# 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 $\alpha^n$ 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. $\alpha$ 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 $\beta$ 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 $\beta$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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

$$M = Rm_1 + \cdots + Rm_n := \{r_1m_1 + \cdots + r_nm_n : r_1, \ldots, r_n \in R\}.$$

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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\pi$ 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 $\pi$ 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 $\alpha$ relative to $K/\mathbb{Q}$ is defined to be $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) := \mathrm{Tr}(T_\alpha)$.

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

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

Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of $\alpha$ (that is, the roots of $p(x)$ in $\mathbb{C}$). Recall that the roots of the characteristic polynomial of an operator are the eigenvalues $\lambda_i$ (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 $\alpha$, which must be sent to another conjugate of $\alpha$. 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 $T_\alpha$ and let $p(x) \in \mathbb{Q}[x]$ be the minimal polynomial of $\alpha$. 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 $T_\alpha$ 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 $\lambda_i$ denote the eigenvalues of $f(x) \in \mathbb{Q}[x]$, the characteristic polynomial of $T_\alpha$. When $p(x) \in \mathbb{Q}[x]$ is the minimal polynomial of $\alpha$ 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 $\alpha$, 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 $\sigma_i$ 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 $\rho_i$ are extensions of $\sigma_i$. 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 $\alpha$. 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 $\alpha$ 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 $\{x_1, \ldots, x_n\}$ 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

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

Note that $\varphi$ 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 $\varphi$. Note that if $\varphi(x) = (0, \ldots, 0)$, then $\mathrm{Tr}_{K/\mathbb{Q}}(xx_i) = 0$ for all $i = 1, \ldots, n$. 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 $\varphi$ 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 $\{x_1, \ldots, x_n\} \subseteq \mathcal{O}_K$ 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 $\{x_1, \ldots, x_n\}$ 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 $\{ax_1, \ldots, ax_n\} \subseteq I$ 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 $\sigma_i$ 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 $\sigma_i$ 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 $\alpha$ 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 $\alpha$. 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 $\alpha$ 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 $\sigma_i$ 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 $\alpha$ 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 $\alpha$. 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 $\varphi$ 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 $\varphi$ 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 $\alpha$ 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 $\alpha$. 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 $\alpha^2 + \alpha + 1 = 0$. We'll assume that $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$ here. The minimal polynomial of $\alpha$ 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 $P_1, \ldots, P_r$ 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 $i \in \{1, \ldots, r\}$ 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 $\lambda IJ$ 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 $\lambda$ 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 $IR = IP$. Cancellation of ideals (Proposition 3.15) implies that $P = R$, which is a contradiction. 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!

**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 $Q_1 \subseteq P_1$. 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 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.

# 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 $\alpha$ 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 $\operatorname{rank}(N) = n$.

(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 $\{d_1 e_1, \ldots, d_n e_n\}$ 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 $\operatorname{disc}(1, \alpha, \beta)$.

(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 $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha)$, $\operatorname{Tr}_{K/\mathbb{Q}}(\beta)$, $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha^2)$, $\operatorname{Tr}_{K/\mathbb{Q}}(\beta^2)$, and $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha\beta)$.

(c) Compute $\operatorname{disc}(1, \alpha, \beta)$.

(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 $a, b, c$.