha-1))=0$. KUMMER noticed, apparently with some help from JACOBI (see [14] and [15]), that when $\lambda=23$ the norm of any element of $Z[\alpha]$ is an integer of the form $(x^2+23y^2)/4$. (The norm of an element $f(\alpha)\in Z[\alpha]$ is simply the product of $f(\alpha)$ with all its conjugates – $Nf(\alpha)=f(\alpha)f(\alpha^2)f(\alpha^3)\cdots f(\alpha^{\lambda-1})$ – which is an ordinary integer. Clearly the norm of a product is the product of the norms.) This is simple to prove (see [16], p. 105) and it shows that no cyclotomic integer for $\lambda=23$ has the norm 47 because $4\cdot 47=188$ cannot be written as a square plus 23 times a square. Thus the equation

$$N(1-\alpha+\alpha^{21})=47\cdot 139 \tag{2.2}$$

(a rather lengthy but altogether elementary calculation – see [16] pp. 104–105) shows that $1-\alpha+\alpha^{21}$ is *irreducible* (a nontrivial factorization would imply a factor with norm 47) but not *prime* (it divides $47\cdot 139$ but it divides neither 47 nor 139 because its norm does not divide $N(47)=47^{22}$ or $N(139)=139^{22}$).

Another way of viewing (2.2) is the following. The left side is, as it stands, a product of 22 irreducible factors each of norm $47\cdot 139$. KUMMER gave, on the other hand, representations

$$\begin{aligned} N(\alpha^{10}+\alpha^{13}+\alpha^{8}+\alpha^{15}+\alpha^{7}+\alpha^{16})&=47^2,\\ N(\alpha^{10}+\alpha^{13}+\alpha^{8}+\alpha^{15}+\alpha^{4}+\alpha^{19})&=139^2. \end{aligned} \tag{2.3}$$

Because of the symmetry of the left sides under $\alpha\mapsto\alpha^{22}=\alpha^{-1}$, each factor on the left occurs twice, and the square root of these relations gives ± 47 and ± 139 as products of 11 irreducible cyclotomic integers of norm 47^2 and 139^2 respectively. Therefore $\pm 47\cdot 139$ can be written as a product of 22 irreducible cyclotomic integers, half of norm 47^2 and half of norm 139^2. This factorization is clearly entirely different from the factorization (2.2) into 22 irreducible factors of norm $47\cdot 139$.

KUMMER regretted this inconvenient fact about the rings $Z[\alpha]$ that he was studying (see [29], p. 202) because he appreciated how important and useful the property of unique factorization was in arithmetic. This appreciation led him in the next few years to devise a substitute, a weakened form of unique factorization, which enabled him to penetrate very far into the study of cyclotomic integers, first to prove significant new results relating to FERMAT's Last Theorem and ultimately to solve the problem of the higher reciprocity laws which was his original goal.

3. Kummer's theory

The main idea of KUMMER's theory is to decompose a cyclotomic integer into its prime factors and, in cases where prime factors do not exist, to introduce *ideal* prime factors.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

The example of the preceding section

$$N(1-\alpha+\alpha^{21})=47\cdot 139 \tag{3.1}$$

where $\alpha \neq 1$ is a root of $\alpha^{23}=1$ and where $N(1-\alpha+\alpha^{21})$ denotes the product of the 22 conjugates $1-\alpha+\alpha^{21}$, $1-\alpha^2+\alpha^{19}$, $1-\alpha^3+\alpha^{17}, \ldots, 1-\alpha^{22}+\alpha^2$, together with the fact that when $\lambda=23$ no cyclotomic integer has norm 47, shows that 47 has no prime factors. (If $f(\alpha)$ were a prime factor of 47 then $Nf(\alpha)$ would divide $N(47)=47^{22}$ and would therefore be a power of 47. On the other hand, since $f(\alpha)$ divides $N(1-\alpha+\alpha^{21})$, it must, by the definition of prime, divide one of the 22 factors of $N(1-\alpha+\alpha^{21})$. Therefore its norm must divide the norm $47\cdot 139$ of this factor. Therefore $Nf(\alpha)=47$, contrary to the fact that no cyclotomic integer has norm 47.) The goal, then, is to define "ideal" prime factors of 47 in such a way that as many of the usual properties are preserved as possible. In all cases with $\lambda<23$ ($\lambda=$prime), an equation of the form (3.1) would indicate that $1-\alpha+\alpha^{21}$ could be decomposed as a product of a prime with norm 47 and a prime with norm 139. Moreover, the $\lambda-1$ conjugates of these primes would all be distinct, that is, no one of them would divide any other. Thus, in the case of (3.1), one would attempt to find 22 *ideal* prime factors of 47, one for each conjugate of $1-\alpha+\alpha^{21}$, and similarly to find 22 ideal prime factors of 139. In the equations (2.3) one would then expect each of the 22 factors on the left to be divisible by *two* ideal prime factors of the primes on the right.

How are these "ideal" prime factors to be described? This is a question that was to occupy much thought on the part of mathematicians for many years after the publication of KUMMER's theory. However, this thought concerned metaphysics and psychology more than mathematics, because from a mathematical point of view KUMMER's original method of description, presented in his first brief announcement [30] of the theory, was entirely satisfactory.

KUMMER described an ideal prime factor by defining precisely what it means to say that a number is *divisible* by it. For the ideal prime factors of 47 considered above, this is easily done as follows. Let P denote the hypothetical prime divisor of 47 which divides $1-\alpha+\alpha^{21}$. Then P is one of 22 distinct ideal prime factors of 47, one for each conjugate $1-\alpha+\alpha^{21}$, $1-\alpha^2+\alpha^{19}$, $1-\alpha^3+\alpha^{17}, \ldots$ of $1-\alpha+\alpha^{21}$. Let $\Psi(\alpha)$ denote the product of the 21 conjugates of $1-\alpha+\alpha^{21}$ other than the one $1-\alpha+\alpha^{21}$ that is divisible by P. Then $\Psi(\alpha)$ is divisible by all ideal prime divisors of 47 *except* P, so that a product $f(\alpha)\Psi(\alpha)$ will be divisible by 47 if and only if $f(\alpha)$ contains the missing prime divisor P. This was KUMMER's definition in this case:

A cyclotomic integer $f(\alpha)$ is said to be divisible by P if $f(\alpha)\Psi(\alpha)$ is divisible by 47. The testing of this condition directly is a rather long computation. It can be greatly simplified by proving* that *$f(\alpha)$ is divisible by P if and only*

* This is not hard to do. Let cyclotomic integers be mapped to integers mod 47 by the rule $f(\alpha)\mapsto f(4) \bmod 47$. This map is well defined because $4^{22}+4^{21}+\cdots+4^1+4^0=(4^{23}-1)/(4-1)=(2^{46}-1)/3\equiv 0 \bmod 47$ (because $2^{46}\equiv 1 \bmod 47$ by FERMAT's theorem) and because if $f_1(x)$ and $f_2(x)$ are two polynomials such that the cyclotomic integers $f_1(\alpha)$ and $f_2(\alpha)$ are equal then $f_1(x)-f_2(x)=q(x)\,(x^{22}+x^{21}+\cdots+x+1)$ for some polynomial $q(x)$

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

if $f(4)$ is divisible by 47. This form of the condition is so much simpler that it appears at first glance to be a better way of defining divisibility by P, but, as KUMMER observed, it has the defect that it gives no way of testing for *multiple* occurrences of P in $f(\alpha)$, whereas the definition KUMMER chose does: *A cyclotomic integer $f(\alpha)$ is said to be divisible μ times by P if $f(\alpha)\Psi(\alpha)^{\mu}$ is divisible by 47^{μ}.*

KUMMER had behind him the experience of extensive calculations with cyclotomic integers for exponents $\lambda<23$, in which no contradictions to unique factorization occurred. From this experience he was well acquainted with such basic knowledge as the fact that the prime factorization of λ always takes the form $\lambda=\text{unit}\cdot(\alpha-1)^{\lambda-1}$ where $\alpha-1$ is prime, the fact that if $g(\alpha)$ is a prime cyclotomic integer then its norm must be a power of a prime integer, and the fact that any norm must be 0 or 1 mod λ. He had observed, moreover, that when $\lambda<23$, he was able, in all cases he tried, to find for a given prime $p\neq\lambda$ a prime cyclotomic integer $g(\alpha)$ for which $g(\alpha)=g(\alpha^{p})$ and for which $Ng(\alpha)=p^{f}$ where f is the *smallest* positive integer such that $p^{f}\equiv 1 \bmod\lambda$. Such a $g(\alpha)$ easily gave him the factorization of p into prime cyclotomic integers because iteration of $g(\alpha^{j})=g(\alpha^{pj})=g(\alpha^{ppj})=\cdots$ shows that the conjugates of $g(\alpha)$ are equal in sets of f so that the equation $Ng(\alpha)=p^{f}$ has the form $[g_1(\alpha)\,g_2(\alpha)\cdots g_e(\alpha)]^{f}=p^{f}$ where* $e=(\lambda-1)/f$ and where $g_1(\alpha),\cdots,g_e(\alpha)$ are conjugates of $g(\alpha)$. Because $g_1(\alpha)\,g_2(\alpha)\cdots g_e(\alpha)$ is invariant under all conjugations it is an integer, and because its f^{th} power is p^{f} it must be $\pm p$ (and must be p if f is odd). Since the conjugates of a prime are obviously prime, this represents $\pm p$ as a product of primes. The primes $g_1(\alpha)\,g_2(\alpha)\cdots g_e(\alpha)$ in this factorization were always *distinct* in the strong sense that no one of them divided any other. It was

---

and $f_1(4)-f_2(4)=q(4)\,(4^{22}+4^{21}+\cdots+4+1)\equiv 0 \bmod 47$. This is a homomorphism from the ring of cyclotomic integers to the field of integers mod 47. Now the image of $1-\alpha+\alpha^{21}=\alpha^{21}(\alpha^{2}-\alpha^{3}+1)$ under this map is $4^{21}(16-64+1)=-4^{21}\cdot 47\equiv 0 \bmod 47$. Thus if $g(x)=1-x+x^{21}$ one has $g(x)=(x-4)\,h(x)+g(4)$ and, since $g(4)\equiv 0 \bmod 47$, $g(\alpha)\equiv(\alpha-4)\,h(\alpha) \bmod 47$. Therefore $(\alpha-4)\Psi(\alpha)=(\alpha-4)\,g(\alpha^{2})\,g(\alpha^{3})\cdots g(\alpha^{22})\equiv(\alpha-4)\,(\alpha^{2}-4)\,h(\alpha^{2})\,(\alpha^{3}-4)\,h(\alpha^{3})\cdots=N(\alpha-4)\,h(\alpha^{2})\,h(\alpha^{3})\cdots h(\alpha^{22})$. Now $N(\alpha-4)$ is an integer and since it is in the kernel of the mapping $\alpha\mapsto 4$ (the factor $\alpha-4$ of $N(\alpha-4)$ becomes 0) $N(\alpha-4)\equiv 0 \bmod 47$. Therefore $(\alpha-4)\Psi(\alpha)\equiv 0 \bmod 47$. Thus if $f(4)\equiv 0 \bmod 47$ it follows that $f(\alpha)=(\alpha-4)\,q(\alpha)+f(4)\equiv(\alpha-4)\,q(\alpha)$ for some $q(\alpha)$ and therefore $f(\alpha)\Psi(\alpha)\equiv(\alpha-4)\Psi(\alpha)\,q(\alpha)\equiv 0 \bmod 47$, that is, P divides $f(\alpha)$. Conversely, if P divides $f(\alpha)$ then $f(\alpha)\Psi(\alpha)=f(\alpha)\,g(\alpha^{2})\,g(\alpha^{3})\cdots g(\alpha^{22})$ is of the form $47\,h(\alpha)$ for some $h(\alpha)$, from which $f(4)\,g(4^{2})\,g(4^{3})\cdots g(4^{22})\equiv 47\,h(4)\equiv 0 \bmod 47$. To reach the desired conclusion $f(4)\equiv 0 \bmod 47$ it suffices to prove that $g(4^{j})\not\equiv 0 \bmod 47$ for $j=2,3,\cdots,22$. But if $g(4^{j})\equiv 0 \bmod 47$ then, as above, $g(x)=(x-4^{j})\,h_1(x)+g(4^{j})\equiv(x-4^{j})\,h_1(x) \bmod 47$, $(\alpha-4^{j})\Psi(\alpha)\equiv N(\alpha-4^{j})\,h_1(\alpha^{2})\,h_1(\alpha^{3})\cdots h_1(\alpha^{22})\equiv 0\equiv(\alpha-4)\,\Psi(\alpha) \bmod 47$. Thus $(4^{j}-4)\Psi(\alpha)\equiv 0 \bmod 47$. The integer $4^{j}-4$ is not zero mod 47 because if it were then so would $N(\alpha^{j}-\alpha)=N(\alpha)\,N(\alpha^{j-1}-1)=N(\alpha-1)$ be, but $N(\alpha-1)=23$ as substitution of 1 for x in the identity $x^{\lambda-1}+x^{\lambda-2}+\cdots+x+1=(x-\alpha)\,(x-\alpha^{2})\cdots(x-\alpha^{\lambda-1})$ shows. Therefore $4^{j}-4$ is invertible mod 47 and $g(4^{j})\equiv 0 \bmod 47$ would imply $\Psi(\alpha)\equiv 0 \bmod 47$. This is impossible because it would imply that the integer $N\Psi(\alpha)$ was divisible by 47^{22} whereas $N\Psi(\alpha)=Ng(\alpha^{2})\cdot Ng(\alpha^{3})\cdots Ng(\alpha^{22})=[Ng(\alpha)]^{21}=47^{21}\cdot 139^{21}$.

* Since KUMMER's time it has become customary to use the letter e to represent a ramification index. Readers familiar with this notation should be warned that here e is *not* a ramification index and that p is here unramified.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

this standard form of the factorization of primes $p \neq \lambda$ that KUMMER attempted to extend to the case of general λ by introducing *ideal* prime cyclotomic integers. He expected to find, when $p \neq \lambda$ is given and f is defined to be the least positive integer for which $p^f \equiv 1 \bmod \lambda$, exactly e distinct *ideal* prime factors of p where $e=(\lambda-1)/f$, and expected a cyclotomic integer to be divisible by p if and only if it was divisible by the e *ideal* prime factors of p. (When $p=47$ and $\lambda=23$, of course $f=1$ so the expectation is that there will be $22=(\lambda-1)/f$ distinct ideal prime factors of 47, as above.)

In cases where he could not find actual prime cyclotomic integers $g(\alpha)$ satisfying $Ng(\alpha)=p^f$ and $g(\alpha)=g(\alpha^p)$ KUMMER was able to find cyclotomic integers $g(\alpha)$ for which $g(\alpha)=g(\alpha^p)$ but $Ng(\alpha)=p^f k^f$ where k is not divisible by p. As before, this equation can be written $[g_1(\alpha)\, g_2(\alpha) \cdots g_e(\alpha)]^f=(pk)^f$, $g_1(\alpha)\, g_2(\alpha) \cdots g_e(\alpha)= \pm pk$, which makes it natural to hypothesize that each of the e distinct ideal prime factors of p that are to be found divides one and only one of the $g_i(\alpha)$. This means that the ideal prime factor P of p which divides $g_1(\alpha)$ will divide $f(\alpha)$ with multiplicity μ if and only if p^μ divides $f(\alpha)\Psi(\alpha)^\mu$ where $\Psi(\alpha)=g_2(\alpha)\, g_3(\alpha) \cdots g_e(\alpha)$. This can then be taken as the *definition* of divisibility by P.

Given $p \neq \lambda$, find a cyclotomic integer $g(\alpha)$ for which $g(\alpha)=g(\alpha^p)$ and for which $Ng(\alpha)$ is divisible by p^f but not by p^{f+1}, where f is the least positive integer satisfying $p^f \equiv 1 \bmod \lambda$. The conjugation $\alpha \mapsto \alpha^p$ partitions the $\lambda-1$ conjugates of $g(\alpha)$ into e orbits of f each $(e=(\lambda-1)/f)$, all conjugates in the same orbit being equal. *Let $\Psi(\alpha)=g_2(\alpha)\, g_3(\alpha) \cdots g_e(\alpha)$ where the $g_i(\alpha)$ consist of one conjugate of $g(\alpha)$ from each of the e orbits except the orbit containing $g(\alpha)$ itself. A cyclotomic integer $f(\alpha)$ is said to be "divisible μ times by the ideal prime factor of p which divides $g(\alpha)$" if $f(\alpha)\, \Psi(\alpha)^\mu$ is divisible by p^μ.*

Here each choice of $g(\alpha)$ gives rise to e ideal prime factors of p, one for each of its conjugates. If $\bar{g}(\alpha)$ is any other cyclotomic integer with the same property as $g(\alpha)$ (that is, $\bar{g}(\alpha)=\bar{g}(\alpha^p)$ and $N\bar{g}(\alpha)$ is divisible by p^f but not by p^{f+1}) then, as is easily deduced from the basic properties below, $\bar{g}(\alpha)$ gives rise to the *same* ideal prime factors of p, that is, each one for $g(\alpha)$ is equal to one for $\bar{g}(\alpha)$ in the sense that they divide any given $f(\alpha)$ with the same multiplicity. Thus, in the statements below, p is to be regarded as having just e distinct ideal prime factors and they can be described explicitly by finding just one $g(\alpha)$ with the required property. In particular, if there is a $g(\alpha)$ which satisfies $g(\alpha)=g(\alpha^p)$ and $Ng(\alpha)=p^f$ then divisibility by the ideal prime factor of p which divides $g(\alpha)$ coincides with divisibility by $g(\alpha)$ and the ideal prime factors can be realized as actual prime factors. All of this defines the ideal prime factors of $p \neq \lambda$. There is only one prime factor of λ, which is the actual factor $\alpha-1$.

To establish his theory, then, KUMMER needed to prove the existence of such a $g(\alpha)$ for each $p \neq \lambda$, and to prove that the ideal prime factors have the expected properties. These he enumerated as follows:

"The product of two or more complex numbers [that is, cyclotomic integers for the prime exponent λ] has exactly the same ideal prime factors as the factors taken together.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

"When a complex number (which is given as a product) contains all e ideal prime factors of p it is divisible by p; however, if it fails to contain any one of these ideal prime factors, then it is not divisible by p.

"When a complex number (in the form of a product) contains all e ideal prime factors of p, and indeed contains each at least μ times, then it is divisible by p^{μ}.

"When $f(\alpha)$ contains m ideal prime factors of p, which may be different or may be partly or entirely equal, the norm $Nf(\alpha)=f(\alpha)\,f(\alpha^2)\cdots f(\alpha^{\lambda-1})$ contains exactly the factor p^{mf}. [Here the f for which $p^f\equiv 1 \bmod \lambda$ is unrelated to $f(\alpha)$.]

"Each complex number [0 should be excepted] contains only a finite, determined number of ideal prime factors.

"Two complex numbers which have exactly the same ideal prime factors differ at most by a complex unit which may enter as a factor.

"A complex number is divisible by another whenever all ideal prime factors in the divisor are contained in the dividend, and the quotient contains exactly the surplus of the ideal prime factors of the dividend over those of the divisor." [30, pp. 322–323]

The most difficult step in establishing KUMMER's theory is the proof of the existence of a $g(\alpha)$ for each $p\neq\lambda$. KUMMER's original expositions of the theory in 1847 [31] and 1851 [32] were in fact defective in that they did not rigorously establish this fact in all cases. (See WEIL's note to p. 213 in [28], or see [14].) However, these defects escaped notice until KUMMER was able to rectify them in 1857. In the meantime, the power, the essential correctness, and the beauty of his theory had begun to be appreciated and the need for generalizations had begun to be felt.

4. The general case

Already in his first publication [30] on the theory of "ideal complex numbers", KUMMER spoke of generalizing the theory to "complex numbers of the form $x+y\sqrt{D}$" and of the relation of this theory to GAUSS's very intriguing and important theory of composition of binary quadratic forms. In his later work he never returned to this subject, but he did generalize the theory in other ways; he gave a complete theory of ideal complex numbers for cyclotomic integers in the case where λ is not a prime [33], and in his *chef d'œuvre*, the proof of the higher reciprocity law for regular prime exponents [35], he developed the theory for extensions of the cyclotomic integers obtained by the adjunction of a λ^{th} root of a cyclotomic integer (the fields HILBERT later called "KUMMER fields"). However, in this last case he avoided dealing with a certain finite collection of primes p which present special difficulties; in fact, he even said that for some primes p it is *impossible* to define ideal prime factors "which deserve this name in the fullest sense."*

* welche im vollen Sinne diesen Namen verdienen [35, p. 55]. An interesting indication of KUMMER'S attitude about the generalization of the theory is to be found on p. 481 of volume 3 of DEDEKIND's *Werke*. One must be cautious about accepting this information at face value because it is at third hand and was allegedly remembered by DEDEKIND some 30 years later, but according to it, KUMMER regarded as a *defect* of DEDEKIND's

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

In the introduction to his resumé [32] of 1851 of the theory of ideal factorization for cyclotomic integers for prime λ, KUMMER even alluded to the most general case of factorization of algebraic numbers (although he left out the essential condition that the defining equation be *monic,* a condition that he surely intended) and said that it was a problem that "has great interest, both in itself and for the numerous and important applications that have been made of it in questions relating to arithmetic and higher algebra." Part of the reason that KUMMER never dealt with the general case may have lain in his personality; in his work he very consistently introduces no more new concepts than are necessary to his purposes and he shows a consistent disinclination toward generalization for generalization's sake.

Another, and perhaps more important, reason that he did not generalize his theory was that his friend and former student (from the days when he was a young gymnasium teacher in Liegnitz), LEOPOLD KRONECKER, had already developed the theory. In 1859 KUMMER wrote, "In regard to [the finiteness of the class number in KUMMER fields], and moreover in regard to the general theorems which are common to all theories of complex [*i.e.* algebraic] numbers, I can refer to a work of Herr KRONECKER, which will soon appear, in which the theory of the most general complex numbers is developed fully and with great simplicity ..."*

It is a great loss to the history of mathematics and to our understanding of the genesis of algebraic number theory that KRONECKER never published this paper "soon to appear". He did refer to it in 1882 in his famous "Grundzüge". About it he said that he wrote it in 1858 and that the development of the general theory had presented "no difficulties whatever" because the ideas already developed by GAUSS and DIRICHLET were all that were needed (§19). His reason for the unfortunate decision not to publish it was that he had already discovered, in 1857, the possibility of what is today called an associated class field in the case of an imaginary quadratic field and that he held up publication of his paper in the hope that he would soon be able to give an analogous construction of a class field in the general case! Fortunately he gave up this hope and published the "Grundzüge" when he did, but after 20 years of refinement and improvement, his theory, elegant and general as it was, certainly no longer has the "great simplicity" that KUMMER ascribed to the original version.

---

theory the fact that he handled the factorization of all primes p the same way and did not single out the ones which divide the discriminant – those for which KUMMER'S later theory did not apply – for special treatment. It is more natural to see this as an *advantage,* and one wonders whether KUMMER did not instead doubt the correctness of DEDEKIND's theory on the grounds that he did not understand how the obstacle he had encountered had been removed.

* Ich kann in Betreff dieser, so wie überhaupt der allgemeinen Sätze, welche allen Theorieen complexer Zahlen gemein sind auch auf eine Arbeit von Hrn. KRONECKER verweisen, welche nächstens erscheinen wird, in welcher die Theorie der allgemeinsten complexen Zahlen, in ihrer Verbindung mit der Theorie der zerlegbaren Formen aller Grade, vollständig und in grossartiger Einfachheit entwickelt ist. [35, p. 57]

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

Despite KRONECKER's claim that he encountered no difficulties, there *is* a difficulty that, as was mentioned above, KUMMER skirted by avoiding a certain finite number of primes* and that foiled DEDEKIND's early attempts to construct a general theory. This difficulty comes from the fact that for for certain very natural kinds of "algebraic integers" a general theory is indeed impossible, and it is only after *extending* the algebraic integers under consideration that a theory becomes possible. This is illustrated by the following simple special case.

Let $\alpha=\sqrt{-3}$. Then any polynomial in α with integer coefficients can be reduced to the form $A+B\alpha$ where A and B are integers. Let $Z[\alpha]$ denote the numbers of this form. Clearly $Z[\alpha]$ is closed under addition and multiplication and is, as we say now, a ring with unit. The elements of $Z[\alpha]$ might seem deserving of being called algebraic integers, but it is impossible to generalize KUMMER'S theory to the arithmetic of $Z[\alpha]$. To see this, note that $(1+\sqrt{-3})^3=1+3\cdot\sqrt{-3}+3(-3)+(-3)\sqrt{-3}=-8$. Therefore a high power of $1+\sqrt{-3}$ is divisible by a power of 2 almost as high. Specifically, if $a=2^3$, $b=1+\sqrt{-3}$, and $c=2$ then for every positive integer k, say $k=3j+i$, where $0\leqq i<3$, we have $ab^k=2^3b^{3j+i}=2^3(-8)^jb^i=\pm c^{3j+3}b^i$, which is divisible by c^k. If a generalization of KUMMER's theory were possible, then, because 2 does not divide $1+\sqrt{-3}$, there would have to be an ideal prime factor of 2, call it P, which divided 2 with multiplicity greater than the multiplicity with which it divides $1+\sqrt{-3}$, that is $\mu_P(c)>\mu_P(b)$ where μ_P of an element of $Z[\alpha]$ is the multiplicity with which it is divisible by P. Since c^k divides ab^k for all k it follows, on the other hand, that $k\mu_P(c)\leqq\mu_P(a)+k\mu_P(b)$, that is, $k[\mu_P(c)-\mu_P(b)]\leqq\mu_P(a)$ for all k, which obviously implies $\mu_P(c)-\mu_P(b)\leqq 0$. This contradiction shows that a generalization of KUMMER's theory is impossible for $Z[\alpha]$.

In the specific case of this ring $Z[\alpha]$ the difficulty is easily overcome by the observation that this ring is *contained in* the cyclotomic integers for the exponent $\lambda=3$ and that *KUMMER's theory itself* applies to this larger ring. (One need only rewrite an element $A+B\alpha$ of $Z[\alpha]$ in the form $A+B\sqrt{-3}=A+B+2B\dfrac{-1+\sqrt{-3}}{2}=A+B+2B\omega$ where $\omega=\frac{1}{2}(-1+\sqrt{-3})$ satisfies $\omega^3=1$.) The above contradiction is resolved by the fact that $c=2$ *does* divide $b=1+\sqrt{-3}=2\omega+2$ when $Z[\alpha]$ is enlarged to include ω.)

This same sort of phenomenon occurs in the case of a general ring of the form $Z[\alpha]$ as described in the next section. The generalization of KUMMER's theory to $Z[\alpha]$ may be impossible unless the ring $Z[\alpha]$ is *extended*. The recognition of this fact and the description, by means of the notion of an *algebraic integer*, of the needed extension of $Z[\alpha]$, are the key steps in the generalization of KUMMER's theory. Once they have been taken, one might almost say, with KRONECKER, that the generalization "presents no difficulties whatever".

* As DEDEKIND observed [7, # 35], KRONECKER's claim that he had the full theory in 1858 – with or without difficulty – is not consistent with KUMMER's statement that in some cases there are no ideal prime factors "which deserve this name in the fullest sense" (see above). Since KUMMER had access to KRONECKER'S theory, if the theory covered all cases KUMMER should have known that a generalization was possible in all cases.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

5. Algebraic integers

Just as the ring of cyclotomic integers was described by KUMMER as all complex numbers of the form $a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n$ where the coefficients a_i are integers and $\alpha\neq 1$ is a solution of $\alpha^\lambda=1$, one can describe other rings of "algebraic numbers" as all numbers $a_0+a_1\alpha+\cdots+a_n\alpha^n$ where $a_j\in Z$ and α is a solution of an algebraic equation $p(\alpha)=0$ ($p(x)$ a polynomial with rational or, as one may assume because one can multiply by the least common denominator of the coefficients, with integer coefficients). If $p(x)$ is reducible, say $p(x)=p_1(x)\,p_2(x)$ where p_1 and p_2 have rational coefficients, then of course either $p_1(\alpha)=0$ or $p_2(\alpha)=0$, so that $p(x)$ can be replaced by a polynomial of lower degree. It is natural, therefore, to assume that $p(x)$ is irreducible.

Algebraically, the ring $Z[\alpha]$ of all complex numbers of the form $a_0+a_1\alpha+\cdots+a_n\alpha^n$, where α is a root of the irreducible polynomial $p(X)$, can be regarded as the quotient $Z[\alpha]\approx Z[X]/(p(X))$ of the ring $Z[X]$ of all polynomials in the variable X with integer coefficients by the ideal $(p(X))$ of all polynomials that are multiples of $p(X)$. This quotient ring is very easy to describe in the case where $p(X)$ has leading coefficient 1 because then division of polynomials can be used to put any given polynomial $f(X)\in Z[X]$ in the form $f(X)=q(X)\,p(X)+r(X)$ where $q(X)$ and $r(X)$ are polynomials in $Z[X]$ and $\deg r(X)<\deg p(X)$; then $f(\alpha)=r(\alpha)$ and every element of $Z[\alpha]$ can be represented as a polynomial in α of degree less than the degree of $p(X)$. At the outset, this simplifying assumption that $p(X)$ has leading coefficient 1 will be made. As will be noted later, this assumption actually involves no loss of generality.

The goal, now, is to generalize KUMMER's theory of ideal prime factors to such rings $Z[\alpha]\approx Z[X]/(p(X))$ where $p(X)$ is an irreducible,* monic** polynomial in $Z[X]$. It was shown in the preceding section that even in the simple case $p(X)=X^2+3$ such a generalization is not possible unless the ring $Z[\alpha]$ is expanded so that $1+\alpha$ is divisible by 2. Otherwise stated, in the general case there may be quotients $f(\alpha)/g(\alpha)$ of elements $f(\alpha)$, $g(\alpha)\in Z[\alpha]$ which should be regarded as *integers* (that is, $g(\alpha)$ divides $f(\alpha)$) even though there is no element $h(\alpha)\in Z[\alpha]$ such that $f(\alpha)=h(\alpha)\,g(\alpha)$. The first – and the only serious – obstacle to be overcome in generalizing KUMMER's theory is to find the correct definition of what it means to say that a quotient $f(\alpha)/g(\alpha)$ of elements of $Z[\alpha]$ is an *integer*.

Let n be the degree of the polynomial $p(X)$ which defines $Z[\alpha]$. The quotients $f(\alpha)/g(\alpha)$ form a *field* which in modern notation it is natural to denote by $Q(\alpha)$. Elements of $Q(\alpha)$ can be written as polynomials of degree less than n in α with *rational* coefficients. Elements are added and multiplied in the obvious way, using $p(\alpha)=0$ to reduce to degree less than n after multiplication. The inverse $1/g(\alpha)$ of a nonzero element $g(\alpha)$ is found as follows: Apply the Euclidean algorithm for polynomials with rational coefficients to $g(X)$ and

---

* The rationale given above justifies the assumption that $p(X)$ is irreducible over the *rationals,* that is, that it cannot be written as a product of polynomials of lower degree with rational coefficients. By GAUSS's lemma (see Section 11) this will follow if it is merely assumed that $p(X)$ is irreducible over the integers.

** A polynomial is said to be *monic* if its leading coefficient is 1.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

$p(X)$ to find a relation of the form $a(X)\,g(X)+b(X)\,p(X)=c(X)$ where $c(X)$ is a polynomial with rational coefficients which divides both $g(X)$ and $p(X)$. Since $p(X)$ is irreducible, $c(X)$ must have degree 0 or degree n. If it had degree n then it would be a nonzero constant times $p(X)$, and it would follow that $p(X)$ divided $g(X)$, contrary to the assumption that $g(\alpha)\neq 0$. Therefore $c(X)$ is a nonzero constant, say c. Then $X=\alpha$ in $a(X)\,g(X)+b(X)\,p(X)=c$ gives $a(\alpha)\,g(\alpha)=c$. Thus $1/g(\alpha)=c^{-1}a(\alpha)$ gives the desired expression of $1/g(\alpha)$ as a polynomial in α with rational coefficients.

The problem, then, is to determine which elements of this field $Q(\alpha)$ should be regarded as being *integers*. Although DEDEKIND and KRONECKER in other respects formulated their ideas in very different ways, they gave identical answers to this question: *An element of $Q(\alpha)$ is an integer if it is the root of a monic polynomial with integer coefficients.** Unfortunately, neither of them gives a reason for this definition or explains how it was arrived at. Insofar as this is the crucial idea of the theory, the genesis of the theory appears, therefore, to be lost.

KRONECKER speaks [26, §20] of a principle of "conservation of the determination of concepts (*Begriffsbestimmung*) in passing from the rational to the algebraic" which guided him in the study of algebraic quantities (numbers or functions). Such a principle would seem to require that "integers" have at least the following properties: (1) Sums and products of integers are integers. (2) A rational number is an integer in the new sense if and only if it is an ordinary integer. (3) Conjugates of integers are integers. That the algebraic integers of $Q(\alpha)$ have these properties is easy to prove.** The only difficult

---

* [3, §160] and [26, §5]. DEDEKIND said in 1894 [9, note to §173] that he did not know whether "integer" had been used in this sense before his use of it in 1871. KRONECKER [25, Preface] strongly implied in 1881 that he was already using this definition in 1857. According to BOURBAKI [1b, p. 127] "the notion of an algebraic integer" was "introduced" independently by DIRICHLET, HERMITE, and EISENSTEIN in the 1840's and 1850's, but the specific references he gives do not, in my view, bear out this contention. Rather, the authors cited merely make the same assumption that was made above, that $p(x)$ is monic with integer coefficients, so that polynomials in α with integer coefficients, and with degree less than the degree of $p(x)$, are closed under multiplication. This is very different from the question under consideration, which is to determine which polynomials in α with rational coefficients should be regarded as integers, a question that none of these authors deal with. Furthermore, I do *not* find the proof that BOURBAKI claims EISENSTEIN has for the theorem that sums and products of integers are integers. What EISENSTEIN proves is that if a polynomial in α and its conjugates is equal to a rational number then it is an integer. This is an easy *consequence* of the fact that sums and products of integers are integers, but this is not at all the approach that EISENSTEIN takes.

** The proof of (1) is given in the text. For (2), note that if $a\in Z$ then $X-a$ is a monic polynomial with integer coefficients of which a is a root. Conversely, if the rational number a/b, where a and b are relatively prime, is a root of the polynomial $X^k+A_1X^{k-1}+\cdots+A_{k-1}X+A_k$ where the A's are integers then $a^k+A_1a^{k-1}b+A_2a^{k-2}b^2+\cdots+A_kb^k=0$. Since b divides all but the first term a^k on the left, it must also divide this term. Since a and b are relatively prime, $b|a^k$ implies $b=\pm 1$, as desired. Finally, for (3) let β be an algebraic integer and let γ be a conjugate of β. Then, by definition, there is an irreducible equation $g(X)$ with rational coefficients of which both β and γ are roots. By assumption, there is a monic polynomial $f(X)$ with integer coefficients of which β is a root. The

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

part to prove is the statement that algebraic integers have property (1). KRONECKER said [26, §5] that this property was obvious (*offenbar*) and gave no proof. *** DEDEKIND gave [3, §160] the following very elegant proof.

Let β and γ be (algebraic) integers in $Q(\alpha)$. It is to be shown that $\beta+\gamma$ and $\beta\gamma$ are algebraic integers. Let $\beta^j+A_1\beta^{j-1}+\cdots+A_j=0$ and $\gamma^k+B_1\gamma^{k-1}+\cdots+B_k=0$ where the A's and B's are (ordinary) integers. Let $m=jk$ and let $\omega_1, \omega_2, \cdots, \omega_m \in Q(\alpha)$ be the m products $\beta^a\gamma^b$ for $0\leqq a<j$, $0\leqq b<k$ in some order. Then $\beta\omega_i$ is a linear combination of the ω's with integer coefficients. Explicitly, $\beta\omega_i=\beta^{a+1}\gamma^b$ is itself one of the ω's unless $a=j-1$, in which case $\beta\omega_i=\beta^j\gamma^b=-A_1\beta^{j-1}\gamma^b-\cdots-A_j\gamma^b$ gives $\beta\omega_i$ as a combination of ω's with integer coefficients. Similarly, $\gamma\omega_i$ is a combination of ω's. Thus $(\beta+\gamma)\omega_i$ is always a combination of ω's. In fact, if $F=F(\beta,\gamma)$ is any polynomial in β and γ with integer coefficients, then $F\omega_i$ is a combination of ω's, say

$$F\omega_i=\sum_{s=1}^{m} c_{is}\omega_s$$

where the c's are ordinary integers. These equations can be written in matrix form as $(C-FI)\omega=0$ where $C=(c_{is})$, where I is the identity matrix, where $F\in Q(\alpha)$, and where ω is a column matrix. Since ω is not the zero matrix

---

Euclidean algorithm can be used to express the greatest common divisor of $g(X)$ and $f(X)$ in the form $r(X)\,g(X)+s(X)f(X)$ where $r(X)$ and $s(X)$ are polynomials with rational coefficients. Since $g(X)$ is irreducible, this greatest common divisor must be a nonzero multiple of $g(X)$ or a nonzero constant. It cannot be a nonzero constant because $r(\beta)g(\beta)+s(\beta)\,f(\beta)=r(\beta)\cdot 0+s(\beta)\cdot 0=0$. Therefore $g(X)$ divides $f(X)$, and it follows that $f(\gamma)=0$, as desired.

*** An approach to the theorem that sums and products of integers are integers which makes it fairly obvious is the following. Let K be a normal extension of Q which contains α (for example, let K be the splitting field of $p(X)$) and let G be its GALOIS group. For a given $\beta\in Q(\alpha)$, let $f_\beta(X)=\prod_{\sigma\in G}(X-\sigma(\beta))$. Then, up to sign, the coefficients of $f_\beta(X)$ are the elementary symmetric functions of the conjugates $\sigma(\beta)$ of β. Because they are invariant under G, they are rational numbers. *They are integers if and only if β is an algebraic integer.* In one direction this is obvious, namely, if the coefficients of $f_\beta(X)$ are integers then β is an integer. What is to be proved is the converse. Assume that β is an algebraic integer, say $h(\beta)=0$ where $h(X)$ is a monic polynomial with coefficients in Z. Let $g_\beta(X)$ be the irreducible monic polynomial satisfied by β. Then, since every $\sigma(\beta)$ is a root of $g_\beta(X)$, it is easy to see that $g_\beta(X)^k=f_\beta(X)$ where k is the number of times that β occurs among the $\sigma(\beta)$. Moreover, $g_\beta(X)$ divides $h(X)$, and therefore by GAUSS's lemma, $g_\beta(X)$ has integer coefficients. (If $h(X)=p(X)\,q(X)$ where p and q are monic polynomials with rational coefficients then p and q must have integer coefficients.) Thus $f_\beta(X)=g_\beta(X)^k$ has integer coefficients, as was to be shown. If β and γ are algebraic integers then the elementary symmetric functions of $\sigma(\beta)$ and of $\sigma(\gamma)$ are all integers. It is then reasonably clear that if σ and τ range *separately* over the GALOIS group then the coefficients of the polynomial $\prod(X-\sigma(\beta)-\tau(\gamma))$ (of degree equal to the square of the order of G) are symmetric in the $\sigma(\beta)$ and the $\tau(\gamma)$ separately and are therefore all integers. Thus $\beta+\gamma$ satisfies a polynomial with integer coefficients and is therefore an algebraic integer. Similarly $\prod(X-\sigma(\beta)\,\tau(\gamma))$ has integer coefficients and $\beta\gamma$ is an algebraic integer. Thus, sums and products of integers are integers, as was to be shown. This proof is the one sketched by HILBERT in the Zahlbericht [20].

It should perhaps be mentioned that DEDEKIND's proof was published some 10 years before KRONECKER'S statement that it was obvious. DEDEKIND himself once said [4] that it was obvious.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

(otherwise $\beta=\gamma=0$ and there is nothing to prove), these equations show that the $m\times m$ homogeneous system of linear equations with coefficients in $Q(\alpha)$ whose matrix of coefficients is $C-FI$ has a nontrivial solution. Therefore $\det(C-FI)=0$. This shows that F is a root of the characteristic equation of C and therefore that F is an integer. In the cases $F=\beta+\gamma$ and $F=\beta\gamma$ this is what was to be shown.

DEDEKIND used the same idea to prove a crucial generalization of this theorem, namely, the theorem that *if* $\omega\in Q(\alpha)$ *satisfies an equation of the form* $F(\omega)=0$ *where* F *is a monic polynomial with coefficients that are algebraic integers in* $Q(\alpha)$ *then* ω *is an algebraic integer*. Let $F(\omega)=\omega^k+\alpha_1\omega^{k-1}+\alpha_2\omega^{k-2}+\cdots+\alpha_k$. Let $\omega_1, \omega_2, \cdots, \omega_m$ be all products of the form $\omega^a\alpha_1^{b_1}\alpha_2^{b_2}\cdots\alpha_k^{b_k}$ where $0\leqq a<k$ and $0\leqq b_i<$ degree of a monic polynomial with integer coefficients of which α_i is a root. Then, as above, ω times any one of the elements $\omega_j\in Q(\alpha)$ can be expressed in the form $\omega\omega_j=\sum_{s=1}^{m} c_{js}\omega_s$ where the c_{js} are integers. Therefore ω is a root of the characteristic equation $\det(C-xI)=0$ of the integral matrix $C=(c_{js})$, and this proves that ω is an integer.

This important theorem can be regarded as an instance of KRONECKER's "conservation of the determination of concepts in passing from the rational to the algebraic" which justifies the definition of "algebraic integer" that was given above. The property that *any solution of a monic algebraic equation with integer coefficients is itself an integer* is true in the rational domain. When the numbers under consideration are extended to some algebraic domain $Q(\alpha)$, it is natural to require that it continue to be true. This means that all algebraic integers *must* be regarded as integers. Then DEDEKIND's theorem shows that this basic property of rational integers continues to hold for algebraic integers when they are defined as above.

Now that the notion of an "integer" in $Q(\alpha)$ has been defined, it is natural to ask which elements of $Q(\alpha)$ are integers and how integers can be found. DEDEKIND gave a very satisfactory answer, embodied in the proposition below, in his first exposition of the theory of algebraic integers.

It has been assumed above that α is a root of a monic irreducible polynomial $p(X)$ with integer coefficients. If $p(X)$ is not monic but instead has leading coefficient k, then multiplication of $p(\alpha)=0$ by k^{n-1}, where n is the degree of $p(X)$, gives an equation of the form $P(k\alpha)=0$ where $P(X)$ is a monic irreducible polynomial with integer coefficients. Thus the above construction can be applied to $\alpha'=k\alpha$ to give the field $Q(\alpha')$. This field obviously coincides with $Q(\alpha)$, so there was no loss of generality in assuming at the outset that α itself was the root of a monic polynomial.

Since α is by assumption itself an integer, the elements of the ring $Z[\alpha]=\{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}: a_i\in Z\}$, because they are sums of products of integers, are also integers. However, α is more or less arbitrarily chosen – for example, as was just noted, α could be replaced by 2α and the field $Q(\alpha)$ would be unchanged – so it is clear that there may be integers in $Q(\alpha)$ that are not in $Z[\alpha]$. The key step in describing the set of all integers is the observation that $Z[\alpha]$ has finite index in the set of all integers of $Q(\alpha)$, that is, that there is a finite set of integers such that every integer is a sum of one of these and an element of $Z[\alpha]$.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

Lemma. There is an integer $N \neq 0$ such that all integers β in $Q(\alpha)$ satisfy $N\beta \in Z[\alpha]$. Moreover, such an N can be determined explicitly from the coefficients of the monic irreducible equation satisfied by α.

Proof.[1] Let $p(X)$ be the equation satisfied by α and let $\alpha_2, \alpha_3, \cdots, \alpha_n$ be the other[2] complex roots of $p(X)$. If $\beta = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$ is an integer then so are $\beta_2, \beta_3, \cdots, \beta_n$ where $\beta_i = a_0 + a_1\alpha_i + a_2\alpha_i^2 + \cdots + a_{n-1}\alpha_i^{n-1}$. This is clear from the fact that the polynomial relation satisfied by β is a consequence of $p(\alpha) = 0$ alone, and from the fact that $p(\alpha_i) = 0$. Now consider the solution of the equations

$$\begin{aligned} a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} &= \beta, \\ a_0 + a_1\alpha_2 + a_2\alpha_2^2 + \cdots + a_{n-1}\alpha_2^{n-1} &= \beta_2, \\ &\cdots \\ a_0 + a_1\alpha_n + a_2\alpha_n^2 + \cdots + a_{n-1}\alpha_n^{n-1} &= \beta_n \end{aligned}$$

for a_j by CRAMER's rule. This comes from substituting the column $\beta, \beta_2, \cdots, \beta_n$ for the j^{th} column of the determinant which has α_i^{j-1} in the i^{th} row of the j^{th} column. On the one hand, this gives an $n \times n$ determinant D_j all of whose entries are algebraic integers so that D_j is an algebraic integer, and on the other hand, when the β's are expressed in terms of α's as above and linearity in this column is used, it gives $a_j \Delta$ where Δ is the original determinant $\det(\alpha_i^{j-1})$. Now Δ is an algebraic integer for the same reason that D_j is, so that $a_j\Delta^2 = D_j\Delta$ is an algebraic integer. At the same time, Δ^2 is obviously a symmetric polynomial in the roots of $p(X)$. Therefore, by the fundamental theorem of the theory of symmetric polynomials, Δ^2 can be expressed as a polynomial with integer coefficients in the coefficients of $p(X)$. In particular, Δ^2 is an integer, say N. Then a_jN is a rational number which, because it is equal to $D_j\Delta$, is an algebraic integer. Therefore, a_jN is an integer for all j, as was to be shown.*

Thus there are at most a finite number $\beta_1, \beta_2, \cdots, \beta_K$ of integers $\beta_i = a_{i0} + a_{i1}\alpha + \cdots + a_{i,n-1}\alpha^{n-1}$ in $Q(\alpha)$ for which the coefficients all lie in the range $0 \leqq a_{ij} < 1$ and they can be found simply by finding the field equations of the

[1] KRONECKER [26, §6]. In somewhat different form, DEDEKIND [3, §162].

[2] The setting for the proof is thus a splitting field for the polynomial $p(X)$. The β_i are integers in this field.

* In KUMMER's case, $\alpha^\lambda = 1$, it is not difficult to carry this argument a step farther and show that $Z[\alpha]$ contains all integers. The determinant Δ is a VANDERMONDE determinant and is therefore a product of factors of the form $\pm(\alpha_i - \alpha_j)$. When $\alpha^\lambda = 1$, the conjugates of α are powers of α, so Δ^2 is a product of factors of the form $\pm(\alpha^i - \alpha^j) = \pm\alpha^i(1 - \alpha^{j-i})$. Now, for any k in the range $0 < k < \lambda$, $1 - \alpha^k = (1-\alpha)(1 + \alpha + \alpha^2 + \cdots + \alpha^{k-1})$; taking the norm of both sides of this equation shows that $1 + \alpha + \alpha^2 + \cdots + \alpha^{k-1}$ has norm one and therefore has an inverse in $Z[\alpha]$. The above argument shows that if $f(\alpha) \in Q(\alpha)$ is an integer then $f(\alpha)\Delta^2 = F(\alpha)$ where $F(\alpha)$ is in $Z[\alpha]$. Thus $f(\alpha)\, U(\alpha)\, (1-\alpha)^r = F(\alpha)$ where $U(\alpha)$ is a unit and $r > 0$. Multiplication by the inverse of $U(\alpha)$ puts this equation in the form $f(\alpha)\,(1-\alpha)^r = G(\alpha)$ where $G(\alpha) \in Z[\alpha]$. To prove that $f(\alpha) \in Z[\alpha]$ it suffices to prove that *if* $g(\alpha) \in Q(\alpha)$ *is an integer and if* $g(\alpha)(1-\alpha) \in Z[\alpha]$ *then* $g(\alpha) \in Z[\alpha]$. To prove this let $g(\alpha)\,(1-\alpha) = G(\alpha) \in Z[\alpha]$. Then by division $G(\alpha) = H(\alpha)\,(1-\alpha) + r$ where $r \in Z$. Set $h(\alpha) = g(\alpha) - H(\alpha)$ so that $h(\alpha)\,(1-\alpha) = r$. Taking the norm of this equation gives $Nh(\alpha) \cdot N(1-\alpha) = r^{\lambda-1}$. Setting $X = 1$ in the equation $X^{\lambda-1} + X^{\lambda-2} + \cdots + X + 1 = (X-\alpha)(X-\alpha^2)\cdots(X-\alpha^{\lambda-1})$ gives $N(1-\alpha) = \lambda$. Thus λ divides r, say $r = t\lambda$. The equation $N(1-\alpha) = \lambda$ shows that $\lambda/(1-\alpha) \in Z[\alpha]$. Therefore $h(\alpha) = r/(1-\alpha) = t\lambda/(1-\alpha) \in Z[\alpha]$. Thus $g(\alpha) = h(\alpha) + H(\alpha) \in Z[\alpha]$, as was to be shown.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

N^n numbers of this type in which $a=k/N$ to see whether they are integers. When the integers $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ are adjoined to this list, one obtains a list of $K+n$ integers with the property that every integer can be expressed as a linear combination with (ordinary) integer coefficients of these $K+n$ integers. (Given any integer β, one can add or subtract integer multiples of $1, \alpha, \cdots, \alpha^{n-1}$ to put all its coefficients in the range $0<a<1$ so that it is in the list of K.) From this fact, the following fundamental proposition of DEDEKIND and KRONECKER follows by a simple elimination process.

Proposition. There exist n integers $\omega_1, \omega_2, \cdots, \omega_n$ in $Q(\alpha)$ with the property that every integer of $Q(\alpha)$ can be written in one and only one way in the form $k_1\omega_1+k_2\omega_2+\cdots+k_n\omega_n$ where $k_i \in Z$.

Such a set $\omega_1, \omega_2, \cdots, \omega_n$ is called an *integral basis* of $Q(\alpha)$. The elimination process which proves the theorem* in fact gives a procedure for constructing an integral basis.

---

* This elimination process can be organized as follows. (DEDEKIND [3, §161] organizes it somewhat differently.) Let $\beta_1, \beta_2, \cdots, \beta_{K+n}$ be the set of integers of $Q(\alpha)$ constructed above ($\beta_{K+1}=1, \beta_{K+2}=\alpha, \cdots, \beta_{K+n}=\alpha^{n-1}$) with the property that every integer of $Q(\alpha)$ can be written as a linear combination, with integer coefficients, of β's. Let M_0 be the matrix of ordinary integers with $K+n$ rows and n columns which has one row for each β and has in the row corresponding to β_i the n integers obtained by multiplying the coefficients of β_i by N. The required basis of ω's will be constructed by operating on the rows of M_0. Let d_1 be the greatest common divisor of the integers in the first column of M_0. Then d_1 can be expressed as a linear combination, with integer coefficients, of entries in the first column of M_0. Therefore there is a row matrix which is equal to a linear combination of the rows of M_0 and which has d_1 as its first entry. Let M_1 be the matrix of integers with $K+n+1$ rows and n columns obtained by putting this row matrix as a new row at the top of M_0 and by subtracting a multiple of this row from each of the $K+n$ rows below it in order to make the first entry in every row after the first row zero. Then each row of the original matrix M_0 can be expressed as a linear combination of the rows of the new matrix M_1 and, conversely, the rows of M_1 are combinations of the rows of M_0.

Construct $M_2, M_3, \cdots, M_n$ successively as follows. M_{i-1} has the property that after the first $i-1$ rows all entries in the first $i-1$ columns are zero. Let d_i be the greatest common divisor of the entries in the i^{th} column below the first $i-1$ rows. (If these entries are all zero – which in the present case they will not be – set $d_i=0$.) Then there is a row matrix which is a linear combination of the rows of M_{i-1} after the first $i-1$ and which has 0 in its first $i-1$ columns, d_i in its i^{th} column. Insert this row matrix as the i^{th} row of the new matrix – between the old $(i-1)^{\text{st}}$ row and the old i^{th} row – and subtract a multiple of it from each succeeding row to make the entries below d_i all 0. (If $d_i=0$ take this row to be the trivial linear combination, that is, all zeros.) This new matrix is M_i. At each stage, all rows of M_{i-1} can be expressed as linear combinations (always with integer coefficients) of the rows of M_i and conversely.

The process terminates with a matrix M_n such that all rows of M_0 can be expressed as linear combinations of rows of M_n and conversely. Since all rows of M_n after the n^{th} are entirely zero, this means that all rows of M_0 can be expressed as linear combinations of these first n rows of M_n. Let (b_{ij}) be the coefficients of these first n rows and let $\omega_i=(b_{i1}+b_{i2}+\cdots+b_{in}\alpha^{n-1})/N$. Then, since every integer is a linear combination of β's, every integer is a linear combination of ω's. The ω's are integers because they are linear combinations of β's. It remains to show that the representation of an integer as a linear combination of the ω's is unique. This amounts to showing that the matrix of coefficients

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

One further theorem about the integers of $Q(\alpha)$ will be necessary in what follows. The fact that KUMMER's theory could not be generalized to $Z[\sqrt{-3}]$ was shown in the last section by showing that there were elements a, b, c *of* $Z[\sqrt{-3}]$ (namely, $a=2^3$, $b=1+\sqrt{-3}$, $c=2$) with the property that c^k divides ab^k for all k but c does not divide b. It is clear from this proof that, in the same way, KUMMER's theory cannot be generalized to any ring in which there exist such a, b, c with $a \neq 0$. Therefore it is essential that the ring of integers of $Q(\alpha)$ *not* contain such a, b, c. This is a basic theorem of the theory.

Theorem. Let a, b, c be integers of $Q(\alpha)$ with the properties that $a \neq 0$ and ab^k/c^k is an integer for all k. Then b/c is an integer.*

6. Dedekind's first version

Once the importance of the notion of "integer" has been recognized, the generalization of KUMMER's theory to the ring of integers of an arbitrary** algebraic number field K is not difficult. This was first*** done by RICHARD DEDEKIND in 1871 in a supplement to the second edition [3] of his version of DIRICHLET's *Vorlesungen über Zahlentheorie.*

(b_{ij}) has nonzero determinant, and this follows immediately from the fact that the last n rows of M_0, which constitute N times the $n \times n$ identity matrix, can all be expressed as linear combinations of the rows of (b_{ij}) – that is, the linear map defined by (b_{ij}) is onto and therefore must be one-to-one.

* **Proof** (DEDEKIND [3, §163, 4]). Note first that there are a finite number of classes of integers of $Q(\alpha)$ mod a. To prove this, let $a^j + A_1 a^{j-1} + \cdots + A_0 = 0$ where the A's are in Z. Then clearly a divides A_0. Moreover, it can be assumed that A_0 is nonzero, since otherwise the equation satisfied by a could be divided by a to give an equation of lower degree. Now two integers $\alpha = h_1\omega_1 + \cdots + h_n\omega_n$, $\beta = k_1\omega_1 + \cdots + k_n\omega_n$ represented in terms of an integral basis $\omega_1, \omega_2, \cdots, \omega_n$ are congruent mod A_0 if and only if $h_i \equiv k_i \bmod A_0$ for $i = 1, 2, \cdots, n$. This shows that there are exactly A_0^n congruence classes of integers mod A_0. Since integers that are congruent mod A_0 are also congruent mod a, there are at most A_0^n congruence classes mod a. Therefore the sequence of integers $a, ab/c, ab^2/c^2, \cdots$ must contain two integers that are congruent mod a. Thus there must be integers $k > j > 0$ such that $(ab^k/c^k) - (ab^j/c^j)$ is divisible by a. Let γ be the quotient. Then, if $x = b/c$, the equation $x^k - x^j - \gamma = 0$ holds. That is, x satisfies a monic equation whose coefficients are algebraic integers, and the desired conclusion that x is an integer follows from DEDEKIND's theorem above.

** The theory of algebraic integers was developed in the preceding section for the case of a field of the form $Q(\alpha)$. That the theorems apply equally well to arbitrary algebraic number fields follows either from the theorem of the primitive element (every finite field extension can be obtained by the adjunction of a single element) or from minor modifications of the proofs of the preceding section.

*** Six years earlier, a generalization of KUMMER's theory to *normal* algebraic number fields was published [37] by EDUARD SELLING, a former student of DEDEKIND. This paper is mentioned by DEDEKIND [3, note to §163] and also by ORE in his notes to DEDEKIND's *Werke* [2, vol. 1, p. 230]. Neither of these writers raises any objections to SELLING's theory, and ORE even endorses it, so that it might seem that the priority belongs to this otherwise unknown mathematician. However, as BOURBAKI points out [1 b, p. 128] SELLING's theory must be dismissed as nonsense. His definition of ideal prime factors is unacceptable even in the easy cases where the defining polynomial does not have multiple factors mod p, because it is based on the use of congruences of the form

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

Let K be a given number field as in the previous section. The problem is to define "ideal prime factors" of integers of K in such a way that the basic properties KUMMER enumerated (see the end of Section 3) are valid. In KUMMER's theory, ideal prime divisors are described by *divisibility tests* of the form $\beta\Psi \equiv 0 \bmod p$, where Ψ is a certain cyclotomic integer, where $p \in Z$ is an ordinary prime integer, and where an arbitrary cyclotomic integer β is said to be divisible by the ideal prime factor of p corresponding to Ψ if the congruence $\beta\Psi \equiv 0 \bmod p$ is satisfied. Ideal prime factors can be defined in exactly the same way in the general case.

Given a prime $p \in Z$, what integers $\Psi \in K$ can be regarded as defining tests for divisibility by ideal prime factors of p? Clearly one must assume $\Psi \not\equiv 0 \bmod p$ (otherwise 1 would be divisible) and one must assume that the ideal factor is *prime*, that is, that it divides a product $\beta\gamma$ only if it divides one of the factors β or γ. As will be shown below, these two conditions are all one needs to assume about Ψ:

Definitions. Let a number field K be given and let $p \in Z$ be prime. Then (Ψ, p) will be said to *represent an ideal prime factor of* p if Ψ is an integer of K which satisfies the two conditions

$$\Psi \not\equiv 0 \bmod p$$

(that is, Ψ/p is not an integer of K) and

If β and γ are integers of K such that $\beta\gamma\Psi \equiv 0 \bmod p$ then either $\beta\Psi \equiv 0 \bmod p$ or $\gamma\Psi \equiv 0 \bmod p$.

When Ψ satisfies these conditions, an integer β of K will be said to be *divisible μ times* by the ideal prime factor of p represented by (Ψ, p), denoted $\beta \equiv 0 \bmod (\Psi, p)^\mu$, if $\beta\Psi^\mu \equiv 0 \bmod p^\mu$. Given two Ψ's, say Ψ_0 and Ψ_1, that satisfy the conditions, (Ψ_0, p) and (Ψ_1, p) will be said to *represent the same ideal prime factor of* p if every β divisible by one is also divisible by the other.

These definitions, which are natural generalizations of KUMMER's, are all that are necessary to generalize KUMMER's theory to an arbitrary number field K. The remainder of this section is devoted to proving that all the expected properties of factorization into ideal primes (see Section 3) hold. The proofs are, in essence, the ones given by DEDEKIND in 1871 in the second edition of DIRICHLET's *Vorlesungen*.

To begin, two points about the definition of multiplicities need to be clarified:

$f(j) \equiv 0 \bmod q^\mu$ for successive values of $\mu = 1, 2, 3, \ldots$, where q is a prime, where j is the generator of a finite field, and where $f(j)$ is a polynomial in j. Now $f(j)$ must be interpreted as an element of a finite field, but, in such a field, congruence $\bmod q^\mu$ is always trivial, and in particular, is independent of μ. More specifically, if q is the characteristic of the finite field that j generates (which is probably what SELLING intends, though it is unclear why he switches from p to q) then $f(j) \equiv 0 \bmod q^\mu$ means $f(j) = 0$, a condition that is independent of μ, and if q is not the characteristic then q^μ is a unit in the field and $f(j) \equiv 0 \bmod q^\mu$ imposes no condition at all on $f(j)$. The fact that DEDEKIND does not mention SELLING in his later works, and that KRONECKER and other writers do not refer to him at all, may indicate that it was generally recognized that SELLING's theory was invalid, but there is no indication of this in DEDEKIND's letter of 1877 to SELLING [12, pp. 160–161] or elsewhere.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

(1) If β is a nonzero integer of K and if (Ψ, p) represents an ideal prime factor of p then there is a nonnegative integer ν such that β is divisible *exactly* ν times by (Ψ, p) in the sense that it is divisible μ times, as defined above, for all $\mu \leqq \nu$ but for no $\mu > \nu$. (2) If (Ψ_0, p) and (Ψ_1, p) define the same ideal prime factor of p and if β is any integer of K then the exact multiplicity with which (Ψ_0, p) divides β is the same as the exact multiplicity with which (Ψ_1, p) divides β.

These statements can be proved as follows. Let β and (Ψ, p) be given. Since $\Psi \not\equiv 0 \bmod p$ and $\beta \neq 0$, Ψ/p is not an integer and, by the theorem of the preceding section, $\beta\Psi^k/p^k$ cannot be an integer for all k. Thus there is an integer $\nu \geqq 0$ such that $\beta\Psi^\nu \equiv 0 \bmod p^\nu$ but $\beta\Psi^{\nu+1} \not\equiv 0 \bmod p^{\nu+1}$. Let γ be the integer $\beta\Psi^\nu/p^\nu$. If $\mu \leqq \nu$ then

$$\left(\frac{\beta\Psi^\mu}{p^\mu}\right)^\nu = \frac{\beta^\nu\Psi^{\mu\nu}}{p^{\mu\nu}} = \frac{\beta^{\nu-\mu}(\beta\Psi^\nu)^\mu}{p^{\mu\nu}} = \beta^{\nu-\mu}\gamma^\mu.$$

Thus $\beta\Psi^\mu/p^\mu$ satisfies the equation $X^\nu - \delta = 0$ where δ is the integer $\beta^{\nu-\mu}\gamma^\mu$. As was shown in the preceding section, this implies that $\beta\Psi^\mu/p^\mu$ is an integer, as was to be shown. By the same token, if $\mu > \nu$ then $\beta\Psi^\mu/p^\mu$ cannot be an integer, because if it were then the statement just proved would imply that $\beta\Psi^\sigma/p^\sigma$ was an integer for all $\sigma \leqq \mu$, and in particular for $\sigma = \nu+1$, contrary to the choice of ν. This proves (1).

For the proof of (2) it is useful to notice first that from (1) it follows easily that multiplicities combine in the expected way, that is, if (Ψ, p) divides β with multiplicity exactly ν and β' with multiplicity exactly ν' then it divides $\beta\beta'$ with multiplicity exactly $\nu+\nu'$. To prove this, let $\gamma = \beta\Psi^\nu/p^\nu$ and $\gamma' = \beta'\Psi^{\nu'}/p^{\nu'}$. Then $\beta\beta'\Psi^{\nu+\nu'} = \gamma\gamma' p^{\nu+\nu'}$, so $\beta\beta'$ is divisible $\nu+\nu'$ times by (Ψ, p). It is not divisible $\nu+\nu'+1$ times because if it were then $\beta\beta'\Psi^{\nu+\nu'+1} = \gamma\gamma'\Psi p^{\nu+\nu'}$ would be divisible by $p^{\nu+\nu'+1}$ and $\gamma\gamma'\Psi$ would be divisible by p; this would mean that (Ψ, p) divided $\gamma\gamma'$ and therefore, because (Ψ, p) is prime, that γ or γ' was divisible by (Ψ, p) which is impossible because if, for example, p divided $\gamma\Psi$ then $p^{\nu+1}$ would divide $\beta\Psi^{\nu+1} = \gamma p^\nu \Psi$, contrary to assumption.

Now for the proof of (2) let (Ψ_0, p) and (Ψ_1, p) represent the same ideal prime factor of p, let β be a nonzero integer of K and let ν_i be the exact multiplicity with which (Ψ_i, p) divides β ($i = 0$ or 1). It is to be shown that $\nu_0 = \nu_1$. Let μ_i denote the function which assigns to nonzero integers of K the exact multiplicity with which they are divisible by (Ψ_i, p). Let $\gamma = \beta\Psi_0^{\nu_0}/p^{\nu_0}$ and take μ_1 of $\gamma p^{\nu_0} = \beta\Psi_0^{\nu_0}$ to find $\mu_1(\gamma) + \nu_0\mu_1(p) = \mu_1(\beta) + \nu_0\mu_1(\Psi_0)$. Now $\mu_1(\gamma) = 0$ since otherwise γ would be divisible by (Ψ_1, p), and therefore by (Ψ_0, p), and divisibility of γ by (Ψ_0, p) would imply $\gamma\Psi_0 \equiv 0 \bmod p$, $\gamma\Psi_0 p^{\nu_0} = \beta\Psi_0^{\nu_0+1} \equiv 0 \bmod p^{\nu_0+1}$, contrary to the definition of ν_0. Since $\mu_1(\beta) = \nu_1$, this gives $\nu_1 = \nu_0[\mu_1(p) - \mu_1(\Psi_0)]$. By symmetry, $\nu_0 = \nu_1[\mu_0(p) - \mu_0(\Psi_1)]$. If $\nu_1 = 0$ then the second equation gives $\nu_0 = 0 = \nu_1$. If $\nu_1 > 0$ the the first equation gives $\nu_0 > 0$ and $\nu_0 \geqq \nu_1$; in this case, the second equation gives $\nu_1 \leqq \nu_0$ and $\nu_1 = \nu_0$ in all cases, as was to be shown.* (Note that it then follows that $\mu_1(p) - \mu_1(\Psi_0) = 1$ in all cases – that is, p is divisible by (Ψ_0, p) exactly one more time than Ψ_0 is.)

* DEDEKIND's original proof of this theorem [3, §163, 4] is inadequate, as he himself pointed out in a publication in early 1873 [2, vol. 3, p. 419].

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

One of the properties enumerated by KUMMER is specific to the cyclotomic integers, namely, the statement that if p has exponent $f \bmod \lambda$ and if β is a cyclotomic integer which is divisible m times by ideal prime factors of p (which may or may not be distinct) then the norm of β is divisible by p exactly mf times. This does not, of course, apply in the general case. However, the main importance of this property is the fact that it implies the following property in KUMMER's list, namely, the statement that *a nonzero integer is divisible by a finite number of distinct ideal prime factors.* This does hold in the general case, as can be proved as follows.

Let β be a given nonzero integer. Then β satisfies an equation of the form $\beta^k + a_1\beta^{k-1} + \cdots + a_k = 0$, where the a's are ordinary integers. Clearly, then, β divides a_k. Since every ideal prime factor which divides β also divides a_k, it will suffice to show that *an ordinary nonzero integer is divisible by at most a finite number of ideal prime factors.* Let $m \in Z$, $m \neq 0$. If $p \in Z$ is a prime which does not divide m then there exist integers i and j such that $im + jp = 1$. If an ideal prime factor of p divided m then $\Psi = im\Psi + jp\Psi$ would be $\equiv 0 \bmod p$, contrary to assumption. Therefore m can be divisible by an ideal prime factor of p only if p divides m. Since m is divisible by a finite number of primes p it suffices to prove that each prime $p \in Z$ is divisible by a finite number of ideal prime factors. Clearly if (Ψ, p) and (Ψ', p) represent ideal prime factors of p and if $\Psi \equiv \Psi' \bmod p$ then (Ψ, p) and (Ψ', p) represent the same ideal prime factor of p. Therefore the number of distinct ideal prime factors of p is at most equal to the number of congruence classes of integers $\bmod p$. If $\omega_1, \omega_2, \cdots, \omega_n$ is an integral basis of K as in the proposition of the preceding section, then two integers $k_1\omega_1 + k_2\omega_2 + \cdots + k_n\omega_n$ and $k'_1\omega_1 + k'_2\omega_2 + \cdots + k'_n\omega_n$ are congruent $\bmod p$ if and only if $k_i \equiv k'_i \bmod p$ for $i = 1, 2, \cdots, n$. Thus there are p^n congruence classes of integers $\bmod p$ and the proof is complete.

The principal step in the verification of KUMMER's properties is the proof of the following central theorem: *If an integer β of K is divisible by all ideal prime factors of p with multiplicity at least as great as the multiplicity with which they divide p then β is divisible by p.* DEDEKIND proved this very simply as follows.

Let β be an integer of K. It will suffice to show that if β is *not* divisible by a certain $p \in Z$ then there is an ideal prime factor of p which divides β with multiplicity less than the multiplicity with which it divides p. Given β and p, define a congruence relation on integers of K by defining $\gamma \equiv \delta \bmod (\beta, p)$ to mean that $\beta\gamma \equiv \beta\delta \bmod p$. It is easy to see that congruence $\bmod (\beta, p)$ has all the expected properties of a congruence – specifically, that it is reflexive, symmetric, transitive, and consistent with addition and multiplication. Moreover, $1 \not\equiv 0 \bmod (\beta, p)$. If it is *prime*, that is, if $\gamma\delta \equiv 0 \bmod (\beta, p)$ implies either $\gamma \equiv 0$ or $\delta \equiv 0 \bmod (\beta, p)$ then (β, p) itself represents, according to the above definition, an ideal prime factor of p. In this case it was shown above that (β, p) divides p with multiplicity one greater than the multiplicity with which it divides β and an ideal prime factor of the desired type has been found.

Assume, therefore, that congruence $\bmod (\beta, p)$ is *not* prime. Let γ and δ be integers of K such that $\gamma \not\equiv 0$, $\delta \not\equiv 0 \bmod (\beta, p)$ but $\gamma\delta \equiv 0 \bmod (\beta, p)$, and let $\beta' = \beta\gamma$. It will suffice to construct an ideal prime factor of p which divides

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

β' with multiplicity less than the multiplicity with which it divides p because from $\beta' = \beta\gamma$ it follows that it divides β with multiplicity no greater than it divides β'. Since $\beta' \not\equiv 0 \bmod p$ (because, by the choice of γ, $\beta\gamma \not\equiv 0 \bmod p$) this is the original problem with β replaced by β'.

If congruence $\bmod(\beta', p)$ is prime then (β', p) represents an ideal prime factor of p with the desired property. Otherwise one can repeat the process above, of choosing γ' and δ' such that $\gamma' \not\equiv 0$, $\delta' \not\equiv 0 \bmod(\beta', p)$ but $\gamma'\delta' \equiv 0 \bmod(\beta', p)$, and of setting $\beta'' = \beta'\gamma'$. It will suffice to show that repetition of this process must eventually result in an integer $\beta^{(\nu)}$ such that congruence $\bmod(\beta^{(\nu)}, p)$ is prime, since then $(\beta^{(\nu)}, p)$ represents an ideal prime factor of p with the desired property.

To show that the process terminates, it suffices to show that the number of congruence classes $\bmod(\beta, p)$ is finite to begin with and decreases at each step. As was observed above, the number of congruence classes $\bmod p$ is p^n. Since congruence $\bmod p$ implies congruence $\bmod(\beta, p)$, this shows that the number of congruence classes $\bmod(\beta, p)$ is at most p^n. (Note, by the way, that this means that the determination of whether congruence $\bmod(\beta, p)$ is prime involves checking only a finite number of possible classes for γ and δ.) The number of classes $\bmod(\beta', p)$ is strictly *less* than the number of classes $\bmod(\beta, p)$ because congruence $\bmod(\beta', p)$ implies congruence $\bmod(\beta, p)$ but there are two integers, namely, δ and 0, which are congruent $\bmod(\beta', p)$ but not $\bmod(\beta, p)$. Therefore the process must terminate with an ideal prime factor of p with the desired property and the proof is complete.

In the general case the theorem above states that *if β and γ are integers of K and if every ideal prime factor that divides γ also divides β with multiplicity at least as great, then γ divides β*, that is, β/γ is an integer. The general case can be proved by a modification of the argument used above for the case $\gamma = p$ and DEDEKIND in fact gave the argument in the general case. On the other hand, the general case follows easily from the special case as follows.

Consider first the case in which γ is an ordinary integer, say $\gamma = m$. Let p be any prime in Z which divides m, say $m = m'p$. Since every ideal prime factor of p divides m with multiplicity at least as great, they also divide β with multiplicity at least as great (by assumption). Therefore, by the case $\gamma = p$ already proved, p divides β, say $\beta = \beta' p$. This reduces the division of β by m to the division of β' by m'. By the way in which multiplicities combine, it is clear that every ideal prime factor that divides m' divides β' with multiplicity at least as great. Therefore the process can be repeated and a prime p' can be removed from m' and β'. Eventually m is reduced in this way to 1 and the case $\gamma = m$ is proved.

Finally, let γ be any integer of K. As was noted above, there is an ordinary integer which is divisible by γ, say $m = \gamma\delta$ where $m \in Z$, $m \neq 0$, and δ is an integer of K. The assumption that every ideal prime factor of γ divides β with multiplicity at least as great implies that the same is true of $\gamma\delta$ and $\beta\delta$. Since $\gamma\delta = m$, this implies, as was just shown, that m divides $\beta\delta$, say $\beta\delta = m\zeta$ where ζ is an integer of K. Then $\beta\delta = \gamma\delta\zeta$, so that $\beta = \gamma\zeta$ and γ divides β, as was to be shown.

The remaining properties of the theory of ideal prime factors enumerated

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

by KUMMER can all be deduced very easily from those that have already been proved. This completes the generalization of KUMMER's ideal prime factors to arbitrary algebraic number fields. Thus the problem of generalizing the theory was solved by DEDEKIND in 1871. However, as the remainder of this paper shows, this is far from the end of the story. There were still many years of struggle over the proper way to formulate and establish the theory, a process in which DEDEKIND himself made major changes in his approach.

7. Dedekind's point of view. Ideals

In order to show the connection between KUMMER's work and DEDEKIND's, the point of view adopted in the preceding section was that of KUMMER's first announcement of his theory in 1846 rather than the one that DEDEKIND took in 1871. The central feature of KUMMER's point of view is the description of ideal prime factors in terms of *divisibility tests*. Although DEDEKIND's proofs can be recast in this language – and this is what was done above – his actual formulation of the theory in terms of his new conception of "ideals" was quite different.

One feature of KUMMER's formulation was avoided above, however, and it is the one that was the most striking to KUMMER's contemporaries – ideal complex numbers. KUMMER very carefully defines the notion of divisibility by ideal prime factors and sets forth the properties of the resulting theory (for the case of cyclotomic integers with prime exponent) in almost exactly the same terms that were used above. However, at the very beginning of his announcement, as well as in the parts after the discussion of ideal prime factors, he speaks of ideal complex *numbers* without saying what he meant by this. What he seems to have meant (see especially the third paragraph of §8 of [31] – Collected Papers, vol. 1, top of p. 234) is simply *a product of ideal prime factors.** Perhaps his most explicit statement about ideal complex numbers is the following rather peculiar one:

"Because ideal complex numbers, as factors of complex numbers, play the same role as actual factors, we will denote them from now on in the same way as these, by $f(\alpha)$, $\phi(\alpha)$, etc., in such a way that $f(\alpha)$, for example, will be a complex number satisfying a certain determined number of characteristic conditions for ideal prime factors, except for [the condition of the] existence of the number $f(\alpha)$." [32, §VI.]†

One need not be deeply concerned with the foundations of mathematics to be unhappy with such a formulation. DEDEKIND, of course, had a lifelong interest in the foundations, and he published two major works on the subject. For him, KUMMER's vaguely defined notion of ideal complex numbers was

* For a discussion of the drawbacks of this terminology see [16], pp. 142–143.

† Puisque les nombres complexes idéaux, comme facteurs des nombres complexes, jouent le même rôle que les facteurs existants, nous les désignerons désormais de la même manière que ceux-ci, par $f(\alpha)$, $\phi(\alpha)$, etc., en sorte que $f(\alpha)$ par exemple, sera un nombre complexe, satisfaisant à un certain nombre déterminé de conditions caractéristiques pour les facteurs premiers idéaux, abstraction faite de l'existence du nombre $f(\alpha)$.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

profoundly disquieting, and he was almost as concerned with giving a satisfactory definition of this notion as he was with extending it to number fields other than cyclotomic fields.

DEDEKIND was also dissatisfied with KUMMER's method of introducing the ideal prime factors themselves. Although he conceded that KUMMER's formulation was legitimate,* he objected to the fact that it depended on a particular explicit representation of the factor – to wit the integer Ψ which defined the divisibility test but was subject to arbitrary choices – rather than being based on *intrinsic properties* of the factors. In this connection, he cited** the example of RIEMANN's approach to the theory of functions, which avoided explicit representations of functions and instead based the study of them on their essential properties.†

In order to base his definition of KUMMER's ideal complex numbers on intrinsic properties, DEDEKIND proceded as follows. The essential property of an ideal complex number is the property of dividing, or not dividing, an actual complex number. Thus one knows all about an ideal complex number if one knows which actual complex numbers (algebraic integers) it divides. DEDEKIND therefore considers *the set of all integers of*†† *K that are divisible by a given product of ideal prime factors* as representative of that product of ideal prime factors (which is one of KUMMER's ideal complex numbers). Such a subset of the integers of K he calls an *ideal.*††† This replaces the problem of defining ideal complex numbers with the problem of defining ideals. He solved this problem very simply and elegantly by finding two properties which characterize them.

Definitions. A subset A of the integers of K is called an *ideal* if it has the properties:

---

* See [4], especially p. 268 and p. 296 of volume 3 of DEDEKIND's *Werke*.

** See, for example, the Preface to the second edition of *Zahlentheorie* (1871), where he says "... I hope that the striving after characteristic basic properties, which in other parts of mathematics has been crowned with such fine success, will not have failed me entirely." That he was thinking here of RIEMANN's principles in the theory of functions is attested to by a statement toward the end of Section 5 of [10] where he refers to "RIEMANN's definition of functions by inner, characteristic properties, from which the forms for representing them spring by necessity" and by the letter of 10 June 1876 to LIPSCHITZ in which he also refers in this connection to "RIEMANN's principles" as his sole example [2, vol. 3, p. 469].

† It may be worth noting that RIEMANN in this way advanced the theory of hypergeometric functions, to which KUMMER had made important contributions.

†† In a discussion of DEDEKIND's philosophy of mathematics, it must be pointed out that the idea of having a single, coordinate-free letter such as K to represent the set of all elements of the field under discussion – as opposed to a notation such as $Q(\alpha)$ that suggests a particular basis for the field – was original with DEDEKIND and stemmed very naturally from his point of view. In fact, in his letter of 10 June 1876 to LIPSCHITZ, he says that in his new exposition [4] of the theory he "mars" (*verunziere*) the concept of a number field in that he introduces it in the form $Q(\alpha)$ where α is the root of an irreducible equation with rational coefficients.

††† This choice of terms has always seemed bizarre to me.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

I. If $\beta, \gamma \in A$ then $\beta \pm \gamma \in A$.

II. If $\beta \in A$ and γ is an integer of K then $\beta\gamma \in A$.

Thus the set of all integers of K is an ideal, as is the set consisting of 0 alone. An ideal is said to be *prime* if it is neither all integers nor 0 alone, and if it has the property:

III. If $\beta\gamma \in A$ then either $\beta \in A$ or $\gamma \in A$.

Finally, an *ideal complex number** (to use KUMMER's terminology) associated with the field K is a formal finite product of ideal prime factors; that is, it is a finite list (possibly empty) of ideal prime factors, with a finite multiplicity assigned to each.

Given an ideal complex number, the set of all integers of K that are divisible by it is obviously an ideal. This establishes a mapping from ideal complex numbers to ideals.

Theorem. The natural mapping from ideal complex numbers to ideals is one-to-one and onto, except that the ideal $\{0\}$ corresponds to no ideal complex number.

The main assertion of the theorem is that an ideal is uniquely determined by the ideal prime factors that divide its elements and specifically that if A is an ideal and $x \notin A$ then there is an ideal prime factor which divides all elements of A with multiplicity greater than that with which it divides x. The proof of this fact given in the note** below is, in essence, to be found in DEDEKIND [3, §163, 5], although in quite different form.

---

* Such an object is usually called a *divisor* today.

** **Proof.** A crucial fact used in the proof is that *if P_1 and P_2 are prime ideals and if $P_1 \subset P_2$ then $P_1 = P_2$*. Otherwise stated, if P_1 and P_2 are distinct prime ideals then neither $P_1 \subset P_2$ nor $P_2 \subset P_1$ so that there is an element of P_1 not in P_2 and vice versa. To prove this, consider the relation of "congruence mod P_1" defined for integers β, γ of K by $\beta \equiv \gamma \bmod P_1$ if and only if $\beta - \gamma \in P_1$. It follows from properties I and II that congruence mod P_1 is a congruence relation (reflexive, symmetric, and transitive) which is consistent with addition and multiplication (if $\beta \equiv \gamma$ then, for all δ, $\beta + \delta \equiv \gamma + \delta$ and $\beta\delta \equiv \gamma\delta$). *The number of classes* mod P_1 *is finite*, because some $k \in Z$ must belong to P_1 (choose any nonzero $\beta \in P_1$ and take k to be any integer divisible by β – for example the constant term of an equation which shows that β is an integer); then congruence mod k implies congruence mod P_1 and, because two integers of the form $h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n$ are congruent mod k if and only if all the h_i's are congruent mod k, this implies that there are at most k^n classes mod P_1. Suppose that $\sigma \in P_2$ but $\sigma \notin P_1$. Then $\sigma \not\equiv 0 \bmod P_1$. Multiplication by $\sigma \bmod P_1$ carries nonzero classes mod P_1 one-to-one to nonzero classes mod P_1 because P_1 is prime. As a one-to-one map of a finite set to itself it must also be onto. Therefore there is an integer τ of K such that $\sigma\tau$ is in the class of 1 ($1 \equiv 0 \bmod P_1$ would imply $\sigma \equiv 0 \bmod P_1$). Thus $\sigma\tau - 1 \in P_1 \subset P_2$, so that $\sigma\tau \equiv 1 \bmod P_2$. On the other hand, $\sigma\tau \equiv 0\tau \equiv 0 \bmod P_2$. Therefore $1 \equiv \sigma\tau \equiv 0 \bmod P_2$, which implies that every integer of K is $0 \bmod P_2$, contrary to assumption. Therefore there can be no such σ and $P_1 = P_2$.

Now let A be an ideal and let β be an integer of K which is not in A. The main step in the proof is to show that *there is an ideal prime factor which divides all elements of A with multiplicity greater than that with which it divides β*. For this, consider the congruence relation defined by saying that σ and τ are congruent if $\beta(\sigma - \tau) \in A$. Let this be denoted

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

Thus, ideals are isomorphic to ideal complex numbers and one can deduce the principal theorems of the theory of ideals from the theorems about ideal prime factors proved in the preceding section. This, in essence, is the procedure DEDEKIND followed in his original presentation of the theory of ideals [3, §163]. More specifically, he defined (§163, 4) *simple* prime ideals to be prime

---

$\sigma \equiv \tau \bmod (\beta, A)$. As was shown above in the case of congruence mod P_1, it is simple to show that congruence mod(β, A) is a congruence relation consistent with addition and multiplication. If $A=\{0\}$, the statement to be proved is trivial. Otherwise the number of classes mod A is finite (because A contains some $k \in Z$ as above) and *a fortiori* the number of classes mod(β, A) is finite. Moreover, $1 \not\equiv 0 \bmod (\beta, A)$. If congruence mod$(\beta, A)$ is prime, set $P=\{\delta : \delta \equiv 0 \bmod (\beta, A)\}$. Otherwise let γ and δ be integers of K such that $\gamma\delta \equiv 0 \bmod (\beta, A)$ but neither γ nor δ is $\equiv 0 \bmod (\beta, A)$. Set $\beta' = \beta\gamma$ and consider congruence mod(β', A). If this is prime, set $P=\{\delta : \delta \equiv 0 \bmod (\beta', A)\}$. Otherwise repeat the process. Since, as before, the number of congruence classes decreases at each step, the process must eventually reach a congruence relation mod$(\beta^{(\nu)}, A)$ that is prime. Let $P=\{\delta : \delta \equiv 0 \bmod (\beta^{(\nu)}, A)\}$. Then P is a prime ideal. It will be shown that P *is the ideal corresponding to an ideal prime factor* and that *this ideal prime factor divides all elements of* A *with multiplicity greater than that with which it divides* β.

It was shown above that every nonzero ideal contains some $k \in Z$. Let k be in P and let k be written as a product of primes. Since congruence mod P is prime by assumption, one of the primes p in the factorization of k must lie in P. Let $p \in P$ and let $P_1, P_2, \cdots, P_j$ be the ideals that correspond to the ideal prime factors $(\Psi_1, p), (\Psi_2, p), \cdots, (\Psi_j, p)$ of p. Then P must be equal to one of the ideals $P_1, P_2, \cdots, P_j$ since otherwise there would be elements $\sigma_1 \in P_1, \sigma_2 \in P_2, \cdots, \sigma_j \in P_j$ none of which were in P; then the integer $(\sigma_1\sigma_2\cdots\sigma_j)^N$ would, on the one hand, not be in P for any $N \in Z$, because it is a product of elements not in P, and would, on the other hand, be in P for sufficiently large N because then it is divisible by all prime divisors of p with multiplicity greater than that with which they divide p, and consequently divisible by p. This contradiction shows that P is the ideal corresponding to an ideal prime factor (Ψ, p).

Let r be the multiplicity with which (Ψ, p) divides β. It is to be shown that every element $\gamma \in A$ is divisible at least $r+1$ times by (Ψ, p). If not, let $\gamma \in A$ be divisible $\leqq r$ times by (Ψ, p). For each *other* prime divisor of γ choose an element σ in the corresponding ideal which is *not* in P. Then, if $\sigma_1, \sigma_2, \cdots, \sigma_t$ is the list of σ's obtained in this way, the element $\beta(\sigma_1\sigma_2\cdots\sigma_t)^N$ is divisible by γ for sufficiently large N. Since $\gamma \in A$ and β divides $\beta^{(\nu)}$, this implies $\beta^{(\nu)}(\sigma_1\sigma_2\cdots\sigma_t)^N \equiv 0 \bmod A$, that is, $(\sigma_1\sigma_2\cdots\sigma_t)^N \equiv 0 \bmod P$, contrary to the fact that the σ's are not in P and P is prime. Therefore, there is no such γ in A and all elements of A are divisible $r+1$ times, at least, by (Ψ, p).

Let A be an ideal other than $\{0\}$. The main statement of the theorem is that A is the ideal corresponding to some ideal complex number. Let $k \in Z$ be an ordinary integer in A, and let $x_1, x_2, \cdots, x_m$ be the list of the congruence classes mod k which contain elements of A. (For this proof to be constructive one must make the mild assumption that A is given in some explicit enough form that one can determine, for a given class mod k, whether it contains an element of A.) Then clearly each $x \subset A$. In each x choose an integer σ of K so that the list $\sigma_1, \sigma_2, \cdots, \sigma_m$ contains a complete set of representatives of A mod k. For each ideal prime factor (Ψ_i, p_i) that divides k, let μ_i be the minimum multiplicity with which (Ψ_i, p_i) divides an entry in the list $k, \sigma_1, \sigma_2, \cdots, \sigma_m$. Then the ideal complex number $\Pi(\Psi_i, p_i)^{\mu_i}$ is the *greatest common divisor* of A in the sense that it divides all elements of A and if it is multiplied by one more ideal prime factors then it no longer has this property. Thus A is contained in the ideal corresponding to $\Pi(\Psi_i, p_i)^{\mu_i}$. It is to be shown that A is *equal* to this ideal, and this follows immediately from what was

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

ideals P for which there is a pair of integers (ν, μ) in K such that P consists of all integers σ in K for which $\nu\sigma \equiv 0 \bmod \mu$. (In the treatment above, consideration was restricted – as may be done without loss of generality – to simple ideals of the special form $(\nu, \mu) = (\Psi, p)$, that is, where μ is a prime $p \in Z$.) Then his *main theorem* (§163, 5) states that if η and μ are two integers and if every *simple* prime ideal which divides μ divides η with multiplicity at least as great then μ divides η. This is the main theorem of Section 6 above. From it he draws all the consequences needed to express the theory in terms of ideals, the first such consequence being the statement that *every prime ideal is simple.*

8. Critique of Dedekind's point of view

DEDEKIND's influence on modern views of the foundations of mathematics is indisputably very great. The set-theoretic approach to defining basic concepts is a characteristic feature of contemporary mathematics whose "birthplace" PIERRE DUGAC [12, p. 29] has said is to be found in precisely the treatise under discussion, DEDEKIND's Supplement X to his second edition of DIRICHLET's *Zahlentheorie.* Indeed, despite the fact that DEDEKIND defines an ideal as a "system" of algebraic integers rather than a "set", the set-theoretic point of view is unmistakable and appears here well before the work of DEDEKIND's colleague CANTOR on this subject, and even before his own famous essay "Stetigkeit und irrationale Zahlen" (1872), in which he first gave his definition of real numbers in terms of "cuts". Furthermore, as DEDEKIND makes clear in a lengthy footnote to his treatise *Sur la théorie des nombres entiers algébriques* (Werke, 3, p. 269), his definition of "ideals" was very closely linked in his mind to the DEDEKIND cut definition of real numbers, so that this theory of ideals (in 1871) can surely be regarded as the first appearance of the set-theoretic approach that was later to become so influential.

Despite the important impact that DEDEKIND's thinking had on views of the foundations of mathematics, in the specific case of the theory of ideal factorization of algebraic integers, his approach has many drawbacks. As was seen above, his method of proof of the fundamental theorem was to introduce temporarily *simple* ideals that are essentially the same as KUMMER'S "ideal

---

proved above, because if $\beta \notin A$ then there is some (Ψ_i, p_i) for which μ_i is greater than the multiplicity with which (Ψ_i, p_i) divides β.

Finally, it remains to be shown that different ideal complex numbers correspond to different ideals. For this, let Π_1 and Π_2 be ideal complex numbers and let (Ψ, p) be an ideal prime factor which divides them with different multiplicities – say it divides Π_1 fewer times. For each other prime factor of Π_1 choose σ_j divisible by that prime factor but not by (Ψ, p). Choose an integer β of K that is divisible exactly as many times by (Ψ, p) as Π_1 is. (Given an ideal prime factor (Ψ, p) and an integer $\mu \geqq 0$ it is easy to find an integer β of K that is divisible exactly μ times by (Ψ, p). For this it suffices, since p^N is divisible as many times by (Ψ, p) as one wants when N is large, to note that if β_1 is divisible exactly ν times for $\nu \geqq 1$ then $\beta_1 \Psi/p$ is divisible exactly $\nu - 1$ times.) Then $\beta(\Pi\sigma_j)^N$ can never be divisible by Π_2 because it is not divisible by (Ψ, p) enough times, but for sufficiently large N it is divisible by Π_1. Therefore Π_1 and Π_2 correspond to different ideals, as was to be shown.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

prime factors" and are represented in a specific way, to prove the theorem, and only then to show that every prime ideal is simple.

He later said* that he had for many years failed in his efforts to find a generalization of KUMMER's theory that was valid in all cases, and it was only when** he based his approach on the conception of ideals that he succeeded. It may well be that his abandonment of his earlier approach – which was based on the theory of higher congruences – played a role in his success, but is is hard to see how the notion of ideals could have been a contributing factor in view of the fact that it had to be circumvented in the proof of the main theorem. What seems much more likely is that it was the crucial notion of *algebraic integer* which had been lacking in his earlier work† and, perhaps, that emphasis on the notion of ideals led him to deal more carefully with the set of integers within which the ideals lie.

Certainly there can be no quarrel with DEDEKIND's emphasis on fundamental properties of mathematical objects as opposed to particular representations of them. In this he was following not only RIEMANN, as he said, but also DIRICHLET. However, before one throws out the representations one must be sure one has extracted from them all the essential properties of the objects they represent. As KUMMER already recognized in his first presentation of his theory (see Section 3, above), the *multiplicities*†† are of crucial importance and it is not enough merely to know which elements are divisible by an ideal prime, that is, it is not enough to know the ideal.

Surely the most important criterion in judging the merit of an approach to a subject is the extent to which it provides insights into the subject and makes it seem natural and clear. In this regard, DEDEKIND made some very damaging comments about his own approach in his letter to LIPSCHITZ dated 29 April 1876, mentioned in the note above. In arguing that an exposition of the theory should include complete proofs of all theorems, he says, "Although the desired goal lay clearly ahead of me at all times, it was still only after inexpressible efforts that I succeeded in moving forward step by step and finally filling all the gaps; I continually had the feeling that I was hanging from a ladder, that I might not succeed in reaching the next rung, and if I did not have before me now in published or written form my presentation of the theory from that time it would give me great difficulty all over again to put

---

* Introduction to *Sur la Théorie des Nombres entiers algébriques* [4], Werke, 3, p. 268.

** In an unpublished draft [5, p. 19] of his Introduction to the treatise cited in the preceding note, DEDEKIND said that it was in August 1870 that he "reached the fundamental concept of an ideal."

† There is a suggestion of this in a passage from DEDEKIND's letter of 29 April 1876 to LIPSCHITZ: "The difficulties, which I had to overcome six years ago in creating this general theory [of ideals] without exception, stem, in my opinion, from the fact that alongside this theory, which embraces *all* the integers of a given field, there are always infinitely many theories that are encumbered with exceptions [because they] ... deal only with *part* of the integers." [2, 3, p. 465]

†† In modern terms, the *valuation* corresponding to a prime ideal, not just the prime ideal, is essential. As WEIL says in his introduction to KUMMER's Collected Papers (Vol. 1, p. 5) "KUMMER constructs explicitly all the valuations of the field $Q(\alpha)$" [where $\alpha^{\lambda}=1$].

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

every little step of the proof together in the right order so that the goal would truly be reached."*

The familiarity of the set-theoretic approach today should not obscure the fact that DEDEKIND's approach was a major departure from established practice at the time. At a time when the notion of a completed infinity was far from uncontroversial, it must have been jarring to many of his readers to have DEDEKIND define his basic concept, his *Grundbegriff,* the ideal, *to be an infinite set* (or system) without any indication at all as to how that set may be generated or described.

The fact is that, in replacing the ideal prime factor (Ψ, p) with the set of all integers it divides, DEDEKIND was replacing a very explicitly defined object (in DEDEKIND's view, too explicitly defined, because the definition involves a particular representation) with a very vague one. What kinds of "systems" of integers are to be allowed as ideals? How are they to be described? Has one defined an ideal if the determination of whether a particular integer belongs to it depends on solving, say, the GOLDBACH conjecture? DEDEKIND does not address these questions at all.

It is not clear what motivated this revolutionary change. In the first presentation [3, end of §162] he said that there was no objection to KUMMER's method of presenting his ideal complex numbers and that the reformulation of the theory in the "new clothes" of ideals is motivated "solely by the fear that the adoption of the terminology that is usually used in treating *actual* numbers might at first inspire some doubt about the rigor of the methods of proof." He later wrote [4, Introduction] that the fact that every ideal corresponds to an ideal complex number** is "of the greatest importance" and that "I could only prove [it] rigorously after many fruitless efforts and after overcoming great difficulties." He went on to say that "this confirmation naturally led me to found the entire theory [of factorization of integers of K] on this simple definition, entirely freed of all obscurity and the admission of ideal numbers." This seems to substantiate that DEDEKIND's objection to ideal numbers was, even at the outset, philosophical and aesthetic and did not stem from any logical or practical difficulty with ideal complex numbers.

Finally, DEDEKIND's theory of ideals does not appear to have opened new vistas or to have led to simplifications or improvements of the theory. On the contrary, as will be seen in the next section, his later versions of the theory were, if anything, less satisfactory, and he became increasingly doctrinaire in his views after 1871. The letters to LIPSCHITZ began (29 April 1876) with an expression of delight over LIPSCHITZ's interest in the theory of ideals, but

* Obgleich damals das zu erreichende Ziel stets klar vor mir lag, so ist es mir doch erst nach wirklich unsäglichen Anstrengungen gelungen, Schritt für Schritt vorwärts zu kommen und endlich jede Lücke auszufüllen; ich hatte fortwährend das Gefühl, an einer Leiter zu hängen mit der Furcht, dass es mir nicht mehr gelingen würde, die folgende Sprosse zu erreichen, und wenn ich meine damalige Darstellung dieser Beweise nicht gedruckt oder geschrieben vor mir hätte, so würde es mir jetzt abermals eine grosse Mühe machen, alle Beweismittelchen, jedes am rechten Orte wieder so zusammenzufügen, dass das Ziel wirklich erreicht würde. [2, 3, p. 466]

** This is the main theorem of the preceding section.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

degenerated very quickly to a polemic* (27 July 1876) on DEDEKIND's views on continuity and irrational numbers, that is, on DEDEKIND cuts.

In 1894 HURWITZ published a paper [21] in which he presented a new and, he believed, much simpler approach to the theory of ideals. DEDEKIND quickly responded with his own paper [10] in which he revealed that he had himself found the same simplifying theorem, and had even published it a few years earlier in a rather out-of-the-way place [8], but for ideological reasons that he explained at some length, he felt that it violated the "unity" of the theory and he preferred the much longer version that he gave in the fourth edition of DIRICHLET-DEDEKIND (1894). A few years later, HILBERT, in his "Zahlbericht" adopted the approach via this simplifying theorem that DEDEKIND had rejected, and this approach has become the standard one.

DEDEKIND was both a great number theorist and an important thinker on foundational questions, and these two aspects of his work are closely linked. His insistence on philosphical principles was responsible for many of his important innovations. However, in the case of ideal theory, this insistence seems to have impelled him to abandon his first, very simple generalization of KUMMER's theory, and to replace it with two later formulations which were more in accord with his philosophical principles but which required much more space and technique to reach the same objective.

9. Dedekind's later versions

DEDEKIND thought that by including his new theory of ideals in the second edition of DIRICHLET's *Zahlentheorie* (1871) he would reach the widest possible audience. He was, however, bitterly disappointed in its reception. In 1876 he told a correspondent** that "for some years now I had more or less given up hope that my presentation and conception of a general theory of ideals would interest anyone at all nowadays except for myself," and the following year he told the translator of *Zahlentheorie* into Italian that it might be better to omit all of Supplement X beyond §158 from the translation because*** "I am firmly convinced that not a single person reads this presentation of my theory of ideals."

In retrospect, this fact – if it was a fact – that no one read DEDEKIND's presentation of the theory of ideals in Supplement X does not seem too surprising. The location of this sophisticated, demanding, and highly original material as the very last item in a book which is for the most part an expository and rather elementary account of classical number theory might be expected to have a discouraging effect. Inexpert readers would probably not get to the end of the book, and experts would probably not expect to find important new material in such a place and therefore would not look.

DEDEKIND, however, saw a different reason. He thought that the problem lay in the presentation itself and, specifically, in the fact that the presentation

---

* Only a portion of this letter is reproduced in [2, vol 3].

** Letter to LIPSCHITZ, 29 April 1876. [2, 3, p. 464]

*** Unpublished letter to FAIFOFER, 2 December 1877. [11]

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

was *too brief!* To the first correspondent mentioned above he went on to say* "I had thought that the inclusion of this research in DIRICHLET's *Zahlentheorie* was the surest means of gaining a larger circle of mathematicians for the cultivation of this field, and only little by little have I convinced myself that the presentation itself probably must bear the blame for the failure of this plan. I must presume that the exaggerated brevity and conciseness has frightened the reader away." Again, he told the translator the following year that he believed no one read beyond §159 because the brevity of the presentation frightened everyone away.

Naturally the remedy was to write a new and more leisurely presentation of the theory, and this is what DEDEKIND proceeded to do. The result was a lengthy treatise that was translated into French and published serially in the *Bulletin des Sciences Mathématiques* under the title *Sur la théorie des nombres entiers algébriques*. Although DEDEKIND maintained** that this version "in essence coincides" with the original version of 1871, there is a very important difference which should be pointed out.

In the original version the notion of *the product of two ideals* was introduced only at the very end, almost as an afterthought (section 6 of §163). Indeed, when the basic facts of the theory are expressed in terms of "ideal complex numbers", which in essence was the approach of the original version, there is no real need to introduce products and, if it is convenient to introduce products, then the fact that ideal complex numbers are *by definition* products of ideal prime factors means that the definition of the product of two ideal complex numbers is immediate. Of course DEDEKIND did, even in the original version, regard ideals as the main objects of study, so that it would have been unnatural for him to define the product of two ideals by going over to the corresponding ideal complex numbers, taking the product, and coming back to the corresponding ideal. Instead, he defines the product of ideals in the natural way (the product of A and B is the set of all sums of terms ab where $a \in A$ and $b \in B$) and then proves the simple theorem*** that the correspondence between ideals and ideal complex numbers carries products to products.

In the second version – and all subsequent versions – DEDEKIND proceeded very differently. He defined products of ideals early in the development of the theory and elevated to the level of "the [principal] difficulty of the theory" the proof of the fact that if A and B are ideals and if $A \subset B$ then there is

---

* [2, 3, p. 464].

** [4], vol. 1, 2nd series, p. 207.

*** Let A and B be ideals, let C be their product, and let Π_A, Π_B, and Π_C be the corresponding ideal complex numbers. It is to be shown that for every ideal prime factor P the number n_C of times that P divides Π_C is equal to the number n_A of times that it divides Π_A plus the number n_B of times it divides Π_B. Now n_C is characterized by the fact that P divides all elements of C at least n_C but divides at least one element of C *only* n_C times, and similarly for n_A and n_B. Clearly every element of C is divisible n_A+n_B times by P. On the other hand, if $a \in A$ is divisible only n_A times by P and if $b \in B$ is divisible only n_B times then $ab \in C$ is divisible only n_A+n_B times and $n_C=n_A+n_B$, as was to be shown.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

an ideal C such that $A=B\cdot C$. In 1895 he still saw* this as "the greatest difficulty in the foundation of ideal theory." In the original version this theorem did not even appear, but it is a simple consequence of theorems which did appear; if Π_A and Π_B are ideal complex numbers and if Π_B does not divide Π_A then it is simple† to construct an integer that is divisible by Π_A but not by Π_B; thus, if every integer divisible by Π_A is divisible by Π_B then $\Pi_A=\Pi_B\Pi_C$ for some ideal complex number Π_C and the desired theorem is obtained by passing to the corresponding ideals.

If one adopts DEDEKIND's point of view that the concept of "ideal" is fundamental then indeed the original version – which was, in form, as DEDEKIND himself said,†† just KUMMER's approach in "new clothes" – is unnatural, precisely because the definition of the product of two ideals does not come until the end and because, in connection with this, the *multiplicities* with which integers are divisible by a prime ideal are not defined in terms of powers of the ideal. As soon as one attempts to answer these objections, one is led to a reformulation in which DEDEKIND's "greatest difficulty" is in a very natural way the cornerstone of the theory.

If A and B are ideals and $A\subset B$ then everything "divisible by A", *i.e.*, in A, is "divisible by B" and it is natural to say then that "B divides A". On the other hand, there is a natural definition of the product of two ideals, and this implies another definiton of "B divides A", namely, that there is an ideal C such that $A=BC$. DEDEKIND's "greatest difficulty" is the proof that these two notions of divisibility are the same. Once this had been shown, the entire theory can be developed fairly easily.

However, the "greatest difficulty" is not easily overcome within DEDEKIND's framework. In the version of the theory in his French treatise *Sur la théorie ...*, which is virtually identical to the one in the third edition of DIRICHLET's** *Zahlentheorie* (1879), the development of the theory is fraught with technical difficulties that remind one of DEDEKIND's image, quoted in the previous section, of hanging from a ladder and doubting whether the next rung can be reached.

The crucial lemma (§21, 4 of *Sur la théorie...*, §171, 12 of the 3rd edition of *Zahlentheorie*) is the statement that *if A is an ideal that is divisible by a prime ideal P then there is an integer v such that* $(v)P$, the product of P and the principal ideal (v), *is the least common multiple of A and* (v). (The conclusion can be restated, once the full theory has been established, in the simpler form $P=\{\beta: v\beta\equiv 0 \bmod A\}$, which makes it seem a bit less arbitrary.) DEDEKIND's proof of this lemma depends on separating two cases, that in which A is divisible by no other prime divisor than P and the contrary case, and it is not at all illuminating.

The main application of the lemma (§25, 1 or §173, 1) is to the proof that *if P is a prime ideal then there exist an integer λ that is divisible by P*

* [10, 1].

† See the proof of the theorem of Section 7 above.

†† [3, end of §162].

** It may seem strange to refer to this book, which was published 20 years after DIRICHLET's death and contained significant new material by DEDEKIND, as DIRICHLET's, but this is how DEDEKIND himself referred to it.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

and an integer κ *that is not divisible by* P *such that* $(\kappa)P$ *is the least common multiple of* (λ) *and* (κ). (The conclusion can be restated in the form $P=\{\beta\colon \kappa\beta \equiv 0 \bmod \lambda\}$ where P divides λ but not κ.) In the proof of this proposition, use is made of integral closure, that is, of the assumption that the entire ring of integers is under consideration.

This proposition establishes a canonical form for prime ideals. Once it has been proved, the remainder of the theory follows fairly easily. Given P, κ, λ as above, let D be the greatest common divisor of (κ) and (λ), that is, $D=\{\beta+\gamma\colon \beta\in(\kappa),\ \gamma\in(\lambda)\}$. Then, by use of elementary propositions of the theory, it is not difficult to prove that $(\lambda)=P\cdot D$. Loosely speaking, this means that *in order to divide by* P *one can multiply by* D *and divide by* λ. In fact, if A is any ideal divisible by P then AD is divisible by (λ) and, since division by principal ideals is elementary, the quotient is easily seen to be an ideal Q with the property that $A=P\cdot Q$. This overcomes the "greatest difficulty" in the case of division by *prime* ideals. This can be used to show that every ideal is a product of prime ideals, from which it follows that division by an arbitrary ideal can be accomplished by a succession of divisions by prime ideals.

DEDEKIND's final version of the theory, which was published in the fourth edition of DIRICHLET's *Zahlentheorie* in 1894, contains an entirely new resolution of the "greatest difficulty." In a later paper [10] he described the process by which he arrived at this, his definitive version, giving even the exact date, 9 November 1888, when he discovered the module formula

$$(A+B+C)\,(BC+CA+AB)=(B+C)\,(C+A)\,(A+B)$$

(both sides are $ABC+A^2B+B^2A+A^2C+C^2A+B^2C+C^2B$) could be used to carry the proof of what had become for him the crucial proposition from the case of modules with 2 generators to those with 3 or more.

This later work of DEDEKIND (he was 57 at the time) continues to show great powers of innovation and generalization. He develops an extensive theory of "modules" (subgroups of the additive group of complex numbers) including a very general theory of *negative powers* of (certain) modules. This arithmetic of modules applies in particular to ideals and gives meaning to the notion of fractional ideals. In this context, if A and B are ideals and if $A\subset B$ then one can obtain the ideal C with the desired property $A=BC$ simply by setting $C=AB^{-1}$.

Admirable as this new theory was, and fruitful as it was in leading to further developments (it contained the germ of modern lattice theory), DEDEKIND's view that it is the best approach to the theory of ideal factorization in algebraic number fields is difficult to endorse. The theory is long, technical, and far removed from the eventual goal of the theory of factorization. On the whole, either DEDEKIND's original approach (especially when the "new clothes" of ideal theory are removed as in Section 6 above) or his approach using the "Prague theorem" (see Section 13 below) seems preferable."*

* NOETHER does not agree. In her editorial notes to the relevant part of DEDEKIND's works [vol. 3, p. 314 and vol. 2, p. 58] she says that the original approach was "still very complicated" (not too brief!) and that twentieth century generalizations had justified DEDEKIND's preference for the module-theoretic approach over the use of the Prague theorem.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

10. Kronecker's *Grundzüge*

As was mentioned in Section 4, KUMMER said in 1859 that KRONECKER would soon publish a work "in which the theory of the most general [ideal] complex numbers ... is developed fully and with enormous simplicity." However, 20 years later no indication of KRONECKER's approach had yet appeared – not to mention a fully developed theory – and DEDEKIND was forced to guess* what the basis of KRONECKER's theory was.

Finally, in 1881, in honor of the 50th anniversary of KUMMER's doctorate, KRONECKER published his *Grundzüge einer arithmetischen Theorie der algebraischen Grössen.* This is his ideal theory or, as he called it, his divisor theory. Here he says (§19) that he had worked out a complete theory by 1858 (he does not say that this theory is the one he develops in the *Grundzüge* and it seems certain that in 20 years it would have evolved) but that he had decided not to publish it until he found the generalization of the "associated genus", which is to say, roughly, that he decided not to publish the general case of the theory of ideal prime factors until he had developed the general case of class field theory!

For both KUMMER and DEDEKIND the basic idea of the theory was that of the *prime* ideals (or, in KUMMER's terminology, ideal prime factors) and the basic theorem stated that divisibility by a number (or an ideal) is equivalent to divisibility by all its prime factors. This approach has prevailed in later developments of the theory. It is therefore surprising and a little confusing for a modern reader to find that, in KRONECKER's version of the theory, the primes do not have such a central role and are introduced late in the development.

As KRONECKER makes clear in the *Grundzüge,* the notion of *prime* cannot be a central one for him because it is a *relative* one, that is, it depends on the particular field under discussion and changes if that field is enlarged (in a field extension a prime may no longer be prime) whereas the basic concepts of his theory are not relative in this sense. Even after he does introduce the notion of "prime" (§17) he uses it only as a tool in the proof of what he calls the *Second Fundamental Theorem* and it is not until the following section that he deals with unique factorization into primes.

Instead of unique factorization into primes, KRONECKER emphasizes the notion of *greatest common divisor.* It is probably for this reason that the basic objects of his theory, corresponding to DEDEKIND's "ideals", are called "divisors". The main points of his theory are the definition of *divisors,* the notion of *divisibility* of one divisor by another, the concomitant notion of *absolute equivalence* of divisors (two divisors are absolutely equivalent if each divides the other), and the interpretation of an algebraic integer as a divisor.

The kernel of KRONECKER's theory is a very simple and explicit idea (§14). Let $x_1, x_2, \ldots, x_k$ be a set of algebraic integers. The main objective is to define their greatest common divisor. This will be done if it can be determined precisely which algebraic integers y are divisible by g.c.d.$(x_1, x_2, \ldots, x_k)$ and which are not. KRONECKER accomplishes this using what he calls the *"methodische*

* [4, §10]. DEDEKIND's guess was wrong.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

Hülfsmittel der unbestimmten Coefficienten," that is, the method of undetermined coefficients. Let $u_1, u_2, \ldots, u_k$ represent unknowns, and consider the expression $x_1u_1+x_2u_2+\cdots+x_ku_k$ where the x's are the given algebraic integers. Assume that the x's are contained in some normal field over the rational numbers so that it is meaningful to speak of conjugates of the x's. A conjugate of the expression $x_1u_1+x_2u_2+\cdots+x_ku_k$ is simply the expression one obtains by performing a conjugation of the x's, which are integers in a certain normal field, and leaving the unknown u's alone. If n is the degree of the normal field containing the x's then the product of all the conjugates of $x_1u_1+\cdots+x_ku_k$, which KRONECKER denotes $Nm\,(x_1u_1+\cdots+x_ku_k)$, is a homogeneous form of degree n in the u's with coefficients which, because they are symmetric functions of the x's, are in Q and, because they are sums of products of integers, are integers. In short, $Nm(x_1u_1+\cdots+x_ku_k)$ has coefficients in Z. Let P be the greatest common divisor of these coefficients and set $Fm(x_1u_1+\cdots+x_ku_k)=P^{-1}\cdot Nm(x_1u_1+\cdots+x_ku_k)$. KRONECKER's rule for determining whether g.c.d. $(x_1, x_2, \cdots, x_k)$ divides y is to say that this is the case if and only if $x_1u_1+\cdots+x_ku_k$ divides $y\cdot Fm(x_1u_1+\cdots+x_ku_k)$ in the sense that the latter is equal to the former times a form in the u's with *integer* coefficients. Another way of stating this definition which makes the computation more precise and explicit is the following: Let $G(x_1u_1+\cdots+x_nu_n)$ be the product of the $n-1$ conjugates of $x_1u_1+\cdots+x_ku_k$ other than itself, that is, $G=Nm(x_1u_1+\cdots+x_ku_k)/(x_1u_1+\cdots+x_ku_k)=P\,Fm(x_1u_1+\cdots+x_ku_k)/(x_1u_1+\cdots+x_ku_k)$. Then

$$\frac{y\,Fm(x_1u_1+\cdots+x_ku_k)}{x_1u_1+\cdots+x_ku_k}=\frac{yG}{P}$$

and the criterion is simply that g.c.d.$(x_1, x_2, \ldots, x_n)$ *divides* y *if and only if all coefficients of the form* yG (which is a form of degree $n-1$ in the unknowns $u_1, u_2, \cdots, u_k$ with coefficients that are integers in the normal field under consideration) *are divisible by the ordinary integer* P.

This is the fundamental definition of KRONECKER's theory. The body of the theory is devoted to showing that this definition has all the expected properties.

A word is in order as to the underlying idea of KRONECKER's approach. In essence, he embeds the ring of integers of the field in question in the larger ring of polynomials in the unknowns u with coefficients in the ring of integers. In this larger ring, polynomials with coefficients in Z which are *primitive*, that is, whose coefficients have no common divisor greater than 1, are by *fiat* to be regarded as *units*. Thus if $x_1u_1+\cdots+x_ku_k$ divides $y\,Fm(x_1u_1+\cdots+x_ku_k)$ then, since the factor $Fm(x_1u_1+\cdots+x_ku_k)$ is by definition primitive, this is to be regarded as the same as saying that y itself is divisible by $x_1u_1+\cdots+x_nu_n$. Conversely, if $yFm(x_1u_1+\cdots+x_ku_k)$ is not divisible then neither is y. In a nutshell, then, KRONECKER's idea is to *regard primitive forms as units*. When this is done, the form $x_1u_1+\cdots+x_ku_k$ represents, in a very concrete way, the greatest common divisor of $x_1, x_2, \cdots, x_k$. For a complete development of the theory along these lines see the appendix to this paper.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

11. Outline of Kronecker's theory

It is fair to say that KRONECKER's theory of ideal factorization, which appears in Sections 14–18 of the *Grundzüge*, did not win wide acceptance. The presentation is difficult to follow, and the development leaves gaps that even a reader as knowledgeable as DEDEKIND found hard to fill.* Nonetheless, the theory is essentially complete, the gaps are not hard to fill if one knows how, and KRONECKER's approach has won the admiration of, and inspired, a number of important mathematicians. This section is devoted to a brief exposition of the theory.

For the sake of simplicity, only the case of integers in an algebraic number field K will be considered. (KRONECKER's theory applies also to the factorization of integers in certain function fields.) Moreover, it will be assumed that K is a *normal* field of degree n, so that every element of K has n conjugates (not necessarily distinct) and any symmetric function of these conjugates is a rational number. In particular, if a is an element of K and if X is an indeterminate, then $Nm(X-a)$, which, by definition, is the product of the n conjugates $X-a$, $X-a'$, $X-a''$, $\cdots$ of $X-a$, is a polynomial with rational coefficients and these coefficients are all integers if and only if a is an integer of K. (If a is an integer then so are all its conjugates and the coefficients of $Nm(X-a)$, being sums of products of integers, are integers. Conversely, if the coefficients of $Nm(X-a)$ are integers then, because the leading coefficient is 1 and because $X=a$ is a root of $Nm(X-a)$, it follows that a is an integer.)

The main advantage of KRONECKER's theory is that he gives an *explicit construction* of the divisors. His main tool for doing this is the method of undetermined coefficients. This means that he does algebraic computations with indeterminates with the intention of leaving them undetermined. In more modern terminology, he considers the ring of polynomials $K[u, u', u'', \cdots]$ with coefficients in K and with infinitely many variables or indeterminates $u, u', u'', \ldots$. Of course each polynomial contains only a finite number of variables, but it is important that one be able to add new indeterminates at will. In addition to the letters $u', u', u'', \cdots$, it will be convenient to use the letters $v, v', v'', \cdots, w, w', w'', \cdots$, and X for indeterminates. KRONECKER calls an element of $K[u, u', u'', \cdots]$ a *form* rather than a polynomial (even though it is *not* assumed to be homogeneous) in order to emphasize the fact that the *coefficients* are of primary interest and that the indeterminates are handled in a formal algebraic way.

Definitions. *A form* with coefficients in K is a polynomial with coefficients in K in some set of indeterminates. Such a form is called *integral* if all its coefficients are integers of K.

Clearly forms can be added and multiplied, and the elements of K themselves can be regarded as forms with coefficients in K, namely, as constant polynomials. Since the conjugations of K also act on polynomials with coefficients in K, the *norm* of a form with coefficients in K has a natural meaning. A major defect in KRONECKER's presentation of his theory is the fact that he implicitly

* See below.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

assumes (§14) the following theorem: *If Q is a form with coefficients in K and if $Nm(X-Q)$, where X is a new indeterminate, has coefficients in Z, then Q is an integral form.* As was noted above, this statement is obvious in the case of *constant* forms Q. For nonconstant forms it is *not* obvious, however, and, to make matters worse, KRONECKER uses the theorem (§14) before he defines the notion of an integral form (§15) so that the reader is left in doubt as to whether an integral form Q might just *be* one for which $Nm(X-Q)$ has coefficients in Z.

When DEDEKIND read the *Grundzüge* he made a series of remarks* on the work, the longest of which (#20) deals with this implicit theorem. DEDEKIND apparently struggled with the theorem and did succeed in proving it, but not in the full generality in which KRONECKER stated it and not in a way that he was satisfied with, as is shown by the fact that he called his proof "artificial" (*kunstlich*). A much more satisfactory and general proof was published by ADOLPH HURWITZ in 1895 [22] in connection with an exchange he had with DEDEKIND on the subject of the foundations of ideal theory. It seems very probable that this proof is, as HURWITZ believed, the one that KRONECKER had in mind.**

The main definition of KRONECKER's theory (§15, VI) generalizes the definition given above of divisibility of an integer y of K by the greatest common divisor of the integers $x_1, x_2, \cdots, x_k$ of K:

Definition. Let α and β be integral forms with coefficients in K. Then β will be said to be *divisible by the divisor corresponding to* α, denoted $\beta \equiv 0 \bmod [\alpha]$, if all coefficients of the integral form $\beta Nm(\alpha)/\alpha$ are divisible by the integer P which is the greatest common divisor of the coefficients of $Nm(\alpha)$. (Note that $Nm(\alpha)/\alpha$ is an integral form with coefficients in K because it is the product of the $n-1$ conjugates of α other than α itself. Thus $\beta Nm(\alpha)/\alpha$ is an integral form with coefficients in K, so that divisibility of these coefficients by the integer P is meaningful.)

---

* These remarks were written in polished form, ready for the printer, under the title *Bunte Bemerkungen zu Kronecker's Abhandlung: Grundzüge einer arithmetischen Theorie der algebraischen Grössen* (§1–22), and were referred to in one of DEDEKIND's published works [10], but they were never published. In the near future they will be published with annotations by OLAF NEUMANN, WALTER PURKERT, and myself.

** Briefly, this proof is as follows. Let u be one of the variables which occur in Q, say $Q = Q_k u^k + Q_{k-1} u^{k-1} + \cdots + Q_1 u + Q_0$ where $Q_k, \ldots, Q_0$ are forms with one less variable than Q. The elementary symmetric function of degree j in the n conjugates of Q (which is the coefficient of X^{n-j} in $Nm(X-Q)$) has as the coefficient of $(u^k)^j$ the elementary symmetric function of degree j in the n conjugates of Q_k. By assumption, this coefficient of u^{kj} is a form with coefficients in Z. Since this is true for all j, $Nm(X-Q_k)$ is a form with coefficients in Z. Therefore, by the argument which proves that differences of integers are integers, all the elementary symmetric functions in the n conjugates of $Q' = Q - Q_k u^k = Q_{k-1} u^{k-1} + \cdots + Q_0$ have coefficients in Z, that is, $Nm(X-Q')$ has coefficients in Z. Therefore $Nm(X-Q_{k-1})$, $Nm(X-Q_{k-2})$, $\cdots$, $Nm(X-Q_0)$ all have coefficients in Z. This reduces the original problem to a set of forms $Q_0, Q_1, \cdots, Q_k$ with one less variable. Repeating the process reduces the theorem to the known case where there are *no* variables.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

In terms of this definition, $y \equiv 0 \bmod [x_1 u_1 + x_2 u_2 + \cdots + x_k u_k]$ is precisely the definition given in the preceding section for divisibility of y by g.c.d. $(x_1, x_2, \cdots, x_k)$. More generally, in the final theory, once it is constructed, $\beta \equiv 0 \bmod [\alpha]$ will mean that all coefficients of β are divisible by the greatest common divisor of the coefficients of α. Note that the relation of congruence $\bmod [\alpha]$ has all the expected properties, that is, the relation $\beta \equiv \gamma \bmod [\alpha]$ defined by $\beta - \gamma \equiv 0 \bmod [\alpha]$ is reflexive, symmetric, transitive, and consistent with addition and multiplication.

KRONECKER states this definition somewhat differently. He says (§15, IV) that the algebraic expression $\alpha/Fm(\alpha)$ "represents a divisor whose elements are the coefficients of α". Here $Fm(\alpha)$ is by definition the form $Nm(\alpha)/P$, which is a primitive form with coefficients in Z. He then defines $\beta \equiv 0 \bmod [\alpha]$ to mean that β divided by $\alpha/Fm(\alpha)$ is an integral form with coefficients in K, by which he means that there is an integral form γ with coefficients in K such that $\beta = (\alpha/Fm(\alpha))\gamma$, that is, $\alpha\gamma = \beta Fm(\alpha) = \beta Nm(\alpha)/P$; clearly this is true if and only if the form $\gamma = P^{-1}\,[\beta Nm(\alpha)/\alpha]$ has integral coefficients, which shows that this definition agrees with the one given above. KRONECKER states it in the way he does because he feels (first paragraph of §15) that in this way he avoids *all* abstraction because $\beta \equiv 0 \bmod [\alpha]$ *means* that β is divisible, in the most obvious sense, by $\alpha/Fm(\alpha)$.

The words "$\alpha/Fm(\alpha)$ represents a divisor" seem to be very carefully chosen and seem to be as close as KRONECKER came to saying what a divisor *is*. In the modern approach to such questions, one would say that a divisor *is* an equivalence class of forms α, where two forms α_1 and α_2 are equivalent if the relations of congruence $\bmod [\alpha_1]$ and $\bmod [\alpha_2]$ coincide. KRONECKER, however, sidesteps the question of what a divisor *is* by describing the way in which they are *represented* and defining what it means to say that two representations represent the *same* divisor, or, in his terminology, what it means to say that two representations represent *absolutely equivalent* divisors.*

KRONECKER says that the divisor $\bmod [\alpha]$ *divides* the divisor $\bmod [\beta]$ if $\beta \equiv 0 \bmod [\alpha]$, and he says that two divisors are *absolutely equivalent* if each divides the other (§15, VI and VIII). As DEDEKIND observed in his remarks on the *Grundzüge* (# 26), KRONECKER should, but does not, prove that his relation of "absolute equivalence" is transitive. Although the proof of this fact is fairly easy to deduce from the propositions that KRONECKER does prove, the proof is not trivial and makes use of what KRONECKER calls (in §17) the "first fundamental theorem". Clearly the transitivity of absolute equivalence follows from the following proposition which should also be (but in KRONECKER's treatment is not) proved if the word "divides" is to be used.

Proposition. If α, β, and γ are integral forms with coefficients in K and if $\bmod [\alpha]$ divides $\bmod [\beta]$ and $\bmod [\beta]$ divides $\bmod [\gamma]$ then $\bmod [\alpha]$ divides $\bmod [\gamma]$.

Proof. What is given is that $\beta \equiv 0 \bmod [\alpha]$ and $\gamma \equiv 0 \bmod [\beta]$, that is, there exist integral forms σ and τ with coefficients in K such that $\beta Fm(\alpha) = \alpha\sigma$ and

* This is an approach with which I am very sympathetic. See p. 375 of my *Advanced Calculus* [13].

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

$\gamma Fm(\beta)=\beta\tau$. These combine to give $\gamma Fm(\alpha)\, Fm(\beta)=\beta Fm(\alpha)\,\tau=\alpha\sigma\tau$, which shows that $\gamma Fm(\beta)\equiv 0 \bmod[\alpha]$, whereas what is to be shown is that $\gamma\equiv 0 \bmod[\alpha]$. Therefore the proposition follows from:

First Fundamental Theorem.* If α and β are integral forms with coefficients in K and if δ is a form with coefficients in Z which is *primitive*, that is, whose coefficients have no common divisor greater than 1, then $\beta\delta\equiv 0 \bmod[\alpha]$ implies $\beta\equiv 0 \bmod[\alpha]$.

KRONECKER's proof of this theorem is given in the next section.

Corollary. A divisor $\bmod[\alpha]$ divides another $\bmod[\beta]$ if and only if congruence $\bmod[\beta]$ implies congruence $\bmod[\alpha]$. Therefore $\bmod[\alpha]$ and $\bmod[\beta]$ are absolutely equivalent if and only if they define the same congruence relation.

Proof. Clearly $\beta\equiv 0 \bmod[\beta]$. Thus if congruence $\bmod[\beta]$ implies congruence $\bmod[\alpha]$ then $\beta\equiv 0 \bmod[\alpha]$, that is, $\bmod[\alpha]$ divides $\bmod[\beta]$. Conversely, if $\bmod[\alpha]$ divides $\bmod[\beta]$ and $\gamma\equiv 0 \bmod[\beta]$ then the proposition shows that $\gamma\equiv 0 \bmod[\alpha]$, so that congruence $\bmod[\beta]$ implies congruence $\bmod[\alpha]$.

Ultimately KRONECKER shows that every divisor is equivalent to a linear divisor (one corresponding to a form α of first degree in the variables) and, more specifically, that *divisors with the same coefficients are absolutely equivalent.* This is the "second fundamental theorem". In other words, a divisor $\bmod[x_1\phi_1+x_2\phi_2+\cdots+x_k\phi_k]$, in which the x's are integers in K and the ϕ's are products of powers of indeterminants, is absolutely equivalent to the linear divisor $\bmod[x_1u_1+x_2u_2+\cdots+x_ku_k]$ where the u's are indeterminates. The proof of this theorem is also given in the next section.

Thus the theory of divisors ultimately reduces to the theory of linear divisors. However, before proving this, KRONECKER finds it convenient to develop first the main facts in the theory of linear divisors. These he presents in five statements (§16).

(1) *Linear divisors with the same coefficients are absolutely equivalent.* (This is the second fundamental theorem for linear divisors.) This follows** immediately from the statement that $x_i\equiv 0 \bmod[x_1u_1+x_2u_2+\cdots+x_ku_k]$, a fact which KRONECKER proves as follows. Let $\alpha=x_1u_1+x_2u_2+\cdots+x_ku_k$, let $N=Nm(\alpha)$, and let $N=P\cdot F$ where $P\in Z$ is the greatest common divisor of the coefficients of N and where F is consequently a primitive form in the u's. What is to be shown is that $x_iF/\alpha=x_i(N/\alpha)\cdot P^{-1}$ is an integral form. For this it is necessary and sufficient – this is the implicit theorem that gave DEDEKIND so much

* KRONECKER's statement (§15, IX) differs slightly from this one in that he does not assume that δ has coefficients in Z but rather that it is an integral form with coefficients in K which is *primitive* in the sense that $Nm(\delta)$ is primitive in the above sense. Since $\beta\delta\equiv 0 \bmod[\alpha]$ implies $\beta Nm(\delta)\equiv 0 \bmod[\alpha]$, this theorem follows immediately from the theorem above.

** Actually the two statements are easily seen to be equivalent. If (1) is known, then $x_1v_1+x_2v_2+\cdots+x_kv_k\equiv 0 \bmod[x_1u_1+x_2u_2+\cdots+x_ku_k]$. Thus $(x_1v_1+\cdots+x_kv_k)\cdot Fm(x_1u_1+\cdots+x_ku_k)=(x_1u_1+\cdots+x_ku_k)\gamma$ where γ is an integral form in the u's and v's, and substitution of $v_i=1$, $v_j=0$ for $j\neq i$ gives $x_i\equiv 0 \bmod[x_1u_1+\cdots+x_ku_k]$.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

trouble – that the form

$$(1) \qquad Nm\left(X-\frac{x_iF}{\alpha}\right)=\frac{Nm(X\alpha-x_iF)}{PF}$$

(where X is a new unknown) be an integral form. Now $X\alpha-x_iF$ is equal to α with u_j changed to Xu_j $(j\neq i)$ and with u_i changed to Xu_i-F. Since these quantities are invariant under all conjugations (F because its coefficients are in Z) the numerator $Nm(X\alpha-x_iF)$ of the form (1) is equal to the form that is obtained by substituting Xu_j for u_j and Xu_i-F for u_j in the form $N=PF$. From this it is clear that the P's cancel and that all terms of the numerator which contain X to a power less than the n^{th} contain an F to cancel the denominator. Since the expression of (1) on the left shows that the coefficient of X^n is 1, this proves the theorem. Note that the theorem shows that $x_1u_1+\cdots+x_ku_k$ *is the* greatest common divisor of* $x_1, x_2,\cdots, x_k$ because it divides all the x's and any divisor (linear or not) which divides all the x's divides it.**

(2) *If* x_{k+1} *is an integer of* K *such that* $x_{k+1}\equiv 0 \bmod[x_1u_1+\cdots+x_ku_k]$ *then the linear divisors* $\bmod[x_1u_1+\cdots+x_ku_k]$ *and* $\bmod[x_1u_1+\cdots+x_ku_k+x_{k+1}u_{k+1}]$ *are absolutely equivalent.* This follows immediately from the observation that (by (1) and the assumption) each divisor divides all the coefficients of the other.

(3) *If* α *and* β *are linear forms which contain distinct indeterminates then* $\bmod[\alpha+\beta]$ *is the*** greatest common divisor of* $\bmod[\alpha]$ and $\bmod[\beta]$ in the sense that it divides both and any divisor which divides both divides it. This follows immediately from (1) and the observation that $\bmod[\alpha+\beta]$ is the greatest common divisor of its coefficients.

(4) *The product of two linear divisors with distinct indeterminates is absolutely equivalent to a linear divisor according to the rule*

$$(2) \qquad \begin{aligned}&\bmod[x_1u_1+x_2u_2+\cdots]\bmod[y_1v_1+y_2v_2+\cdots]\\ &\quad\sim\bmod[x_1y_1w_1+x_1y_2w_2+x_2y_1w_3+\cdots]\end{aligned}$$

where $\sim$ denotes absolute equivalence, where the x's and y's are integers of K, where the u's, v's, and w's are indeterminates, and where there is a distinct w for each distinct pair u_iv_j. KRONECKER does not deal explicitly with the notion of *products* of divisors, but it is easy enough to see what he meant. If one regards $\alpha/Fm(\alpha)$ as *being* the divisor $\bmod[\alpha]$, and not merely as represent-

---

* More precisely, it is *a* greatest common divisor and *any* greatest common divisor is absolutely equivalent to it.

** The "second fundamental theorem", which states that $\bmod[x_1\phi_1+x_2\phi_2+\cdots+x_k\phi_k]\sim\bmod[x_1u_1+x_2u_2+\cdots+x_ku_k]$ where the ϕ's are products of powers of indeterminates and the u's are indeterminates, reduces, in the light of (1), to the apparently simple statement that $x_i\equiv 0 \bmod[x_1\phi_1+x_2\phi_2+\cdots+x_k\phi_k]$ for $i=1, 2,\cdots, k$. KRONECKER proves this, however, by proving the second fundamental theorem first and then deducing it. (See §17, II′.)

*** See note * above.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

ing it, then obviously the product of mod[α] and mod[β] is $\alpha\beta/Fm(\alpha)Fm(\beta)$. Since, as follows from GAUSS's lemma,* $Fm(\alpha)\,Fm(\beta)=Fm(\alpha\beta)$, this amounts to saying that mod[α]$\cdot$mod[β]=mod[$\alpha\beta$]. It is simple to show that this product operation has all the expected properties – for instance, if $\alpha\sim\alpha'$ then $\alpha\beta\sim\alpha'\beta$ for all forms β (without this property it would scarcely be meaningful to call it a multiplication of divisors) and if $x\equiv 0 \bmod[\alpha]$ and $y\equiv 0 \bmod[\beta]$ then $xy \equiv 0 \bmod[\alpha]\cdot\bmod[\beta]$. This latter fact shows that the divisor on the left side of (2) divides the one on the right. Conversely, the divisor on the left is equal to mod$[x_1y_1u_1v_1+x_1y_2u_1v_2+\cdots]$ and, since all its coefficients are divisible by the divisor on the right (by (1)) it is divisible by the divisor on the right.

(5) *If* α, β, γ *are linear forms with distinct indeterminates, if* mod[α] mod[β] *is divisible by* mod[γ], *and if* mod[α] *and* mod[γ] *have no common divisor, then* mod[γ] *divides* mod[β].

Proof. Here the assumption that mod[α] and mod[γ] have no common divisor must be interpreted to mean that any divisor that divides both is absolutely equivalent to mod[1], that is, corresponds to the trivial congruence relation (see §16 between III and IV). Thus, by (3), mod[$\alpha+\gamma$]$\sim$mod[1]. This implies that $1\cdot Fm(\alpha+\gamma)=(\alpha+\gamma)\delta$ for an integral form δ. Since $\alpha\beta\equiv 0 \bmod[\gamma]$ by assumption, and since $\gamma\equiv 0 \bmod[\gamma]$ it follows that $Fm(\alpha+\gamma)\cdot\beta=\delta(\alpha+\gamma)\beta=\delta\alpha\beta+\delta\gamma\beta\equiv 0 \bmod[\gamma]$. Since $Fm(\alpha+\gamma)$ is primitive, $\beta\equiv 0 \bmod[\gamma]$ then follows from the First Fundamental Theorem.

12. Some proofs

First Fundamental Theorem. If α and β are integral forms with coefficients in K (a given normal, algebraic extension of the rational numbers), if δ is

* GAUSS's lemma is the statement that, for forms with coefficients in Z, the greatest common divisor of the coefficients of the product of two forms is equal to the product of the greatest common divisors of the coefficients of the two forms. (For GAUSS's statement, see Article 42 of the *Disquisitiones Arithmeticae*. His statement is weaker than the statement here in that the statement here cannot be easily deduced from his. However, as DEDEKIND [8] points out, GAUSS's *proof* easily implies the statement here – at least in the case of one variable, and the case of many variables is just as easily deduced – which in turn implies GAUSS's statement.) The general case follows from the special case which states that *a product of primitive forms is primitive*. This can be proved as follows. Note first that it will suffice to prove that if γ and δ are forms with coefficients in Z and if $p\in Z$ is a prime which divides neither γ nor δ then p does not divide $\gamma\delta$. Let m be the number of variables in $\gamma\delta$. If $m=0$ then γ, δ, and $\gamma\delta$ are in Z and the desired conclusion follows from the definition of prime. Suppose that it has been proved for forms in $m-1$ variables and let X be one of the variables that occur in $\gamma\delta$ so that $\gamma=\gamma_rX^r+\gamma_{r-1}X^{r-1}+\cdots+\gamma_0$ and $\delta=\delta_sX^s+\delta_{s-1}X^{s-1}+\cdots+\delta_0$ where $\gamma_r, \gamma_{r-1},\cdots, \gamma_0, \delta_s,\cdots, \delta_0$ are forms in $m-1$ variables. Let t be the greatest integer$\leqq r$ such that p does not divide γ_t and $u\leqq s$ the greatest such that p does not divide δ_u. By the induction hypothesis, p does not divide $\gamma_t\delta_u$. Then the coefficient of X^{t+u} in $\gamma\delta$, namely, $\sum_{i+j=t+u}\gamma_i\delta_j$, consists of one term that is not divisible by p while all the remaining terms are, by the choice of u and t, divisible by p. Therefore the sum is not divisible by p and $\gamma\delta$ is not divisible by p, as was to be shown.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

a form with coefficients in Z which is primitive, and if $\beta\delta \equiv 0 \bmod[\alpha]$, then $\beta \equiv 0 \bmod[\alpha]$.

Proof (KRONECKER, §15). Consider first the case where α and β have coefficients in Z and α is a form of degree *zero*, say $\alpha = a \in Z$. Let $\beta = b\beta'$ where $b \in Z$ is the greatest common divisor of the coefficients of β and where, consequently, β' is primitive. Since $Fm(\alpha) = 1$, to say that $\beta\delta \equiv 0 \bmod[\alpha]$ is the same as to say that all coefficients of $\beta\delta$ are divisible by the integer $\alpha = a$. Since $\beta\delta = b\beta'\delta$, and since $\beta'\delta$ is primitive by GAUSS's lemma, this implies that a divides b and proves the theorem in this case.

Next consider the case in which $\alpha = a$ is still of degree zero but α and β have coefficients in K, not necessarily in Z. Again $Fm(\alpha) = 1$ so that $\beta\delta \equiv 0 \bmod[\alpha]$ means that there is an integral form, say γ, such that $\beta\delta = \alpha\gamma$. What is to be shown is that β/α is an integral form. This is the same as saying that $Nm\left(X - \frac{\beta}{\alpha}\right)$ is an integral form (where X is a new indeterminate). Now

$$Nm(\delta)\, Nm(\alpha X - \beta) = Nm(\alpha\delta X - \beta\delta) = Nm(\alpha\delta X - \alpha\gamma) = Nm(\alpha)\, Nm(\delta X - \gamma).$$

Since $Nm(\alpha)$ divides the right side of this equation, it divides the left. Since δ has coefficients in Z, its norm is δ^n, which is primitive.* Therefore $Nm(\alpha)$ divides $Nm(\alpha X - \beta)$ by the case of the theorem already proved. That is, all coefficients of $Nm(\alpha X - \beta)$ are divisible by $Nm(\alpha) \in Z$ and the quotient, which is $Nm\left(X - \frac{\beta}{\alpha}\right)$, is integral, as was to be shown.

Finally, consider the general case. To say that $\beta\delta \equiv 0 \bmod[\alpha]$ means that all coefficients of the integral form $\beta\delta(Nm(\alpha)/\alpha)$ are divisible by the integer P which is the greatest common divisor of the coefficients of $Nm(\alpha)$. Since δ is primitive, the case of the theorem that has been proved implies that P divides $\beta(Nm(\alpha)/\alpha)$, that is, $\beta \equiv 0 \bmod[\alpha]$, as was to be shown.

Second Fundamental Theorem. Divisors corresponding to forms with the same coefficients are absolutely equivalent.

Proof (KRONECKER, §17). Let $\alpha = x_1\phi_1 + x_2\phi_2 + \cdots + x_k\phi_k$ where the x's are integers of K and the ϕ's are products of powers of indeterminates. It will suffice to show that if $\beta = x_1u_1 + x_2u_2 + \cdots + x_ku_k$, where the u's are indeterminates, then $\bmod[\alpha] \sim \bmod[\beta]$. Since $\bmod[\beta]$ is the greatest common divisor of the x's, and since any common divisor of the x's obviously divides α, this amounts to showing that $\bmod[\alpha]$ divides all the x's. KRONECKER's proof of this depends on using *unique factorization of divisors into primes* to show that $\bmod[\alpha]$ is absolutely equivalent to a product of linear divisors; then, by (4) of the preceding section, $\bmod[\alpha]$ is absolutely equivalent to a linear divisor, and from this it is easy to show that it divides the x's. This part of the proof follows the development of the theory of factorization into primes.

* Note that one need not assume that δ has coefficients in Z but only that $Nm(\delta)$ is primitive, which is KRONECKER's definition of a primitive form with coefficients in K.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

Definition. A divisor is said to be *prime** if the congruence relation it defines on integral forms with coefficients in K is nontrivial and prime. That is, $\mathrm{mod}[\pi]$ is prime if $1 \not\equiv 0 \bmod[\pi]$ and if the condition $\alpha\beta \equiv 0 \bmod[\pi]$, where α and β are integral forms with coefficients in K, implies that either $\alpha \equiv 0 \bmod[\pi]$ or $\beta \equiv 0 \bmod[\pi]$.

As follows immediately from the definitions, it would be equivalent to say that $\mathrm{mod}[\pi]$ is prime if it is not absolutely equivalent to $\mathrm{mod}[1]$ and if it divides a product $\mathrm{mod}[\alpha]\ \mathrm{mod}[\beta]$ of two divisors only if it divides one of the factors.

Pending the proof of the second fundamental theorem, it will be convenient to deal specifically with *linear* prime divisors, although that theorem implies that every prime divisor is absolutely equivalent to a linear one.

Lemma. Every prime $p \in Z$ is divisible by a linear prime divisor with coefficients in K.

Proof.** If a linear divisor $\mathrm{mod}[x_1u_1 + x_2u_2 + \cdots + x_ku_k]$ divides p then, by (2) of the preceding section, it is absolutely equivalent to $\mathrm{mod}[pu_0 + x_1u_1 + \cdots + x_ku_k]$. Moreover, if $x_i \equiv x_i' \bmod p$ then x_i can be replaced by x_i' and the new divisor will be absolutely equivalent to the old because each clearly divides all the coefficients of the other. Let S be a representative set of integers of $K \bmod p$, that is, a set of integers of K such that every integer of K is congruent to one and only one element of $S \bmod p$. Then S is finite. (In fact, S has p^n elements where n is the degree of K over Q.) Thus, every linear divisor which divides p is absolutely equivalent to one of the form $\mathrm{mod}[pu_0 + x_1u_1 + \cdots + x_ku_k]$ where the x's all lie in the finite set S. Since repeated x's can be dropped, this shows that *there is a finite set T of linear divisors such that every linear divisor that divides p is absolutely equivalent to a divisor in T.*

The set T contains at least one nontrivial divisor, namely, $\mathrm{mod}[pu_0]$. Let $D_0 \in T$ be a nontrivial divisor. If there is a nontrivial divisor in T which divides D_0 but is not absolutely equivalent to it, let D_1 be such a divisor. Similarly, if there is a nontrivial divisor in T which divides D_1 but is not absolutely equivalent to it let this divisor be D_2, and so forth. This process terminates with a linear divisor D which divides p but which is not properly divisible by any linear divisor in the sense that a linear divisor which divides D is absolutely equivalent either to $\mathrm{mod}[1]$ or to D. The claim is that D is prime.

It will be shown that if a and b are integers of K such that $a \not\equiv 0 \bmod D$ and $b \not\equiv 0 \bmod D$ then $ab \not\equiv 0 \bmod D$. Let*** $D = pu_0 + x_1u_1 + \cdots + x_ku_k$. Since

* As KRONECKER emphasizes, this concept is *relative* to the particular field K under consideration and changes if K is extended. KRONECKER does not define prime (irreducible) in this way, but rather defines (§17) a prime divisor to be one $\mathrm{mod}[\pi]$ such that $\pi \equiv 0 \bmod[\alpha]$ implies $\mathrm{mod}[\alpha]$ is absolutely equivalent either to $\mathrm{mod}[1]$ or to $\mathrm{mod}[\pi]$. He proves, then, that if π is *linear* and prime in his sense then it is prime in the sense of the above definition. He seems to take it as obvious that a given form is divisible by a *linear* prime divisor. I do not see the justification for this assertion and have interpolated the lemma below in order to avoid using it.

** KRONECKER (§18).

*** Strictly speaking, we should write $D = \mathrm{mod}[p_0u_0 + x_1u_1 + \cdots + x_ku_k]$ and in the preceding sentence we should write $a \not\equiv 0(D)$, *etc.*

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

$a \not\equiv 0 \bmod D$, $\bmod[D+av_1]$, the greatest common divisor of D and $\bmod[av_1]$, is not divisible by D and is therefore trivial. If $ab \equiv 0 \bmod D$ then $\bmod[D+av_1]$ $\bmod[b]$ is divisible by D. Therefore, by (5) of the preceding section, $b \equiv 0 \bmod D$, contrary to assumption. Therefore $ab \not\equiv 0 \bmod D$.

The technique used to prove GAUSS's lemma in the note in the preceding section now shows that D is prime. Specifically, let α and β be integral forms with coefficients in K such that $\alpha \not\equiv 0 \bmod D$ and $\beta \not\equiv 0 \bmod D$. It is to be shown that $\alpha\beta \not\equiv 0 \bmod D$. Let m be the total number of indeterminates in $\alpha\beta$. If $m=0$ then this was just proved above. If $m \geqq 1$, let X be one of the variables that occurs in $\alpha\beta$ and set $\alpha=\alpha_r X^r+\alpha_{r-1}X^{r-1}+\cdots+\alpha_0$, $\beta=\beta_s X^s+\cdots+\beta_0$, where $\alpha_r, \cdots, \alpha_0, \beta_s, \cdots, \beta_0$ are forms in $m-1$ indeterminates for which the statement to be proved is true by the induction hypothesis. Let t be the largest integer such that $\alpha_t \not\equiv 0 \bmod D$ and u the largest such that $\beta_u \not\equiv 0 \bmod D$. Then the coefficient of X^{t+u} in $\alpha\beta$ is $\equiv \alpha_t\beta_u \not\equiv 0 \bmod D$, so $\alpha\beta \not\equiv 0 \bmod D$, as was to be shown.

Thus the linear divisor D which divides p is prime and the lemma is proved.

Theorem. Every divisor is absolutely equivalent to a product of prime divisors, and, up to absolute equivalence and reordering of the factors, such a representation is unique.

Proof. Let $\alpha=x_1\phi_1+\cdots+x_k\phi_k$ where the ϕ's are distinct products of powers of indeterminates. Let P_α be the positive integer that is the greatest common divisor of the coefficients of $Nm(\alpha)$. If $P_\alpha=1$ then $\bmod[\alpha] \sim \bmod[1]$ and $\bmod[\alpha]$ is an *empty* product of prime divisors. Otherwise, there is a prime integer $p \in Z$ which divides P_α. By the lemma, there is a linear prime divisor, say $\bmod[\pi]$, which divides p. Then $\bmod[\pi]$ divides $Nm(\alpha)$. This implies that $\bmod[\pi]$ divides one of the factors of $Nm(\alpha)$, that is, divides one of the conjugates of α. Therefore a conjugate of $\bmod[\pi]$, say $\bmod[\pi']$, divides α itself. This implies an equation $\alpha Fm(\pi')=\pi'\beta$ where $\beta=P_{\pi'}^{-1}\alpha Nm(\pi')/\pi'$ is an integral form with coefficients in K. Taking the norm on both sides and using GAUSS's lemma gives $P_\alpha=P_\pi P_\beta$. Since $P_\pi \neq 1$ (otherwise $1 \equiv 0 \bmod[\pi']$), $P_\alpha > P_\beta$.

If $P_\beta=1$ the process terminates. Otherwise one can repeat the process to find a prime divisor $\bmod[\pi'']$ such that $\beta Fm(\pi'')=\pi''\gamma$ where $P_\beta > P_\gamma$. Then $\alpha Fm(\pi') \cdot Fm(\pi'')=\pi'\beta Fm(\pi'')=\pi'\pi''\gamma$. If $P_\gamma=1$, the process terminates. Otherwise, repeat. Since P can decrease at most P_α times, the process terminates with an equation of the form $\alpha Fm(\pi)\, Fm(\pi')\cdots Fm(\pi^{(r)})=\pi'\pi''\cdots\pi^{(r)}\,\delta$ where $\bmod[\pi']$, $\bmod[\pi'']$, $\cdots$ are linear prime divisors, and where $Nm(\delta)$ is primitive. It now follows immediately* from the first fundamental theorem that $\bmod[\pi'\pi''\cdots\pi^{(r)}]$ divides $\bmod[\alpha]$ and that $\bmod[\alpha]$ divides $\bmod[\pi'\pi''\cdots\pi^{(r)}]$, that is, the given divisor $\bmod[\alpha]$ is absolutely equivalent to the product of linear prime divisors $\bmod[\pi]$ $\bmod[\pi'']\cdots \bmod[\pi^{(r)}]$. This proves the first statement of the theorem.

The proof of the second statement depends on establishing the possibility of *division*.

* This proof deviates somewhat from KRONECKER's at this point. KRONECKER seems to overemphasize the difference between the statements "$\bmod[\alpha]$ divides $\bmod[\beta]$" and "there is a divisor $\bmod[\gamma]$ such that $\bmod[\beta]$ is absolutely equivalent to $\bmod[\alpha]$ $\bmod[\gamma]$." It is in fact an easy lemma to show that these two statements are equivalent.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

Lemma. If mod[α] divides mod[β] then there is a divisor mod[γ] such that mod[β] is absolutely equivalent to mod[α] mod[γ] and any two divisors mod[γ] with this property are absolutely equivalent.

Proof. To say that mod[α] divides mod[β] means that $\beta Fm(\alpha)=\alpha\gamma$ where γ is the integral form $P_\alpha^{-1}\beta Nm(\alpha)/\alpha$. Since mod[$Fm(\alpha)$]$\sim$mod[1], this implies, because multiplication is consistent with absolute equivalence, that mod[β]$\sim$ mod[α] mod[γ]. Since mod[α] mod[γ]=mod[$\alpha\gamma$], if mod[γ'] is another divisor with the same property then mod[$\alpha\gamma$]$\sim$mod[$\alpha\gamma'$]. Thus $\alpha\gamma$ divides $\alpha\gamma'$, which means that $\alpha\gamma' Fm(\alpha)Fm(\gamma)=\alpha\gamma\delta$ where δ is an integral form. When the α's are cancelled this gives $\gamma' Fm(\alpha)\equiv 0 \bmod[\gamma]$, so $\gamma'\equiv 0 \bmod[\gamma]$ by the first fundamental theorem. In the same way, $\gamma\equiv 0 \bmod[\gamma']$, so that mod[$\gamma$]$\sim$mod[$\gamma'$], as was to be shown.

Suppose now that mod[$\pi_1\pi_2\cdots\pi_r$]$\sim$mod[$\pi'_1\pi'_2\cdots\pi'_s$] where the divisors mod[π_j] and mod[π'_j] are all prime. Since mod[π_1] divides the left side, it also divides the right and therefore divides one of the factors on the right. In particular, there must *be* a factor on the right, that is, $s\neq 0$, since otherwise mod[π_1] would divide mod[1], contrary to the assumption that mod[π_1] is prime. Let the factors on the right be rearranged, if necessary, so that mod[π_1] divides mod[π'_1]. Thus, by the division lemma, mod[π'_1]$\sim$mod[π_1] mod[α]. Because mod[π'_1] is prime, it must divide one of the factors on the left. If it divided mod[α], then division would give mod[1]$\sim$mod[π_1] mod[β] for some β, and this would give mod[π_1]$\sim$mod[1], contrary to the assumption that mod[π_1] is prime. Therefore mod[π'_1] divides mod[π_1] and these two divisors are absolutely equivalent. Thus mod[$\pi_1\pi_2\cdots\pi_r$]$\sim$mod[$\pi_1\pi'_2\cdots\pi'_s$] and division gives mod[$\pi_2\cdots\pi_r$]$\sim$mod[$\pi'_2\cdots\pi'_s$]. Now repeat the process. Since there remain factors on the right as long as there are factors on the left, $r\leqq s$. By symmetry $s\leqq r$. Therefore the process matches the π_j with the π'_j one by one and the proof is complete.

Conclusion of the proof of the second fundamental theorem. As before, let $\alpha=x_1\phi_1+\cdots+x_k\phi_k$. What is to be shown is that $x_i\equiv 0 \bmod[\alpha]$. By the theorem above, mod[α] is absolutely equivalent to a linear divisor, say mod[θ]. Since the indeterminates in θ are arbitrary, it can be assumed that they are distinct from the ones in α. Since $\alpha Fm(\theta)=\theta\tau$ where τ is an integral form ($\tau=P_\theta^{-1}\alpha\, Nm(\theta)/\theta$), equating coefficients of ϕ_i on the two sides of this equation gives $x_i Fm(\theta)=\theta\tau_i$ where τ_i is an integral form. Thus $x_i\equiv 0 \bmod[\theta]$. Since mod[$\alpha$] is absolutely equivalent to mod[θ], it follows that $x_i\equiv 0 \bmod[\alpha]$, as was to be shown.

13. Dedekind's Prague Theorem

DEDEKIND's critical reading of KRONECKER's *Grundzüge* led him to a new approach to ideal theory. Ironically, he himself rejected the new approach on ideological grounds – it clearly showed its origin in KRONECKER's method of undetermined coefficients and did not lend itself to the formulation of the definition of ideals in terms of properties I and II that DEDEKIND insisted on – but it was adopted by HILBERT in his influential summary of number

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

theory, the so-called *Zahlbericht* [20], and it has therefore found a place in the standard corpus of number theory.

The point of the *Grundzüge* that gave DEDEKIND the most difficulty, and the one to which he devoted by far the longest remark (# 20) in his *Bunte Bemerkungen,* is the theorem in §14 that if $x_1, x_2, \cdots, x_k$ are integers then the linear form $x_1 v_1 + \cdots + x_k v_k$, where the v's are indeterminates, is congruent to zero mod$[x_1 u_1 + \cdots + x_k u_k]$, where the u's are other indeterminates. DEDEKIND saw that this theorem contained within it the kernel of his ideal theory,* but he was unable to prove it in a way that he found satisfactory.

As was seen in Section 11, KRONECKER's theorem in §14 actually can be proved in an elementary way that follows rather closely the ideas KRONECKER indicated. Ironically, it was DEDEKIND's inability to reconstruct KRONECKER's argument that led him to the formulation and proof of a theorem that not only implies the simple theorem of §14 but also implies KRONECKER's "second fundamental theorem". (Let $\alpha = x_1 \phi_1 + \cdots + x_k \phi_k$ where the ϕ's are distinct products of powers of indeterminates and let $\beta = x_1 v_1 + \cdots + x_k v_k$ where the v's are indeterminates. The second fundamental theorem says that the divisors mod$[\alpha]$ and mod$[\beta]$ are absolutely equivalent. The theorem of §14 is the special case where α is linear. DEDEKIND's attempt to prove the special case resulted in a proof of the general case.)

DEDEKIND told the story in a letter he wrote in 1887 to his friend and collaborator HEINRICH WEBER. He had written his *Bunte Bemerkungen* immediately after the *Grundzüge* appeared in 1882, and at that time he had recognized the importance of the theorem of §14 for his own work. However, he could not find a proof of it that he was satisfied with. Then in early 1887 WEBER sent him a work** which DEDEKIND referred to as "your theory of algebraic numbers according to KRONECKER" which led DEDEKIND to refer back to his own remarks on the *Grundzüge* and to his work on the theorem of §14. He became so absorbed with a new line of thought on the problem that he spent a sleepless night,*** at the end of which he had succeeded in solving the problem.

---

* As was seen in Section 9 above, DEDEKIND regarded as the "greatest difficulty" of ideal theory the theorem that if A and B are ideals and $A \subset B$ then there is an ideal C such that $A = BC$. This is easily proved if one can show that for any given ideal A there is an ideal D such that AD is principal. If A is the greatest common divisor of $x_1, x_2, \cdots, x_k$ then an ideal D with the required property is obtained by taking D to be the greatest common divisor of the coefficients y_j of the form $Nm(\alpha)/\alpha$ where $\alpha = x_1 u_1 + \cdots + x_k u_k$. KRONECKER's theorem implies that any x_i (the coefficient of v_i) times any y_j is divisible by the greatest common divisor P of the coefficients of $Nm(\alpha)$. This shows that the principal ideal (P) divides AD. Conversely, AD divides all coefficients of $\alpha \cdot Nm(\alpha)/\alpha = Nm(\alpha)$ and therefore divides their greatest common divisor P, so $AD = (P)$, as desired.

** This work of WEBER does not seem to have been published.

*** The night of 14–15 February 1887, to be exact. DEDEKIND loved to give exact dates. In a letter written to FROBENIUS in 1895 he recalled with pleasure an evening he spent in a Berlin cafe with RIEMANN and WEIERSTRASS in 1859 and he mentioned, parenthetically, that it had been the 25th of September [12, p. 284].

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

What he had discovered was a certain generalization of GAUSS's lemma that enabled him to give a significant simplification of KRONECKER's theory – more significant than even he seems to have realized, because, while he saw the application of the theorem to KRONECKER's theorem of §14 and to the foundations of ideal theory, he seems to have missed the application to the second fundamental theorem. DEDEKIND did not publish this theorem until five years later, when it appeared in the communications of the German mathematical society of Prague [8].

Dedekind's Prague Theorem. Let $P(x)$ and $Q(x)$ be polynomials in one variable whose coefficients lie in an algebraic number field K. If all coefficients of their product $P(x)\,Q(x)$ are integers of K then any coefficient of $P(x)$ times any coefficient of $Q(x)$ must be an integer of K.

The connection of the Prague theorem with GAUSS's lemma can be seen from the following proof of the Prague theorem using ideal theory. Because an arbitrary element of K can be written as an integer of K divided by an ordinary integer, there exist a, $b \in Z$ such that $P(x)=f(x)/a$ and $Q(x)=g(x)/b$ where $f(x)$ and $g(x)$ have integer coefficients, say $f(x)=c_r x^r+\cdots+c_0$ and $g(x)=d_s x^s+\cdots+d_0$. Let P be any ideal prime that divides ab, let μ be the minimum of the multiplicities with which P divides the c's let i be the largest index for which P divides c_i with multiplicity exactly μ, let ν be the minimum of the multiplicities with which P divides the d's, and let j be the largest index for which P divides d_j exactly ν times. The coefficient of x^{i+j} in $f(x)\,g(x)$ is then divisible exactly $\mu+\nu$ times by P. Since $P(x)\,Q(x)=f(x)\,g(x)/ab$ has integer coefficients (by assumption), this coefficient of x^{i+j} must be divisible by ab. Therefore $\mu+\nu$ must be at least as great as the number of times that P divides ab. Therefore any c times any d is divisible by P at least as many times as ab is. Since this holds for all prime divisors P, it follows that any c times any d is divisible by ab, as was to be shown.

DEDEKIND's objective, of course, was to prove the Prague theorem *without* using the theory of ideals, so that it could be used to establish the theory of ideals. He did this as follows.

Proof of the Prague Theorem. Let $P(x)\,Q(x)=f(x)=\eta_0 x^k+\eta_1 x^{k-1}+\cdots+\eta_k$, and let $L \supset K$ be a splitting field for $f(x)$ so that $f(x)=\eta_0(x-\theta_1)(x-\theta_2)\cdots(x-\theta_k)$, where $\theta_1, \theta_2, \cdots, \theta_k$ are in L. The main step of the proof is to show that if θ denotes any one of the k (not necessarily distinct) roots of $f(x)$ then the coefficients of $f(x)/(x-\theta)$ are integers of L.

For this, let $f(x)/(x-\theta)=\eta'_0 x^{k-1}+\eta'_1 x^{k-2}+\cdots+\eta'_{k-1}$. Then

$$\begin{aligned}
\eta'_0 &= \eta_0,\\
\eta'_1 &= \eta_0\theta+\eta_1,\\
\eta'_2 &= \eta_0\theta^2+\eta_1\theta+\eta_2,\\
&\vdots\\
\eta'_{k-1} &= \eta_0\theta^{k-1}+\eta_1\theta^{k-2}+\cdots+\eta_{k-1},\\
0 &= \eta_0\theta^k+\eta_1\theta^{k-1}+\cdots+\eta_k=f(\theta).
\end{aligned}$$

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

Of course $\eta_0'=\eta_0$ is an integer. To see that η_1' is an integer, note that

$$\begin{aligned}
\eta_1' &= \eta_0\theta+\eta_1,\\
\theta\eta_1' &= \eta_0\theta^2+\eta_1\theta,\\
&\vdots\\
\theta^{k-2}\eta_1' &= \eta_0\theta^{k-1}+\eta_1\theta^{k-2},\\
\theta^{k-1}\eta_1' &= \eta_0\theta^k+\eta_1\theta^{k-1}=-\eta_2\theta^{k-2}-\cdots-\eta_k.
\end{aligned}$$

Thus, for each r, $\theta^r\eta_1'$ can be written in the form $\alpha_{r0}+\alpha_{r1}\theta+\alpha_{r2}\theta^2+\cdots+\alpha_{r,k-1}\theta^{k-1}$, where the α's are integers. In other words, the column matrix $(1, \theta, \theta^2, \cdots, \theta^{k-1})$ is annihilated by the matrix $[\alpha_{ri}-\eta_1'\delta_{ri}]$, where $[\delta_{ri}]$ is the identity matrix. Therefore the determinant of this matrix is zero. This gives a polynomial equation of degree k with leading coefficient ± 1 and with the other coefficients integers of K (because they are combinations of the α's) that is satisfied by η_1'. This implies, as was seen in Section 5, that η_1' is an integer. In the same way, for $\eta_2', \eta_3', \cdots, \eta_{k-1}'$ one can always write $\theta^r\eta_s'$ in the form $\alpha_0+\alpha_1\theta+\cdots+\alpha_{k-1}\theta^{k-1}$ and it follows that η_s' is an integer.

Thus the coefficients of $f(x)/(x-\theta)$ are all integers. If θ' is any root of this polynomial, then the same argument shows that $f(x)/(x-\theta)(x-\theta')$ has integer coefficients, and so forth. Therefore the polynomial obtained from $\eta_0(x-\theta_1)(x-\theta_2)\cdots(x-\theta_k)$ by striking out any set of the factors $(x-\theta_i)$ has integer coefficients. In particular, the constant term is an integer, which shows that η_0 times any product of θ's is an integer.

By rearranging the θ's, if necessary, it can be assumed that $P(x)=\alpha(x-\theta_1)\cdot(x-\theta_2)\cdots(x-\theta_r)$ and $Q(x)=\beta(x-\theta_{r+1})\cdots(x-\theta_k)$ where $\alpha\beta=\eta_0$. Each coefficient of $P(x)$ is, up to sign, equal to α times a sum of products of θ's and each coefficient of $Q(x)$ is β times a sum of products of θ's. Thus, a coefficient of $P(x)$ times a coefficient of $Q(x)$ is equal to η_0 times a sum of products of θ's. This proves that every such product is an integer, as was to be shown.

It is simple to deduce from the one variable case that *the Prague theorem also holds for polynomials of several variables*. This can be done using a simple trick due to KRONECKER (*Grundzüge*, §4). Let $P(x_1, x_2, \cdots, x_m)$ and $Q(x_1, x_2, \cdots, x_m)$ be polynomials in several variables with coefficients in some algebraic number field, and suppose that their product has integer coefficients. It is to be shown that any coefficient of P times any coefficient of Q is an integer. For this, let t be a new variable, let g be a positive integer to be determined, and let $\bar{P}(t)$ be the polynomial obtained by substituting t^{g^i} for x_i in $P(x_1, x_2, \cdots, x_m)$. If distinct terms of P correspond to the same term of $\bar{P}$ then g must satisfy a nontrivial polynomial relation $\sum a_i g^i=\sum b_i g^i$. Thus, for all sufficiently large g, distinct terms in P correspond to distinct terms of $\bar{P}$. In the same way let $\bar{Q}(t)$ be obtained from $Q(x_1, x_2, \cdots, x_m)$. Then again, for all sufficiently large g, Q and $\bar{Q}$ have the same number of terms. Choose g large enough that $\bar{P}$ and $\bar{Q}$ have the same number of terms as P and Q. Then the truth of the Prague theorem for $\bar{P}\bar{Q}$ implies its truth for PQ, as desired.

According to HURWITZ [22], KRONECKER's paper [27] of 1883 contains a complete proof of the Prague theorem and "it is clear from the introductory

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

words of this publication that KRONECKER fully recognized the meaning of this theorem for for the foundation of his theory" (the theory of divisors). However, this paper is an obscure one, even by KRONECKER's standards, and it probably would require a reader as knowledgeable and as immersed in the subject as HURWITZ to understand it. In any case, KRONECKER does not spell out the relation of the paper to the theory of divisors and HURWITZ seems to some extent to be reading things into the brief introductory paragraph, which merely says "The attempt to find the simplest foundations for the theory of forms led me quite some time ago to a question which appears at first to be entirely elementary and which I was nevertheless unable to resolve earlier. However, when this question was forced on me anew by other algebraic researches a short time ago, I found the solution by means of extremely simple considerations which, because of the circle of ideas that these researches involved, lay near to hand."* I do not doubt HURWITZ's statement that this paper contains the Prague theorem, but I am forced to admit that I do not see it.

By use of the Prague theorem, the proof of KRONECKER's key theorem that *divisors corresponding to forms with the same coefficients are absolutely equivalent* is immediate. It will suffice to show that if $\alpha = x_1\phi_1 + x_2\phi_2 + \cdots + x_k\phi_k$, where the x's are integers of K and the ϕ's are products of powers of indeterminates, then, for each i, all coefficients of the form $x_i Nm(\alpha)/\alpha$ are divisible by the greatest common divisor P of the coefficients of $Nm(\alpha)$. (This is the definition of $x_i \equiv 0 \bmod [\alpha]$.) Since all coefficients of $\alpha \cdot Nm(\alpha)/\alpha = Nm(\alpha)$ are divisible by P, this follows immediately from the Prague theorem.

14. Dedekind and Kronecker

Because DEDEKIND and KRONECKER had such similar interests, one would expect there to have been more communication between them. They drew their inspiration from the same writers – GAUSS, DIRICHLET, GALOIS, ABEL, KUMMER – and worked on many of the same subjects – generalizing KUMMER's theory not just to number fields but also to function fields, clarifying the foundations of analysis, and unifying GALOIS theory with number theory. Still, they seem to have had very little personal acquaintance and even very little correspondence.

The reason for this lack of contact was probably that their basic attitudes were so totally different that each felt that it would be fruitless to enter into a discussion of mathematical substance. KRONECKER in proposing DEDEKIND for nomination as a corresponding member of the Berlin Academy [1a] said that DEDEKIND's "terminology and much in his method of handling the rather delicate material"** of number theory made judgment of his work more difficult,

* Das Streben nach Erforschung der einfachsten Grundlagen der Theorie der Formen hat mich schon vor langer Zeit auf eine Frage geführt, die dem Anscheine nach ganz elementar ist, und die ich dennoch früher nicht zu erledigen vermochte. Als sich mir aber vor Kurzem bei anderen algebraischen Untersuchungen jene Frage von Neuem aufdrängte, fand ich die Lösung durch höchst einfache Betrachtungen, die mir durch die Ideensphäre, in welcher sich diese Untersuchungen bewegten, sehr nahe gelegt wurden.

** die... Terminologie und auch Manches in der Behandlungsweise des etwas spröden Stoffes ...

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

but that it was precisely the value of DEDEKIND's number-theoretical works on which he based the proposal. For his part, DEDEKIND [10] said he "could not make friends with"† KRONECKER's basic method of undetermined coefficients and that "mixing it with the theory of function of variables muddies the purity of the theory"* of ideals, but on many occasions he expressed his high regard for KRONECKER and his work. An extreme example of this is quoted below.

Not only their mathematical tastes differed. They were men of very different temperaments and inclinations. KRONECKER was a wealthy man who associated with some of the most cultured and powerful people in the Prussian capital of Berlin. DEDEKIND was a retiring man who lived most of his life in his native Braunschweig. KRONECKER lectured at Berlin University beginning in 1861, when his election to membership in the Berlin Academy afforded him this privilege, and he was named to a professorship in Berlin in 1883 when his friend KUMMER retired. DEDEKIND, after leaving Göttingen, where he was a Privat-Dozent, taught for four years 1858–1862 at the Polytechnic Institute in Zurich, and spent the rest of his teaching career at the Polytechnic Institute of Braunschweig. He declined several university appointments which would have taken him away from Braunschweig, but when he retired from teaching at age 62 in 1894 he wrote to FROBENIUS** that he probably would not have retired so soon from university teaching but that his duties in Braunschweig were too strenuous. KRONECKER was a devoted family man who died soon after his wife died. DEDEKIND was a bachelor.

We know that the two men spent some time together in 1880 when KRONECKER visited Braunschweig for the unveiling of a monument to GAUSS, and that they never met again after that (see below). They may have met before – KRONECKER visited DIRICHLET in Göttingen when DEDEKIND was an outstanding young student there – but they probably avoided each other because they knew they were working on similar things and they wanted to avoid any appearance of plagiarism. This problem is touched on by DEDEKIND in the following lines from a letter he wrote in 1877 to his former student EDUARD SELLING:

"... Herr KRONECKER remarks in his letter to you, which I am herewith returning, that his results in number theory (by which he clearly means those in the area of the theory of ideal numbers) have also been known to me for years. I cannot understand this; even today I do not know what *results* KRONECKER has achieved. The goal of the general theory of ideals is of course very obvious, after KUMMER's solution of the special case of cyclotomic integers, and in my view it can only be a question of the *foundations*, that is, of the introduction of the concepts which lead to this goal; to me, at least, this goal, the creation of the general laws of divisibility of algebraic integers, has been completely clear from the beginning, without any communication from KRON-

† nicht befreunden konnte

* durch die Einmischung der Funktionen von Variablen die Reinheit der Theorie nach meiner Ansicht getrübt wird.

** See [12, p. 279].

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

ECKER. On the contrary, I have in fact a rather unclear indication in a letter from KRONECKER of the *path* that he has blazed; it is to this passage that I allude both in the introduction to the second edition of DIRICHLET's *Zahlentheorie* and in a passage of §10 of my article "Sur la théorie des nombres entiers algebraiques" which is now appearing in the Bulletin of Darboux and Houël and which has long been finished and in the possession of the latter in Bordeaux. There can be no question of (*von... keine Rede sein*) an influence of this communication from KRONECKER on my own theory, and I was eager to inform you of this because the passage of KRONECKER's letter I refer to could easily be wrongly construed..." [12, pp. 160–161].

It seems there could very easily have been a conflict between the two men, and both CANTOR and FROBENIUS tried to persuade DEDEKIND that KRONECKER had wronged him. CANTOR in 1882 told DEDEKIND that "the little despot", meaning KRONECKER, was holding up publication of the DEDEKIND-WEBER paper in *Crelle,* of which KRONECKER was the editor, until the *Grundzüge* had appeared.* Indeed, KRONECKER did hold up publication of the paper, but he said publicly [25] that this had been agreed on in advance between him and the joint authors, DEDEKIND & WEBER. DEDEKIND, in his reply to CANTOR, showed some irritation toward KRONECKER. Although he and WEBER both expressed many times the wish that KRONECKER would publish his theory, he denied that there had been an agreement such as KRONECKER described.** And even if KRONECKER had asked for such an agreement, he wrote, they would naturally have expected that it was a question of works of KRONECKER that were *already finished* and would never have expected that they would have to wait 16 months, as they did, before they received galley proofs of their own paper. "Still," DEDEKIND wrote, "I have no doubt that KRONECKER *believes* that he dealt with the matter honorably and I do not judge him as harshly as you; he means no harm, but he sometimes suffers from self-deception. Once a few years ago I had it out with him openly, and I must say that the way he responded to it left me, in the end, with a very good impression."***

FROBENIUS, in 1895, several years after KRONECKER's death, received a similar response when he tried to convince DEDEKIND that KRONECKER did not deserve the consideration he was giving him. DEDEKIND had sent FROBENIUS KRONECKER's famous "Jugendtraum" letter for publication, but asked that the last page not be published because it contained nothing of mathematical

---

* [12, p. 252].

** However, DEDEKIND, in 1894, in the preface to the 4th edition of DIRICHLET's *Zahlentheorie*, reversed himself entirely and said that there *had* been such an agreement.

*** [12], pp. 253–254. Doch zweifle ich gar nicht daran, dass KRONECKER *glaubt,* loyal gehandelt zu haben; ich beurtheile ihn nicht so streng wie Sie; er denkt sich nichts Arges, nur ist er bisweilen in Selbsttäuschungen befangen. Ich habe einmal vor einigen Jahren eine offene Auseinandersetzung mit ihm gehabt und muss sagen, dass die Art, wie er dieselbe aufgenommen, mir schliesslich einen sehr guten Eindruck hinterlassen hat. (DEDEKIND goes on to say that for at least 20 years prior to this incident he had no contact whatever (gar keinen Verkehr) with KRONECKER.)

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

importance and because it contained "some unfortunately chosen words which led to a candid discussion between KRONECKER and myself which was concluded in a thoroughly satisfactory manner and which the public doesn't need to know anything about."† FROBENIUS, having read the passage in question, urged DEDEKIND to let him publish it because it is the only place where "KRONECKER unreservedly acknowledges your priority in the publication of ideal theory," an acknowledgement that FROBENIUS found all the more striking* because "I know for sure that he never forgave you for this publication." He was not able to see** what it was that DEDEKIND wanted the public not to see, but thought it might be KRONECKER's mention of "priority rights that you have secured for yourself by earlier publication." DEDEKIND's response was to send FROBENIUS the further correspondence he had with KRONECKER in 1880. "You will see from this how I feel about so-called priority, which is much less valuable to me than the independence of my research, an independence to which KRONECKER has given sufficiently clear testimony in various places. I have always been far from wanting to compare my *aurea mediocritas,* the strength of which lies in obstinate perseverance, with KRONECKER's outstanding talent, and therefore I also do not want to create a situation which would give new rise to questions about priority. Moreover, KRONECKER, to remove any trace of dissonance, came to Braunschweig at the end of June of the same year of 1880 for the unveiling of our GAUSS monument, and here we discussed a greal deal in a very friendly manner. Also, after that, we occasionally exchanged other friendly letters, without seeing each other again; but because of his thoroughly worthy behavior on that occasion*** I preserve of him, personally as well, a warm and grateful memory."††

† einige nicht glücklich gewählte Worte, die noch eine offenherzige und in durchaus befriedigender Weise abgeschlossene Discussion zwischen KRONECKER und mir veranlasst haben, wovon aber das Publicum gar Nichts zu ahnen braucht. [12, pp. 278–279]

* It is strange that FROBENIUS found it striking. How could KRONECKER do otherwise? DEDEKIND's theory was published in 1871 and KRONECKER published nothing until 1882.

** Note how sensitive these issues are. FROBENIUS was not able to find the offending passage in KRONECKER's letter, but it had so upset DEDEKIND in 1880 that it led him to "have it out" (*eine offene Auseinandersetzung zu haben*) with KRONECKER, as he told CANTOR in 1882.

*** This is the same occasion that DEDEKIND mentioned to CANTOR in the quotation above.

†† Sie werden daraus ersehen, wie ich über die sogenannte Priorität denke, die mir viel weniger wertvoll ist als die Selbständigkeit meiner Forschung, die ja von KRONECKER an verschiedenen Stellen hinreichend deutlich bezeugt ist. Ich bin stets weit davon entfernt gewesen, meine aurea mediocritas, deren Stärke nur in hartnäckiger Ausdauer liegt, mit KRONECKER's hervorragender Begabung vergleichen zu wollen, und wünsche daher auch nicht, neuen Anlass zur Erörterung von Prioritäts-Fragen zu geben. Ich füge noch hinzu, dass KRONECKER, um jede Spur eines Missklanges zu verwischen, Ende Juli desselben Jahres 1880 zur Enthüllung unseres Gauss-Denkmales nach Braunschweig kam, wo wir sehr Vieles freundschaftlich besprochen haben. Auch später haben wir gelegentlich noch freundliche Briefe gewechselt, ohne uns wiederzusehen; aber wegen seiner durchaus würdigen Haltung bei jener Angelegenheit bewahre ich ihm auch persönlich ein herzliches und dankbares Andenken. [12, pp. 282–283]

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

Those who accept CANTOR's and FROBENIUS' views of KRONECKER will feel that DEDEKIND met him more than halfway. However, CANTOR and FROBENIUS were often harsh in their judgements of other mathematicians and quick to take offense.* KRONECKER was a forceful man with strong opinions that often led him to clash with other mathematicians, but, according to the published record, he seems to have been very correct and forthright in his dealings with others, the many complaints against him notwithstanding. I am inclined to accept DEDEKIND's assessment of him. It is pleasing to think of these two great mathematicians, disagreeing as profoundly as they did about basic issues, continuing to hold each other in the highest regard and to recognize the value and the unquestioned independence of each other's work.

Appendix. A reformulation of Kronecker's theory

The discussion of KRONECKER's theory in Sections 11 and 12 follows fairly closely KRONECKER's treatment in order to make the relevant portions of the *Grundzüge* accessible to the reader. However, in order to make the theory itself accessible to a modern reader, it is probably helpful to reformulate it somewhat.

As before, let K be a normal, algebraic extension of the rational number field Q. (KRONECKER deals with the much more general case of a normal, algebraic extension of the field of rational functions in a finite number of variables, which he denotes R, R', R'',..., with coefficients in Z, and of course this greater generality is part of the power of his theory. However, for the sake of simplicity, only the case where there are *no* variables, which KRONECKER indicates by writing $R=1$, will be treated here.) Once this case has been developed, the case in which K is not normal can be handled very easily, as will be seen at the end of this Appendix.

KRONECKER's "method of undetermined coefficients" is to *consider integral forms with coefficients in K*, that is, polynomials in an infinite set of indeterminates (only a finite number of which occur, of course, in any one polynomial) with coefficients that are integers in the algebraic number field K. The set of such forms will be denoted by I. It is a ring because sums and products of integers are integers. Given a form $\alpha \in I$, its *norm*, denoted $Nm(\alpha)$, is defined to be the product of its n conjugates, where n is the degree of the normal extension $K \supset Q$ and where the n elements of the GALOIS group of K over Q act on α by acting on its coefficients and leaving the indeterminates it contains invariant. Thus $Nm(\alpha) \in I$ and, since it is obviously invariant under all conjugations, the coefficients of $Nm(\alpha)$ are in fact in Z.

A form with coefficients in Z is said to be *primitive* if the greatest common divisor of its coefficients is 1. According to GAUSS's lemma, the product of primitive forms is primitive (see Section 11). A form $\alpha \in I$ is said to be *primitive* if $Nm(\alpha)$ is primitive. (Since a form α with coefficients in Z can be regarded as being in I, there are two definitions here of what it means for α to be

* In the case of FROBENIUS, however, mention should be made of his memorial lecture [19] on KRONECKER, where he eloquently and movingly praises KRONECKER, both as a mathematician and as a human being.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

primitive in this case. However, there is no conflict because then $Nm(\alpha)=\alpha^n$ and GAUSS's lemma shows that α^n is primitive if and only if α is.) Since $Nm(\alpha\beta)=Nm(\alpha)\,Nm(\beta)$, GAUSS's lemma shows that a product of two primitive forms in I is itself primitive.

The basic principle of KRONECKER's theory is to regard primitive forms as units, that is, as elements that are multiplicatively neutral.

Definition. Two forms $\alpha, \beta \in I$ are said to be *equivalent* if there exist primitive forms $\delta_1, \delta_2 \in I$ such that $\alpha\delta_1=\beta\delta_2$.

It is simple to show not only that this is an equivalence relation on I but also that equivalence classes can be multiplied in the obvious way. In fact, if the nonzero elements of I are regarded as a commutative semigroup under multiplication then what is involved is simply the *quotient* of this semigroup with respect to the subsemigroup of primitive forms. Explicitly, if α is equivalent to β and β equivalent to γ then $\alpha\delta_1=\beta\delta_2$ and $\beta\delta_3=\gamma\delta_4$ where the δ's are primitive, and $\alpha\delta_1\delta_3=\beta\delta_2\delta_3=\gamma\delta_2\delta_4$, so that α is equivalent to γ. Thus equivalence is reflexive, symmetric, and transitive. If α is equivalent to β then obviously $\alpha\gamma$ is equivalent of $\beta\gamma$ for all γ.

In an adaptation of KRONECKER's notation, the equivalence class of α will be denoted by $[\alpha]$. Thus $[\alpha]=[\beta]$ is a way of saying that the forms α and β are equivalent. It will be seen below that this condition $[\alpha]=[\beta]$ is the same as the condition that, in KRONECKER's terminology, the divisors $\mathrm{mod}[\alpha]$ and $\mathrm{mod}[\beta]$ be absolutely equivalent. (KRONECKER himself, in the second paragraph of §19, makes passing mention of the fact that $\mathrm{mod}[\alpha]\sim\mathrm{mod}[\beta]$ if and only if α/β is equal to a quotient of primitive forms, which is precisely the condition $\alpha\delta_1=\beta\delta_2$.)

It is clear that the equivalence class of the form 0 consists of the single form 0 itself. A *divisor* with coefficients in K is an equivalence class of forms in I other than the class [0]. Since, as was remarked above, there is a natural operation of multiplication of divisors, there is a natural meaning to the statement that $[\alpha]$ divides $[\beta]$, namely, that there exists a form γ such that $[\beta]=[\alpha]\,[\gamma]$.

Proposition. The statement that $[\alpha]$ divides $[\beta]$ is equivalent to any one of the following three statements:

(i) The integer P which is the greatest common divisor of the coefficients of $Nm(\alpha)$ divides all coefficients of the form $\beta Nm(\alpha)/\alpha \in I$.

(ii) The form $\alpha \in I$ divides the form $\beta Fm(\alpha)$ where $Fm(\alpha)=Nm(\alpha)/P$, with P as in (i).

(iii) There is a primitive form δ such that α divides $\beta\delta$.

The proof of this proposition is facilitated by the following lemma, which is the essence of KRONECKER's "first fundamental theorem".

Lemma. If $\alpha, \beta \in I$, if α is a constant form – that is, if α is simply an integer of K – and if $[\alpha]$ divides $[\beta]$ then α divides all the coefficients of β.

Proof. Since $[\alpha]$ divides $[\beta]$ by assumption, $[\beta]=[\alpha][\gamma]$ for some $\gamma \in I$, that is, $\beta\delta_1=\alpha\gamma\delta_2$ for primitive $\delta_1, \delta_2 \in I$. Set $\delta=\delta_1$ and $\theta=\gamma\delta_2$ so that this equation takes the form $\beta\delta=\alpha\theta$ where δ is primitive. Loosely speaking, this means

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

$\beta/\alpha=\theta/\delta$ and what is to be shown is that $Nm\left(X-\frac{\beta}{\alpha}\right)=Nm\left(X-\frac{\theta}{\delta}\right)$ has integer coefficients. More precisely, let X be a new indeterminate and consider

$$Nm(\delta)\ Nm(\alpha X-\beta)=Nm(\alpha\delta X-\beta\delta)=Nm(\alpha\delta X-\alpha\theta)=Nm(\alpha)\ Nm(\delta X-\theta).$$

Here $Nm(\alpha)\in Z$, because α is a constant form, and $Nm(\delta)$ is primitive. Therefore, by GAUSS's lemma, $Nm(\alpha)$ divides all coefficients of $Nm(\alpha X-\beta)$. In other words the form β/α with coefficients in K (not necessarily integral) has the property that $Nm\left(X-\frac{\beta}{\alpha}\right)$, considered as a polynomial in X, has all its coefficients in I. It is to be shown that this implies that β/α itself is in I. The validity of this implication is precisely the implicit theorem in KRONECKER's theory that DEDEKIND objected to and that HURWITZ, many years later, gave a simple proof of (see Section 11 above). Thus $\beta/\alpha\in I$.

Proof of the Proposition. If $[\alpha]$ divides $[\beta]$ then (i) is true. For this, multiply the assumed equation $\beta\delta_1=\alpha\gamma\delta_2$ by $Nm(\alpha)/\alpha\in I$. Then P, since it divides $Nm(\alpha)\gamma\delta_2$, must divide $\beta\delta_1\ Nm(\alpha)/\alpha$. Thus $[P]$ divides $[\beta Nm(\alpha)/\alpha]$ and (i) follows from the lemma.

(i) implies (ii). Given (i) set $\gamma=P^{-1}\beta\,Nm(\alpha)/\alpha$. Then $\alpha\gamma=\beta\,Fm(\alpha)$ and (ii) follows.

(ii) implies (iii). $Fm(\alpha)$ is primitive.

(iii) implies $[\alpha]$ divides $[\beta]$. If $\beta\delta=\alpha\gamma$ then $[\beta]=[\beta\delta]=[\alpha\gamma]=[\alpha]\,[\gamma]$.

The following statements are all easy to verify. If $[\alpha]\,[\beta]=[\alpha]\,[\gamma]$ then $[\beta]=[\gamma]$. If $[\alpha]$ divides $[1]$ then $[\alpha]=[1]$. If $[\alpha]$ divides $[\beta]$ and $[\beta]$ divides $[\alpha]$ then $[\alpha]=[\beta]$. (If $[\beta]=[\alpha]\,[\gamma_1]$ and $[\alpha]=[\beta]\,[\gamma_2]$ then $[\beta]=[\beta]\,[\gamma_1]\,[\gamma_2]$, $[1]=[\gamma_1]\,[\gamma_2]$, $[\gamma_1]=[1]$.) $[\alpha]=[\beta]$ if and only if, in KRONECKER's terminology, the divisors mod$[\alpha]$ and mod$[\beta]$ are absolutely equivalent. (By (i), mod$[\alpha]$ divides mod$[\beta]$ if and only if $[\alpha]$ divides $[\beta]$.) If $[\alpha]$ divides both $[\beta]$ and $[\gamma]$ then it divides $[\beta+\gamma]$.

The two main theorems in the theory of divisors are that *unique factorization into primes holds for divisors* and *a divisor is the greatest common divisor of its coefficients*. In KRONECKER's view, unique factorization into primes is of secondary importance and he prefers to keep it in the background because the notion of "prime" is a relative one, one that changes if the field K is extended. In fact, KRONECKER appears to deal with the subject of unique factorization only because it entered into his proof of the "second fundamental theorem" that a divisor is the greatest common divisor of its coefficients. This theorem can also be formulated as the statement that *a divisor divides all its coefficients* or as the statement that *two forms with the same coefficients are equivalent*.

Once the second fundamental theorem is proved, unique factorization into primes is easy to deduce from elementary facts about linear divisors (see below). On the other hand, as was shown in Section 13, the second fundamental theorem is a simple consequence of the *Prague Theorem: If two forms α and β with coefficients in K have the property that $\alpha\beta$ has integral coefficients then any coefficient of α times any coefficient of β is an integer of K.* This theorem was proved in Section 13. For a simple, general, and explicitly constructive

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

proof of this theorem see pp. 74–80 of J. KÖNIG's *Einleitung in die allgemeine Theorie der algebraischen Grössen* (Teubner, Leipzig, 1903).

The second fundamental theorem follows immediately when one defines, for a given form α, P to be the greatest common divisor of the coefficients of $Nm(\alpha)$, and defines β to be $P^{-1}\, Nm(\alpha)/\alpha$, because then $\alpha\beta = Nm(\alpha)/P$ is integral; by the Prague theorem, any coefficient of α times any coefficient of $P^{-1}\, Nm(\alpha)/\alpha$ is an integer, and it follows from (i) of the proposition above that any coefficient x_i of α has the property that $[x_i]$ is divisible by $[\alpha]$ as was to be shown. Thus, if α and γ have the same coefficients then $[\alpha]$ divides all the coefficients of γ so that $[\alpha]$ divides $[\gamma]$; for the same reason, $[\gamma]$ divides $[\alpha]$, and it follows that $[\alpha]=[\gamma]$. In particular, γ can be chosen to be a linear form with the same coefficients as α, so that *every divisor is a linear divisor,* that is, can be written as $[\gamma]$ where γ is a linear form.

The unique factorization of divisors can now be deduced as follows. A divisor $[\alpha]$ is said to be *irreducible* if the only factorizations $[\alpha]=[\beta]\,[\gamma]$ are those in which $[\beta]=[1]$ or $[\gamma]=[1]$. Then an irreducible divisor is *prime* in the sense that it can divide a product only if it divides one of the factors. For the proof of this fact, let $[\alpha]$ be an irreducible divisor that divides $[\beta]\,[\gamma]$ but does not divide $[\beta]$. It is to be shown that $[\alpha]$ divides $[\gamma]$. It can be assumed, of course, that the forms α and β involve distinct variables (and even that they involve them all linearly). Then $[\alpha+\beta]$ divides all its coefficients and therefore divides $[\alpha]$, say $[\alpha]=[\alpha+\beta]\,[\varepsilon]$. Since $[\alpha]$ is irreducible, either $[\alpha+\beta]=[1]$ or $[\varepsilon]=[1]$. If $[\varepsilon]=[1]$ then $[\alpha]=[\alpha+\beta]$ divides $[\beta]$, contrary to assumption. Therefore $[\alpha+\beta]=[1]$, from which it follows that $[\gamma]=[\gamma]\,[\alpha+\beta]=[\alpha\gamma+\beta\gamma]$ is divisible by $[\alpha]$ because, by assumption, $[\alpha]$ divides $[\beta\gamma]$.

One other fact is needed for the proof of unique factorization, namely, the fact that every divisor is divisible by an irreducible one. Since divisors have norms $(Nm([\alpha])=[Nm(\alpha)]=[P\cdot Fm(\alpha)]=[P])$ that are divisors of elements of Z and since elements of Z can only be factored nontrivially a finite number of times, this is clear in an existential sort of way. More concretely, any divisor which divides $[\alpha]$ also divides $[Nm(\alpha)]=[P]$, where $P\in Z$, and, as was shown in Section 12, there are only a finite number of linear divisors that divide $[P]$, so that at least one divisor of $[P]$ must be irreducible. Unique factorization of divisors into prime divisors now follows from exactly the same arguments that prove unique factorization into primes for positive integers.

This completes the development of the main features of the theory of divisors. Consider, finally, the case in which the field K under consideration is not normal. KRONECKER's approach to this problem is to embed K in a normal field, say L, and to observe that the essential concepts (not including the concept of a prime divisor) are *absolute* in the sense that they are unchanged if L is extended. The basic observation here is that the criterion (i) of the Proposition above is unchanged under extension of the field: if L and L' are normal extensions of K, and if $L\subset L'$, then* $Nm_{L'}(\alpha)=Nm_{L}(\alpha)^{j}$ where j is the degree of

* KRONECKER, however, defined the norm in an "absolute" way, by not taking more conjugates than are necessary to make it lie in Q, or, to say the same thing in a more precise way, he took the norm to be the constant term of the irreducible monic

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

L' over L (the conjugates of α in L' are the same as its conjugates in L but are counted j times as often) so that $\beta Nm(\alpha)/\alpha$ is multiplied by $Nm(\alpha)^{j-1}$ and P is multiplied by P^{j-1}.

In terms of the theory as it is presented in this section, the theory for nonnormal fields can be described as follows. Let $L \supset K$ be an extension of K that is normal over Q. The theory of divisors for L is developed above. The divisors for K are naturally embedded in these, namely, the divisors of the form $[\alpha]$ where the coefficients of α all lie in K. The main fact is that for divisors in K divisibility in L is the same as divisibility in K, that is, if α and β are integral forms with coefficients in K such that there is an integral form γ with coefficients in L such that $[\alpha]=[\beta][\gamma]$ then there is an integral from δ with coefficients in K such that $[\alpha]=[\beta][\delta]$. This is easily proved as follows. By (i) of the Proposition above, the form $\delta = P^{-1}\beta Nm(\alpha)/\alpha$ is integral. Thus it will suffice to show that its coefficients lie in K, and for this it suffices to show that the coefficients of $Nm(\alpha)/\alpha$ all lie in K. This follows from the fact that the division algorithm can be used to divide $Nm(X-\alpha)$ by $X-\alpha$ (in the ring of polynomials in X with coefficients that are forms in K) and the constant term in the quotient is $\pm Nm(\alpha)/\alpha$.

KRONECKER, for reasons explained above, did not include unique factorization into primes as a part of his divisor theory, and therefore did not consider unique factorization into primes for divisors in a nonnormal field K. However, once it is proved that division of divisors in K, when possible, always yields divisors in K, the above proof of unique factorization for divisors in a normal field applies equally well to nonnormal fields.

This material is based on work supported by the U.S. National Science Foundation Grant SOC-7905162 and by the Vaughn Foundation.

References

1a. BIERMANN, KURT-R., Richard Dedekind im Urteil der Berliner Akademie, *Forschungen und Fortschritte,* **40** (1966) 301–302.

1b. BOURBAKI, N., *Eléments d'Histoire des Mathématiques,* Deuxième édition, Hermann, Paris, 1969.

2. DEDEKIND, R., *Gesammelte mathematische Werke,* R. FRICKE, E. NOETHER & O. ORE, eds., 3 Vols., Vieweg, Braunschweig, 1930, 1931, 1932.

3. DEDEKIND, R., Supplement X to *Vorlesungen über Zahlentheorie* von P. G. Lejeune Dirichlet (2nd Ed.) Vieweg, Braunschweig, 1871; also (in part) *Werke,* Vol. 3, 223–261.

4. DEDEKIND, R., *Sur la théorie des nombres entiers algébriques,* Gauthier-Villars, 1877; also *Bull. des Sci. Math. Astron.,* (1), **11** (1876) 278–288; (2), **1** (1877) 17–41, 69–92, 144–164, 207–248 and (in part) *Werke,* Vol 3, 263–296.

5. DEDEKIND, R., Unpublished German Draft of [4], Göttingen State and University Library, Nachlass DEDEKIND, IV, 4.

6. DEDEKIND, R., Supplement XI to *Vorlesungen über Zahlentheorie* von P. G. Lejeune Dirichlet (3rd Ed.), Vieweg, Braunschweig, 1879; also (in part) *Werke*, Vol. 3, 297–313.

---

equation satisfied by an algebraic number. Although this definition is crucial to KRONECKER's viewpoint that the entire theory should remain unchanged if the field is embedded in a larger field, it has the serious drawback that the norm of a product is not always the product of the norms.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

7. DEDEKIND, R., *Bunte Bemerkungen zu Kronecker: Grundzüge einer arithmetischen Theorie der algebraischen Grössen* (§§ 1–22), unpublished manuscript in the Göttingen State and University Library (soon to be published). Nachlass DEDEKIND VII, 14.
8. DEDEKIND, R., Über einen arithmetischen Satz von Gauss, *Mitt. Deut. Math. Ges. Prag,* 1892, 1–11; also *Werke,* Vol. 2, 28–38.
9. DEDEKIND, R., Supplement XI to *Vorlesungen über Zahlentheorie* von P. G. Lejeune Dirichlet (4th Ed.) Vieweg, Braunschweig, 1894; also (in full) *Werke,* Vol. 3, 1–222.
10. DEDEKIND, R., Über die Begründung der Idealtheorie, *Nachr. Königl. Ges. wiss. Göttingen,* Math.-phys. Kl., 1895, 106–113, also *Werke,* Vol. 2, 50–58.
11. DEDEKIND, R., Various unpublished letters, Göttingen State and University Library, Nachlass DEDEKIND, XIII.
12. DUGAC, P., *Richard Dedekind et les Fondements des Mathématiques,* Vrin, Paris, 1976.
13. EDWARDS, H. M., *Advanced Calculus,* Houghton Mifflin, Boston, 1969; Reprint, Krieger Publ. Co., New York, 1980.
14. EDWARDS, H. M. The Background of Kummer's proof of Fermat's Last Theorem for regular primes, *Arch. Hist. Exact Sci.,* **14** (1975) 219–236.
15. EDWARDS, H. M., Postscript to "The Background of Kummer's Proof...", *Arch. Hist. Exact Sci.* **17** (1977) 381–394.
16. EDWARDS, H.M. *Fermat's Last Theorem,* Springer, New York Heidelberg Berlin, 1977.
17. EICHLER, M., *Einführung in die Theorie der algebraischen Zahlen und Funktionen,* Birkhäuser, Basel, 1963; English transl., Academic Press, New York, 1966.
18. EULER, L. *Vollständige Anleitung zur Algebra,* St. Petersburg, 1970; also *Opera* (1), Vol. 1.
19. FROBENIUS, G., Gedächtnisrede auf Leopold Kronecker, *Abh. königl. Preuss. Akad. Wiss.* Berlin, 1893, 3–22; also *Gesammelte Abhandlungen,* Vol. 3, 705–724.
20. HILBERT, D., Die Theorie der algebraischen Zahlkörper, *Jahresber. der Deut. Math. Verein.* **4** (1897) 175–546; also *Gesammelte Abhandlungen,* Vol. 1, 63–363.
21. HURWITZ, A., Über die Theorie der Ideale, *Nachr. königl. Ges. Wiss. Göttingen,* Math.-phys. Kl., 1894, 291–298; also *Werke,* Vol. 2, 191–197.
22. HURWITZ, A., Über einen Fundamentalsatz der arithmetischen Theorie der algebraischen Grössen, *Nachr. königl. Ges. Wiss. Göttingen,* Math.-phys. Kl., 1895, 230–240; also *Werke,* Vol. 2, 198–207.
23. KRONECKER, L., *Werke,* K. HENSEL, ed., 5 Vols., Teubner, Leipzig, 1895, 1897, 1899, 1929, 1930; Reprint, Chelsea, New York, 1968.
24. KRONECKER, L., Auszug aus einem Briefe von L. Kronecker an R. Dedekind vom 15 März 1880, *Sitzber. königl. Preuss. Akad. Wiss. Berlin,* 1895, 115–177; also *Werke,* Vol. 5, 453–457.
25. KRONECKER, L., Über die Discriminante algebraischer Functionen einer Variabeln, *Jour. für Math.* (Crelle), **91** (1881) 301–334; also *Werke,* Vol. 2, 193–236.
26. KRONECKER, L., *Grundzüge einer arithmetischen Theorie der algebraischen Grössen,* Reimer, Berlin, 1882; also *Jour. für Math.* (Crelle) **92** (1882) 1–122 and *Werke,* Vol. 2, 239–387.
27. KRONECKER, L., Zur Theorie der Formen höherer Stufen, Monatsber. königl. Preuss. Akad. Wiss. Berlin, 1883, 957–960; also *Werke,* Vol. 2, 417–424.
28. KUMMER, E. E., *Collected Papers,* ANDRÉ WEIL, ed., Springer-Verlag: Berlin, Heidelberg, New York, 1975.
29. KUMMER, E. E., De numeris complexis, qui radicibus unitatis et numeris integris realibus constant, *Gratulationschrift der Univ. Breslau zur Jubelfeier der Univ. Königsberg;* Reprint, *Jour. de Math.***12** (1847) 185–212 and *Collected Papers,* Vol. 1, 165–192.
30. KUMMER, E. E., Zur Theorie der Complexen Zahlen, *Monatsber. Akad. Wiss. Berlin,* 1846, 87–96; also *Jour. für Math.* (Crelle) **35** (1847) 319–326 and *Collected Papers,* Vol. 1, 203–210.

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms

31. KUMMER, E. E., Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren, *Jour. für Math.* (Crelle) **35** (1847) 327–367; also *Collected Papers,* Vol. 1, 211–251.
32. KUMMER, E. E., Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers, *Jour. de Math.* **16** (1851) 377–498; also *Collected Papers,* Vol. 1, 363–484.
33. KUMMER, E. E., Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist, *Math. Abh. köngl. Akad. Wiss. Berlin,* 1856, 1–47; also *Collected Papers,* Vol. 1, 583–629.
34. KUMMER, E. E., Über die den Gaussischen Perioden der Kreisteilung entsprechenden Congruenzwurzeln, *Jour. für Math.* (Crelle) **53** (1857) 142–148; also *Collected Papers,* Vol. 1, 574–580.
35. KUMMER, E. E., Über die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist, *Math. Abh. köngl. Akad. Wiss. Berlin,* 1859, 19–159; also *Collected Papers,* Vol. 1, 699–839.
36. MERTENS, F., Über einen algebraischen Satz, *Ber. königl. Akad. Wiss. Wien,* 1892, 1560–1566.
37. SELLING, E., Über die idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln einer beliebigen irreductibeln Gleichung rational gebildet sind, *Schlömilch's Zeitschr. für Math. u. Phys.* **10** (1865) 17–47.
38. WEYL, H., *Algebraic Theory of Numbers,* Princeton Univ. Press, Princeton, 1940.

Courant Institute of
Mathematical Sciences
New York University

(Received June 5, 1980)

This content downloaded from 87.81.151.195 on Fri, 27 Jul 2018 22:02:05 UTC
All use subject to https://about.jstor.org/terms