11 Ideals

The presentation here is somewhat different than the text. In particular, the sections do not match up.

We have seen issues with the failure of unique factorization already, e.g., $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ does not have unique factorization. For instance $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ and one can check $2, 3, 1 \pm \sqrt{-5}$ are all irreducible. This cannot be resolved like we resolved factorization in $\mathbb{Z}[\sqrt{-3}]$, namely by adding more integers in the *quotient field*[1] $\mathbb{Q}(\sqrt{-3})$, simply because $\mathbb{Z}[\sqrt{-5}]$ is already the entire ring of integers of the quotient field $\mathbb{Q}(\sqrt{-5})$.

As remarked at the end of the last chapter, one could try passing to the ring of integers $\mathcal{O}_K$ of a larger field K, but this introduces new complications: How do you find the right K, and then $\mathcal{O}_K$ (determining $\mathcal{O}_K$ is harder for non-quadratic fields)? How do you know $\mathcal{O}_K$ has unique factorization? In fact, there are examples (albeit complicated) where one cannot always find such an extension K.

Kummer developed a theory of "ideal numbers" to add to rings to recover unique factorization, which was revolutionized by Dedekind's theory of ideals. Kummer used this to recover unique factorization in the *cyclotomic rings* $\mathbb{Z}[\zeta_p]$ for *regular* primes p, and proved Fermat's Last Theorem for regular prime exponents (I won't define regular yet, but as an example all odd primes ≤ 100 except for $37, 59, 67$ are regular). This chapter we will introduce the notions developed by Dedekind.

11.1 Revisiting $\mathbb{Z}$

In mathematics, when one encounters difficulties, it is often a good idea to take a step back and try to look at things from a different point of view. Let's now take another look at divisibility in $\mathbb{Z}$.

Definition 11.1. *Let $n \in \mathbb{Z}$. The* **(principal) ideal** *(of $\mathbb{Z}$) generated by n is $(n) = n\mathbb{Z}$.*

In other words, (n) is the set of multiples of $\mathbb{Z}$.

Example. $(0) = \{0\}$. $(1) = (-1) = \mathbb{Z}$. $(2) = (-2) = 2\mathbb{Z}$ *is the set of even integers.*

Just like with rings and fields, we could take an axiomatic approach to ideals.

Definition 11.2. *Let R be a ring and $\mathcal{I} \subseteq R$ ($\mathcal{I} \neq \emptyset$). Suppose*
(i) $a, b \in \mathcal{I} \implies a + b \in \mathcal{I}$, and
(ii) $a \in \mathcal{I}, b \in R \implies ra \in \mathcal{I}$.
Then we say $\mathcal{I}$ is an **ideal** *of R.*

It is easy to see properties (i) and (ii) hold for the principal ideals (n) of $\mathbb{Z}$, so they satisfy the general definition of ideals.

Example. *For any ring R, the* zero ideal $\{0\}$ *is an ideal of R. R is also an ideal of R. These are trivial cases and we will often want to avoid them. We say an ideal $\mathcal{I}$ is a* **proper ideal** *of R if $\mathcal{I} \neq R$, and we say $\mathcal{I}$ is a* **nonzero ideal** *of R if it is not the zero ideal.*

Exercise 11.1. *Check (i) and (ii) hold for the principal ideal* (2).

[1] The quotient field of a nonzero subring R or $\mathbb{C}$ is the smallest subfield of $\mathbb{C}$ containing R. It is the set of all quotients $\frac{a}{b}$ where $a, b \in R$, $b \neq 0$, hence the name.

Proposition 11.3. *Every ideal $\mathcal{I}$ of $\mathbb{Z}$ is of the form (n) for some $n \in \mathbb{Z}$.*

Proof. Since $\{0\} = (0)$ and $\mathbb{Z} = (1)$, we may assume $\mathbb{Z}$ is a non-zero proper ideal. Note if $a \in \mathcal{I}$ then $-a \in \mathcal{I}$ by Property (ii), so the non-zero elements of $\mathcal{I}$ occur in pairs $a, -a$. Let n be the smallest non-zero element of $\mathcal{I}$. We claim $\mathcal{I} = (n)$.

First note $\mathcal{I} \supseteq (n)$ by Property (ii). Suppose $\mathcal{I} \neq (n)$, i.e., suppose there is some $m \in \mathcal{I}$ such that $m \notin (n)$. Write $m = qn + r$ where $0 < r < n$. Since $m, -qn \in \mathcal{I}$, $r = m - qn \in \mathcal{I}$, but this contradicts the definition of n being minimal, i.e., $\mathcal{I} = (n)$. □

Corollary 11.4. *The ideals of $\mathbb{Z}$ are in 1-to-1 correspondence with $\mathbb{N} \cup 0$, given by $(n) \leftrightarrow n$.*

In general, the ideals of a ring are not just the multiples of elements in the ring, but more complicated. However, we'll worry about that later. For now let's just keep $\mathbb{Z}$ in mind, and see what ideal theory says in this context.

First we define arithmetic operations on ideals.

Definition 11.5. *Let $\mathcal{I}, \mathcal{J}$ be ideals of a ring R. Their* **sum** *is the ideal*

$$\mathcal{I} + \mathcal{J} = \{i + j : i \in \mathcal{I}, j \in \mathcal{J}\}$$

and their **product** *is the ideal*

$$\mathcal{I}\mathcal{J} = \{i_i j_1 + i_2 j_2 + i_k j_k : i_m \in \mathcal{I}, j_n \in \mathcal{J}\}.$$

Note that the definition of $\mathcal{I}\mathcal{J}$ may seem a little complicated: naively we would like $\mathcal{I}\mathcal{J} = \{ij : i \in \mathcal{I}, j \in \mathcal{J}\}$ but in general this set will not be closed under addition, so we need to consider finite sums of products ij. However for ideals in $\mathbb{Z}$, the situation is simpler, as we will see below.

Exercise 11.2. *Check that $\mathcal{I} + \mathcal{J}$ and $\mathcal{I}\mathcal{J}$ indeed define ideals.*

Example. *Let $R = \mathbb{Z}$. Then $(2) + (4) = \{2m + 4n\} = \{2k\} = (2)$ and $(2) + (3) = \{2m + 3n\} = (1) = \mathbb{Z}$ since $1 = \gcd(2, 3) = 2m + 3n$ for some m, n by Section 2.3. (Or precisely $1 = 2 \cdot 2 + (-1)3$.)*

Example. *Let $R = \mathbb{Z}$. Then $(2)(4) = \{2m_1 \cdot 4n_1 + \cdots + 2m_k \cdot 4n_k\} = \{8k\} = (8)$ and $(2)(3) = \{2m_1 \cdot 3n_1 + \cdots + 2m_k \cdot 3n_k\} = \{6k\} = (6)$.*

Exercise 11.3. *Let $m, n \in \mathbb{Z}$. Show $(m) + (n) = (\gcd(m, n))$ and $(m)(n) = (mn)$. (Cf. Exercise 11.1.1.)*

Definition 11.6. *Let $\mathcal{I}, \mathcal{J}$ be ideals in a ring R. We say $\mathcal{I}$* **divides** *$\mathcal{J}$, and write $\mathcal{I}|\mathcal{J}$ if $\mathcal{I} \supseteq \mathcal{J}$.*

This notion is crucial, so say it to yourself 3 times: *contains means divides, contains means divides, contains means divides.*

Example. $(2)|(4)$ *since every multiple of* 4 *is a multiple of* 2.

Exercise 11.4. *Let $m, n \in \mathbb{Z}$. Show $(m)|(n) \iff m|n$.*

Definition 11.7. *Let $\mathfrak{p}$ be a proper ideal of a ring R. We say $\mathfrak{p}$ is a* **prime ideal** *of R if $\mathfrak{p}|\mathcal{I}\mathcal{J}$ implies $\mathfrak{p}|\mathcal{I}$ or $\mathfrak{p}|\mathcal{J}$, where $\mathcal{I}, \mathcal{J}$ are ideals of R.*

By the previous exercise, it is clear the prime ideals of $\mathbb{Z}$ are $\mathfrak{p} = (p)$ where p is a prime in $\mathbb{N}$. Hence we may state unique factorization in $\mathbb{Z}$ in terms of ideals: *Let $\mathcal{I}$ be a nonzero proper ideal of $\mathbb{Z}$. Then $\mathcal{I} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_k$ where each $\mathfrak{p}_i$ is a prime ideal. Moreover the $\mathfrak{p}_i$'s are uniquely determined (up to reordering).* We can translate this back into the usual statement as follows—we know $\mathcal{I} = (n)$ for some $n \in \mathbb{N}$, $n \neq 1$. Then there is a unique factorization (up to ordering) $n = \prod p_i$ where each $p_i \in \mathbb{N}$ is prime. This corresponds to the prime ideal factorization

$$(n) = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_k = (p_1)(p_2)\cdots(p_k).$$

Note that working with ideals already makes the statement of unique factorization in $\mathbb{Z}$ a little simpler than just working with integers, because one does not need to worry about units. However the main advantage of working with ideals is this: *for any nice ring*[2]*, we always have unique prime factorization of ideals!* The rest of the semester will be devoted to understanding this, and then seeing how one can apply it, for example, to determining which primes p are of the form $x^2 + 5y^2$.

11.2 Revisiting $\mathbb{Z}[\sqrt{-3}]$

While in $\mathbb{Z}$, the ideals correspond to elements of $\mathbb{Z}$ up to units, in general for a ring R, some ideals will correspond to elements of R and some will correspond to the "ideal elements" which are required for unique factorization. The ideals corresponding to actual elements of R have a special name.

Definition 11.8. *Let R be a ring and $\alpha_1, \ldots, \alpha_k \in R$. The* **ideal generated by** $\alpha_1, \ldots, \alpha_k$ *is defined to be the smallest ideal containing $\alpha_1, \ldots, \alpha_k$ and denoted $(\alpha_1, \ldots, \alpha_k)$. Explicitly, this ideal is*

$$(\alpha_1, \ldots, \alpha_k) = \{c_1\alpha_1 + c_2\alpha_2 + \cdots + c_k\alpha_k c_i \in R\}.$$

If the ideal $\mathcal{I}$ of R is generated by a single element, i.e., $\mathcal{I} = (\alpha) = \alpha R = \{r\alpha : r \in R\}$ for some $\alpha \in R$, we say $\mathcal{I}$ is a **principal ideal**.

Note, it is clear from the definition that

$$(\alpha_1, \ldots, \alpha_k) = (\alpha_1) + (\alpha_2) + \cdots + (\alpha_k).$$

The key point will be that the principal ideals (α) corresponds to the element α (and its associates), and the non-principal ideals will correspond to "ideal" elements of R. Specifically $(\alpha_1, \ldots, \alpha_k)$ is the smallest ideal which contains each (α_j), in other words $(\alpha_1, \ldots, \alpha_k)$ is the smallest ideal which *divides* each (α_j) (this was our definition of dividing for ideals), so $(\alpha_1, \ldots, \alpha_k)$ should be the "ideal gcd" of $(\alpha_1), \ldots, (\alpha_k)$. This is a rather revolutionary idea, so let's go through it with the example of $\mathbb{Z}[\sqrt{-3}]$.

Let $R = \mathbb{Z}[\sqrt{-3}]$. The principal ideals of R are $(\alpha) = \alpha R = \{r\alpha : r \in R\}$, where α ranges over the elements of R. Note that $(\alpha) \neq (\beta)$ unless α and β are associates. To see this, suppose $(\alpha) = (\beta)$. This means $\beta = r\alpha$ and $\alpha = s\beta$ for some $r, s \in R$. But then $\alpha = s\beta = rs\alpha$ implies $rs = 1$, i.e., r and s are units, i.e., α and β are associates. Conversely, if $\alpha = u\beta$ for some unit $u \in R$, then we also have $\beta = u^{-1}\alpha$, i.e., α and β are multiples of each other, so $(\alpha) = (\beta)$. Note that this argument applies to any R, so for the record we will record the general statement here.

For $\alpha \in R$, we define the **associate class** of α to be the set $\{u\alpha : u \text{ is a unit of } R\}$.

[2]Technically, the conditions on the ring are being what is called a *Dedekind domain*. The primary examples of Dedekind domains, and what we will care about, are the rings of integers $\mathcal{O}_K$ of number fields K.

Proposition 11.9. *Let R be a subring of $\mathbb{C}$. The principal ideals (α) of R are in 1-1 correspondence with the set of associate classes of R.*

Now the issue with unique factorization in $\mathbb{Z}[\sqrt{-3}]$ was the following:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$$

but 2, $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are all irreducible in $\mathbb{Z}[\sqrt{-3}]$. In the language of ideals, we can write this as

$$(4) = (2)(2) = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

(Note in the former equation $(1 + \sqrt{-3})$ is just the number $1 + \sqrt{-3}$ in parentheses, but in the latter equation it means the ideal generated by $1 + \sqrt{-3}$. Hopefully there will be no confusion about this notation, as the meaning should be clear from context.) The resolution of this non-unique factorization using ideals is the following: the ideals (2), $(1 + \sqrt{-3})$ and $(1 - \sqrt{-3})$ are not irreducible! Indeed, (2) and $(1 + \sqrt{-3})$ have a "common factor"

$$(2, 1 + \sqrt{-3}) = (2) + (1 + \sqrt{-3}) = \left\{ 2m + (1 + \sqrt{-3})n : m, n \in R \right\}.$$

In fact, since $2\sqrt{-3} = 2(-1) + (1 + \sqrt{-3})2$ and $(1 + \sqrt{-3})\sqrt{-3}) = -3 + \sqrt{-3} = 2(-2) + (1 + \sqrt{-3}) \cdot 1$ are both of the form $2m + (1 + \sqrt{-3})n$ for $m, n \in \mathbb{Z}$, we have

$$(2, 1 + \sqrt{-3}) = \left\{ 2m + (1 + \sqrt{-3})n : m, n \in \mathbb{Z} \right\}.$$

(You can just check this set is closed under addition and multiplication by elements in R.) Now this ideal contains both (2) and $(1 + \sqrt{-3})$, so it divides them. It is easy to see $1 \notin (2, 1 + \sqrt{-3})$, hence $(2, 1 + \sqrt{-3}) \neq (1) = R$; in other words, $(2, 1 + \sqrt{-3})$ is a *nontrivial* divisor of R.

Note the non-proper ideal R of R, always divides (contains) every ideal trivially, just like the number 1 divides any integer—in fact R is the principal ideal generated by 1, so in the correspondence described above, it is the principal ideal corresponding to 1 and its associates, i.e., the principal ideal corresponding to the units. Thus any proper ideal which divides another ideal may be thought of as a nontrivial divisor.

Exercise 11.5. *Check that the ideal $(2, 1 + \sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$ is not principal. (Use contradiction.)*

Hence $(2, 1 + \sqrt{-3})$ corresponds to some "ideal number" in $\mathbb{Z}[\sqrt{-3}]$, which should basically be the element ζ_3 that is not in the ring. In fact, if we pass to the ring $\mathbb{Z}[\zeta_3]$, we see that the ideal $(2, 1 + \sqrt{-3}) = (\zeta_3) = (1) = \mathbb{Z}[\zeta_3]$ is principal. Indeed, all ideals of $\mathbb{Z}[\zeta_3]$ are principal, just like for $\mathbb{Z}$, because we have unique factorization. We will go over this formally later.

Actually, this example is of $\mathbb{Z}[\sqrt{-3}]$ does not illustrate the power of ideals because it is not a Dedekind domain. (A Dedekind domain must be *integrally closed*, meaning it should contain all the integers in its quotient field.) If it were a Dedekind domain, we would have unique factorization into prime ideals, e.g., there would be prime ideals $\mathfrak{p}, \mathfrak{q}$ in $\mathbb{Z}[\sqrt{-3}]$ such that $(2) = \mathfrak{pq}$, $(1 + \sqrt{-3}) = \mathfrak{p}^2$ and $(1 - \sqrt{-3}) = \mathfrak{q}^2$. This would resolve the factorization

$$(4) = (2)(2) = (\mathfrak{pq})(\mathfrak{pq}) = \mathfrak{p}^2\mathfrak{q}^2 = (1 + \sqrt{-3})(1 - \sqrt{-3}),$$

however there is only one prime ideal dividing (2), namely $(2, 1 + \sqrt{-3}) = (2, 1 - \sqrt{-3})$. Hence, to really make use of ideals, we need to pass to the integral closure $\mathbb{Z}[\zeta_3]$ of $\mathbb{Z}[\sqrt{-3}]$ which already has unique factorization, so one does not really gain anything by using ideals.

While, this example does not illustrate the full power of ideals, there is some interesting geometry going on. See the pictures in Section 11.4 of Stillwell. To see the full power of ideals, we will need to move to another field F where the full ring of integers $\mathcal{O}_F$ does not have unique factorization.

11.3 A visit to $\mathbb{Z}[\sqrt{-5}]$

Since $\mathbb{Z}[\sqrt{-5}]$ is already the full ring of integers of its quotient field $\mathbb{Q}(\sqrt{-5})$, it is not clear what elements we might adjoin to recover unique factorization. The standard example of non-unique factorization in this ring is

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

Since 2, 3, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are all irreducible in this ring, this is a counter-example to unique factorization into irreducibles/primes. Let's see how we can resolve this with ideal theory.

We set

$$\mathfrak{p} = (2, 1+\sqrt{-5}) = (2) + (1+\sqrt{-5}) = \left\{2m + (1+\sqrt{-5})n : m, n \in \mathbb{Z}\right\}$$

$$\mathfrak{q} = (3, 1+\sqrt{-5}) = (3) + (1+\sqrt{-5}) = \left\{3m + (1+\sqrt{-5})n : m, n \in \mathbb{Z}\right\}$$

and

$$\overline{\mathfrak{q}} = (3, 1-\sqrt{-5}) = (3) + (1-\sqrt{-5}) = \left\{3m + (1-\sqrt{-5})n : m, n \in \mathbb{Z}\right\}.$$

(Note that $\mathfrak{p} = \overline{\mathfrak{p}} = (2, 1-\sqrt{-5})$ since $1-\sqrt{-5} = 2 - (1+\sqrt{-5}) \in \mathfrak{p}$.) It is not difficult to check

$$\mathfrak{p}^2 = (2), \quad \mathfrak{q}\overline{\mathfrak{q}} = (3)$$

and

$$\mathfrak{p}\mathfrak{q} = (1+\sqrt{-5}), \mathfrak{p}\overline{\mathfrak{q}} = (1-\sqrt{-5}).$$

Further $\mathfrak{p}, \mathfrak{q}, \overline{\mathfrak{q}}$ are all "irreducible" (prime). We will go through the details later, but the point is that this will resolve the above non-unique factorization—for at the level of ideals we have

$$(6) = (2)(3) = \mathfrak{p}^2\mathfrak{q}\overline{\mathfrak{q}} = (\mathfrak{p}\mathfrak{q})(\mathfrak{p}\overline{\mathfrak{q}}) = (1+\sqrt{-5})(1-\sqrt{-5}).$$

To help us understand all the details, we will first develop some more theory. If you want to see some of the details, look at 11.8 of the text.

11.4 PID's 'n ED's

First we characterize what it means to have unique factorization in a ring in terms of its ideals. With the philosophy that (i) any ideal has a unique factorization into prime ideals (which we will prove later), and (ii) the elements of R correspond to the principal ideals of R, it makes sense to guess that R has unique factorization if and only if every ideal is principal. Here we will show one direction, and return to the other direction later.

Definition 11.10. *Let R be a non-zero subring of $\mathbb{C}$. We say R is a* **principal ideal domain (PID)**[3] *if every ideal of R is principal.*

Example. *$\mathbb{Z}$ is a PID. We already proved this.*

[3] In general, PID's and ED's need not be subrings of $\mathbb{C}$—I just make this assumption for simplicity since it is the only case we will be interested in. Technically they must be certain kinds of rings called *domains*, which have the property that if $ab = 0$ then $a = 0$ or $b = 0$. This is not true for $\mathbb{Z}/n\mathbb{Z}$ if n is not prime, e.g., $2 \cdot 2 \equiv 0$ in $\mathbb{Z}/4\mathbb{Z}$.

Proposition 11.11. *Let R be a PID. Then R satisfies the prime divisor property, i.e., any non-unit irreducible $\pi \in R$ is prime. Consquently, R has unique factorization, i.e., if α is any nonzero non-unit in $\mathbb{R}$, then it can be written uniquely (up to reordering and units) in the form $\alpha = \pi_1\pi_2\cdots\pi_k$ where π_i are primes of R.*

Proof. The second statement follows formally from the first (I have said many times now that the prime divisor property and unique factorization are equivalent—if you want to review the argument, look back at the cases of $\mathbb{Z}$ or $\mathbb{Z}[i]$). Thus it suffices to show any non-unit irreducible $\pi \in R$ is prime.

Let π be a non-unit irreducible. Recall π is prime means $\pi|\alpha\beta \implies \pi|\alpha$ or $\pi|\beta$. So suppose $\pi|\alpha\beta$ for some $\alpha, \beta \in R$. The idea is to look at the "gcd" $(\pi, \alpha) = (\pi) + (\alpha)$ of π and α. Note that $(\pi, \alpha) = (\gamma)$ for some $\gamma \in R$ since R is a PID. We know $(\gamma) = (\pi, \alpha)|(\pi)$ and $(\gamma) = (\pi, \alpha)|(\alpha)$ by the definition of divides for ideals. This means, $\pi = m\gamma$ and $\alpha = n\gamma$ for some $m, n \in R$.

Since π is irreducible, either m or γ is a unit and the other is an associate of π. If γ is an associate of π, this means $\pi|\alpha = n\gamma$, so the prime divisor property holds. Thus we may assume γ is a unit. This means $1 \in (\gamma) = (\pi, \alpha)$, i.e., $1 = r\pi + s\alpha$ for some $r, s \in R$. Thus $\beta = r\pi\beta + s\alpha\beta$, but π divides both terms on the right, so therefore $\pi|\beta$. Hence the prime divisor property holds. □

Note this argument is similar to the argument we gave in $\mathbb{Z}$ (or $\mathbb{Z}[i]$) to show that the Euclidean algorithm (or more precisely that $\gcd(a, b) = ma + nb$ for some m, n) implies the prime divisor property. Here one idea we used is that if $(\alpha)|(\beta)$ at the level of principal ideals, then $\alpha|\beta$ as elements of R. This justifies the terminology that $\mathcal{I}|\mathcal{J}$ means $\mathcal{I} \supseteq \mathcal{J}$.

Exercise 11.6. *Let R be a ring and $\alpha, \beta \in R$. Show $(\alpha)|(\beta)$ (principal ideals) implies $\alpha|\beta$ (elements). (We already had this exercise for $R = \mathbb{Z}$.)*

Now that we know PID's have unique factorization, how can we tell if a ring is a PID? Well, since the Euclidean algorithm implies unique factorization, one might guess that it implies being a PID.

Definition 11.12. *Let R be a non-zero subring of $\mathbb{C}$. We say R is a Euclidean domain if there is a map (called the absolute value) $|\cdot| : R \to \mathbb{Z}_{\geq 0}$ such that (i) $|a| = 0 \iff a = 0$, (ii) $|1| = 1$,and (iii) for any $a, b \in R$, $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ such that $|r| < |b|$.*

Exercise 11.7. *Suppose R is a Euclidean domain with absolute value $|\cdot|$. Let $a \in R$ such that $|a| = 1$. Show $(a) = R$.*

Proposition 11.13. *If R is a Euclidean domain, it is a PID.*

Proof. This is like the proof that $\mathbb{Z}$ is a PID. Suppose $\mathcal{I}$ is a non-principal ideal R. It is clear that $\mathcal{I}$ must be a non-zero proper ideal. Choose $b \in \mathcal{I}$ such that $|b| > 0$ is minimal. By the previous exercise, $|b| > 1$. Every multiple of $b \in \mathcal{I}$ since $\mathcal{I}$ is an ideal, so if $\mathcal{I} \neq (b)$ there is some $a \in \mathcal{I}$ such that a is not a multiple of b. Then we can write $a = qb + r$ where $0 < |r| < |b|$. But $r = a - qb \in \mathcal{I}$, contradicting the minimality of $|b|$. □

Example. *We showed earlier that $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\zeta_3]$ are Euclidian domains, and therefore a PIDs. This completes the proof that each of these rings have unique factorization.*

In fact the only values of $d < 0$ squarefree such that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ are Euclidean domains are $d = -1, -2, -3, -7, -11$. However, there are 4 more values of $d < 0$ such that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a PID, and

therefore has unique factorization: $d = -19, -43, -67$ and -163. This was conjectured by Gauss (in a different language, from a different context), and is called the Gauss class number problem, which was finally resolved by Heegner, Baker and Stark in the 1950's and 1960's.

For more on the cases $d = -7, -11$, see Section 11.3 and the exercises in the text.

The case of $d > 0$ squarefree is very different. There are still only finitely many d such that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a Euclidean domain: $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. But it is not known for which $d > 0$ $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a PID, or even if this number is finite or infinite. Nevertheless, it is conjectured that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a PID, i.e., has unique factorization, about 75% of the time.

When one considers number fields of higher degree, less is known. In particular, it is not known for which number fields K is $\mathcal{O}_K$ a Euclidean domain.

In any case, we are interested in unique factorization, and not so much in whether a ring has a Euclidean algorithm or not. The known examples show that the existence of a Euclidean algorithm is not necessary for unique factorization. However, we will see later that if $\mathcal{O}_K$ is not a PID, it does not have unique factorization. This characterization of unique factorization in terms of ideals further suggest that ideals are the right thing to look at.

By the way, if you like TLA's (three letter acronyms), one often calls domains with unique factorization UFD's. If you've seen these in algebra, you might be confused by something I've just said. In algebra one typically shows every PID is a UFD, but not the converse. Indeed, the converse is not true for general rings, but it is in the case of rings of integers of number fields.

11.5 Maximal ideals

Our goal is to show the following: *Let K be a number field.*[4] *Then any nonzero proper ideal of $\mathcal{O}_K$ factors uniquely into prime ideals of $\mathcal{O}_K$.* After we show this, we will see how we can use this to surmount difficulties arising from non-unique factorization of elements in $\mathcal{O}_K$.

Before we can show unique factorization into prime ideals, we should first show the existence of factorization into prime ideals, which requires knowing the following: *If $\mathcal{I}$ is an nonzero proper ideal of $\mathcal{O}_K$, then there is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ dividing (containing) $\mathcal{I}$.*

If we think about elements in a ring, it's not always true that a prime factorization exists. For instance, in $\mathbb{Z}[\sqrt{-5}]$ we have the non-unique factorization $6 = 2 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, where 2, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all *irreducible* non-units, but none of them are *prime* (i.e., satisfy the prime divisor property). However, it is easy to show that any element of $\mathcal{O}_K$ factors into a finite number of irreducibles (this is like the proof of existence of prime factorization in $\mathbb{Z}$, where there is no difference between primes and irreducible non-units, though one needs to provide a new argument about the finiteness).

It is a good idea to think about the corresponding notion of (non-unit) irreducibles for ideals. A non-unit irreducible is an element that has no divisors other than units and its associates. So the non-unit "irreducible" ideals of R should be the ideals $\mathcal{I}$ such that the only ideals dividing (containing) $\mathcal{I}$ are $R = (1)$ and $\mathcal{I}$.

Definition 11.14. *Let R be a ring. We say $\mathfrak{m}$ is a* **maximal ideal** *of R if $\mathfrak{m} \neq R$ and the only ideals of R containing $\mathfrak{m}$ are R and $\mathfrak{m}$.*

[4] By the way, the reason one often uses K for fields (though one also often uses F) is because fields were originally introduced by Dedekind who called them *Körper*, meaning body or corpus in German.

Note that we impose the condition $\mathfrak{m} \neq R$ so that $\mathfrak{m}$ does not correspond to the units. It is perhaps an unfortunate confluence of terminology that the terms prime element, prime ideal and maximal ideal exclude the trivial case of either units or R, but the term irreducible includes units. I'm sorry if this is confusing to remember, but I am just going with the standard terminology. Another strange consequence of standard terminology is that 0 is never a prime element but the zero ideal $\{0\}$ is a prime ideal of any domain (see definition below).

Proposition 11.15. *Let $\mathcal{I}$ be a proper ideal in $\mathcal{O}_K$. Then $\mathcal{I}$ is contained in some maximal ideal $\mathfrak{m}$ of $\mathcal{O}_K$.*

Proof. Either $\mathcal{I}$ maximal or not. If so, we are done. If not, it is contained in some strictly larger proper ideal $\mathcal{I}_1$ of $\mathcal{O}_K$. Either $\mathcal{I}_1$ is either maximal or not. If so, we are done. If not, $\mathcal{I}_1$ is contained in a larger proper ideal $\mathcal{I}_2$ of $\mathcal{O}_K$. Hence there is an ascending sequence of ideals

$$\mathcal{I} \subseteq \mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \cdots \subseteq \mathcal{O}_K.$$

The point is that we can only fit a finite number of ideals in such a chain before we get to $\mathcal{O}_K$. I won't prove this, but it's a standard fact from algebra since $\mathcal{O}_K$ is a finitely generated ring. The ideal preceding $\mathcal{O}_K$ in this chain is the desired maximal ideal. □

The key point about working with ideals is that for a general ring of integer $\mathcal{O}_K$, the non-unit irreducible elements and prime elements do not coincide, but the maximal ideals are precisely (non-zero) prime ideals. This fact will allow us to prove unique factorization into prime ideals, but to prove this fact, we first need to characterize prime and maximal ideals in terms of their quotient rings.

11.6 Quotient rings

Definition 11.16. *Let R be a ring and $\mathcal{I}$ an ideal. Denote by $R/\mathcal{I}$ the set of cosets of the subgroup $(\mathcal{I}, +)$ in $(R, +)$. The* **quotient ring** *$R/\mathcal{I}$ is the ring whose underlying set is $R/\mathcal{I}$ with operations $+$ and $\cdot$ defined by*

$$(r + \mathcal{I}) + (s + \mathcal{I}) = (r + s) + \mathcal{I}$$

and

$$(r + \mathcal{I}) \cdot (s + \mathcal{I}) = rs + \mathcal{I}.$$

THe **norm** *of $\mathcal{I}$ is the number of elements of $R/\mathcal{I}$ (if finite).*

This in fact defines a ring (the details are simple, or see an algebra text if you are not satisfied), and we have seen this construction before.

Example. *Let $R = \mathbb{Z}$ and $\mathcal{I} = (n)$. Then $R/I = \mathbb{Z}/n\mathbb{Z}$. The norm of (n) is $|n|$.*

Example. *Let $R = \mathbb{Z}[i]$ and $\mathcal{I} = (1 + i)$. (Recall $1 + i$ is a prime element of $\mathbb{Z}[i]$.) Then $R/\mathcal{I} = \{0 + \mathcal{I}, 1 + \mathcal{I}\} \simeq \mathbb{Z}/2\mathbb{Z}$. To see why this is so, note that we may think of $R/\mathcal{I}$ as the set of possible remainders upon division by $1 + i$. Note that $2 = (1 + i)(1 - i) \equiv 0 \bmod 1 + i$, so the possible remainders mod $1 + i$ are going to be numbers of the form $a + bi$ with $0 \leq a, b < 2$, i.e., 0, 1, i and $1 + i$. Clearly $1 + i \equiv 0 \bmod 1 + i$. Further $i \equiv -1 \equiv -1 + 2 \equiv 1 \bmod 1 + i$. This proves the assertion since $0 \not\equiv 1 \bmod 1 + i$. This means the norm of the principal ideal $\mathcal{I} = (1 + i)$ is $N(\mathcal{I}) = 2$ is same as the norm of the element $1 + i \in \mathbb{Z}[i]$.*

We see these quotient rings generalize the notion of mod, and we write $a \equiv b \bmod \mathcal{I}$ if $b - a \in \mathcal{I}$.

Example. *Let $R = \mathbb{Z}[i]$ and $\mathcal{I} = (3)$. Again 3 is a prime element of $\mathbb{Z}[i]$. Since $3 \equiv 3i \equiv 0 \bmod 3$,* a priori *the possible remainders for $R/\mathcal{I}$ are $0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i$. These are all distinct mod $\mathcal{I}$, since the difference of any two of them is not a multiple of 3. Again, we see the norm of the ideal (3), which is 9, is the same as the norm of the element $3 \in \mathbb{Z}[i]$.*

Definition 11.17. *Let R be a nonzero ring. We say $a \in R$ is a* **zero divisor** *if $a|0$ and $a \neq 0$. If R has no zero divisors, we say R is an* **(integral) domain**.

Proposition 11.18. *Let R be a ring and $\mathcal{I}$ an ideal. Then*
(i) $\mathcal{I}$ is prime $\iff$ $R/\mathcal{I}$ is an integral domain;
(ii) $\mathcal{I}$ is maximal $\iff$ $R/\mathcal{I}$ is a field.

Proof. Proof of (i). ($\Rightarrow$) Suppose $\mathcal{I}$ is prime. We claim $R/\mathcal{I}$ has no zero divisors. Suppose it does, i.e., there are nonzero $a, b \in R/\mathcal{I}$ such that $ab = 0$. We can write $a = r + \mathcal{I}$, $b = s + \mathcal{I}$ where $r, s \notin \mathcal{I}$. Then $ab = 0$ means $rs \in \mathcal{I}$. In other words, $\mathcal{I}|(rs)$ but $\mathcal{I} \nmid (r)$, $\mathcal{I} \nmid (s)$, which contradicts the definition of $\mathcal{I}$ being prime.

($\Leftarrow$) Suppose $R/\mathcal{I}$ is an integral domain. If $\mathcal{I}$ is not prime, then there are ideals $\mathcal{J}, \mathcal{J}'$ such that $\mathcal{I}|\mathcal{J}\mathcal{J}'$ but $\mathcal{I} \nmid \mathcal{J}$, $\mathcal{I} \nmid J'$. Hence there are $r \in \mathcal{J}$, $s \in \mathcal{J}'$ such that $r, s \notin \mathcal{I}$, but $rs \in \mathcal{I}$. This means $a = r + \mathcal{I}$ and $b = s + \mathcal{I}$ are zero divisors of $R/\mathcal{I}$, a contradiction.

Proof of (ii). The ideals of $R/\mathcal{I}$ are in 1-1 correspondence with ideals $\mathcal{J}$ of R such that $\mathcal{I} \subseteq \mathcal{J} \subseteq R$. It is simple to check that R is a field if and only if its only ideals are $\{0\}$ and R. □

Corollary 11.19. *Let R be a ring and $\mathfrak{m}$ a maximal ideal. Then $\mathfrak{m}$ is prime.*

Proof. This is immediate from the previous proposition since any field is an integral domain. □

In particular, any nonzero proper ideal of a ring of integers $\mathcal{O}_K$ is divisible by a prime ideal (cf. Prop. 11.15).

Lemma 11.20. *Let R be a finite integral domain. Then R is a field.*

Proof. Since R is a ring with $0 \neq 1$, to show it is a field it suffices to show every nonzero $a \in R$ is invertible.

Note that in any integral domain, if $ab = ac$ and $a \neq 0$, then $b = c$. This is because $ab - ac = a(b - c) = 0$ which implies $b - c = 0$ since R has no zero divisors.

This means multiplication by a simply permutes the elements of R, hence there is some $b \in R$ such that $ab = 1$. □

Corollary 11.21. *Let K be a number field and $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}$ is maximal.*

Proof. By the propsition $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. Let $\alpha \in \mathfrak{p}$ be nonzero. The set of possible remainders for $\mathcal{O}_K$ mod α is finite, hence $\mathcal{O}_K/(\alpha)$ is finte, hence $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain, and therefore a field by the Lemma. This means $\mathfrak{p}$ is maximal by the same proposition above. □

These two corollaries mean that the "irreducible" (maximal) ideals are exactly the same as the (non-zero) prime ideals. We will use this to prove unique factorization into prime ideals in the next section.

Example. *Since* (3) *is prime in* $\mathbb{Z}[i]$ *and it has norm 9,* $\mathbb{Z}[i]/(3)$ *is a finite field of order* 9*.*

One consequence of this is the following: it is a standard fact in algebra that any finite field has prime power order. Thus if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $N(\mathfrak{p}) = p^r$ for some rational prime p and $r \in \mathbb{N}$.

Exercise 11.8. *Let* $R = \mathbb{Z}[\sqrt{-5}]$ *and consider the ideals* $\mathcal{I} = (2)$*,* $\mathcal{J} = (1 + \sqrt{-5})$ *and* $\mathfrak{p} = (2, 1 + \sqrt{-5})$*. Write down a set of representatives for* $R/\mathcal{I}$*,* $R/\mathcal{J}$ *and* $R/\mathfrak{p}$*. What are their norms? Show that* $\mathcal{I}$ *and* $\mathcal{J}$ *are not prime but* $\mathfrak{p}$ *is.*

11.7 Summary

Here is a summary of what all the concepts we've encountered with ideals mean, thinking in terms of just working with elements in a ring.

Table 1: The language of ideals

Ideals of R	Elements of R
principal ideals of R	elements of R up to units
non-principal ideals of R	"ideal elements" of R
the zero ideal $\{0\}$	0
the ideal R	the units of R
contains	divides
product of ideals	product of elements
sum of ideals	"gcd" of elements
prime ideals	prime elements
maximal ideals	(non-unit) irreducible elements
R is a PID	R has unique factorization

It may helpful to read this chapter from the text to solidify these ideas. The discussion section is also somewhat interesting.