Notes on Chapter 2 of Dedekind's *Theory of Algebraic Integers*

Jeremy Avigad

October 23, 2002

These notes are not a comprehensive summary of Chapter 2, but, rather, an overview of the main ideas.

1 Background

The ring $\mathbb{Z}$ consists of the integers of the field $\mathbb{Q}$, and Dedekind takes the theory of unique factorization in $\mathbb{Z}$ to be clear and well understood. The problem is that unique factorization can fail when one considers the integers in a finite extension of the rationals, $\mathbb{Q}(\alpha)$. Kummer showed that when $\mathbb{Q}(\alpha)$ is a cyclotomic extension (i.e. α is a primitive pth root of unity for a prime number p), one can restore unique factorization by introducing "ideal divisors." Dedekind's goal is both to improve Kummer's theory and to extend it to arbitrary $\mathbb{Q}(\alpha)$.

In Section 5, Dedekind summarizes the properties of the rational integers (i.e. $\mathbb{Z}$) that he would like to extend. In Section 6, Dedekind discusses the Gaussian integers, recalling in particular the notion of the *norm*, $N(\omega)$, of a Gaussian integer ω, and the role of the norm function in showing that $\mathbb{Z}[i]$ is a unique factorization domain.

2 Ideal divisors in $\mathfrak{o} = \mathbb{Z}[\sqrt{-5}]$

Let θ denote $\sqrt{-5}$, and consider $\mathbb{Q}(\theta)$. In Chapter 3 we will see that the integers of $\mathbb{Q}(\theta)$ are exactly the elements of $\mathbb{Z}[\theta]$, which Dedekind denotes $\mathfrak{o}$. For now, take this fact for granted, or simply think of $\mathfrak{o}$ as a ring of "generalized integers" that we would like to understand.

Notions of divisibility and irreducibility are now defined for $\mathfrak{o}$ just as for $\mathbb{Z}$. For example, *a divides b*, written $a|b$, if and only if there is a c such that $ac = b$. In contrast to $\mathbb{Z}$, however, unique factorization fails in $\mathfrak{o}$. For example:

$$\begin{aligned} 6 &= 2 \cdot 3 = (1+\theta)(1-\theta) \\ 9 &= 3 \cdot 3 = (2+\theta)(2-\theta) \\ 21 &= 3 \cdot 7 = (4+\theta)(4-\theta) = (1+2\theta)(1-2\theta). \end{aligned}$$

An easy calculation with norms shows that 2, 3, $1+\theta$, and so on can't be factored into products of non-units. So they are all irreducible but not prime: for example, 2 divides $(1+\theta)(1-\theta)$, but it divides neither $(1+\theta)$ nor $(1-\theta)$.

One way of describing the problem is to say that there aren't enough primes around: if $\mathfrak{o}$ lived inside a unique factorization domain, 2 would have to have at least two prime factors (possibly the same) which get split between $(1+\theta)$ and $(1-\theta)$. The goal is to develop a theory of "ideal divisors" that form such a unique factorization domain, and facilitate reasoning about the *original* domain, $\mathfrak{o}$.

Dedekind shows that with some mathematical detective work, one can infer facts about the behavior of the ideal divisors, i.e. one can determine properties that the collection of divisors *must have* if they are to form a unique factorization domain extending $\mathfrak{o}$. One way is to consider product identities like the ones above; I went through some of the calculations in Section 7 in class.

Another way is to reason directly about elements of $\mathfrak{o}$ in terms of their representations $a + b\theta$, with $a, b \in \mathbb{Z}$. In Section 8, Dedekind shows, for example, that 2 has the following property in $\mathfrak{o}$:

$$\text{if 2 divides } x^2y^2\text{, then 2 divides } x^2 \text{ or 2 divides } y^2$$

In any unique factorization domain, this would mean that 2 is either prime or the square of a prime. To see this, think about the factorization of 2 into primes: if 2 had two different prime factors, or if two were divisible by the cube of a prime, it would be possible to divide the factors of 2 between x and y to make the property above fail. Now, we know that 2 does not behave like a prime in $\mathfrak{o}$, so we conclude that if we were to embed $\mathfrak{o}$ in a suitable unique factorization domain of ideal divisors, 2 would have to be the square of a prime, α.

What more can we say about α? Rather than trying to *define* α, one can, as Kummer did, reason about α indirectly. More precisely, one can introduce the following definition:

Definition 2.1 *If ω is any element of $\mathfrak{o}$, ω* is divisible by *α if ω^2 is divisible by 2. More generally, if n is any natural number, ω* is divisible by *α^n if ω^2 is divisible by 2^n.*

Note that there is something unusual about this definition: one defines a property $P_\alpha(\omega)$, which, intuitively, corresponds to the assertion $\alpha|\omega$. But the two objects on either side of the divisibility symbol are not on equal footing: we haven't said what α "really" is. In other words, as it stands, α is an object we can only refer to via the divisibility relation. So, for example, if another divisor, β, is introduced the same way, it makes no sense, on the surface, to ask whether or not α divides β. We can introduce such a notion of divisibility for divisors by taking $\alpha|\beta$ to mean that for every ω in $\mathfrak{o}$, if $\beta|\omega$, then $\alpha|\omega$. But then we have to prove that this surrogate notion of divisibility has the properties we think it does.

To illustrate some of the subtleties involved, note that Dedekind proves the following

Theorem 2.2 *An element ω is divisible by α^2 if and only if ω is divisible by 2. More generally, ω is divisible by α^{2n} if and only if ω is divisible by 2^n.*

This theorem is clear from the intuition that "$2 = \alpha^2$," and, indeed, it isn't immediately clear how it differs from the definition above. But the fact that it is a separate theorem and *does* require proof shows that one has to be careful.

In Section 9, Dedekind goes on to analyze the behavior of 3 and 7, and their divisors, along similar lines. In Section 10, he gives a complete characterization of the behavior of primes in $\mathfrak{o}$ with respect to factorization into ideal elements. At this point, however, he announces his dissatisfaction with this general approach:

> ...to become completely certain that the general laws of divisibility governing the domain of rational numbers extend to our domain $\mathfrak{o}$ with the help of the ideal numbers we have introduced, it is necessary, as we shall soon see when we attempt a rigorous derivation, to make a very deep investigation.... We can indeed reach the proposed goal with all rigour; however, as we have remarked in the Introduction, the greatest circumspection is necessary to avoid being led to premature conclusions. In particular, the notion of a *product* of arbitrary factors, actual or ideal, cannot be exactly defined without going into minute detail. Because of these difficulties, it has seemed desirable to replace

the ideal number of Kummer, which is never defined in its own right, but only as a divisor of actual numbers ω in the domain $\mathfrak{o}$, by a *noun* for something which actually exists.... (page 94)

3 Towards the theory of ideals

Returning to the example of $\mathfrak{o}$, let α be the prime dividing 2, and let $\mathfrak{a}$ be the set $\{\omega \in \mathfrak{o} \mid \alpha | \omega\}$. It is not hard to show from the definition that this set has the following properties:

1. $\mathfrak{a}$ is closed under $+$

2. If η is any element of $\mathfrak{o}$ and ω is any element of $\mathfrak{a}$, $\eta\omega$ is in $\mathfrak{a}$.

In Dedekind's terminology, 1 says that $\mathfrak{a}$ is a submodule of $\mathfrak{o}$. 2 adds the extra information that multiplication by arbitrary elements of $\mathfrak{o}$ still keeps one in $\mathfrak{a}$. Any set satisfying 1 and 2 is called an *ideal*. In general, if β is any ideal divisor, the set of elements of $\mathfrak{o}$ divisible by β will have these properties (think about why this makes sense, under the intuitive notion of divisibility); so every ideal divisor gives rise to an ideal. In the Introduction, Dedekind reports that the converse also holds: every ideal corresponds to one of Kummer's ideal divisors.

This, then, is Dedekind's solution to the problem above: let the ideal $\mathfrak{a}$ *be* the divisor α. Say that an ideal $\mathfrak{a}$ *divides* an ideal $\mathfrak{b}$ if and only if $\mathfrak{a} \supseteq \mathfrak{b}$; remember that one way to make sense of this is to think of $\mathfrak{a}$ as being "finer" than $\mathfrak{b}$. On the surface, we have a typing problem, because we want to be have ideal divisors (now identified with ideals) dividing elements of $\mathfrak{o}$ (numbers). The solution is to identify each number η in $\mathfrak{o}$ with the principal ideal

$$\eta\mathfrak{o} = \{\eta\omega \mid \omega \in \mathfrak{o}\},$$

i.e. all the multiples of η in $\mathfrak{o}$. In particular, $\mathfrak{o}$ itself is the principal ideal corresponding to 1. Now it makes sense to talk about an ideal α dividing a number η in $\mathfrak{o}$, and we have the collection of divisors we need; the elements of $\mathfrak{o}$ are represented by principal ideals, whereas the truly "ideal" divisors are represented by the nonprincipal ones.

The sum of two ideals is defined by

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a} \text{ and } b \in \mathfrak{b}\}.$$

The product of two ideals is defined to be the ideal *generated* by products from $\mathfrak{a}$ and $\mathfrak{b}$, i.e.

$$\mathfrak{a} \cdot \mathfrak{b} = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a} \text{ and } b_i \in \mathfrak{b}\}.$$

You should check that these two are really ideals, i.e. satisfy 1 and 2 above.

At this point, however, a discrepancy between the theory of ideals and the theory if $\mathbb{Z}$ becomes apparent. With respect to ideals, we have said that $\mathfrak{a}|\mathfrak{b}$ means that $\mathfrak{a} \supseteq \mathfrak{b}$. But when it comes to numbers, $a|b$ means that there is some c such that $ac = b$. In fact, for ideals these two notions are equivalent:

Theorem 3.1 *If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals (in the ring of integers of a finite extension of $\mathbb{Q}$), then $\mathfrak{a} \supseteq \mathfrak{b}$ if and only if there is an ideal $\mathfrak{c}$ such that $\mathfrak{ac} = \mathfrak{b}$.*

Modern presentations take "$\mathfrak{a}$ divides $\mathfrak{b}$" to mean that $\mathfrak{ac} = \mathfrak{b}$ for some $\mathfrak{c}$, contrary to Dedekind's definition. With the modern terminology, the theorem above is summarized by the slogan: "to contain is to divide."

Proving the theorem, however, is the hard part, and really the linchpin of the whole theory. Once it is in place, unique factorization follows easily (see below). The rest of Chapter 2 is devoted to showing this fact (and hence, unique factorization) for $\mathfrak{o}$, via an explicit calculation. Chapters 3 and 4 are devoted to showing, in a conceptually clearer way, that the theorem is true for the ring of integers of any number field.

Jumping ahead, I will note here that Dedekind defines the *norm* of an ideal $\mathfrak{a}$, $N(\mathfrak{a})$, to be $(\mathfrak{o}, \mathfrak{a})$, where $\mathfrak{a}$ is viewed as a module in the last expression. Recall that from the discussion of Chapter 1, we can interpret $(\mathfrak{o}, \mathfrak{a})$ in a number of ways:

- It is the cardinality of the quotient module, $\mathfrak{o}/\mathfrak{a}$.
- If a basis of $\mathfrak{a}$ is obtained from from a basis for $\mathfrak{o}$ by applying a matrix M, then $(\mathfrak{o}, \mathfrak{a}) = |\det M|$.
- In particular, if M is lower triangular, $(\mathfrak{o}, \mathfrak{a})$ is just the absolute value of the product of the elements along the diagonal of M.
- Under the lattice interpretation of free modules and their submodules, $(\mathfrak{o}, \mathfrak{a})$ is the volume (or number of points in) the fundamental region of the lattice corresponding to $\mathfrak{a}$ (assuming the fundamental region of $\mathfrak{o}$ is given a volume of 1).

The notion of norm will be very important later on.

4 Ideals in $\mathfrak{o}$

What do ideals in $\mathfrak{o}$ look like? This is where considerations from Chapter 1 become useful: every ideal is, in particular, a module. The ring currently under study, $\mathfrak{o}$, is generated as a module by two elements, 1 and θ. Hence, as a submodule of the complex numbers, it can be written $[1, \theta]$. Now let $\mathfrak{a}$ be any submodule. As long as $[1, \theta]/\mathfrak{a}$ is finite (as it will be for any ideal), we know that $\mathfrak{a}$ will have a basis α_1, α_2 determined by a lower-triangular matrix:

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} k & 0 \\ l & m \end{pmatrix} \begin{pmatrix} 1 \\ \theta \end{pmatrix} = \begin{pmatrix} k \\ l + m\theta \end{pmatrix}.$$

In other words, $\mathfrak{a}$ is of the form $[k, l + m\theta]$.

But now suppose that $\mathfrak{a}$ is, additionally, an ideal. A little reflection shows that this amounts to the assertion that $\mathfrak{a}$ is closed under multiplication by θ. So, in particular, the elements

$$k\theta \quad \text{and} \quad (l + m\theta)\theta = -5m + l$$

are in $\mathfrak{a}$.

Keep in mind that if a, b, c, and d are all integers, and

$$a + b\theta = c + d\theta,$$

then $a = c$ and $b = d$. In other words, any equation between elements of $\mathfrak{o}$ determines two equations in $\mathbb{Z}$. We can now see why the representation of $\mathfrak{a}$ as $[k, l + m\theta]$ is useful. First, $k\theta$ is to be written as a linear combination of k and $l + m\theta$, then equating the coefficients of θ tells us that, in particular, k has to be a multiple of m. We can therefore write $k = ma$ for some a. Similarly, from the fact that $-5m + l\theta$ is in $\mathfrak{a}$, we see that l also have to be a multiple of m, say mb.

So, let us rewrite $\mathfrak{a}$ as $[ma, mb + m\theta]$. From the fact that $\mathfrak{a}$ is closed under multiplication by θ, we have that $m(b + \theta)\theta$ is in $\mathfrak{a}$. So $m(b + \theta)\theta$ can be written as a linear combination of ma and $mb + m(\theta)$, i.e.

$$mb\theta - 5m = uma + vmb + vm\theta.$$

Equating the coefficients of θ, it is easy to see that v must be b. Making this substitution, dividing through by m, and equating the integer parts, we have that for some u

$$-5 = ua + b^2.$$

But this is equivalent to saying that $b^2 \equiv -5 \mod a$. One can further check than any module of the above form satisfying this condition is, in fact, an ideal.

In other words, we have the following conclusion: the ideals in $\mathfrak{o}$ are exactly the modules of the form $[ma, mb + m\theta]$ with $b^2 \equiv -5 \mod a$.

Note that the norm of the ideal $[ma, mb + m\theta]$ is $m^2 a$. Dedekind shows in particular how a principal ideal, $\mu\mathfrak{o}$, can be put in the right form; and that the resulting representation tells us that the norm of $\mu\mathfrak{o}$ is exactly the norm of μ as a Gaussian integers (i.e. $N(\mu\mathfrak{o}) = N(\mu)$).

5 Multiplication of ideals in $\mathfrak{o}$

In Section 11, Dedekind considers divisibility and multiplication of ideals.

As far as divisibility goes (in Dedekind's sense), suppose $\mathfrak{m}$ is the ideal $[ma, mb + m\theta]$, and $\mathfrak{m}''$ is the ideal $[m''a'', m''b'' + m''\theta]$, where a, b, a'', and b'' satisfy the condition above. Then saying $\mathfrak{m} \supseteq \mathfrak{m}''$ is equivalent to saying that each generator of $\mathfrak{m}''$ is in $\mathfrak{m}$. With some work we can show the following equivalence:

- $\mathfrak{m} \supseteq \mathfrak{m}'$ if and only if

$$m''a \equiv m''a'' \equiv m'(b'' - b) \equiv 0 \quad (mod\ ma).$$

As far as multiplication goes, suppose $\mathfrak{m}$ is the ideal $[ma, mb + m\theta]$, and $\mathfrak{m}'$ is the ideal $[m'a', m'b' + m'\theta]$, where a, b, a', and b' satisfy the condition above. The product, $\mathfrak{m}\mathfrak{m}'$, will be generated by the products of the generators; in other words,

$$\mathfrak{m}\mathfrak{m}' = [mam'a', ma(m'b' + m'\theta), (mb + m\theta)m'a', (mb + m\theta)(m'b' + m'\theta)].$$

From the proceeding considerations, we know that we can distill these generators down to two, of the form $m''a'', m''(b'' + \theta)$. The question is: given m, a, b, m', a', and b', how do we find m'', a'' and b''?

Using raw calculation and facts from linear algebra developed in Chapter 1, Dedekind provides the following precise answer. Let p be the greatest common divisor of a, a', and $b + b'$. Write

$$a = pq', \quad a' = pq'', \quad b + b' = pq'''$$

Then we have

$$m'' = pmm', \quad a'' = \frac{aa'}{p^2} = q'q'',$$

and b'' is determined by the congruences

$$q'b'' \equiv q'b', \quad q''b'' \equiv q''b, \quad q'''b'' \equiv \frac{bb'-5}{p} \quad (mod\ a'').$$

These explicit equations are not so interesting in their own right, but they are important because they allow one to derive the following two consequences:

1. For any two ideal $\mathfrak{m}$ and $\mathfrak{m}'$, one has $N(\mathfrak{m}\mathfrak{m}') = N(\mathfrak{m})N(\mathfrak{m}')$.

2. Given any ideal $\mathfrak{m} = [ma, m(b+\theta)]$, let $\mathfrak{m}_1$ be the "conjugate" ideal $\mathfrak{m}_1 = [ma, m(-b+\theta)]$. Then $\mathfrak{m}\mathfrak{m}_1 = \mathfrak{o}N(\mathfrak{m})$, i.e. the principal ideal generated by the rational integer $N(\mathfrak{m})$.

6 Unique factorization in $\mathfrak{o}$

The desired relation between divisibility and multiplication (or, in modern terms, containing and dividing) now follows from the two facts just indicated, together with the characterization of divisibility above. Remember that we want to show that $\mathfrak{m} \supseteq \mathfrak{m}''$ if and only if $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$ for some $\mathfrak{m}'$. One direction is straightforward: suppose $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$ for some $\mathfrak{m}'$. It is easy to see from the definition on an ideal that $\mathfrak{m}\mathfrak{m}' \subseteq \mathfrak{m}$, so we have $\mathfrak{m} \supseteq \mathfrak{m}''$.

For the converse direction, the argument at the end of Section 11 is roughly as follows:

- Suppose $\mathfrak{m} \supseteq \mathfrak{m}''$.

- Let $\mathfrak{m}_1$ be the ideal conjugate to $\mathfrak{m}$. Then $\mathfrak{m}_1\mathfrak{m} \supseteq \mathfrak{m}_1\mathfrak{m}''$.

- By consequence 2, $\mathfrak{m}_1\mathfrak{m} = \mathfrak{o}N(\mathfrak{m})$, so $\mathfrak{o}N(\mathfrak{m}) \supseteq \mathfrak{m}_1\mathfrak{m}''$.

- Write $\mathfrak{m}_1\mathfrak{m}'' = [m'''a', m'''(b'+\theta)]$. By the characterization of divisibility, we have that $N(\mathfrak{m})|m'''$.

- Let $m' = m'''/N(\mathfrak{m})$. Let $\mathfrak{m}' = [m'a', m'(b'+\theta)]$. Then $\mathfrak{m}'$ is the ideal we are looking for, i.e. the unique ideal satisfying $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$.

Dedekind defines an ideal $\mathfrak{p}$ to be *prime* if it is a proper ideal in $\mathfrak{o}$ (i.e. not all of $\mathfrak{o}$), with the property that there is no ideal between it and $\mathfrak{o}$:

$$\text{if } \mathfrak{p} \subseteq \mathfrak{m} \text{ then } \mathfrak{m} = \mathfrak{o} \text{ or } \mathfrak{m} = \mathfrak{p},$$

where $\mathfrak{m}$ ranges over ideals in $\mathfrak{o}$. He then shows that if $\mathfrak{p}$ is prime, then $\mathfrak{p}$ satisfies the following:

$$\text{if } \mathfrak{p} \supseteq \mathfrak{m}\mathfrak{m}', \text{ then } \mathfrak{p} \supseteq \mathfrak{m} \text{ or } \mathfrak{p} \supseteq \mathfrak{m}',$$

where $\mathfrak{m}$ and $\mathfrak{m}'$ range over ideals in $\mathfrak{o}$. In modern terms, we would use "maximal" to denote the first condition, and "prime" to denote the second; so, in these terms, what Dedekind has shown is that every maximal ideal is prime. I will go over the arguments in class.

Using the connection between divisibility and multiplication (i.e. containing and dividing), we know that being maximal is the same as being *irreducible*:

$$\text{if } \mathfrak{m}|\mathfrak{p}, \text{ then } \mathfrak{m} = \mathfrak{o} \text{ or } \mathfrak{m} = \mathfrak{p}.$$

Here I am using $|$ in the modern sense, i.e. $\mathfrak{a}|\mathfrak{b}$ means that $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ for some $\mathfrak{c}$. We also know that primality for ideals is similar to primality for the integers:

$$\text{if } \mathfrak{p}|\mathfrak{m}\mathfrak{m}', \text{ then } \mathfrak{p}|\mathfrak{m} \text{ or } \mathfrak{p}|\mathfrak{m}'.$$

Unique factorization now follows just as for the integers. Every ideal factors into irreducible element: just keep factoring reducible components, noting that the norm decreases at each step. Furthermore, this factorization is unique: this follows in the usual way by comparing two factorizations term by term, and using the fact that irreducibles are prime, in the second sense above.

The proof presented in this chapter relied on the explicit representation of ideals in $\mathfrak{o}$, in characterizing $\mathfrak{m} \supseteq \mathfrak{m}'$, and in deriving the two consequences at the end of the previous section. According to Dedekind, this is a significant shortcoming of the approach.

7 Additional notes

In this last section, let me note some of the methodologically interesting features of this chapter. All of them deserve to be discussed in class.

First, there is Kummer's mathematically sound but awkward way of introducing ideal elements via their properties with respect to divisibility, i.e. saying what it means to be divisible by an ideal element α, without saying what α is. Dedekind admits that Kummer's approach is mathematically sound and rigorous, but rejects it on the grounds that it is complicated, and likely to lead one to make careless errors. (Moral: the correctness of a theory is not everything.)

Second, there is Dedekind's solution to the problem: identifying Kummer's ideal divisor with the *set* (or "system") of actual numbers it divides. On the surface, this involves treating an infinite set of objects as an object in its own right; so, for example, ideal multiplication and ideal norm are functions that act on sets. For this reason, Dedekind's theory of ideals is often viewed as being an important component in the rise of set-theoretic thinking in mathematics. The issues are subtle, however. For example, all of Dedekind's ideals are finitely generated, and so can be represented with a finite amount of information. And one might argue that the underlying computations with representations are in a sense implicit in Dedekind's "conceptual" approach. Modern set-theoretic presentations of mathematics give one a good deal of latitude in defining operations on sets, without worrying about finite representations or effective computations using these representations. By these standards, Dedekind's use of set theory is relatively tame; for example, Hilbert's later proofs of his *Basis theorem* and *Nullestellensatz* offer more dramatic uses of nonconstructive, set-theoretic methods. So it is worth paying careful attention to the precise form of the set theoretic inferences Dedekind relies on, and what seems to justify them from his point of view.

Third, there is Dedekind's rejection of what he takes to be Kronecker's approach of interpreting the ideal elements as algebraic integers in a larger ring. Dedekind objects:

> Although this way is capable of leading to our goal, it does not seem to me as simple as desirable, because one is forced to pass from the given domain $\mathfrak{o}$ to a more complicated domain $\mathfrak{o}'$. It is also easy to see that the choice of the new domain $\mathfrak{o}'$ is highly arbitrary. (page 95)

Fourth, this chapter provides a nice example of the general mathematical strategy of understanding a complex structure by understanding simpler structures associated with it. In trying to characterize the ideals in $\mathfrak{o}$, Dedekind begins with a characterization of the (full rank) submodules; then asks what additional information the ideal structure brings. In Chapter 4, when extending the analysis to more general rings of integers, Dedekind introduces a further gradation: he separates what can be learned about the ideals by virtue of the fact that they are submodules of a ring of integers; what can be learned by virtue of the fact that they are ideals; and what can further be learned when the ambient ring is *the* ring of integers of a finite extension of the rationals, which is to say, *all* the integers in the particular field.

Finally, there is the Dedekind's oft-quoted conclusion at the end of Chapter 2:

> However, even though this approach to the theory leaves nothing to be desired in the way of rigour, it is not at all what I propose

> to carry out. One notices, in fact, that the proofs of the most important propositions depend on the representation of an ideal by the *expression* $[ma, m(b+\theta)]$ and on the effective realization of multiplication, that is, on a *calculus* which coincides with the composition of binary quadratic forms given by Gauss. If we want to treat a field Ω of arbitrary degree in the same way, then we shall run into difficulties, perhaps even insurmountable ones. Even if there were such a theory, based on calculation, it still would not be of the highest degree of perfection, in my opinion. It is preferable, as in the modern theory of functions, to seek proofs based immediately on fundamental characteristics, rather than on calculation; and indeed to construct the theory in such a way that it is able to predict the results of calculation (for example the composition of decomposable forms of all degrees). Such is the goal I shall pursue in the chapters of this memoir that follow.

We will have to wait until we get to Chapters 3 and 4 to gauge the extent to which Dedekind's proof of unique factorization for general number fields succeeds in this respect.