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

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

We say that $f(x)$ is **primitive** if $\mathrm{Content}(f(x)) = 1$. 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 $(r_1 + r_2)m = r_1 m + r_2 m$;

(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 $(r_1 r_2)m = r_1(r_2 m)$.

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

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

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

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

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

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

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

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

Definition 1.5

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

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

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

   If f is also bijective, then we call it an **isomorphism**.

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

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

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

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

Definition 1.6

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

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

Theorem 1.7

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

Proof of Theorem 1.7.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Theorem 1.8

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

Proof of Theorem 1.8.

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

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

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

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

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

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

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

Definition 1.9

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

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

Theorem 1.10

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