Axiomatics, methodology, and Dedekind's theory of ideals

Doug White

June 26, 2004

Abstract

Richard Dedekind has had an incredible influence on modern mathematics, largely due to his methodological demands which are still valued by mathematicians today. Through an investigation of some of his works written between 1854 and 1877, I reveal a connection between these methodological demands and features of axiomatic reasoning that he employed. I discuss two foundational/philosophic works (his *Habilitationsrede* and *Stetigkeit und irrationale Zahlen*), and his first two versions of the theory of ideals. Dedekind himself assists in the endeavor as he often expresses his reasoning for choosing one method over another. This self-reflective feature of Dedekind's efforts provides a unique opportunity to use his comments as a guide to reading both the foundational and mathematical works. Furthermore, his methodological preferences can often inform an interpretation of the chronological development of his work. Distinctive changes occurring between his first two versions of the theory of ideals are particularly relevant to such a discussion. I provide evidence demonstrating that Dedekind's methodological demands surrounding the issues of ontology, domain extension, and conceptualization are most fruitfully pursued using features of axiomatics.

Contents

Introduction

Through the investigation of Dedekind's early foundational and mathematical works I will show that his methodological demands are the driving force behind his use of axiomatic reasoning. Dedekind is among the first "modern" mathematicians, and his work is widely regarded as marking a turning point in the method and practice of mathematics. There are a number of methodological guidelines prevalent throughout his work, and many of them were even the object of his own considerations. Through an analysis of Dedekind's writings I intend to show that he employs features of modern axiomatics for attaining other methodological goals. I do not claim that Dedekind focused on axiomatization itself, but rather, that it was a necessary requirement for fruitfully achieving his other goals.

I will focus on two of Dedekind's foundational works, his *Habilitationsrede* (1854), and *Stetigkeit und irrationale Zahlen* (1872), and his first two versions of the theory of ideals, the first found in the Tenth Supplement to Dirichlet's *Vorlesungen über Zahlentheorie* (1871), and the second, a French version from 1877, *Theory of Algebraic Integers* (translated by John Stillwell in 1996). I will first present each one of these independently, focusing on features of each that best highlight some of his methodological concerns. In particular, three general methodological guidelines followed by Dedekind will be emphasized.

First, there are ontological aspects which guide Dedekind in defining new objects. Dedekind's emphasis on the fundamental characteristics and properties of the rational and real number domains (in *Stetigkeit*) is analogous to his method for extending the application of an operation on a limited domain to an extension (in his *Habilitation* lecture). The term "Dedekind abstraction" has come to be associated with one aspect of his method for defining new number domains, particularly in his pamphlet on defining the natural numbers *Was sind und was sollen die Zahlen* (1888). But there also appears to be a connection to his definition of the real numbers in *Stetigkeit*.

Three requirements, explicitly stated by Dedekind, accompany any definition of a number domain. These methodological demands are shared in the construction of the real numbers and the ideals. Each of the ontological demands for defining mathematical concepts can best be achieved by focusing one's attention on the fundamental characteristics of the object under consideration.

Second, Dedekind finds it valuable to extend domains in such a way that fundamental operations, or properties, carry over to the extension. Of particular importance here will be the introduction of the product of ideals in the second version of the ideal theory. There are properties of the ideals that are analogous to those of the rational integers. Thus, one is, at times, able to reason about the ideals in a similar manner. Furthermore, I will show that the second presentation of the theory of ideals follows more closely the proof of unique factorization on the rational integers, a feature of great importance to Dedekind.

Finally, in several places Dedekind comments on his preference for conceptual reasoning over algorithmic, or calculational reasoning. Dedekind explicitly tries to focus on fundamental principles of mathematical objects rather than on their representations and calculations based on these representations. I will show that the manifestation of this method provides a distinctive axiomatic flavor to Dedekind's work. Exemplary of the method is his isolation of two auxiliary propositions in the second version of the theory of ideals.

Each of these three methodological pursuits is clearly present throughout the works I will present, and they are most fruitfully implemented through features of the axiomatic method. I do not argue that Dedekind has a fully developed, modern axiomatic approach to mathematics; rather that the same sorts of concerns that axiomatics addresses are required for fulfilling his methodological demands. Modern axiomatics is usually associated with a structural approach to mathematics, the objects being defined by their relation to other objects in the structure. There is some support for the position that Dedekind did have a well developed notion of axiomatics, but my argument, that he used aspects of the axiomatic method in order to pursue his other methodological demands, is not affected by such concerns.

Chapter 1

Dedekind's early foundational work

The mid-to-late 1850's was a productive time for Dedekind's foundational work. On 30 June 1854 he delivered his *Habilitationsrede*, the talk which accompanies the *Habilitation* paper required for German scholars entering professional life. Candidates are required to submit three topics related to their paper's thesis, but intended to demonstrate breadth of knowledge, then their committee chooses which will be presented. The title of Dedekind's talk was *Über die Einführung neuer Funktionen in der Mathematik*.[1] The topic relates the fruitful developments of mathematics to the introduction of new functions (operations) or concepts. The discussion can be viewed as representative of Dedekind's earliest foundational thoughts and a foreshadowing of many of his methodological principles.

In 1858 Dedekind taught a course on differential analysis, and, as a result, found great dissatisfaction in the central theorem's reliance on appeals to geometric considerations. Dedekind felt that such an appeal may be pragmatically useful in understanding the subject but it does not provide "a purely arithmetic and perfectly rigorous foundation for the principles of infinitesimal analysis" [3]. The period between 1858 and 1872 was a time of great growth for Dedekind and the methodological changes are evident in *Stetigkeit und irrationale Zahlen*. Although not published until 1872 it was conceived in 1858 as Dedekind notes in the introduction to [3].

These two foundational works will be analyzed, in Chapter 4, with three

[1] *On the Introduction of New Functions In Mathematics*

goals in mind. First, I show that similar methodological issues arise in the two texts, and that Dedekind's views evolve and grow between them. Second, I will clarify those principles that are apparent in his formulation of the theory of ideals. Finally, principles that have appeared in these earlier works will be shown to be the motivation for the changes which occur in his second presentation of ideal theory.

1.1 Dedekind's *Habilitationsrede*

In this section I will focus on two features of Dedekind's methodology that are evident in his *Habilitationsrede*. By focusing on his examples of mineralogy and law, I will clarify what Dedekind means when he says that the introduction of a concept can be seen as a hypothesis "one puts to the inner nature of the science" [1, ¶3]. Then I will elucidate Dedekind's emphasis on discovering and utilizing basic, or characteristic, properties and laws for extending operations. Dedekind's explication of the manner in which exponentiation is generalized will be helpful in this endeavor.

It is obvious that scientists form hypotheses as part of the scientific method, but whether we can say the same of mathematicians is a controversial point. Dedekind thinks that, in some sense (to be fully developed in this section), when mathematicians introduce concepts, or form definitions, they are doing just that. Dedekind provides two examples, mineralogy and the science of law, that are helpful in understanding what he intends by such a claim.

Mineralogy is the science dealing with the classification and properties of minerals. Stated in this manner, the goal of mineralogy is open to any number of methodological pursuits. That is, a mineralogist could attempt to classify the minerals based on smell, hardness, solubility, color, or any other discernible quality. But mineralogy is not in a state of complete disarray, each scientist pursuing her own research methods. Dedekind notes that there are, in fact, two qualities that are used in the classification process, chemical composition and crystallography. One may question why these two, and none of the others mentioned above, have come to the fore of the science. The simple answer lies in the benefit of adopting them as fundamental distinctions among minerals. "Each of these systems is perfectly justified, for science itself shows that similar bodies group themselves together most naturally in these ways" [1, ¶3]. Dedekind goes on to say that there is no a priori reason that

such a conclusion be reached, rather it is through experience that color is realized to be contingent to the "true nature of bodies" and that chemical composition and crystallography are recognized by scientists as distinctive characteristics. To clarify the relation these comments have to hypotheses he concludes:

> The introduction of such a concept as a *motif* for the arrangement of the system is, as it were, a hypothesis which one puts to the inner nature of the science; only in further development does the science answer; the greater or lesser *effectiveness* of such a concept determines its worth or worthlessness. [1, ¶3]

The phrase "as it were" should alert the reader to be careful not to take the statement at face value. A hypothesis is normally interpreted as a conjecture offered to account for some state of affairs. In the sciences hypotheses are suppositions that accord with known facts and provide a foundation for research which will either produce evidence for the truth of the hypothesis or its refutation. Thus, one should ask the question "In what sense does the introduction of a concept meet such criteria?" In formulating the basic definitions scientists choose the concepts that are most perspicuous given their background information. The definitions delimit testable hypotheses by their logical form. Those hypotheses that are not compatible with the basic concepts are eliminated from the research program. Scientists then choose hypotheses that can best explain some phenomena and thereby determine the path for future research. The success of the hypotheses (or progress of the science) determines the "effectiveness" of the original concepts.

The example of law helps to further clarify this idea. In formulating laws, legislators have specific guidelines they believe to be most beneficial to (at least a portion of) society. That is, they have specific values that help to shape the types of laws they will consider. Implementing these values through laws can be considered the goal of their efforts. In order to systematize their values certain definitions will be necessary. Dedekind proposes, for example, that the definition of legal institutions would be essential. The form of the definitions will restrict the laws that can be consistently formulated. As the laws emerge some of them will be logical consequences of others, and all of them "react upon the formation of the definitions" [1, ¶4]. So, again the initial concepts act as hypotheses, this time their worth is determined by how well the resulting laws capture the initial values of the legislators. It is possible that the laws fail to do so, in which case it is necessary to go back and

reformulate the definitions. "The greatest art of the systematizer lies in this turning and manipulation of definitions for the sake of the discovered laws or truths in which they play a role" [1, ¶4]. When the systematizer is required to replace an old concept with a new, one can say that the concept failed as a hypothesis in the most general sense. The intuitions of the systematizer were not successful in predicting the most effective definitions for the foundation of the science. It is the same as the mineralogist who first tried to classify the minerals by color.

One of the mathematical examples from Dedekind's *Habilitationsrede* involves the operation of multiplication. Originally, multiplication is conceived as a sort-of short hand for multiple applications of the addition operator on the same value. For instance, the expression $4 + 4 + 4 + 4 + 4$ is equivalent to the expression $4 \cdot 5$ because the number 4 is added 5 times to the number 0. If multiplication is nothing more than iterated addition then the operation can handle the case when the multiplicand (from above, 4) and multiplier (5) are both positive and when only the multiplier is positive (i.e. $(-3) + (-3) = (-3) \cdot 2$). But, under this interpretation, multiplication is not generally valid on the integers, for it makes no sense to say some number is added to 0 a negative number of times. Therefore, if multiplication is to be generally valid for the integers, it is necessary to define multiplication in such a way that the multiplicand and the multiplier can both take positive and negative values. In the context of hypotheses, the conception of multiplication as iterated addition has failed and a more general definition must be proposed as the current "hypothesis".

In mineralogy, a scientist chooses to pursue a particular research program, such as using crystallography for classification purposes, and by doing so "elevates [the distinction] to a chief touchstone of classification" [1, ¶3]. If an operation needs to be extended, then, if the new definition is to arise in a non-arbitrary, or necessary manner, a similar thing must occur.

> Laws which emerge from the initial definitions and which are *characteristic*[2] for the concepts that they designate are to be considered as *of general validity*. Then these laws conversely become the source of the generalized definitions if one asks: How must the general definition be conceived in order that the discovered *characteristic*[3] laws be always satisfied? [1, ¶6]

[2] My emphasis.
[3] My emphasis.

The passage implies that some of the laws resulting from the originally conceived operation should be considered as essential to it. Dedekind does not make it clear which laws are characteristic and which are not, but he does provide an example that will help to clarify what he means.

The initial concept of exponentiation is the result of iterating multiplication. Or, more precisely, the product of a single rational number x by itself y times can be seen as a single operation x^y. But, this only makes sense for nonzero natural number exponents. It is senseless to say that one multiplies 4 by itself -3, or $\frac{1}{2}$, times. Dedekind suggests that, in order to generalize the conception of exponentiation, we compare numbers of the following sort:

$$x^y, x^{y+z}, x^{y-z}, x^{y\cdot z}, x^{y/z}$$

where $x \in \mathbb{Q}$, $y, z \in \mathbb{N}$ and the exponent remains a natural number. "Once the laws prevailing here are known, they yield in turn the generalized definition if one requires that these laws set the standard for the character of exponentiation in general" [1, ¶9].

Dedekind first directs our attention to the following theorem:

$$x^y \cdot x = \underbrace{x \cdots x}_{y \text{ times}} \cdot x = x^{y+1}, \tag{1.1}$$

which follows from the definition of exponentiation, and which he sees as the starting point for our generalization. This is the simplest of operations on exponents and the more complex operations arise naturally from it. By applying the operation multiple times we achieve the addition theorem:

$$x^y \cdot x^z = x^y \cdot \underbrace{x \cdots x}_{z \text{ times}} = x^{y+1} \cdot \underbrace{x \cdots x}_{z-1 \text{ times}} = \cdots = x^{y+z}. \tag{1.2}$$

For $y, z \in \mathbb{N}$ there exists $w \in \mathbb{N}$ such that $y + z = w$ and thus $y = w - z$. From this, the following theorem for subtraction is derived:

$$x^{w-z} = x^y = \underbrace{x \cdots x}_{y \text{ times}} = \frac{\overbrace{x \cdots x}^{y+z \text{ times}}}{\underbrace{x \cdots x}_{z \text{ times}}} = \frac{\overbrace{x \cdots x}^{w \text{ times}}}{\underbrace{x \cdots x}_{z \text{ times}}} = x^w / x^z. \tag{1.3}$$

For instance

$$x^{6-2} = x^4 = x \cdot x \cdot x \cdot x = \frac{x \cdot x \cdot x \cdot x \cdot x \cdot x}{x \cdot x} = x^6 / x^2$$

If we hold equation (1.3) to be generally valid, as the quote above demands, the first two extensions of the operation are discovered, the rule for powers with zero exponents:

$$x^0 = x^{y-y} = x^y/x^y = 1 \text{ for all rational numbers } x, \tag{1.4}$$

and a rule for negative whole number exponents:

$$x^{-y} = x^{0-y} = x^0/x^y = 1/x^y. \tag{1.5}$$

It is clear from equation (1.2), that we have the following theorem:

$$(x^y)^z = \underbrace{x^y \cdots x^y}_{z \text{ times}} = x^{\overbrace{y+\cdots+y}^{z \text{ times}}} = x^{y \cdot z} \tag{1.6}$$

Now, Dedekind claims "it obviously follows [from equation (1.6)] that the division of an exponent requires us to perform the unique inverse of the original operation of exponentiation, namely, to split a given number into an (also given) number of equal factors" [1, ¶9]. While the exponent remains a natural number, for y divisible by z there exists $w \in N$ such that $y/z = w$, hence:

$$x^{y/z} = x^w = x^{y \cdot \frac{1}{z}} = (x^{1/z})^y = \underbrace{x^{1/z} \cdots x^{1/z}}_{y \text{ times}} \tag{1.7}$$

which is represented as

$$x^{y/z} = \underbrace{\sqrt[z]{x} \cdots \sqrt[z]{x}}_{y \text{ times}}.$$

Finally, if this law is to be valid in general then the properties that any new definition of exponentiation must fulfill have been determined. Furthermore, this last theorem demonstrates the need for the irrational and complex numbers. Consider, for instance, the examples:

$$2^{1/2} = \sqrt{2} \text{ and } (-5)^{1/2} = \sqrt{-5} = \sqrt{-1}\sqrt{5} = i\sqrt{5}.$$

In the example Dedekind wants to show how the laws resulting from the original conception of exponentiation, iterated multiplication, necessarily determines the definition of its extension, which must be able to take all rational numbers as exponents. The laws derived above, where the exponent is a natural number are taken to be characteristic of the operation of exponentiation. They are essential to the original conception of exponentiation

because they make sense for multiplying a rational number by itself a specified number of times. If they are then taken to be generally valid, that is for any $y, z \in \mathbb{Z}$, then the new definition of exponentiation must be such that these theorems are true. With the generalization of exponentiation, "one is thereby compelled to create the irrational numbers (with which the concept of limit appears)..." It is evident here that Dedekind recognizes the definition of the reals necessarily entail the property of continuity. There is no suggestion for the correct method to define the real numbers, but whatever it may be, the completeness of the new domain must be a result of the definition. In fact, this is the feature of the real numbers that he focuses on in [3].

1.2 Defining the real numbers

Although there is some evidence that, in 1854, Dedekind thought the number extensions could be defined through the operations themselves, such an assumption does not affect my argument.[4] Hence, I will not assume here that he had any opinion on the subject at that time. The content of Dedekind's first published foundational work, *Stetigkeit und irrationale Zahlen*, was the first precise implementation of his method for defining domain extensions, in this case the extension from the rational to real numbers. However, there are similarities between the method described in the *Habilitationsrede* and the one used in *Stetigkeit*, after discussing the work I will describe them.

As mentioned above, the impetus for Dedekind's concern regarding the real numbers was the reliance of some proofs in differential calculus on geometric intuitions. While he felt that these could be used as helpful aids in teaching the subject they can not provide a solid foundation. It appeared to Dedekind that the problem was that there was no arithmetic origin for the notion of continuity, and so such a discovery would solve the difficulty.

In order to solve this problem Dedekind introduces some important properties of the rational numbers.

I. For all $a, b, c \in \mathbb{Q}$, if $a > b$, and $b > c$, then $a > c$.

II. Let $a, c \in \mathbb{Q}$, if $a \neq c$, then there are infinitely many numbers $b \in \mathbb{Q}$ such that $a < b < c$ or $a > b > c$.

[4] For an excellent discussion on this topic see [9].

III. For $a \in \mathbb{Q}$, all the numbers of the system $\mathbb{Q}$ fall into two classes, A_1 and A_2, each of which contains infinitely many individuals; the first class A_1 is composed of all numbers a_1 such that $a_1 < a$, the second class A_2 is composed of all numbers a_2 such that $a_2 > a$; the number a itself may be assigned to either the first or second class, being respectively the greatest number of the first class or the least of the second.

Although the geometric considerations can not be used explicitly in solving the problem, Dedekind does rely on them analogically. The above properties can be interpreted as relating to the straight line by considering a, b, c to be points and interpreting $a < b$ as a being to the left of b on the line (similarly for $>$). But there is an important difference between the two domains, the straight line contains no "gaps" whereas the rational numbers do. The analogy between the straight line and the rational numbers draws out the feature of the rationals that must be improved upon. "Of the greatest importance, however, is the fact that in the straight line L there are infinitely many points which correspond to no rational number" [3, §III].

The real numbers, like the line, do not contain "gaps". This leads Dedekind to question the arithmetic "essence" of this continuity. "Everything must depend on the answer to this question, and only through it shall we obtain a scientific basis for the investigation of *all* continuous domains" [3, §III]. He finds that the essence of continuity for the line lies in the fact that whenever the line is divided into two classes, where every point in one class is to the left of every point in the other class, there is a unique point that has produced the division. Interpreted arithmetically, this becomes what Dedekind takes to be the essence of continuity for the real numbers, and then defines his basic concept for the domain extension.

> If now any separation of the system R [the rational numbers] into two classes A_1, A_2 is given which possesses only *this* characteristic property that every number a_1 in A_1 is less than every number a_2 in A_2, then for brevity we shall call such a separation a *cut* and designate it by (A_1, A_2). [3, §IV]

Now, it must be noted that every cut which is engendered by a rational number contains either a greatest number in A_1 or a least number in A_2 that produces the cut, and this is just property III. Although these two possibilities can be considered as different "objects", it is suggested that we consider them "not essentially different". For instance, consider the cut

engendered by the rational number $\frac{4}{5}$, either

$$A_1 = \{x \in \mathbb{Q} \mid x \leq \tfrac{4}{5}\}, \ A_2 = \{x \in \mathbb{Q} \mid x > \tfrac{4}{5}\},$$

or

$$A_1 = \{x \in \mathbb{Q} \mid x < \tfrac{4}{5}\}, \ A_2 = \{x \in \mathbb{Q} \mid x \geq \tfrac{4}{5}\}.$$

In the first case $\frac{4}{5}$ is the greatest element of A_1 and in the second $\frac{4}{5}$ is the least element of A_2. It would be unnecessarily complicated to take these as two different cuts, both of which are engendered by the number $\frac{4}{5}$. Hence, we will say, at Dedekind's behest, that they are not essentially different.

After showing that there are an infinite number of cuts not produced by rational numbers—that is, there does not exist a greatest element of A_1 nor a least element of A_2—Dedekind claims that this provides for us an arithmetic account of the discontinuity of the rational numbers. If one considers the straight line with a point taken to be the origin and another point, off of the origin, then the distance between the two can be taken to be the unit length. Now, the cuts the cuts which are not produced by any rational number are intimately related to the points on the straight line that have incommensurate measure with the unit length. Hence the irrational numbers are completely defined by all those cuts which are not produced by a rational number. The new numbers are distinguishable one from another by the cuts that they produce, that is, by investigating the sets of rational numbers that are less than and greater than them. Three simple theorems assure the reader that the set of reals is a dense linear ordering.

Finally, Dedekind is in a position to show that his definition of cut satisfies the theorem for completeness and therefore the reals also must satisfy the property.

Theorem 1.2.1 *If the set $\mathfrak{R}$ (the real numbers) is divided into two sets $\mathfrak{A}$ and $\mathfrak{B}$ such that for all a in $\mathfrak{A}$ and for all b in $\mathfrak{B}$, $a < b$, then there exists exactly one real number c which produces the separation.*

The proof for the theorem relies heavily on the three properties (mentioned before) of the rational numbers. By recognizing that any separation of the real numbers corresponds to a cut on the rationals Dedekind is able to fully utilize these properties. The completion of the proof is not the end of Dedekind's work, he also must show that the usual operations can be defined for cuts.

Since each real number corresponds uniquely to a cut, some method must be found which take cuts as arguments and produces a cut which corresponds to each operation on the real numbers. The operation of addition is easily definable for cuts. Suppose that α and β in the real numbers, corresponding to the cuts (A_1, A_2) and (B_1, B_2) respectively, are to be added. Their sum equals the real number γ corresponding to (C_1, C_2). The cut (C_1, C_2) is determined in the following way:

> If c is any rational number, we put it into the class C_1, provided there are two numbers one a_1 in A_1 and one b_1 in B_1 such that their sum $a_1 + b_1 \geq c$; all other rational numbers shall be put into the class C_2. [3, §IV]

Although Dedekind did not use the modern set theoretic notation for this definition, his language is clear enough that we can easily interpret it as

$$C_1 = \{c \in \mathbb{Q} \mid \exists\ a_1 \in A_1,\ b_1 \in B_1\ (c \leq a_1 + b_1)\}.$$

Of course C_2 would be the complement of C_1 in the rationals. So, the cut (C_1, C_2), corresponding to the sum of α and β, has been constructed using their counterparts. Little more is needed to show that this characterization of addition on cuts is sufficient. Dedekind claims that the other operations can be defined in a similar manner—and though the definitions do become more complicated, as can be seen in such a definition for multiplication—"and in this way we arrive at proofs of the theorems (as, e.g., $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$), which to the best of my knowledge have never been established before" [3, §IV].

Chapter 2

Overview of the theory of ideals

I have pointed out key elements in Dedekind's first two foundational works that are relevant to his mathematical practice. Now I will shift focus and give an overview of the theory of ideals. First, in §2.1, I will show why something like Kummer's ideal divisors were needed in number theoretic studies. This will be followed, in §2.2, by an introduction to the algebraic integers, and a demonstration of how unique factorization fails on this most general notion of integer. Then, §2.3 will illustrate the manner in which Kummer was able to reason about the ideal divisors by their behavior as divisors. Finally, I will give, in §2.4, a brief account of Dedekind's explanation of the investigations that led him from Kummer's ideal divisors to the definition of ideals.

2.1 Why ideal divisors?

In his *Elements*, Euclid presented not only geometric results but also key results in the theory of numbers. Unique factorization is a characteristic feature of the rational integers. Although Euclid did not prove that the integers could be uniquely factored, in book seven, he demonstrated what has come to be known as the Euclidean algorithm which ultimately leads one to a proof of unique factorization.

The theorems of number theory are remarkable in that they relate features of the well known rational integers in often surprising ways. Some of these theorems can be proved by relying on unique factorization of extensions of the rational integers. For instance, the Two Square Theorem (TST), discovered by Fermat, can be proved using the unique factorization of the Gaussian

integers[1]:

Theorem 2.1.1 *If a prime $p \in \mathbb{Z}$ is of the form $4n+1$, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.*

Proof. Using Wilson's lemma[2], one can show that there exists $m \in \mathbb{N}$ such that $p \mid m^2 + 1$. In the complex numbers $m^2 + 1 = (m + i)(m - i)$. But $p \nmid m \pm i$, therefore p is not prime in the complex numbers. Thus, there exist $x, y \in \mathbb{Z}[i]$ such that neither x nor y is a unit, and $p = xy$, so that $p^2 = N(p) = N(x)N(y)$. Thus, it must be the case that $p = N(x) = N(y)$. Remembering that $N(x) = a^2 + b^2$ for some $a, b \in \mathbb{Z}$, the proof is complete. □

Fermat claimed to have a proof of the theorem using the method of descent though this one was not known to him.

Other theorems known by Fermat that are related to the TST hint at a generalization:

$$p = x^2 + 2y^2 \text{ if and only if } p = 8n + 1 \text{ or } p = 8n + 3,$$

$$\text{and } p = x^2 + 3y^2 \text{ if and only if } p = 3n + 1.$$

These theorems can be proved using the property of unique factorization in extensions of the rational integers, the first for numbers of the form $a+b\sqrt{-2}$ and the second $a + b\sqrt{-3}$, $a, b \in \mathbb{Z}$. It may appear that these theorems can be easily generalized to yield a rule for primes that can be written $x^2 + dy^2$, $d \in \mathbb{Z}$. However, a difficulty arises immediately.

For primes that can also be written $x^2 + 5y^2$, the corresponding numbers of the form $a + b\sqrt{-5}$ do not factor uniquely.[3] For example,

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

In the two factorizations the factors can all be shown to be irreducible, that is, they are only divisible by the units and their conjugates. By definition an

[1]The Guassian integers, $\mathbb{Z}[i]$, are the set of numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$ and $i = \sqrt{-1}$. For any number $x + yi \in \mathbb{Z}[i]$ the norm is defined to be $N(x + yi) = x^2 + y^2$ for some $x, y \in \mathbb{Z}$, and $N(xy) = N(x)N(y)$.

[2]For all rational primes $p \in \mathbb{Q}$, $(p - 1)! \equiv 0 \pmod{p}$.

[3]Those numbers of the form $x^2 + 4y^2$ can be reduced to $x^2 + (2y)^2$, hence they are a special case of the Two Square theorem.

integer is prime when if it divides a product, it also divides one of the factors, so 2, if it is prime, must divide either $(1+\sqrt{-5})$ or $(1-\sqrt{-5})$. Because this is not possible the irreducible numbers in $\mathbb{Z}[\sqrt{-5}]$ are not necessarily primes. This demonstrates a failure of unique factorization in the domain. So, in order to reintroduce the desired property of unique factorization, new numbers must be introduced that act like primes and are divisors of those irreducible numbers that are not primes. In a similar way, in trying to generate the higher reciprocity laws (anticipated by Gauss), Kummer was led to develop his theory of ideal divisors.[4]

2.2 Algebraic integers

Kummer's cyclotomic integers were the first extension of the notion of integer since Gauss. The concept of algebraic integer, first introduced by Dedekind in the tenth supplement to second edition of Dirichlet's *Vorlesungen über Zahlentheorie*, provided a fully generalized concept of integer. The definition and its properties will help to clarify the problem of unique factorization from this vantage point. Any number θ which satisfies the equation

$$\theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \cdots + a_{n-1}\theta + a_n = 0,$$

where $a_1, a_2, \ldots, a_{n-1}, a_n$ are rational numbers, is called an *algebraic number* and if $a_1, a_2, \ldots, a_{n-1}, a_n$ are rational integers then the number is an *algebraic integer*. From now on I will refer to these as integers and specify when discussing the rational integers, which are the only algebraic integers in the field of rational numbers. As Dedekind notes From the definition arises a theorem which leads to the failure of unique factorization for these integers.

Theorem 2.2.1 *For any two integers α, β the three numbers $\alpha+\beta, \alpha-\beta, \alpha\cdot\beta$ will also satisfy equations described above, so they are also integers.*

The next theorem demonstrates the problem of unique factorization arising from this formulation of the concept of integer.

[4]Actually Kummer's theory of cyclotomic integers (or circle division, as it was known in his lifetime) was limited to non-unit complex divisors of 1, but the discussion here, and the one in §2.4, outline the general problem he encountered and a generalization of his method to other domains.

Theorem 2.2.2 *Any number satisfying an equation of the form*

$$F(\omega) = \omega^m + \alpha\omega^{m-1} + \cdots + \epsilon = 0,$$

where $\alpha, \ldots, \epsilon$ *are integers, is also an integer.*

In general, this implies that for any integer α, the number $\sqrt[s]{\alpha^r}$ is also an integer. An example might help to clarify why this causes difficulties.

Clearly the number -2 is an integer for it satisfies the equation

$$\theta + 2 = 0.$$

Now, according to Theorem 2.2.2, any number satisfying the following equation is also an integer:

$$F(\omega) = \omega^2 + (-2) = 0.$$

This implies that $\sqrt{2}$ is an integer, for

$$\omega^2 = 2 \implies \omega = \pm\sqrt{2}.$$

By similar reasoning, one can show that the square root of any integer is also an integer. But this implies that every integer has an infinite number of divisors. The proof of unique factorization in the integers rests on the fact that the prime numbers are also irreducible, that is only divisible by itself and 1. Thus it is clear that something must be done in order to recover unique factorization.

An algebraic integer will satisfy an infinite number of equations of the form above, but only one of these is minimal in degree. This equation, whose lead exponent is smallest, will be said to be *irreducible*. Now, assume that we have an irreducible equation satisfied by θ. The set of numbers generated by the equation

$$\phi(\theta) = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1}, \tag{2.1}$$

where $x_0, x_1, \ldots, x_{n-1} \in \mathbb{Q}$, will be called a *field of degree* n and represented as Ω.[5] The set is a field because, as in the field of rational numbers, these new numbers are closed under addition, subtraction, multiplication, and division (except by 0). A subset of this field are the integers of the field and will be represented by $\mathfrak{o}$.[6] This is the set on which Dedekind intends to introduce unique factorization through his concept of ideal.

[5] In modern notation, we would denote Ω by $\mathbb{Q}[\theta]$

[6] I will discuss, in §3.1 and §3.2, an additional requirement for the theory, that $\mathfrak{o}$ contain *all* of the integers of the field. This means that, in general, $\mathfrak{o}$ is larger than $\mathbb{Z}[\theta]$.

2.3 Ideal divisors

Here I will discuss an example in order to show how Kummer used divisibility properties to reason about his ideal divisors.[7] In particular, theorems from number theory can be used to show that 2 acts like the square of an ideal prime in the ring $\mathbb{Z}[\sqrt{-5}]$. Then, I will demonstrate how Kummer could use properties of divisibility to reason about the ideal divisor of 2. That is, he does not actually introduce the ideal numbers as new objects in the domain, but rather, he simply shows how such ideal numbers must behave as divisors of the numbers in the domain.

The next two theorems from elementary number theory serve to characterize the squares of primes.

Theorem 2.3.1 *For any $a \in \mathbb{N}$, if for every $x, y \in \mathbb{N}$, $a \mid x^2y^2$ implies that $a \mid x^2$ or $a \mid y^2$, then $a = 1$ or there exists a prime number p such that $a = p$ or $a = p^2$.*

Theorem 2.3.2 *For any $a \in \mathbb{N}$ if there exists $x \in \mathbb{N}$ such that $a \nmid x$ and $a \mid x^2$, then there exists a $y \neq 1$ and $z \in \mathbb{N}$ such that $a = y^2z$.*

Suppose a satisfies the antecedents of the two theorems, that is:

(1) $a \mid x^2y^2 \implies a \mid x^2$ or $a \mid y^2$.

(2) There exists $x \in \mathbb{N}$ such that $a \nmid x$ and $a \mid x^2$.

Then a is necessarily the square of a prime. Conversely, if a is the square of a prime, then it will satisfy the two relations above. Therefore the two properties completely characterize the squares of primes, and so they can be used to show that the number 2 acts like the square of a prime in the domain $\mathbb{Z}[\sqrt{-5}]$. In order to do this it will be shown that the number 2 satisfies the two properties in the domain. Doing so will require the introduction of three concepts.

An irreducible equation will likely have more than one root. Let all of the roots of an irreducible equation $\theta, \theta_1, \theta_2, \ldots, \theta_{n-1}$ be called the *conjugates* of the equation. As in the complex numbers, the numbers $1 + 2i$ and $1 - 2i$ are said to be conjugates because they are the only numbers satisfying the equation $x^2 - 2x + 5 = 0$. Obviously all of the conjugates will be integers since

[7] I will follow Dedekind's description, found in [5, §8].

they satisfy the same equation. So, also analogous to the complex numbers, the *norm* of a number $\mu = \phi(\theta)$ in Ω will be defined as the product

$$N(\mu) = \mu\mu_1\mu_2 \cdots \mu_{n-1},$$

where $\mu = \phi(\theta),\ \mu_1 = \phi(\theta_1), \ldots,\ \mu_{n-1} = \phi(\theta_{n-1})$. This concept is extremely important to the analysis of $\mathfrak{o}$, so I should mention a few of its properties. The norm of any integer is always a rational integer and $N(\mu) = 0$ if and only if $\mu = 0$. Furthermore, for any two $\alpha, \beta \in \Omega$,

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Finally, for three numbers $\alpha, \beta, \gamma \in \mathfrak{o}$ say that α and β are *congruent* (or *incongruent*) to one another *modulo* γ whenever $\pm(\alpha - \beta)$ is divisible by γ (or not). If they are congruent the relationship will be denoted

$$\alpha \equiv \beta \pmod{\gamma}.$$

Clearly, also analogous to the rational or complex numbers, $\mathfrak{o}$ can be partitioned into a finite number of *classes* modulo some number γ, except when $\gamma = 0$. Now every number in a class is congruent (modulo γ) and any number from a class is said to represent that class. Furthermore, Dedekind shows that the number of classes modulo γ is less than or equal to $N(\gamma)$. But this implies that $N(\mu) = 1$ just in case μ is a unit.

Now it is possible to show that 2 acts like the square of a prime in $\mathbb{Z}[\sqrt{-5}]$. First, notice that any two conjugates $x + y\theta,\ x - y\theta \in \mathbb{Z}[\sqrt{-5}]$ are congruent modulo 2, since their difference, $\pm 2y\theta$, is divisible by 2. Now, let $\omega = x + y\theta$ and $\overline{\omega} = x - y\theta$, so that

$$\omega \equiv \overline{\omega} \pmod{2} \implies \omega^2 \equiv N(\omega) \pmod{2} \tag{2.2}$$

Hence, the same can be said to be true for any other ω':

$$\omega'^2 \equiv N(\omega') \pmod{2}. \tag{2.3}$$

Now, by the rules of congruence[8]

$$\omega^2\omega'^2 \equiv N(\omega)N(\omega') \pmod{2}. \tag{2.4}$$

[8] $a \equiv b \pmod{c},\ d \equiv e \pmod{c} \implies ad \equiv be \pmod{c}$

For any values of x, y, x', y' for which 2 divides $\omega^2\omega'^2$, it must also be the case, by equation (2.4), that 2 divides $N(\omega)N(\omega')$. But, norms are always rational integers and since 2 is a rational prime, either $2 \mid N(\omega)$ or $2 \mid N(\omega')$. This, in conjunction with equation (2.2), necessitates the divisibility of either ω^2 or ω'^2 by 2. Thus 2 satisfies the antecedent of Theorem 2.3.1. Furthermore, if $\omega = x + y\theta$, where x and y are both odd, then $2 \nmid \omega$, but a calculation[9] shows $2 \mid \omega^2$. Thus the antecedent of Theorem 2.3.2 is satisfied. Hence, 2 acts like the square of a prime number in $\mathbb{Z}[\sqrt{-5}]$.

As stated previously, Kummer did not introduce new mathematical objects into the domain. Rather, he defined a number α based on the divisibility properties of it in the domain (in our example $\mathbb{Z}[\sqrt{-5}]$). If the number α existed in the domain, then it would be true that $\alpha^2 = 2$, therefore it can be said that for any number ω,

$$\alpha^n \mid \omega \iff (\alpha^n)^2 \mid \omega^2 \iff \alpha^{2n} \mid \omega^2 \iff (\alpha^2)^n \mid \omega^2 \iff 2^n \mid \omega^2. \quad (2.5)$$

Hence, for any number ω in $\mathbb{Z}[\sqrt{-5}]$ the highest power of α that divides it is equal to the highest power of 2 that divides ω^2. This will work fine for this particular instance but it does not provide a general method for solving problems of this sort. Equation (2.5) relies on the property that the ideal divisor is the square of a rational prime, but this will not be true in general, and so the method of calculation must only use α to the first power. In the deduction of such an equation other important divisibility properties of α in the domain will be discovered. The first is the primality of α in $\mathbb{Z}[\sqrt{-5}]$.

First, consider the situation where n=1 in equation (2.5), that is, 1 is the highest power of 2 that divides ω^2, and so 1 is also is the highest power of α that divides ω. Then, for some $a, b \in Z$

$$2(a + b\theta) = (x + y\theta)^2 = x^2 + 2xy\theta - 5y^2 = (x^2 - 5y^2) + 2xy\theta$$

$$\implies a + b\theta = \frac{x^2 - 5y^2}{2} + xy\theta.$$

Hence, it must be the case that $\frac{x^2-5y^2}{2}$ is an integer, but $N(\omega) = x^2 + 5y^2$, so $N(\omega)$ must be even. Now, assume that $N(\omega)$ is even, then for some $n \in \mathbb{Z}$,

[9] If x, y are odd then there exist $m, n \in \mathbb{Z}$ such that

$$\begin{aligned}\omega^2 &= ((2m+1) + (2n+1)\theta)^2 \\ &= 4m^2 + 4m + 1 + 2(4mn + 2m + 2n + 1)\theta + (4n^2 + 4n + 1)\theta^2 \\ &= 4m^2 - 20n^2 + 8mn + 8m - 16n - 2 = 2(2m^2 - 10n^2 + 4mn + 4m - 8n - 1)\end{aligned}$$

$2n = N(\omega) = x^2 + 5y^2$. Considering cases shows that either x and y are both even or both odd. A calculation proves that in either case

$$\text{for all } \omega = x + y\theta,\ \alpha|\omega \iff x \equiv y \pmod 2, \tag{2.6}$$

or equivalently, when $N(\omega)$ is even.[10] Kummer takes the divisibility properties of the ideal divisor α to define it in the domain. Additionally, from equation (2.6) it can be proven that α actually acts like a prime number in $\mathbb{Z}[\sqrt{-5}]$. For any product $\omega\omega'$,

$$\begin{aligned} \alpha \mid \omega\omega' &\implies N(\omega\omega') \text{ is even} \implies N(\omega)N(\omega') \text{ is even} \\ &\implies N(\omega) \text{ is even, or } N(\omega') \text{ is even} \\ &\implies \alpha \mid N(\omega) \text{ or } \alpha \mid N(\omega') \\ &\implies \alpha \mid \omega \text{ or } \alpha \mid \omega'. \end{aligned} \tag{2.7}$$

But a complete method of reasoning about elements of the domain that will determine the highest power of α by which it is divisible is desired. This is accomplished by first proving the following (taken verbatim from [5, §8]):

Theorem 2.3.3 *"The exponent of the highest power of α that divides a product is equal to the sum of the exponents of the highest powers of α that divide the factors."*

Proof. Suppose that s is the highest power of 2 that divides a number ω. Then there must exist $\omega_1 = x_1 + y_1\theta \in \mathbb{Z}[\sqrt{-5}]$ such that

$$\omega = 2^s(x_1 + y_1\theta.)$$

We must consider three cases. First, x_1 and y_1 cannot both be even, otherwise ω_1 is divisible by two and ω is divisible by 2^{s+1}. Second, if both are odd then,

[10] If $N(\omega)$ the first case

$$\omega^2 = (2m + 2n\theta)^2 = 4m^2 + 4mn\theta - 20n^2 = 2(2m^2 + 2mn\theta - 10n^2)$$

which is clearly divisible by 2. When x and y are both odd

$$\begin{aligned} \omega^2 &= ((2m+1) + (2n+1)\theta)^2 \\ &= (4m^2 + 4m + 1) + 2(4mn + 2m + 2n + 1)\theta - 5(4n^2 + 4n + 1) \\ &= 4m^2 + 4m - 20n^2 - 20n - 4 + 2(4mn + 2m + 2n + 1)\theta \\ &= 2[2m^2 + 2m - 10n^2 - 10n - 4 + (4mn + 2m + 2n + 1)\theta], \end{aligned}$$

which is again divisible by 2.

by equation (2.6), we have $\alpha \mid \omega_1$ and the highest power of α that divides ω is $2s+1$. Finally, if one of x_1, y_1 is even and the other odd we have $\alpha \nmid \omega_1$ so that $2s$ is the highest power of α dividing ω. This result combined with equation (2.7) shows that the theorem is true. □

The complete characterization of the divisibility of a number in $\mathbb{Z}[\sqrt{-5}]$ is near at hand. Notice that, according to equation (2.6), $1+\theta$ is divisible by α but it is not divisible by $\alpha^2 = 2$. This fact together with Theorem (2.3.3) leads us directly to the following congruence determining the highest power n of α that divides a number ω

$$\omega(1+\theta)^n \equiv 0 \pmod{2^n}. \tag{2.8}$$

This, of course, is equivalent to the statement that $2^n \mid (\omega(1+\theta)^n)$. If ω is divisible by α but not α^2 then $\omega(1+\theta)$ will be divisible by $\alpha^2 = 2$ (by Theorem 2.3.3), so that $n = 1$ in equation (2.8) as expected.

This example of the ideal divisor of 2 in the domain $\mathbb{Z}[\sqrt{-5}]$ will provide the means for understanding Dedekind's development of the concept of ideal, but first I will provide a quick overview of the process I have just completed. As with the number 2 in $\mathbb{Z}[\sqrt{-5}]$, theorems from the theory of rational integers can be used in order to determine the properties of those rational primes that are irreducible but do not act like primes in other extensions. In the example, 2 is the square of a prime. With similar information it is possible to determine all the necessary ideal divisors for a domain. The divisibility properties of the integers provides a method for determining the highest power of the ideal divisors that divide any number in the domain. Thus, the reintroduction of unique factorization in extensions of the rational integers can be reclaimed.

2.4 Ideals

Now that we have seen a process similar to that used by Kummer for reintroducing unique factorization to the cyclotomic integers, the explanation Dedekind provides for the development of the concept of ideal should be clear. The first feature Dedekind recognizes relates to the fundamental method Kummer used for defining the ideal divisors of a domain. They are defined by all those numbers that they divide. So, it seems natural to begin by considering precisely that set of numbers. For any two numbers ω, ω' in $\mathbb{Z}[\sqrt{5}]$

that are divisible by α, $\omega \equiv \omega'$ (mod α) and furthermore for any number κ that is not divisible by α it is the case that $\omega \not\equiv \kappa$ (mod α). That is, if $\alpha \mid \omega$ then the congruence relation can be used as a test to determine the class of numbers that are all divisible by α. By thinking of the number α as nothing more than the numbers that it divides one is not driven to sidestep the question of what the ideal divisors *are*. Since the ideal divisors have been introduced for the purpose of realizing unique factorization the actual numbers in the domain must be represented in the same manner as the ideal divisors. This is unproblematic because they can be considered as a special case, that is they are generated by an integer in the domain. For instance, in the domain $\mathbb{Z}[\sqrt{-5}]$, the set of numbers generated by the integer 7 can be represented in modern notation by

$$[7] = \{7\omega \mid \omega \in \mathbb{Z}[\sqrt{-5}]\}.$$

These considerations provide the reason for Dedekind's focus on the class of numbers divisible by the number the set is taken to represent.

Given the definition of integer in §2.2 there are two theorems that relate divisibility properties of a number to addition (likewise subtraction) and multiplication.

Theorem 2.4.1 *If two integers $\alpha = \mu\omega, \alpha' = \mu\omega'$ are divisible by the integer μ, then so are their sum $\alpha + \alpha' = \mu(\omega + \omega')$ and their difference $\alpha - \alpha' = \mu(\omega - \omega')$, since the sum $\omega + \omega'$ and difference $\omega - \omega'$ of two integers ω, ω' are themselves integers.*

Theorem 2.4.2 *If $\alpha = \mu\omega$ is divisible by μ, each number $\alpha\omega' = \mu(\omega\omega')$ divisible by α will also be divisible by μ, since each product $\omega\omega'$ of integers ω, ω' is itself an integer.*

These two theorems can now be related to the elements of the domain $\mathfrak{o}$ in the following way, where μ is a particular number in $\mathfrak{o}$, $\omega \in \mathfrak{o}$, and $\mathfrak{a}$ is the set generated by μ (i.e. $\mathfrak{a} = \{\mu\omega \mid \omega \in \mathfrak{o}\}$):

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 $\mathfrak{a}$.

Since these properties simply rely on the laws of divisibility and the ideal divisors were designed to fulfill those laws, the properties can be extended to them. That is, for example, the system of numbers in $\mathbb{Z}[\sqrt{-5}]$ divisible by the ideal divisor α satisfies the two properties. Thus Dedekind has discovered two properties that are necessary conditions for all of the integers, real and ideal, in the domain. Therefore, these sets that represent the integers in the domain will be called *ideals*, and those that are generated by actual numbers in the domain will be especially designated as *principal ideals*, and the ideal generated by the number η will be denoted $\mathfrak{o}\eta$. "A fact of the highest importance, which [Dedekind] 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" [5, Introduction]. That is, for any set of numbers satisfying the two properties, the set corresponds to either an ideal divisor or an actual integer in the domain. To demonstrate the connection the properties have to the class generated by an ideal divisor, I will again consider the example of $\alpha^2 = 2$ in $\mathbb{Z}[\sqrt{-5}]$.

Define $\mathfrak{a}'$ to be the set of all integers that are divisible by α (i.e. $\mathfrak{a}' = \{\alpha\omega \mid \omega \in \mathbb{Z}[\sqrt{-5}]\}$), so that according to equation (2.6) for any two integers $\omega, \omega' \in \mathfrak{a}'$

$$x \equiv y \pmod 2 \text{ and } x' \equiv y' \pmod 2.$$

By the rules of congruence, this implies that $x + x' \equiv y + y' \pmod 2$ and therefore

$$\alpha|(x + x' + (y + y')\theta) = (x + y\theta) + (x' + y'\theta) = \omega + \omega'.$$

This simply states that the sum of any two numbers divisible by α is also divisible by α (similar for subtraction). Furthermore, if $\alpha \mid \omega$ and $\omega' \in \mathbb{Z}[\sqrt{-5}]$, then we have

$$2 \mid N(\omega) \implies 2 \mid N(\omega)N(\omega') \implies 2 \mid N(\omega\omega').$$

Therefore, α divides $\omega\omega'$ and $\omega\omega' \in \mathfrak{a}'$. Thus, the two properties are fulfilled by the set $\mathfrak{a}'$ whose generator is α, and $\mathfrak{a}'$ is an ideal. This should help clarify how Dedekind came to found his explorations of the algebraic integers on the concept of ideal.

Chapter 3

The first two versions

This chapter will provide a high-level sketch of each of the first two versions of the theory of ideals developed by Dedekind in 1871 and 1877. I will note some of the changes occurring between them here, but leave a fuller discussion of these changes and the motivation behind the distinguishing features to the next chapter where I will focus on his methodology in relation to the changes occurring between the two versions.

3.1 The theory of ideals: 1871

In this section I will follow the path carved out by Dedekind, in 1871, that led to the unique factorization of the ideals. Following the introduction of some concepts shared with the presentation of 1877, the fundamental theorem is derived in three, very general, steps: introduce simple ideals, use simple ideals to deduce important relationships, and then show that every prime ideal is also a simple ideal.

The concepts of ideal, principal ideal, class, congruent, conjugate, and norm have already been introduced in either §2.3 or §2.4. Because the numbers of the domain are to be represented by sets, any operations, or relations, must be defined for sets. The number α is said to be *divisible* by the ideal $\mathfrak{a}$ if α is contained in the ideal $\mathfrak{a}$. Likewise the ideal $\mathfrak{a}$ *divides* the ideal $\mathfrak{m}$ if all of the elements in $\mathfrak{m}$ are also elements of $\mathfrak{a}$. Given two ideals $\mathfrak{a}, \mathfrak{b}$, the *least common multiple* (LCM), $\mathfrak{m}$, can be defined as the intersection of $\mathfrak{a}$ and $\mathfrak{b}$, or equivalently, the set of all elements common to both ideals. Furthermore the *greatest common divisor* (GCD), $\mathfrak{d}$, is simply the set of all sums $\alpha + \beta$

where $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$.

The next concept introduced is not relegated a term in 1871, but it is important to the theory none the less. For any number $\eta \in \mathfrak{o}$ and ideal $\mathfrak{a}$, there exists an ideal $\mathfrak{r} = \{\rho \mid \eta\rho \equiv 0 \pmod{\mathfrak{a}}\}$, such that $\mathfrak{r} \mid \mathfrak{a}$.[1] I will say that such an ideal $\mathfrak{r}$ *arises from the correspondence-congruence* for the number η and the ideal $\mathfrak{a}$. The related statement for the rational integers simply affirms that for all $a, n \in \mathbb{Z}$, there exists $r \in \mathbb{Z}$ such that $an \mid r$. This is evidently true as r can be taken to be the product of all the powers of primes that divide a but do not divide n. Using this concept and the basic laws of modules Dedekind deduces the following theorem.

Theorem 3.1.1 *If $\mathfrak{a}$ is any ideal, $\mathfrak{b} = \mathfrak{o}\eta$ is a principal ideal, $\mathfrak{r}$ is the ideal dividing $\mathfrak{a}$ that corresponds to η, and $\mathfrak{d}$ is the GCD of $\mathfrak{a}$ and $\mathfrak{b}$, then $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d})$.*

Although he does not say so, it is obvious that the ideal $\mathfrak{r}$ divides $\mathfrak{a}$ as every element of $\rho \in \mathfrak{r}$ is divisible by $\mathfrak{a}$, and so $\rho \in \mathfrak{a}$.

In secondary school mathematics the notions of prime and irreducible are often taken to be synonyms. This is because in the rational and complex integers the two concepts are coextensive. But, in modern algebra the concepts must be clearly distinguished one from another. In the two versions of Dedekind's theory of ideals an ideal is said to be *prime* when it is divisible by no other ideals except $\mathfrak{o}$ and $\mathfrak{p}$ (usually this is considered to be irreducible). But, he then shows that the prime ideals can be characterized by theorems which are more closely related to the usual definition.

Theorem 3.1.2 *If $\mathfrak{p}$ is prime then $\eta\rho \equiv 0 \pmod{\mathfrak{p}}$ (i.e. $\mathfrak{p} \mid \eta\rho$) implies either $\mathfrak{p} \mid \eta$ or $\mathfrak{p} \mid \rho$.*

Next, Dedekind derives the converse of the theorem, thus demonstrating that the prime ideals are completely characterized by Theorem 3.1.2. These two theorems can be seen as a method, and are used, for testing the primality of ideals. Furthermore, they necessitate that for any prime ideal $\mathfrak{p}$, the smallest rational number, p, in $\mathfrak{p}$ is a rational prime. Since $\mathfrak{o}p \subseteq \mathfrak{p}$, it is also the case that $N(\mathfrak{p}) \mid N(p) = p^n$ which implies that for some $f \in \mathbb{N}$, $N(\mathfrak{p}) = p^f$.

Theorem 3.1.2 is used almost immediately to introduce the key concept of simple ideal. A preliminary theorem is required and then the concept can be formally defined through the following theorem:

[1] Of course Dedekind did not use the set theoretic notation, but his language can clearly be interpreted in it.

Theorem 3.1.3 *For any nonzero, nonunit $\mu \in \mathfrak{o}$, there exists a number ν such that all of the roots π of the congruence $\nu\pi \equiv 0$ (mod μ) form a prime ideal.*

Dedekind thus writes "We will henceforth call prime ideals which arise as the roots of such a congruence *simple* ideals" [2, §163.4]. If $r \in \mathbb{N}$, then the roots ρ of the congruence $\nu^r\pi \equiv 0 \pmod{\mu^r}$ will form an ideal called the r^{th} *power* of $\mathfrak{p}$, and it will be denoted $\mathfrak{p}^r$. The set theoretic representation of the simple ideals, and their powers, are clearly seen to be

$$\mathfrak{p} = \{\pi \mid \nu\pi \equiv 0 \pmod{\mu}\}$$

and

$$\mathfrak{p}^r = \{\pi \mid \nu^r\pi \equiv 0 \pmod{\mu^r}\}$$

respectively. It is helpful to consider what the theorem regarding simple ideals says about the rational integers: for all nonzero, nonunit $m \in \mathbb{Z}$ there exists $n, p \in \mathbb{Z}$ such that p is prime and $m \mid np$. If we suppose that $m = p_1p_2\cdots p_k$ then n can be taken to be any number divisible by $p_1p_2\cdots p_{k-1}$ and then $p = p_k$. The same reasoning can be followed for the r^{th} power of $\mathfrak{p}$. Theorem 3.1.2 is used in conjunction with the definition of simple ideal to deduce the theorems which make up the heart of the theory.

Unless specified otherwise, all future references to an ideal $\mathfrak{p}$ will be about simple ideals. The goal now is to build enough machinery, using the useful concept of simple ideal, so that unique factorization is regained once it is shown that all prime ideals are simple ideals. Although the two key theorems discussed here may be clearly true for powers of primes in the rational integers, they are nontrivially true for ideals. In fact, a further assumption is required for these theorems.

After the introduction of simple ideals and their powers Dedekind moves on to the following theorem:

Theorem 3.1.4 *If $s \geq r$, then $\mathfrak{p}^r \mid \mathfrak{p}^s$.*

In the proof Dedekind informs the reader that a certain important quotient is an integer in the field Ω, "and therefore contained in $\mathfrak{o}$, since $\mathfrak{o}$ comprises *all* the integers of the field Ω" [2, §163.4]. In the footnote attached to the comment Dedekind informs the reader that the theorem is not generally valid without this additional assumption. Dedekind does not make it clear which

theorems rely on this property, but in fact all of the remaining theorems are dependent on it, more or less, indirectly.

Until it is shown that all prime ideals are also simple ideals all of the theorems rely on the special manner in which the simple ideals arise. While the analogous rational integer theorems would rest on the notion of multiplication, these are reliant on the inclusion relation for divisibility. The following theorem exemplifies this pattern:

Theorem 3.1.5 *If $\rho \in \mathfrak{o}$ is nonzero, then there exists a highest power of $\mathfrak{p}$ that divides ρ.*

Proof. There are only a finite number of incongruent numbers (mod ρ). Suppose, for the sake of deriving a contradiction, that there are infinitely many exponents r such that $\mathfrak{p}^r \mid \rho$, then by the definition of simple ideals there would be two, $\mathfrak{p}^q$ and $\mathfrak{p}^s$, such that

$$\nu^q\rho \equiv 0 \pmod{\mu^q} \quad \text{and} \quad \nu^s\rho \equiv 0 \pmod{\mu^s},$$

would be equivalent (mod ρ); that is

$$\frac{\nu^q\rho}{\mu^q} \equiv \frac{\nu^s\rho}{\mu^s} \pmod{\rho} \implies \left(\frac{\nu}{\mu}\right)^q = \left(\frac{\nu}{\mu}\right)^s + \omega,$$

where ω is an integer. Thus, it must be the case (by Theorem 2.2.2) that $\frac{\nu}{\mu}$ is an integer. From this, $1 \cdot \nu \equiv 0 \pmod{\mu}$ implies that $1 \in \mathfrak{p}$ and $\mathfrak{p} = \mathfrak{o}$ which cannot be the case. □

The calculation involved in this proof will be important for later considerations but for now it is enough to notice the use of simple ideals, and the definition of divisibility. Furthermore, the connection between this theorem and the rational integers needs no clarification.

Also key to the properties of simple ideals is the following very simple theorem:

Theorem 3.1.6 *Each power $\mathfrak{p}^r$ of a simple ideal $\mathfrak{p}$ is not divisible by any other prime ideal.*

The proof relies only on the definitions of simple ideal, divisibility, primality, and the primality test for prime ideals. In the rational integers the theorem is interpreted in a straight forward manner. If $p \in \mathbb{Z}$ is prime then for any $n \in \mathbb{N}$, p^n is not divisible by any prime other than p.

As Dedekind mentions, the importance of simple ideals to the theory is demonstrated by the next theorem.

Theorem 3.1.7 *For all $\mu \in \mathfrak{o}$, $\mathfrak{o}\mu$ is the LCM of all the powers of simple ideals that divide μ.*

Just as the statement that any $n \in \mathbb{Z}$ is the LCM of all the powers of primes that divide it, so too this theorem expresses the uniqueness of factorization for principal ideals by simple ideals. At this juncture the goal has nearly been achieved, but notice that the theorem is relevant only to those ideals generated by numbers in the domain $\mathfrak{o}$. Furthermore, these ideals are, now, only uniquely factored by the special simple ideals, not the prime ideals in general. Dedekind quickly dispels the second difficulty by showing that all prime ideals are simple ideals. The only thing left to do is augment Theorem 3.1.7 to be true for all ideals and not just the principal.

Before coming to the final statement of unique factorization I would like to draw attention to the restricted formulation. Remember that the test for prime ideals is only testable for integers in $\mathfrak{o}$, not for ideals. Since Dedekind has not defined the product of ideals this, of course, must be the case. For this reason the theorem above cannot focus directly on the ideals, in general, but must be restricted to principal ideals (i.e. those which are in direct correlation to integers in $\mathfrak{o}$). The fully general proof of unique factorization of ideals is proved in the equivalent formulation:

Theorem 3.1.8 *If all the powers of prime ideals that divide an ideal $\mathfrak{m}$ also divide a number η, then $\mathfrak{m} \mid \eta$.*

Clearly, this theorem, in conjunction with Theorem 3.1.7, states that once the highest powers of prime ideals that divide an ideal $\mathfrak{m}$ are known, then $\mathfrak{m}$ is completely determined.

3.2 The theory of ideals: 1877

Here I will sketch Dedekind's presentation of the theory of ideals found in 1877. The overview will consist of four parts: first comes the definition of the product of ideals, then I will explain what Dedekind takes to be, "the only [difficulty] presented by the theory" [5, §23], next I will show how Dedekind builds up to unique factorization for all ideals, lastly, the final piece to unique factorization will be the generalization of a familiar theorem for norms. I will rely on the concepts of divisibility, LCM, and GCD which are defined the same for the two versions.

In the last section I used the term correspondence-congruence in relation to the ideal $\mathfrak{r}$ which arises as the roots π of the congruence

$$\eta\pi \equiv 0 \pmod{\mathfrak{a}}$$

given the number η and the ideal $\mathfrak{a}$. Although, in 1877, Dedekind does mention the congruence, he does not use it to introduce the ideal. In fact, he merely points out that given the ideals $\mathfrak{b} = \mathfrak{o}\eta$ and $\mathfrak{a}$, there exists an ideal $\mathfrak{r}$, such that $\eta\mathfrak{r}$ is the least common multiple of $\mathfrak{o}\eta$ and $\mathfrak{a}$. "This case occurs frequently in what follows, and for that reason we say, for brevity, that the ideal $\mathfrak{r}$ dividing the ideal $\mathfrak{a}$ *corresponds* to the number η" [5, §19]. Notice the concept even adds the requirement of LCM to its counterpart in 1871, but Dedekind does not find it necessary to focus on the calculations that accompany the concept there.

The deduction of Theorem 3.1.1 relies on facts that are important to this presentation, so I will provide the proof now.

Proof of Theorem 3.1.1 Let $\mathfrak{a}$ and $\mathfrak{b}$ be any two modules (ideals being a special case of these) and $\mathfrak{d}$ and $\mathfrak{m}$ their GCD and LCM respectively. Let $(\mathfrak{b}, \mathfrak{a})$ be the *number of incongruent elements of* $\mathfrak{b}$ *modulo the module* $\mathfrak{a}$. In the more general theory of modules Dedekind has shown that

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{m}) = (\mathfrak{d}, \mathfrak{a}), \tag{3.1}$$

and since $\mathfrak{d}$ is divisible by $\mathfrak{o}$,

$$(\mathfrak{o}, \mathfrak{a}) = (\mathfrak{o}, \mathfrak{d})(\mathfrak{d}, \mathfrak{a}),\ (\mathfrak{o}, \mathfrak{m}) = (\mathfrak{o}, \mathfrak{b})(\mathfrak{b}, \mathfrak{m})$$

hence

$$N(\mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})N(\mathfrak{d}), N(\mathfrak{m}) = (\mathfrak{b}, \mathfrak{a})N(\mathfrak{b}) \tag{3.2}$$

and

$$N(\mathfrak{m})N(\mathfrak{d}) = N(\mathfrak{a})N(\mathfrak{b}).\ [5, §20]$$

So, in this case, by equations (3.1) and (3.2), $N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d})$ as was to be shown. □

Using the definition of prime ideals, in 1877, Dedekind gives only the contrapositive of Theorem 3.1.2. Thus, in contrast to 1871, here he does not prove that the prime ideals are completely characterized by this theorem. Such a

characterization is not necessary for the theory, so he has chosen to discard it from the presentation.

In 1877 the feel of the theory of ideals is drastically changed by the introduction of a very simple concept. For any two ideals $\mathfrak{a}$ and $\mathfrak{b}$, and $\alpha_1, \alpha_2 \in \mathfrak{a}$, $\beta_1, \beta_2 \in \mathfrak{b}$, let the ideal $\mathfrak{c}$ be composed of the sums $\alpha_1\beta_1 + \alpha_2\beta_2$. The ideal $\mathfrak{c}$ will be called the *product* of the ideals $\mathfrak{a}$ and $\mathfrak{b}$. Although Dedekind did know the definition for the product of ideals in 1871, he did not use it in that presentation. As I will discuss later, the definition allows one to deduce that the order of multiplication for any number of ideals does not change the result. Immediately one is able to define the related concept of exponentiation. That is, if an ideal $\mathfrak{a}$ is multiplied by itself m times, the ideal will be called the m^{th} *power* of $\mathfrak{a}$, and will be denoted $\mathfrak{a}^m$.

A few basic theorems for products of ideals demonstrate the close analogy this version has with the rational integers. Most notably is the theorem which extends the characteristic property of prime ideals, Theorem 3.1.2, to relate ideals to one another (rather than to numbers in $\mathfrak{o}$).

Theorem 3.2.1 *If* $\mathfrak{p} \nmid \mathfrak{a}$ *and* $\mathfrak{p} \nmid \mathfrak{b}$*, then* $\mathfrak{p} \nmid \mathfrak{ab}$.

Proof. $\mathfrak{p} \nmid \mathfrak{a}$ and $\mathfrak{p} \nmid \mathfrak{b}$ imply that there exist elements $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{b}$, such that $\alpha, \beta \notin \mathfrak{p}$. Hence $\alpha\beta \in \mathfrak{ab}$, but $\alpha\beta \notin \mathfrak{p}$ (by Theorem 3.1.2). □

Dedekind states that many of the rational number theoretic theorems connecting primes, and relative primes, to all integers could easily be shown to be true for ideals, but they cannot lead one to unique factorization of them. A problem arises in connecting the concepts of product and divisibility.

In number theory one learns that a divides c, for $a, c \in \mathbb{Z}$, simply means that there exists a unique $b \in \mathbb{Z}$ such that $ab = c$. As I have shown, this definition is not the one Dedekind uses in his theory of ideals. In fact, the two definitions cannot be shown to be equivalent for ideals in an arbitrary ring of algebraic integers. Sometimes it occurs that $\mathfrak{a} \mid \mathfrak{c}$ but there does not exist $\mathfrak{b}$ in the domain such that $\mathfrak{ab} = \mathfrak{c}$.[2] It is important to note that at this

[2]Dedekind gives the example of the field Ω "resulting from a root

$$\theta = \frac{-1 + \sqrt{-3}}{2}$$

of the equation $\theta^2 + \theta + 1 = 0$ whose integer elements are generated by the basis $[1, \sqrt{-3}]$.[5, §23] Let $\mathfrak{p} = [2, 1 + \sqrt{-3}]$ and $\mathfrak{o}(2) = [2, 2 + \sqrt{-3}]$. It happens that $\mathfrak{p} \mid \mathfrak{o}(2)$, but there is no ideal $\mathfrak{q}$ such that $\mathfrak{pq} = \mathfrak{o}(2)$, as is required.

point in the theory Dedekind recognizes there is a more general theory, which does not make the assumption that $\mathfrak{o}$ contains *all* the integers in a field Ω, as is required for his purposes, in the more restricted version.

Two lemmas requiring the additional premise are key calculational tools relating the integers of the domain $\mathfrak{o}$. There is no mention of ideals, other than $\mathfrak{o}$, in either the theorems or their proofs, but their importance to the theory is exemplified by Dedekind's dedication of a section to both an analysis of the difficulty and the theorems themselves. I will have more to say about these later, so that I may now move on to Dedekind's development towards rectifying the difficulty. That is, he must now show how his definition of divisibility on the ideals corresponds to the definition found in the usual presentation of the rational integers.

The next portion of 1877 is dedicated to showing that, given the necessary assumption that $\mathfrak{o}$ contains all the integers of Ω, for all $\mathfrak{a} \mid \mathfrak{c}$ there exists a unique $\mathfrak{b}$ such that $\mathfrak{ab} = \mathfrak{c}$, so that divisibility and multiplication have the right relationship to one another. Dedekind deduces a string of theorems each of which achieves the desired result in a limited sense.

Theorem 3.2.2 *For all prime ideals* $\mathfrak{p}$ *there exists a number* η *and an ideal* $\mathfrak{d}$ *such that* $\mathfrak{pd} = \mathfrak{o}\eta$.

The connection between principal ideals and $\mathfrak{o}$ should assist one in appreciating the significance of the theorem which clearly limits the goal by not requiring every number divisible by $\mathfrak{p}$ to fulfill the theorem that an ideal $\mathfrak{m}$ exists, but also restricting the divisor to prime ideals.

There are two other theorems of this nature. The first simply replaces the prime ideal, in theorem 3.2.2, with an ideal which is divisible by $\mathfrak{p}$. But Dedekind does add an important addendum to the theorem that the ideal multiplied by $\mathfrak{p}$ has norm less than the norm of the product. The last theorem, stated in Dedekind's own words, of this sort has nearly achieved generality but does limit the product to principal ideals.

Theorem 3.2.3 *Each ideal* $\mathfrak{a}$*, when multiplied by a suitable ideal* $\mathfrak{m}$*, becomes a principal ideal.*

Through these theorems Dedekind finds himself in a position to prove the theorem in full generality. That is, for any two ideals $\mathfrak{a}$ and $\mathfrak{c}$ such that $\mathfrak{a} \mid \mathfrak{c}$, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathfrak{c}$.

In §2.3 I stated that, for two numbers in $\mathfrak{o}$, the norm of a product is the product of their norms; this has not been shown to be true for ideals.

This fact is the last theorem necessary for Dedekind to prove his theorem for unique factorization of the ideals. A good deal of the machinery from the last section is necessary for the proof which is by no means obvious. This theorem was not required in 1871 as the product did not have a role in the theory. It is another feature of the theory which is more analogous to previous theories of unique factorization, this time that of the complex integers.

The theorem which demonstrates the unique factorization of ideals is state in a slightly different form from the theorem in 1871.

Theorem 3.2.4 *An ideal* $\mathfrak{a}$ *(or a number* α*) is divisible by an ideal* $\mathfrak{d}$ *(or a number* δ*) if and only if each power of a prime ideal which divides* $\mathfrak{d}$ *(or* δ*) also divides* $\mathfrak{a}$ *(or* α*).*

The theory presented in 1877 follows much more closely rational number theoretic considerations for unique factorization. In fact, we will see in §4.2 that the connection between divisibility and multiplication on the ideals allows Dedekind to finish the proof of unique factorization in a manner nearly identical to that in which one proves unique factorization for the rational integers. After stating Theorem 3.2.4 he even presents the more familiar statement: "If we combine all factors of the same prime in the decomposition of an ideal $\mathfrak{a}$ then we find

$$\mathfrak{a} = \mathfrak{p}^a \mathfrak{q}^b \mathfrak{r}^c \cdots ,$$

where $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots$ are different prime ideals" [5, §25]. No such statement occurs in 1871. That the theory should be as similar as possible to the theory of rational integers appears to be one of Dedekind's methodological demands, but he also seems to have had other reasons for changing the theory in the manner in which he did. I will discuss these reasons in the next chapter.

Chapter 4

Method and practice

In the first three chapters I have independently developed some of Dedekind's methodological concerns and his mathematical practice. The present chapter will be devoted to demonstrating connections between the two. First, in §4.1, I will discuss some of the ontological concerns relating both to his foundational and mathematical work. Next, §4.2 will focus on Dedekind's requirement that essential properties and operations carry over from one domain to another. Following this will be, §4.3, a discussion of Dedekind's preference for conceptual over algorithmic reasoning, the latter being reasoning which relies on specific representations. Finally, in §4.4, I will argue that all of these methodological demands require the use of axiomatic characterizations, so that Dedekind should be viewed as implementing the axiomatic method, and not emphasizing it as an independent goal or demand.

4.1 Ontological concerns

There are three features of Dedekind's work that are relevant to a discussion of his ontological concerns and their relation to defining new mathematical objects. I agree with Stein in the opinion that Dedekind is not overly focused on the ontological status of mathematical objects themselves [10, §VII]. Rather, this section will recognize the methodological demands he emphasizes when defining new objects. Additionally, I will briefly show how these considerations relate to his preference for his ideals over Kummer's ideal divisors.

I would first like to mention what has come to be known in the literature as

"Dedekind abstraction". As I mentioned before, it was originally introduced in relation to [4], but the method can be used informatively in the reading of *Stetigkeit*. That is, through the method introduced in [4], one can determine the necessary additions and interpretations required for understanding how the method could be implemented in *Stetigkeit*.[1] After using the notion of cut to construct the real numbers Dedekind adds the following comment.

> Whenever, then, we have to do with a cut (A_1, A_2) produced by no rational number, we create a new, an *irrational* number α, which we regard as completely defined by this cut (A_1, A_2); we shall say that the number α corresponds to this cut, or that it produces this cut. From now on, therefore, to every definite cut there corresponds a definite rational or irrational number, and we regard two numbers as *different* or *unequal* always and only when they correspond to essentially different cuts. [3, §IV]

In this quote Dedekind refers to each cut *corresponding* to a real number three times. It is quite clear that the real number should not be taken to be the cut, but rather, the two have a special connection. This hallmark of Dedekind's definitions of number domains (even more explicit in *Was sind und was sollen die Zahlen*) has been the topic of much discussion concerning Dedekind (see [8], [11], or [12]). I will not say more about the topic here, as it would take the discussion too far afield; however, it is an important aspect of Dedekind's methodology for defining number domains. Related to this are the three demands he places on extending a number domain.

In his *Habilitation* lecture, Dedekind's focus is on the method for extending operations themselves, not the domains. That is, he does not provide a clear explanation for the manner in which one should define a domain (or its extension).[2] But, it is clear that by the first version of his theory of ideals he did have a well conceived method for extending domains. The method, is laid out in a footnote in the introduction to [5]. Additionally, the note is a testament to the close relationship Dedekind saw between the theory of ideals and real numbers. In the footnote Dedekind discusses the method for introducing new elements and its relation to his introduction of the real numbers in 1872. I will discuss not only the method as applied to cuts and

[1] Tait makes this suggestion in footnote 12 in [12].

[2] Although there is some ambiguity about whether Dedekind gives some explanation for defining number domains, I will not concern myself here with the question. For a discussion of the circularity involved in such an explanation see [9].

the real numbers but also to the ideals and algebraic integers. As laid out in 1877, Dedekind stipulates three necessary requirements for any introduction of "new arithmetic elements":

1. The definition should be composed of elements available before the introduction.

2. The new elements should all be engendered simultaneously.

3. Any necessary calculations must have clear definitions for the new elements.

As I said, these three requirements are also adhered to by Dedekind in the construction of the ideals, but they are not the only similarities between the two introductions of new numbers. Not only does Dedekind use infinite sets of numbers in both presentations, the two constructions share a deeper connection.

In both the introduction of the presentations, [2] and [3], Dedekind is attempting to show that a specific property holds in the new domain, continuity on the reals and unique factorization on the ideals of a given field. In order to do this he assumes that all of the usual facts about the restricted domain (i.e. the rational numbers and algebraic integers respectively) may be used for the purposes of reasoning. By considering special sets of the domains, cuts and ideals, Dedekind is able to show that, when taken together, the cuts fill in the "gaps" in the rationals and the ideals add the missing primes to the algebraic integers.

Key to these considerations is Dedekind's use of infinite sets of elements. There are two fundamental features relevant to his definitions of cut and ideal: the fact that Dedekind takes a set of elements to be a mathematical object and that the sets contain a completed infinity. I will not spend much time on either of these topics but I would like to mention that, in both respects, Dedekind's work was only accepted with skepticism by his peers in the mathematical community and that his work had a great influence on the modern view. Whether or not Dedekind had a "modern" understanding of sets is unrelated to my considerations here; rather, I simply want to point to the widespread use of set theoretic language by Dedekind.[3] It is important to note that Dedekind took sets of rational numbers as a given in the theory.

[3]For a further discussion of Dedekind's set theoretic approach see [7, Chapters II and III].

He did not think that by considering a set of the rational numbers he was extending the foundation available to him for introducing the real numbers, and this brings us to the first requirement mentioned above.

Dedekind required that "arithmetic remain free from intermixture with extraneous elements" and that any definition of the real numbers should "be based on phenomena one can already define clearly *in the domain* R of rational numbers" [5, Introduction]. Clearly the cut satisfies this condition as it is just two sets of rationals. Furthermore, given the notion of a field of numbers and the algebraic integers of that field, the same can be said for ideals. They are simply composed of the subset of the integers in the field that are divisible by the integer or ideal number that they correspond to. There are no further elements to add to the theory, so the theory of ideals also satisfies the demand.

The second stipulation, that all the elements be "engendered simultaneously", is slightly more complex, but Dedekind has good reason for the condition. There are means, other than cuts, by which one may define the real numbers. In fact, Dedekind cites the effort of Heine as a reason for his decision to publish *Stetigkeit*. It is possible to define real numbers as roots of equations or as logarithms, but in Dedekind's opinion, these methods, and others like them, make the mistake of allowing the new numbers to be introduced consecutively, rather than all resulting from a single definition. The problem with such a definition is that each element is reliant on the form by which it is defined, and each element is the result of a different form. Thus, any operations on the new numbers would be dependent on the form of the number under consideration. Such a state of affairs was undesirable for Dedekind, and his concept of cut was not open to this criticism. Although two cuts may correspond to the same real number (i.e. for (A_1, A_2) generated by a rational number, A_1 has a greatest element or A_2 has a least element), Dedekind recognizes them as not essentially different and any calculation involving the two would be identical, as it would only rely on the rational numbers which approach the number that generated the cut. For the ideals there isn't even a distinction of this magnitude to be made. Furthermore, all of the ideals are simultaneously generated by the definition.

As Dedekind's goal for the theory of real numbers was a solid grounding for arithmetic, it is necessary to show that all of the usual operations be definable on the new elements. I have shown Dedekind's definition for addition (subtraction could be defined similarly) on cuts, and although the definition of multiplication and division are more complex they may be clearly defined.

The situation for the theory of ideals is a little more complicated than that for the real numbers. In 1871 Dedekind demonstrates that multiplication is not a necessary operation for proving unique factorization on the ideals; all that is required is a non-operational sense of divisibility, and the operations GCD and LCM. But in the quote above he says that "a general definition of their multiplication, seems all the more necessary since the ideal numbers do not actually exist in the numerical domain $\mathfrak{o}$." The fact that he changes the theory of ideals to include multiplication relates to his methodological demands in an important way which will be explored in §4.3. For now it is enough to notice that because unique factorization of the algebraic integers is the goal for the theory of ideals it is not required to define addition, subtraction, and the other operations. Hence, the third requirement for introducing new elements has been fulfilled.

The last ontological concern on which I will focus is one reason for Dedekind's preference for his ideals over the ideal divisors; that is, having a definition which provides some reference. Remember that the ideal divisors are defined only by their action as divisors in the domain. That is, the ideal divisors are never given explicit definitions, instead, one can only reason about their properties. Dedekind finds this aspect of Kummer's treatment of ideal divisors to be a shortcoming of the theory. In response to the possibility of achieving unique factorization in the algebraic integers via a theory which employs a general notion of the ideal divisors Dedekind remarks as follows.

> 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, and this can be done in several ways. [5, §10]

Let me clarify the line of reasoning that Dedekind is here pursuing. As I explained in the discussion above, Dedekind requires that, when introducing new numbers, one is able to give definitions for the necessary operations. Furthermore, in the introduction to [5], he claims that since the ideal numbers do not actually exist in the domain $\mathfrak{o}$ a general definition of multiplication "seems all the more necessary". In order to accomplish this, in the simplest manner, one must have some objects to refer to. In this way the ideals are

considered to be superior to the ideal divisors as the product of two ideals is easily defined.

4.2 Preservation of operations and properties

In §1.1 I discussed Dedekind's opinion, expressed in his *Habilitationsrede*, that the introduction of a concept serves as an hypothesis in a theory. The concept of multiplication of ideals, in his second version of the theory of ideals, is no exception to the rule. Remember that the success of the hypothesis depends on the fruitfulness of the science, and the role played by the concept. Thus, it will be good to ask what are the changes that Dedekind finds of value in the new theory. In addition to the benefits described in this section I will show, in §4.3, how the second version focuses less on calculation and representation and more on the fundamental properties of the theory, another demand of great importance to Dedekind. But there seems to be another, very basic, feature of the new theory that Dedekind is attracted to. The new theory is much more in accord with the theory of rational integers than the previous.

Dedekind often speaks of carrying over properties, or theorems, from one theory to another. Whenever possible he attempts to simplify the theory by relying on already known principles whose conditions for truth are not only met in some previously known theory, but also in the theory he is considering. For a very simple example consider Dedekind's more general theory of modules introduced prior to the theory of ideals. He shows that ideals are simply special cases of the modules so that "we immediately carry over to ideals the notion of divisibility of modules" [5, §19]. In the second version, the analogy with the theory of rational integers can be exploited to a much greater extent because multiplication actually has a role in the theory.

The first meaningful occurrence of a reference to the theory of rational integers occurs in §22 where Dedekind introduces the concept of multiplication of ideals. After defining the concept, he wants to show that one can multiply any number of ideals, in any order, and the outcome will be the same.

> It follows immediately from this definition that $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$, $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$ and, if $\mathfrak{c}$ is any third ideal, $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$, whence we conclude by well-known arguments that in a product of any number of ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ the order of the multiplications, which combine *two*

> ideals into a single product, has no influence on the final result, which can be written simply as $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_m\ldots$

The clause "well-known arguments" is accompanied by a footnote referring the reader to a passage in Dirichlet's *Vorlesungen über Zahlentheorie*. Thus, one can rely on the proof in the rational integers which shows that if the three properties on multiplication hold, then it can be determined that order of multiplication does not change the result. Dedekind again directs the reader's attention to Dirichlet's work in the proof of the following theorem.

Theorem 4.2.1 *For all ideals $\mathfrak{a} \neq \mathfrak{o}$, $\mathfrak{a}$ is prime or uniquely expressible as a product of primes.*

The proof is very similar to that of the rational integers, with the exception that it relies on the concept of norm. Dedekind has already shown that every ideal is divisible by a prime. If $\mathfrak{a}$ is only divisible by that prime and $\mathfrak{o}$, then we are finished. If $\mathfrak{a}$ is divisible by the prime ideal and another ideal, then we can use the same reasoning to break the new composite ideal down into a prime ideal and another, each time the resulting ideals have norm less than or equal to the norm of $\mathfrak{a}$. This shows that every ideal can be represented as a product of prime ideals. To achieve the uniqueness, Dedekind assumes that there are two (not necessarily different) products of prime ideals that equal $\mathfrak{a}$:

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_m.$$

Now, since one of these $\mathfrak{p}_i$ must divide one of the $\mathfrak{q}_j$ (by Theorem 3.2.1), it can be assumed, without loss of generality, that $\mathfrak{p}_1 \mid \mathfrak{q}_1$, and since neither of these are $\mathfrak{o}$, they must be equal, so that

$$\mathfrak{p}_1(\mathfrak{p}_2\mathfrak{p}_3\cdots\mathfrak{p}_m) = \mathfrak{p}_1(\mathfrak{q}_2\mathfrak{q}_3\cdots\mathfrak{q}_m).$$

This implies that

$$\mathfrak{p}_2\mathfrak{p}_3\cdots\mathfrak{p}_m = \mathfrak{q}_2\mathfrak{q}_3\cdots\mathfrak{q}_m$$

so that by relying on the same argument as in the theory of rational numbers it is determined that each factor of the two products has an equivalent ideal in the other factor, so that the product of prime ideals is unique.

It is obvious that Dedekind is concerned with relying on corresponding theorems in the rational integers for proving things about the ideals. But there is more to it than this. Mathematicians are very comfortable with the

reasoning accompanying the theory of rational integers, the second version of the theory of ideals is therefore much more intuitive. The first version does not even utilize the notion of product which is logically prior to the concept of divisibility in the usual presentation of the rational integers. In the opening section of the 1877 version Dedekind even mentions the connection. In relation to the fact that when every ideal of a field is a principal ideal, the indecomposable and prime numbers are coextensive so that the laws of the rational integers will govern the field. "This will follow easily from the results below, but I mention it now to encourage the reader to make continual comparisons with the special cases, and especially the theory of rational numbers, because without doubt it will help greatly in understanding our general theory." [5, §19]

Dedekind criticizes Kummer's theory on this point; while remarking that the definition of ideal divisor is legitimate, he also says that

> 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 integers, may lead to hasty conclusions and incomplete proofs. And in fact this danger is not always completely avoided. 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 $\mathfrak{o}$. [5, Introduction]

So, because it would be preferable to reason about the ideals (and integers) in a manner similar to the rational integers, one must be able to speak of the product of ideals. Since this is not possible for the ideal divisors, it is possible that faulty reasoning, due to the analogy, could lead one to make mistakes.

4.3 Conceptual reasoning

This section will focus on Dedekind's emphasis on conceptual reasoning, as opposed to calculation or algorithmic reasoning. A representation, or form, is required for any calculation, so I will take Dedekind's desire to suppress calculation and/or representation to be one and the same. In either case the

antithesis will be the use of fundamental concepts, or properties, which do not rely on particular representations, or calculation, for developing the theory. I will first discuss how this relates to another reason for Dedekind's preference for his ideals over a generalized theory similar to Kummer's method. This will be followed by related comments on the absence of simple ideals, which are akin to Kummer's ideal divisors, from the second version of the theory of ideals. Lastly I will discuss the importance of the auxiliary propositions and a likely reason, beyond the fact that they require $\mathfrak{o}$ to contain all the integers in Ω, for Dedekind's setting them apart in the presentation.

I have already discussed both Kummer's ideal divisors and Dedekind's ideals, but I will now focus on the motivation behind his preference for ideals, their conceptual power in formulating a theory which does not rely excessively on calculation. In §2.3 I provided an example of how one can use the divisibility of the number 2 in $\mathbb{Z}[\sqrt{-5}]$ to reason about its ideal divisor α, where $\alpha^2 = 2$. Remember that for $\omega \in \mathbb{Z}[\sqrt{-5}]$, $\alpha \mid \omega = x + y\sqrt{-5}$, where $x, y \in \mathbb{Z}$, if and only if $x \equiv y \pmod 2$ (by equation 2.6). But this means that for some $z \in \mathbb{Z}$, $x = y + 2z$, and by substitution $\omega = 2z + (1 + \sqrt{-5})y$, that is the multiples of α form an module whose basis consists of the numbers 2 and $(1 + \sqrt{-5})$. This can be represented as

$$\mathfrak{a} = [2, 1 + \sqrt{-5}].$$

Dedekind notes that such a module is also an ideal because the sum/difference of any two numbers in $\mathfrak{a}$ is also in $\mathfrak{a}$, and the product of any element in $\mathfrak{a}$ and an element of $\mathbb{Z}[\sqrt{-5}]$ is again in $\mathfrak{a}$.

If all the ideals of the domain are to be represented by this form, then one discovers that there is a general form for them. Dedekind uses properties of the norm of an element in the domain to show that all of the ideals can be represented as

$$\mathfrak{m} = [ma, m(b + \sqrt{-5})],$$

where $a, b, m \in \mathbb{Z}$ and

$$b^2 \equiv -5 \pmod a.$$

Furthermore, the ideal $\mathfrak{m}$ is unchanged by substituting any number congruent to b modulo a for the number b. Thus, it is also the case that

$$\mathfrak{a} = [2, -1 + \sqrt{-5}].$$

In order to show how such a theory might achieve unique factorization in the domain Dedekind goes on to define principal ideals, congruence, norm,

multiplication, and divisibility on these representations of ideals. Next it is necessary to demonstrate that multiplication and divisibility are related in the appropriate way. Accomplishing this requires a great deal of calculations relying on congruence relations, determinants of various systems, and also norms. Finally, the notion of a prime ideal is introduced as an ideal divisible only by itself and $\mathfrak{o}$. For some number η, the ideal $\mathfrak{r}$, consisting of all the roots ρ of the congruence $\eta\rho \equiv 0 \pmod{\mathfrak{p}}$, which is either $\mathfrak{o}$ or $\mathfrak{p}$ is then used to show that $\mathfrak{p}$ has the characteristic feature of primes; for any product of numbers divisible by $\mathfrak{p}$ one of the factors must be divisible by $\mathfrak{p}$. Finally, the contrapositive of the theorem is deduced, but this time for ideals rather than numbers. This leads one immediately to the theorem for unique factorization in the domain.

Dedekind is unsatisfied with the methods employed in such a theory. His main complaint is that the proofs of the propositions rely on the representation of the ideals. As stated above, the ideal $\mathfrak{a}$ has two different representations. So, for instance, there are two different proofs for the same theorem involving $\mathfrak{a}$, and this will always be the case for the theory. Any theory reliant on such arbitrary features as these does not rely on characteristic elements.

> 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 (for example the composition of decomposable forms of all degrees). [5, §12]

As with the definitions of operations in Dedekind's *Habilitationsrede*, he hopes to express that, to a great extent, mathematics proceeds in a necessary fashion, not dependent on the mathematician. A theory in greater accord with Kummer's ideal divisors relies heavily on the calculation, and arbitrary representation, therefore it would be in conflict with this principle.

There is a close connection between Kummer's ideal divisors and the simple ideals. The latter relies on representation in much the same way as the former, and this seems to be the primary reason for Dedekind's reformulation in 1877 which is free from explicit definition of the special prime ideals. As I have not yet shown the connection, nor the manner in which simple ideals are reliant on representation let me do so now. Again, I must refer the reader

to the discussion in §2.3 regarding the ideal divisor of the number 2. Recall that the final deduction in that demonstration is equation (2.8)

$$\omega(1+\theta)^n \equiv 0 \pmod{2^n},$$

which serves as a test to determine whether a number is divisible by α^n. Or equivalently it can be thought of as a definition for the ideal generated by α^n. That is, the ideal consisting of all the roots ω of the above equivalence. Clearly this is closely related to the definition of the power of a simple ideal.

Remember that the r^{th} power of a simple ideal $\mathfrak{p}$ is a prime ideal that arises as roots, ρ, of the equivalence

$$\rho\nu^r \equiv 0 \pmod{\mu^r},$$

where μ is a nonzero (non-unit) number in $\mathfrak{o}$, and ν is an appropriately chosen number in $\mathfrak{o}$. In the example it is known that, in $\mathbb{Z}[\sqrt{-5}]$, the number 2 is indecomposable, but not prime so that there must exist an ideal divisor α. Then, by reasoning about the divisibility properties of 2 in the domain it was deduced that $\alpha \mid (1+\theta)$ and $\alpha^2 \nmid (1+\theta)$. Hence, in this example, the goal is to find the prime ideal which divides the number 2, and the properly chosen ν in the domain is $(1+\theta)$. Similarly, the number which will divide this prime ideal is precisely the ideal divisor α.

In this example it is discovered that the ideal corresponding to the ideal divisor α must depend on the two numbers 2 and $1+\theta$. But, the ideal could similarly rely on the numbers 2 and $-1+\theta$, so that the ideal can in some sense be represented by different pairs of numbers. As stated previously, the presentation in 1871 relies heavily on these special prime ideals and therefore on their special representation. In fact, many of the proofs of the theorems rely on the special relationships arising from the numbers ν and μ. Dedekind says as much about a theory which would follow Kummer's method.

> One notices, in fact, that the proofs of the most important propositions depend upon the representation of an ideal by the *expression* $[ma, m(b+\theta)]$. [5, §12]

Because of the similarities between this method and the 1871 presentation, this comment, can be taken as a reason for the changes occurring in his theory of ideals between 1871 and 1877.

Dedekind has isolated two theorems in a section titled *Auxiliary propositions* because they are the first two in his theory which must rely on the fact

that all the integers of Ω must be in the domain $\mathfrak{o}$. In the 1871 version he does mention the additional property, but Dedekind prefers his new presentation on this matter as "the principal difficulty to be surmounted is now thrown more clearly into relief" [5, Chapter 4]. Remember that the "principal difficulty" is to show that when $\mathfrak{a} \mid \mathfrak{c}$ there is a unique ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathfrak{c}$. This property requires us to assume that $\mathfrak{o}$ contains all of the integers in Ω. It is important to notice that the property is not even expressible in terms available in the 1871 version. That is, since the product of ideals was not a part of the theory, the "principal difficulty" manifested itself in a different form.

Although the additional requirement is first mentioned in the proof of Theorem 3.1.4, the "difficulty" is most clearly evident in Theorem 3.1.5 (which I reproduce here):

> If $\rho \in \mathfrak{o}$ is nonzero, then there exists a highest power of $\mathfrak{p}$ that divides ρ.

Because the 1871 theory does not follow the modern route to proving unique factorization of the rational integers, it is difficult to see the relationship, but the proofs of this theorem and the first of the auxiliary propositions will help to clarify its reliance on $\mathfrak{o}$ containing all the integers of Ω.

Theorem 4.3.1 *Let ω, μ, ν be three nonzero numbers in $\mathfrak{o}$ such that $\mu \nmid \nu$. Then all of the terms*

$$\omega,\ \omega\frac{\nu}{\mu},\ \omega\left(\frac{\nu}{\mu}\right)^2,\ \omega\left(\frac{\nu}{\mu}\right)^3, \ldots,$$

up to some finite number e,

$$\omega\left(\frac{\nu}{\mu}\right)^e$$

will be in $\mathfrak{o}$ (will all be integers), and beyond that none of them will be.

The first part of the proof is identical to the proof for Theorem 3.1.5 with ω replacing ρ, ω' replacing ω, and setting η equal to $\frac{\nu}{\mu}$. The second part is just another means to show that all powers of $\mathfrak{p}$ greater than e do not divide ω. Thus, the theorem could be restated:

> For every integer ω satisfying the congruence $\omega\nu \equiv 0 \pmod{\mu}$, which taken together make up the prime ideal $\mathfrak{p}$, there is some highest power e such that $\omega\nu^e \equiv 0 \pmod{\mu^e}$, so that $\mathfrak{p}^e \mid \omega$, but $\mathfrak{p}^{e+1} \nmid \omega$.

The proof of the second auxiliary proposition also plays a role in the 1871 theory.

Theorem 4.3.2 *Let μ, ν be nonzero elements of $\mathfrak{o}$ such that $\mu \nmid \nu$. Then there exists two nonzero elements of $\kappa, \lambda \in \mathfrak{o}$ such that*

$$\frac{\kappa}{\lambda} = \frac{\nu}{\mu}$$

and $\lambda \nmid \kappa^2$.

The proof follows the same reasoning found in 1871 used to support the claim that for any simple ideal $\mathfrak{p}$, the two ideals $\mathfrak{p}^r$ and $\mathfrak{p}^{r+1}$ are distinct. The proof relies on the supposition that $e \geq 1$ is the highest power of $\mathfrak{p} = \{\omega \mid \omega\nu \equiv 0 \pmod{\mu}\}$ which divides μ itself, or in terms of 1877, e is the last integral term of the series

$$\mu,\ \mu\frac{\nu}{\mu},\ \mu\left(\frac{\nu}{\mu}\right)^2, \ldots,\ \mu\left(\frac{\nu}{\mu}\right)^e.$$

Then, by defining $\lambda\mu\left(\frac{\nu}{\mu}\right)^{e-1}$, the desired result follows immediately:

$$\frac{\kappa}{\lambda} = \frac{\nu}{\mu},\ \frac{\kappa^2}{\lambda} = \mu\left(\frac{\nu}{\mu}\right)^{e+1},$$

the latter of which is not an integral, by our assumption, so that $\lambda \nmid \kappa^2$. Although this is all that is said in 1871, the reasoning continues in 1871 in the following manner. Since

$$\frac{\kappa}{\lambda} = \frac{\nu}{\mu} \implies \lambda\nu = \kappa\mu \text{ (i.e. } \mathfrak{p} \mid \lambda) \implies \nu\lambda\nu = \left(\frac{\kappa\mu}{\lambda}\right)$$

$$\lambda\nu^2 = \left(\frac{\kappa^2}{\lambda}\right)\mu^2.$$

Remember that $\frac{\kappa^2}{\lambda}$ is not an integer so that $\mathfrak{p}^2 \nmid \lambda$. Finally, this implies that $\mathfrak{p}^r \mid \lambda^r$ and $\mathfrak{p}^{r+1} \nmid \lambda^r$ so that $\mathfrak{p}^r$ and $\mathfrak{p}^{r+1}$ really are distinct. Hence, it has been shown that the reasoning in Dedekind's two auxiliary propositions, from 1877, is used in 1871 to support claims about prime ideals, in particular simple ideals, as these considerations occur before the proof that all prime ideals are also simple ideals. Now, I would like to provide a reason, in accordance with Dedekind's methodological demands, that inspired the separation of the auxiliary propositions and their neglect of ideals (other than $\mathfrak{o}$).

In addition to the two auxiliary propositions reliance on that additional premise that $\mathfrak{o}$ contain all of the integers in Ω, I would like to point out that Dedekind also uses the section to isolate the bulk of algorithmic reasoning necessary for the theory. In neither the statement of the two theorems nor their proofs does Dedekind refer to ideals (other than $\mathfrak{o}$). The section is completely devoted to properties of the numbers in Ω. As the 1871 version does rely on similar arguments, Dedekind could easily have formulated theorems which seemed less ad hoc and included reasoning about ideals. But this would have infected his theory of ideals with undue calculations, and in Dedekind's view reduced the value of including the product of ideals in the theory. Instead, Dedekind accepts the result that these two theorems seem unconnected to the rest of his theory of ideals in order to maintain the conceptual purity of the rest of his theory. Additionally, there seems to be no way around the feeling of ad hoc requirements in the theory, as that is precisely why Dedekind has isolated these theorems in the first place. There can be no argument for $\mathfrak{o}$ containing all of the integers, only the explanation that the theory cannot be completed without the stipulation. So, in order to maintain a conceptually pure theory of ideals, the two auxiliary propositions are purposefully stated in such a manner that ideals are not mentioned.

4.4 Axiomatic characterization

Now that I have described what I take to be (at least some of) Dedekind's methodological demands, I would like to focus on the role of axiomatic characterization in both his foundational and mathematical works. My concern is not whether a modern notion of axiomatics is either a methodological priority for Dedekind or even present in the works I have investigated.[4] Rather, I suggest that many of the characteristic features of the axiomatic method aid Dedekind in best accomplishing his methodological goals. In this section I will show how Dedekind uses features of axiomatics for achieving his methodological demands described in the previous three sections. But before I do this I would like to draw attention to a similar reliance on characteristic, or fundamental, properties in the two foundational works.

Much of Dedekind's effort in *Stetigkeit* has an axiomatic character. He is very clear about what properties he allows himself to rely on for reasoning

[4] A more developed use of axiomatic reasoning is evident in *Was sind und was sollen die Zahlen*.

about the rational numbers. Since he is mostly concerned with achieving the continuity principle for the real numbers he focuses on the ordering principles of the rationals. But, as his further goal is to construct a system which will provide a "scientific foundation for arithmetic" [3, Introduction], he must be able to use the new domain for everything the real numbers are used for in arithmetic. In §159, of [2], Dedekind notes that "system" R (the set of rational numbers) is closed under the four fundamental operations (with the exception of division by 0). That is, as clarified in 1877, the rational numbers are a member of the general class of fields [5, §15]. Together with the three properties given for the rational numbers (at the beginning of this section), which Dedekind notes are more important for his purposes, he has provided a complete list of the fundamental properties open to him for reasoning purposes.

Dedekind's treatment foreshadows the modern axiomatic method in additional ways. He also makes a list of features that must be satisfied by the new domain, the real numbers, corresponding to the cuts on rationals. So, although he does not simply give the axioms for the real number domain, what he does, is show that any definition intended to capture the same properties as the real numbers must satisfy the same fundamental properties that modern mathematicians take as the axioms for the real numbers. The three properties given for the rational numbers, which Dedekind also shows to be true for the reals, and the property of continuity provide an axiomatic characterization of the ordering of the real numbers up to an isomorphism.[5] But continuity of the cuts is not enough to show that they can be used to reason about the real numebrs. Dedekind goes on to say that "the problem is to indicate a precise characteristic of continuity that can serve as a basis for valid deductions" [3, §3]. These "deductions" that he refers to are simply the usual operational facts associated with the real numbers. This seems clear when one considers a passage found soon after the previous quote:

> Still lengthier considerations seem to loom up when we attempt to adapt the numerous theorems of the arithmetic of the rational numbers (as, e.g., the theorem $(a + b)c = ac + bc$) to any real numbers. [3, §6]

Hence, Dedekind recognizes the importance of those characteristic results, or in modern terms, the axioms. Something similar to this reliance on fundamental characteristics also occurs in Dedekind's *Habilitation* lecture.

[5]While Dedekind did not explicitly show that this was the case, [8] explores the issue.

The definition of cut, which serves as the basic object for constructing the real numbers, focuses on the characteristic property of arithmetic continuity. In the *Habilitationsrede*, once it is discovered that a new definition for an operation must be provided (because the old one is not applicable to the extended domain), Dedekind directs the investigation to the "characteristic" features of the operation. These are determined to be the properties that must be true for any definition intended to take members of the domain extension as arguments. For instance, since exponentiation must be defined in such a way that negative numbers can occur in the exponent, one should investigate the manner in which negative integers result from the positive integers (i.e. $y - z$ for $y, z \in \mathbb{N}$ and $z > y$) as exponents. This necessitates a property ($x^{y-z} = \frac{x^y}{x^z}$ for all $y, z \in Z$) that any definition of exponentiation must fulfill. Again, Dedekind has given a list of the necessary properties that must result from any newly proposed definition of the operation. One feature of the axiomatic method is to define objects by their necessary and sufficient conditions. Although Dedekind does not define the operations, nor the domains, by giving their necessary and sufficient conditions (or fundamental characteristics), he does make it clear that the definition of the operation, or domain, must satisfy these properties.

In §4.1, I argued that the construction of real numbers and ideals both satisfy the three requirements for domain extensions which were also described there. Each of the requirements expresses one of Dedekind's methodological concerns, which rely on different features of the axiomatic method. When he requires that the properties of the rational numbers, and his definition of cut, be the only elements used in the construction of the real numbers he brings to light the paths of reasoning open to us. In a sense, the properties are just the axioms of the rationals, and their logical results. Then, as he states what must be true for the construction, the axioms for the reals, Dedekind shows that his definition and the properties of the rational numbers are enough. Thus, the method appears to be of the following nature. Using the axiomatization of the rational numbers, Dedekind must find a definition that, with the properties of the rationals, is able to fulfill the axiomatization of the real numbers.

The simultaneous creation of all of the numbers in the domain to be defined is the second demand for introducing new domains suggested by Dedekind. In order to achieve such a goal, one must isolate those features of the mathematical objects that are sufficient for picking them out. By doing so, one is able to determine what sorts of properties are required for

any proposed definition. Obviously, when this is accomplished all of the elements of the domain can be defined by the single definition which satisfies the required properties.

The final aspect of Dedekind's demands on defining new domains is that all of the necessary operations for a domain be definable on the new objects. This is simply a recognition that the new domains are not completely defined without the usual operations and their properties (like the distributive property of multiplication over addition on the real numbers). Here again, the usual axioms for operations are shown to be deducible given the three properties of the rational numbers and the definition of cut. So, although the fundamental characteristics of the real numbers are not taken as a definition for the domain, they are necessarily derivable from the definition of cut.

In §4.2 I claimed that carrying operations and properties over from a one domain to another is of great importance to Dedekind. By investigating what is required for such an accomplishment, and looking at an example in Dedekind's work I will show how he, once again, relies on axiomatic thinking. As I have already discussed the way in which operations should be extended I will now focus the discussion on properties, as expressible in theorems. If a theorem is true in a restricted domain and one hopes that it also be true in an extension then one of two possibilities must occur, either it must rely on a subset of the axioms that are also axioms for the extension, or one must be able to derive the lemmas in the extension on which the theorem relies in the restricted domain. Since Dedekind does not have an explicit list of axioms for either the rational numbers, nor the ideals, only the latter option is open.

In the second version of the theory of ideals Dedekind introduces multiplication as a fundamental operation, and by doing so he is able to rely on proofs from the theory of rational integers to fill out the particulars of proofs on the ideals. As I showed in §4.2, one is able to multiply ideals in any order without changing the result. In the rational numbers one finds that the product of two rational numbers is commutative, so that for all $a, b \in \mathbb{Z},\ ab = ba$. Furthermore, multiplication is associative on the rational numbers, for all $a, b, c \in \mathbb{Z},\ a(bc) = (ab)c$. These two properties on multiplication determine that the order of multiplying any number of rational numbers will not change the product. Similarly, once it is know that the product of ideals is commutative and associative, it can further be claimed that the order of multiplying any number of ideals does not change the product. So, because the ideals have been shown to have the right properties in common with the rational

integers, we can determine that it shares other properties. Obviously this example, once again, highlights Dedekind's emphasis on listing the necessary properties, this time for proving a theorem. Therefore, by relying on this feature of the axiomatic method Dedekind is able to show how reasoning on the rational integers can be used for the ideals.

Very often, Dedekind makes comments about the importance of fundamental characteristics, and conceptual reasoning. I have highlighted some of these comments in §4.3, and also shown how his methodology is evident in the theory of ideals. There are two aspects of conceptual reasoning on which I will comment. First, if mathematics should not rely on representation, and calculation, then it must rely on those features of the concepts which pick it out in some other way. That is, like with the ideals, the necessary and sufficient conditions which determine the objects are of utmost importance. But this is just a demand for axiomatic characterizations of systems of mathematical objects. Dedekind's constant focus on the fundamental concepts, or characteristics, thus requires an axiomatic standpoint. Second, although it is sometimes unclear what is meant by "conceptual" reasoning in mathematics, it should not be denied that the rise of axiomatics has played a major role in a more conceptual practice. Furthermore, it is Dedekind's emphasis on these *fundamental* features of operations, mathematical objects (like fields, rings, and ideals), and domains that flavor his work with a more conceptual approach. He ultimately desires to isolate those properties that are necessary and sufficient for reasoning so that it is perfectly clear what must be assumed in a theory. This is also a characteristic of the axiomatic method. The auxiliary propositions in 1877 are an excellent example of his adherence to the approach.

Dedekind makes a list of the necessary requirements on $\mathfrak{o}$, in the theory, up to the auxiliary propositions:

> (a) The system $\mathfrak{o}$ is a finitely generated module $[\omega_1, \omega_2, \ldots, \omega_n]$ whose basis is also a basis for the field Ω.
>
> (b) The number 1 is in $\mathfrak{o}$, hence so are all the rational numbers.
>
> (c) Each product of two numbers in $\mathfrak{o}$ is also in $\mathfrak{o}$. [5, §23]

This list of properties on $\mathfrak{o}$ could be interpreted as the axioms, relating to $\mathfrak{o}$, necessary for the more general theory of ideals (which Dedekind even refers to). Dedekind comments that

> By attentively considering the theory developed until now, one notices that all the definitions retain their meaning, and the proofs of all theorems still hold, when one *no longer supposes* that the domain $\mathfrak{o}$ consists of *all* integers in the field Ω. [5, §23]

But for the completion of unique factorization of the ideals this is not enough. For that, one must make the extra assumption that $\mathfrak{o}$ contain all the integers of Ω. The addition of the section, in 1877, devoted to the two auxiliary propositions exemplify Dedekind's strict demand that the required assumptions for a theory be clearly spelled out, analogous to axioms.

In all of the circumstances one finds Dedekind pursuing a methodological goal that can best be achieved through axiomatic characterizations, or listing of required properties. Thus, it seems quite clear that his methodological demands drive him to rely on an axiomatic approach.

While Dedekind continued to publish important works through the 1890s, my analysis has been limited to those works published by 1877. Further research investigating Dedekind's axiomatic tendencies through his final publications should prove to be very interesting and informative, not only to Dedekind's work but also with respect to the modern view of axiomatics.

Bibliography

[1] Richard Dedekind. On the Introduction of New Functions In Mathematics. In Ewald [6], pages 755–762. Translated as "On the concept of number" by William Ewald, Vol. 2.

[2] Richard Dedekind. Supplement X to *Vorlesungen über Zahlentheorie* von P.G. Lejeune Dirichlet *(2^{nd} Ed.)*. Vieweg, 1871. Translated by Jeremy Avigad, 2003.

[3] Richard Dedekind. *Stetigkeit und irrationale Zahlen.* Vieweg, 1872. Translated by Wooster Beman as "Continuity and irrational numbers" in *Essays on the theory of numbers*, Open Court, Chicago, 1901; reprinted by Dover, New York, 1963. The Beman translation is reprinted, with corrections by William Ewald, in [6], volume 2, pages 765-779.

[4] Richard Dedekind. *Was sind und was sollen die Zahlen.* Vieweg, Braunschweig, 1888. The second edition, with a new preface, was published in 1893, and is translated by Wooster Beman as "The nature and meaning of numbers" in *Essays on the theory of numbers*, Open Court, Chicago, 1901; reprinted by Dover, New York, 1963. The Beman translation is reprinted, with corrections by William Ewald, in [6], volume 2, pages 787-833.

[5] Richard Dedekind. *Theory of Algebraic Integers.* Cambridge University Press, Cambridge, 1996. A translation of *Sur la théorie des nombres Entiers Algébrique* (1877), translated and introduced by John Stillwell.

[6] William Ewald, editor. *From Kant to Hilbert: A Source Book in the Foundations of Mathematics.* Clarendon Press, Oxford, 1996. Volumes 1 and 2.

[7] José Ferreirós. *Labyrinth of Thought: A History of Set Theory and Its Role In Modern Mathematics*. Birkhäuser Verlag, Basel-Boston-Berlin, 1999.

[8] Dirk Schlimm. Richard Dedekind: Axiomatic Foundations of Mathematics. Master's thesis, Carnegie Mellon University, 2000.

[9] Wilfried Sieg and Dirk Schlimm. Dedekind's Analysis of Number: Systems and Axioms. To be published in *Synthese*.

[10] Howard Stein. Logos, logic, and logistiké. In William Aspray and Phillip Kitcher, editors, *History and Philosophy of Modern Mathematics*, pages 238–259. University of Minnesota, 1988.

[11] William W. Tait. Critical notice: Charles Parsons' mathematics in philosphy. *Philosophy of Science*, 53:588–606, 1986.

[12] William W. Tait. Truth and proof: The platonism of mathematics. *Synthese*, 69:341–370, 1986.