

The Roots of Commutative Algebra in Algebraic Number Theory
Author(s): Israel Kleiner
Source: *Mathematics Magazine*, Vol. 68, No. 1 (Feb., 1995), pp. 3-15
Published by: Mathematical Association of America
Stable URL: http://www.jstor.org/stable/2691370
Accessed: 15-01-2016 12:10 UTC

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at http://www.jstor.org/page/info/about/policies/terms.jsp

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.



Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *Mathematics Magazine*.

http://www.jstor.org

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

ARTICLES

The Roots of Commutative Algebra in Algebraic Number Theory

ISRAEL KLEINER
York University
North York, Ontario, Canada M3J 1P3

Introduction

The concepts of field, (commutative) ring, ideal, and unique factorization are among the fundamental notions of (commutative) algebra. How did they arise? In large measure, from three central problems in number theory: Fermat's Last Theorem, reciprocity laws, and binary quadratic forms. In this paper we will describe how this happened.

To put the issues in a broader context, these three number-theoretic problems were instrumental in the emergence of algebraic number theory—one of the two main sources of the modern discipline of commutative algebra.[1] The other source was algebraic geometry. It was in the setting of these two subjects that many of the main concepts and results of commutative algebra evolved in the 19th century. Thus commutative algebra can be said to have been well developed before it was created.

To set the scene for our story, a word about mathematics, and especially algebra, in the 19th century. The period witnessed fundamental transformations in mathematics —in its concepts, its methods, and in mathematicians' attitude toward their subject. These included a growing insistence on rigor and abstraction; a predisposition for founding general theories rather than focusing on specific problems; an acceptance of nonconstructive existence proofs; the emergence of mathematical specialties and specialists; the rise of the view of mathematics as a free human activity, neither deriving from, nor dependent on, nor necessarily applicable to concrete setting; the rise of set-theoretic thinking; and the reemergence of (a new variant of) the axiomatic method. As for algebra, its subject-matter and methods changed beyond recognition. Algebra as the study of solvability of polynomial equations gave way to algebra as the study of abstract structures defined axiomatically. While in the past algebra was on the periphery of mathematics, it now (the 19th and early 20th centuries) became one of its central concerns. Moreover, algebra began to penetrate other mathematical fields (e.g. geometry, analysis, logic, topology, number theory) to such an extent that in the early decades of the 20th century one began to speak of the algebraization of mathematics ([3, p. 135] and [22]).

[1] Commutative algebra is nowadays understood to be the study of commutative noetherian rings. The first book on the subject, dating from the 1950s, was Zariski and Samuel's *Commutative Algebra*. In the first decades of the 20th century, what we understand as commutative algebra was known as Ideal Theory, a name which reflects the sources of the subject.

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

Algebraic Number Theory and Unique Factorization

Algebraic number theory arose (as noted) from the investigation of three fundamental problems: Fermat's Last Theorem, reciprocity laws, and binary quadratic forms. Although these problems had their roots in the 17th and 18th centuries, they began to be intensively studied only in the 19th century. The strategy that began to emerge was to embed the domain Z of integers, in terms of which these problems were formulated, in domains of (what came to be known as) algebraic integers. Let me explain.

Fermat's Last Theorem states that $x^n + y^n = z^n$ has no nontrivial integer solutions for $n > 2$. It suffices to consider $n = 4$ and $n = p$, an odd prime. Fermat proved the conjecture for $n = 4$ in the early 17th century, and Euler proved it for $n = 3$ in the 18th (Euler's proof had a gap). In the early 19th century, Dirichlet and Legendre proved Fermat's conjecture for $n = 5$, but the case $n = 7$ defied the efforts of the best mathematicians, including Dirichlet and Gauss.[2] A new approach was called for. It was provided by Lamé.

On March 1, 1847, Lamé excitedly announced before the Paris Academy of Sciences that he had proved Fermat's Last Theorem. His basic idea was to factor the left-hand side of $x^p + y^p = z^p$ as follows:

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

where ω is a primitive pth root of 1. Since $x^p + y^p = z^p$, the product of the factors on the right-hand side of (1) is a pth power. Lamé claimed that if these factors are relatively prime, then each is a pth power. From this a contradiction can be derived using Fermat's method of infinite descent. If the factors $x + y, x + \omega y, \ldots, x + \omega^{p-1} y$ are not relatively prime, then, upon division by a suitable a, we obtain the relatively prime factors

$$\frac{x + y}{a}, \frac{x + \omega y}{a}, \ldots, \frac{x + \omega^{p-1} y}{a},$$

and the proof, Lamé asserted, proceeds analogously.[3]

Following Lamé's presentation, Liouville, who was in the audience, took the floor and pointed to what seemed to him to be a gap in Lamé's proof. The gap, he said, was Lamé's contention that if a product of relatively prime factors is a pth power, then each of the factors must be a pth power. This result is of course true for the integers, Liouville noted, but it required a proof for the complex entities Lamé was dealing with.

Liouville's observation went to the heart of what was wrong with Lamé's proof. Specifically, to prove Lamé's claim one had to show that unique factorization holds in the domain

$$D_p = \{a_0 + a_1\omega + \cdots + a_{p-1}\omega^{p-1} : a_i \in \mathrm{Z}\}$$

of so-called cyclotomic integers. About three months after Lamé's presentation

[2] Gauss was apparently not very interested in Fermat's problem. In a letter to Olbers in 1816 he said: "I confess indeed that Fermat's theorem as an isolated proposition has little interest for me, since a multitude of such propositions, which one can neither prove nor refute, can easily be formulated" [**20**, pp. 818–819].

[3] The essential idea of Lamé's approach is contained in the following method for finding all primitive pythagorean triples (x, y, z): Factoring the left-hand side of $x^2 + y^2 = z^2$ we get $(x + yi)(x - yi) = z^2$. It can be shown that $x + yi$ and $x - yi$ are relatively prime (since $(x, y, z) = 1$), and since their product is a square, each is a square. In particular, $x + yi = (a + bi)^2 = (a^2 - b^2) + 2abi$, hence $x = a^2 - b^2$, $y = 2ab$, and it follows that $z = a^2 + b^2$. This is the standard formula yielding all pythagorean triples.

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

Kummer wrote to Liouville that D_p is in general *not* a unique factorization domain (UFD). (The first p for which it is not is $p = 23$.)

It is important to note that although Lamé's proof was false (it *is* correct for those p for which D_p is a UFD), his overall strategy proved fundamental for subsequent approaches to Fermat's Last Theorem. In particular, he proved the theorem for $n = 7$(!), a feat that (we recall) eluded the likes of Dirichlet and Gauss.

We turn now to reciprocity laws.[4] Gauss was the first to define formally the notion of congruence. Thus it was natural for him to pose the question of solvability of the congruence $a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \equiv 0 \pmod{n}$. The problem in this generality proved intractable (it is so to this day), and so (as Pólya would advise) Gauss considered a simpler case, namely $a_0 + a_1x + a_2x^2 \equiv 0 \pmod{n}$. Several reductions show that it suffices to consider the congruence $x^2 \equiv q \pmod{p}$, where both p and q are odd primes (the case of even primes has to be considered separately). Gauss proved that there is a "reciprocity relation" between the solvability of $x^2 \equiv q \pmod{p}$ and $x^2 \equiv p \pmod{q}$. Specifically, $x^2 \equiv q \pmod{p}$ is solvable if, and only if, $x^2 \equiv p \pmod{q}$ is solvable, unless $p \equiv q \equiv 3 \pmod{4}$. In the latter case, $x^2 \equiv q \pmod{p}$ is solvable if, and only if, $x^2 \equiv p \pmod{q}$ is not. This is the celebrated quadratic reciprocity law, one of the "jewels of number theory," proved in Gauss' *Disquisitiones Arithmeticae* of 1801.

What about higher reciprocity laws? That is, is there a "reciprocity relation" between the solvability of $x^m \equiv q \pmod{p}$ and $x^m \equiv p \pmod{q}$ for $m > 2$? Gauss opined that such laws cannot even be properly conjectured within the context of natural numbers [**28**, p. 105], adding that

> The previously accepted laws of arithmetic are not sufficient for the foundations of a general theory... Such a theory demands that the domain of higher arithmetic be endlessly enlarged [**17**, p. 108].

A prophetic statement, indeed. Gauss was calling (in modern terms) for the founding of an arithmetic theory of algebraic numbers. In fact, Gauss himself began to enlarge the domain of arithmetic by introducing what came to be known as the Gaussian integers,

$$Z[i] = \{a + bi: a, b \in Z\},$$

and showing that they form a UFD. This he did in two papers in 1829 and 1831, in which he used $Z[i]$ to formulate the law of biquadratic reciprocity.[5] In the 1831

---

[4] It is no easy matter to define what a reciprocity law is (see [**10**], [**21**], [**29**]). For our purposes, the descriptions that follow suffice.

[5] The law can be stated (essentially) as follows [**8**, p. 64]:

$$\left(\frac{\pi}{\sigma}\right)_4\left(\frac{\sigma}{\pi}\right)_4 = (-1)^{[(N(\pi)-1)/4][(N(\sigma)-1)/4]},$$

where π and σ are distinct primes in $Z[i]$, $N(\alpha)$ is the norm of the Gaussian integer α, and

$$\left(\frac{\alpha}{\pi}\right)_4 = \begin{cases} 1 \text{ if } x^4 \equiv \alpha \pmod{\pi} \text{ is solvable in } Z[i] \\ -1, i, \text{ or } -i \text{ otherwise} \end{cases}$$

(We recall that the quadratic reciprocity law can be stated in terms of the Legendre symbol as

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

The *proof* of the biquadratic reciprocity law was found in Gauss' diaries. The first published proof was given by Eisenstein in 1844. The theorem can be used to determine the solvability in Z of $x^4 \equiv q \pmod{p}$ [**17**, p. 127].

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

paper Gauss also introduced the geometric representation of complex numbers as points in the Euclidean plane. At about the same time, Jacobi and Eisenstein (as well as Gauss in unpublished papers) formulated the cubic reciprocity law. Here one needed to consider the domain

$$Z[\rho] = \{a + b\rho : a, b \in Z\},$$

where ρ is a primitive cube root of 1. $Z[\rho]$ was also shown to be a UFD. The search was on for higher reciprocity laws. But as in the case of Fermat's Last Theorem, here too one needed new methods to deal with cases beyond the first few, since unlike $Z[i]$ and $Z[\rho]$, other domains of higher arithmetic needed to formulate such laws were not UFDs.

We now turn to the third number-theoretic problem related to the rise of algebraic number theory, namely representation of integers by binary quadratic forms. (This problem is, in fact, intimately connected to reciprocity laws; see [**10**].) An (integral) binary quadratic form is an expression of the form $f(x, y) = ax^2 + bxy + cy^2$, $a, b, c \in Z$. The major problem of the theory of quadratic forms was: Given a form f, find all integers m that can be represented by f; that is, for which $f(x, y) = m$. This problem was studied for specific f by Fermat, and intensively investigated by Euler. For example, Fermat considered the representation of integers as sums of two squares. It was, however, Gauss in the *Disquisitiones* who made the fundamental breakthroughs and developed a comprehensive and beautiful theory of binary quadratic forms. Most important was his definition of the *composition* of two forms and his proof that the (equivalence classes of) forms with a given "discriminant" $D = b^2 - 4ac$ form a commutative group under this composition.

The *idea* behind composition of forms is simple: If forms f and g represent integers m and n, respectively, then their composition $f * g$ should represent the product mn. The *implementation* of this idea is subtle and "extremely difficult to describe" [**12**, p. 334]. Attempts to gain conceptual insight into Gauss' theory of composition of forms inspired the efforts of some of the best mathematicians of the time, among them Dirichlet, Kummer, and Dedekind. The key idea here, too, was to extend the domain of higher arithmetic and view the problem in a broader context. Here is perhaps the simplest illustration: If m_1 and m_2 are sums of two squares, so is $m_1 m_2$. Indeed, if $m_1 = x_1^2 + y_1^2$ and $m_2 = x_2^2 + y_2^2$, then $m_1 m_2 = (x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + x_2 y_1)^2$. In terms of the composition of quadratic forms this can be expressed as $f(x_1, y_1) * f(x_2, y_2) = f(x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$, or $f * f = f$, where $f(x, y) = x^2 + y^2$. But even this "simple" law of composition seems mysterious and ad hoc until one introduces Gaussian integers, which make it transparent ($\overline{\alpha}$ denotes the conjugate of α):[6]

$$\begin{aligned}
&(x_1^2 + y_1^2)(x_2^2 + y_2^2) \\
&\quad = (x_1 + y_1 i)(x_1 - y_1 i)(x_2 + y_2 i)(x_2 - y_2 i) \\
&\quad = (x_1 + y_1 i)(x_2 + y_2 i)\overline{(x_1 + y_1 i)(x_2 + y_2 i)} \\
&\quad = [(x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1) i]\overline{[(x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1) i]} \\
&\quad = (x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + x_2 y_1)^2.
\end{aligned}$$

In general, $ax^2 + bxy + cy^2 = m$ can be written as

$$\frac{1}{a}\left(ax + \frac{b + \sqrt{D}}{2} y\right)\left(ax + \frac{b - \sqrt{D}}{2} y\right) = m,$$

[6]The following example gives a better sense of the subtlety and apparent arbitrariness of Gauss' law of composition of binary quadratic forms: If $g(x, y) = 2x^2 + 2xy + 3y^2$, then $g(x_1, y_1) * g(x_2, y_2) = h(2x_1 x_2 + x_1 y_2 + x_2 y_1 - 2y_1 y_2, x_1 y_2 + x_2 y_1 + y_1 y_2)$, where $h(x, y) = x^2 + 5y^2$, so $g * g = h$.

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

where $D = b^2 - 4ac$ is the discriminant of the quadratic form. We have thus expressed the problem of representation of integers by binary quadratic forms in terms of the domain

$$R = \left\{ \frac{u + v\sqrt{D}}{2} : u, v \in Z,\ u \equiv v \pmod 2 \right\}.$$

Specifically, if we let

$$a = \alpha,\ \frac{b + \sqrt{D}}{2} = \beta,$$

then

$$ax^2 + bxy + cy^2 = \frac{1}{a}(\alpha x + \beta y)(\bar{\alpha} x + \bar{\beta} y) = \frac{1}{a} N(\alpha x + \beta y),$$

where N denotes the *norm*. Thus to solve $ax^2 + bxy + cy^2 = m$ is to find $x, y \in Z$ such that $N(\alpha x + \beta y) = m$. In fact, Kummer noted in the 1840s that the entire theory of binary quadratic forms can be regarded as the theory of "complex numbers" (Kummer's terminology) of the form $x + y\sqrt{D}$ [**6**, p. 585]. And since such domains of "complex numbers" did not, in general, possess unique factorization, the development of their arithmetic theory became an important goal. (Gauss' theory of binary quadratic forms may, in fact, be seen as the first major (implicit) attempt to deal with nonunique factorization.)

It is time to take stock. We have seen that in dealing with central problems in number theory, namely Fermat's Last Theorem, reciprocity laws, and binary quadratic forms, it was found important to formulate them as problems in domains of (what came to be called) algebraic integers. This often transformed additive problems into multiplicative ones (e.g. $x^3 + y^3 = z^3$ was changed to $(x + y)(x + \rho y)(x + \rho^2 y) = z^3$, ρ a primitive cube root of unity). Now, multiplicative problems in number theory are, in general, much easier to handle than additive problems—provided that one has the (multiplicative) machinery to do it, namely unique factorization in the domain under consideration. Thus the study of unique factorization in domains of algebraic integers became the major problem of a newly emerging subject—algebraic number theory. Number theory had lost its innocence (which, at the appropriate time, is of course no bad thing). After more than 2000 years in which number theory meant the study of properties of the (positive) integers, its scope became enormously enlarged. One could no longer use the term "integer" with impunity. The term had to be qualified —a rational (ordinary) integer, a Gaussian integer, a cyclotomic integer, a quadratic integer, or any one of an infinite species of other algebraic integers. Of course the real difficulty was not the multiplicity of types of integers, but the fact that, in general, domains of such integers no longer possessed unique factorization.

Could one regain the paradise lost by establishing unique factorization in *some* sense for these domains? An affirmative answer was given by Dedekind and Kronecker in the last third of the 19th century. We will describe the work of Dedekind, who introduced the notions of ideal and prime ideal, and showed that every nonzero ideal in an arbitrary domain of algebraic integers is a unique product of prime ideals. (An ideal P is prime if $xy \in P$ implies $x \in P$ or $y \in P$.) This result generalizes the theorems on unique factorization of elements into primes in (for example) Z, $Z[i]$, and $Z[\rho]$. But it was preceded by very significant contributions by Kummer to the problem of unique factorization, which inspired both Dedekind and Kronecker (in different ways). We begin with a sketch of Kummer's contribution.

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

Kummer and Ideal Numbers

We recall that the domains of cyclotomic integers $D_p = \{a_0 + a_1\omega + \cdots + a_{p-1}\omega^{p-1}$: $a_i \in Z$, ω a primitive pth root of 1$\}$ were central in the study of Fermat's conjecture. They also proved important in the investigation of higher reciprocity laws. The two problems are, in fact, related, and progress on one was often linked with progress on the other (see [17, p. 203]). Gauss contended that if he were able to derive higher reciprocity laws, then Fermat's Last Theorem would be one of the less interesting corollaries. That is one prediction where Gauss proved to be wrong: A general reciprocity law (due to Artin) was obtained in the 1920s, but Fermat's problem is not resolved.[7]

Both Fermat's problem and higher reciprocity laws were of great interest to Kummer (the latter apparently more than the former), and to make serious progress on them it was essential to establish unique factorization (of some type) in the domains D_p. This Kummer accomplished in the 1840s. As he put it in a letter to Liouville, unique factorization in D_p "can be saved by the introduction of a new kind of complex numbers that I have called ideal complex numbers" [3, p. 101]. Kummer then showed that every element in the domain of cyclotomic integers is a unique product of "ideal primes".

Kummer's theory was vague and computational. In fact, the central notion of ideal number was only *implicitly* defined in terms of its divisibility properties (see [12] or [13]).[8] Kummer noted that in adopting the implicit definition he was guided by the idea of "free radical" in chemistry, a substance whose existence can only be discerned by its effects [9, p. 35].

The following example (even if not of a cyclotomic domain) may give a sense of Kummer's theory of ideal numbers. Let $D = \{a + b\sqrt{5}\,i$: $a, b \in Z\}$. This is a standard example (due to Dedekind) of a domain in which factorization is not unique. For example, $6 = 2 \times 3 = (1 + \sqrt{5}\,i)(1 - \sqrt{5}\,i)$, where 2, 3, and $1 \pm \sqrt{5}\,i$ are primes (indecomposables) in D [1, p. 250]. To restore unique factorization of $6 \in D$, adjoin the "ideal numbers" $\sqrt{2}$, $(1 + \sqrt{5}\,i)/\sqrt{2}$, and $(1 - \sqrt{5}\,i)/\sqrt{2}$. These are, in fact, *ideal primes*.[9] We then have

$$6 = 2 \times 3 = \sqrt{2} \times \sqrt{2} \times \frac{1 + \sqrt{5}\,i}{\sqrt{2}} \times \frac{1 - \sqrt{5}\,i}{\sqrt{2}},$$

[7]These unprophetic words were of course uttered prior to Wiles' June 1993 announcement of his proof of Fermat's Last Theorem. In a widely distributed e-mail note in December 1993 Wiles noted that "during the review process a number of problems emerged" but that he believes that he "will be able to finish [closing the gaps in the proof] in the near future." In any case, Wiles' proof (when (if) the gaps are closed) would by no means follow from Artin's reciprocity law.

[8]Every ideal number of D_p is of the form $\sqrt[h]{\alpha}$, where $\alpha \in D_p$ [3, p. 105], although not every number of this form is an ideal number. The positive integer h (which is independent of α) is called the *class number* of D_p. It is a measure of "how far" D_p is removed from possessing unique factorization: $h = 1$ if, and only, if D_p is a UFD. In modern terms, the ideal numbers (of D_p) are in one-one correspondence with the valuations on the cyclotomic field $Q_p = \{q_0 + q_1\omega + \cdots + q_{p-1}\omega^{p-1}$: $q_i \in Q\}$ (see [6, p. 581]).

[9]An ideal prime had no more explicit definition than an ideal number. It was described in terms of the set of all cyclotomic integers divisible by it [13, p. 325]. Note also that the adjoined ideal numbers are square roots of elements of D, since

$$\frac{1 \pm \sqrt{5}\,i}{\sqrt{2}} = \sqrt{-2 \pm \sqrt{5}\,i},$$

hence D is "not too far removed" from being a unique factorization domain (assuming that this is true for all elements of D); that is, its "class number" is 2.

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

and $6 = (1 + \sqrt{5}\,i)(1 - \sqrt{5}\,i) = \sqrt{2} \times (1 + \sqrt{5}\,i)/\sqrt{2} \times \sqrt{2} \times (1 - \sqrt{5}\,i)/\sqrt{2}$; that is, the decomposition of 6 into primes is now unique. Furthermore, although the choice of the ideal primes $\sqrt{2}$, $(1 \pm \sqrt{5}\,i)/\sqrt{2}$ seems to have been ad hoc, it will come to seem natural after ideals are introduced.

A cruder but perhaps more revealing example is the "domain" $H = \{3k + 1: k = 0, 1, 2, \ldots\} = \{1, 4, 7, 10, 13, \ldots\}$, introduced by Hilbert. (This is not an integral domain, but its structure as a multiplicative semigroup illustrates the ideas involved.) Here $100 = 10 \times 10 = 4 \times 25$, where 4, 10, and 25 are primes of H. We can eliminate the nonuniqueness of this factorization by adjoining the "ideal primes" 2 and 5. Then $100 = 10 \times 10 = 2 \times 5 \times 2 \times 5$ and $100 = 4 \times 25 = 2 \times 2 \times 5 \times 5$.

The notion of adjoining elements to a given mathematical structure in order to obtain a desired property is commonplace and important in various areas of mathematics. Thus we adjoin $\sqrt{-1}$ to the reals to obtain algebraic closure, and adjoin "ideal points" (points at infinity) to the euclidean plane to obtain symmetry (duality) between points and lines. The adjunction of ideal numbers to the cyclotomic integers should be seen in the same light.

Kummer's ideas were brilliant but difficult and not clearly formulated. The fundamental concepts of ideal number and ideal prime were not intrinsically defined. "Today," notes Edwards, "few mathematicians would find [Kummer's] definition [of ideal primes] acceptable" [**15**, p. 6]. Most importantly, Kummer's decomposition theory was devised only for cyclotomic integers (he mentions, without elaboration, that an analogous theory could be developed for algebraic integers of the form $x + y\sqrt{D}$). What was needed was a decomposition theory that would apply to arbitrary domains of algebraic integers. This called for a fundamentally new approach to the subject, provided (independently, and in different ways) by Dedekind and Kronecker. We will focus (as mentioned) on Dedekind's formulation, which is the one that has generally prevailed.

Dedekind and Ideals

Dedekind's work (in 1871)[10] was revolutionary in several ways: in its formulation, its grand conception, its fundamental new ideas, and its modern spirit. Its main result was that every nonzero ideal in the domain of integers of an algebraic number field is a unique product of prime ideals. Before one could state this theorem one had, of course, to define the concepts in its statement, especially "the domain of integers of an algebraic number field" and "ideal." It took Dedekind about 20 years to formulate them.

The number-theoretic domains studied at the time, such as the Gaussian integers, the integers arising from cubic reciprocity, and the cyclotomic integers, are all of the form $Z[\theta] = \{a_0 + a_1\theta + \cdots + a_n\theta^n: a_i \in Z\}$, where θ satisfies an "appropriate" polynomial with integer coefficients. It was therefore tempting to define the domains to which Dedekind's theorem would apply as objects of this type. These were, however, the wrong objects, Dedekind showed. For example, he proved that Kummer's theory of unique factorization could *not* be extended to the domain $Z[\sqrt{3}\,i] = \{a + b\sqrt{3}\,i: a, b \in Z\}$ [**13**, p. 337], and, of course, Dedekind's objective was to try to extend Kummer's theory to *all* domains of algebraic integers. One had to begin the search for the appropriate domains, Dedekind contended, within an "algebraic

[10] It appeared as Supplement X to the 2nd edition of Dirichlet's *Vorlesungen über Zahlentheorie*, which was written as commentary on, and explication of, Gauss' *Disquisitiones*. Dedekind wrote two other versions of his theory, in Supplements to the 3rd and 4th editions of Dirichlet's *Zahlentheorie* (in 1879 and 1894 respectively).

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

number field"—a finite field extension $Q(\alpha) = \{q_0 + q_1\alpha + \cdots + q_s\alpha^s\colon\ q_i \in Q\}$ of the rationals, α an algebraic number (the notion of "algebraic number" was well known at the time, but not that of "algebraic integer"). He showed that $Q(\alpha)$ is closed under the four algebraic operations of addition, subtraction, multiplication, and division, and then defined axiomatically (for the first time) the notion of a *field*:[11]

> A system A of real or complex numbers is called a field if the sum, difference, product, and quotient of any two numbers of A belongs to A [**3**, p. 118].

This procedure was typical of Dedekind's modus operandi: He would distill from a concrete object (in this case $Q(\alpha)$) the properties of interest to him (in this case closure under the four algebraic operations) and proceed to define an abstract object (in this case a field) in terms of those properties. This is, of course, standard practice nowadays, but it was revolutionary in Dedekind's time. Dedekind used it again and again, as we shall see.

To come back to the domain of algebraic integers to which Dedekind's result was to apply: He defined it to be the set R of all elements of $Q(\alpha)$ that are roots of *monic* polynomials with integer coefficients. (*All* the elements of $Q(\alpha)$ are roots of polynomials, not necessarily monic, with integer coefficients.) He showed that these elements "behave" like integers—they are closed under addition, subtraction, and multiplication. They are the "integers" of the algebraic number field $Q(\alpha)$. Dedekind did not, however, motivate this basic definition of the domain of algebraic integers, a fact lamented by Edwards: "Insofar as this is the crucial idea of the theory, the genesis of the theory appears, therefore, to be lost" [**13**, p. 332].

This is not to say, of course, that the notion of the domain of algebraic integers cannot be motivated. The (algebraic) integers of $Q(\alpha)$ are to $Q(\alpha)$ what the (rational) integers (the elements of Z) are to Q. Now, the elements of Q can be thought of as roots of *linear* polynomials with integer coefficients (viz. $p(x) = ax + b$). Among these, the integers are the roots of *monic* linear polynomials (viz. $q(x) = x + b$). If we extend this analysis to polynomials of arbitrary degree (over Z), their roots (in $Q(\alpha)$) yield (all of) $Q(\alpha)$, while the roots of the monic polynomials among them yield the domain of integers of $Q(\alpha)$. Moreover, just as Q is the field of quotients of Z, so $Q(\alpha)$ is the field of quotients of *its* domain of integers. (See also [**27**, pp. 264–265], for a discussion, from a different perspective, of the issue of motivation of algebraic integers.)

Having defined the domain R of algebraic integers (of $Q(\alpha)$) in which he would formulate and prove his result on unique decomposition of ideals, Dedekind considered, more generally, sets of integers of $Q(\alpha)$ closed under addition, subtraction, and multiplication. He called them "orders". (The domain R of integers of $Q(\alpha)$ is the largest order.) Here, then, was another algebraic first for Dedekind—an essentially axiomatic definition of a (commutative) ring, albeit in a concrete setting.[12]

The second fundamental concept of Dedekind's theory, that of ideal, derived its motivation (and name) from Kummer's ideal numbers. Dedekind wanted to characterize them *internally*, within the domain D_p of cyclotomic integers. Thus, for each ideal number σ he considered the set of cyclotomic integers divisible by σ. These, he noted, are closed under addition and subtraction, as well as under multiplication by all elements of D_p. Conversely, he proved (and this is a difficult theorem) that every

[11]Algebraic number theory was not the only source of the field concept. Others were Galois theory and algebraic geometry. See [24].

[12]Algebraic number theory was *one* of the sources of commutative ring theory. The other was algebraic geometry. Noncommutative ring theory had entirely different origins. See [19].

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

set of cyclotomic integers closed under these operations is precisely the set of cyclotomic integers divisible by some ideal number τ. Thus there is a one-one correspondence between ideal numbers and subsets of the cyclotomic integers closed under the above operations. Such subsets of D_p Dedekind called *ideals*. These subsets, then, characterized ideal numbers internally, and served as motivation for the introduction of ideals in arbitrary domains of algebraic integers.[13] Dedekind defined them abstractly as follows [**13**, p. 343]:

> A subset I of the integers R of an algebraic number field K is an *ideal* of R if it has the following two properties:
> (i) If $\beta, \gamma \in I$ then $\beta \pm \gamma \in I$.
> (ii) If $\beta \in I$, $\mu \in R$ then $\beta\mu \in I$.

Dedekind then defined a prime ideal—perhaps the most important notion of commutative algebra—as follows: An ideal P of R is *prime* if its only divisors are R and P. Given ideals A and B, A was said to divide B if $A \supseteq B$. In later versions of his work Dedekind showed that A divides B if, and only if, $B = AC$ for some ideal C of R (see [**7**, p. 122]). Having defined the notion of prime ideal, Dedekind proved his fundamental theorem that every nonzero ideal in the ring of integers of an algebraic number field is a unique product of prime ideals.

Here is another way of introducing ideals, in the spirit of *Kronecker's* work on establishing unique factorization in domains of algebraic integers. It is perhaps best illustrated with an example. Let $D = \{a + b\sqrt{5}\,i\colon a, b \in \mathbf{Z}\}$. As we noted, D is not a UFD. Since uniqueness of factorization in a domain is equivalent to the existence of the greatest common divisor (g.c.d.) of any two nonzero elements in the domain [**16**, p. 199], it follows that one way to reestablish unique factorization in D is to introduce g.c.d.s in D. (This is Kronecker's motivation for the introduction of divisors (ideals); see [**5**, p. 125], or [**13**, p. 353].) How do we introduce the g.c.d. of, say, 2 and $1 + \sqrt{5}\,i$, which appear in the factorizations of 6 into primes, $6 = 2 \times 3 = (1 + \sqrt{5}\,i)(1 - \sqrt{5}\,i)$? We look at $\mathbf{Z}$ (or any UFD) for guidance.

If $a, b \in \mathbf{Z}$, the g.c.d. of a and b can be found among the elements of the set $I = \{ax + by\colon x, y \in \mathbf{Z}\}$. In fact, I is a principal ideal of $\mathbf{Z}$, $I = \langle d\rangle = \{dm\colon m \in \mathbf{Z}\}$, and g.c.d. $(a, b) = d$. (An ideal J of a ring R is principal if it is generated by a single element $a \in R$. We write $J = \langle a\rangle$.) In like manner, if D were a UFD, then g.c.d. $(2, 1 + \sqrt{5}\,i)$ would be found among the elements of $P = \{2\alpha + (1 + \sqrt{5}\,i)\beta\colon \alpha, \beta \in D\}$. Moreover, we would have $P = \langle s\rangle$ (the principal ideal of D generated by some $s \in D$) and g.c.d. $(2, 1 + \sqrt{5}\,i) = s$. Since D is not a UFD, there is no $s \in D$ such that $P = \langle s\rangle$. But why not have all of P represent (capture) g.c.d. $(2, 1 + \sqrt{5}\,i)$? Indeed, this is Kronecker's idea. (Dedekind would have argued for an "ideal element" $\hat{s}$ ($\hat{s} \notin D$) to describe P, so that P would be the set of elements in D divisible by $\hat{s}$; we exhibit such an $\hat{s}$ below.) We note that P is an ideal of D, though not a principal ideal. Similarly we let $Q = \langle 3, 1 + \sqrt{5}\,i\rangle = \{3\alpha + (1 + \sqrt{5}\,i)\beta\colon \alpha, \beta \in D\}$ and $R = \langle 3, 1 - \sqrt{5}\,i\rangle$ (note that $\langle 2, 1 - \sqrt{5}\,i\rangle = \langle 2, 1 + \sqrt{5}\,i\rangle$). We then easily verify that $P^2 = \langle 2\rangle$, $PQ = (1 + \sqrt{5}\,i)$, $QR = \langle 3\rangle$, and $PR = \langle 1 - \sqrt{5}\,i\rangle$. (If A and B are ideals of a ring R, their product is the ideal $AB = \{\Sigma_{\text{finite}} a_i b_i\colon a_i \in A,\ b_i \in B\}$.)

Returning now to the factorizations $6 = 2 \times 3 = (1 + \sqrt{5}\,i)(1 - \sqrt{5}\,i)$, they yield the following factorizations of ideals: $\langle 6\rangle = \langle 2\rangle\langle 3\rangle = P^2(QR)$ and $\langle 6\rangle = \langle 1 + \sqrt{5}\,i\rangle\langle 1 - \sqrt{5}\,i\rangle = (PQ)(PR) = P^2QR$. One can readily verify that the ideals P, Q, R are prime. Thus the *ideal* $\langle 6\rangle$ (if not the *element* 6) has been factored uniquely into prime ideals. Paradise regained. See [**5**], [**13**].

[13] Ideals also arose in an entirely different setting in noncommutative algebra. They appeared in the works of Cartan (1898) and especially of Wedderburn (1907), who called them "invariant subalgebras". See [**19**].

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

Let us compare this factorization of $\langle 6 \rangle$ into *prime ideals* with the factorization of 6 into *ideal primes* (à la Kummer) that we gave earlier:

$$6 = 2 \times 3 = \sqrt{2} \times \sqrt{2} \times \frac{1+\sqrt{5}\,i}{\sqrt{2}} \times \frac{1-\sqrt{5}\,i}{\sqrt{2}},$$

and

$$6 = (1+\sqrt{5}\,i)(1-\sqrt{5}\,i) = \sqrt{2} \times \frac{1+\sqrt{5}\,i}{\sqrt{2}} \times \sqrt{2} \times \frac{1-\sqrt{5}\,i}{\sqrt{2}}.$$

Performing some 18th-century symbolic callisthenics, we obtain the following: Since $P^2 = \langle 2 \rangle$, $P \sim \sqrt{2}$ (where " $\sim$ " stands for "corresponds to", "captures," "represents"). In fact, P is the ideal consisting of all elements of D divisible by the ideal number $\sqrt{2}$ (that is, such that the quotient is an algebraic integer [7, p. 235]). This would have been Dedekind's way of introducing P (that is, $\hat{s} = \sqrt{2}$). We also have $PQ = \langle 1+\sqrt{5}\,i \rangle$, hence $PQ/P \sim (1+\sqrt{5}\,i)/\sqrt{2}$, so that the ideal Q corresponds to the ideal number $(1+\sqrt{5}\,i)/\sqrt{2}$. And since $PR = \langle 1-\sqrt{5}\,i \rangle$, $PR/R \sim (1-\sqrt{5}\,i)/\sqrt{2}$, hence $R \sim (1-\sqrt{5}\,i)/\sqrt{2}$. This removes the mystery associated with our earlier introduction of the ideal numbers $\sqrt{2}$ and $(1 \pm \sqrt{5}\,i)/\sqrt{2}$. (How might Dedekind have restored unique factorization to the "domain" $H = \{1, 4, 7, 10, 13, \ldots\}$ we considered earlier?)

Dedekind's Legacy

Dedekind's Supplement X to Dirichlet's *Zahlentheorie* was the culmination of 70 years of investigations of problems related to unique factorization. It created, in one swoop, a new subject—algebraic number theory. It introduced, albeit in a concrete setting, some of the most fundamental concepts of commutative algebra, such as field, ring, ideal, prime ideal, and module (the last we have not discussed). These became basic in algebra and beyond. Supplement X also established one of the central results of algebraic number theory, namely the representation of ideals in domains of integers of algebraic number fields as unique products of prime ideals. The theorem was soon to play a fundamental role in the study of algebraic curves. It would also serve as a model for decomposition results in algebra.

As important as his concepts and results were Dedekind's methods. In fact, "his insistence on philosophical principles was responsible for many of his important innovations" [13, p. 349]. One of his philosophical principles was a focus on intrinsic, conceptual properties over formulas, calculations, or concrete representations. Another was the acceptance of nonconstructive procedures (definitions, proofs) as legitimate mathematical methods. Dedekind's great concern for teaching also influenced his mathematical thinking. His two very significant methodological innovations were the use of the axiomatic method and the institution of set-theoretic modes of thinking. See [14], [15].

To illustrate, compare Dedekind's and Kronecker's definitions of a field. (Recall that these two mathematicians developed essentially the same theory, at about the same time, but used entirely different methods and approaches.) Dedekind defined a field axiomatically (even if in a concrete setting), as the set of all real or complex numbers satisfying certain properties. Kronecker did not, in fact, define a field in the way *we* think of a definition. He *described* it, calling it a "domain of rationality": It consisted of all rational functions in the quantities $R', R'', R''', \ldots$ with integer

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

coefficients ($Q(R', R'', R''', \ldots)$ in current notation). He put no restrictions on these quantities—they could be indeterminates or roots of algebraic equations. In this sense, Kronecker's field concept is more general than Dedekind's. On the other hand, the elements $R', R'', R''', \ldots$ had to be given explicitly, so that (for example) the field of all algebraic numbers would not be considered a domain of rationality, whereas it qualified as a field under Dedekind's definition. Here was a foreshadowing of the formalist-intuitionist controversy, to emerge in full force in the early decades of the 20th century.

The axiomatic method was just beginning to surface after 2000 years of near dormancy. Dedekind was instrumental in pointing to its mathematical power and pedagogical value. In this he inspired (among others) David Hilbert and Emmy Noether. His use of set-theoretic formulations (recall, for example, his definition of an ideal as the set of elements of a domain satisfying certain properties), including the use of the completed infinite—taboo at the time—preceded by about 10 years Cantor's seminal work on the subject.[14] Undeniably, it justifies the description of his 1871 memoir as "the 'birthplace' of the modern set-theoretic approach to the foundations of mathematics" [**14**, p. 9]. Edwards' tribute (especially as it comes from one who is a great admirer of Kronecker's approach to the subject) is fitting [**14**, p. 20]:

> Dedekind's legacy ... consisted not only of important theorems, examples, and concepts, but of a whole *style* of mathematics that has been an inspiration to each succeeding generation.

Postscript

What of the three fundamental number-theoretic problems that gave rise to the development of algebraic number theory? In the 1871 memoir Dedekind gave a very satisfactory explanation, in terms of ideals, of Gauss' theory of binary quadratic forms, in particular of the composition of such forms. Specifically, with each quadratic form $f(x, y) = ax^2 + bxy + cy^2$ with discriminant $D = b^2 - 4ac$ Dedekind associated the ideal I of integers of the quadratic field $Q(\sqrt{D})$ generated by a and $(-b + \sqrt{D})/2$, that is, $I = \langle a, (-b + \sqrt{D})/2 \rangle$. He showed that this establishes a one-one correspondence between quadratic forms with discriminant D and ideals of the domain of integers of $Q(\sqrt{D})$, and that under this correspondence composition of forms corresponds to multiplication of ideals (see [**1**]). Although this result made Gauss' composition of forms transparent, it did not end interest in the (arithmetic) study of binary quadratic forms. In particular, the representation of integers by specific forms and the determination of the class number of forms are problems of current interest. See [**10**].

Various reciprocity laws beyond the biquadratic were formulated and proved in the 19th century, especially by Eisenstein, Kummer, and Hilbert. Kummer's work relied on his results on unique factorization of cyclotomic integers, Hilbert's initiated class-field theory (see [**10**], [**17**]). But these efforts were not entirely satisfactory. In fact, one of Hilbert's 23 problems presented at the 1900 International Congress of Mathematicians was to find a general reciprocity law. Artin solved the problem in the 1920s with his celebrated reciprocity law—a centerpiece of class-field theory. It establishes (in one of its incarnations, and roughly speaking) a connection between the Galois group of an abelian extension of an algebraic number field and the

[14] Several authors have commented on the methodological analogy between Dedekind's definitions of "ideal" and of "Dedekind cut". The definition of a cut, in fact, preceded that of an ideal. See [3], [13].

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

arithmetical properties of the ground field (see [**10**]). A far cry from the quadratic, cubic, and biquadratic reciprocity laws! See [**21**], [**29**].

Having instituted unique factorization in the domains D_p of cyclotomic integers, Kummer proved Fermat's Last Theorem for "regular" primes. (A prime p is *regular* if it does not divide the class number h of D_p; equivalently, if for any ideal I of D_p, if I^p is a principal ideal then so is I.) He then showed that all primes $p < 100$ (with the exception of 37, 59, and 67) are regular. Thus Fermat's Last Theorem was established for all primes $p < 100$ (about 10 years later Kummer disposed of the three remaining cases). Given that Gauss and Dirichlet failed to prove Fermat's theorem even for $n = 7$, this was quite an accomplishment. It showed the power of Kummer's theory of ideal numbers in cyclotomic domains. Much progress was made on Fermat's Last Theorem following Kummer's work (see [**12**] and [**25**]). In 1976, through the use of powerful computers along with powerful abstract mathematics, Fermat's Last Theorem was shown to hold for all primes $p < 125{,}000$ (see [**25**]). In another direction, as a corollary of his pioneering work on abelian varieties, Faltings showed in 1983 that *for each fixed* $n > 2$ the equation $x^n + y^n = z^n$ has at most finitely many solutions (See [**4**, pp. 41–42]). Wiles' very recent "proof" of Fermat's Last Theorem has its roots in Taniyama's 1955 conjecture about elliptic curves. It took 30 years to tie the conjecture to Fermat's Last Theorem. The high point of these developments was Ribet's 1987 proof that a special case of the Taniyama conjecture implies Fermat's Last Theorem. Wiles (apparently) devoted the past six years to proving this special case of Taniyama's conjecture. See [**11**], [**26**].

Emmy Noether used to say modestly of her work that it can already be found in Dedekind's. It would not be amiss to say that much of the subject matter of this paper originated in, or was inspired by, Gauss' *Disquisitiones Arithmeticae* of 1801. A new subject, algebraic number theory, came into being. It embodied fundamental concepts whose consequences reached far beyond number theory. Yet some of the major number-theoretic problems of that period are still with us today, two centuries later. Of course, the tools that have been brought to bear on their study are recent, and they are powerful. Gauss, Kummer, and Dedekind would likely have found them initially inscrutable, but in time wondrous. Mathematics is alive and well (if any evidence were needed).

REFERENCES

1. W. W. Adams and L. J. Goldstein, *Introduction to Number Theory*, Prentice-Hall, Englewood Cliffs, NJ, 1976.
2. M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Co., Reading, MA, 1969.
3. I. G. Bashmakova and A. N. Rudakov, The theory of algebraic numbers and the beginnings of commutative algebra, in *Mathematics in the 19th Century*, ed. by A. N. Kolmogorov and A. P. Yushkevich, Birkhäuser, Boston, 1992, pp. 86–135.
4. S. Bloch, The proof of the Mordell Conjecture, *Math. Intell.* 6:2 (1984), 41–47.
5. E. D. Bolker, *Elementary Number Theory: An Algebraic Approach*, W. A. Benjamin, New York, 1970.
6. N. Bourbaki, Historical note, in his *Commutative Algebra*, Addison-Wesley Publishing Co., Reading, MA, 1972, pp. 579–606.
7. H. Cohn, *Advanced Number Theory*, Dover Publications, Mineola, NY, 1980.
8. M. J. Collison, The origins of the cubic and biquadratic reciprocity laws, *Arch. Hist. Ex. Sc.* 17 (1977), 63–69.
9. G. Cornell, Review of two books on algebraic number theory, *Math. Intell.* 5:1 (1983), 53–56.
10. D. A. Cox, *Primes of the Form* $x^2 + ny^2$*: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons, Inc., New York, 1989.
11. K. Devlin, F. Gouvêa, and A. Granville, Fermat's Last Theorem, a theorem at last, *Focus* 13:4 (1993), 3–4.

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions

12. H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag New York, 1977.
13. _____, The genesis of ideal theory, *Arch. Hist. Ex. Sc.* 23 (1980), 321–378.
14. _____, Dedekind's invention of ideals, *Bull. Lond. Math. Soc.* 15 (1983), 8–17.
15. _____, Mathematical ideas, ideals, and ideology, *Math. Intell.* 14:2 (1992), 6–19.
16. E. Grosswald, *Topics from the Theory of Numbers*, 2nd edition, Birkhäuser, Boston, 1984.
17. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag New York, 1982.
18. I. Kaplansky, Commutative rings, in *Proc. of Conf. on Commutative Algebra*, ed. by J. W. Brewer and E. A. Rutter, Springer-Verlag New York, 1973, pp. 153–166.
19. I. Kleiner, A sketch of the evolution of (noncommutative) ring theory, *L'Enseign. Math.* 33 (1987), 227–267.
20. M. Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York, 1972.
21. E. Lehmer, Rational reciprocity laws, *Amer. Math. Monthly* 85 (1978), 467–472.
22. A. F. Monna, *L'algébrisation de la Mathématique: Réflexions Historiques*, Comm. Math. Inst. Rijksuniversiteit, Utrecht, 1977.
23. H. Pollard and H. G. Diamond, *The Theory of Algebraic Numbers*, 2nd edition, MAA, Washington, DC, 1975.
24. W. Purkert, Zur Genesis des abstrakten Körperbegriffs, I, II, NTM 8 (1971), 23–37 and 10 (1973), 8–20.
25. P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag New York, 1979.
26. K. Ribet, Wiles proves Taniyama's conjecture; Fermat's Last Theorem follows, *Notices Amer. Math. Soc.* 40 (1993), 575–576.
27. H. Stark, *An Introduction to Number Theory*, MIT Press, Cambridge, MA, 1978.
28. A. Weil, Two lectures on number theory, past and present, *L'Enseign. Math.* 20 (1974), 87–110.
29. B. F. Wyman, What is a reciprocity law?, *Amer. Math. Monthly* 79 (1972), 571–586.

It had to be *e*!

(Sung to the tune of "It Had to be You!")

It had to be *e*,
Nonintegral *e*,
I looked around
Until I found
A base that would do.
To diff'rentiate
Or to integrate,
One that would not
Carry along
Some ugly weight.

Some bases I know
Are simpler to state,
A snap to invert,
Exponentiate,
But they wouldn't do.
For no other base can fit Math so well,
With all its digits I love it still!
It had to be *e*,
Irrational *e*,
It had to be *e*!

—Wayne Barrett
Brigham Young University
Provo, UT 84602

This content downloaded from 192.122.237.41 on Fri, 15 Jan 2016 12:10:04 UTC
All use subject to JSTOR Terms and Conditions