Dedekind's Theory of Ideals and Modern Algebraic Abstraction

Jeremy Avigad

April 17, 2024

Department of Philosophy
Department of Mathematical Sciences
Director, Hoskinson Center for Formal Mathematics
Carnegie Mellon University

Methodological questions

Things that mathematicians have worried about:

- The legitimacy of the axioms and inferences in Euclid's *Elements*.
- The seventeenth century retreat from geometric foundations.
- The use of infinitesimals in calculus.
- The use of infinitary, nonconstructive methods in nineteenth century mathematics.
- The abstract treatment of sets and functions.
- The use of computers in contemporary proofs.

Responses

Philosophy first: reflect on the nature and meaning of mathematics, and use that to determine what is acceptable.

Philosophy last, if at all: determine what is needed to get the mathematical job done.

A thesis of today's talk: mathematics is a mixture of the two, and there isn't a sharp line between them.

I'll explore the interplay between them in the nineteenth-century development of algebraic number theory.

Ontological questions

Sometimes, questions have to do with the nature and existence of mathematical objects:

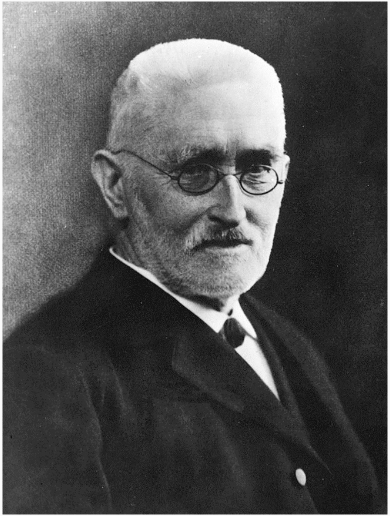
- zero, negative numbers, imaginary numbers
- infinitesimals
- points at infinity
- space-filling curves
- continuous nowhere differentiable functions

In modern mathematics, set theory provides a (remarkably good) means of adjudication.

But even so, questions remain as to which set-theoretic objects one should reason about, and how.

Richard Dedekind

- Born 1831 in Braunschweig.
- Student of Gauss in Göttingen.
- Doctorate in 1852.
- Studied in Berlin at the same time as Riemann.
- Habilitation in 1854.
- Returned to Göttingen.
- Polytechnic in Zurich 1858–1862.
- Returned to Braunschweig.
- Retired 1894, died 1916.



Modern aspects of Dedekind’s work

“Es steht alles schon bei Dedekind” (attributed to Emmy Noether)

- Infinitary, set-theoretic language
- Nonconstructive arguments
- Axiomatic / algebraic characterization of structures
- Use of modules, fields, ideals, lattices
- Describing properties in terms of mappings between structures
- Quotienting by an equivalence relation
- Emphasis on ”concepts,” and ”fundamental characteristics”
- De-emphasis of calculation

I will explain how these play out in the theory of ideals.

When is $x^2 + 2$ a perfect cube?

Euler: consider numbers of the form $a + b\sqrt{-2}$, where a and b are integers.

Write $x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2})$.

He showed that $x + \sqrt{-2}$ and $x - \sqrt{-2}$ have no factors in common.

So, if $x^2 + 2$ is a perfect cube, so are $x + \sqrt{-2}$ and $x - \sqrt{-2}$.

Write $x + \sqrt{-2} = (c + d\sqrt{-2})^3$.

Expand the product, set components equal.

Get solutions $x = \pm 5$.

The problem

Extended rings of "integers" don't always have unique factorization.

For example, in the ring of numbers of the form $a + b\sqrt{-5}$, we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

and 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible.

Kummer's diagnosis: the behavior is explained by the existence of "ideal" prime divisors. In this case:

$$\begin{aligned} 2 &\approx \alpha^2 \\ 3 &\approx \beta \cdot \gamma \\ 1 + \sqrt{-5} &\approx \alpha \cdot \beta \\ 1 - \sqrt{-5} &\approx \alpha \cdot \gamma \end{aligned}$$

Kummer's theory

For rings of *cyclotomic integers*, Kummer showed how to define predicates $P_\alpha(x)$,

"x is divisible by the ideal prime α,"

in terms of ordinary operations and predicates on the ring of integers.

He then showed that unique factorization holds of these ideal prime divisors. Thus

> *. . . it follows that calculation with complex numbers through the introduction of the ideal prime factors becomes exactly the same as calculations with the integers and their actual integer prime factors.*

A nod to metaphysics

Why do we posit the existence of abstract objects?

Kummer, in 1846:

> *. . . one sees that the ideal factors unlock the inner nature of the complex numbers, make them, as it were, transparent, and show their inner crystalline structure.*

H. J. S. Smith's *Report* to the Royal Society, in 1860:

> *. . . the complex numbers of Gauss, Jacobi, and M. Kummer force themselves upon our consideration, not because their properties are generalizations of the properties of ordinary integers, but because certain of the properties of integral numbers can only be explained by a reference to them.*

These are the data that need to be explained.

Dedekind 1877

Kummer did not define ideal numbers themselves, but only the divisibility of these numbers. If a number α has a certain property A, to the effect that α satisfies one more more congruences, he says that α is divisible by an ideal number corresponding to the property A. While this introduction of new numbers is entirely legitimate, it is nevertheless to be feared at first that the language which speaks of ideal numbers being determined by their products, presumably in analogy with the theory of rational numbers, may lead to hasty conclusions and incomplete proofs. And in fact this danger is not always completely avoided.

Dedekind 1877

On the other hand, a precise definition covering all the ideal numbers that may be introduced in a particular numerical domain $\mathfrak{o}$*, and at the same time a general definition of their multiplication, seems all the more necessary since the ideal numbers do not actually exist in the numerical domain* $\mathfrak{o}$*. To satisfy these demands it will be necessary and sufficient to establish once and for all the common characteristic of the properties* $A, B, C, \ldots$ *that serve to introduce the ideal numbers, and then to indicate how one can derive, from properties* A*,* B *corresponding to particular ideal numbers, the property* C *corresponding to their product.*

Dedekind 1877

This problem is essentially simplified by the following considerations. Since a characteristic property A serves to define, not an ideal number itself, but only the divisibility of the numbers in $\mathfrak{o}$ by the ideal number, one is naturally led to consider the set $\mathfrak{a}$ of all numbers α of the domain $\mathfrak{o}$ which are divisible by a particular ideal number. I now call such a system an ideal for short, so that for each particular ideal number there corresponds a particular ideal $\mathfrak{a}$.

. . . we obtain the following two fundamental properties of such a numerical system $\mathfrak{a}$:

I. The sum and difference of any two numbers in the system $\mathfrak{a}$ are always numbers in the same system $\mathfrak{a}$.
II. Any product of a number in the system $\mathfrak{a}$ by a number of the system $\mathfrak{o}$ is a number in the system $\mathfrak{a}$.

Dedekind 1877

A fact of the highest importance, which I was able to prove rigorously only after numerous vain attempts, and after surmounting the greatest difficulties, is that, conversely, each system enjoying properties I and II is also an ideal. That is, it is the set $\mathfrak{a}$ *of all numbers* α *of the domain* $\mathfrak{o}$ *divisible by a particular number; either an actual number or an ideal number indispensable for the completion of the theory.*

Dedekind 1877

Summary:

- Instead of reasoning about a property, $P_{\mathfrak{a}}(\alpha)$, which says that α is divisible by an ideal number $\mathfrak{a}$, consider $\{\alpha \mid P_{\mathfrak{a}}(\alpha)\}$.
- Dedekind shows that this set satisfies the modern definition of an ideal.
- Dedekind determines that, in any ring of integers, the ideals are exactly what is needed to restore unique factorization.

This is now Algebraic Number Theory 101.

A chronology of the theory of ideal divisors

1846–1847: Kummer's theory

1871: Dedekind's first version

1877: Dedekind's second version

1878: Dedekind, "Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen"

1879: Dedekind's third version

1882: Kronecker's *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*

1887: An unpublished version by Dedekind

1894: Dedekind's fourth version

1894: Hurwitz's version

1895: Dedekind, "Über die Begründung der Idealtheorie"

1897: Hilbert's *Zahlbericht*

Contrasts

Dedekind 1871 vs. Kummer:

- generalized from cyclotomic rings of integers to arbitrary rings
- determined the appropriate definition of integer
- determined appropriate handling of primes dividing the discriminant
- uses the set-theoretic notion of an ideal

Dedekind 1877/1879 vs. Dedekind 1871:

- cleaner separation of theory of modules, orders, rings of integers
- calculations buried
- multiplication defined from the start

Contrasts (continued)

Dedekind vs. Kronecker:

- set-theoretic notion of an ideal vs. symbolic representation (Kronecker takes gcd to be fundamental)
- nonconstructive definitions of operations on ideals vs. explicit calculations
- avoidance of calculations and representations

Dedekind 1887 vs. Dedekind 1877/1879:

- key property is localized: if $\mathfrak{c}$ is divisible by $\mathfrak{a}$, then $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ for some $\mathfrak{b}$
- given a purer formulation in terms of modules
- proved using a generalization of Gauss's theorem on the product of primitive polynomials

Dedekind 1894:

- eliminates (hides) the calculation using an identity involving modules

Historical data

Throughout his work, Dedekind often takes the time to explain why he preferred one approach to another, or why a certain manner of proceedings is desirable.

So we have:

- the evolution of Dedekind's versions
- the contrasts to other versions
- Dedekind's methodological pronouncements

These are a gift to philosophers and historians.

Methodological pronouncements

- emphasis on “fundamental” and “essential” properties (often axiomatic characterization)
- definitions and proofs should not depend on representations
- proofs should avoid calculations
- emphasis on generality
- emphasis uniformity
    - within a theory
    - within definitions
    - within proofs
- familiarity / analogy
    - reuse of proofs
    - analogies guide extensions
    - discrepancies lead to errors
- nouns should refer to (set-theoretic) *objects*
- totalities (ideals, real numbers) should be defined uniformly, at once
- purity: proofs should not depend on irrelevant features

Avoiding representations

Let $\omega = -1/2 \pm \sqrt{-3}/2$ be a principal cube root of 1.

Then $\mathbb{Q}(\omega)$ and $\mathbb{Q}(\sqrt{-3})$ are the same field.

Should we take the integers of this field to be

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

or

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b, \in \mathbb{Z}\}?$$

Answer: the first. The second does not admit a theory of unique factorization.

The problem: define the integers of a finite extension of $\mathbb{Q}$ in a way that does not depend on the representation.

Similarly: define the ideal divisors of a field in such a way.

Avoiding representations

Dedekind wrote in 1878:

> *I first developed the new principles, through which I reached a rigorous and exceptionless theory of ideals, seven years ago. . . Excited by Kummer's great discovery, I had previously worked for a number of years on this subject. . . but although this research brought me very close to my goal, I could not decide to publish it because the theory obtained in this way principally suffers two imperfections. One is that the investigation of a domain of algebraic integers is initially based on the consideration of a definite number and the corresponding equation, which is treated as a congruence; and that the definition of ideal numbers (or rather, of divisibility by ideal numbers) so obtained does not allow one to recognize the invariance these concepts in fact have from the outset. The second imperfection of this kind of foundation is that sometimes peculiar exceptions arise which require special treatment.*

Avoiding representations

> *My newer theory, in contrast, is based exclusively on concepts like that of field, integer, or ideal, that can be defined without any particular representation of numbers. Hereby, the first defect falls away; and just so, the power of these extremely simple concepts shows itself in that in the proofs of the general laws of divisibility no case distinction ever appears.*

Note the emphasis on:

- Avoiding representations.
- Invariance of concepts. (Essential features.)
- Algebraic characterizations.
- Uniformity.
- Generality.

Concepts vs. calculations

Dedekind is often contrasted with the Berlin school (Kronecker, Weierstrass, . . .), which favored a syntactic, computational style of mathematics.

In 1877, Dedekind wrote of the theory of ideals:

> *Even if there were such a theory, based on calculation, it still would not be of the highest degree of perfection, in my opinion. It is preferable, as in the modern theory of functions, to seek proofs based immediately on fundamental characteristics, rather than on calculation, and indeed to construct the theory in such a way that it is able to predict the results of calculation. . .*

Concepts vs. calculation

Galois 1830 (quoted and translated by Tignol):

> *If you now give me an equation that you have chosen at your pleasure, and if you want to know if it is or is not solvable by radicals, I could do no more than to indicate to you the means of answering your question, without wanting to give myself or anyone else the task of doing it. In a word, the calculations are impracticable.*

Concepts vs. calculation

From that, it would seem that there is no fruit to derive from the solution that we propose. Indeed, it would be so if the question usually arose from this point of view. But, most of the time, in the applications of the Algebraic Analysis, one is led to equations of which one knows beforehand all the properties: properties by means of which it will always be easy to answer the question by the rules we are going to explain. . . . All that makes this theory beautiful and at the same time difficult, is that one has always to indicate the course of analysis and to foresee its results without ever being able to perform [the calculations].

Concepts vs. calculations

From a letter from Dedekind to Lipschitz in 1876:

> *My efforts in number theory have been directed towards basing the work not on arbitrary representations or expressions but on simple foundational concepts and thereby — although the comparison may sound a bit grandiose — to achieve in number theory something analogous to what Riemann achieved in function theory, in which connection I cannot suppress the passing remark the Riemann's principles are not being adhered to in a significant way by most writers — for example, even in the newest work on elliptic functions. Almost always they mar the purity of the theory by unnecessarily bringing in forms of representation which should be results, not tools, of the theory.*

Concepts vs. calculations (continued)

In 1895, Dedekind quotes from Gauss's *Disquisitiones Arithmeticae*: "...in our opinion truths of this kind should be drawn from the notions involved rather than from notations."

> *When one takes them in the most general sense, a great scientific thought is expressed in these words, a decision in favor of the internal [Innerliche], in contrast to the external [Äußerlichen]. This constrast is repeated in almost every area of mathematics; one need only think of the theory of [Complex] functions, and Riemann's definition of functions through internal characteristic properties, from which the external forms of representation necessarily arise.*

Concepts vs. calculations

It is helpful to contrast Kronecker and Dedekind on the real numbers.

Kronecker:

- Start with the natural numbers.
- Construct the integers and the rationals.
- To construct $\sqrt{2}$, add a new symbol, x, consider expressions of the form $ax + b$, and calculate using $x^2 = 2$.

Features:

- It's based on representations and means of calculation.
- It's open-ended: construct more numbers, in the same way, as needed.

Concepts vs. calculations

Dedekind 1872 (really 1858):

- Identify the desired property, the principle of continuity, i.e. completeness.
- Show that the system of Dedekind cuts has the desired property.
- The real numbers are anything meeting that criterion.
- Worry about representing particular ones later (if at all).

His 1888 construction of the natural numbers explicitly established categoricity, i.e. uniqueness up to isomorphism.

Features:

- Get a categorical characterization of the reals.
- Get *all* the real numbers at once.

Concepts vs. calculations

The differences in the approaches to algebraic numbers were similar.

Kummer called his new objects *ideal divisors*.

Kronecker developed the theory of *divisors*, based on representations and calculation.

Dedekind developed the theory of *ideals*.

The set-theoretic notion of an ideal

Dedekind 1871:

> *[Kummer] came upon the fortunate idea of nonetheless feigning [fingieren] such numbers μ' and introducing them as ideal numbers. The divisibility of a number α' by these ideal numbers μ' depends entirely on whether α' is a root of the congruence $\eta\alpha' \equiv 0 \bmod \mu$, and consequently these ideal numbers are only treated as moduli; so there are absolutely no problems with this manner of introducing them. The only misgiving is that the immediate transfer of the usual concepts of the actual numbers can, initially, easily evoke mistrust of the certainty of the proof. This has caused us to inquire after a means of clothing the theory in a different garb, so that we always consider systems of actual numbers.*

The set-theoretic notion of an ideal

Dedekind 1877:

> *We can indeed reach the proposed goal with all rigour; however, as we have remarked in the Introduction, the greatest circumspection is necessary to avoid being led to premature conclusions. In particular, the notion of product of arbitrary factors, actual or ideal, cannot be exactly defined without going into minute detail. Because of these difficulties, it has seemed desirable to replace the ideal number of Kummer, which is never defined in its own right, but only as a divisor of actual numbers* ω *in the domain* $\mathfrak{o}$*, by a noun for something which actually exists.*

Set theoretic characterization

Let $\alpha_1, \ldots, \alpha_n$ be complex numbers.

In 1894, Dedekind defines

$$\mathbb{Q}(\vec{\alpha}) = \bigcap \{F \text{ a field} \mid \mathbb{C} \supset F \supset \{\vec{\alpha}\}\}$$

rather than

$$\mathbb{Q}(\vec{\alpha}) = \{f(\vec{\alpha})/g(\vec{\alpha}) \mid f, g \in \mathbb{Q}[\vec{x}] \wedge g(\vec{\alpha}) \neq 0\}.$$

His definition is impredicative. Why does he like it?

- It doesn't depend on representations.
- It is "structural" (characterizes the field in relation to others, rather than by its elements).
- The method is general.

Familiarity / analogy

In Dedekind’s 1871 presentation, as in Kummer’s, divisibility of ideals is the fundamental notion.

Multiplication of ideals plays no role in the development.

In his 1877/1879 presentations, multiplication is defined from the start.

Familiarity / analogy

Kummer did not define ideal numbers themselves, but only the divisibility of these numbers. If a number α has a certain property A, to the effect that α satisfies one more more congruences, he says that α is divisible by an ideal number corresponding to the property A. While this introduction of new numbers is entirely legitimate, it is nevertheless to be feared at first that the language which speaks of ideal numbers being determined by their products, presumably in analogy with the theory of rational numbers, may lead to hasty conclusions and incomplete proofs. And in fact this danger is not always completely avoided.

Familiarity / analogy

> *On the other hand, a precise definition covering all the ideal numbers that may be introduced in a particular numerical domain* $\mathfrak{o}$*, and at the same time a general definition of their multiplication, seems all the more necessary since the ideal numbers do not actually exist in the numerical domain* $\mathfrak{o}$*. To satisfy these demands it will be necessary and sufficient to establish once and for all the common characteristic of the properties* $A, B, C, \ldots$ *that serve to introduce the ideal numbers, and to indicate, how one can derive, from properties* A, B *corresponding to particular ideal numbers, the property* C *corresponding to their product.*

Understanding Dedekind

The philosophical literature has focused largely on Dedekind's metaphysical views:

- Platonism: classical, nonconstructive, infinitary reasoning; treating sets as objects; quantifying over sets; impredicative constructions.
- Structuralism: the focus on algebraic structures and relationships between them; categorical definitions; "Dedekind abstraction."
- Logicism: grounding of mathematics (and set theory) in logical constructions.

There is something to all of these. But where does it come from?

Methodological pronouncements

- emphasis on “fundamental” and “essential” properties (often axiomatic characterization)
- definitions and proofs should not depend on representations
- proofs should avoid calculations
- emphasis on generality
- emphasis uniformity
  - within a theory
  - within definitions
  - within proofs
- familiarity / analogy
  - reuse of proofs
  - analogies guide extensions
  - discrepancies lead to errors
- nouns should refer to (set-theoretic) *objects*
- totalities (ideals, real numbers) should be defined uniformly, at once
- purity: proofs should not depend on irrelevant features

Making sense of mathematics

The philosophical literature sometimes acts as though there were two Dedekinds:

- the mathematician Dedekind, proving theorems.
- the philosopher Dedekind, making pronouncements on the nature of mathematics.

But there was only one, doing both at the same time.

This is true of mathematics in general:

- Mathematicians all harbor some fundamental understanding of the nature of (good) mathematics.
- Mathematicians have to prove theorems and publish.

Philosophical reflection on mathematics can help us come to better terms with our fundamental understanding and how it bears on the practice.

From there to here

The nineteenth century was a time of great change in mathematics.

- The rise of abstract algebra.
- The rise of set-theoretic language and methods.
- Infinitary and nonconstructive methods in algebra and analysis.
- The emphasis on concepts over calculation.

Twentieth-century axiomatic foundations were designed to cope: ramified type theory, set theory, higher-order logic, simple type theory, dependent type theory, . . .

- they spell out the rules
- they move the explicit representations to a higher plane

These, in turn, have given rise to proof assistants like Lean, which implement these foundations.

From there to here

Here is a proof of Dirichlet's theorem in Lean.

From there, we can explore the definition of a Dirichlet character

We have unique factorization of ideals in Dedekind domains.

The ring of integers in a number field is a Dedekind domain.

Alex Kontorovich and Terence Tao are leading the Prime Number Theorem And project to formalize classical results in number theory.

I will show you the blueprint.