PMATH 441 Course Notes

Algebraic Number Theory

Blake Madill • Winter 2023 • University of Waterloo

Table of Contents

1 Algebraic Integers

1.1 Motivation

At its most elementary, number theory is the study of integers. Some of the topics typically discussed in a first-year number theory course include primes, divisibility, the Euclidean algorithm, and prime factorization. Our goal in this course is to generalize these topics using commutative algebra.

One naive approach would be to consider unique factorization domains, or UFDs. However, a classic example of an integral domain that is not a UFD is $\mathbb{Z}[\sqrt{5}]$, which is far too integer-like to be disqualified from our discussion.

Let's do some investigation. Consider $\alpha = \frac{1}{2}(1+\sqrt{5})$. We have $(2\alpha-1)^2 = 5$, and expanding gives us $4\alpha^2 - 4\alpha - 4 = 0$. In particular, we see that

$$\alpha^2 = \alpha + 1.$$

Next, let's consider the ring $\mathbb{Z}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Z}[x]\}$. Since $\alpha^2 = \alpha + 1$, we have that

$$\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\},$$

since there are no need for terms α^n with $n \geq 2$. What made this simplification work?

(a) We needed a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

(b) Moreover, notice that $5 \equiv 1 \pmod 4$, so we could nicely divide all the terms by 4 in the equation $4\alpha^2 - 4\alpha - 4 = 0$.

More generally, why do we want to work with $\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$? This is because it allows us to do finite-dimensional "linear algebra" over $\mathbb{Z}$ (which is actually module theory, as we'll see soon).

1.2 Algebraic Integers

Inspired by our toy example above, let's introduce the algebraic integers.

Definition 1.1

We call $\alpha \in \mathbb{C}$ an **algebraic integer** if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Note that in the above definition, we do not insist that $f(x) \in \mathbb{Z}[x]$ is irreducible.

It is not hard to see that n and $\sqrt{n}$ are algebraic integers for all $n \in \mathbb{Z}$. By our previous work, we see that $\frac{1}{2}(1+\sqrt{5})$ is an algebraic integer. It can also be shown that i, $1+i$ and $\zeta_n = e^{2\pi i/n}$ are all algebraic integers.

We can ignore all transcendental numbers here, because they are certainly not algebraic integers. But how do we tell if an algebraic number $\alpha \in \mathbb{C}$ (i.e. α is algebraic over $\mathbb{Q}$) is an algebraic integer? The following theorem gives us a simple test to do so.

Theorem 1.2

An algebraic number $\alpha \in \mathbb{C}$ is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

An easy corollary we can obtain is that the only algebraic integers in $\mathbb{Q}$ are the ordinary integers. Indeed, the minimal polynomial of a rational number $q \in \mathbb{Q}$ is $m(x) = x - q$, which is in $\mathbb{Z}[x]$ if and only if $q \in \mathbb{Z}$.

For another example, let us consider $\beta = \frac{1}{2}(1+\sqrt{3})$ (noting that $3 \not\equiv 1 \pmod 4$ here). Performing the same manipulations as before, we deduce that $4\beta^2 - 4\beta - 2 = 0$ and hence $\beta^2 - \beta - 1/2 = 0$. In fact, $m(x) = x^2 - x - 1/2$ is the minimal polynomial for β over $\mathbb{Q}$. Indeed, $m(x)$ is monic by performing the eyeball test, and it is irreducible since we know the roots are $\frac{1}{2}(1 \pm \sqrt{3})$, which are not in $\mathbb{Q}$. By applying Theorem 1.2, it follows that β is *not* an algebraic integer.

A concern one might have is that $\beta = \frac{1}{2}(1+\sqrt{3})$ also seems to be integer-like, and so we shouldn't dismiss it. However, we shouldn't expect it to work that nicely because it behaves more like a rational; we were more lucky with $\alpha = \frac{1}{2}(1+\sqrt{5})$ because it happened to be the case that $5 \equiv 1 \pmod 4$, as we observed earlier.

With these examples out of the way, let's jump into the proof of the theorem. Recall that for a polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, the **content** of $f(x)$ is

$$\text{Content}(f(x)) = \gcd(a_n, a_{n-1}, \ldots, a_0).$$

We say that $f(x)$ is **primitive** if $\text{Content}(f(x)) = 1$. Moreover, an equivalent formulation of Gauss' lemma states that if $f(x), g(x) \in \mathbb{Z}[x]$ are primitive, then $f(x)g(x)$ is also primitive.

Proof of Theorem 1.2.

> ($\Leftarrow$) This is immediate by considering the minimal polynomial of α over $\mathbb{Q}$, say $m(x) \in \mathbb{Z}[x]$, which is monic and satisfies $m(\alpha) = 0$.
>
> ($\Rightarrow$) Let $\alpha \in \mathbb{C}$ be an algebraic integer and let $m(x) \in \mathbb{Q}[x]$ be its minimal polynomial. Let $f(x) \in \mathbb{Z}[x]$ be monic such that $f(\alpha) = 0$. Then by the properties of a minimal polynomial, we have $m(x) \mid f(x)$. That is, we can write $f(x) = m(x)g(x)$ for some $g(x) \in \mathbb{Q}[x]$.
>
> Let $N_1, N_2 \in \mathbb{N}$ be minimal such that $N_1 m(x), N_2 g(x) \in \mathbb{Z}[x]$. Note that if p is a prime dividing all coefficients of $N_1 m(x)$, then $(N_1/p)m(x) \in \mathbb{Z}[x]$, and in fact, we also have $N_1/p \in \mathbb{Z}$ since $m(x)$ is monic. This contradicts the minimality of N_1, so $N_1 m(x)$ must be primitive. Similarly, $N_2 g(x)$ is primitive by the same argument, noting that $g(x)$ is monic since $f(x)$ and $m(x)$ are.
>
> Now, observe that $N_1 N_2 f(x) = (N_1 m(x))(N_2 g(x))$ is primitive by Gauss' lemma. Again, we note that $f(x)$ is monic, so equating contents gives us $N_1 N_2 = 1$. It follows that $N_1 = N_2 = 1$, and in particular, we have $m(x) \in \mathbb{Z}[x]$ as desired. □

1.3 Rings of Integers

We now work through an example which is considered a rite of passage through algebraic number theory. Let $d \in \mathbb{Z}$ be square-free where $d \neq 1$. Recall that being square-free means that there is no multiplicity in its prime factorization. Consider the field extension

$$K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$

In particular, $K/\mathbb{Q}$ is a finite extension and hence algebraic. We wish to find all the algebraic integers in K.

Suppose that $\alpha = a + b\sqrt{d}$ is an algebraic integer, and let $\overline{\alpha} = a - b\sqrt{d}$ be its complex conjugate. Using some Galois theory, the minimal polynomial of α is

$$m(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - 2ax + a^2 - db^2.$$

We know that $m(x) \in \mathbb{Z}[x]$ by Theorem 1.2, so we must have $2a$, $a^2 - db^2 \in \mathbb{Z}$. Next, we have

$$4(a^2 - db^2) = (2a)^2 - d(2b)^2 \in \mathbb{Z},$$

so $d(2b)^2 \in \mathbb{Z}$. Then by a denominator argument, we find that $2b \in \mathbb{Z}$ as well since d is square-free.

Write $u = 2a$ and $v = 2b$ so that $a = u/2$ and $b = v/2$. We obtain

$$a^2 - db^2 = \left(\frac{u}{2}\right)^2 - d\left(\frac{v}{2}\right)^2 = \frac{u^2 - dv^2}{4} \in \mathbb{Z},$$

so $u^2 - dv^2 \equiv 0 \pmod 4$. We now consider what form α can take under a few cases. Note that the $d \equiv 0 \pmod 4$ case is impossible since d is square-free.

Case 1. If $d \equiv 1 \pmod 4$, then $u^2 \equiv v^2 \pmod 4$. Recall that the square of an even number is $0 \pmod 4$ and the square of an odd number is $1 \pmod 4$, so this is equivalent to $u \equiv v \pmod 2$. That is, we have $\alpha = a + b\sqrt{d} = (u/2) + (v/2)\sqrt{d}$ for u and v with the same parity.

Case 2. If $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$, then it can be shown that $u^2 - dv^2 \equiv 0 \pmod 4$ is equivalent to having $u \equiv v \equiv 0 \pmod 2$. This means that $\alpha = a' + b'\sqrt{d}$ for some $a', b' \in \mathbb{Z}$.

We leave it as an exercise to check that these conditions are also sufficient, which can be done by reversing the arguments above.

More generally, given a finite field extension $K/\mathbb{Q}$, we want to describe all the algebraic integers in K. This leads us to the following definitions.

Definition 1.3

We call a finite field extension K of $\mathbb{Q}$ a **number field**. For a number field K, we call

$$\mathcal{O}_K = \{\alpha \in K : \alpha \text{ an algebraic integer}\}$$

the **ring of integers** of K.

Obviously, we'll need to prove that $\mathcal{O}_K$ is indeed a ring (namely, a subring of $\mathbb{C}$). To do this, we'll define

$$\mathbb{A} = \{z \in \mathbb{C} : z \text{ an algebraic integer}\}$$

and show that $\mathbb{A}$ is a ring, which will imply that $\mathcal{O}_K = \mathbb{A} \cap K$ is a ring too.

Before that, let's move on to some more definitions. Recall that in Section 1.1, we wanted to work with

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$$

where $\alpha \in \mathbb{A}$ in order to do "linear algebra" over $\mathbb{Z}$. But $\mathbb{Z}$ is not a field, so we'll need something more general.

Definition 1.4

Let R be a ring. An **R-module** is an abelian group $(M, +)$ together with an operation $\cdot : R \times M \to M$ such that

(i) for all $m \in M$, we have $1m = m$;

(ii) for all $r_1, r_2 \in R$ and $m \in M$, we have $(r_1 + r_2)m = r_1m + r_2m$;

(iii) for all $r \in R$ and $m_1, m_2 \in M$, we have $r(m_1 + m_2) = rm_1 + rm_2$;

(iv) for all $r_1, r_2 \in R$ and $m \in M$, we have $(r_1r_2)m = r_1(r_2m)$.

We can think of the operation $\cdot : R \times M \to M$ as the "R-action on M". Note that if R is a field, then an R-module is the same as an R-vector space, so this definition indeed captures the essence of doing linear algebra. Let's go over a few examples of R-modules.

(1) Every ring R is an R-module over itself with operation $r \cdot m = rm$.

(2) If S is a subring of R, then R is an S-module with operation $s \cdot r = sr$.

(3) Thinking in the linear algebra setting, we can view $\mathbb{R}^n$ as an R-module for every ring R with operation $r \cdot [x_1, \ldots, x_n]^T = [rx_1, \ldots, rx_n]^T$.

(4) Let $R = \mathbb{Z}$ and let $(M, +)$ be an R-module. For $n \in \mathbb{N}$, observe that

$$\begin{aligned} n \cdot m &= (1 + \cdots + 1) \cdot m \\ &= 1 \cdot m + \cdots + 1 \cdot m \\ &= m + \cdots + m \\ &= nm. \end{aligned}$$

Similarly, we can show that $(-n) \cdot m = -(n \cdot m) = -nm$. Therefore, the only possible $\mathbb{Z}$-action on M is the one we expect, namely that of repeated addition. In particular, the $\mathbb{Z}$-module structure does not impose anything on M; it is just an abelian group.

We now do a quick crash course in module theory and list more definitions.

Definition 1.5

Let R be a ring, and let M be an R-module.

(1) We say that $N \subseteq M$ is an **R-submodule** of M if N is an R-module under the same operations as M. That is, N is an additive subgroup of M closed under the R-action.

(2) Let M_1 and M_2 be R-modules. Then $f : M_1 \to M_2$ is a **homomorphism** if
   (i) $f(m_1 + m_2) = f(m_1) + f(m_2)$ for all $m_1, m_2 \in M_1$;
   (ii) $f(rm) = rf(m)$ for all $r \in R$ and $m \in M_1$.
   If f is also bijective, then we call it an **isomorphism**.

(3) We say that M is **finitely generated** if there exists $m_1, \ldots, m_n \in M$ such that

$$M = Rm_1 + \cdots + Rm_n := \{r_1 m_1 + \cdots + r_n m_n : r_1, \ldots, r_n \in R\}.$$

For example, if we view R as an R-module over itself, then the R-submodules are precisely the ideals of R. Indeed, by definition, ideals are additive subgroups that are closed under multiplication by R. In this course, there is no need to specify left or right ideals because we assume that every ring is commutative and unital.

Let's move back to number theory! We give a definition that takes the idea of algebraic integers and generalizes it to arbitrary rings. Note that in this course, the notation $R \subseteq S$ means that R is a subring of S under the same operations.

Definition 1.6

Let $R \subseteq S$ be integral domains. We say that $\alpha \in S$ is **integral** over R if there exists a monic polynomial $f(x) \in R[x]$ such that $f(\alpha) = 0$.

If we take $R = \mathbb{Z}$ and $S = \mathbb{C}$, then being integral is the same as being an algebraic integer. All of these definitions are handy to know for a course in commutative algebra, but why are we moving in this direction? The following theorem gives us a nice characterization of being integral, which allows us to apply it to our number theory setting for algebraic integers.

Theorem 1.7

Let $R \subseteq S$ be integral domains. Then $\alpha \in S$ is integral over R if and only if $R[\alpha] = \{f(\alpha) : f(x) \in R[x]\}$ is finitely generated as an R-module.

Proof of Theorem 1.7.

($\Rightarrow$) Let $\alpha \in S$ be integral over R. Then we can write

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

for some $a_i \in R$, as α is the root of some monic polynomial over R. In particular, we have

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0,$$

so every element in $R[\alpha]$ can be written as a linear combination of elements from $\{1, \alpha, \ldots, \alpha^{n-1}\}$. In other words, $R[\alpha] = R + R\alpha + \cdots + R\alpha^{n-1}$ is finitely generated.

($\Leftarrow$) Since R is finitely generated, we can write it in the form

$$R[\alpha] = Rf_1(\alpha) + \cdots + Rf_n(\alpha)$$

for some polynomials $f_i(x) \in R[x]$. Take $N = \max_{1 \le i \le n}\{\deg f_i(x)\}$. Note that $\alpha^{N+1} \in R[\alpha]$, so we have

$$\alpha^{N+1} = r_1 f_1(\alpha) + \cdots + r_n f_n(\alpha)$$

for some $r_i \in R$. Next, consider the polynomial

$$g(x) = x^{N+1} - r_1 f_1(x) - \cdots - r_n f_n(x) \in R[x].$$

Note that $g(\alpha) = 0$ and $g(x)$ is monic by our choice of N, so we conclude that α is integral over R. □

As we have seen in a course in Galois theory, finding a polynomial $f(x) \in \mathbb{Z}[x]$ which has α as a root is generally a difficult task. Showing that $\mathbb{Z}[\alpha]$ is finitely generated is often easier than doing this!

For a number field K, we still haven't shown that $\mathcal{O}_K$ is a ring. We mentioned our approach before, which is to show that $\mathbb{A} = \{z \in \mathbb{C} : z \text{ an algebraic integer}\}$ is a subring of $\mathbb{C}$, which implies that $\mathcal{O}_K = \mathbb{A} \cap K$ is also a ring. Let's try to do this now with the machinery we have.

Theorem 1.8

The algebraic integers $\mathbb{A}$ form a subring of $\mathbb{C}$.

Proof of Theorem 1.8.

Let $\alpha, \beta \in \mathbb{A}$. By the subring test, it suffices to show that $\alpha - \beta$ and $\alpha\beta$ are elements of $\mathbb{A}$. By Theorem 1.7, we just need to show that $\mathbb{Z}[\alpha - \beta]$ and $\mathbb{Z}[\alpha\beta]$ are finitely generated $\mathbb{Z}$-modules.

We know that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated $\mathbb{Z}$-modules again by Theorem 1.7, so we can write $\mathbb{Z}[\alpha] = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$ and $\mathbb{Z}[\beta] = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_m$ for some $\alpha_i \in \mathbb{Z}[\alpha]$ and $\beta_j \in \mathbb{Z}[\beta]$. Then

$$\mathbb{Z}[\alpha, \beta] = \{f(\alpha, \beta) : f(x, y) \in \mathbb{Z}[x, y]\}$$

is also finitely generated as a $\mathbb{Z}$-module by $\{\alpha_i\beta_j : 1 \le i \le n, 1 \le j \le m\}$. We have that $\mathbb{Z}[\alpha - \beta]$ and $\mathbb{Z}[\alpha\beta]$ are $\mathbb{Z}$-submodules of the finitely generated $\mathbb{Z}$-module $\mathbb{Z}[\alpha, \beta]$. □

In our attempted argument above, we may have lost track of the goal. We see that $\mathbb{Z}[\alpha, \beta]$ is an extremely large $\mathbb{Z}$-module, and in fact, it is not true in general that a submodule of a finitely generated R-module is also finitely generated!

For example, take $R = \mathbb{Z}[x_1, x_2, \ldots]$. Then R is a finitely generated R-module since $R = R1$. However, consider the ideal $I = \langle x_1, x_2, \ldots \rangle$, which is a submodule of R as we discussed before. Then I is not finitely generated because any possible generating set would only give us finitely many indeterminates.

To get out of this mess, we need a new definition.

Definition 1.9

Let R be a ring. We say that R is **Noetherian** if every submodule (ideal) of R (as an R-module) is finitely generated.

Now, the submodules of $\mathbb{Z}$ are the most finitely generated we could possibly get since $\mathbb{Z}$ is a PID (namely, every submodule is generated by a single element), so $\mathbb{Z}$ is Noetherian. In particular, the following theorem is enough to rescue our proof of Theorem 1.8, so $\mathbb{A}$ is a ring and so is $\mathcal{O}_K$ for a number field K.

Theorem 1.10

Let R be a Noetherian ring, and let M be a finitely generated R-module. Then every submodule of M is also finitely generated.

We first make a reduction. Suppose that M is a finitely generated R-module with $M = R\alpha_1 + \cdots + R\alpha_n$ for some $\alpha_i \in M$. This can be "relabelled" with a surjective homomorphism $f : R^n \to M$ defined by $(r_1, \ldots, r_n) \mapsto r_1\alpha_1 + \cdots + r_n\alpha_n$. In particular, if $N \subseteq M$ is a submodule, then $f^{-1}(N) \subseteq R^n$. Moreover, provided that $f^{-1}(N)$ is finitely generated, say $f^{-1}(N) = R\beta_1 + \cdots + R\beta_n$ for some $\beta_i \in N$, then $N = Rf(\beta_1) + \cdots + Rf(\beta_n)$ is also finitely generated.

Proof of Theorem 1.10.

Due to the above reduction, we may assume that $M = R^n$. If $n = 1$, then since R is Noetherian, every submodule is finitely generated by definition. Next, assume the result holds for n and consider $M = R^{n+1}$.

Consider the projection homomorphism $\pi : R^{n+1} \to R$ given by

$$\pi(r_1, \ldots, r_{n+1}) = r_{n+1}.$$

Let N be a submodule of M, and consider the submodule

$$N_1 = \{(r_1, \ldots, r_{n+1}) \in N : r_{n+1} = 0\}.$$

This is isomorphic to a submodule of R^n by simply ignoring the last element, so N_1 is finitely generated by the inductive hypothesis. Moreover, $N_2 = \pi(N)$ is a submodule of R, which is finitely generated because R is Noetherian. Thus, we can write $N_1 = Rx_1 + \cdots + Rx_p$ for some $x_i \in N_1$ and $N_2 = R\pi(y_1) + \cdots + R\pi(y_q)$ for some $y_j \in N$.

Let $x \in N$. Then by applying π to x, we have

$$\pi(x) = r_1\pi(y_1) + \cdots + r_q\pi(y_q)$$

for some $r_1, \ldots, r_q \in R$. But π is a homomorphism, so

$$\pi(x - r_1y_1 - \cdots - r_qy_q) = 0.$$

This means that $x - r_1y_1 - \cdots - r_qy_q \in N_1$, so we can find $\tilde{r}_1, \ldots, \tilde{r}_p \in R$ such that

$$x - r_1y_1 - \cdots - r_qy_q = \tilde{r}_1x_1 + \cdots + \tilde{r}_px_p.$$

In particular, rearranging this gives us

$$x = r_1y_1 + \cdots + r_qy_q + \tilde{r}_1x_1 + \cdots + \tilde{r}_px_p,$$

so we deduce that $N = Ry_1 + \cdots + Ry_q + Rx_1 + \cdots + Rx_p$ is finitely generated. □

1.4 Additive Structure

Let K be a number field so that $[K:\mathbb{Q}] < \infty$. So far, it has been very useful to consider $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Let's investigate the $\mathbb{Z}$-module $(\mathcal{O}_K, +)$, throwing away the multiplicative structure.

Definition 1.11

Let R be a ring and M be an R-module.

(1) We say $B \subseteq M$ is **linearly independent** if for all $m_1, \dots, m_n \in B$, the dependence relation $r_1 m_1 + \cdots + r_n m_n = 0$ implies that $r_1 = \cdots = r_n = 0$.

(2) We say $B \subseteq M$ **spans** M if for all $x \in M$, there exist $b_1, \dots, b_n \in B$ and $r_1, \dots, r_n \in R$ such that

$$x = r_1 b_1 + \cdots + r_n b_n.$$

(3) We say $B \subseteq M$ is a **basis** for M if B is a linearly independent set that spans M.

(4) If M has a basis, we call it a **free** R-module. The (unique) size of a basis for M is called the **rank** of M, denoted $\operatorname{rank}(M)$.

Note that $B \subseteq M$ is a basis for M if and only if every $x \in M$ can be uniquely written as $x = r_1 b_1 + \cdots + r_n b_n$ for some $r_i \in R$ and $b_i \in B$. In particular, M is free with $\operatorname{rank}(M) = n < \infty$ if and only if $M \cong R^n$ via the mapping $(r_1, \dots, r_n) \leftrightarrow r_1 b_1 + \cdots + r_n b_n$, where $B = \{b_1, \dots, b_n\}$ is a basis. We give some examples below.

(1) Let $R = \mathbb{Z}$ and $M = \mathbb{Z}[x]$. Then M has basis $B = \{1, x, x^2, \dots\}$, so M is free but not finitely generated.

(2) Let $R = \mathbb{Z}$ and $M = \mathbb{Z}_2$. Note that $2 \cdot 1 = 0$, but $2 \neq 0$ in R. This means that the only linearly independent set is $\varnothing$, and since this is the only candidate for a basis, it follows that M is not free (but it is certainly finitely generated).

(3) **Warning!** Let $R = \mathbb{Z}$, $M = \mathbb{Z} \times \mathbb{Z}$, and $N = \mathbb{Z} \times 2\mathbb{Z}$. Note that M is free with basis $B_1 = \{(1,0), (0,1)\}$ and has $\operatorname{rank}(M) = 2$. Similarly, N is free with basis $B_2 = \{(1,0), (0,2)\}$ and has $\operatorname{rank}(N) = 2$. However, we have $M \neq N$! So unlike the linear algebra over fields we saw in previous courses where every linearly independent set with size equal to the rank will also span, this is not the case here.

We now steal some facts from commutative algebra without proof.

Proposition 1.12

Let R be a PID. Let M be a free R-module with $\operatorname{rank}(M) = n < \infty$.

(1) Let $N \subseteq M$ be a submodule. Then N is free with $\operatorname{rank}(N) \leq n$.

(2) Any maximal linearly independent subset of M has n elements.

However, as we saw from the example above, being a maximal linearly independent subset of M does not imply that it must span M.

Let K be a number field with $[K:\mathbb{Q}] = n$. Our goal is to find an embedding (injective ring homomorphism) $\varphi : \mathcal{O}_K \to \mathbb{Z}^n$ such that $\operatorname{rank}(\varphi(\mathcal{O}_K)) = n$. This will tell us that $\mathcal{O}_K \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules. In particular, $(\mathcal{O}_K, +)$ is a free $\mathbb{Z}$-module of rank n. This leads us to the following definition.

Definition 1.13

Let M be a free $\mathbb{Z}$-module. A basis for M is called an **integral basis**.

In other words, an integral basis is just a basis in the case that $R = \mathbb{Z}$.

We now give the tools of the trade for algebraic number theory. These are not the usual definitions given in the literature, but we do it this way to motivate why they are called norms and traces.

Definition 1.14

Let K be a number field with $[K : \mathbb{Q}] = n$. Let $\alpha \in K$ and let $T_\alpha : K \to K$ defined by $T_\alpha(x) = \alpha x$ (which is viewed as a $\mathbb{Q}$-linear transformation).

(1) The **trace** of α relative to $K/\mathbb{Q}$ is defined to be $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) := \mathrm{Tr}(T_\alpha)$.

(2) The **norm** of α relative to $K/\mathbb{Q}$ is defined to be $N_{K/\mathbb{Q}}(\alpha) := \det(T_\alpha)$.

Since T_α is a $\mathbb{Q}$-linear operator, the entries of any matrix representation must be rational. In particular, we have $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$.

Investigation 1. Let K be a number field of degree $[K : \mathbb{Q}] = n$, and let $\alpha \in K$. Let's see if we can find some properties of the trace and norm in the special case that $K = \mathbb{Q}(\alpha)$.

Let β be a basis for $K/\mathbb{Q}$ and let $A = [T_\alpha]_\beta$, the matrix of T_α relative to β. Let

$$f(x) = \det(xI - A) \in \mathbb{Q}[x]$$

be the characteristic polynomial of A, and let $p(x) \in \mathbb{Q}[x]$ be the minimal polynomial of A. That is, $p(x)$ is the unique monic irreducible generating the ideal

$$\langle p(x) \rangle = \{g(x) \in \mathbb{Q}[x] : g(T_\alpha) = 0\}.$$

Note that if $g(x) \in \mathbb{Q}[x]$ and $v \in K$, then

$$g(T_\alpha)(v) = g(\alpha)v$$

since $T_\alpha^m(v) = \alpha^m v$ for all $m \in \mathbb{N}$. In particular, we have $g(T_\alpha) = 0$ if and only if $g(\alpha) = 0$, so $p(x)$ is also the minimal polynomial for α over $\mathbb{Q}$. Recall that Cayley-Hamilton states that an operator makes its characteristic polynomial vanish, so $f(\alpha) = f(T_\alpha) = 0$ and hence $p(x) \mid f(x)$.

Now, we have $\deg f(x) = [K : \mathbb{Q}] = n$ and $\deg p(x) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ since $K = \mathbb{Q}(\alpha)$. Since $f(x)$ and $p(x)$ are both monic, it turns out that $f(x) = p(x)$ in this special case. With this in mind, we are now equipped with several different ways to compute the trace and norm of α relative to $K/\mathbb{Q}$.

Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α (that is, the roots of $p(x)$ in $\mathbb{C}$). Recall that the roots of the characteristic polynomial of an operator are the eigenvalues λ_i (with multiplicity). Since $f(x) = p(x)$, we have $\lambda_i = \alpha_i$ and thus

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}(A) = \sum_{i=1}^{n} \lambda_i = \sum_{i=1}^{n} \alpha_i,$$
$$N_{K/\mathbb{Q}}(\alpha) = \det(A) = \prod_{i=1}^{n} \lambda_i = \prod_{i=1}^{n} \alpha_i.$$

Moreover, if we explicitly expand out the terms in $p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$, then we obtain

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \alpha_i = -[x^{n-1}]p(x),$$
$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \alpha_i = (-1)^n [x^0]p(x) = (-1)^n p(0),$$

where $[x^i]p(x)$ denotes the coefficient corresponding to the x^i term in $p(x)$.

Finally, recall from Galois theory that the embeddings of $K = \mathbb{Q}(\alpha)$ into $\mathbb{C}$ must fix $\mathbb{Q}$ and are completely determined by their action on α, which must be sent to another conjugate of α. Writing the embeddings as $\sigma_i(\alpha) = \alpha_i$ for $i = 1, \ldots, n$, we also see that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \sigma_i(\alpha),$$
$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \alpha_i = \prod_{i=1}^{n} \sigma_i(\alpha).$$

The condition that $K = \mathbb{Q}(\alpha)$ was very restrictive because this does not hold for every $\alpha \in K$. Let's now try to compute the trace and norm in the general case without this assumption. We will use the following lemma, whose proof is quite technical.

Lemma 1.15

Let K be a number field with $[K : \mathbb{Q}] = n$, and let $\alpha \in K$ be such that $[K : \mathbb{Q}(\alpha)] = m$. Consider the map $T_\alpha : K \to K$ given by

$$T_\alpha(x) = \alpha x.$$

Let $f(x) \in \mathbb{Q}[x]$ be the characteristic polynomial of T_α and let $p(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α. Then we have $f(x) = p(x)^m$.

Note that by our investigation above, we can also view $p(x)$ as the minimal polynomial of T_α restricted to $\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$. Moreover, when $m = 1$, we have $K = \mathbb{Q}(\alpha)$ and we recover our special case.

Proof of Lemma 1.15.

Let $\beta = \{y_1, \ldots, y_d\}$ be a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$, and let $\beta' = \{z_1, \ldots, z_m\}$ be a basis for K over $\mathbb{Q}(\alpha)$. By the tower theorem, which states that algebraic field extensions are transitive, we have that $\{y_i z_j : 1 \le i \le d, 1 \le j \le m\}$ is a basis for K over $\mathbb{Q}$.

Let $A = [T_\alpha]_\beta \in M_d(\mathbb{Q})$, where we consider the restriction $T_\alpha : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$. Then we have

$$\alpha y_i = T_\alpha(y_i) = A[y_i]_\beta \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_d \end{bmatrix} = Ae_i \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_d \end{bmatrix} = \sum_{k=1}^{d} a_{ki} y_k.$$

This implies that

$$\alpha y_i z_j = \sum_{k=1}^{d} a_{ki} y_k z_j.$$

Consider now the ordered basis

$$\gamma = (y_1 z_1, \ldots, y_d z_1, y_1 z_2, \ldots, y_d z_2, \ldots, y_1 z_m, \ldots, y_d z_m).$$

We leave it as an exercise to verify that

$$[T_\alpha]_\gamma = \mathrm{diag}(A, A, \ldots, A) = \begin{bmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{bmatrix}.$$

It follows from our investigation that $f(x) = \det(xI - A)^m = p(x)^m$. □

Investigation 2. Equipped with this lemma, let's look at the general case. Let K be a number field with $[K:\mathbb{Q}] = n$, and let $\alpha \in K$ satisfy $[K:\mathbb{Q}(\alpha)] = m$. Let λ_i denote the eigenvalues of $f(x) \in \mathbb{Q}[x]$, the characteristic polynomial of T_α. When $p(x) \in \mathbb{Q}[x]$ is the minimal polynomial of α over $\mathbb{Q}$, we know by Lemma 1.15 that $f(x) = p(x)^m$, so the eigenvalues of $f(x)$ are the eigenvalues of $p(x)$ each repeated m times. Thus, we obtain

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}(T_\alpha) = \sum_{i=1}^{n} \lambda_i = m(\alpha_1 + \cdots + \alpha_{n/m}),$$

where $n/m = [\mathbb{Q}(\alpha):\mathbb{Q}]$ by the tower theorem. Similarly, we have

$$N_{K/\mathbb{Q}}(\alpha) = (\alpha_1 \alpha_2 \cdots \alpha_{n/m})^m.$$

As before, let $\alpha = \alpha_1, \ldots, \alpha_{n/m}$ be the conjugates of α, which are the roots of $p(x)$ in $\mathbb{C}$. The embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$ are given by $\sigma_i(\alpha) = \alpha_i$ for $i = 1, \ldots, n/m$. Then by **A1-4**, each σ_i extends to exactly $m = [K:\mathbb{Q}(\alpha)]$ embeddings of K into $\mathbb{C}$. If $\rho_1, \ldots, \rho_n$ are the embeddings of K into $\mathbb{C}$, then

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = m(\sigma_1(\alpha) + \cdots + \sigma_{n/m}(\alpha)) = \rho_1(\alpha) + \cdots + \rho_n(\alpha),$$

since for each $i = 1, \ldots, n/m$, exactly m of the ρ_i are extensions of σ_i. Similarly, we have

$$N_{K/\mathbb{Q}}(\alpha) = \rho_1(\alpha) \cdots \rho_n(\alpha) = (\sigma_1(\alpha) \cdots \sigma_{n/m}(\alpha))^m.$$

Let's investigate some more properties of norm and trace. Suppose that $[K:\mathbb{Q}] = n$. Let $\alpha, \beta \in K$ and $q \in \mathbb{Q}$. We'll do a reset of notation and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$.

(1) Looking at trace, we have

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}(q\alpha + \beta) &= \sigma_1(q\alpha + \beta) + \cdots + \sigma_n(q\alpha + \beta) \\ &= q\sigma_1(\alpha) + \sigma_1(\beta) + \cdots + q\sigma_n(\alpha) + \sigma_n(\beta) \\ &= q\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + \mathrm{Tr}_{K/\mathbb{Q}}(\beta),\end{aligned}$$

where the second equality is because the embeddings fix $\mathbb{Q}$. In particular, trace is a $\mathbb{Q}$-linear map!

(2) We also have that

$$N_{K/\mathbb{Q}}(q\alpha\beta) = \prod_{i=1}^{n} \sigma_i(q\alpha\beta) = \prod_{i=1}^{n} q\sigma_i(\alpha)\sigma_i(\beta) = q^n N_{K/\mathbb{Q}}(\alpha) N_{K/\mathbb{Q}}(\beta).$$

So norm doesn't behave too well with respect to scalar multiplication, but it is a multiplicative map.

(3) Finally, suppose that $\alpha \in \mathcal{O}_K$. Note that the $\sigma_i(\alpha)$ are also roots of the minimal polynomial $p(x)$ of α. In particular, we have $\sigma_i(\alpha) \in \mathcal{O}_K$, and hence

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

Similarly, we see that $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

To end our discussion on traces and norms, let's compute them on a simple example. Consider $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is square-free. Let $\alpha = a + b\sqrt{d}$ with $b \neq 0$. Then α has the conjugate $a - b\sqrt{d}$, so we have

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) &= (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a, \\ N_{K/\mathbb{Q}}(\alpha) &= (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.\end{aligned}$$

Recall from ring theory that an element $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if $a^2 - db^2 = \pm 1$. In fact, we can prove something more general. Let K be a number field, let $R = \mathcal{O}_K$ be its ring of integers, and let $\alpha \in R$. We leave it as an exercise to show that $\alpha \in R^\times$ if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$, where $R^\times$ denotes the group of units.

Let's not lose track of why we moved towards discussing traces and norms. Recall that we were discussing the additive structure of $\mathcal{O}_K$ for a number field K with $[K:\mathbb{Q}] = n$. Our aim was to prove that $(\mathcal{O}_K, +) \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules so that $(\mathcal{O}_K, +)$ is a free $\mathbb{Z}$-module of rank n. Trace turns out to be the star of the show here!

Theorem 1.16

Let K be a number field with degree $[K:\mathbb{Q}] = n$. Then $(\mathcal{O}_K, +) \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules. In particular, $(\mathcal{O}_K, +)$ is a free $\mathbb{Z}$-module of rank n.

Proof of Theorem 1.16.

Let $\{x_1, \dots, x_n\}$ be a $\mathbb{Q}$-basis for K. By part (b) of **A1-1**, we may assume without loss of generality that $x_i \in \mathcal{O}_K$. Define a map $\varphi : K \to \mathbb{Q}^n$ by

$$\varphi(x) = (\mathrm{Tr}_{K/\mathbb{Q}}(xx_1), \dots, \mathrm{Tr}_{K/\mathbb{Q}}(xx_n)).$$

Note that φ is $\mathbb{Q}$-linear because we showed earlier that $\mathrm{Tr}_{K/\mathbb{Q}}$ is a $\mathbb{Q}$-linear map.

Let's look for the kernel of φ. Note that if $\varphi(x) = (0, \dots, 0)$, then $\mathrm{Tr}_{K/\mathbb{Q}}(xx_i) = 0$ for all $i = 1, \dots, n$. But this implies that $\mathrm{Tr}_{K/\mathbb{Q}}(xy) = 0$ for all $y \in K$ since the x_i form a $\mathbb{Q}$-basis for K. Moreover, if $x \neq 0$, then

$$\mathrm{Tr}_{K/\mathbb{Q}}(xx^{-1}) = \mathrm{Tr}_{K/\mathbb{Q}}(1) = n \neq 0.$$

Thus, $\ker \varphi = \{0\}$ and φ is an injective linear transformation.

Next, we see that $\mathcal{O}_K \cong \varphi(\mathcal{O}_K) \subseteq \mathbb{Z}^n$ because we showed before that the trace of an algebraic integer was in $\mathbb{Z}$. So $\mathcal{O}_K$ is isomorphic to a $\mathbb{Z}$-submodule of $\mathbb{Z}^n$. By Proposition 1.12, it follows that $\mathcal{O}_K$ is free with $\mathrm{rank}(\mathcal{O}_K) \leq n$. But $\{x_1, \dots, x_n\} \subseteq \mathcal{O}_K$ is linearly independent over $\mathbb{Q}$ and hence linearly independent over $\mathbb{Z}$ as well. This gives us $\mathrm{rank}(\mathcal{O}_K) \geq n$ and thus $\mathrm{rank}(\mathcal{O}_K) = n$, as desired. □

This gives us the existence of an integral basis for $\mathcal{O}_K$. The existence of this integral basis allows us to prove an avalanche of corollaries which we'll be able to make use of later.

Warning! Note that for a number field K, a $\mathbb{Q}$-basis consisting only of algebraic integers is not necessarily an integral basis for $\mathcal{O}_K$. For example, let $K = \mathbb{Q}(\sqrt{5})$. Then $\{1, \sqrt{5}\} \subseteq \mathbb{Q}(\sqrt{5})$ is a $\mathbb{Q}$-basis of algebraic integers for $\mathbb{Q}(\sqrt{5})$, but is not an integral basis for $\mathcal{O}_K$ since $\frac{1}{2}(1 + \sqrt{5}) \in \mathcal{O}_K$.

Corollary 1.17

Let K be a number field with $[K:\mathbb{Q}] = n$, and let $R = \mathcal{O}_K$ be its ring of integers. If I is a nonzero ideal of R, then $(I, +) \cong \mathbb{Z}^n$.

Proof of Corollary 1.17.

Let $\{x_1, \dots, x_n\}$ be an integral basis for $R = \mathcal{O}_K$, which exists due to Theorem 1.16. Take $a \in I$ such that $a \neq 0$. We leave it as an exercise to show that $\{ax_1, \dots, ax_n\} \subseteq I$ is linearly independent over $\mathbb{Z}$, so $\mathrm{rank}(I) \geq n$. Then by Proposition 1.12, we have $\mathrm{rank}(I) \leq n$ and thus $\mathrm{rank}(I) = n$. □

We steal one more fact from commutative algebra. This is a consequence of the structure theorem of finitely generated modules over PIDs, and we know that $\mathbb{Z}$ is a PID.

Proposition 1.18

If M is a finitely generated $\mathbb{Z}$-module, then $M \cong \mathbb{Z}^k \times T$ as $\mathbb{Z}$-modules, where T is finite. (We call $\mathbb{Z}^k$ the free part and T the torsion part.)

We make use this fact to prove the following corollary.

Corollary 1.19

Let K be a number field with degree $[K : \mathbb{Q}] = n$, and let $R = \mathcal{O}_K$ be its ring of integers. If I is a nonzero ideal of R, then R/I is finite.

Proof of Corollary 1.19.

By Proposition 1.18, we have $R/I \cong \mathbb{Z}^k \times T$ as $\mathbb{Z}$-modules, where T is finite. It is enough to show that R/I has no elements of infinite order, as this will imply that $R/I \cong T$ is finite. Suppose otherwise, and let $\bar{x} = x + I \in R/I$ be an element of infinite order. Let $\{x_1, \dots, x_n\}$ be an integral basis for I, which exists by Corollary 1.17. Note that $x \notin I$ for otherwise $\bar{x} = \bar{0}$, which has finite order. In particular, we see that x is distinct from the x_i. We claim that $\{x, x_1, \dots, x_n\}$ is linearly independent over $\mathbb{Z}$. Consider the relation

$$cx + \sum_{i=1}^{n} c_i x_i = 0.$$

for some $c, c_i \in \mathbb{Z}$. Since $\sum_{i=1}^{n} c_i x_i \in I$, this gives us $c\bar{x} = \bar{0}$, and thus $c = 0$ since $\bar{x}$ has infinite order. Then the linear independence of $\{x_1, \dots, x_n\}$ over $\mathbb{Z}$ implies that $c_1 = \cdots = c_n = 0$, so $\{x, x_1, \dots, x_n\}$ is linearly independent over $\mathbb{Z}$. But this contradicts the fact that R has rank n, so the result follows. □

We prove two more easy but important corollaries.

Corollary 1.20

Let K be a number field with $[K : \mathbb{Q}] = n$ and let $R = \mathcal{O}_K$. Every nonzero prime ideal of R is maximal.

Proof of Corollary 1.20.

Let P be a prime ideal. Then R/P is an integral domain, and by Corollary 1.19, it is finite. A finite integral domain is a field, which implies that P must be maximal. □

Corollary 1.21

Let K be a number field with $[K : \mathbb{Q}] = n$ and let $R = \mathcal{O}_K$. Then R is Noetherian.

Proof of Corollary 1.21.

Let I be an ideal of R. Then I is a free $\mathbb{Z}$-module with finite rank n by Corollary 1.17, so I is a finitely generated $\mathbb{Z}$-module by using the integral basis as a generating set. Since $\mathbb{Z} \subseteq R$, it follows that I is also a finitely generated R-module. □

2 Discriminants

2.1 Elementary Properties

Let K be a number with $[K:\mathbb{Q}] = n$ and consider its ring of integers $R = \mathcal{O}_K$. Given $\{v_1, \ldots, v_n\} \subseteq R$, we want to find a way to discriminate whether or not $\{v_1, \ldots, v_n\}$ is an integral basis for R. This leads us to the notion of the discriminant.

Definition 2.1

Let K be a number field with $[K:\mathbb{Q}] = n$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. The **discriminant** of $\{a_1, \ldots, a_n\} \subseteq K$ is

$$\operatorname{disc}(a_1, \ldots, a_n) = \det\left[\sigma_i(a_j)\right]^2.$$

In the matrix $[\sigma_i(a_j)]$ above, the rows are encoded by the embeddings σ_i and the columns are encoded by the elements a_j. Now, let's investigate some properties of the discriminant.

(1) The discriminant is independent of the choice of ordering for both the embeddings σ_i and the elements a_j. This is because squaring the determinant kills any negatives obtained by flipping rows or columns.

(2) Let $B = [\sigma_i(a_j)]$ and $A = [\sigma_j(a_i)] = B^T$. Taking the transpose leaves the determinant unchanged, so

$$\operatorname{disc}(a_1, \ldots, a_n) = \det(AB).$$

Now, observe that the (i,j)-th entry of AB is

$$\begin{bmatrix} \sigma_1(a_i) \\ \sigma_2(a_i) \\ \vdots \\ \sigma_n(a_i) \end{bmatrix} \cdot \begin{bmatrix} \sigma_1(a_j) \\ \sigma_2(a_j) \\ \vdots \\ \sigma_n(a_j) \end{bmatrix} = \sum_{k=1}^{n} \sigma_k(a_i a_j) = \operatorname{Tr}_{K/\mathbb{Q}}(a_i a_j).$$

Thus, we obtain an equivalent definition of the discriminant seen in some texts, which is given by

$$\operatorname{disc}(a_1, \ldots, a_n) = \det\left[\operatorname{Tr}_{K/\mathbb{Q}}(a_i a_j)\right] \in \mathbb{Q}.$$

Moreover, if we also assume that $a_1, \ldots, a_n \in \mathcal{O}_K$, then

$$\operatorname{disc}(a_1, \ldots, a_n) \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}.$$

(3) Let $v, w \in K^n$ and $A \in M_n(\mathbb{Q})$ be such that $Av = w$. Observe that

$$A \begin{bmatrix} \sigma_i(v_1) \\ \vdots \\ \sigma_i(v_n) \end{bmatrix} = \begin{bmatrix} \sigma_i(a_{11}v_1 + \cdots + a_{1n}v_n) \\ \vdots \\ \sigma_i(a_{n1}v_1 + \cdots + a_{nn}v_n) \end{bmatrix} = \begin{bmatrix} \sigma_i(w_1) \\ \vdots \\ \sigma_i(w_n) \end{bmatrix}.$$

Therefore, we deduce that

$$A \begin{bmatrix} \sigma_1(v_1) & \cdots & \sigma_n(v_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(v_n) & \cdots & \sigma_n(v_n) \end{bmatrix} = \begin{bmatrix} \sigma_1(w_1) & \cdots & \sigma_n(w_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_n(w_n) \end{bmatrix}.$$

The matrices above are the transposes of the matrices in the definition of the discriminant, since the columns encode the embeddings and the rows encode the elements this time. Taking squared determinants gives the nice relationship

$$(\det A)^2 \cdot \operatorname{disc}(v) = \operatorname{disc}(w).$$

(4) Let $\{v_1, \dots, v_n\} \subseteq \mathcal{O}_K$ be an integral basis. Suppose that $\{w_1, \dots, w_n\} \subseteq \mathcal{O}_K$. Then for all $i = 1, \dots, n$, there must exist some $c_{ij} \in \mathbb{Z}$ such that

$$w_i = c_{i1}v_1 + \cdots + c_{in}v_n.$$

Then we can write $w = Cv$ where $C = [c_{ij}]$, which yields

$$\operatorname{disc}(w) = (\det C)^2 \cdot \operatorname{disc}(v).$$

Denoting the integral basis by $\beta = \{v_1, \dots, v_n\}$ and defining the map $T : \mathcal{O}_K \to \mathcal{O}_K$ by $T(v_i) = w_i$ (which is a $\mathbb{Z}$-linear homomorphism), we obtain

$$[T]_\beta = \Big[[T(v_1)]_\beta \ \cdots \ [T(v_n)]_\beta \Big] = \Big[[w_1]_\beta \ \cdots \ [w_n]_\beta \Big] = C^T.$$

(5) Let $A \in M_n(\mathbb{Z})$. If A is invertible, then

$$A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A),$$

where $\operatorname{adj}(A)$ denotes the adjugate of A. In particular, we have $\operatorname{adj}(A) \in M_n(\mathbb{Z})$, so $A^{-1} \in M_n(\mathbb{Z})$ if and only if $\det(A) \in \{\pm 1\}$.

(6) Let $\{a_1, \dots, a_n\} \subseteq K$ and consider the dependence relation

$$c_1a_1 + \cdots + c_na_n = 0$$

for some $c_i \in \mathbb{Q}$ which are not all zero. Then we have

$$c_1\sigma_i(a_1) + \cdots + c_n\sigma_i(a_n) = 0$$

for all $i = 1, \dots, n$, which implies that the columns of $[\sigma_i(a_j)]$ are linearly dependent. Hence, we obtain

$$\operatorname{disc}(a_1, \dots, a_n) = \det [\sigma_i(a_j)]^2 = 0.$$

We leave it as an exercise to verify that the converse holds. That is, $\{a_1, \dots, a_n\} \subseteq K$ is linearly dependent if and only if $\operatorname{disc}(a_1, \dots, a_n) = 0$.

(7) Let $\{v_1, \dots, v_n\}, \{w_1, \dots, w_n\} \subseteq \mathcal{O}_K$. If $\operatorname{disc}(v) = \operatorname{disc}(w)$ and $\{v_1, \dots, v_n\}$ is an integral basis, then we have $Cv = w$ for some $C \in M_n(\mathbb{Z})$ by (4). Then we have

$$(\det C)^2 \cdot \operatorname{disc}(v) = \operatorname{disc}(w),$$

which implies that $(\det C)^2 = 1$ since $\{v_1, \dots, v_n\}$ is an integral basis and hence $\operatorname{disc}(v) = \operatorname{disc}(w) \neq 0$. By (5), it follows that C is invertible with $C^{-1} \in M_n(\mathbb{Z})$. Then C^T is also invertible with integer inverse, which implies that the map $T : \mathcal{O}_K \to \mathcal{O}_K$ given by $T(v_i) = w_i$ is an invertible $\mathbb{Z}$-linear map; in other words, it is an isomorphism! Hence, $\{w_1, \dots, w_n\}$ is also an integral basis.

Conversely, if $\{v_1, \dots, v_n\}, \{w_1, \dots, w_n\} \subseteq \mathcal{O}_K$ are both integral bases, then $Av = w$ and $Bw = v$ for some $A, B \in M_n(\mathbb{Z})$. Then we have

$$(\det A)^2 \cdot \operatorname{disc}(v) = \operatorname{disc}(w),$$
$$(\det B)^2 \cdot \operatorname{disc}(w) = \operatorname{disc}(v),$$

which gives us $\operatorname{disc}(w) \mid \operatorname{disc}(v)$ and $\operatorname{disc}(v) \mid \operatorname{disc}(w)$ since $\det(A), \det(B) \in \mathbb{Z}$. Moreover, they have the same sign, so $\operatorname{disc}(v) = \operatorname{disc}(w)$.

In summary, given an integral basis $\{v_1, \dots, v_n\} \subseteq \mathcal{O}_K$, another subset $\{w_1, \dots, w_n\} \subseteq \mathcal{O}_K$ is an integral basis for $\mathcal{O}_K$ if and only if $\operatorname{disc}(v) = \operatorname{disc}(w)$.

2.2 Discriminant of a Number Field

Let K be a number field with degree $[K:\mathbb{Q}] = n$. Due to (7) above, every integral basis for $\mathcal{O}_K$ has the same discriminant. This motivates the following definition.

Definition 2.2

Let K be a number field with degree $[K:\mathbb{Q}] = n$, and let $\{v_1, \dots, v_n\}$ be an integral basis for $\mathcal{O}_K$. The **discriminant** of K is

$$\operatorname{disc}(K) := \operatorname{disc}(v_1, \dots, v_n).$$

Let's take a number field we've already worked with before. Let $d \neq 1$ be squarefree and consider $K = \mathbb{Q}(\sqrt{d})$. We saw in the beginning of Section 1.3 that the algebraic integers in K took different forms depending on the choice of d.

(1) If $d \equiv 1 \pmod 4$, then $\{1, \frac{1+\sqrt{d}}{2}\}$ is an integral basis for $\mathcal{O}_K$. The discriminant of K is

$$\operatorname{disc}(K) = \det \begin{bmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{bmatrix}^2 = \left(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2} \right)^2 = (-\sqrt{d})^2 = d.$$

(2) If $d \equiv 2, 3 \pmod 4$, then $\{1, \sqrt{d}\}$ is an integral basis for $\mathcal{O}_K$. The discriminant of K is

$$\operatorname{disc}(K) = \det \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix}^2 = 4d.$$

2.3 Computational Considerations

The reason why we could compute the discriminant so easily in the above example is because we already knew what an integral basis for $\mathcal{O}_K$ was. However, finding an integral basis in general is a difficult task. Therefore, we should consider alternative ways of computing the discriminant.

Definition 2.3

Let $p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \in \mathbb{C}[x]$. The **discriminant** of $p(x)$ is

$$\operatorname{disc}(p(x)) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

It is not hard to verify that the discriminant of a monic quadratic is

$$\operatorname{disc}(x^2 + bx + c) = b^2 - 4c,$$

and the discriminant of a depressed cubic is

$$\operatorname{disc}(x^3 + bx + c) = -4b^3 - 27c^2.$$

Note that a general monic cubic $x^3 + ax^2 + bx + c$ can be converted into a depressed cubic by making the substitution $x \mapsto x - \frac{a}{3}$ to eliminate the x^2 term. The discriminant remains unchanged because the linear shifts are cancelled out by the $\alpha_i - \alpha_j$ terms.

We give another definition of the discriminant for simple extensions.

Definition 2.4

Let $\alpha \in \mathbb{C}$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Then the **discriminant** of α is

$$\operatorname{disc}(\alpha) := \operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}).$$

Let's jump into another investigation, this one much shorter than the last.

(1) Let $\alpha \in \mathcal{O}_K$ with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an integral basis for $\mathbb{Z}[\alpha]$. This particular basis is often called a **power basis**.

(2) Let $\alpha \in \mathcal{O}_K$. Set $K = \mathbb{Q}(\alpha)$ and suppose that $[K : \mathbb{Q}] = n$. Then we have

$$\operatorname{disc}(\alpha) = \det \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \operatorname{disc}(p(x)),$$

where $p(x)$ is the minimal polynomial of α. Here, we got a Vandermonde matrix squared!

(3) Let $\alpha \in \mathcal{O}_K$. Set $K = \mathbb{Q}(\alpha)$ and suppose that $[K : \mathbb{Q}] = n$. Let $\{v_1, \ldots, v_n\}$ be an integral basis for $\mathcal{O}_K$. Then for some $A \in M_n(\mathbb{Z})$, we have

$$\begin{bmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{bmatrix} = A \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}.$$

Then we deduce that

$$\operatorname{disc}(\alpha) = (\det A)^2 \cdot \operatorname{disc}(K) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \operatorname{disc}(K).$$

The last equality follows from **A2-4**, noting that $\mathcal{O}_K \cong \mathbb{Z}^n$ and $\mathbb{Z}[\alpha]$ is a submodule of $\mathcal{O}_K$ of rank n. In particular, if $\operatorname{disc}(\alpha)$ is squarefree, then we must have $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Suppose that $\alpha \in \mathbb{C}$ is a root of $p(x) = x^3 + x + 1$, which is irreducible by the rational roots theorem. Then

$$\operatorname{disc}(\alpha) = -4 - 27 = -31$$

is squarefree, so if $K = \mathbb{Q}(\alpha)$, then $\mathcal{O}_K = \mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Z}\}$.

In this spirit of this course, let's do some more investigation. Let $\alpha \in \mathbb{C}$ such that $K = \mathbb{Q}(\alpha)$, and suppose that $[K : \mathbb{Q}] = n$. Let $p(x)$ be the minimal polynomial of α over $\mathbb{Q}$, and let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates. Then we have $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, and its derivative is

$$p'(x) = \sum_{i=1}^{n} (x - \alpha_1) \cdots (x - \alpha_{i-1})(x - \alpha_{i+1}) \cdots (x - \alpha_n).$$

Substituting $x = \alpha_i$ gives

$$p'(\alpha_i) = (\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \cdots (\alpha_i - \alpha_n)$$

because all terms with $x - \alpha_i$ vanish. Looking at the norm of $p'(\alpha)$ (which is legal because $\alpha \in K$), we have

$$\begin{aligned} N_{K/\mathbb{Q}}(p'(\alpha)) &= \prod_{r=1}^{n} \sigma_r(p'(\alpha)) = \prod_{r=1}^{n} p'(\sigma_r(\alpha)) = \prod_{r=1}^{n} p'(\alpha_r) \\ &= \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}} \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} \operatorname{disc}(p(x)) = (-1)^{n(n-1)/2} \operatorname{disc}(\alpha). \end{aligned}$$

The second equality follows because the embeddings σ_i permute the roots and fix $\mathbb{Q}$. The fourth equality follows from our equation for $p'(\alpha_i)$ above, and the fifth equality comes from considering the pairs in the order $i > j$ and pulling out a -1 from each of them. Thus, one other way to compute the discriminant of α is

$$\operatorname{disc}(\alpha) = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(p'(\alpha)).$$

If all else fails, we give one more way of computing discriminants.

Definition 2.5

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + \cdots + b_1 x + b_0$ be polynomials in $\mathbb{C}[x]$. The **resultant** of $f(x)$ and $g(x)$ is defined to be

$$\operatorname{Res}(f(x), g(x)) := \det \left[\begin{array}{ccccc} a_n & a_{n_1} & \cdots & & \\ 0 & a_n & a_{n-1} & \cdots & \\ 0 & 0 & a_n & a_{n-1} & \cdots \\ \hline b_m & b_{m_1} & \cdots & & \\ 0 & b_m & b_{m-1} & \cdots & \\ 0 & 0 & b_m & b_{m-1} & \cdots \end{array}\right] \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} n \text{ rows} \end{array}$$

where we add zeroes at the end of each row if we run out of coefficients, and we ensure that the matrix is $(n+m) \times (n+m)$.

For a concrete example, we have

$$\operatorname{Res}(x^3 + x + 2, x^2 + 4x - 1) = \det \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 1 & 2 \\ 1 & 4 & -1 & 0 & 0 \\ 0 & 1 & 4 & -1 & 0 \\ 0 & 0 & 1 & 4 & -1 \end{bmatrix}.$$

Here, we have $n = 3$ and $m = 2$. The first two rows correspond to the coefficients of $x^3 + x + 2$ and the last three rows correspond to the coefficients of $x^2 + 4x - 1$.

The following proposition relates the resultant to discriminants. We didn't prove it in class, but this video by Professor Yuly Billig provides a nice proof of it.

Proposition 2.6

Let K be a number field with degree $[K : \mathbb{Q}] = n$. Suppose that $\alpha \in \mathcal{O}_K$ is such that $K = \mathbb{Q}(\alpha)$, and let $p(x)$ be the minimal polynomial of α. Then we have

$$\operatorname{disc}(\alpha) = (-1)^{n(n-1)/2} \operatorname{Res}(p(x), p'(x)).$$

We give one example of this. Suppose $\alpha \in \mathbb{C}$ is a root of $p(x) = x^3 - x^2 - 1$, and let $K = \mathbb{Q}(\alpha)$. Notice that $p(x)$ is irreducible by the rational roots theorem and so $[K : \mathbb{Q}] = 3$. Then $p'(x) = 3x^2 - 2x$ and hence

$$\operatorname{disc}(\alpha) = (-1)^{3(3-1)/2} \det \begin{bmatrix} 1 & -1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 & -1 \\ 3 & -2 & 0 & 0 & 0 \\ 0 & 3 & -2 & 0 & 0 \\ 0 & 0 & 3 & -2 & 0 \end{bmatrix} = -31,$$

which shows that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ since -31 is squarefree.

3 Prime Factorization

3.1 Ring Theory

Let K be a number field and let $R = \mathcal{O}_K$ be its ring of integers. Recall that in Section 1.4, we uncovered some purely ring theoretic facts about R. We'll restate them here as they'll be very useful to us soon. Note that when we speak about rings in this course, they are always commutative and unital.

(1) Corollary 1.19: If I is a nonzero ideal of R, then R/I is finite.

(2) Corollary 1.20: Every nonzero prime ideal of R is maximal.

(3) Corollary 1.21: R is Noetherian.

We now give a few characterizations of being a Noetherian ring.

Proposition 3.1

Let R be a ring. The following are equivalent:

(1) R is Noetherian.

(2) If $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals of R, then there exists some $N \in \mathbb{N}$ such that $I_k = I_N$ for all $k \geq N$; that is, the chain terminates.

(3) Every nonempty set of ideals of R has a maximal element (with respect to $\subseteq$).

Proof of Proposition 3.1.

(1) $\Rightarrow$ (2): Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals in R. Let $I = \bigcup_{j \in \mathbb{N}} I_j$, and note that I is an ideal of R. Since R is Noetherian, we see that I is finitely generated, say by $a_1, \ldots, a_s$. Then for each $i = 1, \ldots, s$, there exists some $N_i \in \mathbb{N}$ such that $a_i \in I_{N_i}$. Taking $N = \max\{N_1, \ldots, N_s\}$, we have $a_i \in I_N$ for all $i = 1, \ldots, s$ and thus $I \subseteq I_N$. But $I_N \subseteq I$ by definition, so equality follows. In particular, we have $I_k = I_N$ for all $k \geq N$.

(2) $\Rightarrow$ (3): Suppose $\mathcal{I}$ is a nonempty set of ideals of R, and let $I_1 \in \mathcal{I}$ (which exists because $\mathcal{I}$ is nonempty). If I_1 is maximal, we're done. Otherwise, $\mathcal{I} \setminus \{I_1\}$ must be nonempty; we can find I_2 from this collection such that $I_1 \subseteq I_2$ (else I_1 was maximal). If I_2 is not maximal, pick $I_3 \in \mathcal{I} \setminus \{I_1, I_2\}$ such that $I_1 \subseteq I_2 \subseteq I_3$. But by assumption, this process terminates; for some $N \in \mathbb{N}$, we have $I_k = I_N$ for all $k \geq N$, and I_N is our desired maximal element in $\mathcal{I}$.

(3) $\Rightarrow$ (1): Let I be an ideal of R. Let $\mathcal{I}$ denote the collection of all finitely generated ideals of R contained in I, which is nonempty because $\langle 0 \rangle \in \mathcal{I}$. By assumption, $\mathcal{I}$ has a maximal element J. If $J \neq I$, then we can find some $a \in I \setminus J$. Then $\langle J, a \rangle$ is also finitely generated and contained in $\mathcal{I}$, contradicting maximality. It follows that $J = I$ and so I is finitely generated. □

Note that the rings that we work with in this course are not generally UFDs, so we do not have the classical prime factorization from first year number theory. However, the following proposition gives us the idea to consider the factorization of proper ideals into prime ideals. The reason why we are only considering proper ideals here is because taking $I = R$ fails condition (1); every prime ideal of R is proper by definition.

Proposition 3.2

Let R be Noetherian and let $I \neq R$ be an ideal. There exist prime ideals $P_1, \ldots, P_n$ of R such that

(1) $I \subseteq P_i$ for all $i = 1, \ldots, n$; and

(2) $P_1 P_2 \cdots P_n \subseteq I$.

Note that the prime ideals P_i above are not necessarily distinct. To prove this proposition, we will use an extremely common tactic in commutative algebra: we assume that the set of objects that does not satisfy the property is nonempty, take a maximal element, and derive a contradiction.

Proof of Proposition 3.2.

Let X be the set of proper ideals of R not having this property. By contradiction, assume that $X \neq \varnothing$. Let $I \in X$ be a maximal element (with respect to $\subseteq$). Then I itself is not prime (otherwise we can simply take $P_1 = I$), so we can find $a, b \in R$ such that $ab \in I$ but $a, b \notin I$. By the maximality of I, we have $I + \langle a \rangle, I + \langle b \rangle \notin X$.

Note that $(I + \langle a \rangle)(I + \langle b \rangle) \subseteq I$ since I^2, $\langle a \rangle I$, $\langle b \rangle I$, and $\langle ab \rangle$ are all subsets of I. In particular, we have $I + \langle a \rangle \neq R$ and $I + \langle b \rangle \neq R$ since multiplying by R does not change an ideal.

Therefore, we can find prime ideals $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ of R such that

(1) $I + \langle a \rangle \subseteq P_i$ for all $i = 1, \ldots, n$ and $I + \langle b \rangle \subseteq Q_j$ for all $j = 1, \ldots, m$;

(2) $P_1 P_2 \cdots P_n \subseteq I + \langle a \rangle$ and $Q_1 Q_2 \cdots Q_m \subseteq I + \langle b \rangle$.

But then we have $I \subseteq I + \langle a \rangle \subseteq P_i$ and $I \subseteq I + \langle b \rangle \subseteq Q_j$. Moreover, we see that

$$P_1 \cdots P_n Q_1 \cdots Q_m \subseteq (I + \langle a \rangle)(I + \langle b \rangle) \subseteq I.$$

Here, we find that $I \notin X$, which is a contradiction. □

We now introduce some familiar ring theory from PMATH 347, namely the notion of coprime ideals and the (generalized) Chinese remainder theorem.

Definition 3.3

Let R be a ring, and let I and J be proper ideals of R. We say that I and J are **coprime** if $I + J = R$.

The term coprime is used interchangeably with comaximal, but being a number theory course, it feels more appropriate to say coprime. The following proposition tells us that powers of coprime ideals are also coprime.

Proposition 3.4

Let R be a ring. Let I and J be proper ideals such that $I + J = R$. Then for all $n, m \in \mathbb{N}$, we have $I^n + J^m = R$.

Proof of Proposition 3.4.

Suppose that $I^n + J^m \neq R$. Then we have $I^n + J^m \subseteq M$ for some maximal ideal M. This gives us $I^n \subseteq M$ and $J^m \subseteq M$ as well. But maximal ideals are prime. In particular, if $a \in I$, then $a^n \in M$, but since M is prime, we also have $a \in M$. Thus, we have $I \subseteq M$, and by an identical argument, we obtain $J \subseteq M$. (This result also follows from another characterization of prime ideals.) It follows that $I + J \subseteq M$, which is a contradiction since maximal ideals are proper by definition. □

This leads us to the following famous theorem that we all know and love.

Theorem 3.5: Chinese Remainder Theorem

Let R be a ring and let I and J be coprime ideals of R. Then

$$R/IJ \cong R/I \times R/J.$$

Proof of Theorem 3.5.

Define the map $\varphi : R \to R/I \times R/J$ by $\varphi(x) = (x+I, x+J)$. Then we have $\ker\varphi = I \cap J$. But $IJ \subseteq I+J$ always holds and since I and J are coprime, we obtain

$$\begin{aligned} I \cap J &= (I \cap J)R \\ &= (I \cap J)(I+J) \\ &= (I \cap J)I + (I \cap J)J \subseteq IJ \end{aligned}$$

since $I \cap J \subseteq I$, $I \cap J \subseteq J$, and R is commutative. Thus, we have $\ker\varphi = I \cap J = IJ$. To see that φ is surjective, let $a \in I$ and $b \in J$ such that $a + b = 1$ (which exist because I and J are coprime). Then for $x, y \in R$, we have

$$\begin{aligned} \varphi(ax+by) &= (ax+by+I, ax+by+J) \\ &= (by+I, ax+J) \\ &= (b+I, a+J)(y+I, x+J) \\ &= (1+I, 1+J)(y+I, x+J) \\ &= (y+I, x+J), \end{aligned}$$

where the second last equality follows from looking at b modulo I and a modulo J. So φ is surjective, and it follows from the first isomorphism theorem that $R/IJ \cong R/I \times R/J$. □

The generalized Chinese remainder theorem then follows from a straightforward induction.

Theorem 3.6: Generalized Chinese Remainder Theorem

Let R be a ring, and let $I_1, \ldots, I_n$ be pairwise coprime ideals (i.e. $I_i + I_j = R$ when $i \neq j$). Then

$$R/I_1 \cdots I_n \cong R/I_1 \times \cdots \times R/I_n.$$

We end this section on ring theory with a property of finite rings.

Proposition 3.7

Let R be a finite ring. There exist distinct prime ideals $P_1, \ldots, P_m$ of R and $n_i \in \mathbb{N}$ such that

$$R \cong R/P_1^{n_1} \times \cdots \times R/P_m^{n_m}.$$

Note that if R is an integral domain, then this proposition tells us almost nothing as we can simply take $P_1 = \{0\}$. This is much more interesting when we are not working with integral domains.

Proof of Proposition 3.7.

We can find prime ideals $Q_1, \ldots Q_k$ of R such that $Q_1 Q_2 \cdots Q_k = \{0\}$ by using Proposition 3.2 with $I = \{0\}$ and noting that finite rings are Noetherian. Grouping the Q_i's with multiplicity, we can write

$$P_1^{n_1} \cdots P_m^{n_m} = \{0\}$$

where $P_i \neq P_j$ for $i \neq j$. Note that each P_i is prime, so R/P_i is a finite integral domain and hence a field. This means that P_i is also maximal. So we have $P_i + P_j = R$ for $i \neq j$ because these are each independently maximal and distinct, and hence any bigger ideal must be the whole ring. By Proposition 3.4, we obtain $P_i^{n_i} + P_j^{n_j} = R$, and the generalized Chinese remainder theorem (Theorem 3.6) gives

$$R \cong R/P_1^{n_1} \cdots P_m^{n_m} \cong R/P_1^{n_1} \times \cdots \times R/P_n^{n_m}.$$ □

3.2 Prime Ideals of the Ring of Integers

Let K be a number field of degree $[K:\mathbb{Q}] = n$, and let $R = \mathcal{O}_K$. Let I be a nonzero proper ideal of R. We know the following facts:

(1) Corollary 1.19: R/I is finite, which allows us to apply Proposition 3.7.

(2) Corollary 1.21: R is Noetherian, so we can apply Proposition 3.2.

(3) **Correspondence theorem for rings.** There is a one-to-one correspondence between the ideals of R that contain I and the ideals of the quotient ring R/I. In other words, every ideal $\overline{J}$ of R/I is of the form $\overline{J} = J/I$, where $J \subseteq R$ is an ideal such that $I \subseteq J$. Moreover, $\overline{J}$ is prime if and only if J is prime.

(4) Since R/I is finite, we have by (3), Proposition 3.7, and the third isomorphism theorem that

$$\begin{aligned} R/I &\cong (R/I)/(P_1^{n_1}/I) \times \cdots \times (R/I)/(P_m^{n_m}/I) \\ &\cong R/P_1^{n_1} \times \cdots \times R/P_m^{n_m} \end{aligned}$$

where each $P_i \subseteq R$ is prime and $I \subseteq P_i$.

Therefore, to understand the ideal I, we study the prime ideals $P \supseteq I$. It turns out that $P \supseteq I$ if and only if P is a "prime factor" of I, as we'll see later in the course.

For now, we'll introduce a couple of big ideas. Note that by the correspondence theorem, the prime ideals of R/I are precisely P/I where $P \supseteq I$ is a prime ideal. Moreover, for a prime ideal $P \supseteq I$, we know that R/P is a finite field, so its cardinality is $|R/P| = p^m$ for some prime number $p \in \mathbb{N}$. This tells us that

$$p^m + P = p^m(1 + P) = 0 + P$$

where the last equality is by Lagrange. Then $p^m \in P$. Since P is a prime ideal, we get $p \in P$ and so $\langle p \rangle \subseteq P$.

Next, we go through a computational example. Let $K = \mathbb{Q}(\sqrt{2})$ and let $R = \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. Let's try to find all the prime ideals P such that $\langle 5 \rangle \subseteq P$ (or equivalently, $5 \in P$). We have the isomorphisms

$$R/\langle 5 \rangle = \mathbb{Z}[\sqrt{2}]/\langle 5 \rangle \cong \mathbb{Z}[x]/\langle x^2 - 2, 5 \rangle \cong \mathbb{Z}_5[x]/\langle x^2 - 2 \rangle.$$

Note that $x^2 - 2$ is irreducible over $\mathbb{Z}_5[x]$ because it has no roots. So $\langle x^2 - 2 \rangle$ is a maximal ideal of $\mathbb{Z}_5[x]$ and hence $R/\langle 5 \rangle \cong \mathbb{Z}_5[x]/\langle x^2 - 2 \rangle$ is a field. This tells us that $\langle 5 \rangle \subseteq R$ is maximal, so the only prime ideal P of R sitting above $\langle 5 \rangle$ is $P = \langle 5 \rangle$ itself.

That was rather simple, so let's keep going. Take $K = \mathbb{Q}(\sqrt{2})$ and $R = \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ as before. Now, let's try to find the prime ideals such that $\langle 7 \rangle \subseteq P$. We have the isomorphisms

$$R/\langle 7 \rangle \cong \mathbb{Z}[x]/\langle x^2 - 2, 7 \rangle \cong \mathbb{Z}_7[x]/\langle x^2 - 2 \rangle,$$

but this time, we have $x^2 - 2 = (x + 3)(x + 4)$ over $\mathbb{Z}_7[x]$. Then the Chinese remainder theorem implies that

$$\mathbb{Z}_7[x]/\langle x^2 - 2 \rangle \cong \mathbb{Z}_7[x]/\langle x + 3 \rangle \times \mathbb{Z}_7[x]/\langle x + 4 \rangle \cong \mathbb{Z}_7 \times \mathbb{Z}_7,$$

where the last isomorphism is obtained by sending x to -3 and -4 respectively (or we can formally justify this using the first isomorphism theorem if we'd like).

The prime ideals of $\mathbb{Z}_7 \times \mathbb{Z}_7$ are $P_1 = \langle (1, 0) \rangle$ and $P_2 = \langle (0, 1) \rangle$. Our goal now is to retrace our isomorphisms backwards. We have

$$\begin{aligned} (1, 0) \in \mathbb{Z}_7 \times \mathbb{Z}_7 &\mapsto (1 + \langle x + 3 \rangle, 0 + \langle x + 4 \rangle) \in \mathbb{Z}_7[x]/\langle x + 3 \rangle \times \mathbb{Z}_7[x]/\langle x + 4 \rangle \\ &\mapsto x + 4 + \langle x^2 + 2 \rangle \in \mathbb{Z}_7[x]/\langle x^2 - 2 \rangle \\ &\mapsto x + 4 + \langle x^2 - 2, 7 \rangle \in \mathbb{Z}[x]/\langle x^2 - 2, 7 \rangle \\ &\mapsto \sqrt{2} + 4 + \langle 7 \rangle \in R/\langle 7 \rangle. \end{aligned}$$

The trickiest one to reverse here is the second one: we needed to reverse the map from the Chinese remainder theorem. We needed to find a polynomial that was congruent to 1 mod $x+3$ and congruent to 0 mod $x+4$, and $x+4$ happened to do the trick. Similarly, we have

$$\begin{aligned}(0,1) \in \mathbb{Z}_7 \times \mathbb{Z}_7 &\mapsto (0+\langle x+3\rangle, 1+\langle x+4\rangle) \in \mathbb{Z}_7[x]/\langle x+3\rangle \times \mathbb{Z}_7[x]/\langle x+4\rangle \\ &\mapsto -x-3+\langle x^2+2\rangle \in \mathbb{Z}_7[x]/\langle x^2-2\rangle \\ &\mapsto -x-3+\langle x^2-2,7\rangle \in \mathbb{Z}[x]/\langle x^2-2,7\rangle \\ &\mapsto -\sqrt{2}-3+\langle 7\rangle \in R/\langle 7\rangle,\end{aligned}$$

where $-x-3$ is congruent to 0 mod $x+3$ and congruent to 1 mod $x+4$. Thus, the prime ideals in R containing 7 are $Q_1 = \langle \sqrt{2}+4, 7\rangle$ and $Q_2 = \langle -\sqrt{2}-3, 7\rangle = \langle 2+\sqrt{3}, 7\rangle$, keeping in mind that we are looking for the prime ideals of R and not those of $R/\langle 7\rangle$. Note that we have $(\sqrt{2}+3)(\sqrt{2}-3) = -7$ so we in fact have $Q_2 = \langle 2+\sqrt{3}\rangle$. However, it doesn't hurt to include the 7 to ensure that it is actually living above $\langle 7\rangle$.

The main takeaways of this computation were as follows:

(1) The minimal polynomial x^2-2 factored as $(x+3)(x+4)$ over $\mathbb{Z}_7$.

(2) We have $(\sqrt{2}+3)(\sqrt{2}+4) = 14+7\sqrt{2}$; the coefficients are both divisible by 7.

(3) By (2), we have $Q_1Q_2 \subseteq \langle 7\rangle$. It can be checked that $Q_1Q_2 = \langle 7\rangle$ is the prime factorization of $\langle 7\rangle$.

We'll do one more example. This time, we find the prime ideals such that $P \supseteq \langle 2\rangle$. We have the isomorphisms

$$R/\langle 2\rangle \cong \mathbb{Z}[x]/\langle x^2-2,2\rangle \cong \mathbb{Z}_2[x]/\langle x^2\rangle.$$

Since this quotient ring only consists of 4 elements, let's just look at the elements explicitly. Let P be a prime ideal of $\mathbb{Z}_2[x]/\langle x^2\rangle$. Being an ideal, we must have $0+\langle x^2\rangle \in P$. But P is proper, so $1+\langle x^2\rangle \notin P$. Since $(x+1+\langle x^2\rangle)^2 = 1+\langle x^2\rangle \notin P$, we must have $x+1+\langle x^2\rangle \notin P$ for otherwise P would not be closed under multiplication by $\mathbb{Z}_2[x]/\langle x^2\rangle$. Also, note that P cannot be the zero ideal $\{0+\langle x^2\rangle\}$ since $\mathbb{Z}_2[x]/\langle x^2\rangle$ is not an integral domain. Therefore, we must have

$$P = \langle x+\langle x^2\rangle\rangle = \{0+\langle x^2\rangle, x+\langle x^2\rangle\}.$$

Retracing isomorphisms, we have $x+\langle x^2\rangle \mapsto x+\langle x^2-2,2\rangle \mapsto \sqrt{2}+\langle 2\rangle$. It follows that $Q = \langle \sqrt{2},2\rangle = \langle \sqrt{2}\rangle$ is the only prime ideal of R such that $2 \in Q$. Note that $\langle 2\rangle = \langle \sqrt{2}\rangle^2$ here.

One observation here is that $\operatorname{disc}(K) = 8$ and $p \mid 8$ if and only if $p = 2$. As we'll see later, the primes that divide the discriminant are the only ones with multiplicity in their ideal prime factorization.

We state a fact relating the minimal polynomial of α and the ideal prime factorization of $\langle p\rangle$ where p is prime, under the strong assumption that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. We'll prove this later, but we require a lot of machinery first.

Theorem 3.8

Let K be a number field with $[K:\mathbb{Q}] = n$ where $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{C}$. Assume that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let $m(x) \in \mathbb{Z}[x]$ be the minimal polynomial for α. If $p \in \mathbb{N}$ is prime and $m(x)$ factors over $\mathbb{Z}_p[x]$ as

$$\bar{m}(x) = q_1(x)^{n_1} \cdots q_k(x)^{n_k} \in \mathbb{Z}_p[x]$$

where $q_i(x) \neq q_j(x)$ for $i \neq j$ and each $q_i(x)$ is irreducible, then

(1) the prime ideals $P \subseteq \mathcal{O}_K$ such that $p \in P$ are exactly $P = \langle q_i(\alpha), p\rangle$; and

(2) we have $\langle p\rangle = \langle q_1(\alpha), p\rangle^{n_1} \cdots \langle q_k(\alpha), p\rangle^{n_k}$.

In particular, this fact gives us all the prime ideals as well as how to do the ideal prime factorization!

For example, suppose that $\alpha \in \mathbb{C}$ satisfies $\alpha^2+\alpha+1=0$. Note that $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$ because $\operatorname{disc}(x^2+x+1) = -3$ is squarefree. The minimal polynomial of α is $m(x) = x^2+x+1$. Over $\mathbb{Z}_3[x]$, this factors as

$$\bar{m}(x) = (x+2)(x+2) \in \mathbb{Z}_3[x],$$

so by Theorem 3.8, we have $\langle 3\rangle = \langle \alpha+2, 3\rangle^2$ and that $\langle \alpha+2, 3\rangle$ is a prime ideal of $\mathcal{O}_K$. On the other hand, x^2+x+1 is irreducible over $\mathbb{Z}_2[x]$ and so the prime factorization of $\langle 2\rangle$ is just itself since $\langle \alpha^2+\alpha+1, 2\rangle = \langle 2\rangle$.

3.3 Dedekind Domains

Dedekind domains are the rings where ideal prime factorization happens! Before we give the definition, we'll give some motivation for the desired properties.

Let $R \subseteq S$ be integral domains.

(1) Recall that $\alpha \in S$ is **integral** over R (see Definition 1.6) if there exists a monic polynomial $f(x) \in R[x]$ such that $f(\alpha) = 0$. By Theorem 1.7, this is equivalent to $R[\alpha]$ being finitely generated as an R-module.

(2) We say that S is **integral** over R if all elements of S are integral over R.

We now introduce a few more related definitions.

Definition 3.9

Let $R \subseteq S$ be integral domains.

(1) The **integral closure** of R in S is $\{\alpha \in S : \alpha \text{ is integral over } R\}$.

(2) We say that R is **integrally closed** if the integral closure of R in its field of fractions is R itself.

For example, we see that $\mathbb{Z}$ is integrally closed because its field of fractions is $\mathbb{Q}$, and the only algebraic integers in $\mathbb{Q}$ are the ordinary integers.

Consider a number field K and let $R = \mathcal{O}_K$ be its ring of integers. Let F be the field of fractions of R. Note that if $x \in K$, there exists $0 \neq N \in \mathbb{Z}$ such that $Nx \in R$ by part (a) of **A1-1**. This means that $x \in F$, and thus $K = F$. So the field of fractions of the ring of integers is precisely the number field.

Proposition 3.10

Let K be a number field. Then $\mathcal{O}_K$ is integrally closed.

Proof of Proposition 3.10.

We give a sketch of the proof up to writing down some generating sets. Suppose that $\alpha \in K$ is in the integral closure of $\mathcal{O}_K$, so there exists some monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_K[x]$$

with $f(\alpha) = 0$. Since $a_i \in \mathcal{O}_K$ (i.e. a_i is integral over $\mathbb{Z}$), it follows from Theorem 1.7 that $\mathbb{Z}[a_i]$ is a finitely generated $\mathbb{Z}$-module. This implies that $\mathbb{Z}[a_{n-1}, a_{n-2}, \ldots, a_0]$ is also finitely generated. But we can write

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0,$$

so $\mathbb{Z}[\alpha, a_{n-1}, \ldots, a_1, a_0]$ is also finitely generated. Note that $\mathbb{Z}[\alpha] \subseteq \mathbb{Z}[\alpha, a_{n-1}, \ldots, a_1, a_0]$. Since $\mathbb{Z}$ is Noetherian, we have by Theorem 1.10 that $\mathbb{Z}[\alpha]$ is also finitely generated, so $\alpha \in \mathcal{O}_K$ by Theorem 1.7. □

With this result, we are now ready to state the definition of a Dedekind domain.

Definition 3.11

Let R be an integral domain. We say that R is a **Dedekind domain** if

(1) R is Noetherian;

(2) R is integrally closed; and

(3) every nonzero prime ideal of R is maximal.

In particular, we see that $\mathcal{O}_K$ satisfies all three of these properties (by Corollary 1.21, Proposition 3.10, and Corollary 1.20 respectively).

Why is this definition of a Dedekind domain the right one for prime factorization?

(1) Being Noetherian gives us the existence of prime factorization by using the classic Noetherian contradiction proof technique.

(2) Because every nonzero prime is maximal, primes can't be factored further.

(3) It turns out that being integrally closed will give us the uniqueness of prime factorization!

Now, our goal is to explore the connection between being integrally closed and prime factorization. The following lemma will be a useful "contradiction getter" soon. In particular, if $\lambda \in F \setminus R$ is a root of a monic polynomial with coefficients in R, this will contradict the fact that R is integrally closed.

Lemma 3.12

Let R be a Dedekind domain, let I be a nonzero proper ideal, and let F be the field of fractions of R. Then there exists $\lambda \in F \setminus R$ such that $\lambda I \subseteq R$.

Proof of Lemma 3.12.

Let $0 \neq a \in I$. Note that R is Noetherian since it is a Dedekind domain, so by Proposition 3.2, we can find nonzero prime ideals $P_1, \dots, P_r$ of R such that $P_1 P_2 \cdots P_r \subseteq \langle a \rangle$. Moreover, assume that r is minimal (i.e. pick the smallest number of prime ideals possible). Let M be a maximal ideal such that $I \subseteq M$.

Since $P_1 P_2 \cdots P_r \subseteq I \subseteq M$ and M is prime, it follows by the ideal-wise characterization of a prime ideal that there is some $i \in \{1, \dots, r\}$ with $P_i \subseteq M$. Without loss of generality, assume that $P_1 \subseteq M$. Note that P_1 is prime and hence maximal since R is a Dedekind domain, so $P_1 = M$.

Case 1. If $r = 1$, then $P_1 \subseteq \langle a \rangle \subseteq I \subseteq M = P_1$ and we get equality throughout. This gives us $I = \langle a \rangle$, so we can take $\lambda = 1/a \in F \setminus R$ (where we know a is not a unit for otherwise $I = R$).

Case 2. If $r > 1$, then by the minimality of r, there exists some element $b \in P_2 \cdots P_r \setminus \langle a \rangle$. Then we have $bP_1 \subseteq P_1 P_2 \cdots P_r \subseteq \langle a \rangle$. Moreover, we see that $bI \subseteq bM = bP_1 \subseteq \langle a \rangle$, so we may take $\lambda = b/a$. Note that this works because if $x \in I$, then $\lambda x = \frac{b}{a} x$. But $bx \in I \subseteq \langle a \rangle$, so we can write $bx = ar$ for some $r \in R$, giving us $\lambda x = \frac{ar}{a} = r \in R$. Also, since $b \notin \langle a \rangle$, we have $\lambda \notin R$ as well. □

Equipped with this "contradiction getter", we can prove an extremely useful result using the integrally closed property of a Dedekind domain.

Proposition 3.13

Let R be a Dedekind domain, and let I be a nonzero proper ideal. Then there exists a nonzero ideal J of R such that IJ is principal.

Proof of Proposition 3.13.

Let $0 \neq a \in I$ and consider the nonzero ideal

$$J = \{x \in R : xI \subseteq \langle a \rangle\}.$$

We already know it is nonzero because $a \in J$, so just verify the ideal properties.

Note that $IJ \subseteq \langle a \rangle$. Consider the "fractional ideal" $A = \frac{1}{a}IJ \subseteq R$ (this trick will come up a lot). If $A = R$, then $IJ = aR = \langle a \rangle$ and we are already done.

Now suppose that $A \neq R$. We'll show that this case is actually impossible. We leave it as an exercise that A is a nonzero ideal of R. Then by Lemma 3.12, there exists $\lambda \in F \setminus R$ such that $\lambda A \subseteq R$, where F is the field of fractions of R.

Notice that $J = \frac{1}{a}aJ \subseteq A$ since $a \in I$, and so $\lambda J \subseteq \lambda A \subseteq R$. Moreover, if we write $\lambda A = \frac{\lambda}{a}IJ \subseteq R$, then multiplying both sides by a gives us $\lambda IJ \subseteq aR = \langle a \rangle$. In particular, we can regroup λIJ as $(\lambda J)I$ by commutativity with $(\lambda J)I \subseteq \langle a \rangle$, and we see by the definition of J that $\lambda J \subseteq J$.

Since R is Noetherian, J is finitely generated, say by $\alpha_1, \ldots, \alpha_n$. We can find $B \in M_m(R)$ such that

$$\begin{bmatrix} \lambda\alpha_1 \\ \vdots \\ \lambda\alpha_m \end{bmatrix} = B \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}.$$

Note that $(\alpha_1, \ldots, \alpha_m)^T$ is nonzero and rearranging the above gives us

$$(\lambda I - B) \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} = 0.$$

This means that $\lambda I - B$ is not invertible, and so $\det(\lambda I - B) = 0$. But $\det(xI - B)$ is the characteristic polynomial of B; in particular, it is a monic polynomial with coefficients in R having λ as a root. This is a contradiction because $\lambda \notin R$ and R is integrally closed. □

By Proposition 3.13 and what we proved in **A2-3**, it now makes sense to make the following definition. We won't be using this immediately, but it will come up later in the course.

Definition 3.14

Let R be a Dedekind domain and let X be the set of nonzero ideals of R. Put an equivalence relation on X by $I \sim J$ if and only if there exist $\alpha, \beta \in R \setminus \{0\}$ such that $\alpha I = \beta J$. Then

$$G := \{[I] : I \in X\}$$

is a group under the operation $[I][J] = [IJ]$, called the **ideal class group** of R. The identity is the equivalence class of principal ideals.

The following result, which we will call cancellation of ideals, is our best friend for proving the uniqueness of prime factorization! It allows us to inductively chop off ideals.

Proposition 3.15: Cancellation of Ideals

Let R be a Dedekind domain. Let A, B, and C be nonzero ideals. If $AB = AC$, then $B = C$.

Proof of Proposition 3.15.

By Proposition 3.13, we can find a nonzero ideal J such that $JA = \langle a \rangle$ for some $0 \neq a \in R$. We have $AB = AC$, and multiplying by J gives us $\langle a \rangle B = JAB = JAC = \langle a \rangle C$. Then $aB = aC$, and hence $B = C$ since R is an integral domain. □

The following definition is a very natural one to make.

Definition 3.16

Let R be a ring and let A and B be ideals of R. We say that A **divides** B, written $A \mid B$, if there exists an ideal C such that $B = AC$.

The next result tells us that in a Dedekind domain, the factors of a ideal are precisely the ideals living above.

Proposition 3.17

Let R be a Dedekind domain. Let A and B be nonzero proper ideals of R. Then $A \mid B$ if and only if $B \subseteq A$.

Proof of Proposition 3.17.

($\Rightarrow$) If $A \mid B$, then $B = AC$ for some ideal C and $AC \subseteq A$.

($\Leftarrow$) Suppose that $B \subseteq A$. By Proposition 3.13, we can find a nonzero ideal J such that $JA = \langle a \rangle$ for some $0 \neq a \in R$. Note that $JB \subseteq JA = \langle a \rangle$. Consider the fractional ideal $C = \frac{1}{a}JB$ (verify that this is indeed an ideal of R). Note that $JAC = \langle a \rangle \frac{1}{a} JB = JB$, so by ideal cancellation (Proposition 3.15), we have $AC = B$ and thus $A \mid B$. □

We are ready to prove the golden result that every nonzero proper ideal of a Dedekind domain can be uniquely factored into primes. Note that $\{0\}$ is prime but cannot be uniquely factored, while R does not have a prime factorization because no primes can live above it.

Theorem 3.18

Let R be a Dedekind domain and let I be a nonzero proper ideal. Then I can be written uniquely (up to reordering) as a product of prime ideals.

Proof of Theorem 3.18.

Existence. We use the Noetherian contradiction method we alluded to before. Let X be the set of proper nonzero ideals of R which cannot be written as a product of prime ideals. Suppose that $X \neq \varnothing$. Let $I \in X$ be maximal (with respect to $\subseteq$). Then I is not a prime ideal and hence not a maximal ideal (since being prime is the same as being maximal in a Dedekind domain). Let P be a maximal ideal such that $I \subsetneq P$. By Proposition 3.17, we have $P \mid I$, so there exists an ideal J such that $I = PJ$.

Note that $I = PJ \subseteq J$. If $I = J$, then $I = IR = IP$. Cancellation of ideals (Proposition 3.15) implies that $P = R$, which is a contradiction since prime ideals are proper. Therefore, we must have $I \subsetneq J$. By the maximality of I in X, we have $J \notin X$, so J can be written as a product of primes. Then $I = PJ$ is also a product of primes, which is a contradiction! So $X = \varnothing$ and every nonzero proper ideal of R can be written as a product of prime ideals.

Uniqueness. Suppose that $I = P_1 P_2 \cdots P_n = Q_1 Q_2 \cdots Q_m$ where P_i and Q_j are prime ideals. Note that

$$Q_1 Q_2 \cdots Q_m = P_1 P_2 \cdots P_n \subseteq P_1.$$

Since P_1 is prime, we have (without loss of generality) that $Q_1 \subseteq P_1$. But Q_1 is prime and hence maximal, so $Q_1 = P_1$. Then by ideal cancellation, we obtain

$$P_2 \cdots P_n = Q_2 \cdots Q_m.$$

Continuing inductively, we find that $P_i = Q_i$ (up to reordering) and $n = m$. □

3.4 Ideal Norm

In the previous section, we proved that every nonzero proper ideal of a Dedekind domain has a unique prime factorization, which is great. But *how* do we actually find such a prime factorization?

Let's start by proposing a potential tool we could use.

Definition 3.19

Let K be a number field and let $R = \mathcal{O}_K$ be its ring of integers. The **norm** of a nonzero ideal I is

$$N(I) := |R/I|.$$

Note that this is always finite because R/I is finite by Corollary 1.19.

Assume for now that the ideal norm is multiplicative; that is, $N(IJ) = N(I)N(J)$ for nonzero ideals I and J. Suppose that $n = N(I) = |R/I|$. We know from Theorem 3.18 that I has a unique prime factorization $I = P_1^{n_1} \cdots P_k^{n_k}$. Using our assumption that the ideal norm is multiplicative, we have

$$N(I) = N(P_1)^{n_1} \cdots N(P_k)^{n_k}.$$

But we previously saw that $N(P_i) = |R/P_i| = p_i^{m_i}$ where $p_i \in \mathbb{N}$ is prime with $p_i \in P_i$. For a prime $p \in \mathbb{N}$ such that $p \mid n$, it must be the case that $p = p_i$ for some $i \in \{1, \ldots, k\}$. Then $p \in P_i$ implies that $\langle p \rangle \subseteq P_i$, so $P_i \mid \langle p \rangle$ by Proposition 3.17. So if we could factor each $\langle p_i \rangle$, then we could find candidates for the P_i's and factor I. The value of $N(I)$ could help us to find the n_i's as well.

Therefore, we have two goals in mind:

(1) Prove that the ideal norm is multiplicative.

(2) Show that $\langle p \rangle$ is easily factored for "almost all" primes $p \in \mathbb{N}$ (namely, we get something similar to Theorem 3.8 in most cases).

Let's work towards the first goal. Suppose that $I = P_1^{n_1} \cdots P_k^{n_k}$ where P_i are distinct prime ideals (so P_i and P_j are pairwise coprime for $i \neq j$). Then the Chinese remainder theorem (Theorem 3.6) gives us

$$R/I \cong R/P_1^{n_1} \times \cdots \times R/P_k^{n_k},$$

and thus $N(I) = N(P_1^{n_1}) \cdots N(P_k^{n_k})$. Therefore, to prove that the ideal norm is multiplicative, it is enough to show that $N(P_i^{n_i}) = N(P_i)^{n_i}$. This innocent looking result requires a lot of machinery, namely localization, local rings, and discrete valuation rings.

To end this section, we prove a useful relationship between the ideal norm of a principal ideal and the field norm. Let $\{v_1, \ldots, v_n\}$ be an integral basis for $R = \mathcal{O}_K$ and recall that a nonzero ideal I of R has an integral basis $\{w_1, \ldots, w_n\}$ because of Corollary 1.17. By taking $M = R$ and $N = I$ in **A2-4**, we obtain

$$\begin{aligned} \operatorname{disc}(w_1, \ldots, w_n) &= [R : I]^2 \cdot \operatorname{disc}(v_1, \ldots, v_n) \\ &= N(I)^2 \cdot \operatorname{disc}(v_1, \ldots, v_n). \end{aligned}$$

If $I = \langle \alpha \rangle$ where $\alpha \neq 0$, then $w_i = \alpha v_i$ is an integral basis for I. (Linear independence comes from R being an integral domain, and spanning comes from the fact that $I = \alpha R$.) Our calculation above shows that

$$\operatorname{disc}(\alpha v_1, \ldots, \alpha v_n) = N(I)^2 \cdot \operatorname{disc}(K).$$

On the other hand, we can also see that

$$\begin{aligned} \operatorname{disc}(\alpha v_1, \ldots, \alpha v_n) &= \det\left[\sigma_i(\alpha v_j)\right]^2 \\ &= \det\left[\sigma_i(\alpha)\sigma_i(v_j)\right]^2 \\ &= \left(\sigma_1(\alpha) \cdots \sigma_n(\alpha)\right)^2 \cdot \det\left[\sigma_i(v_j)\right]^2 \\ &= N_{K/\mathbb{Q}}(\alpha)^2 \cdot \operatorname{disc}(K). \end{aligned}$$

In particular, we have $N(I)^2 = N_{K/\mathbb{Q}}(\alpha)^2$ and thus

$$N(\langle \alpha \rangle) = |N_{K/\mathbb{Q}}(\alpha)|.$$

3.5 Localization

We introduce local rings, which will lead us to the notion of localization.

Definition 3.20

A **local ring** is a ring which has a unique maximal ideal.

The following is a useful characterization of a local ring.

Proposition 3.21

A ring R is local if and only if $I = R \setminus R^\times$ is an ideal of R. In this case, I is the unique maximal ideal.

Proof of Proposition 3.21.

($\Rightarrow$) Let R be a local ring and M be a maximal ideal of R. Note that $M \subseteq I$ because maximal ideals are proper and cannot contain units. Conversely, if $\alpha \in I$, we see that $\langle \alpha \rangle$ is proper. But M is the unique maximal ideal, so $\langle \alpha \rangle \subseteq M$ and thus $I \subseteq M$.

($\Leftarrow$) Suppose that $I = R \setminus R^\times$ is an ideal of R. Then for all maximal ideals M, we have $M \subseteq I$. But M being maximal means that $M = I$. □

Every field F is a local ring because the units are $F^\times = F \setminus \{0\}$, and $F \setminus F^\times = \{0\}$ is the only maximal ideal.

Another example of a local ring is $\mathbb{Z}_{p^n}$ where $n > 1$. Indeed, observe that $x \notin \mathbb{Z}_{p^n}^\times$ if and only if $\gcd(x, p^n) \neq 1$. In particular, the non-units are the multiples of p, which form an ideal.

However, this is not the type of example that we want. How can we construct local integral domains? The answer is localization!

Definition 3.22

Let R be an integral domain, let K be the field of fractions of R, and let P be a prime ideal of R. The **localization** of R at P is defined to be

$$R_P = \left\{ \frac{a}{b} \in K : b \notin P \right\}.$$

Let's make a few remarks about the localization by a prime ideal.

(1) Note that we are using lazy notation here; it is possible to have $\frac{a}{b} \in R_P$ where $b \in P$. We only require the existence of elements $c, d \in R$ such that $\frac{a}{b} = \frac{c}{d}$ where $d \notin P$. For a simple example, take $R = \mathbb{Z}$ and $P = \langle 2 \rangle$. Observe that we have $\frac{4}{6} = \frac{2}{3} \in \mathbb{Z}_{\langle 2 \rangle}$ even though $6 \in \langle 2 \rangle$.

(2) Let $\frac{a}{b}, \frac{c}{d} \in K$ where $b, d \notin P$. Note that $bd \notin P$ since P is a prime ideal, so $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in R_P$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in R_P$. In particular, R_P is a subring of K.

(3) It is clear that PR_P is an ideal of R. We show that $PR_P = R_P \setminus R_P^\times$ and so R_P is a local ring by Proposition 3.21. (It better be if we're going to call it the localization!)

First, we show that every element of $R_P \setminus PR_P$ is a unit. Let $\frac{a}{b} \in R_P$ where $b \notin P$, and suppose that $\frac{a}{b} \notin PR_P$. Note that $a \notin P$ for otherwise $\frac{a}{b} = \frac{a}{1}\frac{1}{b} \in PR_P$ by definition. This implies that $\frac{b}{a} \in R_P$ and so $\frac{a}{b}$ is a unit.

On the other hand, every element of PR_P is not a unit. Let $\frac{a}{b} \in P$ where $a \in P$ and $b \notin P$, and let $\frac{c}{d} \in R_P$ where $c \in R$ and $d \notin P$. Suppose by way of contradiction that $\frac{a}{b} \cdot \frac{c}{d} = \frac{1}{1}$. Then there must exist some $u \notin P$ such that $uac = ubd$. But this is a contradiction because $uac \in P$, but $ubd \notin P$.

We denote the unique maximal ideal PR_P by $P_P = \{\frac{a}{b} : a \in P, b \notin P\}$.

We have now shown that if R is an integral domain, then R_P is a local ring. But what if R is a Dedekind domain? Then R_P is of course local, but as we might expect, there is much more!

3.6 Discrete Valuation Rings

We mentioned discrete valuation rings as another tool we needed to prove the multiplicativity of the ideal norm. We now give the definition.

Definition 3.23

A **discrete valuation ring (DVR)** is an integral domain R such that

(1) R is not a field;

(2) R is Noetherian;

(3) R is a local ring;

(4) the unique maximal ideal M of R is principal.

If $M = \langle \pi \rangle$, we call π a **uniformizer**.

Our goal is to show that if R is a Dedekind domain and P is a nonzero prime ideal, then R_P is a DVR! Note that we are excluding the case where $P = \{0\}$ because we would then have $R_P = K$, which is a field and hence not a DVR.

We first prove Nakayama's lemma, which will allow us to prove an important property of a DVR.

Lemma 3.24: Nakayama

Let R be a ring. Let I be a nonzero proper ideal of R and M be a finitely generated R-module such that $IM = M$. There exists $a \in R$ such that

(1) $a + I = 1 + I$; and

(2) $aM = \{0\}$ (that is, a annihilates the module).

Proof of Lemma 3.24.

Since M is a finitely generated R-module, we can write $M = Rx_1 + \cdots + Rx_n$ for some $x_i \in M = IM$. In particular, each x_i can be written in the form $x_i = a_{i1}x_1 + \cdots + a_{in}x_n$ where $a_{ij} \in I$. Let $A = [a_{ij}] \in M_n(I)$ and $v = [x_1, \ldots, x_n]^T$ so that $Av = v$. Consider the characteristic polynomial $f(x) = \det(xI_n - A)$ of A. Note that Cayley-Hamilton holds for commutative rings with unity, so we have $f(A) = 0$. Writing $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ where $c_i \in I$, we obtain

$$\begin{aligned} 0 = f(A)v &= (A^n + c_{n-1}A^{n-1} + \cdots + c_1A + c_0I_n)v \\ &= v + c_{n-1}v + \cdots + c_1v + c_0v \\ &= f(1)v, \end{aligned}$$

where the second equality follows from the fact that $Av = v$. Letting $a = f(1)$, we have $av = 0$, which implies that $ax_i = 0$ for all $i = 1, \ldots, n$. But $M = Rx_1 + \cdots + Rx_n$, so $aM = \{0\}$. Finally, since $c_i \in I$, we have $a = f(1) = 1 + c_{n-1} + \cdots + c_1 + c_0 \equiv 1 \pmod{I}$. □

Proposition 3.25

Let R be a DVR and let $M = \langle \pi \rangle$ be its unique maximal ideal. If I is a nonzero proper ideal, then $I = M^n$ for some $n \in \mathbb{N}$.

Proof of Proposition 3.25.

Consider the fractional ideal $J = \frac{1}{\pi}R$. (This doesn't live in R, but in the field of fractions.) Note that $MJ = R$. Denoting $I_1 = IJ$, we see that $I = IR = IJM = I_1M \subseteq I_1$.

Suppose that $I = I_1$. Then we see that $I = IM$, so by Nakayama's lemma (Lemma 3.24), there exists $a \in R$ such that $a - 1 \in M$ and $aI = \{0\}$. (Note that the roles of I and M are switched; we had some unfortunate notation here.) But R is an integral domain, so the only thing that can kill a nonzero ideal is $a = 0$. This implies that $-1 \in M$ and so $M = R$, which is a contradiction! Therefore, we have $I \subsetneq I_1$.

If $I_1 = R$, then $I = I_1M = RM = M$ and we are done. Otherwise, we have $I_1 \neq R$. Denoting $I_2 = I_1J$, we see that $I_1 = I_1R = I_1JM = I_2M \subseteq I_2$. An identical argument shows that $I_1 \subsetneq I_2$, and if $I_2 = R$, then $I_1 = M$ and so $I = I_1M = M^2$. Repeating this process gives us an ascending chain of ideals

$$I \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$$

and since DVRs are Noetherian, this process must terminate. □

Let's take a look at some useful consequences of this proposition. Let R be a DVR and as usual, let $M = \langle \pi \rangle$ be its unique maximal ideal.

(1) Note that if I is a nonzero proper ideal of R, then $I = M^n = \langle \pi^n \rangle$. Therefore, being a DVR is equivalent to being a local PID that is not a field.

(2) Let $0 \neq x \in R$. There are two possibilities: either $x = u \in R^\times$ or $x \notin R^\times$. In the latter case, we have that $\langle x \rangle$ is a nonzero proper ideal of R, so $\langle x \rangle = \langle \pi^n \rangle$ for some $n \in \mathbb{N}$. Then we can write $x = u\pi^n$ for some $u \in R^\times$. Since everything in the ring is a unit multiple of a power of π, it now makes sense why we call π a uniformizer.

The next proposition tells us that the localization of a Noetherian integral domain is still Noetherian.

Proposition 3.26

Let R be a Noetherian integral domain and P is a nonzero prime ideal. Then R_P is Noetherian.

Proof of Proposition 3.26.

Let $I \subseteq R_P$ be an ideal. Our goal is to show that I is a finitely generated R_P-module. Note that $J = I \cap R$ is an ideal of R. Since R is Noetherian, we can write $J = Rx_1 + \cdots + Rx_n$ where $x_i \in J$.

Let $x = \frac{a}{b} \in I$ where $a, b \in R$ and $b \notin P$. Then $a = bx \in I \cap R = J$, so we can write $a = r_1x_1 + \cdots + r_nx_n$ for some $r_i \in R$. In particular, we have

$$x = \frac{a}{b} = \frac{r_1}{b}x_1 + \cdots + \frac{r_n}{b}x_n$$

where $\frac{r_i}{b} \in R_P$ and $x_i \in J \subseteq I$, so $I = R_Px_1 + \cdots + R_Px_n$ is finitely generated as desired. □

We are now ready to prove our goal that the localization of a Dedekind domain by a prime ideal is a DVR.

Theorem 3.27

Let R be a Dedekind domain and let P be a nonzero prime ideal. Then R_P is a DVR.

Proof of Theorem 3.27.

Since P is nonzero, we know that R_P is not a field. Proposition 3.26 tells us that R_P is Noetherian, and we have shown that R_P is local (it's a localization for goodness' sake). It suffices to prove that P_P, the unique maximal ideal of R_P, is principal.

Since R is a Dedekind domain, we know by Proposition 3.13 that there exists an ideal I of R such that $IP = \langle \alpha \rangle$ for some $0 \neq \alpha \in P$. Consider the fractional ideal $J = \frac{1}{\alpha}I$ and note that $JP = R$. Then we can write $1 = a_1b_1 + \cdots + a_nb_n$ where $a_i \in J$ and $b_i \in P$. Choose i such that $a_ib_i \notin P$. (Such an i must exist because if $a_ib_i \in P$ for all i, then $1 \in P$.) We see that $\frac{1}{a_ib_i} \in R_P$.

Now, let $x \in P_P$. We have $x = a_ib_i \cdot \frac{1}{a_ib_i}x$. Letting $y = \frac{1}{a_ib_i}x$, we have $y \in P_P$ since P_P is an ideal of R_P. Then we can write $y = \frac{u}{v}$ where $u, v \in R$ with $u \in P$ and $v \notin P$. This yields

$$x = b_i\frac{a_iu}{v}.$$

Since $a_i \in J$ and $u \in P$, we get $a_iu \in JP = R$, so $x \in \langle \frac{b_i}{1} \rangle \subseteq R_P$. This holds for all $x \in P_P$, so $P_P \subseteq \langle \frac{b_i}{1} \rangle$. The reverse containment follows because $b_i \in P$ and $1 \notin P$, so $P_P = \langle \frac{b_i}{1} \rangle$. □

3.7 Multiplicativity of the Ideal Norm

Equipped with all the tools, let's start proving that the ideal norm is multiplicative.

Proposition 3.28

Let R be an integral domain and P be a nonzero prime ideal of R. For all $n \in \mathbb{N}$, we have

$$R/P^n \cong R_P/P_P^n.$$

Proof of Proposition 3.28.

We leave it as an exercise to check that the map $r + P^n \mapsto \frac{r}{1} + P_P^n$ is a well-defined isomorphism between these quotient spaces. □

Recall that in Section 3.4, we showed that the Chinese remainder theorem reduces the problem to proving that $N(P^n) = N(P)^n$. The next result is the key to this fact.

Proposition 3.29

Let R be a DVR and let P be its maximal ideal. If R/P is finite, then for all $n \in \mathbb{N}$, we have

$$|R/P^n| = |R/P|^n.$$

Proof of Proposition 3.29.

We proceed by induction. The base case is obvious. Suppose that $|R/P^n| = |R/P|^n$ for some $n \geq 1$. Consider the map $\varphi : R/P^{n+1} \to R/P^n$ defined by

$$\varphi(r + P^{n+1}) = r + P^n.$$

Since $P^{n+1} \subseteq P^n$, we see that φ is well-defined. It is easily verified that φ is a surjective homomorphism. Moreover, the kernel of φ consists of the elements already living in P^n, namely $\ker \varphi = P^n/P^{n+1}$. By the first isomorphism theorem, we get

$$(R/P^{n+1})/(P^n/P^{n+1}) \cong R/P^n.$$

Therefore, we have $|R/P^{n+1}| = |P^n/P^{n+1}| \cdot |R/P|^n$ by the inductive hypothesis. (Note that we could've used the third isomorphism theorem to get this isomorphism as well, but modding out by P^{n+1} would seemingly come out of nowhere.) To finish off the proof, it is enough to show that $|P^n/P^{n+1}| = |R/P|$. We'll do this using linear algebra. Consider the field $F = R/P$, and let $V = P^n/P^{n+1}$ be an F-vector space where scalar multiplication is defined by

$$(r + P)(a + P^{n+1}) = ra + P^{n+1}.$$

(Check that this is well-defined.) Write $P = \langle \pi \rangle$ and let $x \in V$. Then $x = a + P^{n+1}$ for some $a \in P^n$. But then $a \in \langle \pi^n \rangle$ and so $a = c\pi^n$ for some $c \in R$. This gives us

$$x = c\pi^n + P^{n+1} = (c + P)(\pi^n + P^{n+1}).$$

In particular, we see that V is spanned by $\pi^n + P^{n+1}$, which shows that $\dim_F(V) = 1$ and $V \cong F$. From this, we deduce that $|R/P| = |F| = |V| = |P^n/P^{n+1}|$. □

Using these two results, we finally have the multiplicativity of the ideal norm.

Theorem 3.30

Let $R = \mathcal{O}_K$. If I and J are nonzero ideals of R, then

$$N(IJ) = N(I)N(J).$$

Proof of Theorem 3.30.

Let P be a nonzero prime ideal. It suffices to show that $N(P^n) = N(P)^n$. Observe that

$$N(P^n) = |R/P^n| = |R_P/P_P^n| = |R_P/P_P|^n = |R/P|^n = N(P)^n$$

where the second and fourth equalities follow from Proposition 3.28, and the third equality follows from Proposition 3.29. □

We have already seen that this property is extremely useful from our work on the assignments, and now we don't have to assume it as a fact!

3.8 Further Applications of DVRs

It would be a shame to have all of this beautiful DVR theory only to use it to prove the multiplicativity of the ideal norm and leave it at that. Let's take it a bit further.

Theorem 3.31: DVR Characterization

Let K be a number field, let $R = \mathcal{O}_K$, and let $S \subseteq R$ be a subring with index $[R : S] = n < \infty$ (as additive groups).

(1) We have $S = R$ if and only if S_P is a DVR for all nonzero prime ideals P of S.

(2) Let P be a prime ideal of S such that $p \in \mathbb{N}$ is prime with $p \in P$. (Note that every nonzero prime ideal contains a prime by **A4-3**, and it is unique by Bézout.) If $p \nmid n$, then S_P is a DVR.

Before we prove this, we'll see how to make use of it. The DVR characterization tells us that the only subring of $R = \mathcal{O}_K$ such that localization by *every* nonzero prime ideals leads to a DVR is the whole ring itself. If we have some subring S of R which we think is equal to R itself, the DVR characterization gives us a way to test for that. By taking $S = \mathbb{Z}[\alpha]$, we can check whether or not R is the smallest possible ring.

Note that for $R = \mathcal{O}_K$ and $S = \mathbb{Z}[\alpha]$, we have $\operatorname{rank}(R) = \operatorname{rank}(S) = [K : \mathbb{Q}]$. That is, S is a submodule of R of equal rank. It follows from **A2-4** that $[R : S] < \infty$, and we know that

$$\operatorname{disc}(f(x)) = \operatorname{disc}(\alpha) = [R : S]^2 \cdot \operatorname{disc}(K).$$

In particular, if $p^2 \nmid \operatorname{disc}(f(x))$, then $p \nmid [R : S]$. Then the second part of the DVR characterization tells us that we only need to check the "bad primes", namely those such that $p^2 \mid \operatorname{disc}(f(x))$.

Proposition 3.32

Let $\alpha \in \mathbb{C}$ be an algebraic integer, and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Let $p \in \mathbb{N}$ be prime, and suppose that the irreducible factorization of $f(x) \in \mathbb{Z}_p[x]$ is

$$f(x) = p_1(x)^{n_1} p_2(x)^{n_2} \cdots p_k(x)^{n_k} \in \mathbb{Z}_p[x].$$

Then the prime ideals of $\mathbb{Z}[\alpha]$ containing p are exactly

$$P_i = \langle p_i(\alpha), p \rangle.$$

We leave the proof of this to **A6-1**. Note that this proposition does *not* say that

$$\langle p \rangle = P_1^{n_1} \cdots P_k^{n_k}.$$

An example where this fails is $S = \mathbb{Z}[\sqrt{5}]$ and $p = 2$, which we'll show on **A6-2**.

Let $R = \mathcal{O}_K$ and $S = \mathbb{Z}[\alpha]$ where $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$. Let $P \subseteq S$ be a nonzero prime ideal. Note that $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/\langle f(x) \rangle$ where $f(x)$ is the minimal polynomial of α. In particular, $\mathbb{Z}[x]$ is Noetherian (as a consequence of the Hilbert basis theorem), and the quotient of a Noetherian ring is Noetherian, so $\mathbb{Z}[\alpha]$ is Noetherian. Therefore, S_P is a local Noetherian ring by Proposition 3.26 which is not a field since P is nonzero. As a result, in order to check that S_P is a DVR, we only need to verify that its unique maximal ideal P_P is principal.

We'll go through a few examples of applying the DVR characterization.

(1) Let $\alpha \in \mathbb{C}$ be a root of the irreducible polynomial $f(x) = x^4 - 5x^2 + 7$ with discriminant $1008 = 2^4 \cdot 3^2 \cdot 7$. Let $K = \mathbb{Q}(\alpha)$, let $R = \mathcal{O}_K$, and let $S = \mathbb{Z}[\alpha]$.

We show that $S = R$. From our above discussion, we only need to check that localization by prime ideals of S containing 2 or 3 are DVRs, and we further reduced this to showing that the unique maximal ideal is principal.

- Working modulo 2, we have $f(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2 \in \mathbb{Z}_2[x]$, where $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2[x]$ because it has no roots. By Proposition 3.32, the only prime ideal of S containing 2 is $P = \langle \alpha^2 + \alpha + 1, 2\rangle$.

  We check that $P_P \subseteq S_P$ is principal. Using polynomial long division, we have

  $$x^4 - 5x^2 + 7 = (x^2 + x + 1)(x^2 - x - 5) + 6x + 12.$$

  In particular, we see that

  $$0 = f(\alpha) = \alpha^4 - 5\alpha^2 + 7 = (\alpha^2 + \alpha + 1)(\alpha^2 - \alpha - 5) + 6\alpha + 12,$$

  which implies that $6\alpha + 12 = 2(3\alpha + 6) \in \langle \alpha^2 + \alpha + 1\rangle$. Note that $3\alpha + 6 \notin P$. (Indeed, if $3\alpha + 6 \in P$, then $3\alpha \in P$ since $6 = 2 \cdot 3 \in P$. Then $2\alpha \in P$ implies that $\alpha \in P$, and $\alpha^2 + \alpha + 1 \in P$ implies that $1 \in P$, which is a contradiction.) This means that

  $$2 = \frac{-1}{3\alpha + 6}(\alpha^2 + \alpha + 1)(\alpha^2 - \alpha - 5) \in S_P,$$

  and thus $2 \in (\alpha^2 + \alpha + 1)S_P$. We conclude that

  $$P_P = 2S_P + (\alpha^2 + \alpha + 1)S_P = (\alpha^2 + \alpha + 1)S_P$$

  is a principal ideal and S_P is a DVR.

- The irreducible factorization of $f(x) \in \mathbb{Z}_3[x]$ is $f(x) = x^4 + x^2 + 1 = (x + 1)^2(x + 2)^2 \in \mathbb{Z}_3[x]$, so there are two prime ideals of S containing 3, namely $P_1 = \langle \alpha + 1, 3\rangle$ and $P_2 = \langle \alpha + 2, 3\rangle$.

  Recall that the remainder when $f(x)$ is divided by a linear polynomial $x - a$ is $f(a)$. We see that $f(-1) = 3 \in \langle \alpha + 1\rangle$ since $f(x) = (x+1)q(x) + f(-1)$ implies that $0 = f(\alpha) = (\alpha+1)q(\alpha) + f(-1)$, and similarly, we have $f(-2) = 3 \in \langle \alpha + 2\rangle$.

  Therefore, we already have that $P_1 = \langle \alpha + 1\rangle$ and $P_2 = \langle \alpha + 2\rangle$, which implies that $(P_1)_{P_1} = (\alpha + 1)S_{P_1}$ and $(P_2)_{P_2} = (\alpha + 2)S_{P_2}$ are both principal. Then S_{P_1} and S_{P_2} are both DVRs.

(2) Let $\alpha \in \mathbb{C}$ be a root of the irreducible polynomial $f(x) = x^3 - x^2 + 5x + 1$ whose discriminant is $-2^2 \cdot 3 \cdot 7$. Let $K = \mathbb{Q}(\alpha)$, let $R = \mathcal{O}_K$, and let $S = \mathbb{Z}[\alpha]$.

We show that $S = R$. This time, we only need to check the primes 2 and 7.

- The irreducible factorization of $f(x) \in \mathbb{Z}_2[x]$ is $f(x) = x^3 + x^2 + x + 1 = (x + 1)^3 \in \mathbb{Z}_2[x]$, so the only prime ideal of S containing 2 is $P = \langle \alpha + 1, 2\rangle$. Then $f(-1) = -6$, which implies that $6 \in \langle \alpha + 1\rangle$. Note that $3 \notin P$ for otherwise $3 \in P$ and $2 \in P$ would imply $1 \in P$, so we have $2 = \frac{1}{3}6 \in (\alpha + 1)S_P$ and $P_P = (\alpha + 1)S_P$.
- The irreducible factorization of $f(x) \in \mathbb{Z}_7[x]$ is $f(x) = (x + 2)^3 \in \mathbb{Z}_7[x]$, so the only prime ideal of S containing 7 is $Q = \langle \alpha + 2, 7\rangle$. We have $f(-2) = -21$, so $21 \in \langle \alpha + 2\rangle$. Then $3 \notin Q$ (by noting that $7 - 2 \cdot 3 = 1$ or applying Bézout), so $7 = \frac{1}{3}21 \in (\alpha + 2)S_Q$ and hence $Q_Q = (\alpha + 2)S_Q$.

Let R be a DVR with unique maximal ideal $M = \langle \pi\rangle$, and let $K = \mathrm{Frac}(R)$ be the field of fractions. Let $x \in R$ be nonzero and nonunit. Recall that $\langle x\rangle = \langle \pi\rangle^m = \langle \pi^m\rangle$ for some $m \in \mathbb{N}$, so $x = u\pi^m$ where $u \in R^\times$, which is where the name uniformizer came from.

If we instead have $x \in K$, then there exists $m \in \mathbb{Z}$ such that $x = u\pi^m$ where $u \in R^\times$. In particular, m can be negative! So if $x = u\pi^m \in K$ where $m \in \mathbb{Z}$, then we have $x \in R$ or $\frac{1}{x} \in R$.

Making use of this fact, we'll do another example of applying the DVR characterization where $R \neq S$ for $R = \mathcal{O}_{\mathbb{Q}(\alpha)}$ and $S = \mathbb{Z}[\alpha]$.

(3) Let $\alpha \in \mathbb{C}$ be a root of $f(x) = x^3 + 2x - 8$, which is irreducible with discriminant $-1760 = -2^5 \cdot 5 \cdot 11$. Let $K = \mathbb{Q}(\alpha)$, let $R = \mathcal{O}_K$, and let $S = \mathbb{Z}[\alpha]$.

We show that $S \neq R$. The irreducible factorization of $f(x) \in \mathbb{Z}_2[x]$ is $f(x) = x^3 \in \mathbb{Z}_2[x]$, so the only prime ideal containing 2 is $P = \langle \alpha, 2 \rangle$.

We show that S_P is not a DVR. From our previous discussion, we know that S_P is a local Noetherian ring which is not a field, so it must be that the unique maximal ideal P_P of S_P is not principal.

Suppose towards a contradiction that $P_P = \langle \pi \rangle$ where π is a uniformizer. Then $\alpha = u_1 \pi^n$ and $2 = u_2 \pi^m$ for some $u_1, u_2 \in S^\times$ and $n, m \in \mathbb{N}$, and from the above fact, we must have $\frac{\alpha}{2} \in S_P$ or $\frac{2}{\alpha} \in S_P$. We'll see that both of these lead to a contradiction. Note that $\{1, \alpha, \alpha^2\}$ is an integral basis for $\mathbb{Z}[\alpha]$.

- If $\frac{\alpha}{2} \in S_P$, then we can write it in the form

$$\frac{\alpha}{2} = \frac{a + b\alpha + c\alpha^2}{d + e\alpha + f\alpha^2}$$

where $d + e\alpha + f\alpha^2 \notin P$. Using the fact that $\alpha^3 + 2\alpha - 8 = 0$, we get

$$d\alpha + e\alpha^2 + f(-2\alpha + 8) = 2a + 2b\alpha + 2c\alpha^2.$$

We already know that $e\alpha + f\alpha^2 \in P = \langle \alpha, 2 \rangle$. Looking at the coefficients of the α term, we have $d - 2f = 2b$ and hence $d = 2(f + b) \in P$. So we see that $d + e\alpha + f\alpha^2 \in P$, which is a contradiction.

- If $\frac{2}{\alpha} \in S_P$, then we can write it in the form

$$\frac{2}{\alpha} = \frac{a + b\alpha + c\alpha^2}{d + e\alpha + f\alpha^2}$$

where $d + e\alpha + f\alpha^2 \notin P$. Then we obtain

$$2d + 2e\alpha + 2f\alpha^2 = a\alpha + b\alpha^2 + c(-2\alpha + 8).$$

As before, we already know that $e\alpha + f\alpha^2 \in P$. Equating the constant terms, we have $2d = 8c$ and so $d = 4c \in P$, which leads to another contradiction.

Therefore, our assumption that P_P was principal must be incorrect. Then S_P is not a DVR and we must have $S \neq R$.

For more practice on these types of problems, we refer to lmfdb.org. In the "Number Fields" section, there is a giant database of irreducible polynomials, and the website supplies discriminants of the number fields along with an integral basis. If the integral basis is a power basis, then $R = S$; otherwise, we have $R \neq S$. We can then use the DVR characterization to verify this.

Now that we have seen why the DVR characterization is useful through our many examples, let's get back on track to proving it. We first consider why the condition $[R : S] = n < \infty$ is useful. Recall that $K = \text{Frac}(\mathcal{O}_K) = \text{Frac}(R)$, which we argued at the beginning of Section 3.3. Then for all $r \in R$, we have $nr \in S$ by Lagrange since $n(r + S) = nr + S = 0 + S$. In particular, if $x = \frac{a}{b} \in \text{Frac}(R)$, then we have $x = \frac{na}{nb} \in \text{Frac}(S)$, which implies that $\text{Frac}(R) \subseteq \text{Frac}(S)$. The reverse inclusion is obvious since $S \subseteq R$, so $\text{Frac}(S) = \text{Frac}(R) = K$. Consequently, if P is a nonzero prime ideal of S, then $\text{Frac}(S_P) = K$.

The following result from commutative algebra will be of great help to us. We leave out some of the details because we are more interested in its application.

Lemma 3.33: Lying-Over Theorem

Let $S \subseteq R$ be integral domains such that R is integral over S, and let P be a prime ideal of S. Then there exists a prime ideal Q of R such that $P = S \cap Q$.

Proof of Lemma 3.33.

Define $R_P := \{\frac{a}{b} : a \in R, b \in S \setminus P\}$. We leave it as an exercise to verify that R_P is a local ring. Note that this is *not* the localization of R by P since P is a prime ideal of S, not R. Therefore, despite having the same notation, we cannot immediately conclude that R_P is a local ring from our discussion in Section 3.5. This set is almost S_P, but we allow for the numerator to be in R.

Clearly, we have $S_P \subseteq R_P$. Moreover, R_P is integral over S_P; this can be verified using the finitely generated module characterization (Theorem 1.7). Let M be the unique maximal ideal of R_P. Consider $Q = M \cap R$. By **A1-3**, Q is a prime ideal of R. Moreover, we have

$$\begin{aligned} Q \cap S &= (M \cap R) \cap S \\ &= (M \cap S_P) \cap S \\ &= P_P \cap S = P. \end{aligned}$$

The second equality uses the fact that $R \supseteq S$ and $S_P \supseteq S$, so intersecting with R and S_P is redundant. Then R_P being integral over S_P implies that $M \cap S_P$ is maximal by **A1-3**, so $M \cap S_P$ is in fact the unique maximal ideal P_P. Finally, the last equality is because we are left with only the numerator part. □

We now prove the DVR characterization, with most of the heavy lifting being done by the lying-over theorem.

Proof of Theorem 3.31.

(1) ($\Rightarrow$) If $S = R$, then S_P is a DVR for all nonzero prime ideals P of S by Theorem 3.27.

($\Leftarrow$) Suppose that S_P is a DVR for all nonzero prime ideals P of S. Note that $R = \mathcal{O}_K$ is integral over S since $S \supseteq \mathbb{Z}$. Let P be a nonzero prime ideal of S. By the lying-over theorem (Lemma 3.33), there exists a prime ideal Q of R such that $P = Q \cap S$.

Claim 1. We have $S_P = R_Q$.

Proof of Claim 1. ($\subseteq$) Let $x \in S_P$. Then we can write $x = \frac{a}{b}$ where $a, b \in S$ and $b \notin P$. In particular, we have $a, b \in R$ and $b \notin Q$, so $x \in R_Q$.

($\supseteq$) We prove the contrapositive. Suppose that $\alpha \in K \setminus S_P$. Since $K = \mathrm{Frac}(S_P)$, we can write $\alpha = u\pi^n$ for some $u \in S_P^\times$ and $n \in \mathbb{Z}$, where π is a uniformizer for S_P. But $\alpha \notin S_P$, which implies that $n < 0$ (otherwise, we would have $\pi^n \in S_P$). Then $-1 - n \geq 0$, and so

$$\pi^{-1-n} \cdot \pi^n = \pi^{-1} \in S_P[\alpha],$$

where $\pi^{-1-n} \in S_P$ and $\pi^n \in S_P[\alpha]$. This implies that $S_P[\alpha] = K$ as we can generate all negative powers of π using $\pi^{-1} \in S_P[\alpha]$. However, observe that $S_P \subseteq R_Q \subsetneq K$ since Q is nonzero. This means that $\alpha \notin R_Q$, because $\alpha \in R_Q$ would imply $R_Q = K$. ■

Note that if $y \in R$, then we can write $y = \frac{a}{b}$ for some $a, b \in S$ since $R \subseteq \mathrm{Frac}(R) = \mathrm{Frac}(S) = K$. Fix $y \in R$ and consider the set of potential denominators

$$D = \{b \in S : by \in S\}.$$

We leave it as an exercise to verify that D is an ideal of S.

Claim 2. We have $D = S$.

Proof of Claim 2. Assume towards a contradiction that $D \neq S$. Let P be a prime ideal of S containing D. By the lying-over theorem (Lemma 3.33), we can find a prime ideal Q of R with $P = S \cap Q$. By Claim 1, we have $S_P = R_Q$. Moreover, if $y = \frac{a}{b}$ for some $a, b \in S$, then $by = a \in S$ and hence $b \in D \subseteq P$. This implies that $y \notin S_P = R_Q$, which is a contradiction since $y \in R \subseteq R_Q$. Thus, we must have $D = S$. ■

In particular, we have $1 \in D$, so for any $y \in R$, we also have $y \in S$. Therefore, we obtain $R = S$.

(2) Let P be a prime ideal of S containing a prime $p \in \mathbb{N}$ such that $p \nmid n$. Since $\gcd(p, n) = 1$, we see that $n \notin P$ for otherwise we would have $1 \in P$ by Bézout. Let Q be a prime ideal of R such that $P = Q \cap S$ obtained from the lying-over theorem (Lemma 3.33).

Claim 3. We have $S_P = R_Q$.

Note that this appears to be the same as Claim 1, but we have different hypotheses.

Proof of Claim 3. ($\subseteq$) The proof of this inclusion is identical to that of Claim 1.

($\supseteq$) Let $x \in R_Q$. Then we can write $x = \frac{a}{b}$ for some $a, b \in R$ with $b \notin Q$. By Lagrange, we have $na, nb \in S$. Moreover, since $b \notin P$ and $n \notin P$, it follows that $nb \notin P$ since P is a prime ideal. This implies that $x = \frac{a}{b} = \frac{na}{nb} \in S_P$. ■

This claim is enough to conclude the result because R_Q is a DVR by Theorem 3.27. □

3.9 The Kummer-Dedekind Theorem

Recall from Section 3.4 that we had two goals: proving that the ideal norm was multiplicative, and proving that $\langle p \rangle$ is usually easy to factor. The second goal is now in reach: this is the Kummer-Dedekind theorem.

Theorem 3.34: Kummer-Dedekind

Let K be a number field, which can be written as $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$. Let $R = \mathcal{O}_K$, let $S = \mathbb{Z}[\alpha]$, and let $m(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Let $p \in \mathbb{N}$ be a prime such that $p \nmid [R : S]$. Suppose that $m(x) \in \mathbb{Z}_p[x]$ factors into irreducibles as

$$m(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_k(x)^{e_k} \in \mathbb{Z}_p[x].$$

Let $P_i = \langle p_i(\alpha), p \rangle \subseteq R$. Then the prime factorization of $\langle p \rangle$ in R is

$$\langle p \rangle = P_1^{e_1} P_2^{e_2} \cdots P_k^{e_k}.$$

Proof of Theorem 3.34.

Consider the homomorphism $\varphi : \mathbb{Z}[x] \to R/P_i$ given by

$$\varphi(f(x)) = f(\alpha) + P_i.$$

Note that $\langle p_i(x), p \rangle \subseteq \ker \varphi$. Moreover, we see that

$$\mathbb{Z}[x]/\langle p_i(x), p \rangle \cong \mathbb{Z}_p[x]/\langle p_i(x) \rangle$$

is a field since $p_i(x) \in \mathbb{Z}_p[x]$ is irreducible, so $\langle p_i(x), p \rangle$ is maximal. In particular, we either have $\ker \varphi = \langle p_i(x), p \rangle$ or $\ker \varphi = \mathbb{Z}[x]$.

We claim that φ is surjective. To see this, note that $p \nmid [R : S] = [R : \mathbb{Z}[\alpha] + pR] \cdot [\mathbb{Z}[\alpha] + pR : S]$ so that p does not divide either of these degrees. Next, we can write $[R : pR]$ in two different ways. One way is

$$[R : pR] = [R : \mathbb{Z}[\alpha] + pR] \cdot [\mathbb{Z}[\alpha] + pR : pR],$$

and a second way is given by

$$[R : pR] = |R/pR| = N(\langle p \rangle) = |N_{K/\mathbb{Q}}(p)| = p^{[K : \mathbb{Q}]}.$$

Since $p \nmid [R : \mathbb{Z}[\alpha] + pR]$, it must be that $[R : \mathbb{Z}[\alpha] + pR] = 1$ and hence $R = \mathbb{Z}[\alpha] + pR$. Then a general element in R/P_i is of the form $f(\alpha) + pr + P_i = f(\alpha) + P_i$. We see that $\varphi(f(x)) = f(\alpha) + P_i$, so φ is surjective as claimed.

By the first isomorphism theorem, we see that either $R/P_i \cong \mathbb{Z}[x]/\langle p_i(x), p\rangle$ or $P_i = R$. Separating these two cases, we let $P_1, \dots, P_r$ be such that

$$R/P_i \cong \mathbb{Z}[x]/\langle p_i(x), p\rangle,$$

and let $P_{r+1} = \cdots = P_k = R$. Note that for $1 \le i \le r$, we have that $P_i = \langle p_i(\alpha), p\rangle$ is a prime ideal of R since $R/P_i \cong \mathbb{Z}[x]/\langle p_i(x), p\rangle \cong \mathbb{Z}_p[x]/\langle p_i(x)\rangle$ is a field. Set $f_i = \deg(p_i(x))$ so that

$$N(P_i) = |R/P_i| = p^{f_i}.$$

Exercise: Check that $P_1^{e_1} \cdots P_k^{e_k} = \langle p_1(\alpha), p\rangle^{e_1} \cdots \langle p_k(\alpha), p\rangle^{e_k} \subseteq \langle p\rangle$. (Hint: If we select a single p, we are done; otherwise, we get $p_1(\alpha)^{e_1} \cdots p_k(\alpha)^{e_k}$.)

Hence, we have that $P_1^{e_1} \cdots P_r^{e_r} \subseteq \langle p\rangle$ as the tail end of the P_i consists of just R. This implies that $\langle p\rangle \mid P_1^{e_1} \cdots P_r^{e_r}$ by Proposition 3.17, so the prime factorization of $\langle p\rangle$ is

$$\langle p\rangle = P_1^{d_1} \cdots P_r^{d_r}$$

for some $0 \le d_i \le e_i$. Taking norms, we obtain

$$p^{[K:\mathbb{Q}]} = N(P_1)^{d_1} \cdots N(P_r)^{d_r} = p_1^{f_1 d_1} \cdots p_r^{f_r d_r}$$

and hence $[K:\mathbb{Q}] = f_1 d_1 + \cdots + f_r d_r$. But we also know that $[K:\mathbb{Q}] = \deg(m(x)) = f_1 e_1 + \cdots + f_k e_k$. Since $0 \le d_i \le e_i$, this forces us to have $r = k$ and $d_i = e_i$ for all $1 \le i \le k$. □

In summary, let K be a number field, which can be written as $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$. Let $R = \mathcal{O}_K$, let $S = \mathbb{Z}[\alpha]$, and suppose we want to factor some nonzero proper ideal I of R.

We know that in theory, a prime factorization $I = P_1^{e_1} P_2^{e_2} \cdots P_k^{e_k}$ exists (by Theorem 3.18), and by the multiplicativity of the ideal norm (Theorem 3.30), we have

$$N(I) = N(P_1)^{e_1} N(P_2)^{e_2} \cdots N(P_k)^{e_k}.$$

Moreover, we know that $N(P_i) = |R/P_i| = p_i^{f_i}$ for some prime $p_i \in \mathbb{N}$ since R/P_i is a finite field.

By Lagrange, we know that $p_i \in P_i$, so $\langle p_i\rangle \subseteq P_i$ and hence $P_i \mid \langle p_i\rangle$. These P_i's are the candidates of the prime factors of I. As long as $p_i \nmid [R:S]$, the Kummer-Dedekind theorem tells us that $\langle p_i\rangle$ factors like the minimal polynomial of α in $\mathbb{Z}_{p_i}[x]$. In addition, if we have $P_i = \langle q_i(\alpha), p_i\rangle$ in the case where $p_i \nmid [R:S]$, then

$$N(P_i) = |\mathbb{Z}_{p_i}[x]/\langle q_i(x)\rangle| = p_i^{\deg(q_i(x))}. \qquad (\star)$$

This helps us determine the multiplicities e_i.

We go through an example of factoring an ideal. Let $f(x) = x^3 - x^2 + 3$, which is irreducible by the rational roots theorem and has discriminant $-231 = -3 \cdot 7 \cdot 11$. Let α be a root of $f(x)$, let $K = \mathbb{Q}(\alpha)$, and let $R = \mathcal{O}_K$. Let's factor the ideal $I = \langle \alpha + 2\rangle$. (This example is a bit artificial, but demonstrates all the techniques we need to use in general. Since $\operatorname{disc}(f(x)) = -231$ is squarefree, we could just apply Theorem 3.8.)

Note that $K = \mathbb{Q}(\alpha + 2)$, and the minimal polynomial of $\alpha + 2$ is simply $f(x-2)$ because $x \mapsto x + k$ is an isomorphism for any $k \in \mathbb{Z}$. This implies that

$$N(I) = |N_{K/\mathbb{Q}}(\alpha + 2)| = |f(-2)| = 9 = 3^2.$$

Hence, we only need to factor $\langle 3\rangle$. Since $3^2 \nmid \operatorname{disc}(f(x))$, we have $3 \nmid [R:S]$. Then $f(x) = x^3 - x^2 = x^2(x-1)$ over $\mathbb{Z}_3[x]$, so Kummer-Dedekind implies that $\langle 3\rangle = \langle \alpha, 3\rangle^2 \langle \alpha - 1, 3\rangle$.

Next, we need to consider which of these prime factors contain $\alpha + 2$, because $P \mid \langle \alpha + 2\rangle$ if and only if $\langle \alpha + 2\rangle \subseteq P$. We see that $\alpha + 2 \notin \langle \alpha, 3\rangle$, because otherwise, we would have $(\alpha + 3) - (\alpha + 2) = 1 \in \langle \alpha, 3\rangle$. On the other hand, we have $\alpha + 2 = \alpha - 1 + 3 \in \langle \alpha - 1, 3\rangle$, which implies that $I = \langle \alpha - 1, 3\rangle^{e_1}$ for some $e_1 \in \mathbb{N}$.

Taking norms above and making use of equation $(\star)$, we have that

$$9 = N(\langle \alpha - 1, 3\rangle)^{e_1} = (3^{\deg(x-1)})^{e_1} = 3^{e_1},$$

so we have $e_1 = 2$ and $I = \langle \alpha - 1, 3\rangle^2$.

We make one last remark. Suppose that K is a number field with $[K : \mathbb{Q}] = n$, and that $p \in \mathbb{N}$ is a prime with $\langle p\rangle = P_1^{e_1} \cdots P_k^{e_k}$ and $N(P_i) = p^{f_i}$ for all $i = 1, \ldots, k$. Taking norms, we have

$$p^n = N(\langle p\rangle) = p^{f_1 e_1} \cdots p^{f_k e_k},$$

which implies that $n = f_1 e_1 + \cdots + f_k e_k$.

3.10 Ramification

The Kummer-Dedekind theorem tells us how to factor the ideal $\langle p\rangle$ in the case that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, but what if we had $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$? These primes can be thought of as badly behaved.

Definition 3.35

Let K be a number field and let $p \in \mathbb{N}$ be prime. Suppose that $\langle p\rangle = P_1^{e_1} \cdots P_k^{e_k}$ is the prime factorization of $\langle p\rangle$ in $R = \mathcal{O}_K$, and write $N(P_i) = p^{f_i}$ for all $i = 1, \ldots, k$.

(1) We call e_i the **ramification index** of P_i over p.

(2) We call f_i the **residue field degree** of P_i over p.

(3) We say that p is **ramified** in K if there exists $i = 1, \ldots, k$ such that $e_i > 1$. Otherwise, we say that p is **unramified** in K.

The ramified primes are precisely the ones with multiplicity in their ideal prime factorization, and these are the "problematic" or "complicated" primes. The following result gives us a way of easily detecting these.

Theorem 3.36

Let K be a number field and let $p \in \mathbb{N}$ be prime. Then p is ramified in K if and only if $p \mid \operatorname{disc}(K)$.

Proof of Theorem 3.36.

($\Leftarrow$) This is beyond the scope of the course. However, it is within reach with a couple weeks of algebra.

($\Rightarrow$) Suppose that p is ramified in K. Then there exists a prime ideal P of $\mathcal{O}_K$ such that $p \in P$ and $P^2 \mid \langle p\rangle$. We write $\langle p\rangle = PI$ where I is another ideal of $\mathcal{O}_K$.

Note that if $Q \subseteq \mathcal{O}_K$ is a prime ideal with $p \in Q$, then $I \subseteq Q$. Indeed, we have $Q \mid \langle p\rangle$, which implies that $Q \mid I$, and hence $I \subseteq Q$ by Proposition 3.17. We could have $Q = P$, but this is fine since there is a copy of P in I due to ramification.

Moreover, we have $\langle p\rangle \subsetneq I$ because otherwise, applying ideal cancellation (Proposition 3.15) to $\langle p\rangle = PI$ would imply that $P = R$. Therefore, we can pick an element $\alpha \in I \setminus \langle p\rangle$.

Let $\{v_1, \ldots, v_n\}$ be an integral basis for $\mathcal{O}_K$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$. We can write

$$\alpha = m_1 v_1 + \cdots + m_n v_n$$

for some $m_i \in \mathbb{Z}$. Note that we cannot have $p \mid m_i$ for all $i = 1, \ldots, n$ because this would imply $\alpha \in \langle p\rangle$.

Hence, we may assume without loss of generality that $p \nmid m_1$. From elementary column operations, we have

$$\begin{aligned}\operatorname{disc}(\alpha, v_2, \ldots, v_n) &= \operatorname{disc}(m_1 v_1, v_2, \ldots, v_n) \\ &= m_1^2 \operatorname{disc}(v_1, \ldots, v_n) \\ &= m_1^2 \operatorname{disc}(K).\end{aligned}$$

To complete the proof, it is enough to show that $p \mid \operatorname{disc}(\alpha, v_2, \ldots, v_n)$ since $p \nmid m_1$. We may extend each embedding $\sigma_i : K \to \mathbb{C}$ to $\sigma_i : L \to L$ where $K \subseteq L$ and $L/\mathbb{Q}$ is a Galois extension. In particular, we can take L to be the Galois closure of K (obtained by adjoining all the conjugates) so that $\sigma_i \in \operatorname{Gal}(L/\mathbb{Q})$.

Let $S = \mathcal{O}_L$. Suppose that Q is a prime ideal of S such that $p \in Q$. By **A1-3**, we see that $Q \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ containing p, which implies that $I \subseteq Q \cap \mathcal{O}_K$ by our previous remark. In particular, we have $\alpha \in Q$. Similarly, for any $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$, we have $\alpha \in \sigma^{-1}(Q)$, where $\sigma^{-1}(Q)$ is a prime ideal of S using the fact that $\sigma(S) = S$. This means that $\sigma(\alpha) \in Q$.

Note that the entire first column of the matrix corresponding to $\operatorname{disc}(\alpha, v_2, \ldots, v_n)$ consists of $\alpha \in Q$ and $\sigma_i(\alpha) \in Q$. This implies that $\operatorname{disc}(\alpha, v_2, \ldots, v_n) \in Q \cap \mathbb{Z} = p\mathbb{Z}$ and thus $p \mid \operatorname{disc}(\alpha, v_2, \ldots, v_n)$. □

4 Ideal Class Group

4.1 Preliminaries

Let K be a number field and let $R = \mathcal{O}_K$. Recall from **A2-3** that if X is the set of nonzero ideals of R, then we can put an equivalence relation on X by $I \sim J$ if and only if $\alpha I = \beta J$ for some nonzero $\alpha, \beta \in R$. Then

$$G_K := \{[I] : I \in X\}$$

is a group under the operation $[I][J] = [IJ]$, called the **ideal class group** of K. The identity element is the equivalence class of nonzero principal ideals. In fact, this construction works for all Dedekind domains because nonzero ideals are invertible due to Proposition 3.13.

Definition 4.1

Let K be a number field. The **class number** of K is defined to be

$$\mathrm{cl}(K) = |G_K|.$$

The ideal class group G_K is structural information that is attached to the number field K or the ring of integers $\mathcal{O}_K$. The class number $\mathrm{cl}(K)$ is a measure (in terms of complexity) of how far away $\mathcal{O}_K$ is from being a PID because we have that $\mathrm{cl}(K) = 1$ if and only if $\mathcal{O}_K$ is a PID.

The next result tells us that $\mathrm{cl}(K)$ is also a measure of how far away $\mathcal{O}_K$ is from being a UFD, and so having unique prime factorization of elements!

Proposition 4.2

Let R be a Dedekind domain. Then R is a PID if and only if R is a UFD.

Proof of Proposition 4.2.

($\Rightarrow$) This holds for any ring R.

($\Leftarrow$) Suppose that R is a UFD and let I be a nonzero proper ideal of R. By Proposition 3.13, we can find an ideal J of R such that $IJ = \langle \alpha \rangle$, where $\alpha \in I$ is nonzero. But we can write $\alpha = p_1^{n_1} \cdots p_k^{n_k}$ for some prime elements $p_i \in R$ and $n_i \in \mathbb{N}$. Then

$$IJ = \langle \alpha \rangle = \langle p_1^{n_1} \cdots p_k^{n_k} \rangle = \langle p_1 \rangle^{n_1} \cdots \langle p_k \rangle^{n_k},$$

where each $\langle p_i \rangle$ is a prime ideal of R. It follows that

$$I = \langle p_{i_1} \rangle^{m_1} \cdots \langle p_{i_\ell} \rangle^{m_\ell} = \langle p_{i_1}^{m_1} \cdots p_{i_\ell}^{m_\ell} \rangle$$

for some $i_1, \ldots, i_\ell \in \{1, \ldots, k\}$, so I is principal and R is a PID. □

At this point, it is not obvious that $\mathrm{cl}(K) < \infty$. Therefore, our next goal is to show that G_K is a finite group.

Proposition 4.3

Let K be a number field and let $R = \mathcal{O}_K$. Then there exists $\lambda > 0$ such that for all nonzero ideals I of R, there is an nonzero element $\alpha \in I$ satisfying

$$N(\langle \alpha \rangle) \leq \lambda N(I).$$

Note that we always have $N(I) \leq N(\langle\alpha\rangle)$ since $\langle\alpha\rangle \subseteq I$ and hence $I \mid \langle\alpha\rangle$. This proposition gives us an inequality in the other direction up to some $\lambda > 0$.

Proof of Proposition 4.3.

Let $n = [K : \mathbb{Q}]$, let $\{v_1, \ldots, v_n\}$ be an integral basis for $\mathcal{O}_K$, and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in $\mathbb{C}$. Pick $m \in \mathbb{N}$ such that $m^n \leq N(I) < (m+1)^n$. Consider the elements of the form

$$m_1 v_1 + \cdots + m_n v_n,$$

where $0 \leq m_i \leq m$ and $m_i \in \mathbb{Z}$. There are $(m+1)^n$ such elements. Since $(m+1)^n > N(I) = |R/I|$, there exist two such elements that are congruent modulo I. Subtracting these yields a nonzero $\alpha \in I$ of the form $\alpha = m_1 v_1 + \cdots + m_n v_n$ where $0 \leq |m_i| \leq m$. Then we obtain

$$\begin{aligned} N(\langle\alpha\rangle) = |N_{K/\mathbb{Q}}(\alpha)| &= \left|\prod_{i=1}^n \sigma_i(\alpha)\right| = \prod_{i=1}^n |\sigma_i(\alpha)| \\ &\leq \prod_{i=1}^n \sum_{j=1}^n |m_j \sigma_i(v_j)| \leq \prod_{i=1}^n \sum_{j=1}^n m|\sigma_i(v_j)| \\ &= m^n \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(v_j)| \leq N(I) \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(v_j)|. \end{aligned}$$

Taking $\lambda = \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(v_j)|$ gives the result. □

The next result tells us that every ideal class has a representative whose norm is bounded.

Proposition 4.4

Let K be a number field and let $R = \mathcal{O}_K$. Let $\lambda > 0$ be as in Proposition 4.3. For all nonzero ideals I of R, there exists an ideal J of R such that $[I] = [J]$ and $N(J) \leq \lambda$.

Proof of Proposition 4.4.

Let I be a nonzero ideal of R. Consider the ideal class $[I]^{-1} = [I']$ represented by some ideal I' of R. By Proposition 3.13, we can find an ideal J of R such that $I'J = \langle\alpha\rangle$, where $\alpha \in I$ is the nonzero element chosen as in Proposition 4.3. Taking norms gives us

$$N(I')N(J) = N(\langle\alpha\rangle) \leq \lambda N(I'),$$

and thus $N(J) \leq \lambda$. Moreover, we have $[I'][J] = [\langle\alpha\rangle] = [\langle 1\rangle]$, so $[J] = [I']^{-1} = [I]$. □

This gives us the finiteness of the ideal class group.

Corollary 4.5

Let K be a number field. Then G_K is finite.

Proof of Corollary 4.5.

Let $[I] \in G_K$ be an ideal class. By Proposition 4.4, we may assume that $N(I) \leq \lambda$. Suppose that the prime factorization of I is $I = P_1^{n_1} \cdots P_k^{n_k}$, where $N(P_i) = p_i^{f_i}$ for all $i = 1, \ldots, k$. Since $p_i \in P_i$, we have $P_i \mid \langle p_i\rangle$. Note that we must have $p_i \leq \lambda$. Moreover, there are only finitely many prime ideals Q of R such that $p \in Q$, where $p \in \mathbb{N}$ is prime with $p \leq \lambda$. □

4.2 Minkowski's Bound

We know that the ideal class group is finite, but what now? The bound λ we found has a couple of problems:

(1) It is difficult to compute; we require an integral basis for $\mathcal{O}_K$, the embeddings of K in $\mathbb{C}$, and there are a large amount of sums and products.

(2) In addition, λ can be significantly larger than needed.

It turns out that there is a much better bound, obtained from our work on the geometry of numbers in Assignment 5! In **A5-5**, we proved the following result:

Theorem 4.6: Minkowski

Let K be a number field with $[K:\mathbb{Q}] = n$, and let $R = \mathcal{O}_K$. Let s be the number of pairs of nonreal embeddings of K in $\mathbb{C}$. Then every ideal class of R contains an ideal I such that

$$N(I) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |\text{disc}(K)|^{1/2}.$$

The main thing to notice is that $n!/n^n$ approaches 0 extremely quickly, so this bound tends to be small. This helps us narrow down the primes to look at.

Example. Let $K = \mathbb{Q}(\alpha)$, where α is a root of the 2-Eisenstein polynomial $f(x) = x^3 - 2x - 2$. with discriminant $-76 = -2^2 \cdot 19$. By **A6-4**, we have $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Since $\text{disc}(f(x)) = -76 < 0$, we see that $f(x)$ must have a pair of nonreal roots, because if they were all real, then $\text{disc}(f(x))$ would be positive. But $\deg(f(x)) = 3$, so this gives us $s = 1$. Then the Minkowski bound is

$$B_K = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)^1 \sqrt{76} \approx 2.467.$$

By Theorem 4.6, we have $G_K = \{[I] : N(I) \leq 2\}$. It follows that G_K is generated by the prime ideals P such that $N(P) = 2$ by the multiplicativity of the ideal norm. But working modulo 2, we have $f(x) = x^3 \in \mathbb{Z}_2[x]$. Then Kummer-Dedekind gives us $\langle 2\rangle = \langle \alpha, 2\rangle^3 = \langle \alpha\rangle^3$, where $2 = \alpha^3 - 2\alpha \in \langle\alpha\rangle$. Therefore, we have $G_K = \{[\langle 1\rangle], [\langle\alpha\rangle]\} = \{[\langle 1\rangle]\}$ and $\text{cl}(K) = 1$, which shows that $\mathcal{O}_K$ is a PID.

Example. Let $K = \mathbb{Q}(\sqrt{-23})$. We wish to compute the ideal class group of K (i.e. find a well-known group that is isomorphic to G_K). Note that G_K is a finite abelian group, so it is the direct product of cyclic groups.

We have $-23 \equiv 1 \pmod 4$, so $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1}{2}(1 + \sqrt{-23})$. Since $(2\alpha - 1)^2 = -23$, we obtain $4\alpha^2 - 4\alpha + 24 = 0$, implying that the minimal polynomial of α is $f(x) = x^2 - x + 6$. We know that the roots of $f(x)$ are α and its conjugate, which are not real. Then we have $s = 1$, and moreover, we know that $\text{disc}(K) = -23$. Therefore, the Minkowski bound is

$$B_K = \frac{2!}{2^2} \cdot \frac{4}{\pi} \cdot \sqrt{23} \approx 3.053.$$

Then every ideal class of K contains a representative with norm at most 3, and so G_K is generated by the prime ideals containing 2 or 3. Modulo 2, we have $f(x) = x(x-1) \in \mathbb{Z}_2[x]$, so Kummer-Dedekind implies that $\langle 2\rangle = \langle \alpha, 2\rangle\langle \alpha - 1, 2\rangle$. Set $P_1 = \langle \alpha, 2\rangle$ and $P_2 = \langle \alpha - 1, 2\rangle$, which satisfy $N(P_1) = N(P_2) = 2$. Similarly, working modulo 3, we have that $f(x) = x(x-1) \in \mathbb{Z}_3[x]$, we so $\langle 3\rangle = \langle \alpha, 3\rangle\langle \alpha - 1, 3\rangle$. We set $Q_1 = \langle \alpha, 3\rangle$ and $Q_2 = \langle \alpha - 1, 3\rangle$ with $N(Q_1) = N(Q_2) = 3$. Therefore, we obtain

$$G_K = \{[\langle 1\rangle], [P_1], [P_2], [Q_1], [Q_2]\}$$

since these are the only ideals of norm at most 3.

Since $\langle 2\rangle = P_1P_2$, we see that $[P_1]^{-1} = [P_2]$. Similarly, we have $[Q_1]^{-1} = [Q_2]$ since $\langle 3\rangle = Q_1Q_2$. In particular, we can write $G_K = \langle [P_1], [Q_1]\rangle$. Notice that $\alpha^2 - \alpha + 6 = 0$, so $-6 = \alpha(\alpha - 1)$. Using the equivalence relation on the nonzero ideals of $\mathcal{O}_K$, we have that

$$(\alpha - 1)P_1 = \langle \alpha(\alpha-1), 2(\alpha-1)\rangle = \langle -6, 2(\alpha-1)\rangle = 2\langle 3, \alpha - 1\rangle = 2Q_2,$$

so $[P_1] = [Q_2]$. By taking inverses, we obtain $[P_2] = [P_1]^{-1} = [Q_2]^{-1} = [Q_1]$, so we have reduced the ideal class group to $G_K = \langle [P_1]\rangle$. That is, G_K is a cyclic group.

It remains to find the order of $[P_1]$. First, suppose that P_1 were a principal ideal. Write $P_1 = \langle \beta\rangle$ where $\beta = \frac{1}{2}(a + b\sqrt{-23})$ for some $a, b \in \mathbb{Z}$. Taking norms, we have

$$2 = |N_{K/\mathbb{Q}}(\beta)| = \left|\frac{a + b\sqrt{-23}}{2}\right|\left|\frac{a - b\sqrt{-23}}{2}\right| = \frac{a^2 + 23b^2}{4},$$

which implies that $a^2 + 23b^2 = 8$. But this has no solutions, so P_1 cannot be principal. Next, suppose that $P_1^2 = \langle \beta\rangle$ where β is as above. This time, taking norms gives

$$4 = \frac{a^2 + 23b^2}{4},$$

so $a^2 + 23b^2 = 16$. This has solutions $a = \pm 4$ and $b = 0$. But this would imply that $P_1^2 = \langle 2\rangle = P_1P_2$. By the uniqueness of ideal prime factorization, we obtain $P_1 = P_2$. But then α and $\alpha - 1$ are both in P_1 and hence $1 \in P_1$, which is a contradiction. Hence, P_1^2 is not principal.

Now, observe that

$$G_K = \{[\langle 1\rangle], [P_1], [P_2], [Q_1], [Q_2]\} = \{[\langle 1\rangle], [P_1], [P_1]^{-1}\}$$

since we have seen that $[P_1] = [P_2]^{-1} = [Q_2]$ and $[P_2] = [Q_1]$. In showing that P_1 is not principal, we have $[P_1] \neq [\langle 1\rangle]$. This also gives us $[P_1]^{-1} \neq [\langle 1\rangle]$. Indeed, if we had $[P_1]^{-1} = [\langle 1\rangle]$, then $[\langle 1\rangle] = [P_1][P_2] = [P_1][\langle 1\rangle]$, which would imply that $[P_1] = [\langle 1\rangle]$. Moreover, since P_1^2 is not principal, we have $[P_1] \neq [P_1]^{-1}$. Therefore, the elements $[\langle 1\rangle]$, $[P_1]$, and $[P_1]^{-1}$ are all distinct, which gives

$$G_K = \{[\langle 1\rangle], [P_1], [P_1]^{-1}\} \cong \mathbb{Z}_3.$$

Exercise. Let $K = \mathbb{Q}(\sqrt{-15})$. Show that $G_K \cong \mathbb{Z}_2$.

Example. Let $K = \mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{C}$ is a root of $f(x) = x^3 + 4x + 1$. Note that $f(x)$ has discriminant -283, which is prime. Let $R = \mathcal{O}_K$. Is R a PID?

Since $\operatorname{disc}(f(x)) = -283$ is squarefree, we have $R = \mathbb{Z}[\alpha]$ and $\operatorname{disc}(K) = \operatorname{disc}(f(x)) = -283$. Moreover, it is negative, so $s = 1$. This gives the Minkowski bound

$$B_K = \frac{3!}{3^3} \cdot \frac{4}{\pi} \cdot \sqrt{283} \approx 4.76.$$

Then every ideal class contains a representative with norm at most 4, and G_K is generated by the prime ideals containing 2 or 3.

- Modulo 2, we have $f(x) = x^3 + 1 = (x+1)(x^2 + x + 1) \in \mathbb{Z}_2[x]$, so $\langle 2\rangle = \langle \alpha + 1, 2\rangle\langle \alpha^2 + \alpha + 1, 2\rangle$. Set $P_1 = \langle \alpha + 1, 2\rangle$ and $P_2 = \langle \alpha^2 + \alpha + 1, 2\rangle$. We have $N(P_1) = 2$ and $N(P_2) = 2^2 = 4$.
- Modulo 3, we have $f(x) = x^3 + x + 1 = (x-1)(x^2 + x + 2) \in \mathbb{Z}_3[x]$, so $\langle 3\rangle = \langle \alpha - 1, 3\rangle\langle \alpha^2 + \alpha^2 + 2, 3\rangle$. Set $Q_1 = \langle \alpha - 1, 3\rangle$ and $Q_2 = \langle \alpha^2 + \alpha^2 + 2, 3\rangle$. Note that $N(Q_1) = 3$ and $N(Q_2) = 3^2 = 9 > 4$.

Putting these together, the ideals with norm at most 4 are

$$G_K = \{[\langle 1\rangle], [P_1], [Q_1], [P_2], [P_1^2]\}.$$

Note that $[P_1^2] = [P_1]^2$ and $[P_1] = [P_2]^{-1}$. Our next idea is to look at $[Q_1]$ first since all the other elements are generated by $[P_1]$. By polynomial long division, we find that

$$x^3 + 4x + 1 = (x-1)(x^2 + x + 5) + 6.$$

This looks very promising to us since $6 = 2 \cdot 3$, and we can write $-6 = (\alpha - 1)(\alpha^2 + \alpha + 5)$. Observe that

$$\begin{aligned}(\alpha^2 + \alpha + 5)Q_1 &= \langle (\alpha-1)(\alpha^2+\alpha+5), 3(\alpha^2+\alpha+5)\rangle \\ &= \langle 6, 3(\alpha^2+\alpha+5)\rangle \\ &= 3\langle 2, \alpha^2+\alpha+5\rangle \\ &= 3\langle 2, \alpha^2+\alpha+1\rangle \\ &= 3P_2,\end{aligned}$$

so $[Q_1] = [P_2] = [P_1]^{-1}$ and $G_K = \langle [P_1] \rangle$. To conclude if $R = \mathcal{O}_K$ is a PID or not, we must check whether or not P_1 is a principal ideal. But this is a very difficult problem in general! It turns out that in this case, P_1 is not principal, so $\mathcal{O}_K$ is not a PID. We'll revisit this example later.

We devise a strategy to check that an ideal P_1 of $\mathcal{O}_K$ is not principal. Suppose that we could write $P_1 = \langle \beta \rangle$. Then we also have $P_1 = \langle u\beta \rangle$ for all $u \in \mathcal{O}_K^\times$.

(1) Compute the group of units $\mathcal{O}_K^\times$.

(2) Argue that $P_1 = \langle u\beta \rangle$ for "small" $u\beta$. We'll explain what we mean by "small" later.

(3) This will give us a short list of $u\beta$ to check that $P_1 \neq \langle u\beta \rangle$, so P_1 is not principal.

Alternatively, if it were the case that $P_1 = \langle u\beta \rangle$ for some $u\beta$ in that short list, then P_1 is principal.

5 Dirichlet's Unit Theorem

5.1 Motivation

We begin with a simple example. Let $K = \mathbb{Q}(\sqrt{2})$ and $R = \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. We compute the group of units $R^\times$.

From ring theory, we know that $a + b\sqrt{2} \in R^\times$ if and only if $|a^2 - 2b^2| = 1$. By inspection, we have that ± 1 and $1 + \sqrt{2}$ are units of R.

Claim. If $u \in R^\times$ with $u > 1$, then $u \geq 1 + \sqrt{2}$.

Proof of Claim. Suppose that $u \in R^\times$ with $1 < u \leq 1 + \sqrt{2}$. To prove the claim, it suffices to show that $u = 1 + \sqrt{2}$. Write $u = a + b\sqrt{2}$ for some $a, b \in \mathbb{Z}$ and note that

$$|a^2 - 2b^2| = |a - b\sqrt{2}||a + b\sqrt{2}| = 1.$$

Since $u = a + b\sqrt{2} > 1$, we must have $|a - b\sqrt{2}| < 1$, or equivalently, $-1 < a - b\sqrt{2} < 1$. Adding these inequalities together with $1 < u \leq 1 + \sqrt{2}$ yields $0 < 2a < 2 + \sqrt{2}$, which implies that $a = 1$ since $a \in \mathbb{Z}$. But then $1 < 1 + b\sqrt{2} \leq 1 + \sqrt{2}$, and the only solution is $b = 1$. We conclude that $a = b = 1$ and $u = 1 + \sqrt{2}$. ■

Suppose now that $u \in \mathbb{R}^\times \setminus \{\pm 1\}$. By considering $\pm u$ and $\pm 1/u$, we may assume that $u > 1$. By the claim, we have $u \geq 1 + \sqrt{2}$. In particular, we can find $k \in \mathbb{N}$ such that

$$(1 + \sqrt{2})^k \leq u < (1 + \sqrt{2})^{k+1}.$$

Dividing through by $(1+\sqrt{2})^k$, we have $1 \leq u(1+\sqrt{2})^{-k} < 1+\sqrt{2}$. Then the claim tells us that $1 = u(1+\sqrt{2})^{-k}$ and thus $u = (1 + \sqrt{2})^k$. By considering $\pm u$ and $\pm 1/u$ as before, we can conclude that

$$R^\times = \{\pm(1 + \sqrt{2})^k : k \in \mathbb{Z}\}.$$

In fact, this argument can be generalized to compute $\mathcal{O}_K^\times$ where $K = \mathbb{Q}(\sqrt{m^2 + 1})$ for some $m \in \mathbb{Z}$.

5.2 The Unit Theorem

The following definition is the idea of $\mathbb{Z}$-linear independence with respect to multiplication instead of addition.

Definition 5.1

Let $\varepsilon_1, \ldots, \varepsilon_m \in \mathbb{C} \setminus \{0\}$. We say $\varepsilon_1, \ldots, \varepsilon_m$ are **multiplicatively independent** if for $n_1, \ldots, n_m \in \mathbb{Z}$, we have $\varepsilon_1^{n_1} \cdots \varepsilon_m^{n_m} = 1$ if and only if $n_1 = \cdots = n_m = 0$.

This leads us to Dirichlet's unit theorem, which allows us to characterize the units of a ring of integers.

Theorem 5.2: Dirichlet's Unit Theorem

Let K be a number field with $[K : \mathbb{Q}] = n$ and let $R = \mathcal{O}_K$. Let r be the number of real embeddings of K in $\mathbb{C}$, and let s be the number of complex embedding pairs of K in $\mathbb{C}$. Let $m = r + s - 1$. Then there exists multiplicatively independent $\varepsilon_1, \ldots, \varepsilon_m \in K$ such that

$$R^\times = \{\zeta \varepsilon_1^{n_1} \cdots \varepsilon_m^{n_m} : n_i \in \mathbb{Z},\ \zeta \text{ a root of unity in } K\}.$$

We call $\varepsilon_1, \ldots, \varepsilon_m$ a **fundamental system of units** for K.

In our above example, the multiplicatively independent set consisted of just $\varepsilon_1 = 1 + \sqrt{2}$ and the roots of unity in $K = \mathbb{Q}(\sqrt{2})$ are ± 1, so the result we got is in line with the theorem.

Let's make some observations on what Dirichlet's unit theorem tells us.

(1) Note that $n = r + 2s$.

(2) Suppose that $\varepsilon_1^{n_1} \cdots \varepsilon_m^{n_m} = \varepsilon_1^{k_1} \cdots \varepsilon_m^{k_m}$. We can write this as

$$\varepsilon_1^{n_1 - k_1} \cdots \varepsilon_m^{n_m - k_m} = 1.$$

But $\varepsilon_1, \ldots, \varepsilon_m$ are multiplicatively independent, so $n_i - k_i = 0$ and hence $n_i = k_i$ for all $i = 1, \ldots, m$. So multiplicative independence gives us the unique representation of products in this form, similar to linear independence with addition.

(3) Suppose now that $\zeta_1 \varepsilon_1^{n_1} \cdots \varepsilon_m^{n_m} = \zeta_2 \varepsilon_1^{k_1} \cdots \varepsilon_m^{k_m}$ for some roots of unity ζ_1 and ζ_2. We can find $N \in \mathbb{N}$ such that $\zeta_1^N = \zeta_2^N = 1$, which gives us

$$\varepsilon_1^{Nn_1} \cdots \varepsilon_m^{Nn_m} = \varepsilon_1^{Nk_1} \cdots \varepsilon_m^{Nk_m}.$$

By (2), we have $Nn_i = Nk_i$ and hence $n_i = k_i$ for all $i = 1, \ldots, m$. But then $\zeta_1 = \zeta_2$ as well, so we also have unique representations in the form $\zeta \varepsilon_1^{n_1} \cdots \varepsilon_m^{n_m}$.

(4) **Exercise.** By applying Dirichlet's unit theorem, we have

$$R^\times \cong T \times \mathbb{Z}^m,$$

where T is the group of roots of unity in K. This can be done by identifying $\zeta \varepsilon_1^{n_1} \cdots \varepsilon_m^{n_m}$ with $(\zeta, (n_1, \ldots, n_m))$. In other words, we are identifying ε_i with the standard basis vector e_i.

(5) Suppose that $r > 0$ so that K has a real embedding $\sigma : K \to \mathbb{R}$. Let $\zeta \in K$ be a root of unity with $\zeta^\ell = 1$ for some $\ell \in \mathbb{N}$. Then we have

$$\sigma(\zeta)^\ell = \sigma(\zeta^\ell) = \sigma(1) = 1.$$

Then $\sigma(\zeta)$ is a real root of unity, so $\sigma(\zeta) \in \{\pm 1\}$. But σ is injective and fixes $\mathbb{Q}$, so we must have $\zeta \in \{\pm 1\}$. Therefore, in the case that $r > 0$, the group of roots of unity is simply $\{\pm 1\}$.

To prove Dirichlet's unit theorem, we need the Minkowski business that we worked with on Assignment 5.

(1) A **lattice** in $\mathbb{R}^n$ is a set $L = \operatorname{span}_{\mathbb{Z}}\{v_1, \ldots, v_k\}$ where $\{v_1, \ldots, v_k\} \subseteq \mathbb{R}^n$ is $\mathbb{R}$-linearly independent. We say that L is a **full lattice** if $k = n$. (This is a slight relaxation of the definition we gave in **A5-1**. The definition of lattice we gave there required that $k = n$, which corresponds to a full lattice here.)

(2) Let K be a number field with $[K : \mathbb{Q}] = n$, and let r and s be as usual. Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings of K in $\mathbb{C}$, and let $\sigma_{r+1}, \ldots, \sigma_{r+s}$ be the representatives of the complex pair embeddings of K in $\mathbb{C}$. Define a map $\psi : K \to \mathbb{R}^n$ by

$$\psi(x) = (\sigma_1(x), \ldots, \sigma_r(x), \ldots, \operatorname{Re}(\sigma_{r+1}(x)), \operatorname{Im}(\sigma_{r+1}(x)), \ldots, \operatorname{Re}(\sigma_{r+s}(x)), \operatorname{Im}(\sigma_{r+s}(x))).$$

Through an abuse of notation, we will write

$$\psi(x) = (\sigma_1(x), \ldots, \sigma_r(x), \sigma_{r+1}(x), \ldots, \sigma_{r+s}(x))$$

where we identify each $\sigma_{r+j}(x) = a + bi$ with the pair (a, b). We call ψ the **Minkowski embedding**. Note that ψ is an embedding of additive groups; in other words, it is a map $(K, +) \to (\mathbb{R}^n, +)$.

We then define $M_K := \psi(\mathcal{O}_K)$, which we saw was a full lattice in $\mathbb{R}^n$ by **A5-2**. We call M_K the **Minkowski lattice** of K.

The Minkowski lattice M_K gives us a way to geometrically visualize $\mathcal{O}_K$. For example, consider $K = \mathbb{Q}(\sqrt{2})$. Since $\mathcal{O}_K$ is dense in $\mathbb{R}$, viewing $\mathcal{O}_K$ on the real line is not of much help. But drawing M_K in $\mathbb{R}^2$ gives us a parallelogram type shape, which is a lot easier to visualize.

Next, note that $R^\times$ is a multiplicative group and $\mathbb{R}^n$ is an additive group, so the restriction of the Minkowski embedding $\psi : R^\times \to \psi(R^\times)$ is not a homomorphism. But we can use logarithms to transform multiplication into addition!

From now on, we fix the following notation.

- Let K be a number field with $[K : \mathbb{Q}] = n$.
- Let r be the number of real embeddings of K in $\mathbb{C}$, and let s be the number of complex embedding pairs of K in $\mathbb{C}$. Let $\sigma_1, \dots, \sigma_r$ denote the real embeddings, and let $\sigma_{r+1}, \dots, \sigma_{r+s}$ be the complex pair representatives.
- Let $\psi : K \to \mathbb{R}^n$ be the Minkowski embedding, where we use the abuse of notation
$$\psi(x) = (\sigma_1(x), \dots, \sigma_{r+s}(x))$$
that we discussed above by identifying the real and imaginary parts of $\sigma_{r+s}(x)$ with just $\sigma_{r+s}(x)$ itself.
- Let $\varphi : K^\times \to \mathbb{R}^{r+s}$ be the map
$$\varphi(x) = (\log|\sigma_1(x)|, \dots, \log|\sigma_{r+s}(x)|).$$
Here, there is no abuse of notation, and $|\cdot|$ denotes the complex modulus.

Proposition 5.3

The restriction $\varphi : R^\times \to \mathbb{R}^{r+s}$ is a group homomorphism.

We leave the proof of Proposition 5.3 as an exercise; it really just uses logarithm properties.

Proposition 5.4

We have $\varphi(R^\times) \subseteq H$, where H is the hyperplane
$$H = \{x \in \mathbb{R}^{r+s} : x_1 + \cdots + x_r + 2x_{r+1} + \cdots + 2x_{r+s} = 0\}.$$

Proof of Proposition 5.4.

Consider a point $\varphi(a) = (\log|\sigma_1(a)|, \dots, \log|\sigma_{r+s}(a)|)$ where $a \in R^\times$. Note that
$$\begin{aligned}
&\log|\sigma_1(a)| + \cdots + \log|\sigma_r(a)| + 2\log|\sigma_{r+1}(a)| + \cdots + 2\log|\sigma_{r+s}(a)| \\
&= \log|\sigma_1(a)\cdots\sigma_r(a)\sigma_{r+1}(a)^2\cdots\sigma_{r+s}(a)^2| \\
&= \log|N_{K/\mathbb{Q}}(a)| \\
&= \log 1 = 0,
\end{aligned}$$
where the second equality follows from part (a) of **A5-4**, so $\varphi(a) \in H$. □

Recall that the dimension of a hyperplane is always one less than the ambient space. In particular, we see that $\dim_{\mathbb{R}}(H) = r + s - 1 = m$.

We now state a couple of facts about lattices:

(1) If $L \subseteq \mathbb{R}^n$ is a lattice and $X \subseteq L$ is bounded, then X is finite.

(2) We say that $A \subseteq \mathbb{R}^n$ is **discrete** if for all $a \in A$, there exists $\varepsilon > 0$ such that $B_\varepsilon(a) \cap A = \{a\}$ (intuitively, the points are spread out). It is known that every discrete subgroup $L \subseteq \mathbb{R}^n$ is a lattice; in fact, this is an equivalent definition of a lattice.

Proposition 5.5

The kernel of $\varphi : K^\times \to \mathbb{R}^{r+s}$ is finite.

Proof of Proposition 5.5.

We know that $\ker\varphi \subseteq \{x \in K^\times : |\sigma_i(x)| = 1 \text{ for all } i = 1, \dots, r+s\} =: X$. Then $\psi(X) \subseteq M_K$ is bounded as each component of the Minkowski map is in the interval $[-1, 1]$. By fact (1) above, we have that $\psi(X)$ is finite. But ψ is injective, so X is finite, and hence $\ker\varphi \subseteq X$ is finite. □

We recall the following result from Galois theory.

Proposition 5.6

Let F be a field. Then every finite subgroup $G \subseteq F^\times$ is cyclic.

Proof of Proposition 5.6.

By the fundamental theorem of finite abelian groups, we can write

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

where each n_i is a prime power. Let $N = n_1 \cdots n_k = |G|$ and $M = \operatorname{lcm}(n_1, \dots, n_k)$. It is clear that $M \leq N$. Conversely, every element of G (of which there are N of them) is a root of $x^M - 1$, which has at most M roots. This means that $N \leq M$, so $M = N$. It follows that the n_i's are powers of distinct primes, so $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \cong \mathbb{Z}_N$ is cyclic. □

Next, let's look at the structure of the kernel of φ.

Proposition 5.7

We have $\ker\varphi = \{\zeta \in K : \zeta \text{ a root of unity}\}$.

Proof of Proposition 5.7.

We know from Proposition 5.5 that $\ker\varphi$ is finite. Write $N = |\ker\varphi|$. By Lagrange, we know that if $x \in \ker\varphi$, then $x^N = 1$. Conversely, if $\zeta \in K$ with $\zeta^\ell = 1$, we have

$$\sigma_i(\zeta)^\ell = \sigma_i(\zeta^\ell) = \sigma_i(1) = 1$$

for all $i = 1, \dots, r+s$. Then

$$\varphi(\zeta) = (\log|\sigma_1(\zeta)|, \dots, \log|\sigma_{r+s}(\zeta)|) = (0, \dots, 0),$$

which implies that $\zeta \in \ker\varphi$. □

Since K is a field and $\ker\varphi \subseteq K^\times$ is a finite subgroup, we see that $\ker\varphi$ is cyclic by Proposition 5.6.

Proposition 5.8

We have that $\varphi(R^\times) \subseteq \mathbb{R}^{r+s}$ is a lattice.

Proof of Proposition 5.8.

It is enough to show that $\varphi(R^\times)$ is discrete because it is clear that $\varphi(R^\times)$ being the image of a group under a homomorphism is a subgroup of $\mathbb{R}^{r+s}$, and so we can apply fact (2) about lattices.

Fix $N \in \mathbb{N}$ and consider the N-cube $X = [-N, N]^{r+s} \subseteq \mathbb{R}^{r+s}$. Let $Y = \varphi^{-1}(X)$. For all $u \in Y$, we have $\varphi(u) \in X$, implying that $|\log|\sigma_i(u)|| \leq N$. Then there must exist some $N' \in \mathbb{N}$ such that $|\sigma_i(u)| \leq N'$ for all $u \in Y$. (This is because the logarithm is increasing, so if we could find arbitrarily large $|\sigma_i(u)|$, then $|\log|\sigma_i(u)||$ would also be arbitrarily large.) It follows that $\psi(Y) \subseteq M_K$ is finite by lattice fact (1). But ψ is injective, so Y is finite. By a set counting argument (exercise), it follows that $\varphi(R^\times) \cap X$ is finite. But every finite set is discrete, so we are done. □

The following result is then enough to prove Dirichlet's unit theorem.

Proposition 5.9

We have $W := \operatorname{span}_{\mathbb{R}} \varphi(R^\times) = H$.

We'll save the proof of Proposition 5.9 for later, as it is quite tricky. First, let's see how it implies Dirichlet's unit theorem (Theorem 5.2).

Proof of Dirichlet.

We know that $\varphi(R^\times) \subseteq \mathbb{R}^{r+s}$ is a lattice by Proposition 5.8, so we can write $\varphi(R^\times) = \operatorname{span}_{\mathbb{Z}}\{u_1, \dots, u_k\}$ where $\{u_1, \dots, u_k\}$ is $\mathbb{R}$-linearly independent. Then by Proposition 5.9, we have

$$H = \operatorname{span}_{\mathbb{R}} \varphi(R^\times) = \operatorname{span}_{\mathbb{R}}\{u_1, \dots, u_k\} \cong \mathbb{Z}^k.$$

This means that $\{u_1, \dots, u_k\}$ is a basis for H, so $k = \dim_{\mathbb{R}} H = r + s - 1$. This gives us $\varphi(R^\times) \cong \mathbb{Z}^{r+s-1}$. Combining this with the first isomorphism theorem, it follows that there exists an isomorphism

$$\rho : R^\times / \ker\varphi \to \mathbb{Z}^{r+s-1}.$$

For all $i = 1, \dots, r + s - 1$, we can pick a representative $\varepsilon_i \ker\varphi \in R^\times / \ker\varphi$ such that $\rho(\varepsilon_i \ker\varphi) = e_i$, where e_i is the i-th standard basis vector in $\mathbb{Z}^{r+s-1}$. For all $u \in R^\times$, we can write

$$\rho(u \ker\varphi) = n_1 e_1 + \cdots + n_m e_m$$

for some $n_i \in \mathbb{Z}$. But then $u \ker\varphi = \varepsilon_1^{n_1} \cdots \varepsilon_m^{n_m} \ker\varphi$ since φ is an isomorphism. In particular, there exists $\zeta \in \ker\varphi$ such that $u = \zeta\varepsilon_1^{n_1} \cdots \varepsilon_m^{n_m}$. Note that $\varepsilon_1, \dots, \varepsilon_m$ is a multiplicatively independent set since the standard basis vectors e_i are $\mathbb{Z}$-linearly independent, which completes the proof. □

Finally, we prove Proposition 5.9 using Minkowski's lemma (**A5-3**), which states that if a Lebesgue measurable set is compact, convex, and symmetric about the origin with "large" volume, then it contains some nonzero point from the lattice.

Proof of Proposition 5.9.

We already know that $W \subseteq H$. To prove that $H \subseteq W$, we show that $W^\perp \subseteq H^\perp$, noting that orthogonal complements reverse inclusion. To do this, we'll proceed by contrapositive. Suppose that $z = (z_1, \dots, z_{r+s}) \in \mathbb{R}^{r+s}$ with $z \notin H^\perp$. We claim that $z \notin W^\perp$.

Define the map $f : K^\times \to \mathbb{R}$ by $f(x) = z \cdot \varphi(x)$, where $\cdot$ denotes the dot product in $\mathbb{R}^{r+s}$. If we can show that there exists some $u \in R^\times$ such that $f(u) \neq 0$, then we're done. Let $C = (2/\pi)^s |\operatorname{disc}(K)|^{1/2}$ and pick any positive $c_1, \dots, c_{r+s} \in \mathbb{R}$ such that

$$C = c_1 \cdots c_r c_{r+1}^2 \cdots c_{r+s}^2.$$

This is always possible since $C \in \mathbb{R}$; one possible choice is $c_1 = C$ and $c_i = 1$ otherwise. Then the set

$$A := \{(x_1, \dots, x_n) \in \mathbb{R}^n : |x_i| \le c_i \text{ for all } i = 1, \dots, r \text{ and } x_i^2 + x_{i+s}^2 \le c_i^2 \text{ for all } i = r+1, \dots, r+s\}$$

is compact, convex, symmetric about the origin, and Lebesgue measurable. In particular, we have

$$m(A) = \left(\prod_{i=1}^{r} 2c_i\right)\left(\prod_{i=r+1}^{r+s} \pi c_i^2\right) = 2^r \pi^s C = 2^{r+s}|\mathrm{disc}(K)|^{1/2} = 2^n \cdot \frac{1}{2^s}|\mathrm{disc}(K)|^{1/2} = 2^n \operatorname{Vol}(M_K).$$

By Minkowski's lemma (**A5-3**), there exists a nonzero $a \in A \cap M_K$. We write $a = \psi(b)$ for some $b \in \mathcal{O}_K$.

We have that $|N_{K/\mathbb{Q}}(b)| = N(a) \le c_1 \cdots c_r c_{r+1}^2 \cdots c_{r+s}^2 = C$, where $N(\cdot)$ denotes the map from **A5-4** and the inequality is from the fact that $a \in A$.

Claim. We have $|\sigma_i(b)| \ge c_i/C$ for all $i = 1, \dots, r$ and $|\sigma_i(b)|^2 \ge c_i^2/C$ for all $i = r+1, \dots, r+s$.

Proof of Claim. Since $a = \psi(b) = (\sigma_1(b), \dots, \sigma_{r+s}(b)) \in A$, we have that $|\sigma_i(b)| \le c_i$ for all $i = 1, \dots, r$ and $|\sigma_i(b)|^2 \le c_i^2$ for all $i = r+1, \dots, r+s$.

Suppose towards a contradiction that there exists $i = 1, \dots, r$ with $|\sigma_i(b)| < c_i/C$. Then we have

$$1 \le |N_{K/\mathbb{Q}}(b)| = |\sigma_1(b)| \cdots |\sigma_r(b)||\sigma_{r+1}(b)|^2 \cdots |\sigma_{r+s}(b)|^2 < \frac{c_1 \cdots c_r c_{r+1}^2 \cdots c_{r+s}^2}{C} = \frac{C}{C} = 1,$$

which is a contradiction. If we assume there exists $i = r+1, \dots, r+s$ such that $|\sigma_i(b)| < c_i^2/C$, the same argument applies. ■

There are finitely many nonzero principal ideals of $\mathcal{O}_K$ with norm at most C, say $\langle b_1 \rangle, \dots, \langle b_\ell \rangle$. Without loss of generality, suppose that $\langle b \rangle = \langle b_1 \rangle$. Then we can write $b = ub_1$ for some $u \in R^\times$.

Let $L = z \cdot (\log c_1, \dots, \log c_{r+s}) = z_1 \log c_1 + \cdots + z_{r+s} \log c_{r+s}$. Note that

$$\begin{aligned} f(b) = f(ub_1) &= z \cdot \varphi(ub_1) \\ &= z \cdot (\varphi(u) + \varphi(b_1)) \\ &= f(u) + f(b_1). \end{aligned}$$

From this, it can be shown using the claim and the triangle inequality that

$$|f(u) - L| \le |f(b_1)| + \left(\sum_{i=1}^{r} |z_i| + \frac{1}{2}\sum_{i=r+1}^{r+s} |z_i|\right) \cdot \log C =: B.$$

Note that B depends only on z and C, and not the choice of $c_1, \dots, c_{r+s}$.

Case 1. If $r + s - 1 = 0$, then $\dim_{\mathbb{R}} H = r + s - 1 = 0$ so that $W \subseteq H = \{0\}$, and hence $W = H$.

Case 2. Suppose that $r + s - 1 > 0$. By replacing $z \notin H^\perp$ with a multiple of $[1, \dots, 1, 2, \dots, 2]^T \in H^\perp$ (where 1 appears r times and 2 appears s times), we may assume that there exists $p, q \in \{1, \dots, r+s\}$ such that $z_p = 0$ and $z_q \ne 0$. Now, pick representatives $c_1, \dots, c_{r+s} > 0$ with $C = c_1 \cdots c_r c_{r+1}^2 \cdots c_{r+s}^2$ such that

(1) c_q is arbitrarily large;

(2) c_p is arbitrarily small;

(3) $c_i = 1$ for all $i \notin \{p, q\}$.

Note that we have $L = z \cdot (\log c_1, \dots, \log c_{r+s}) = z_q \log c_q$ since $z_p = 0$ and $c_i = 1$ for all $i \notin \{p, q\}$. By a careful choice of c_p and c_q, we may assume that $|L| = |z_q \log c_q| > B$. But we also have $|f(u) - L| \le B$, which implies that $f(u) \ne 0$. We conclude that $f(u) = z \cdot \varphi(u) \ne 0$, so $z \notin W^\perp$. □

We revisit the example from the end of Section 4.2. Let $K = \mathbb{Q}(\alpha)$ where $\alpha \in \mathbb{C}$ is a root of $f(x) = x^3 + 4x + 1$. The discriminant of $f(x)$ is -283, which is prime, so $R = \mathcal{O}_K = \mathbb{Z}[\alpha]$. We claimed that R was not a PID. We had reduced the problem to determining if the ideal $P = \langle \alpha + 1, 2 \rangle$ was principal or not, and now we have the tools to show that it is in fact not principal.

Suppose that $P = \langle \alpha + 1, 2 \rangle$ were principal with $P = \langle \beta \rangle$. Note that $\alpha \in R^\times$ since the constant term of $f(x)$ is 1 and hence $|N_{K/\mathbb{Q}}(\alpha)| = 1$. In particular, we also have $P = \langle \alpha^t \beta \rangle$ for all $t \in \mathbb{Z}$.

Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f(x)$ where $\alpha_1 \in \mathbb{R}$ and $\alpha_2, \alpha_3 \in \mathbb{C} \setminus \mathbb{R}$ with $\overline{\alpha_2} = \alpha_3$. The embeddings of K in $\mathbb{C}$ are $\sigma_i(\alpha) = \alpha_i$ for $i \in \{1, 2, 3\}$. Using a computer, we find that

$$\alpha_1 \approx 0.24627 \approx 1/4.$$

This implies that $1 = |N_{K/\mathbb{Q}}(\alpha)| = |\alpha_1||\alpha_2|^2 \approx |\alpha_2|^2/4$, so $|\alpha_2| \approx 2$. Then we have

$$\varphi(\alpha) \approx (\log 1/4, \log 2) = (-\log 4, \log 2).$$

Write $\varphi(\beta) = (\log|\beta_1|, \log|\beta_2|)$ where $\beta_1 = \sigma_1(\beta)$ and $\beta_2 = \sigma_2(\beta)$. This yields

$$\varphi(\alpha^t \beta) = t\varphi(\alpha) + \varphi(\beta) \approx (-t \log 4 + \log|\beta_1|, t \log 2 + \log|\beta_2|).$$

As we alluded to before, we now reduce to the "small" cases where

$$0 \leq \log|\beta_1| \leq \log 4,$$

or equivalently, $1 \leq |\beta_1| \leq 4$. But we also have $2 = N(P) = |N_{K/\mathbb{Q}}(\beta)| = |\beta_1||\beta_2|^2$, which combined with

$$|\beta_2|^2 \leq |\beta_1||\beta_2|^2 \leq 4|\beta_2|^2$$

gives $\frac{1}{\sqrt{2}} \leq |\beta_2| \leq \sqrt{2}$. In **A9-2**, we show that the only possibilities are $\beta \in \{1, 3 + \alpha^2\}$.

It is clear that $P \neq \langle 1 \rangle$, and we have $P \neq \langle 3 + \alpha^2 \rangle$ by checking that $|N_{K/\mathbb{Q}}(3 + \alpha^2)| \neq 2$. It follows that P is not principal, so R is not a PID.

A Assignment Problems

Sometimes, we'll use facts that we cover on the assignments, so we list the problems here for reference.

Assignment 1.

A1-1 Let K be a number field.

(a) Let $\alpha \in K$. Suppose that α is a root of

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Prove that $a_n\alpha \in \mathcal{O}_K$.

(b) Prove that there exists a basis for K over $\mathbb{Q}$ consisting entirely of algebraic integers.

A1-2 Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$ and let

$$\mathbb{Z}[\sqrt{3}, \sqrt{7}] = \{a + b\sqrt{3} + c\sqrt{7} + d\sqrt{21} : a, b, c, d \in \mathbb{Z}\}.$$

Prove that $\mathcal{O}_K \neq \mathbb{Z}[\sqrt{3}, \sqrt{7}]$.

A1-3 Let R and S be integral domains, where R is a subring of S. Suppose S is integral over R. That is, assume that every element of S is integral over R.

(a) Prove that R is a field if and only if S is a field.

(b) Let Q be a prime ideal of S and let $P = Q \cap R$. Prove that P is a prime ideal of R, and that P is maximal if and only if Q is maximal.

A1-4 Let L/K be a finite extension of number fields. Prove that every embedding (injective ring homomorphism) $\varphi : K \to \mathbb{C}$ can be extended to exactly $[L : K]$ embeddings $\psi : L \to \mathbb{C}$.

Assignment 2.

A2-1 Let $K = \mathbb{Q}(\sqrt{-5})$.

(a) Suppose that $\{a, b\} \subseteq \mathcal{O}_K$ is an integral basis for $\mathcal{O}_K$. Prove that we must have

$$\det \begin{bmatrix} a & \bar{a} \\ b & \bar{b} \end{bmatrix}^2 = -20.$$

Here, we mean $\overline{x + y\sqrt{-5}} = x - y\sqrt{-5}$ for $x, y \in \mathbb{Q}$.

(b) Suppose that $a, b \in \mathcal{O}_K$ satisfy

$$\det \begin{bmatrix} a & \bar{a} \\ b & \bar{b} \end{bmatrix}^2 = -20.$$

Prove that $\{a, b\}$ is an integral basis for $\mathcal{O}_K$.

A2-2 Let $\alpha \in \mathbb{C}$ such that $\alpha^4 + 3\alpha^2 + 6\alpha - 3 = 0$.

(a) Compute $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$.

(b) Compute $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^4 + \alpha + 2)$.

A2-3 Let R be an integral domain and let I and J be ideals of R. Recall that

$$IJ := \{a_1b_1 + \cdots + a_nb_n : n \in \mathbb{N},\ a_i \in I,\ b_i \in J\}$$

is also an ideal of R. Now, let X be the set of nonzero ideals of R.

(a) Put a relation $\sim$ on X by $I \sim J$ if and only if $\langle\alpha\rangle I = \langle\beta\rangle J$ for some nonzero $\alpha, \beta \in R$. Prove that $\sim$ is an equivalence relation on X.

(b) Prove that $I, J \in X$ are isomorphic as R-modules if and only if $I \sim J$.

(c) Prove that if $I \in X$ and there exists a nonzero $\alpha \in R$ such that $\langle\alpha\rangle I$ is principal, then I itself is principal. What does this tell you about the principal ideals of R relative to $\sim$?

(d) Prove that the set of ideal classes (with respect to $\sim$) form a group under the operation $[I][J] = [IJ]$ if and only if for all $I \in X$, there exists $J \in X$ such that IJ is principal.

A2-4 Let $M = \mathbb{Z}^n$ and let N be a submodule of M such that $\text{rank}(N) = n$.

(a) Prove that M/N is finite.

(b) Read Theorem 2.10 of Keith Conrad's notes, which also requires Definition 2.8. If $\{e_1, \ldots, e_n\}$ is the standard integral basis for M, this guarantees the existence of a basis $\{d_1e_1, \ldots, d_ne_n\}$ for N, where $d_i \in \mathbb{Z}$.

(c) Prove that $M/N \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$.

(d) Let $\{v_1, \ldots, v_n\}$ be an integral basis for N. Since $N \subseteq M$, we can find $a_{ij} \in \mathbb{Z}$ such that $v_i = \sum_{j=1}^{n} a_{ij}e_j$. Use this to construct the matrix $A = [a_{ij}] \in M_n(\mathbb{Z})$. Prove that $[M : N] = |\det(A)|$, where $[M : N]$ is the index of the subgroup N in M.

Assignment 3.

A3-1 Let $\alpha \in \mathbb{C}$ be a root of $f(x) = x^4 - x^3 + 2x^2 - x + 2$, and let $K = \mathbb{Q}(\alpha)$. Prove that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Note that $f(x)$ is irreducible by the rational roots theorem.

A3-2 Let $\alpha \in \mathbb{C}$ be a root of $f(x) = x^3 + 18x - 26$, and let $K = \mathbb{Q}(\alpha)$. Note that $f(x)$ is irreducible by Eisenstein with $p = 2$.

(a) Prove that $\beta = \frac{\alpha^2-\alpha+1}{3} \in \mathcal{O}_K$.

(b) Compute $\text{disc}(1, \alpha, \beta)$.

(c) Prove that $[\mathcal{O}_K : \mathbb{Z}[\alpha]] \in \{3, 6\}$.

A3-3 Let $\alpha \in \mathbb{C}$ be a root of $f(x) = x^3 - x^2 - 2x - 8$, and let $K = \mathbb{Q}(\alpha)$. Note that $f(x)$ is irreducible by the rational roots theorem.

(a) Prove that $\beta = \frac{4}{\alpha} \in \mathcal{O}_K$.

(b) Compute $\text{Tr}_{K/\mathbb{Q}}(\alpha)$, $\text{Tr}_{K/\mathbb{Q}}(\beta)$, $\text{Tr}_{K/\mathbb{Q}}(\alpha^2)$, $\text{Tr}_{K/\mathbb{Q}}(\beta^2)$, and $\text{Tr}_{K/\mathbb{Q}}(\alpha\beta)$.

(c) Compute $\text{disc}(1, \alpha, \beta)$.

(d) Prove that $\{1, \alpha, \beta\}$ is an integral basis for $\mathcal{O}_K$.

A3-4 Let $\alpha \in \mathbb{C}$ be a root of $f(x) = x^3 - x^2 - 2x - 8$ as before, and let $K = \mathbb{Q}(\alpha)$. Prove that there does not exist $\theta \in \mathcal{O}_K$ such that $\{1, \theta, \theta^2\}$ is an integral basis for $\mathcal{O}_K$.

Hint: By **A3-3**, we know that $\{1, \alpha, \beta\}$ is an integral basis for $\mathcal{O}_K$, so we have $\theta = a + b\alpha + c\beta$ and $\theta^2 = A + B\alpha + C\beta$ for some $a, b, c, A, B, C \in \mathbb{Z}$. Try to write A, B, C in terms of a, b, c.

Assignment 4.

A4-1 (a) Prove that every UFD is integrally closed.

(b) Prove that every PID is a Dedekind domain.

(c) Give an example of a UFD that is not a Dedekind domain.

A4-2 Let $K = \mathbb{Q}(\alpha)$ where α is a root of $f(x) = x^3 - x^2 - 3$. Note that $\text{disc}(f(x)) = -255$. Factor $\langle p\rangle$ as a product of prime ideals in $\mathcal{O}_K$ for all $p \in \{2, 3, 5, 7\}$. Which of these primes divide 255? How does this affect the corresponding prime factorization?

A4-3 Suppose that $[K : \mathbb{Q}] = n$ and let P be a nonzero prime ideal of $\mathcal{O}_K$. Prove that P contains a prime number $p \in \mathbb{N}$ and that $\mathcal{O}_K/P$ contains at most p^n elements.

A4-4 Let α be a root of $f(x) = x^3 - 2x - 3$.

(a) Prove that $R := \mathbb{Z}[\alpha]$ is a Dedekind domain.

(b) Let $I = \langle \alpha - 5 \rangle \subseteq R$. Prove that $|R/I| = 112$.

(c) Factor $\langle 2 \rangle$ as a product of prime ideals.

(d) Factor $\langle 7 \rangle$ as a product of prime ideals.

(e) Factor I as a product of prime ideals.

Assignment 5. This assignment was a guided reading exercise on the geometry of numbers, following Marcus' *Number Fields* pages 93 to 99.

A5-1 A **lattice** in $\mathbb{R}^n$ is defined to be a subset L of $\mathbb{R}^n$ of the form $L = \text{span}_{\mathbb{Z}}\{v_1, \dots, v_n\}$, where $\{v_1, \dots, v_n\}$ is a basis for $\mathbb{R}^n$ over $\mathbb{R}$. We define the **volume** of L by

$$\text{Vol}(L) = |\det [v_1| \cdots |v_n]|.$$

(a) Prove that the definition of the volume of a lattice is independent of the choice of basis.

(b) Let $M \subseteq L$ be lattices in $\mathbb{R}^n$. Prove that

$$\text{Vol}(M) = [L : M] \cdot \text{Vol}(L).$$

A5-2 Let K be a number field and let $R = \mathcal{O}_K$. Suppose that $\sigma_1, \dots, \sigma_r$ are the real-valued embeddings of K in $\mathbb{C}$ and that $\tau_1, \dots, \tau_{2s}$ are the non-real-valued (i.e. complex) embeddings of K in $\mathbb{C}$. Assume that $\tau_{i+1} = \overline{\tau_i}$ for all odd i. Consider the **Minkowski map** $\psi : K \to \mathbb{R}^n$ given by

$$\psi(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \text{Re}(\tau_1(\alpha)), \text{Im}(\tau_1(\alpha)), \text{Re}(\tau_3(\alpha)), \text{Im}(\tau_3(\alpha)), \dots).$$

(a) Prove that $\psi(R)$ is a lattice in $\mathbb{R}^n$. We will denote this lattice by M_K and we call it the **Minkowski lattice** of K.

(b) Prove that

$$\text{Vol}(M_K) = \frac{1}{2^s} |\text{disc}(K)|^{1/2}.$$

(c) Let I be a nonzero ideal of R so that $L_I := \psi(I)$ is a sublattice of M_K. Prove that

$$\text{Vol}(L_I) = \frac{1}{2^s} |\text{disc}(K)|^{1/2} N(I).$$

A5-3 We now take a look at Minkowski's lemma. Let L be a lattice in $\mathbb{R}^n$ and let $E \subseteq \mathbb{R}^n$ be such that

(1) E is convex (for all $a, b \in E$ and $t \in [0, 1]$, we have $(1 - t)a + tb \in E$);

(2) E is Lebesgue measurable;

(3) if $a \in E$, then $-a \in E$.

Furthermore, assume that E is large; more precisely, assume that $m(E) > 2^n \text{Vol}(L)$ where $m(E)$ denotes the Lebesgue measure of E. It turns out that E is so big that it must contain a nonzero vector from L. If E is compact, then the strict inequality can be weakened to $\geq$.

(a) Read about what Lebesgue measure is from page 96 of Marcus.

(b) Read the proof of Minkowski's lemma from pages 96 and 97 of Marcus.

A5-4 Let K, R, r, and s be as in **A5-2**. For $x = (x_1, \dots, x_n) \in \mathbb{R}^n$, let

$$N(x) = x_1 x_2 \cdots x_r (x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2).$$

(a) Prove that if $\alpha \in R$ and $x = \psi(\alpha)$, then $N(x) = N_{K/\mathbb{Q}}(\alpha)$.

(b) Let $A \subseteq \mathbb{R}^n$ be compact and satisfy conditions (1), (2), and (3) from **A5-3**, where A has positive Lebesgue measure. Additionally, assume that $|N(a)| \leq 1$ for all $a \in A$. Prove that if L is a lattice in $\mathbb{R}^n$, then there exists a nonzero vector $x \in L$ with

$$|N(x)| \leq \frac{2^n}{m(A)} \operatorname{Vol}(L).$$

Hint: You can freely use the fact that if $A \subseteq \mathbb{R}^n$ is Lebesgue measurable and $t \in \mathbb{R}$, then tA is Lebesgue measurable with $m(tA) = |t|^n m(A)$.

A5-5 Let K, R, r, and s be as in **A5-2**. Consider the set

$$A = \left\{ x \in \mathbb{R}^n : |x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leq n \right\}.$$

It can be shown that A satisfies the hypotheses from part (b) of **A5-4**.

(a) From pages 98 and 99 of Marcus, read the integration-based argument that

$$m(A) = \frac{n^n}{n!} 2^r \left(\frac{\pi}{2}\right)^s.$$

(b) Prove that every lattice L in $\mathbb{R}^n$ contains a nonzero vector $x \in L$ such that

$$|N(x)| \leq \frac{n!}{n^n} \left(\frac{8}{\pi}\right)^s \operatorname{Vol}(L).$$

(c) Prove that every ideal class of R (as per **A2-3**) contains an ideal I such that

$$N(I) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s |\operatorname{disc}(K)|^{1/2}.$$

Assignment 6.

A6-1 Let $\alpha \in \mathbb{C}$ be an algebraic integer and let $S = \mathbb{Z}[\alpha]$. Suppose that $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial of α and let $p \in \mathbb{N}$ be prime. Suppose the irreducible factorization of $f(x) \in \mathbb{Z}_p[x]$ is

$$f(x) = p_1(x)^{n_1} p_2(x)^{n_2} \cdots p_k(x)^{n_k} \in \mathbb{Z}_p[x].$$

Prove that the prime ideals of S containing p are exactly

$$P_i = \langle p_i(\alpha), p \rangle.$$

Hint: Retrace isomorphisms.

A6-2 Let $S = \mathbb{Z}[\sqrt{5}]$ and let $P = \langle \sqrt{5} + 1, 2 \rangle$.

(a) Prove that P is the only prime ideal of S containing 2.

(b) Prove that S_P is not a DVR.

(c) Prove that $\langle 2 \rangle \neq P^2$. Why does this not contradict our prime factorization fact (Theorem 3.8)?

A6-3 (a) Let $\alpha \in \mathbb{C}$ be a root of the irreducible polynomial $f(x) = x^3 - x^2 - 8x - 18$, whose discriminant is $-9300 = -2^2 \cdot 3 \cdot 5^2 \cdot 31$. Let $K = \mathbb{Q}(\alpha)$, let $R = \mathcal{O}_K$, and let $S = \mathbb{Z}[\alpha]$. Use the DVR characterization (Theorem 3.31) to prove that $R = S$.

(b) Let $\alpha \in \mathbb{C}$ be a root of the irreducible polynomial $f(x) = x^3 - 6x - 16$, whose discriminant is $-6048 = -2^5 \cdot 3^3 \cdot 7$. Let $K = \mathbb{Q}(\alpha)$, let $R = \mathcal{O}_K$, and let $S = \mathbb{Z}[\alpha]$. Use the DVR characterization (Theorem 3.31) to prove that $R \neq S$.

A6-4 Let $p \in \mathbb{N}$ be a prime number and let $\alpha \in \mathbb{C}$ be the root of a p-Eisenstein polynomial (i.e. a monic, integer polynomial which is irreducible by p-Eisenstein). Let $R = \mathcal{O}_{\mathbb{Q}(\alpha)}$ and $S = \mathbb{Z}[\alpha]$.

(a) Prove that there is exactly one prime ideal P of S that contains p.

(b) Let P be the prime ideal from part (a). Prove that S_P is a DVR and prove that α is a uniformizer for S_P.

Assignment 7.

A7-1 In this problem, we explore where the ideal class equivalence relation comes from. Let R be a Dedekind domain with field of fractions $K = \text{Frac}(R)$. A **fractional ideal** of K is any set of the form αI, where $\alpha \in K^\times$ and I is a nonzero ideal of R. We define the product of two fractional ideals by $(\alpha I)(\beta J) = \alpha\beta IJ$. Let G denote the set of all fractional ideals of K.

(a) List three results from lecture whose proof has used fractional ideals.

(b) Prove that the multiplication of fractional ideals is well-defined.

(c) Prove that G forms a group under the above multiplication.

(d) Prove that every proper fractional ideal can be uniquely written in the form $P_1^{n_1} \cdots P_k^{n_k}$, where each P_i is a nonzero prime ideal of R and $n_i \in \mathbb{Z}$.

(e) Let H denote the set of fractional ideals of the form αR where $\alpha \in K^\times$. Prove that H is a subgroup of G.

(f) Let $R = \mathcal{O}_K$ where K is a number field. Prove that G/H is isomorphic to the ideal class group of K.

A7-2 Let $K = \mathbb{Q}(\alpha)$ be a number field with $\alpha \in \mathcal{O}_K$. Let $R = \mathcal{O}_K$, let $S = \mathbb{Z}[\alpha]$, let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α, and let $p \in \mathbb{N}$ be a prime such that $p \nmid \text{disc}(\alpha)$. Prove that $f(x) \in \mathbb{Z}_p[x]$ can be written as a product of distinct irreducible polynomials in $\mathbb{Z}_p[x]$.

A7-3 Let $\alpha \in \mathbb{C}$ be a root of $f(x) = x^3 - 2x + 5$. How many nonzero ideals of $\mathbb{Z}[\alpha]$ have norm 8 or less?

A7-4 Let $\alpha \in \mathbb{C}$ be a root of the irreducible polynomial $f(x) = x^4 - 2x^3 + 3x^2 - 1$, whose discriminant is -976. Let $K = \mathbb{Q}(\alpha)$.

(a) Prove that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(b) Prove that $\mathcal{O}_K$ is a PID.

Assignment 8.

A8-1 Compute the ideal class group of $\mathbb{Q}(\sqrt{-21})$.

A8-2 Compute the ideal class group of $\mathbb{Q}(\sqrt{10})$.

A8-3 Compute the ideal class group of $\mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{C}$ is a root of $f(x) = x^3 + 3x - 6$. Note that $\text{disc}(f(x)) = -1080 = -2^3 \cdot 3^3 \cdot 5$.

A8-4 List the elements of $\mathcal{O}_K^\times$, where $K = \mathbb{Q}(\sqrt{26})$.

Assignment 9.

A9-1 Let L/K be an extension of number fields with $L \neq K$. Prove that if $\mathcal{O}_K^\times = \mathcal{O}_L^\times$, then $[L : K] = 2$. Give an example of such an extension.

A9-2 Let $\alpha \in \mathbb{C}$ be a root of $f(x) = x^3 + 4x + 1$, whose discriminant is -283. Find all $\beta \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ such that $\psi(\beta) = (\beta_1, \beta_2)$ satisfies $1 \leq \beta_1 \leq 4$ and $\frac{1}{\sqrt{2}} \leq |\beta_2| \leq \sqrt{2}$.

Hint: Use a computer to approximate the real and complex pair of roots of $f(x)$.

A9-3 Let $K = \mathbb{Q}(\alpha)$ where $\alpha \in \mathbb{C}$ is a root of $f(x) = x^3 - 7x^2 + 14x - 7$. You may assume that $f(x)$ has three real roots, lying in the intervals $(0.7, 0.8)$, $(2.4, 2.5)$, and $(3.8, 3.9)$. Let $u_1 = \alpha - 1$ and $u_2 = \alpha - 2$. Prove that u_1 and u_2 are multiplicatively independent units of $\mathcal{O}_K$.

Hint: If $u_1^a = u_2^b$, consider $\psi(u_1^a) = \psi(u_2^b)$.