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 hot topics typically discussed in a first-year number theory course include primes, divisibility, the Euclidean algorithm, and of most interest to us, 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, the canonical example of a principal ideal domain (PID) 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 $\alpha = (1+\sqrt{5})/2$. 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

Now that we are properly motivated, 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 $(1+\sqrt{5})/2$ 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 $\beta = (1 + \sqrt{3})/2$ (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 $(1 \pm \sqrt{3})/2$, 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 $\beta = (1 + \sqrt{3})/2$ 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 $\alpha = (1 + \sqrt{5})/2$ 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

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

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 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 $N = \max_{1 \leq i \leq n}\{\deg f_i(x)\}$. 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 $\{\alpha_i\beta_j : 1 \leq i \leq n, 1 \leq j \leq m\}$. 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 $R = \mathbb{Z}[x_1, x_2, \dots]$. Then R is a finitely generated R-module since $R = R1$. However, consider the ideal $I = \langle x_1, x_2, \dots \rangle$, 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 $(r_1, \dots, r_n) \mapsto r_1\alpha_1 + \cdots + r_n\alpha_n$. 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

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

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

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

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 $r_1, \dots, r_q \in R$. 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 $m_1, \ldots, m_n \in B$, the dependence relation $r_1m_1 + \cdots + r_nm_n = 0$ implies that $r_1 = \cdots = r_n = 0$.

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

$$x = r_1b_1 + \cdots + r_nb_n.$$

(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 $x = r_1b_1 + \cdots + r_nb_n$ 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 $(r_1, \ldots, r_n) \leftrightarrow r_1b_1 + \cdots + r_nb_n$, where $B = \{b_1, \ldots, b_n\}$ is a basis. We give some examples below.

(1) Let $R = \mathbb{Z}$ and $M = \mathbb{Z}[x]$. Then M has basis $B = \{1, x, x^2, \ldots\}$, 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 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

$$\operatorname{Tr}_{K/\mathbb{Q}}(\alpha) = \operatorname{Tr}(T_\alpha).$$

(2) The **norm** of α relative to $K/\mathbb{Q}$ is

$$N_{K/\mathbb{Q}}(\alpha) = \det(T_\alpha).$$

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

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. 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 $A = [T_\alpha]_\beta \in \mathbb{Q}^{d \times d}$, 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

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

We leave it as an exercise to verify that

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

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

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

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 $\alpha = \alpha_1, \dots, \alpha_{n/m}$ 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 $i = 1, \dots, n/m$. Then by **A1-4**, each σ_i extends to exactly $m = [K : \mathbb{Q}(\alpha)]$ embeddings of K into $\mathbb{C}$. If $\rho_1, \dots, \rho_n$ are the embeddings of K into $\mathbb{C}$, then

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

since for each $i = 1, \dots, n/m$, 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 $\sigma_1, \dots, \sigma_n$ be the embeddings of K in $\mathbb{C}$.

(1) Looking at trace, we have

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

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 lengthy 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 one other conjugate, namely $a - b\sqrt{d}$, 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 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 $\varphi(x) = (0, \ldots, 0)$, 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 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 $\{x_1, \ldots, x_n\} \subseteq \mathcal{O}_K$ 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 $\mathcal{O}_K$.

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 $K = \mathbb{Q}(\sqrt{5})$. $\{1, \sqrt{5}\} \subseteq \mathbb{Q}(\sqrt{5})$ is a $\mathbb{Q}$-basis of algebraic integers, but is not an integral basis for $\mathcal{O}_K$ since $\frac{1+\sqrt{5}}{2} \in \mathcal{O}_K$.

Due to Theorem 1.16, we also get the following corollary.

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 non-zero 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 $\operatorname{rank}(I) \geq n$. Then by Proposition 1.12, we have $\operatorname{rank}(I) \leq n$ and thus $\operatorname{rank}(I) = n$. □

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 $M \cong \mathbb{Z}^n \times T$ where T is finite. (We call $\mathbb{Z}^n$ the free part and T the torsion part.)

We make use this fact to prove one more 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 non-zero ideal of R, then R/I is finite.

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 $\mathbb{Q}$ 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 $\psi : L \to \mathbb{C}$.