Summer 2016

Richard Dedekind and the Creation of an Ideal: Early Developments in Ring Theory

Janet Heine Barnett
Colorado State University-Pueblo, janet.barnett@csupueblo.edu

Richard Dedekind and the Creation of an Ideal: Early Developments in Ring Theory

Janet Heine Barnett*

December 10, 2017

1 Introduction

In the historical development of mathematics, the nineteenth century was a time of extraordinary change during which the discipline became more abstract, more formal and more rigorous than ever before. Within the subdiscipline of algebra, these tendencies led to a new focus on studying the underlying *structure* of various number (and number-like) systems related to the solution of various equations. The concept of a *group*, for example, was singled out by Évariste Galois (1811-1832) as an important algebraic structure related to the problem of finding all complex solutions of a general polynomial equation. Two other important algebraic structures — *ideals* and *rings* — emerged later in that century from the problem of finding all integer solutions of various equations in number theory. In their efforts to solve these equations, nineteenth century number theorists were led to introduce generalizations of the seemingly simple and quite ancient concept of an integer. In this project, we examine how obstacles they encountered along the way led to the sophisticated new mathematical concepts of an 'ideal' and a 'ring' by examining the work of German mathematician Richard Dedekind (1831-1916).

A native of Brunswick (Braunschweig) in Germany, Dedekind spent most of his life in his hometown, first as a youth and student, and later as a professor at the Brunswick Polytechnikum. In 1850, he entered the University of Göttingen and attended his first course with the celebrated mathematician Carl Friedrich Gauss (1777-1855); he completed his doctorate under Gauss' supervision just two years later. Dedekind remained at Göttingen to complete his *habilitation* degree in order to qualify as a university teacher, completing that degree in 1852. He then taught as an instructor at the University of Göttingen until 1858, when he accepted a teaching position at the Polytechnikum in Zürich. Dedekind remained in Zürich until his return to Brunswick in 1862. A lifetime bachelor, he lived out the remainder of his days in Brunswick with his sister Julia, a novelist, until her death in 1914. Following his retirement from the Brunswick Technische Hochschule (a university with an engineering focus) in 1894, he continued publishing and occasionally teaching. By the time of his own death in 1916, he was already something of a legend among the next generation of mathematicians.[1] Today, Dedekind

*Department of Mathematics and Physics; Colorado State University-Pueblo; Pueblo, CO 81001 - 4901; janet.barnett@csupueblo.edu.

[1] In *Men of Mathematics*, E. T. Bell tells the following amusing anecdote [Bell, 1937, p. 519]:

> [Dedekind] lived so long that although some of his works ... had been familiar to all students of analysis for a generation before his death, he himself had become almost a legend and many classed him with the shadowy dead. Twelve years before his death, Teubner's *Calendar for Mathematicians* listed Dedekind as having died on September 4, 1899, much to Dedekind's amusement. The day, September 4, might possibly prove to be correct, he wrote to the editor, but the year certainly was wrong. "According to my own memorandum I passed this day in perfect health and enjoyed a very stimulating conversation on 'system and theory' with my luncheon guest and honored friend Georg Cantor of Halle."

is widely recognized for his contributions to algebraic number theory, the foundations of the real numbers, the early development of set theory, and abstract algebra, especially the theory of ideals.

While teaching at Göttingen, Dedekind attended courses taught by two other important nineteenth century mathematicians, Peter Gustav Lejeune Dirichlet (1805-1855) and Bernhard Riemann (1826-1866). Later in his life, he also became a close associate and friend of Georg Cantor (1845-1918), the creator of set theory, whom he met while both were on holiday in the Black Forest in 1874. The work of these three men, along with that of Gauss, had a significant influence on Dedekind's understanding of and approach to mathematics. In its turn, Dedekind's unique approach to mathematics was a major influence on and inspiration for subsequent generations. The highly influential algebraist Emmy Noether (1882-1935), for instance, is reported to have frequently told her own students during discussions of her own theory of ideals that "Alles steht schon bei Dedekind" ("Everything is already in Dedekind").

A key feature of Dedekind's approach was the formulation of a new conceptual framework for studying problems that were previously treated algorithmically. Dedekind himself described his interest in solving problems via the introduction of new concepts as follows [Dedekind, 1888, p. 16]:

> The greatest and most fruitful progress in mathematics and other sciences is through the creation and introduction of new concepts; those to which we are impelled by the frequent recurrence of compound phenomena which are only understood with great difficulty in the older view.

Notice here Dedekind's emphasis on *abstraction*: the creation of new concepts through the identification of the common properties that frequently recur in a collection of related phenomena. Another distinguishing characteristic of Dedekind's work was his insistence on formulating concepts in terms that did not depend on their notational representation, so as to obtain the greatest *generality* possible.

Dedekind's quest for abstraction and generality, together with his careful methodology, frequently required long periods of study and gestation before he felt satisfied with his creations. Between 1871 and 1894, for example, he published four different versions of his theory of ideals[2], none of which was simply a revision of an earlier paper. Instead, each of these four publications described a new version of the theory of ideals in which Dedekind reformulated the underlying concepts in clearer and more abstract terms.[3] Each of the four also went through repeated early drafts in Dedekind's working notebook (or *Nachlass*), as was the case with all his publications. Both the brilliant mathematical insights resulting from these patient years of working (and re-working) his ideas, and the precision and clarity with which he expressed those ideas, have justifiably earned Dedekind renown as one of the most influential mathematicians of the nineteenth century.

In this project, we will encounter Dedekind's brilliance first hand through excerpts from his 1877 version of this theory of ideals, *Theory of Algebraic Integers* [Dedekind, 1966]. Sections 2 and 3 begin an exploration of the number theoretic concerns that motivated Dedekind to develop the concept of an ideal. In Section 4 and 5, we then introduce and explore his definition of an ideal and the associated algebraic structure of a ring. Sections 6 and 7 then connect the concept of an ideal back to Dedekind's original motivation for introducing this new algebraic object.

---

[2] Three of Dedekind's four publications on ideals appeared (in 1871, 1879, and 1894) as appendices to the second, third, and fourth editions of Dirichlet's *Vorlesungen über Zahlentheorie* (*Lectures on Number Theory*), a text that Dedekind edited based on lectures that he himself attended. The third version of Dedekind's theory of ideals first appeared in French as a series of articles in 1876-1877, and was later published as an independent monograph in 1877. The excerpts we will read in this project are taken from the (1996) English translation of that monograph.

[3] For more details about Dedekind's development of ideal theory, see [Edwards, 1980] or the preface to [Dedekind, 1966].

2 Germ of the theory of ideals

In this section, we examine Dedekind's description of the motivating idea behind the theory of ideals through excerpts from Chapter 2 of his monograph [Dedekind, 1966]. We begin with a short excerpt in which Dedekind reminded his readers of some basic integer properties. Notice that Dedekind uses the expression "rational integer" here, where we would typically just say 'integer'. Because he did so for a very good reason (which will become clear as we read later excerpts), we adopt Dedekind's terminology throughout this project. We do, however, denote the *set* of all rational integers by $\mathbb{Z}$, whereas Dedekind himself did not use any special notation for this set.[4]

§ 5. The rational integers[5]

The theory of numbers is at first concerned exclusively with the system of rational integers $0, \pm1, \pm2, \pm3, \ldots$, and it will be worthwhile to recall in a few words the important laws that govern this domain.[6] Above all, it should be recalled that these numbers are closed under addition, subtraction and multiplication, that is, the sum, difference and products of any two members in this domain also belong to the domain. The theory of *divisibility* considers the combination of numbers under multiplication. The number a is said to be divisible by the number b when $a = bc$, where c is also a [rational] integer. The number 0 is divisible by any number; the two units ±1 divide all numbers, and they are the only numbers that enjoy this property. If a is divisible by b, then $\pm a$ will also be divisible by $\pm b$, and consequently we can restrict ourselves to the consideration of positive numbers. Each positive number, different from unity, is either a *prime* number, that is, a number divisible only by itself and unity, or else a *composite* number. In the latter case we can always express it as a product of prime numbers and — which is the most important thing — in only one way. That is, the system of prime numbers occurring as factors in this product is completely determined by giving the number of times a designated prime number occurs as factor. This property depends essentially on the theorem that a prime divides a product of two factors only when it divides one of the factors.

The simplest way to prove these fundamental propositions of number theory is based on the algorithm taught by Euclid, which serves to find the greatest common divisor of two numbers.[7] This procedure as we know, is based on repeated application of the theorem that, for a positive number m, any number z can be expressed in the form $qm + r$, where q and r are also integers and r is *less* than m. It is for this reason that the procedure always halts after a finite number of divisions.[8]

---

[4] The now-standard notation $\mathbb{Z}$ for the set of integers comes from the German word *Zahlen*, which means 'number'.

[5] To set them apart from the project narrative, all original source excerpts are set in sans serif font and bracketed by the following symbol at their beginning and end:

[6] Notice that Dedekind used the word 'domain' here to refer to the system of rational integers together with its arithmetic operations; there is no connection here to the way we use the word 'domain' when talking about functions.

[7] Dedekind's footnote: See, for example, the *Vorlesungen über Zahlentheorie* of Dirichlet.

[8] As a reminder of how this process works, consider the following example in which we determine $\gcd(1386, 13090)$:

- Divide 13090 by 1386 to obtain: $13090 = 9(1386) + 616$ $(m_1 = 1386,\ q_1 = 9,\ r_1 = 616)$
- Divide 1386 by 616 to obtain: $1386 = 2(616) + 154$ $(m_2 = 616,\ q_2 = 2,\ r_2 = 154)$
- Divide 616 by 154 to obtain: $616 = 4(154)$ $(m_3 = 154,\ q_3 = 4,\ r_3 = 0)$

Since the last non-zero remainder is 154, we conclude that $\gcd(1386, 13090) = 154$.

As Dedekind noted, the ideas in this excerpt were well-known at least since the time of Euclid. Of particular importance in what follows are the theorems mentioned at the end of the first paragraph:

- *Unique Factorization*[9] Every (positive) rational integer has a unique factorization as a product of primes (up to the order of the factors).
- *Prime Divisibility of a Product*[10] A prime number divides a product of two rational integer factors only if it divides one of the two factors.

Dedekind's specific motivation for singling out these two important theorems in his paper was due to their connection to nineteenth century efforts to determine integer solutions of certain number-theoretic equations. A famous example is the equation in Fermat's Last Theorem, which asserts that $x^n + y^n = z^n$ has no non-trivial[11] integer solutions for $n \geq 3$. To their dismay, mathematicians found that certain approaches to proving this theorem for larger values of n that initially seemed quite promising were ultimately blocked by technical difficulties related to the Unique Factorization and Prime Divisibility Properties.[12] The work that we are reading in this project grew out of Dedekind's effort to remove those technical obstacles.

Another nineteenth century number theory problem related to these two theorems involved 'polynomial' congruence[13] equations of the form $x^m \equiv p \pmod{q}$, where p and q are odd primes and $x, m \in \mathbb{Z}^+$. An especially famous result of this type is the *quadratic reciprocity law* which describes a relation between the solvabilty of the equations $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$ for two different odd primes p, q. This difficult and beautiful result was first proven by Gauss in his important 1801 treatise on number theory, *Disquisitiones Arithmeticae*.[14] Gauss also looked for reciprocity laws for higher powers, eventually formulating a law for the 'biquadratic' case $[x^4 \equiv p \pmod{q}]$ by introducing a new set of 'integers.' These 'complex integers', also known as the 'Gaussian integers,' were described in our next excerpt from Dedekind.

§ 6. The complex integers of Gauss

The first and greatest step in the generalisation of these notions was made by Gauss, in his second memoir on biquadratic residues, when he transported them to the domain of complex integers $x + yi$, where x and y are any rational integers and i is $\sqrt{-1}$, that is, a root of the irreducible quadratic equation $i^2 + 1 = 0$. The numbers in this domain[15] are closed under addition, subtraction and multiplication, and consequently we can define divisibility for these numbers in the same way as for rational numbers. One can establish very simply, as Dirichlet

[9] The Unique Factorization Theorem is also often called the *Fundamental Theorem of Algebra*.

[10] The Prime Divisibility of a Product Theorem is also called *Euclid's Lemma*.

[11] Trivial integer solutions of the equation $x^n + y^n = z^n$ are those in which the value of one or more of the variables is zero, such as $(-1)^3 + (1)^3 = 0^3$, or $x^n + 0^n = x^n$ for any $x \in \mathbb{Z}$ and any $n \in \mathbb{N}$.

[12] For additional details about the connection of these theorems to Fermat's Last Theorem, see [Kleiner, 2009].

[13] Recall that for $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, we say that a, b are equivalent modulo m if and only if $m \mid (a - b)$. This implies that a and b have the same remainder when divided by m, and can thus be treated as equivalent as far as division by m is concerned. The theory of congruences was first systematically developed by Gauss, who also introduced the notation '$a \equiv b \pmod{m}$.'

[14] Gauss stated the quadratic reciprocity law for primes p, q as follows:

> If $q \equiv 1 \pmod{4}$, then $x^2 \equiv p \pmod{q}$ is solvable if and only if $x^2 \equiv q \pmod{p}$ is solvable.
> If $q \equiv 3 \pmod{4}$, then $x^2 \equiv p \pmod{q}$ is solvable if and only if $x^2 \equiv -q \pmod{p}$ is solvable.

[15] Recall from footnote number 6 that Dedekind used the word 'domain' to refer to a system of numbers under certain arithmetic operations.

showed in a very elegant manner,[16] that the general propositions on the composition of numbers from primes continue to hold in this new domain, as a result of the following remark. If we define the *norm* $N(w)$ of a number $w = u + vi$, where u and v are any rational numbers, to be the product $u^2 + v^2$ of the two conjugate numbers $u + vi$ and $u - vi$, then the norm of a product will be equal to the product of the norms of the factors, and it is also clear that for any given w we can choose a complex *integer* q such that $N(w - q) \leq 1/2$. If we now let z and m be any complex integers, with m nonzero, it follows by taking $w = z/m$ that we can put $z = qm + r$ where q and r are complex integers such that $N(r) < N(m)$. We can then find a greatest common divisor of any two complex integers by a finite number of divisions, exactly as for rational numbers, and the proofs of the general laws of divisibility for rational integers can be applied word for word in the domain of complex integers.

Using today's notation, we can denote and define the set of Gaussian complex integers by $\mathbb{Z}[i] = \{x+yi \,|\, x, y \in \mathbb{Z}\}$. Notice that without giving any detailed proofs, Dedekind described the *mathematical tool* that Dirichlet used to prove that the *Unique Factorization Theorem* and the *Prime Divisibility of a Product Theorem* hold in $\mathbb{Z}[i]$ — namely, the existence of a *norm* for complex integers which allows us to find the gcd of two complex integers via Euclid's Division Algorithm. This omission was intentional on Dedekind's part, since he wished to focus only on those properties of *divisibility* that were most relevant to the concept of an ideal that he was leading up to. We follow Dedekind's lead in this respect, pausing only briefly in our reading of his text to see how the norm of a complex integer is computed and used to find the greatest common divisor (gcd) of two complex integers within an adaptation of Euclid's Division Algorithm.

Task 1 This task explores the geometric meaning of the definition of the *norm* of a complex number $w = u + iv$, where $N(u + iv) = (u + iv)(u - iv) = u^2 + v^2$ for all $u, v \in \mathbb{R}$.

(a) Begin by plotting the following complex numbers in the imaginary plane.
Use the standard convention of plotting the real component on the horizontal axis and the imaginary component on the vertical axis.

(i) $w = 3 + 4i$ (ii) $x = -4 + 3i$ (iii) $x = -3 + 4i$
(iv) $x = 5 + 2i$ (v) $x = -8 + 6i$ (vi) $x = -2.7 + 4.6i$

(b) Now compute the norm of each of the complex numbers in part (a).
Describe how the norm of each number relates to their geometric placement.

(c) Geometrically, how can we describe the set of complex numbers q for which $N(q) = 1$?

Task 2 This task includes some computations and a proof related to Dedekind's claims concerning the the norm of a complex number in the previous excerpt.

(a) Show that the norm of the product of two complex numbers w, q is the product of their norms; that is, for all $w, q \in \mathbb{C}$, $N(wq) = N(w)N(q)$.

(b) For $q = 4.7 + 3.2i$, show that the complex *integer* $w = 5 + 3i$ is such that $N(w - q) \leq 1/2$.

(c) For $q = -1.2 + 2.56i$, find a complex *integer* w such that $N(w - q) \leq 1/2$.

(d) Given an arbitrary $w = u + vi$ with u, v rational, describe in general how to find a complex *integer* q such that $N(w - q) \leq 1/2$. Describe what this means geometrically.

[16] Dedekind's footnote: *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes* (Crelle's Journal, 24).

Let's now look at an example of how the Euclidean algorithm for computing the gcd of two natural numbers can be adapted to find the greatest common divisor of two complex integers.

Example In this example, we let $z = -8 + 51i$ and $m = -8 - i$ and find $\gcd(z, m)$.

- *Step 1* Since $N(z) = 2665 > 65 = N(m)$, we begin by dividing z by m; that is, we begin by finding complex *integers* $q_1, r_1 \in Z[i]$ such that $z = q_1 m + r_1$ and $N(r_1) < N(m)$. To estimate the quotient q_1, we use the complex conjugate of m in order to divide z by m:

$$\frac{z}{m} = \frac{-8+51i}{-8-i} = \frac{-8+51i}{-8-i} \cdot \frac{-8+i}{-8+i} = \frac{13-416i}{65} = \frac{13}{65} - \frac{416}{65}i$$

  Rounding the real and complex components of this quotient separately to the nearest rational *integer*, we obtain the *complex integer* $q_1 = 0 - 6i$.
  To obtain the corresponding remainder, we solve $z = q_1 m + r_1$ for r_1 to obtain:

$$r_1 = z - q_1 m = (-8 + 51i) - (-6i)(-8 - i) = -2 + 3i$$

  This concludes the first step of the process, giving us $\boxed{z = \underbrace{(-6i)}_{q_1} m + \underbrace{(-2+3i)}_{r_1}.}$

  Note that $N(r_1) = 13 < 65 = N(m)$.

- *Step 2* We next repeat this process, but now we divide the previous divisor m by the previous remainder r_1 in order to find complex *integers* $q_2, r_2 \in Z[i]$ with $m = q_2 r_1 + r_2$ and $N(r_2) < N(r_1)$:

$$\frac{m}{r_1} = \frac{-8-i}{-2+3i} = \frac{-8-i}{-2+3i} \cdot \frac{-2-3i}{-2-3i} = \frac{13+26i}{13} = 1 + 2i$$

  Since this quotient is already a complex integer, there is no need to round in this step; we simply take $q_2 = 1 + 2i$ and set $r_2 = 0$. Note that $N(r_2) = 0 < 13 = N(r_1)$.

Having arrived at a zero remainder,[17] we now conclude that the sought-after gcd is the final non-zero remainder r_1; that it, $\boxed{\gcd(z, m) = -2 + 3i}$.

To verify that $-2 + 3i$ is a common divisor in this example, we can 'unravel' the results of the two steps to obtain the following:

$$m = \underbrace{(1+2i)}_{q_2}\underbrace{(-2+3i)}_{r_1}$$

$$\begin{aligned} z &= \underbrace{(-6i)}_{q_1}\underbrace{(1+2i)\mathbf{(-2+3i)}}_{m} + \underbrace{\mathbf{(-2+3i)}}_{r_1} \\ &= [\,(-6i)(1+2i) + 1\,]\mathbf{(-2+3i)} \\ &= (13-6i)(-2+3i) \end{aligned}$$

This verifies that $-2 + 3i$ is indeed a common divisor[18] of m and z.

[17] Had we obtained a non-zero remainder in step 2, we would repeated the process until we reached a stage with a zero remainder. Note that we can be confident that this process will halt since the norms of these remainders form a decreasing sequence of non-negative rational integers.

[18] The verification that $-2 + 3i$ is a *greatest* of the common divisors of z and m is less relevant to the questions we are studying in this project, and thus is omitted.

But notice that we could also have written these factorizations as follows:

$$\begin{aligned} m &= (1+2i)(-2+3i) \\ &= (1)[(1+2i)(-2+3i)] \\ &= (-i^2)[(1+2i)(-2+3i)] \\ &= \underbrace{(2-i)}_{-i(1+2i)}\ \underbrace{(-3-2i)}_{i(-2+3i)} \end{aligned} \qquad \begin{aligned} z &= (13-6i)(-2+3i) \\ &= (1)[(13-6i)(-2+3i)] \\ &= (-i^2)[(13-6i)(-2+3i)] \\ &= \underbrace{(-6-13i)}_{-i(13-6i)}\ \underbrace{(-3-2i)}_{i(-2+3i)} \end{aligned}$$

Since $N(-3-2i) = 13 = N(-2+3i)$, note also that neither of the two complex integers $-3-2i$ and $-2+3i$ is 'bigger' than the other when we use their norms to compare them. In other words, we could just as well say that $\gcd(z, m) = -3-2i$. In fact, since $N(\pm(-2+3i)) = N(\pm i(-2+3i))$, there are four different complex integers that can be considered to be a gcd of z and m in this example! This may seem disquieting at first ... until we remember that a similar situation occurs within the set of rational integers. For instance, in the positive integers, we say that $\gcd(12, 15) = 3$, but since $12 = (-4)(-3)$ and $15 = (-5)(-3)$, it would make sense to also say that -3 is a "greatest common divisor" of 12 and 15. Of course, we typically avoid this issue with rational integers by limiting our attention to just positive integer factors. The situation with complex integers is more complicated simply because, once we know that $d = \gcd(a, b)$, there is no straightforward way to decide which of the four numbers $\pm d$, $\pm id$ should have 'priority' as *the* gcd[19]. This is because the four numbers 1, -1, i, $-i$ play a special role within the set of complex integers. Notice in the next excerpt how Dedekind incorporated this special feature of the complex integers into his definition of what it means for a complex integer to be 'prime.'

> There are four units ± 1, $\pm i$, that is, four numbers which divide all numbers, and whose norm is consequently 1. Every other nonzero number is either a composite number, so called when it is the product of two factors, neither of which is a unit, or else it is a prime, and such a number cannot divide a product unless it divides at least one of the factors. Every composite number can be expressed uniquely as a product of prime numbers, provided of course the four associated primes $\pm q$, $\pm qi$ are regarded as representatives of the same prime number q.

Task 3 In this task, you will prove Dedekind's claim that ± 1 and $\pm i$ are the only units in $\mathbb{Z}[i]$.

(a) Explain why $N(\omega) \in \mathbb{Z}^+$ for every non-zero $\omega \in \mathbb{Z}[i]$.

(b) Now use part (a) and the fact that "the norm of a product is the product of the norms" to complete the following proof.

> Assume $u \in \mathbb{Z}[i]$ is a unit; that is, assume u is a divisor of every complex integer.
> In particular u must be a divisor of 1.
> Use this to first show that $N(u) = 1$.
> Then use the definition of norm to show that $u = \pm 1$ or $u = \pm i$.
>
> *Note: If $u = \pm 1$ or $u = \pm i$, then clearly $N(u) = 1$.*
> *The last part of this task asks you to prove the converse of this fact!*

[19] In our example above, these four numbers are $d = -2+3i$, $-d = 2-3i$, $id = -3-2i$ and $-id = 3+2i$

Notice how Dedekind's definition of a prime within the set of complex integers $\mathbb{Z}[i]$ mirrors the definition of prime within the set of rational integers $\mathbb{Z}$. Intriguingly, numbers that are prime in the set $\mathbb{Z}$ may not be prime in the set $\mathbb{Z}[i]$. For example, it is possible to factor the number 2 within $\mathbb{Z}[i]$ as $2 = (1+i)(1-i)$; since neither $1+i$ nor $1-i$ is a unit in $\mathbb{Z}[i]$, the rational prime number 2 is thus *not* a prime complex integer!

On the other hand, the number 7 *is* a prime in $\mathbb{Z}[i]$. To see this, suppose that we factor 7 in $\mathbb{Z}[i]$ to obtain $7 = wq$ with $w, q \in \mathbb{Z}[i]$. Then $N(7) = N(wq) = N(w)N(q)$, where we also know that $N(7+0i) = 7^2 + 0^2 = 49$. This gives us $N(w)N(q) = 49$, where $N(w)$ and $N(q)$ are positive integers. If we now assume that both $N(w) \neq 1$ and $N(q) \neq 1$ (so that neither w or q is unit), it would have to be the case that $N(w) = N(q) = 7$. Setting $w = u + iv$ with $u, v \in \mathbb{Z}$, this would imply that $7 = N(w) = u^2 + v^2$. But a moment's reflection shows that the equation $7 = u^2 + v^2$ has *no* integer solutions! In other words, the only way to obtain $7 = wq$ with $w, q \in \mathbb{Z}[i]$ is to have either $N(w) = 1$ or $N(q) = 1$. This means that 7 is the product of two factors in $\mathbb{Z}[i]$ only if one of the factors (either w or q) is a unit, so that 7 is a prime number in the set of complex integers.

Task 4 This task examines ideas related to primes in the set of complex integers.
Recall from the previous excerpt that the norm of a product is the product of the norms.
Use this fact to complete each of the following.

(a) Show that the following are NOT prime in the set of complex integers:
(i) 5 (Hint? $5 = 1 + 4$) (ii) 13 (iii) $6 + 7i$

(b) Show that the following ARE prime in the set of complex integers:
(i) 3 (ii) $1 + i$ (iii) $10 + 9i$

As you worked the previous task, you may have noticed a pattern in terms of which rational prime numbers are also primes in the set of complex integers. In the next excerpt, Dedekind described precisely which complex integers are primes.

The set of all prime numbers q in the domain of complex integers consists of:

1. All the rational prime numbers (taken positively) of the form $4n + 3$;
2. The number $1 + i$, dividing the rational prime $2 = (1 + i)(1 - i) = -i(1 + i)^2$;
3. The factors $a + bi$ and $a - bi$ of each rational prime p of the form $4n + 1$ with norm $a^2 + b^2 = p$.

The existence of the primes $a \pm bi$ just mentioned, which follows immediately from the celebrated theorem of Fermat on the equation $p = a^2 + b^2$, and which likewise implies that theorem, can now be derived without the help of the theorem, with marvellous ease. It is a splendid example of the extraordinary power of the principles we have reached through generalisation of the notion of integer.

The 'celebrated theorem of Fermat' mentioned in Dedekind's justification for the third class of complex primes is a theorem in number theory that is known today as the *Two Square Theorem*:[20]

A prime p is the sum of two squares if and only if it is of the form $4n + 1$.

Notice that Dedekind's own interest in this number-theoretic result centered on how its connection to the complex integers demonstrates the power of generalization. In the next excerpt, Dedekind continued to pursue this notion of 'generality' by looking at other number systems of the form $\mathbb{Z}[\theta] = \{x + y\theta \,|\, x, y \in \mathbb{Z}\}$, but for values of $\theta \neq i$.

§ 7. The domain[21] of numbers $x + y\sqrt{-5}$

There are still other numerical domains which can be treated in absolutely the same manner. For example, let θ be any root of any of the five equations

$$\theta^2 + \theta + 1 = 0, \quad \theta^2 + \theta + 2 = 0,$$

$$\theta^2 + 2 = 0, \quad \theta^2 - 2 = 0, \quad \theta^2 - 3 = 0,$$

and let x, y be rational integers. Then the numbers $x + y\theta$ form a corresponding numerical domain. In each of these domains it is easy to see that one can find the greatest common divisor of two numbers by a finite number of divisions, so that one immediately has general laws of divisibility agreeing with those for rational numbers, even though there happen to be an infinite number of units in the last two examples.

Notice that Dedekind once more omitted any proof that it is always possible to 'find the greatest common divisor of two numbers by a finite number of divisions' within the five particular numerical domains $\mathbb{Z}[\theta]$ discussed in the previous excerpt, and instead simply stated that each of these sets can be treated 'in absolutely the same manner' as the set of complex integers $\mathbb{Z}[i]$. In fact, Dedekind had little interest in these 'well behaved' numerical systems, and mentioned them primarily to provide contrast for the much more interesting domain $\mathbb{Z}[\theta]$ of numbers $x + y\sqrt{-5}$. As we will soon see, this latter system turns out to be interesting precisely because *the general laws of divisibility do not hold in it!!* Furthermore, it was precisely this anomalous behavior of the domain $\mathbb{Z}[\sqrt{-5}]$ that provided the motivation for the concept of 'an ideal number,' which in turn motivated the concept of an 'ideal'. We thus forego commentary on the more tame numerical systems mentioned in the previous excerpt, and

[20] The number-theoretic problem of determining whether an integer is the sum of two squares, and in how many ways, dates back to the ancient Greek mathematician Diophantus (c. third century). In a posthumously published note of 1634, the French mathematician Albert Girard (1595-1632) observed that every prime of the form $4n + 1$ can be written as the sum of two squares. Pierre de Fermat (1601-1655) asserted this same claim (without proof) in a letter to Marin Mersenne (1588-1648) dated December 25, 1640, stating that 'every prime of the form $4n + 1$ is the hypotenuse of a right triangle in a single way.' For this reason, the theorem is sometimes called 'Fermat's Christmas Theorem.' Although Fermat claimed in his correspondence with Mersenne and others to also have a proof, the first published proof was due to Leonhard Euler (1707-1783) in 1755. This history is further described in [Dickson, 2005].

[21] Recall from footnote number 6 that Dedekind used the word 'domain' to refer to a system of numbers under certain arithmetic operations. Here and elsewhere, Dedekind denoted this particular number domain by '$\mathfrak{o}$.' In order to have consistent notation for this set in the primary source excerpts from Dedekind and in the project commentary on those excerpts, Dedekind's notation '$\mathfrak{o}$' has either been omitted or replaced by today's notation $\mathbb{Z}[\theta]$ throughout this section of the project. The author apologizes for this historical anachronism, which has been committed in the interest of greater clarity for the reader.

move directly to Dedekind's discussion of how the notion of 'ideal numbers' arises out of the intriguing behavior of $\mathbb{Z}[\sqrt{-5}]$. As we do so, we will pause at various points in our reading in order to work through some of the details omitted by Dedekind.

As you read through the remainder of this section, keep in mind that Dedekind began this discussion (in the first sentence of the excerpt below) by explicitly stipulating that θ is a root of the equation $\theta^2 + 5 = 0$; **throughout the rest of this section, we will thus set** $\theta = \sqrt{-5}$.

On the other hand, this method is not applicable to the domain of integers

$$\omega = x + y\theta$$

where θ is a root of the equation

$$\theta^2 + 5 = 0,$$

and x, y again take all rational integer values. Here we encounter the phenomenon which suggested to Kummer the creation of ideal numbers, and which we shall now describe in detail by means of examples.

The numbers ω of the domain we shall now be concerned with are closed under addition, subtraction and multiplication, and we therefore define the notions of divisibility ... of numbers exactly as before. Also, if we define the norm $N(\omega)$ of a number $\omega = x + y\theta$ to be the product $x^2 + 5y^2$ of the two conjugate number $x \pm y\theta$, then the norm of a product will be equal to the product of the norms of the factors. ..... If μ is a unit, and hence divides all numbers, then we must have $N(\mu) = 1$ and therefore $\mu = \pm 1$.

Before continuing with your reading of Dedekind, pause to look at the following task to make sure the details of the ideas presented in the previous excerpt are clear.

Task 5 This task examines ideas related to norms and units in the domain $\mathbb{Z}[\theta] = \{x + y\theta \,|\, x, y \in \mathbb{Z}\}$, where $\theta = \sqrt{-5}$.

(a) First verify Dedekind's claim that $\mathbb{Z}[\sqrt{-5}]$ is closed under addition, subtraction and multiplication. What is the additive identity of this set? What is the multiplicative identity of this set?

(b) Given $\omega \in \mathbb{Z}[\sqrt{-5}]$ with $\omega = x + y\theta$, $x, y \in \mathbb{Z}$, note that Dedekind's definition of the norm of ω is exactly analogous to the definition of norm for the complex integers:

$$N(\omega) = N(x + y\theta) = (x + y\theta)(x - y\theta) = x^2 - y^2\theta^2 = x^2 - y^2(\sqrt{-5})^2 = x^2 + 5y^2$$

Find the norm of each of the following elements of $\mathbb{Z}[\sqrt{-5}]$.
(i) $\omega_1 = 4 - 7\theta$ (ii) $\omega_2 = -3 + 2\theta$ (iii) $\omega_1\omega_2$
Then use these values to verify that $N(\omega_1\omega_2) = N(\omega_1)N(\omega_2)$ in this case.

(c) Verify Dedekind's claim that any unit $\mu \in \mathbb{Z}[\sqrt{-5}]$ satisfies $N(\mu) = 1$.
Then explain why this implies that $\mathbb{Z}[\sqrt{-5}]$ contains only two units, $\mu = \pm 1$.

Returning now to our reading of Dedekind, we will see how $\theta = \sqrt{-5}$ leads to strange new divisibility behavior in the domain $\mathbb{Z}[\theta]$.

A number (different from zero and ± 1) is called *decomposable* when it is the product of two factors, neither of which is a unit. In the contrary case the number is called *indecomposable*. Then it follows from the theorem on the norm that each decomposable number can be expressed as the product of a finite number of indecomposable factors. However, in infinitely many cases an entirely new phenomenon presents itself here, namely, the same number is susceptible to several, essentially different, representations of this kind. The simplest examples are the following. It is easy to convince oneself that each of the following numbers is indecomposable.

$$\begin{array}{llll} a=2, & b=3, & c=7; & \\ b_1=-2+\theta, & b_2=-2-\theta, & c_1=2+3\theta, & c_2=2-3\theta; \\ d_1=1+\theta, & d_2=1-\theta, & e_1=3+\theta, & e_2=3-\theta; \\ f_1=-1+2\theta, & f_2=-1-2\theta, & g_1=4+\theta, & g_2=4-\theta; \end{array}$$

In fact, for a rational prime p to be decomposable, and hence of the form $\omega\omega'$, it is necessary that $N(p)=p^2=N(\omega)N(\omega')$, and since ω, ω' are not units we must have $p=N(\omega)=N(\omega')$, that is, p must be representable by the binary quadratic form x^2+5y^2. But the three prime number 2, 3, 7 cannot be represented in this way, as one sees from the theory of these forms,[22] or else by a small number of direct trials. They are therefore indecomposable. It is easy to show the same thing similarly, for the other twelve numbers, whose norms are products of two of these three primes.

Notice that Dedekind's discussion of 'indecomposability' of the fifteen numbers in the list above is simply the first part of his description of the 'entirely new phenomenon' that occurs within $\mathbb{Z}[\sqrt{-5}]$. Before we continue to read further about this phenomenon, let's pause to consider this list of numbers and the definition of 'indecomposable' more carefully. The fact that the numbers 2, 3, 7 are indecomposable in $\mathbb{Z}[\sqrt{-5}]$ may seem at first glance to need no proof ... after all, each of these numbers is prime (and therefore indecomposable) within the set of rational integers $\mathbb{Z}$. But remember the situation with the complex integers $\mathbb{Z}[i]$, where 2 is *not* a prime number since $2=(1-i)(1+i)$, where neither of these factors is a unit in $\mathbb{Z}[i]$.

Dedekind's argument concerning the indecomposability of rational prime numbers (e.g., 2, 3, 7) in $\mathbb{Z}[\sqrt{-5}]$ is thus not simply belaboring the obvious ... a proof really is needed. Let's consider the details of that proof[23] for just one specific value, $a=2$. Arguing by contradiction, suppose that 2 is decomposable in $\mathbb{Z}[\theta]$. By definition of decomposable, this would give us non-units $\omega, \omega' \in \mathbb{Z}[\theta]$ such that $\omega\omega'=2$. Taking the norm, we then have $N(\omega\omega')=N(2)=N(2+0\theta)=2^2+5(0^2)=4$, which in turn implies that $N(\omega)N(\omega')=4$ (since the norm of the product is the product of the norms). Since neither ω nor $\omega'$is a unit, we also know that $N(\omega)\neq 1$ and $N(\omega')\neq 1$. The only way for this to occur (i.e., $N(\omega)N(\omega')=4$, $N(\omega)\neq 1$, $N(\omega')\neq 1$) would be if $N(\omega) = N(\omega')=2$. *(It's important to remember that the norm of a number in $\mathbb{Z}[\sqrt{-5}]$ is necessarily a non-negative rational integer ... do you see why?)* But this implies that there exist $x, y \in \mathbb{Z}$ such that $\omega = x+y\theta$ and $N(\omega)=x^2+5y^2=2$. However, this latter equation clearly has no integer solutions. Our conclusion? The rational prime number $a=2$ is indecomposable in the set $\mathbb{Z}[\sqrt{-5}]$.

[22] Dedekind's footnote: See Dirichlet's *Vorlesungen über Zahlentheorie,* § *71.*

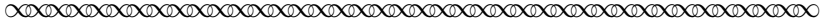
[23] You can check your understanding of the general proof simply by replacing '2' by 'p' (and $2^2=4$ by p^2), where p is an arbitrary prime, throughout this paragraph.

Task 6 This task establishes the indecomposability of two other numbers in $\mathbb{Z}[\theta]$, where $\theta = \sqrt{-5}$.

(a) Let $b_1 = -2 + \theta$. Assume that b_1 is decomposable in $\mathbb{Z}[\theta]$, so that $b_1 = \omega\omega'$ for some non-units $\omega, \omega' \in \mathbb{Z}[\theta]$. Use the fact that the product of norms is the norm of products, together with the fact that $N(x + iy) = x^2 + 5y^2$ for any $x + iy \in \mathbb{Z}[\theta]$, to derive a contradiction.

(b) Use a similar proof by contradiction to show that $e_2 = 3 - \theta$ is indecomposable in $\mathbb{Z}[\theta]$.

Let's now return to Dedekind's discussion of how the indecomposability of the fifteen numbers in the list leads to an 'entirely new phenomenon' with respect to divisibility within $\mathbb{Z}[\sqrt{-5}]$.



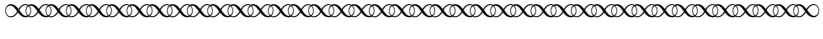
However, despite the indecomposability of these fifteen numbers, there are numerous relations between their products , which can all be deduced from the following.

$$(1) \qquad ab = d_1 d_2, \qquad b^2 = b_1 b_2, \qquad ab_1 = d_1^2$$

$$(2) \qquad ac = e_1 e_2, \qquad c^2 = c_1 c_2, \qquad ac_1 = e_1^2$$

$$(3) \qquad bc = f_1 f_2 = g_1 g_2, \quad af_1 = d_1 e_1, \quad ag_1 = d_1 e_2$$

In each of these ten relations, the same number is represented in two or three *different* ways as a product of indecomposable numbers. Thus one sees that an indecomposable number may very well divide a product without dividing any of its factors. Such an indecomposable number therefore does not possess the property which, in the theory of rational numbers, is characteristic of a *prime number*.



If you were wondering why Dedekind used the term 'indecomposable' (rather than the more familiar term 'prime') to describe a number that can not be factored except as the product of itself and a unit, his reason for having done so should now be clear! Remember the following theorem from Euclid on prime numbers:

Prime Divisibility of a Product: A prime number divides a product of two rational integer factors only when it divides one of the factors.

Yet each of the relationships in this last excerpt from Dedekind directly violates this theorem within $\mathbb{Z}[\sqrt{-5}]$! Take the first relationship on the list, for instance: $ab = d_1 d_2$. It is easy to verify that $ab = 6$ (since $a = 2$ and $b = 3$), and also that $d_1 d_2 = 6$ (since $d_1 = 1 + \sqrt{-5}$ and $d_2 = 1 - \sqrt{-5}$). But d_1 and d_2 are both indecomposable in $\mathbb{Z}[\sqrt{-5}]$, so that neither d_1 nor d_2 is divisible by 2 within this domain. We thus have a product $d_1 d_2$ which is divisible by the indecomposable number 2, and yet neither factor d_1 , d_2 of that product is divisible by 2. In other words, the number 2 does *not* satisfy our expectations concerning how prime numbers should behave, and therefore should *not* be called a prime number. Yet the number 2 *does* have the feature of having no factors other than itself and 1 (up to units), so that it makes sense to give it some special designation (i.e., 'indecomposable').

In the excerpt below, Dedekind further analyzed the fifteen indecomposable numbers that lead to this new phenomenon, with an eye towards trying to restore the *Prime Divisibility of a Product Theorem* to $\mathbb{Z}[\sqrt{-5}]$. Before reading this excerpt, check your understanding of the new phenomenon he has described by completing the following task.

Task 7 This task further examines the failure of the *Prime Divisibility of a Product Theorem* in $\mathbb{Z}[\sqrt{-5}]$.

Choose another of the equalities listed in (1), (2) and (3) of the previous excerpt (other than the equality $ab = d_1 d_2$), and verify the details of that equality. (For instance, if you choose the equality '$ag_2 = d_1 e_2$', explain why this equality holds.) Then explain how your chosen equality illustrates the fact that "an indecomposable number may very well divide a product without dividing any of its factors" within $\mathbb{Z}[\sqrt{-5}]$.

If we imagine for a moment that the fifteen preceding numbers are rational integers then, by the general laws of divisibility, we easily deduce from the relations (1) that there are decompositions of the form[24]

$$\begin{array}{lll} a = \mu\alpha^2, & d_1 = \mu\alpha\beta_1 & d_2 = \mu\alpha\beta_2 \\ b = \mu\beta_1\beta_2, & b_1 = \mu\beta_1^2 & b_2 = \mu\beta_2^2 \end{array}$$

and from the relations (2) that there are decompositions of the form

$$\begin{array}{lll} a = \mu'\alpha'^2, & e_1 = \mu'\alpha'\gamma_1 & e_2 = \mu'\alpha'\gamma_2 \\ c = \mu'\gamma_1\gamma_2, & c_1 = \mu'\gamma_1^2 & c_2 = \mu'\gamma_2^2 \end{array}$$

where all the Greek letters denote rational integers. And it follows immediately, by virtue of the equations $\mu\alpha^2 = \mu'\alpha'^2$, that the four numbers f_1, f_2, g_1, g_2 appearing in the rationals (3) will likewise be *integers*. These decompositions are simplified if we make the additional assumptions that a is prime to b and c, since this implies $\mu = \mu' = 1$, $\alpha = \alpha'$ and hence the fifteen numbers can be expressed as follows in terms of the five numbers α, β_1, β_2, γ_1, γ_2:

$$(4) \qquad \begin{cases} a = \alpha^2, & b = \beta_1\beta_2, & c = \gamma_1\gamma_2 & \\ b_1 = \beta_1^2, & b_2 = \beta_2^2, & c_1 = \gamma_1^2 & c_2 = \gamma_2^2 \\ d_1 = \alpha\beta_1, & d_2 = \alpha\beta_2, & e_1 = \alpha\gamma_1 & e_2 = \alpha\gamma_2 \\ f_1 = \beta_2\gamma_1, & f_2 = \beta_2\gamma_2, & g_1 = \beta_1\gamma_2 & g_2 = \beta_2\gamma_1 \end{cases}$$

Now even though our fifteen numbers are in reality indecomposable, the remarkable thing is that they behave, in all questions of divisibility in the domain $\mathbb{Z}[\theta]$, exactly as if they were composed, in the manner indicated above, of five different *prime numbers* α, β_1, β_2, γ_1, γ_2.

...

[24] Translator's footnote: Since these decompositions do not seem obvious to me, I include the following proof of the consequences of (1) as an example. Note first that $ab_1 = d_1^2$ and $b_1 b_2 = b^2$ are both squares. Suppose that

$$a = \mu\alpha^2, \;\; b_1 = \mu_1\beta_1^2, \;\; b_2 = \mu_2\beta_2^2,$$

where μ, μ_1, μ_2 are square free. Then $ab_1 = \mu\mu_1\alpha^2\beta_1^2$ is not a square unless $\mu = \mu_1$. Similarly, $b_1 b_2$ is not a square unless $\mu_1 = \mu_2$. Thus in fact $\mu = \mu_1 = \mu_2$ and hence

$$a = \mu\alpha^2, \;\; b_1 = \mu\beta_1^2, \;\; b_2 = \mu\beta_2^2.$$

Forming products of these, we get

$$d_1^2 = ab_1 = \mu^2\alpha^2\beta_1^2 \;\Rightarrow\; d_1 = \mu\alpha\beta_1,$$

$$d_2^2 = ab_2 = \mu^2\alpha^2\beta_2^2 \;\Rightarrow\; d_2 = \mu\alpha\beta_2,$$

$$b^2 = b_1 b_2 = \mu^2\beta_1^2\beta_2^2 \;\Rightarrow\; b = \mu\beta_1\beta_2,$$

which completes the proof of the decompositions claimed by Dedekind.

In the subsequent section of his paper, Dedekind went on to analyze the divisibility properties of the number 2 in the domain $\mathbb{Z}[\theta]$ and arrived at the conclusion that ... the number 2 behaves in our domain as though it were the square of the prime number α. He further commented that

> Although such a prime number α does not actually exist in the domain $\mathbb{Z}[\theta]$, it is by no means necessary to introduce it, since in fact Kummer managed in similar circumstances with great success by taking such a number α to be an *ideal* number, ...

Dedekind then demonstrated that this ideal number α *(as well as ideal numbers $\beta_1, \beta_2, \gamma_1, \gamma_2$ that appear in (4) above)* does indeed have the essential property of a prime; namely, if the product of two factors is divisible by α, then one of the factors must also be divisible by α. Rather than examine his analysis of this particular example further, we now turn to Dedekind's more general discussion of how he transformed this notion of an *ideal prime number*, initially used by Kummer in the context of number theory, into the considerably more general concept that plays a central role in the study of abstract algebra today: an *ideal*.

3 From *Ideal Numbers* to *Ideals*

Before looking at Dedekind's general definition of an ideal, we first look at some important background remarks from the introduction of his 1877 work.

> Kummer did not define ideal numbers themselves, but only the divisibility of these numbers. If a number α has a certain property A, ... he says that α is divisible by an ideal number corresponding to the property A. While this introduction of new numbers is entirely legitimate, it is nevertheless to be feared at first that the language which speaks of ideal numbers being determined by their products, presumably in analogy with the theory of rational numbers, may lead to hasty conclusions and incomplete proofs. And in fact this danger is not always completely avoided. On the other hand, a precise definition covering *all* the ideal numbers that may be introduced in a particular numerical domain $\mathfrak{o}$, and at the same time a general definition of their multiplication, seems all the more necessary since the ideal numbers do not actually exist in the numerical domain $\mathfrak{o}$. To satisfy these demands it will be necessary and sufficient to establish once and for all the common characteristic of the properties $A, B, C \ldots$ that serve to introduce the ideal numbers, and then to indicate how one can derive, from properties A, B corresponding to a particular ideal number, the property C corresponding to their product.

Notice Dedekind's emphasis in this last excerpt on the role played by general characterizations and precise definitions in avoiding the dangers of 'hasty conclusions and incomplete proofs'. As noted earlier in this project, both standards — generality and precision — were part of all his work. The next several excerpts provide a lovely description of how Dedekind approached the problem of attaining these standards within the context of the theory of ideals.

This problem is essentially simplified by the following considerations. Since a characteristic property A serves to define, not an ideal number itself, but only the divisibility of the numbers in $\mathfrak{o}$ by the ideal number, one is naturally led to consider the set $\mathfrak{a}$ of *all* numbers α of the domain $\mathfrak{o}$ which are divisible by a particular ideal number. I now call such a system an *ideal* for short, so that for each particular ideal number there corresponds a particular ideal $\mathfrak{a}$. Now if, conversely, the property A of divisibility of a number α by an ideal number is equivalent to the membership of α in the corresponding ideal $\mathfrak{a}$, one can consider, in place of the properties $A, B, C, \ldots$ defining the ideal numbers, the corresponding ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ in order to establish their common and exclusive character. Bearing in mind that these ideal numbers are introduced with no other goal than restoring the laws of divisibility in the numerical domain $\mathfrak{o}$ to complete conformity with the theory of rational numbers, it is evidently necessary that the numbers actually existing in $\mathfrak{o}$ and which are always present as factors of composite numbers, be regarded as a special case of ideal numbers. Thus if μ is a particular number of $\mathfrak{o}$, the system $\mathfrak{a}$ of all numbers $\alpha = \mu\omega$ in the domain $\mathfrak{o}$ divisible by μ likewise has the essential character of an ideal, and it will be called a *principal ideal*. ... Now, the notion of integer ... immediately yields the following two elementary theorems on divisibility:

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 $\omega - \omega'$ are themselves integers.
2. If $\alpha = \mu\omega$ is divisible by the μ, then 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.

If we apply these theorems, true for all integers, to the numbers ω of our numerical domain $\mathfrak{o}$, with μ denoting a particular one of these numbers and $\mathfrak{a}$ the corresponding principal ideal, we obtain the following two fundamental properties of such a numerical system $\mathfrak{a}$:

I. *The sum and difference of any two numbers in the system* $\mathfrak{a}$ *are always numbers in the same system* $\mathfrak{a}$.

II. *Any product of a number in the system* $\mathfrak{a}$ *by a number of the system* $\mathfrak{o}$ *is a number in the system* $\mathfrak{a}$.

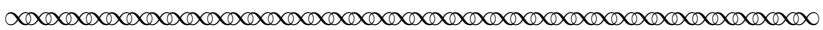
In Section 4 below, we will consider Dedekind's definition of a *principal ideal* from this last excerpt in more detail. For now, simply note that a 'principal ideal' is a particular set of numbers that Dedekind will use as a representative of an actual integer μ in the number domain $\mathfrak{o}$. Use this idea to complete the next task before continuing with your reading of Dedekind.

Task 8 Complete the following restatements of properties 1 and 2 for divisibility by the integer μ.

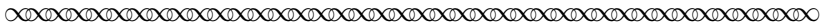
1. *The sum and difference of any two numbers that are divisible by* μ *are always* _____.
2. *The product of a number that is divisible by* μ *by any other number is always* _____.

Comment on how properties 1 and 2 for divisibility of integers, as re-stated here, relate to Dedekind's 'two fundamental properties' I and II for the principal ideal $\mathfrak{a}$ that corresponds to the number μ. How are these two pairs of properties the same? How are they different?

Up to this point, Dedekind has described the properties of only the special case of a principal ideal. In the continuation of the previous excerpt, we witness how he took the two fundamental properties that he distilled from this particular case, and generalized these properties to obtain a general definition that will also apply to sets of numbers that will represent the ideal numbers for the domain $\mathfrak{o}$ (or "non-principal ideals").



Now as we pursue the goal of restoring the laws of divisibility in the domain $\mathfrak{o}$ to complete conformity with those ruling the domain of rational integers, by introducing ideal numbers and a corresponding language, it is apparent that the definitions of these ideal numbers and their divisibility should be stated in such a way that the elementary theorems 1 and 2 above remain valid not only when the number μ is actual, but also when it is ideal. Consequently the properties I and II should hold not only for principal ideals but for *all* ideals. We have therefore found a common characteristic of all ideals: to each actual or ideal number there corresponds a unique ideal $\mathfrak{a}$, enjoying the properties I and II.



Here we see in its entirety the motivation behind Dedekind's definition of an ideal! Since ideal numbers are intended to restore the essential properties of integer divisibility within a system for integers that may be lacking those properties, and since ideals are *sets* of numbers that serve as representatives of the numbers — either actual or ideal — associated with that system, then an ideal must be a set of numbers that has properties (i.e., I and II) that exactly mimic the properties of integer divisibility (i.e., 1 and 2).

To obtain the level of abstraction and generality he sought, it was typical for Dedekind to define new concepts by treating *sets* of numbers as objects of study in their own right. In his celebrated work on the foundations of the real numbers, for example, he defined irrational numbers as sets of rational numbers (now known as "Dedekind cuts"), with arithmetic and order operations defined on the sets themselves. In this project, we will see how Dedekind defined an ideal to be a certain type of set on which one could operate algebraically. Although it is now commonplace to operate directly on sets of numbers in this way — or even on sets of sets of sets of sets of numbers! — Dedekind was among the first to successfully adopt this style.

Later in this project, we will examine some basic theorems about ideals that follow from Dedekind's formal definition of an ideal based on properties I and II. In the next section, we first introduce some terminology and examples related to the underlying algebraic structure in which an ideal is defined.

4 Number Fields, Rings and Integral Domains

Before we examine Dedekind's formal treatment of the theory of ideals, some comments concerning the underlying algebraic structure in which he situated this theory are in order. As is often the case with the original explorers of an algebraic concept, Dedekind developed his theory of ideals within a fairly concrete context: the set of complex numbers under their ordinary operations. Thus, when Dedekind talked about a *field* — a term that he was the first to use to describe this type of algebraic structure — he was always referring to a set A of complex numbers that satisfied certain algebraic properties. Dedekind himself described these properties simply as follows:

> I call a system A of numbers a (not all zero) a *field* when the sum, difference, product and quotient of any two numbers in A also belongs to A.

In other words, A must be closed under the four arithmetic operations (where division by 0 is implicitly excluded). But because Dedekind also assumed that elements of A were complex numbers under their ordinary operations, his definition implicitly included several additional algebraic properties, properties which are made explicit in today's definition of a *field*:

Definition 1
A set A with two binary operations $+$ and $\times$ is a *field* if and only if

1. A is an abelian group under $+$.
2. The set of non-zero elements of A is an abelian group under $\times$.
3. $\times$ is distributive over $+$.

In this definition, the term *group* refers to a set that is closed under an associative binary operation and satisfies both the Identity Property and the Inverse Property; in an *abelian group*, the operation is also commutative. By convention, the identity of an additive group is called 'zero' (denoted '0'), while the identity of a multiplicative group is called the 'unity' (denoted '1'). Listing these properties separately thus results in the following alternative (but lengthier!) definition of a field.

Definition $1'$
A set A with two binary operations $+$ and $\times$ is a *field* if and only if

1. A closed under $+$.
2. For all $a, b, c \in A$, $(a + b) + c = a + (b + c)$.
3. For all $a, b \in A$, $a + b = b + a$.
4. There exists an element $0 \in A$ such that for all $a \in A$, $a + 0 = a$.
5. For all $a \in A$, there exists an element $b \in A$ such that $a + b = 0$.
6. A closed under $\times$.
7. For all $a, b, c \in A$, $(ab)c = a(bc)$.
8. For all $a, b \in A$, $ab = ba$.
9. There exists an element $1 \in A$ such that for all $a \in A$, $a \times 1 = a$.
10. For all $a \in A$ with $a \neq 0$, there exists an element $c \in A$ such that $ac = 1$.
11. For all $a, b, c \in A$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

It is straightforward to prove that inverses in any group are unique, as is the identity element. The element specified by property 5 is called the *additive inverse of* a (or simply the *negative of* a), and denoted by $-a$. The element specified by property 10 is called the *multiplicative inverse of* a (or simply the *inverse of* a), and denoted by a^{-1}. The uniqueness of group inverses can be used to show that $(ab)^{-1} = b^{-1}a^{-1}$ for all elements a, b in a multiplicative group; translating this fact to additive notation, see obtain $-(a + b) = -b + -a$ for all elements a, b of an additive group.

In addition to explicitly specifying all the algebraic properties of a field (once the definition of 'abelian group' is unpacked!), notice that the modern definition of a field makes no assumptions about the nature of the elements of A itself. The following task illustrates how this more general definition allows for fields that do not satisfy Dedekind's more concrete notion of a (number) field.

Task 9 Decide which of the following are fields, and which are not.

Assume the standard addition and multiplication operations for each set in parts (a) — (d). In part (f), assume x is an arbitrary symbol and use standard polynomial addition and multiplication on the set $\mathbb{R}[x]$ of all polynomials in x with real-valued coefficients.[25]

(a) $\mathbb{Q}$

(b) $\mathbb{Z}$

(c) $\mathbb{R}$

(d) $\mathbb{Z}[i] = \{x + yi | x, y \in \mathbb{Z}\}$

(e) $\mathbb{Z}_5$ (under addition and multiplication modulo 5)

(f) $\mathbb{R}[x] = \left\{ a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \,\middle|\, a_i \in \mathbb{R} \text{ for } 0 \leq i \leq n,\ n \in \mathbb{Z}^+ \right\}$

Two of the fields in Task 9 are also 'fields' in Dedekind's more limited sense of the term, since the elements in those examples are complex numbers under ordinary arithmetic operations. *(Do you see which ones these are?)* Because Dedekind worked only with this more restricted type of of field, he was able to single out the set $\mathfrak{o}$ of all 'integers' within a field as an important algebraic substructure. As we have already seen, however, the 'integers' of a field A might not be just the 'rational integers'. Within the field $\mathbb{C}$ of all complex numbers, for instance, the set $\mathfrak{o}$ of 'integers' is the set $\mathbb{Z}[i]$ consisting of all elements of the form $x + yi$ where both x and y are integers (and $i = \sqrt{-1}$). Similarly, in the field A associated with the equation $\theta^2 + 5 = 0$, we saw that the set of integers is given by $\mathfrak{o} = \{x + y\sqrt{-5}\,|x, y \in \mathbb{Z}\}$.

What earns an element of a field the name 'integer' is thus not its actual value, but rather its membership in a particular subset of the field, where that subset satisfies certain special *algebraic* properties. Dedekind himself described the essential algebraic properties satisfied by the set $\mathfrak{o}$ of integers in a given field simply by stating that '$\mathfrak{o}$ is closed under addition, subtraction and multiplication'. Again, his particular context of a *number field* implied certain additional algebraic properties were also satisfied by the set $\mathfrak{o}$. Unlike the definition of field, the full collection of properties implicitly assumed by Dedekind about the set of integers in the field turns out to be significantly stronger than the collection of properties included in today's definition of the underlying algebraic structure in which ideal theory is developed. As you read the following definition for this structure — known today as a *ring* — pay particular attention to which properties implicitly assumed by Dedekind have since been dropped. (Some of these will be more obvious than others!)

Definition 2

A set A with two binary operations $+$ and $\times$ is a *ring* if and only if

1. A is an abelian group under $+$.
2. A is closed under $\times$.
3. $\times$ is associative.
4. $\times$ is distributive over $+$.

Task 10 This task examines how Dedekind's notion of a 'domain of integers' differs from today's 'ring'.

(a) Make an explicit list of all properties in the definition of ring, similar to that given in Definition $1'$ for a field. What properties were implicitly assumed to hold in a 'domain of integers' by Dedekind that are no longer used in today's definition of a 'ring'?

(b) Notice that neither Dedekind's definition of 'domain of integers' nor today's definition of 'ring' assumes the existence of multiplicative inverses. Use the standard arithmetic properties of the set of actual integers $\mathbb{Z}$ to explain why this is the case.

[25] Notice that$\mathbb{Z}[i]$ and $\mathbb{R}[x]$ use the same notation. In general, given a set B and an object $\clubsuit$ (either a number or an arbitrary symbol), we define $\mathcal{B}[\clubsuit] = \left\{ b_n\clubsuit^n + b_{n-1}\clubsuit^{n-1} + \ldots + b_1\clubsuit + \clubsuit_0 | \clubsuit_i \in B \text{ for } 0 \leq i \leq n,\ n \in \mathbb{Z}^+ \right\}$. Do you see why $\mathbb{Z}[i]$ does not need to mention any higher power of i?

A ring for which multiplication is also commutative is called a ***commutative ring***.[26] Because Dedekind himself worked only in the context of commutative rings, the remainder of this project focuses on this particular type of ring; as appropriate, comments on non-commutative ring properties are provided in footnotes[27]

Task 11 This task examines the definition of commutative ring by providing several examples and non-examples, and introduces terminology related to some special types of rings that are studied today.

(a) Verify that each of the following sets is a commutative ring under standard addition and multiplication.
Which of these are also fields? Justify your response.

(i) $\mathbb{Z}$ (ii) $\mathbb{Q}$ (iii) $\mathbb{R}$
(iv) $\mathbb{C}$ (v) $\mathbb{Z}[i] = \{x + yi | x, y \in \mathbb{Z}\}$ (vi) $\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} | x, y \in \mathbb{R}\}$
(Hint? $(x + y\sqrt{-5})(x - y\sqrt{-5}) = x^y + 5y^2$*)*

(b) Verify that each of the following sets is a commutative ring under the specified operations.
Which of these are also fields? Justify your response.

(i) $\mathbb{Z}_5$ under addition and multiplication modulo 5
(ii) $\mathbb{Z}_6$ under addition and multiplication modulo 6

(iii) $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$ under standard addition and multiplication
(iv) $2\mathbb{Z}_5 = \{2n | n \in \mathbb{Z}_5\}$ under addition and multiplication modulo 5
(v) $2\mathbb{Z}_6 = \{2n | n \in \mathbb{Z}_6\}$ under addition and multiplication modulo 6

(vi) $\mathbb{R}[x]$ under polynomial addition and multiplication (see footnote 22 for the definition of $\mathbb{R}[x]$)
(vii) $\mathbb{Z}[x]$ under polynomial addition and multiplication (see footnote 22 for the definition of $\mathbb{Z}[x]$)

(viii) $R_1 \times R_2 = \{(x, y) | x \in R_1, y \in R_2\}$, where R_1, R_2 are rings,
under componentwise addition and multiplication

(c) A ring that contains a multiplicative identity, or unity, is called a *ring with unity*.[28]
Identify which of the rings from parts (a) and (b) contain a unity, and which do not.
Hint? The ring $2\mathbb{Z}_6$ DOES include a unity ... what is it?

(d) An element a of a ring with unity that has a multiplicative inverse a^{-1} is said to be *invertible*.[29] Describe the invertible elements in the rings from parts (a) and (b).

(e) Use the terminology introduced above to complete the following to give a more concise definition of field:

Definition $1''$
A *field* is a _____ ring with _____ in which
all non-zero elements are _____.

[26] By definition of *ring*, addition in a ring is necessarily commutative. Thus, there is no need to assign a special name related to the commutativity of addition, but only to the commutativity of multiplication.

[27] As an optional task, you can verify that $M_{22} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$ is a non-commutative ring under matrix addition and multiplication.

[28] Recall that a ring always contains an additive identity, which is called the zero element and denoted 0.

[29] Recall that every element a of a ring has an additive inverse, which is called the negative of a and denoted $-a$.

Task 12 This task highlights some elementary properties of negatives and zero in a ring.

Assume A is a ring, so that A is an abelian group under addition.[30]
Use facts about group identities and inverses stated on page 17, together with relevant ring axioms, to prove each of the following holds for all $x, y \in A$.

(a) $x0 = 0$ (b) $x(-y) = -(xy)$ (c) $(-x)(-y) = xy$ (d) $-(x+y) = (-x) + (-y)$

Hints? For Part (a): $0 = 0 + 0$ For Part (b): Show that $x(-y) + xy = 0$; why is this helpful?

Task 13 This task looks at a property that implicitly held in Dedekind's special context of a number field, but which is today considered a defining characteristic of just one very special type of ring. The idea behind this property is based on the following familiar property of complex numbers:

Zero Factor Theorem for Complex Numbers
If a, b are complex numbers such that $ab = 0$, then either $a = 0$ or $b = 0$.

Given its ubiquitous nature within standard arithmetic, it is likely that you overlooked the fact that this property is *not* stipulated in today's definition of ring in completing Task 10a. However, several examples of rings in Task 11 include non-zero elements a, b with $ab = 0$. For example, in the ring $\mathbb{Z}_6$ under addition and multiplication modulo 6, the non-zero elements 2, 3 and 4 are such that $2 \times 3 = 0 = 4 \times 3$. Non-zero elements such as these are called *zero divisors* (or, alternatively, *divisors of zero*).

(a) For each of the following rings, identify all zero divisors, or argue that there are none. Assume the operation in each case is the natural one for the set in question.

(i) $\mathbb{Z}$ (ii)$2\mathbb{Z}$ (iii) $\mathbb{Z}[i] = \{x + yi | x, y \in \mathbb{Z}\}$
(iv) $\mathbb{Z}_5$ (v) $\mathbb{Z}_{12}$ (vi) $\mathbb{Z}_n$, where $n \in \mathbb{Z}^+$
(vii) $\mathbb{Z}_6 \times \mathbb{Z}_6$ (viii) $\mathbb{Z} \times \mathbb{Z}$ (ix) $R_1 \times R_2$, where R_1, R_2 are rings
(x) $\mathbb{Z}[x]$ (See footnote 22 for the definition.) (xi) $\mathbb{Z}_6[x]$ (See footnote 22 for the definition.)

(b) Today, there is a particular type of ring that restores the Zero Product Theorem back to our algebraic tool kit by excluding the possibility of zero divisors. Interestingly, the name of this special type of ring harkens back to Dedekind's work on 'domains of integers':

Definition 3
An *integral domain* is a commutative ring with unity containing no zero divisors.

The quintessential example of an integral domain is the set of rational integers $\mathbb{Z}$.
Identify which other rings in part (a) are integral domains, and which are not.
For each that is not, identify all properties of an integral domain that fail.

(c) Prove each of the following elementary theorems concerning integral domains.

(i) A ring A is an integral domain if and only if A satisfies the *cancellation property*:
For every $a, b, c \in A$, if $a \neq 0$ and $ab = ac$, then $b = c$.

(ii) All fields are integral domains.
Hint? First prove that an invertible element can not be a zero divisor;
that is, if a^{-1} exists, then a is not a zero divisor.

(iii) Not all integral domains are fields.

(d) Now prove the following theorems about zero divisors; notice how these particular properties suggest an analogy between 'zero' and a 'zero divisor'. Assume A is a ring.

(i) If $a, b \neq 0$ and ab is a zero divisor, then either a or b is a zero divisor.

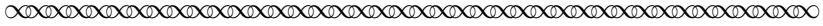
(ii) If A is commutative, $ab \neq 0$, and either a or b is a zero divisor,
then ab is a zero divisor.

[30] Note that we do not need to assume that A is a commutative ring for these properties to hold.

5 Dedekind's Elements of the Theory of Ideals

The previous sections of this project have set the stage for us to consider Dedekind's notion of ideals in a somewhat more general sense than even Dedekind himself did. Interestingly, it is possible to read large portions of Dedekind's description of this theory either within Dedekind's more restricted context (of integer domains within number fields), or within today's more abstract context (of any arbitrary ring). **Unless otherwise noted below, we will assume the more general context in which $\mathfrak{o}$ is an arbitrary commutative ring,** making mention of issues pertaining to non-commutative rings via footnotes along the way.

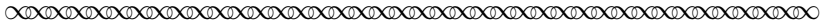
We now return to Dedekind's own words, making only minor changes where needed to adapt to this more general setting.[31] We begin with his formal definition of an ideal, based on the properties that he discussed in the excerpts we read in Section 3 of this project.



An *ideal* of this (ring) $\mathfrak{o}$ is a system $\mathfrak{a}$ of elements α in $\mathfrak{o}$ with the following two properties:

I. The sum and difference of any two elements in $\mathfrak{a}$ also belong to $\mathfrak{a}$;

II. The product $\alpha\omega$ of any element α in $\mathfrak{a}$ with an element ω in $\mathfrak{o}$ is an element in $\mathfrak{a}$.



Using modern symbolic notation, we re-state this definition of an ideal as follows:

Definition 4[32]
A non-empty subset $\mathfrak{a}$ of the ring $\mathfrak{o}$ is an *ideal* of $\mathfrak{o}$ if and only if

I. $(\forall \alpha, \alpha' \in \mathfrak{a})\,[(\alpha + \alpha' \in \mathfrak{a}) \wedge (\alpha - \alpha' \in \mathfrak{a})]$

II. $(\forall \alpha \in \mathfrak{a})(\forall \omega \in \mathfrak{o})(\alpha\omega \in \mathfrak{a})$

In modern terminology, note that Property I simply states that the set $\mathfrak{a}$ is closed under addition and subtraction. In Task 14, you will be asked to prove that this is equivalent to the assertion that $(\mathfrak{a}, +)$ is a subgroup of the the group $(\mathfrak{o}, +)$; in other words, $\mathfrak{a}$ is a non-empty subset of $\mathfrak{o}$ that is itself a group under the additive operation $+$ of the group $\mathfrak{o}$. This means that theorems pertaining to groups and subgroups will automatically transfer over to the relation between $\mathfrak{a}$ and $\mathfrak{o}$ when we restrict our attention to just the additive operation of the ring. Some of these 'transferred properties' are also explored in Task 14.

As you may have already noticed, however, Property II is much *stronger* than asserting that $\mathfrak{a}$ is closed under multiplication! This is because Property II asserts that if we begin with some α in the ideal $\mathfrak{a}$ and look at *all* the possible products $\alpha\omega$ for *every element ω in the entire ring* $\mathfrak{o}$, then all of these products[33] end up inside the ideal $\mathfrak{a}$ — regardless of whether ω comes from inside of $\mathfrak{a}$ or from outside of $\mathfrak{a}$. In contrast, checking that a set $\mathfrak{a}$ is 'closed under multiplication' requires us to consider the products $\alpha\omega$ only for elements ω that lie inside the set $\mathfrak{a}$ itself.

[31] In particular, the word 'number' has been replaced by 'element' throughout.

[32] In the case of a non-commutative ring, Condition II becomes: $(\forall \alpha \in \mathfrak{a})(\forall \omega \in \mathfrak{o})(\alpha\omega \in \mathfrak{a} \wedge \omega\alpha \in \mathfrak{a})$

[33] For a non-commutative ring, all the products $\omega\alpha$ also end up inside the ideal $\mathfrak{a}$.

Today, we say that a subset $\mathfrak{a}$ of a ring $\mathfrak{o}$ with the stronger property specified in II is a set that *absorbs products*. To see why the stronger 'product absorption' property was desired by Dedekind, you may find it helpful to look back at the discussion of the integer divisibility properties which Dedekind was trying to recapture with ideals (in section 3 of this project). Task 15 includes examples that illustrate the difference between 'absorption of products' and mere 'closure under products'. That task also introduces another type of substructure of rings — called a *subring* — that is based on the weaker property of 'closure under products'.

Task 14 This task examines how theorems from group theory can be transferred over to ring theory, using the additive structure of a ring. Assume that $\mathfrak{a}$ is a non-empty subset of the ring $\mathfrak{o}$.[34]

(a) Given a group G, recall that a non-empty subset H of G is a subgroup of G provided that H is a group in its own right under the operation of the given group G.
Also recall (from the definition of *ring*) that $(\mathfrak{o}, +)$ is an abelian group.
PROVE: If $\mathfrak{a}$ is closed under subtraction, then $(\mathfrak{a}, +)$ is a subgroup of $(\mathfrak{o}, +)$.

(b) Use part (a) to explain why the following gives an alternative definition of *ideal*.

> **Definition** $4'$
> A non-empty subset $\mathfrak{a}$ of the ring $\mathfrak{o}$ is an *ideal* of $\mathfrak{o}$ if and only if $\mathfrak{a}$ is an additive subgroup of $\mathfrak{o}$ that absorbs products.

(c) Suppose that $\mathfrak{a}$ is an ideal of the finite ring $\mathfrak{o}$. Explain why $|\mathfrak{a}|$ is a divisor of $|\mathfrak{o}|$.
Hint? Lagrange's Theorem for Finite Groups!

Task 15 This task defines the concept *subring* and explores how it differs from an ideal via examples.

(a) The concept of a *subring* is analogous to that of a subgroup (see Task 14a):

> **Definition** 5
> A non-empty subset $\mathfrak{a}$ of the ring $\mathfrak{o}$ is a *subring* if and only if $\mathfrak{a}$ is itself a ring under the operations of the given ring $\mathfrak{o}$.

Prove the following theorem regarding criteria for verifying that a given set $\mathfrak{a}$ is a subring of a given ring $\mathfrak{o}$:

> **Subring Criteria Theorem** A non-empty subset $\mathfrak{a}$ of a ring $\mathfrak{o}$ is a subring $\mathfrak{o}$ if and only if $\mathfrak{a}$ is closed under subtraction and products.

NOTE: To use this theorem in practice, notice that there are four criteria to check:
(1) $\mathfrak{a} \neq \emptyset$; (2) $\mathfrak{a} \subseteq \mathfrak{o}$; (3) $\mathfrak{a}$ is closed under subtraction; and (4) $\mathfrak{a}$ is closed under products.

(b) For each of the following non-empty subsets B of the ring $\mathbb{Z} \times \mathbb{Z}$, determine which are (i) subrings and (ii) ideals. Justify your responses.

1. $B = \{(n, n) \,|\, n \in \mathbb{Z}\}$
2. $B = \{(3n, 5m) \,|\, n, m \in \mathbb{Z}\}$
3. $B = \{(n, m) \,|\, n + m \text{ is even }, n, m \in \mathbb{Z}\}$
4. $B = \{(n, m) \,|\, nm \text{ is even }, n, m \in \mathbb{Z}\}$

(c) Give an example of a subring of $\mathbb{Z}_3 \times \mathbb{Z}_3$ that is not an ideal, or explain why this is not possible. Justify your response.

[34] Note that we do not need to assume that $\mathfrak{a}$ is a commutative ring for these theorems to hold.

Task 16 This task explores how properties of a subring may differ from those of the larger ring.

(a) Note that $A = \mathbb{Z}_{18}$ is a commutative ring with unity, but not an integral domain. Find subrings of the ring $A = \mathbb{Z}_{18}$ to illustrate that the following can occur:

(i) A is a ring with unity, D is a subring of A, but D is not a ring with unity. Note that this shows that a subring of ring with unity might not contain a unity.

(ii) A is a ring with unity, D is a subring of A, but the unity of D is not the same as the unity of A.

(b) Now consider the ring $B = \mathbb{Z}$, which is an integral domain but not a field. Find a subring of the ring $B = \mathbb{Z}$ to illustrate that the following can occur:

B is a ring with unity, D is a subring of B, but D is not a ring with unity.

(c) Next consider the polynomial ring $C = \mathbb{R}[x]$, which is an integral domain but not a field. Find a subring of the ring $C = \mathbb{R}[x]$ to illustrate that the following can occur:

C is not a field, D is a subring of C, and D is a field.

(d) Give an example to show that a subring of a field need not be a field.

(e) Is a subring of an integral domain always an integral domain? Prove or disprove.

Task 17 This task explores the elementary properties of ideals in rings with unity in order to identify all possible ideals for a field. Assume $\mathfrak{a}$ is an an ideal of the ring $\mathfrak{o}$, where $\mathfrak{o}$ has unity 1.

(a) Prove that if $1 \in \mathfrak{a}$, then $\mathfrak{a} = \mathfrak{o}$.

(b) Prove that if $\mathfrak{a}$ contains an invertible element of $\mathfrak{o}$, then $\mathfrak{a} = \mathfrak{o}$.

(c) Use the previous parts to prove that a field $\mathfrak{f}$ can have no nontrivial ideals; that is, $\mathfrak{f}$ has only two ideals, $\{0\}$ and the field $\mathfrak{f}$ itself.

Returning now to Dedekind's 1877 treatment of ideals, pay particular attention to Dedekind's definition of *principal ideal*.

We begin by mentioning an important special case of the concept of ideal. Let μ be a particular element [of the ring $\mathfrak{o}$]; then the system $\mathfrak{a}$ of all elements $\alpha = \mu\omega$ divisible by μ forms an ideal. We call such an ideal a *principal ideal* and denote it by $\mathfrak{o}(\mu)$, or more simply by $\mathfrak{o}\mu$ or $\mu\mathfrak{o}$. It is evident that this ideal will be unchanged when μ is replaced by an associate, that is, an element of the form $\epsilon\mu$, where ϵ is a unit.[35] If μ is itself a unit we have $\mathfrak{o}\mu = \mathfrak{o}$, since all elements in $\mathfrak{o}$ are divisible by μ. It is easy to see that no other ideal can contain a unit. Because if the unit ϵ is in the ideal $\mathfrak{a}$ then (by II) all products $\epsilon\omega$, and hence all elements ω in the principal ideal $\mathfrak{o}$ are in $\mathfrak{a}$. But since, by definition, all elements in the ideal $\mathfrak{a}$ are likewise in $\mathfrak{o}$, we have $\mathfrak{a} = \mathfrak{o}$. The ideal $\mathfrak{o}$ plays the same role among the ideals as the number 1 plays among the rational integers. The notion of principal ideal $\mathfrak{o}\mu$ also includes the singular case where $\mu = 0$, where the resulting ideal consists of the single element zero. However, we shall exclude this case from now on.

[35] Recall that a unit is an element of $\mathfrak{o}$ that divides every element of $\mathfrak{o}$.

In the case where $\mathfrak{o}$ is a commutative ring with unity (such as a field or an integral domain), Dedekind's definition of a *principal ideal* in the preceding excerpt remains in use today.[36] In this project, we will sometimes employ Dedekind's notation $\mu\mathfrak{o}$ for the principal ideal generated by the element μ; in fact, we have already used this notation in Section 3 (for instance, when we wrote $2\mathbb{Z}$ to denote the set of even integers), and Dedekind's notation is still convenient to use in some contexts. Within other contexts (including much of the remainder of this project), the following alternative notation for the principal ideal generated by the element μ is used today:

$$\langle \mu \rangle = \mu\mathfrak{o} = \{\mu\alpha \,|\, \alpha \in \mathfrak{o}\}.$$

As it turns out, there are certain rings for which every ideal is a principal ideal.[37] This fact was especially important for Dedekind's goal in this paper, as he explained in the continuation of the preceding excerpt:

> In the case . . . where our theory becomes the old theory of numbers, every ideal is evidently a principal ideal; . . . The same is true for the special quadratic fields considered in Chapter 2 (§6 and the beginning of §7). In all these cases, where every ideal of [the ring]. . . is a principal ideal, numbers are governed by the same laws that govern the theory of rational integers, because every indecomposable number also has the character of a *prime number* (see the Introduction and §7). 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 with the old theory of rational numbers, because without doubt it will help greatly in understanding our general theory.

Despite Dedekind's claims that it 'will follow easily from the results below', the proof that every indecomposable number 'also has the character of a *prime number*' in rings in which every ideal is a principal ideal goes well beyond the scope of this project. As an optional task, you might try your hand at something more straightforward and provide a proof that every ideal of the ring of complex integers $\mathbb{Z}[i] = \{x + yi \,|\, x, y \in \mathbb{Z}\}$ is a principal ideal. But first: complete the proofs requested in Task 18 for the theorems related to principal ideals that Dedekind stated in the two preceding excerpts, including the claim that every ideal of the ring $\mathbb{Z}$ is a principal ideal. Then provide a proof that non-principal ideals *can* exist in other rings by completing Task 19.

Task 18 In this task, you will supply the details of a modern proof for some of the theorems stated by Dedekind in the preceding excerpt.

Assume that $\mathfrak{o}$ is a commutative ring with unity 1 that contains more than one element and that μ, ϵ are non-zero elements of $\mathfrak{o}$. Using today's notation for principal ideals, further assume that $\langle \mu \rangle = \{\mu\omega \,|\, \omega \in \mathfrak{o}\}$. Write a complete proof for each of the following.

(a) $\langle \mu \rangle$ is an ideal of $\mathfrak{o}$.

(b) If ϵ is a unit of $\mathfrak{o}$, then $\langle \epsilon \rangle = \mathfrak{o}$.

(c) If $\mathfrak{o} = \mathbb{Z}$ and $\mathfrak{a}$ is an ideal of $\mathfrak{o}$, then $\mathfrak{a}$ is a principal ideal; that is, there exists $\mu \in \mathfrak{o}$ such that $\mathfrak{a} = \langle \mu \rangle$.

[36] For a non-commutative ring, algebraists typically distinguish between a principal left ideal and a principal right ideal — *do you see why?*

[37] An integral domain in which every ideal is a principal ideal is called a *principal ideal domain.*

Task 19 This task provides an example of a non-principal ideal in the polynomial ring $\mathbb{Z}[x]$.

Let $\mathfrak{a} = \{2p(x) + xq(x) \,|\, p(x), q(x) \in \mathbb{Z}[x]\}$.

(a) Show that $\mathfrak{a}$ is an ideal of the polynomial ring $\mathbb{Z}[x]$.
Note: We say that the set $\{2, x\}$ is a *Dedekind-basis* of the ideal $\mathfrak{a}$, or equivalently, that $\mathfrak{a}$ is the ideal generated by 2 and x. Adapting today's modern notation principal ideals to ideals with finite bases such as this, we can also write $\mathfrak{a} = \langle 2, x\rangle$.

(b) Show that $\mathfrak{a}$ is a *proper* ideal of $\mathbb{Z}[x]$ by showing that $1 \notin \mathfrak{a}$.

(c) Now show that $\mathfrak{a}$ is not a principal ideal. *Hint?* Use contradiction.

In the next excerpt, Dedekind discussed various ideas related to the *division of an ideal* by another *ideal*. These ideas are directly related to his overall goal of using ideals as a means to restore the essential properties of prime numbers to systems such as $\mathbb{Z}[\sqrt{-5}]$ (explored in section 2 of this project). In this project, we will instead explore these ideas primarily to consolidate our understanding of this new algebraic structure, but also to get a glimpse of how the process of abstraction proceeds in mathematics.

We say that an ideal $\mathfrak{m}$ is *divisible* by an ideal $\mathfrak{a}$, or that it is a *multiple* of $\mathfrak{a}$, when all the elements in $\mathfrak{m}$ are also in $\mathfrak{a}$. At the same time we say that $\mathfrak{a}$ is a divisor of $\mathfrak{m}$. According to this definition, each ideal is divisible by the ideal $\mathfrak{o}$. ...

. . . . . .

We finally remark that divisibility of the principal ideal $\mathfrak{o}\mu$ by the principal ideal $\mathfrak{o}\nu$ is completely equivalent to divisibility of the *number* μ by the *number* ν. The laws of divisibility of *numbers* in $\mathfrak{o}$ are therefore included in the laws of divisibility of *ideals*.

Notice that divisibility for ideals is defined simply in terms of the subset relation: $\mathfrak{a}$ divides $\mathfrak{m}$ if and only if $\mathfrak{m} \subseteq \mathfrak{a}$. This may seem reversed to you initially, so let's pause here for some examples related to this definition, before returning to our reading of Dedekind.

Task 20 This task examines the definitions in the preceding excerpt for the ring $\mathfrak{o} = \mathbb{Z}$.
Recall (from Task 18) that this particular commutative ring contains only principal ideals.

(a) Find all the ideals of $\mathbb{Z}$ that divide the ideal $\mathfrak{a} = \langle 8\rangle = \{8k | k \in \mathbb{Z}\}$.
Use the definition of divisibility for ideals to verify your answer.

(b) PROVE: For all $\mu, \alpha \in \mathbb{Z}$, α divides μ if and only if $\langle \mu\rangle \subseteq \langle \alpha\rangle$.

(c) Find all the non-trivial ideals of $\mathbb{Z}$ that divide both $\mathfrak{a} = \langle 8\rangle$ and $\mathfrak{b} = \langle 20\rangle$.

(d) Find at least three different ideals of $\mathbb{Z}$ that are divisible by both $\mathfrak{a} = \langle 8\rangle$ and $\mathfrak{b} = \langle 5\rangle$.

(e) Find at least three different ideals of $\mathbb{Z}$ that are divisible by both $\mathfrak{a} = \langle 8\rangle$ and $\mathfrak{b} = \langle 20\rangle$.

(f) Based on the above examples, how would you define the following?

* The *least common multiple* of the ideals $\mathfrak{a}$, $\mathfrak{b}$.
* The *greatest common divisor* of the ideals $\mathfrak{a}$, $\mathfrak{b}$.

As suggested by the previous task, the concepts of least common multiple and greatest common divisor can now be extended to ideals in a natural way. Dedekind's own definitions of these two notions were as follows:

> The set $\mathfrak{m}$ of all that elements that belong to both [$\mathfrak{a}$ and $\mathfrak{b}$] ... is called the *least common multiple* of $\mathfrak{a}$ and $\mathfrak{b}$.
>
> .....
>
> If α becomes equal in succession to all the elements in the [ideal] $\mathfrak{a}$, and β to all the elements in the [ideal] $\mathfrak{b}$, then the system $\mathfrak{d}$ of all elements $\alpha + \beta$ is ... called the *greatest common divisor* of $\mathfrak{a}$ and $\mathfrak{b}$ ...

Notice that Dedekind's clear statements of the defining properties of the sets $\mathfrak{m}$ and $\mathfrak{d}$ can be captured in modern set notation simply as follows:

$$\begin{array}{rcl} \mathfrak{m} & = & \{\gamma \,|\, \gamma \in \mathfrak{a} \wedge \gamma \in \mathfrak{b}\} \quad = \quad \mathfrak{a} \cap \mathfrak{b} \\ \mathfrak{d} & = & \{\alpha + \beta \,|\, \alpha \in \mathfrak{a} \wedge \beta \in \mathfrak{b}\} \end{array}$$

Dedekind's own statement of these two definitions are taken from the first chapter of his 1877 text. In that chapter, he began by first setting out the properties of an algebraic structure $\mathfrak{a}$ that is closed simply under addition and subtraction. This strategy of exposition then allowed him to simply reference results pertaining to additive properties as they were needed later in his text for the development of the theory of ideals, much as this project has done by referencing certain facts from elementary theory of groups.[38]

As the careful mathematician that he was, Dedekind naturally did more than simply define the two sets $\mathfrak{m}$ and $\mathfrak{d}$; he also provided proofs to show that they are, in fact, ideals. We examine these proofs, which serve as nice models of how to demonstrate a given set is an ideal, in the next two excerpts from Dedekind. The first of these two excerpts gives his proofs (taken from Chapter 1 of his text) of closure under addition and subtraction, along with his proofs that $\mathfrak{m}$ and $\mathfrak{d}$ satisfy the definitions of 'least common multiple' and 'greatest common divisor' respectively. For the convenience of the reader, the definitions of these sets are re-stated in this excerpt, and some minor changes in Dedekind's language have been made.[39] Throughout the next two excerpts from Dedekind, assume that $\mathfrak{a}$ and $\mathfrak{b}$ both are ideals of the commutative ring $\mathfrak{o}$.

---

[38] Because he was only interested in algebraic structures imposed on subsets of the complex numbers, Dedekind provided these less complicated structures with their own special name, calling them *modules*. At the end of his chapter on modules, however, he included the following remarks:

> The researches in this first chapter have been expounded in a special form suited to our goal, but it is clear that they do not cease to be true when the (Greek) letters denote not only numbers, but any objects of study, any two of which α, β produce a determined third element $\gamma = \alpha + \beta$ of the same type, under a commutative and uniformly invertible operation (composition), taking the place of addition. The module $\mathfrak{a}$ becomes a *group* of elements, the composites of which all belong to the same group.

The idea of a group of permutations was introduced by the French mathematician Évariste Galois (1811-1832), in his work on the unsolvability of polynomial equations of degree 5 or higher. In a collection of papers written in two periods (1812-1814 and 1844-1846), the algebraic properties of permutation groups were later developed independently of the theory of equations by Augustin Cauchy (1789-1857). Permutation groups then appeared as just one example of a much more general group concept in the 1854 paper *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$, written by British mathematician Arthur Cayley (1821-1895).

[39] In particular, the word 'number' is again replaced by the word 'element' throughout, and the word 'module' replaced either by the expression 'additive group' or the word 'ideal' as most appropriate.

The set $\mathfrak{m}$ of all the elements that belong to both [$\mathfrak{a}$ and $\mathfrak{b}$] will itself be an additive group. It will be called the *least common multiple* of $\mathfrak{a}$ and $\mathfrak{b}$ because each common multiple of $\mathfrak{a}$, $\mathfrak{b}$ is divisible by $\mathfrak{m}$.

Indeed, let μ, μ' be any two elements in the system $\mathfrak{m}$, and hence in both $\mathfrak{a}$ and $\mathfrak{b}$. Each of the two elements $\mu \pm \mu'$ will belong (by I) not only to the ideal $\mathfrak{a}$ but also to the ideal $\mathfrak{b}$, and hence also to the system $\mathfrak{m}$, whence it follows that $\mathfrak{m}$ is an additive group. Since all members of the additive group $\mathfrak{m}$ are in $\mathfrak{a}$ and also in $\mathfrak{b}$, $\mathfrak{m}$ is a common multiple of $\mathfrak{a}$, $\mathfrak{b}$. However, if the ideal $\mathfrak{m}'$ is any common multiple of $\mathfrak{a}$, $\mathfrak{b}$, then (by virtue of the definition of the system $\mathfrak{m}$) these elements will also be in $\mathfrak{m}$, that is, $\mathfrak{m}'$ is divisible by $\mathfrak{m}$.

If α becomes equal in succession to all the elements in the ideal $\mathfrak{a}$, and β to all the elements in the ideal $\mathfrak{b}$, then the system $\mathfrak{d}$ of all numbers $\alpha + \beta$ will form an ideal. This ideal is called the *greatest common divisor* of $\mathfrak{a}$ and $\mathfrak{b}$ because every common divisor of $\mathfrak{a}$, $\mathfrak{b}$ is also a divisor of $\mathfrak{d}$.

Indeed any two elements δ, δ' in the system $\mathfrak{d}$ can be put in the form $\delta = \alpha + \beta$, $\delta' = \alpha' + \beta'$ where α, α' belong to the ideal $\mathfrak{a}$ and β, β' to the ideal $\mathfrak{b}$, whence

$$\delta \pm \delta' = (\alpha \pm \alpha') + (\beta \pm \beta');$$

and, since the elements $\alpha \pm \alpha'$ are in $\mathfrak{a}$ and the elements $\beta \pm \beta'$ are in $\mathfrak{b}$, then elements $\delta \pm \delta'$ also belong to the system $\mathfrak{d}$. That is, $\mathfrak{d}$ is an additive group. Since the element zero is in every ideal, all the elements $\alpha = \alpha + 0$ of the ideal $\mathfrak{a}$ and all the elements $\beta = 0 + \beta$ of the ideal $\mathfrak{b}$ belong to the ideal $\mathfrak{d}$. Consequently, the latter is a common divisor of $\mathfrak{a}$ and $\mathfrak{b}$. Also, if the ideal $\mathfrak{d}'$ is any common divisor of $\mathfrak{a}$, $\mathfrak{b}$, so that all the elements in $\mathfrak{a}$ and all the elements in $\mathfrak{b}$ are in $\mathfrak{d}'$ then (by virtue of I) all the elements $\alpha + \beta$, that is, all the elements in the ideal $\mathfrak{d}$, also belong to the ideal $\mathfrak{d}'$. Thus, $\mathfrak{d}'$ is divisible by $\mathfrak{d}$.

Having thus established (in his chapter 1) that $\mathfrak{m}$ and $\mathfrak{d}$ are additive groups that satisfy the definitions of 'least common multiple' and 'greatest common divisor' respectively, Dedekind only needed to prove that these two sets absorb products in order to complete the proofs that both are ideals. He accomplished this in the following brief paragraph.[40]

Also, if $\mu = \alpha = \beta$ is an element in $\mathfrak{m}$ and hence also in $\mathfrak{a}$ and $\mathfrak{b}$, and if $\delta = \alpha' + \beta'$ is an element in the module $\mathfrak{d}$ then the product $\mu\omega = \alpha\omega = \beta\omega$ will likewise be in $\mathfrak{m}$ and the product $\delta\omega = \alpha'\omega + \beta'\omega$ will also be in $\mathfrak{d}$ since (by virtue of II) the products $\alpha\omega$, $\alpha'\omega$ are in $\mathfrak{a}$ and the products $\beta\omega$, $\beta'\omega$ are in $\mathfrak{b}$. Thus $\mathfrak{m}$ and $\mathfrak{d}$ enjoy all the properties of ideals.

[40] Although Dedekind himself assumed that he was working within a commutative structure, and thus needed only to check absorption by right-products, note how easily his argument that right-multiplication (by ω) gives products ($\mu\omega$ and $\mu\delta$) that are absorbed by the sets in question ($\mathfrak{m}$ and $\mathfrak{d}$ respectively) could be adapted to the case of left-multiplication by ω.

To get a better idea of how well Dedekind's argument in these two excerpts serves as a model for proving a given subset of a ring is an ideal, let's pull out just the portion of these excerpts that pertain to showing the intersection of two ideals is an ideal. With some slight modifications to Dedekind's presentation to adapt his proof to the modern definitions and results we have looked at in this project, we obtain the following. As you read this revised proof, notice the (few) additional details that have been added to fully address the definition of ideal in its modern form.

> *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be any two ideals of the commutative*[41] *ring* $\mathfrak{o}$.
>
> *We show that the set* $\mathfrak{m}$ *of all the elements that belong to both* $\mathfrak{a}$ *and* $\mathfrak{b}$ *will then itself be an ideal.*
>
> *Indeed, let* μ, μ' *be any two elements in the intersection* $\mathfrak{m}$, *and hence in both* $\mathfrak{a}$ *and* $\mathfrak{b}$. *The element* $\mu - \mu'$ *will belong (by I) not only to the ideal* $\mathfrak{a}$ *but also to the ideal* $\mathfrak{b}$, *and hence also to the intersection* $\mathfrak{m}$, *whence it follows that* $\mathfrak{m}$ *is closed under subtraction and, therefore, an additive subgroup.*
>
> *Also, if* μ *is an element in* $\mathfrak{m}$, *and hence also in* $\mathfrak{a}$ *and* $\mathfrak{b}$, *then given any element* $\omega \in \mathfrak{o}$, *the product* $\mu\omega$ *will belong (by II) not only to the ideal* $\mathfrak{a}$ *but also to the ideal* $\mathfrak{b}$, *and hence also to the intersection* $\mathfrak{m}$. *Thus,* $\mathfrak{m}$ *absorbs products.*
>
> *Note also that* $\mathfrak{m}$ *is non-empty since* $0 \in \mathfrak{a}$ *and* $0 \in \mathfrak{b}$.
>
> *Thus* $\mathfrak{m}$ *enjoys all the properties of ideals.*

Task 21 This task provides some additional examples of how to form an ideal, along with practice in writing 'ideal' proofs. For each of the following, modify the format shown above (for the proof that the intersection of two ideals is an ideal) to provide a fully detailed proof.

(a) Let $\mathfrak{o}$ be a commutative ring and $\alpha \in \mathfrak{o}$, and define $A_\alpha = \{x \in \mathfrak{o} \mid \alpha x = 0\}$.
Prove that A_α is an ideal (called the *annihilator of* α).

(b) Let $\mathfrak{o}$ be a commutative ring, define $A = \{x \in \mathfrak{o} \mid (\forall \alpha \in \mathfrak{o})(\alpha x = 0)\}$.
Prove that A is an ideal (called the *annihilating ideal of* $\mathfrak{o}$).
Also prove that $A = \{0\}$ whenever $\mathfrak{o}$ is a ring with unity.

(c) Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in the commutative ring $\mathfrak{o}$, and let $\gamma \in \mathfrak{o}$.
Define $\mathfrak{c} = \{\gamma x + \alpha + \beta \mid \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}, x \in \mathfrak{o}\}$. Prove that $\mathfrak{c}$ is an ideal.

6 Maximal Ideals and Prime Divisibility of a Product

In the previous two sections of this project, we have studied ideals and the associated algebraic structure of a ring somewhat independently of Dedekind's motivation for introducing the ideal concept. In this section, we come back to his original motivation and consider the sense in which ideals serve to recover the essential properties of divisibility — such as the fact that a prime divides a product of two rational integer factors only if it divides one of the factors — to rings like $\mathbb{Z}[\sqrt{-5}]$ that fail to satisfy these properties.

To gain insight into how ideals help to accomplish this restoration, let's review what we know about ideals in a ring that *does* satisfy these two properties, like $\mathbb{Z}$. In particular, recall from Task 18 that *every* ideal of $\mathbb{Z}$ is a principal ideal. In other words, there is a natural correspondence between

[41] Again, the adaptation of this proof to non-commutative rings is straightforward.

the *elements of* $\mathbb{Z}$ and the *ideals of* $\mathbb{Z}$, with each integer ω corresponding to the principal ideal $\langle\omega\rangle$ that it generates, and vice versa.[42] Dedekind's definition of divisibility for ideals also implies that an ideal $\langle\nu\rangle$ divides the ideal $\langle\omega\rangle$ if and only if this same divisibility relationship holds between their generating integers ν and ω. These two facts ensure that Dedekind's definition of a 'prime ideal' in the following excerpt suffices to transfer properties like *Prime Divisibility of a Product*, which we know holds in the ring $\mathbb{Z}$, over to the collection of its ideals $\{\langle\omega\rangle \mid \omega \in \mathbb{Z}\}$.

An ideal $\mathfrak{p}$ is called *prime* when it is different from [the given ring] $\mathfrak{o}$ and divisible by no ideals other than $\mathfrak{o}$ and $\mathfrak{p}$.

Recalling that the entire ring $\mathfrak{o}$ plays a role with respect to divisibility of ideals that is analogous to the role played by the unity 1 within a ring, Dedekind's definition of a 'prime ideal' should sound exactly like the concept of a prime number as you have come to understand that concept from working with rational integers $\mathbb{Z}$. Although today's algebraists still study this type of structure, they now refer to the type of ideal that Dedekind defined above as a *maximal ideal* (rather than a prime ideal). They also still study a structure that is called a 'prime ideal', but define that type of ideal based on the property of *Prime Divisibility of a Product* — a property that Dedekind also studied, but which he took to be equivalent to the definition above. These differences in terminology and the classification of different types of ideals came about as the result of certain post-Dedekind developments in abstract ring theory that took place in the early 20^{th} century. Within the more concrete context of the particular type of ring that Dedekind himself studied (today called a 'Dedekind domain'), these two notions turn out to be equivalent; that is, within a Dedekind domain, an ideal is prime if and only if it is maximal. Although a proof of this fact (and even the modern definition of a Dedekind domain) goes beyond the scope of this project, in the concluding section of this project, we will see the current definition for the structure now called a prime ideal, and take a brief look at the relationship between maximal ideals and prime ideals in more general commutative rings.

With these observations in mind, **we will employ today's current terminology within this project**, sometimes augmented by a reminder of Dedekind's original terminology to remind us of his motivation. Recalling that an ideal $\mathfrak{a}$ is divisible by the ideal $\mathfrak{b}$ if and only if $\mathfrak{a} \subseteq \mathfrak{b}$, we thus restate the definition above as follows.

Definition 6
Let $\mathfrak{p}$ be an ideal of the ring $\mathfrak{o}$.
Then $\mathfrak{p}$ is a *maximal ideal* [also called a Dedekind-prime ideal in this project] if and only if

1. $\mathfrak{p} \neq \mathfrak{o}$; and
2. If $\mathfrak{b}$ is an ideal of $\mathfrak{o}$ such that $\mathfrak{p} \subseteq \mathfrak{b}$, then either $\mathfrak{b} = \mathfrak{p}$ or $\mathfrak{b} = \mathfrak{o}$.

As a first example, let's show that the ideal $\mathfrak{p} = \langle 2\rangle$ is a maximal ideal in the ring $\mathfrak{o} = \mathbb{Z}$. The first requirement ($\mathfrak{p} \neq \mathfrak{o}$) clearly holds, since $\mathfrak{p}$ contains no odd integers. For the second requirement, suppose that $\mathfrak{b}$ is an ideal of $\mathfrak{o}$ such that $\mathfrak{p} \subseteq \mathfrak{b}$. Our goal is to show that either $\mathfrak{b} = \mathfrak{p}$ or $\mathfrak{b} = \mathfrak{o}$. Let's suppose that $\mathfrak{b} \neq \mathfrak{p}$. In this case, $\mathfrak{b}$ must necessarily include an odd integer; that is, $2k + 1 \in \mathfrak{b}$ for some $k \in \mathbb{Z}$. Since $\mathfrak{p} = \langle 2\rangle$, we also know $2k \in \mathfrak{p}$. This means that $2k \in \mathfrak{b}$ as well (since $\mathfrak{p} \subseteq \mathfrak{b}$). Closure of $\mathfrak{b}$ under subtraction then gives us $1 = (2k + 1) - 2k \in \mathfrak{b}$. And once we know that $1 \in \mathfrak{b}$,

[42] Note that this correspondence is not one-to-one, since $\langle\omega\rangle = \langle -\omega\rangle$ for every integer ω.

absorption of products allow us to conclude that $\mathfrak{b} = \mathfrak{o}$. Thus, either $\mathfrak{b} = \mathfrak{p}$ or $\mathfrak{b} = \mathfrak{o}$, and we conclude that $\mathfrak{p} = \langle 2 \rangle$ is a maximal ideal in the ring $\mathfrak{o} = \mathbb{Z}$. (Or, using the alternative terminology we are using in this project, we can also say that $\mathfrak{p} = \langle 2 \rangle$ is a Dedekind-prime ideal in the ring $\mathfrak{o} = \mathbb{Z}$.) Since the integer 2 is itself a prime in the ring $\mathbb{Z}$, this example may have come as no surprise. In the next task, you will show that the maximal ideals of the ring $\mathbb{Z}$ are indeed precisely the principal ideals that are generated by a prime number.

Task 22 This task examines the maximal ideals of the ring $\mathbb{Z}$.

Let $m \in \mathbb{Z}$ and use the definition of maximal ideal above to prove the following:

$\langle m \rangle$ is a maximal ideal of the ring $\mathbb{Z}$ if and only if m is prime.

In light of the fact that we get no new divisibility relationships by talking about ideals within the ring $\mathbb{Z}$, you may be thinking that using ideals in place of integers to talk about concepts like divisibility and primes just complicates matters. If so, then you're right — there really is no good reason to transfer these concepts over from elements of $\mathbb{Z}$ to the corresponding principal ideals of $\mathbb{Z}$. In fact, as Dedekind asserted in a previous excerpt, in *any* case 'where every ideal of the ring is a principal ideal, numbers are governed by the same laws that govern the theory of rational integers. Thus, ideals really add nothing new to the study of divisibility relationships in the set of complex integers $\mathbb{Z}[i]$ either, since every ideal of that ring is also a principal ideal.

Importantly, Dedekind also noted the reason why this phenomenon occurs in such rings: '**because every indecomposable number [in such a ring] also has the character of a prime number**.' But not every ring has this property! As we saw in Section 2, the ring $\mathbb{Z}[\sqrt{-5}]$ includes indecomposable elements (e.g., $a = 2$, $d_1 = 1 + \theta$, $d_2 = 1 - \theta$, where $\theta = \sqrt{-5}$) that are *not* prime, as evidenced by the failure of the *Prime Divisibility of a Product* property for these elements: since $(1+\theta)(1-\theta) = 6$, we know $2|(1 + \theta)(1 - \theta)$, but $2 \nmid (1 + \theta)$ and $2 \nmid (1 - \theta)$ due to the indecomposability of these two factors. Again thinking back to the examples we saw in Section 3, this situation arises because the prime numbers that are needed to factor the indecomposable numbers are somehow missing from the ring — if we could somehow restore the missing prime factors of 2, $1 + \theta$ and $1 - \theta$ back to the ring, then these numbers would no longer be indecomposable, and the difficulty would be removed.

Given Dedekind's comments about rings in which every ideal is a principal ideal, the strange behavior we see in $\mathbb{Z}[\sqrt{-5}]$ must mean that the collection of all ideals of $\mathbb{Z}[\sqrt{-5}]$ includes *non-principal ideals that are also maximal*.[43] Because such ideals do *not* correspond to any existing element of the ring (because they are not principal ideals), shifting our attention to the collection of all ideals will thus give us 'new numbers' that can take the place of primes that are 'missing' from the ring itself. These new 'ideal numbers' are precisely what are needed to show that the *collection of all ideals of the ring* $\mathbb{Z}[\sqrt{-5}]$ *does satisfy the Prime Divisibility of a Product property* — even though the ring itself fails to satisfy the essential properties of division!

In the remainder of this section, we will illustrate this idea with a specific example of such an ideal (i.e., non-principal but maximal) in the ring $\mathbb{Z}[\sqrt{-5}]$. The next task establishes a property of principal ideals generated by indecomposable elements that will be useful for that example.

[43] Or, in the alternate terminology we are using in this project, there will be non-principal ideals in $\mathbb{Z}[\sqrt{-5}]$ that are also Dedekind-prime ideals.

Task 23 This task establishes a property of principal ideals generated by indecomposable elements.

Let $\mathfrak{o}$ be a commutative ring with unity and assume $\alpha \in \mathfrak{o}$ is indecomposable.[44]
Set $\mathfrak{a} = \langle \alpha \rangle$, and further assume that $\mathfrak{b}$ is an ideal of $\mathfrak{o}$ with $\mathfrak{a} \subset \mathfrak{b} \subset \mathfrak{o}$.
Prove that $\mathfrak{b}$ is not a principal ideal. (Task 18b will be useful.)

We now focus our attention on a particular example of a non-principal maximal in the ring $\mathbb{Z}[\sqrt{-5}]$ as an illustration of the idea that Prime Divisibility of a Product property can be restored by looking at the collection of all ideals of the ring $\mathbb{Z}[\sqrt{-5}]$. To this end, we introduce the following notation and definitions.

Definitions to be used for remainder of this section

- $\theta = \sqrt{-5}$ (so that $\theta^2 = -5$)
- $\mathfrak{a} = \langle 2 \rangle = \{2\omega \,|\, \omega \in \mathbb{Z}[\theta]\} = \{2(x + y\theta) \,|\, x, y \in \mathbb{Z}\}$
- $\mathfrak{p} = \{\mu \in \mathbb{Z}[\theta] \,|\, \mu^2 \in \mathfrak{a}\} = \{x + y\theta \,|\, x, y \in \mathbb{Z} \wedge (x + y\theta)^2 \in \langle 2 \rangle\}$

In Task 24, you will prove that $\mathfrak{p}$ is an ideal of $\mathbb{Z}[\theta]$. First, notice that $1 \notin \mathfrak{p}$ (since $1^2 = 1 \notin \mathfrak{a}$); thus, $\mathfrak{p}$ is a proper ideal of $\mathbb{Z}[\theta]$. (That is, $\mathfrak{p}$ is an ideal of $\mathbb{Z}[\theta]$ with $\mathfrak{p} \subset \mathbb{Z}[\theta]$.) Also notice that $\mathfrak{a} \subset \mathfrak{p}$. To verify this, we must check two things: $\mathfrak{a} \subseteq \mathfrak{p}$ and $\mathfrak{a} \neq \mathfrak{p}$. The fact that $\mathfrak{a} \subseteq \mathfrak{p}$ follows from the observation that the ideal $\mathfrak{a}$ absorbs products, so that for any $\mu \in \mathfrak{a}$, we have $\mu^2 = \mu\mu \in \mathfrak{a}$, which in turn implies that $\mu \in \mathfrak{p}$ by definition of $\mathfrak{p}$. To show that $\mathfrak{a} \neq \mathfrak{p}$, we only need to find an element of $\mathfrak{p}$ that lies outside of $\mathfrak{a}$; computing $(1 + \theta)^2 = (1 + \theta^2) + 2\theta = (1 - 5) + 2\theta = 2(-2 + \theta)$, we see that $(1 + \theta)^2 \in \mathfrak{a}$, which implies $1 + \theta \in \mathfrak{p}$, while $1 + \theta \notin \mathfrak{a}$. *(Do you see why $1 + \theta \notin \mathfrak{a}$?)* Combining the two facts established in this paragraph, we thus have $\mathfrak{a} \subset \mathfrak{p} \subset \mathbb{Z}[\theta]$.

Task 24 This task provides a proof that the set $\mathfrak{p}$ (defined above) is an ideal of $\mathbb{Z}[\theta]$, where $\theta = \sqrt{-5}$.

Towards this end, note that we have already proved that $\mathfrak{p}$ is a non-empty subset of $\mathbb{Z}[\theta]$. Complete the proof by proving that $\mathfrak{p}$ is closed under subtraction and absorbs products.

Let's now examine the other properties possessed by the ideal $\mathfrak{p}$. We begin by noting that $\mathfrak{p}$ is not a principal ideal; since 2 is indecomposable in $\mathbb{Z}[\theta]$, this follows simply from Task 23. *(Make sure you see why this is the case!)* We further claim that $\mathfrak{p}$ is a maximal (or Dedekind-prime) ideal. To prove this, note that we already know that the first requirement from the definition of maximal ideal is met; namely, $\mathfrak{p} \neq \mathbb{Z}[\theta]$. To verify that the second requirement is met, assume $\alpha, \beta \in \mathbb{Z}[\theta]$ are such that $\alpha\beta \in \mathfrak{p}$. We need to show that either $\alpha \in \mathfrak{p}$ or $\beta \in \mathfrak{p}$. To do so, some analysis of the form exhibited by elements of the ideal $\mathfrak{p}$ will be useful. The boxed text on the following page provides such an analysis.

[44] Recall that α is indecomposable if and only if α can not be factored except as the product of itself and a unit.

Analysis of the form exhibited by elements of the ideal $\mathfrak{p}$

First suppose $x + y\theta \in \mathfrak{p}$ with $x, y \in \mathbb{Z}[\theta]$.
Then $(x + y\theta)^2 \in \mathfrak{a}$, which can only occur if $(x + y\theta)^2$ has a factor of 2.
Since $(x + y\theta)^2 = (x^2 - 5y^2) + 2xy\theta$, we see that $x^2 - 5y^2$ must be even.
But $x^2 - 5y^2$ is even in only two cases: if x and y are both even, or if x and y are both odd.

Conversely, assume $x, y \in \mathbb{Z}$ have the same parity (i.e., both even or both odd).
Then $x^2-5y^2 = 2k$ for some $k \in \mathbb{Z}$, and $(x+y\theta)^2 = (x^2-5y^2)+2xy\theta = 2(k+xy\theta) \in \langle 2\rangle = \mathfrak{a}$.
This implies in turn that $x + y\theta \in \mathfrak{p}$.

In summary, $x + y\theta \in \mathfrak{p}$ if and only if the integers x, y have the same parity.

Let's now use this analysis to complete the proof that $\mathfrak{p}$ is a maximal ideal. Recall that we have assumed that $\alpha\beta \in \mathfrak{p}$, and wish to prove that either $\alpha \in \mathfrak{p}$ or $\beta \in \mathfrak{p}$. Let's take $x, y, u, v \in \mathbb{Z}$ such that $\alpha = x + y\theta$ and $\beta = u + v\theta$. Since $\alpha\beta \in \mathfrak{p}$, we must then have $\alpha^2\beta^2 = (\alpha\beta)^2 \in \mathfrak{a}$. That is, $(x + y\theta)^2(u + v\theta)^2 \in \mathfrak{a}$. Expanding and simplifying this expression, we get the following:

$$\begin{aligned}
(x + y\theta)^2(u + v\theta)^2 &= \big[(x^2 - 5y^2) + 2xy\theta\big]\big[(u^2 - 5v^2) + 2uv\theta\big] \\
&= \big[(x^2 - 5y^2)(u^2 - 5v^2) + (2xy\theta)(2uv\theta)\big] + \big[(x^2 - 5y^2)(2uv\theta) + (u^2 - 5v^2)(2xy\theta)\big] \\
&= \big[(x^2 - 5y^2)(u^2 - 5v^2) - 20xyuv\big] + 2\big[(x^2 - 5y^2)uv + (u^2 - 5v^2)xy\big]\theta
\end{aligned}$$

Note that the coefficient of θ in this number is clearly even, while its real part is even if and only if the product $(x^2-5y^2)(u^2-5v^2)$ is even. *(Convince yourself of this!)* We arrive thus at the conclusion that one of the factors of $(x^2 - 5y^2)(u^2 - 5v^2)$ must be even. Without loss of generality, suppose that the first factor $x^2 - 5y^2$ is even. This then implies that x, y have the same parity *(convince yourself of this!)*, so that $\alpha = x + y\theta \in \mathfrak{p}$, as we set out to prove. Hence, $\mathfrak{p}$ is a maximal ideal of $\mathbb{Z}[\theta]$ (but *not* a principal ideal).

To conclude this illustration of how the collection of ideals recovers the essential properties of divisibility that are missing from a ring like $\mathbb{Z}[\theta]$, we need one last excerpt from Dedekind.

§ 22. Multiplication of ideals

If α runs through all the elements in an ideal $\mathfrak{a}$ and β runs through those of an ideal $\mathfrak{b}$, then all the products of the form $\alpha\beta$, together with their sums, form an ideal $\mathfrak{c}$. These elements are in [the ring] $\mathfrak{o}$ and they are closed under additions; also under subtraction, because the elements $(-\alpha)$ are likewise in $\mathfrak{a}$. Finally, each product of an element $\sum \alpha\beta$ in $\mathfrak{c}$ by an element ω in $\mathfrak{o}$ also belongs to $\mathfrak{c}$, since each product $\alpha\omega$ again belongs to $\mathfrak{a}$. This ideal $\mathfrak{c}$ is called the *product* of the two *factors* $\mathfrak{a}$, $\mathfrak{b}$, and we denote it by $\mathfrak{ab}$.

In symbolic notation, the ideal just defined by Dedekind could be written as:

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} \alpha_i\beta_i \;\middle|\; n \in \mathbb{Z}^+ \wedge (\forall i \leq n)(\alpha_i \in \mathfrak{a} \wedge \beta_i \in \mathfrak{b}) \right\}$$

For the example that we are considering in this section, our purpose in looking at this definition is to illustrate how the maximal (or Dedekind-prime ideal) $\mathfrak{p}$ defined above for the ring $\mathbb{Z}[\theta]$ allows us to give a prime factorization of the principal ideal $\mathfrak{a} = 2\mathbb{Z}[\theta]$ that corresponds to the indecomposable (but non-prime) number $a = 2$. We do this by proving that $\mathfrak{p}^2 = \mathfrak{a}$.

Let's first recall and clarify the definitions that we will be using:

Definitions to be used for remainder of this section

- $\theta = \sqrt{-5}$ (so that $\theta^2 = -5$)
- $\mathfrak{a} = \langle 2 \rangle = \{2\omega \,|\, \omega \in \mathbb{Z}[\theta]\} = \{2(x + y\theta) \,|\, x, y \in \mathbb{Z}\}$
- $\mathfrak{p} = \{\mu \in \mathbb{Z}[\theta] \,|\, \mu^2 \in \mathfrak{a}\} = \{x + y\theta \,|\, x, y \in \mathbb{Z} \wedge (x + y\theta)^2 \in \langle 2 \rangle\}$
- $\mathfrak{p}^2 = \mathfrak{p}\mathfrak{p} = \left\{ \sum_{i=1}^{n} \alpha_i \beta_i \;\middle|\; n \in \mathbb{Z}^+ \wedge (\forall i \leq n)(\alpha_i, \beta_i \in \mathfrak{p}) \right\}$

Note that the elements of $\mathfrak{p}^2$ are finite sums of products of pairs of elements from $\mathfrak{p}$, where the factors in each product need not be equal. For instance, setting $\alpha_1 = 4$, $\beta_1 = 1 + \theta$, $\alpha_2 = 1 - \theta$ and $\beta_2 = 3 - \theta$ gives us four elements of the ideal $\mathfrak{p}$ *(do you see why these lie in* $\mathfrak{p}$*?)*, which means that $\alpha_1\beta_1 + \alpha_2\beta_2 \in \mathfrak{p}^2$. Computing the value of this element, we have:

$$\alpha_1\beta_1 + \alpha_2\beta_2 = 4(1 + \theta) + (1 - \theta)(3 - \theta) = [4 + 4\theta] + [(3 - 5) - 4\theta] = 2,$$

which implies that $2 \in \mathfrak{p}^2$. Notice also that since $2 \in \mathfrak{p}^2$, absorption of products allows us to conclude that every multiple of 2 also lies in $\mathfrak{p}^2$. In other words, the principal ideal generated by 2 is a *subset* of $\mathfrak{p}^2$, and we have just shown that $\mathfrak{a} \subseteq \mathfrak{p}^2$.

Having thus already accomplished half of the proof that $\mathfrak{p}^2 = \mathfrak{a}$, all that remains is to show that $\mathfrak{p}^2 \subseteq \mathfrak{a}$. Since this follows in a straightforward fashion by using cases based on the parity of both components of elements from $\mathfrak{p}^2$, the details are left for you check in the next task. Once this is complete, notice that we will have succeeded in factoring the principal ideal $\mathfrak{a}$ generated by the indecomposable number $a = 2$ as a product of maximal (or Dedekind-prime) ideals!

Task 25 This task outlines a proof that $\mathfrak{p}^2 \subseteq \mathfrak{a}$, thereby completing the proof that the maximal ideal $\mathfrak{p}$ provides us with the prime factorization of the principal ideal $\mathfrak{a}$ generated by the indecomposable number $a = 2$ in the ring $\mathbb{Z}[\theta]$.

Using the definitions introduced above:

(a) Let $x, y, u, v \in \mathbb{Z}$ and set $\alpha = x + y\theta$, $\beta = u + v\theta$. Assume $\alpha, \beta \in \mathfrak{p}$.
Use cases based on the parity of the pairs x, y and u, v to prove that $\alpha\beta \in \mathfrak{a}$.
NOTE: This can be done using the following three cases:

- x, y even and u, v even
- x, y even and u, v odd
- x, y odd and u, v odd

(b) Now use part (a) and the fact that ideals are closed under sums to explain why $\mathfrak{p}^2 \subseteq \mathfrak{a}$.

7 Conclusion

In the closing sections of his monograph, Dedekind stated (and proved) a number of important theorems about products of ideals, using the definition stated in the previous section of this project. We end this project by listing a few of these, and with one final project task. As you read the list below, remember that Dedekind is talking here about *ideals*, not numbers, so that statements about 'divisibility' refer to subset relationships, and the product $\mathfrak{ab}$ is the set of finite sums of pairs of elements from the ideals $\mathfrak{a}$ and $\mathfrak{b}$ — given this, the correspondence of these results to well-known facts about natural numbers seems truly remarkable!

- The product $\mathfrak{ab}$ is divisible by $\mathfrak{a}$ and $\mathfrak{b}$.
- If $\mathfrak{a}$ is divisible by $\mathfrak{a}'$ and $\mathfrak{b}$ is divisible by $\mathfrak{b}'$, then $\mathfrak{ab}$ is divisible by $\mathfrak{a}'\mathfrak{b}'$.
- If neither of the ideals $\mathfrak{a}$, $\mathfrak{b}$ is divisible by the prime ideal $\mathfrak{p}$, then the product $\mathfrak{ab}$ is also not divisible by $\mathfrak{p}$.

Notice that the third theorem in this list is the contrapositive form of the *Prime Divisibility of a Product* property, but here applied to ideals:

> If the product $\mathfrak{ab}$ is divisible by the prime ideal $\mathfrak{p}$, then one of the two ideals $\mathfrak{a}$, $\mathfrak{b}$ is also divisible by $\mathfrak{p}$.

With this result in hand, Dedekind thus fulfilled his promise to restore the familiar properties of prime numbers to the collection of mathematical tools available to nineteenth century number theorists, while also setting the stage for the increasingly general development of abstract algebra in the twentieth century.

As part of those twentieth century developments, the *Prime Divisibility of a Product* property itself became the property on which today's definition of a prime ideal is based. Making use of Dedekind's terminology, we can state that definition as follows:

> **Definition** 7
> Let $\mathfrak{p}$ be an ideal of the ring $\mathfrak{o}$. Then $\mathfrak{p}$ is a *prime ideal* if and only if
>
> 1. $\mathfrak{p} \neq \mathfrak{o}$; and
> 2. Given ideals $\mathfrak{a}$ and $\mathfrak{b}$ for which the product $\mathfrak{ab}$ is divisible by $\mathfrak{p}$, one of the two ideals $\mathfrak{a}$, $\mathfrak{b}$ is also divisible by $\mathfrak{p}$.

Recalling once more that the ideal $\mathfrak{a}$ is divisible by $\mathfrak{p}$ if and only if $\mathfrak{a}$ is a subset of $\mathfrak{p}$ then allows us to re-state this definition as follows:

> **Definition** 7′
> Let $\mathfrak{p}$ be an ideal of the ring $\mathfrak{o}$. Then $\mathfrak{p}$ is a *prime ideal* if and only if
>
> 1. $\mathfrak{p} \neq \mathfrak{o}$; and
> 2. Given ideals $\mathfrak{a}$ and $\mathfrak{b}$ for which $\mathfrak{ab} \subseteq \mathfrak{p}$, either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.

As noted in the previous section, it is possible to prove that an ideal is prime if and only if it is maximal with the particular type of ring that Dedekind himself studied (today called a Dedekind domain). We close this project with one final task that examines the relationship between these two types of ideals within the more general context of an arbitrary commutative ring with unity. As an illustration of how the process of abstraction that Dedekind initiated with his theory of ideals has grown into an ever more powerful set of tools for today's algebraist, the interested reader is also encouraged to find a proof of the main result of this final task within a current textbook, where ideals are used to define an even more abstract structure known as a 'quotient ring' that offers some surprising simplifications.

Task 26 This task examines the relationship between prime ideals and maximal ideals within an arbitrary commutative ring with unity.

(a) Explain why the second condition of Definition $7'$ can be replaced by following property:

For every $a, b \in \mathfrak{o}$ with $ab \in \mathfrak{p}$, either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

That is, show that condition 2 of Definition $7'$ holds if and only if the property stated above holds. NOTE: Algebraists today typically use this statement to replace condition 2 in Definition $7'$ of a prime ideal.

(b) Use definition 6, definition $7'$ and part a of this task to prove the following:

If $\mathfrak{o}$ is a commutative ring with unity,
then every maximal ideal is also a prime ideal.

Hint? Assume $\mathfrak{o}$ is a commutative ring with unity and $\mathfrak{m}$ is a maximal ideal of $\mathfrak{o}$; also let $a, b \in \mathfrak{o}$ be such that $ab \in \mathfrak{m}$ and $a \notin \mathfrak{m}$. Show that the set $\mathfrak{n} = \{ax + y \,|x \in \mathfrak{o}, y \in \mathfrak{m}\}$ is an ideal of $\mathfrak{o}$ that satisfies $\mathfrak{m} \subset \mathfrak{n} \subseteq \mathfrak{o}$. Then use the maximality of $\mathfrak{m}$, the definition of an ideal and the fact that $1 \in \mathfrak{o}$ to show that $b \in \mathfrak{m}$.

Side Note: The ideal $\mathfrak{n}$ is the smallest ring that contains both a and $\mathfrak{m}$;
in today's notation, we could also write $\langle a, \mathfrak{m}\rangle = \{ax + y \,|x \in \mathfrak{o}, y \in \mathfrak{m}\}$.

References

E. T. Bell. *Men of Mathematics.* Simon and Schuster, New York, 1937.

A. Cayley. On the theory of groups, as depending on the symbolic equation $\theta^n = 1$, Part I. *Philosophical Magazine*, 7:40–47, 1854. and in *The Collected Mathematical Papers of Arthur Cayley*, Cambridge: Cambridge University Press, Vol. 2 (1889), 123–130.

L. Corry. *Modern Algebra and the Rise of Mathematical Structures.* Birkhäuser, Basel, second revised edition, 2004.

R. Dedekind. *Stetigkeit und irrationale Zahlen (Essays on the Theory of Numbers).* F. Vieweg und Sohn, Braunschweig, 1888. English translation by Beman, The Open Court Publishing Company, Chicago, 1901.

R. Dedekind. *Theory of Algebraic Integers.* Cambridge University Press, Cambridge, 1966. English tranlation by J. Stillwell of *Sur la Théorie des Nombres Entiers Algébriques*, first published in 1877.

L. E. Dickson. *History of the Theory of Numbers, Volume II.* Dover, Mineola MN, 2005. First published in 1919.

H. M. Edwards. The genesis of ideal theory. *Archives for the History of the Exact Sciences*, 15:321–378, 1980.

I. Kleiner. The roots of commutative algebra in algebraic number theory. In M. Anderson, V. Katz, and R. Wilson, editors, *Who Gave you the Epsilson? & Other Tales of Mathematical History*, pages 299–308. Mathematical Association of America, Washington DC, 2009.

Notes to Instructors

This Primary Source Project (PSP) draws on the 1877 version of Dedekind's theory of ideals as a means to introduce students to the elementary theory of rings and ideals. Characteristics of Dedekind's work that make it an excellent vehicle for students in a first course on abstract algebra include his emphasis on abstraction, his continual quest for generality and his careful methodology. The 1877 version of his ideal theory (the third of four versions he developed in all) is an especially good choice for students to read, due to the care Dedekind devoted therein to motivating why ideals are of interest to mathematicians by way of examples from number theory that are readily accessible to students at this level.

No prior familiarity with ring theory is assumed. The project has also been successfully used with students who had not yet studied group theory. That said, some familiarity with elementary group theory can be useful in Sections 4 and 5. The decision to proceed in this way was based in part on Dedekind's own familiarity with this structure in his work on ideals. For those who have not yet studied group theory (or those who have forgotten it!), basic definitions and results about identities, inverses and subgroups are fully stated when they are first used within the PSP (with the minor exception of Lagrange's Theorem for Finite Groups which is needed for Task 13c).

The only number theory concepts required should be familiar to students from their K-12 experiences; namely, the definitions (within $\mathbb{Z}$) of *prime*, *composite*, *factor*, *multiple*, *divisor*, *least common multiple*, and *greatest common divisor*. Euclid's algorithm for finding the GCD of two natural numbers is used briefly in Section 2; the example provided in footnote 7 should suffice to illustrate this algorithm for the purposes of the PSP (even for students who have never seen it).

To reap the full mathematical benefits offered by this PSP, students should be required to read assigned sections in advance of any in-class discussion, or to work through reading excerpts together in small groups in class. The author's method of ensuring that advance reading takes place is to require student completion of daily "Reading Guides" based on the assigned reading for the next class meeting; see pages 37 — 38 for a sample guide. Reading Guides typically include "Classroom Preparation" exercises (drawn from the PSP Tasks) for students to complete prior to arriving in class; they may also include "Discussion Questions" that ask students only to read a given task and jot down some notes in preparation for class discussion. On occasion, tasks are also assigned as follow-up to a prior class discussion. In addition to supporting students' advance preparation efforts, these guides provide helpful feedback to the instructor about individual and whole class understanding of the material. The author's students receive credit for completion of each Reading Guide (with no penalty for errors in solutions).

With regard to PSP implementation, a combination of whole class discussions, small group work, student presentations and homework assignments drawn from the PSP tasks is recommended in order to take advantage of the variety of questions provided in the PSP. The section descriptions below include suggestions concerning instructional strategies that are especially well-suited to different parts of the PSP. For small group work on individual tasks, the author recommends providing students with a copy of the task (with space provided to complete each part thereof). LaTeX code of the entire PSP may be requested from author to facilitate preparation of such 'in-class task sheets'. The PSP itself can also be modified by instructors to better suit their goals for the course; in such cases, the author requests a copy of the modified PSP and an implementation report following class completion of the PSP.

The full PSP is divided into six sections of differing length, described in more detail below. The estimated number of class periods (based on a class length of 50 minutes) is given for each section. The actual number of class periods spent on each section naturally depends on the instructor's goals and on how the PSP is actually implemented with students. Estimates on the high end of the range assume most PSP work is completed by students working in small groups during class time.

- Section 1: Germ of the theory of ideals (2 – 3 class days)
  This section includes Dedekind's discussion of a specific integral domain that fails to satisfy certain expected number theoretic properties (e.g., a prime divisor of a product should divide one of the factors of that product), thereby setting the stage for his eventual introduction of the concept of an *ideal*. Instructors should clearly explain to students that this material is primarily intended to set the stage for the main concepts of the PSP, as there is some danger of students becoming overly caught up in the specific details of this example due to the novelty of the ideas in this section. At the same time, sufficient attention to these details is needed to allow students to understand the way in which Dedekind is working towards a generalization of well-known concept of a 'number'. For these reasons, having students work through most details in small groups during class time is recommended for this section, as is some whole class discussion to help students consolidate their understanding of these ideas.

- Section 2: From *Ideal Numbers* to *Ideals* (0.5 – 1 class days)
  This short section includes Dedekind's first presentation of the definition of an *ideal*, together with his explanation of its motivation in the divisibility relationship between two rational integers. This definition is studied in much greater detail in Section 4 of the PSP. This section could thus simply be assigned for students to complete outside of class (including Task 7), with minimal discussion of its content in class. This approach would not only provide students an opportunity to wrestle with Dedekind's definition of an ideal on their own at this preliminary stage, but could also provide the instructor with helpful feedback about their progress in coming to understand Dedekind's ideas.

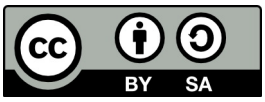
- Section 3: Number Fields, Rings and Integral Domains (3 – 4 days)
  This section temporarily sets aside Dedekind's writing about ideals, in order to introduce students to the general algebraic structures of a ring, integral domain and fields. This marks a departure from the historical story, since rings were first singled out as a separate structure only in Emmy Noether's later work. The decision to adopt this approach was made in large part because ideals are treated today as a substructure of a ring. This approach also allows the PSP to draw on students' familiarity with group theory as they examine a set of examples of various types of rings (including fields and integral domains) that will help to consolidate their understanding of an abstract ideal. Given the way in which this material builds on students prior knowledge of the group structure, group work is especially well-suited for many of the tasks in this section. There are also a number of proof exercises that instructors can choose to present as class examples, or to assign as pre- or post-reading assignments to students.

- Section 4: Dedekind's Elements of the Theory of Ideals (3 – 4 days)
  This section returns to a reading of Dedekind's discussion of ideals and their basic properties. Starting only with his formal definition, Tasks 13 – 15 prompt students to explore the basic concept of and elementary theorems about ideals (e.g., the difference between ideals and subrings, how properties of subrings and ideals may differ from the properties of the larger ring, properties of ideals in rings with unity). These particular tasks are well-suited for completion during class in small groups. The section then turns towards an exploration of Dedekind's study of principal ideals and divisibility relationships between ideals, and concludes with his (very modern!) proofs that the least common multiple and the greatest common divisor of two ideals are also ideals. The more formal proofs requested in the tasks in the later part of this section are well-suited as individual homework assignments for students.

- Section 5: Prime Ideals (1.5 –3 days)
  This section returns to Dedekind's original motivation for developing a theory of ideals, and considers the sense in which ideals serve to recover the essential properties of divisibility — such as the fact that a prime divides a product of two rational integer factors only if it divides one of the factors — for rings like $\mathbb{Z}[\sqrt{-5}]$ that fail to satisfy these properties. Using very select excerpts from Dedekind, this section contains a relatively large amount of narrative that seeks to support student understanding of a particular example of a prime ideal in $\mathbb{Z}[\sqrt{-5}]$ (chosen for its connection to an example encountered in the Dedekind excerpts from Section 1 of this PSP). Depending on the time available and/or instructor's objectives, students could be asked to work through this material together, with minimal whole group discussion. Alternatively, the instructor could pre-assign the reading, and then lead a whole class discussion that outlines the basic aspects of the example. In either case, the tasks interspersed within this section could be used as the basis for group work during class time, or assigned as individual out-of-class homework. They are also appropriate for student presentations.
- Section 6: Conclusion (0 – 1 days)
  This very short conclusion is intended simply to bring closure to the PSP, and contains only one new mathematical task. It could be assigned for students to read and complete outside of class, with little or no in-class discussion.

Acknowledgments

The development of this student project has been partially supported by the Transforming Instruction in Undergraduate Mathematics via Primary Historical Sources (TRIUMPHS) Program with funding from the National Science Foundation's Improving Undergraduate STEM Education (IUSE) Program under grant number 1523494. Any opinions, findings, and conclusions or recommendations expressed in this project are those of the author and do not necessarily represent the views of the National Science Foundation.



For more information about TRIUMPHS, visit `http://webpages.ursinus.edu/nscoville/TRIUMPHS.html`.

SAMPLE READING GUIDE

Background Information: This guide was assigned following a whole-class discussion of the definitions and examples of a field (drawn from Task 9), and a preliminary discussion of the definition and a (very) few examples of a ring. The goals of the reading and tasks assigned in this guide were to (a) prepare students for continued whole-class discussion of the definition and examples of different types of rings; and (b) assess their understanding of the concept of a 'zero divisor' based solely on their reading of the relevant sections of the PSP.

****

Reading Assignment - *Dedekind PSP* - pp. 16 – 19 (with some re-reading, some omissions)

1. Re-read pages 16 – 17 as appropriate for you.

   Any new questions or comments about fields or rings?

2. **Class Prep** Complete the modified version **Task 10, parts cdef** from page 18 on the reverse.

3. READ the introductory paragraph to Task 11 on page 19.

   - **Write down a definition for 'zero divisor' here**.

   - **Does the ring $\mathbb{Z}$ have any zero divisors? If so, what are they? If not, why not?**

   - **Does the ring $\mathbb{Z}_{12}$ have any zero divisors? If so, what are they? If not, why not?**

4. Also from Task 11 (page 19), READ part b (but don't complete it).

   - **Write down the definition of 'integral domain' here**.

   - *Any questions or comments about 'zero divisors' or 'integral domain' yet?*

CPR Task 10 (modified) This task examines the definition of ring by providing examples and non-examples, and introduces terminology for some special types of rings.

GIVEN: Each of the following is a ring, under the appropriate operations.
(*Even if we haven't verified this for all of them, take this as a given!)*

(i) $\mathbb{Q}$ (ii) $\mathbb{R}$ (iii) $\mathbb{Z}[i] = \{x + yi | x, y \in \mathbb{Z}\}$
(iv) $\mathbb{Z}$ (v) $\mathbb{Z}_5$ (vi) $\mathbb{Z}_6$
(vii) $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$ (vii) $2\mathbb{Z}_5 = \{2n | n \in \mathbb{Z}_5\}$ (ix) $2\mathbb{Z}_6 = \{2n | n \in \mathbb{Z}_6\}$
(x) $M_{22} = \{X | X \text{ is } 2 \times 2 \text{ matrix with } \det(X) \neq 0\}$
(xi) $\mathbb{Z}_5 \times \mathbb{Z}_5 = \{(x, y) | x \in \mathbb{Z}_5, y \in \mathbb{Z}_5\}$ (under componentwise addition and multiplication)

(c) A ring for which multiplication is also commutative is called a *commutative ring.*[45]
Identify which rings list above are commutative rings, and which are not.

Commutative	Non- commutative

(d) A ring that contains a multiplicative identity, or unity, is called a *ring with unity.*
Identify which of the rings listed above contains a unity, and indicate the unity in each. A starting point is given. *Hint?* The ring $2\mathbb{Z}_6$ DOES include *a* unity ... what is it?

Rings with unity	What is the unity?
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}$	1

(e) An element a of a ring with unity that has a multiplicative inverse a^{-1} is said to be *invertible.*
Describe the invertible elements in the rings listed above. A starting point is given.

Rings with unity	Invertible elements
$\mathbb{Q}$, $\mathbb{R}$	all non-zero elements (since these are fields)
$\mathbb{Z}$	± 1

(f) **Use the terminology introduced in parts (c) — (e) above to complete the following to give a more concise definition of field:**

Definition $1''$
A *field* is a _____ ring with _____ in which all non-zero elements are _____.

[45] By definition of *ring*, addition in a ring is necessarily commutative. Thus, there is no need to assign a special name related to the commutativity of addition, but only to the commutativity of multiplication. Similarly, in parts (d) and (e) of this task, there is no need to assign a special name related to additive identities or additive inverses, since every ring is necessarily an additive group.