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 $\mathbb{Z}$-linear algebra (actually module theory, since $\mathbb{Z}$ is not a field).

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.