Monogenic Number Fields by Example

Hanson Smith

California State University San Marcos

Number Theory

Potentially the first mathematical advance in human history was the advent of counting. By creating a bijection between $\{1, 2, 3, 4, 5, \dots\}$ and a set of objects, we attach an abstract notion of quantity to collections of objects in the real world.

Very broadly speaking, number theory is the study of the set of natural numbers $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$. As such, it is one of the oldest mathematical disciplines.

For reasons that become apparent when one attempts to do algebra, it is often advantageous for number theorists to study the integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ and the rationals $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0, \frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc\right\}$.

Number Fields and Rings of Integers

Since it is much more pleasant to work in a ring (a nice place where we can add, subtract, and multiply), number theorists are interested in studying $\mathbb{Z}$ and equations involving $\mathbb{Z}$. Algebraic number theorists are often interested in algebraic structures that generalize and preserve some of the fundamental properties of $\mathbb{Z}$ and $\mathbb{Q}$. We make the following somewhat abstract definitions (don't worry we'll unpack these definitions with examples):

Let $f(x) \in \mathbb{Z}[x]$ be monic irreducible polynomial of degree n. Suppose α is a root of $f(x)$ (in $\mathbb{C}$ say) and consider $\mathbb{Q}(\alpha)$, the smallest field containing $\mathbb{Q}$ and α. We call $\mathbb{Q}(\alpha)$ a *number field*. You can think of a number field as a generalization of $\mathbb{Q}$. Number theorists love $\mathbb{Z}$, and $\mathbb{Z}$ lives in $\mathbb{Q}$, so what is the analogue of $\mathbb{Z}$ living in $\mathbb{Q}(\alpha)$? Define *the ring of integers of* $\mathbb{Q}(\alpha)$, denoted $\mathcal{O}_{\mathbb{Q}(\alpha)}$, to be the set of all solutions to monic polynomials in $\mathbb{Z}[x]$ that are in $\mathbb{Q}(\alpha)$.

Number Fields and Rings of Integers Example

Let $f(x) = x^2 - 2$. One root of this polynomial is $\sqrt{2}$. We can consider the smallest field containing $\mathbb{Q}$ and $\sqrt{2}$. We'll denote this field $\mathbb{Q}(\sqrt{2})$.

With a little work we can show that $\mathbb{Q}(\sqrt{2}) = \left\{r + s\sqrt{2} : r, s \in \mathbb{Q}\right\}$. Addition and multiplication in this number field work as you might expect:

$$\left(\frac{1}{3} + 7\sqrt{2}\right) + \left(\frac{2}{3} - \sqrt{2}\right) = 1 + 6\sqrt{2},$$

and

$$\left(3 + \sqrt{2}\right) \cdot \left(2 - \sqrt{2}\right) = 3 \cdot 2 + \sqrt{2} \cdot 2 - 3\sqrt{2} - 2 = 4 - \sqrt{2}.$$

Number Fields and Rings of Integers Example

The number field $\mathbb{Q}(\sqrt{2})$ is a generalization of $\mathbb{Q}$, so what is the analogue of $\mathbb{Z}$ living in $\mathbb{Q}(\sqrt{2})$? What is the ring of integers of $\mathbb{Q}(\sqrt{2})$?

Notice that we can think of $\mathbb{Q}$ as the set of all solutions (in $\mathbb{C}$ say) to linear polynomials with integer coefficients. Indeed, if $a \in \mathbb{Z} - \{0\}$, then $ax + b$ corresponds to the rational number $-\frac{b}{a}$. How do we describe the integers in terms of polynomials with integer coefficients?

The integers are all the elements of $\mathbb{Q}$ that are solutions to monic linear polynomials with integer coefficients. Indeed, $b \in \mathbb{Z}$ corresponds to the polynomial $x - b \in \mathbb{Z}[x]$.

Thus the ring of integers of $\mathbb{Q}(\sqrt{2})$ is the set of all elements of this field that satisfy a monic polynomial in $\mathbb{Z}[x]$. In other words,

$$\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \left\{ r + s\sqrt{2} : f(r + s\sqrt{2}) = 0 \text{ with } f(x) \in \mathbb{Z}[x] \text{ monic} \right\}.$$

Number Fields and Rings of Integers Example

It turns out that the ring of integers of $\mathbb{Q}(\sqrt{2})$ admits a slightly more down-to-earth description:

$$\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \left\{ r + s\sqrt{2} : f(r + s\sqrt{2}) = 0 \text{ with } f(x) \in \mathbb{Z}[x] \text{ monic} \right\}$$

is simply

$$\mathbb{Z}[\sqrt{2}] = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Z} \right\}.$$

To see this let's pick an element of $\mathbb{Z}[\sqrt{2}]$, say $2 - 13\sqrt{2}$. In order for this element to be in $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$, it must satisfy a monic polynomial with integer coefficients.

Our instincts tell us it might be good to also consider the conjugate $2 + 13\sqrt{2}$, so we compute

$$\left(x - (2 - 13\sqrt{2})\right)\left(x - (2 + 13\sqrt{2})\right) = x^2 - 4x - 334.$$

A Historical Interlude

The person responsible for the definition of the ring of integers of a number field is Richard Dedekind:

Figure 1: Richard Dedekind (1831-1916)

A Historical Interlude

Two of the main figures who developed Dedekind's ideas into the modern notion of a ring are David Hilbert and Emmy Noether:

(a) David Hilbert (1862-1943)

(b) Emmy Noether (1882-1935)

The Ring of Integers of a Quadratic Number Field

After our previous example, we might be tempted to guess that the ring of integers of a quadratic number field $\mathbb{Q}(\sqrt{d})$ is simply $\mathbb{Z}\left[\sqrt{d}\right]$. However, the situation is a bit more subtle.

Take $\mathbb{Q}(\sqrt{-3})$ and consider the element $\frac{1+\sqrt{-3}}{2}$. We use the idea of multiplying by the conjugate to compute

$$\left(x-\left(\frac{1+\sqrt{-3}}{2}\right)\right)\left(x-\left(\frac{1-\sqrt{-3}}{2}\right)\right)=x^2-x+1.$$

Thus $\frac{1+\sqrt{-3}}{2}$ is in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ the ring of integers of $\mathbb{Q}(\sqrt{-3})$.

Aside from linear polynomials, which only generate trivial extensions of $\mathbb{Q}$, quadratic polynomials are the most approachable polynomials. Thus, it makes sense for us to first attempt to understand the ring of integers of a number field generated by a quadratic.

The Ring of Integers of a Quadratic Number Field

First off, if we have a monic quadratic polynomial $f(x) = x^2 + c_1x + c_0$ in $\mathbb{Z}[x]$, then we notice the roots are $\frac{1}{2}\big(-c_1 \pm \sqrt{c_1^2 - 4c_0}\big)$. Since we can get from $\frac{1}{2}\big(-c_1 + \sqrt{c_1^2 - 4c_0}\big)$ to $\sqrt{c_1^2 - 4c_0}$ by addition and multiplication of rational numbers, the number fields $\mathbb{Q}\Big(\frac{1}{2}\big(-c_1 + \sqrt{c_1^2 - 4c_0}\big)\Big)$ and $\mathbb{Q}(\sqrt{c_1^2 - 4c_0})$ are equal. Thus we do not lose any generality by solely considering number fields of the form $\mathbb{Q}(\sqrt{d})$.

We'll also assume d is square free, since, for example, $\sqrt{20} = 2\sqrt{5}$.

The Ring of Integers of a Quadratic Number Field

We take an arbitrary element $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. We want to know what conditions on a and b ensure that $a + b\sqrt{d}$ is an algebraic integer, i.e., satisfies a monic integer polynomial of degree 2. Using the conjugate, we compute

$$\left(x - \left(a + b\sqrt{d}\right)\right)\left(x - \left(a - b\sqrt{d}\right)\right) = x^2 - 2ax + a^2 - b^2 d.$$

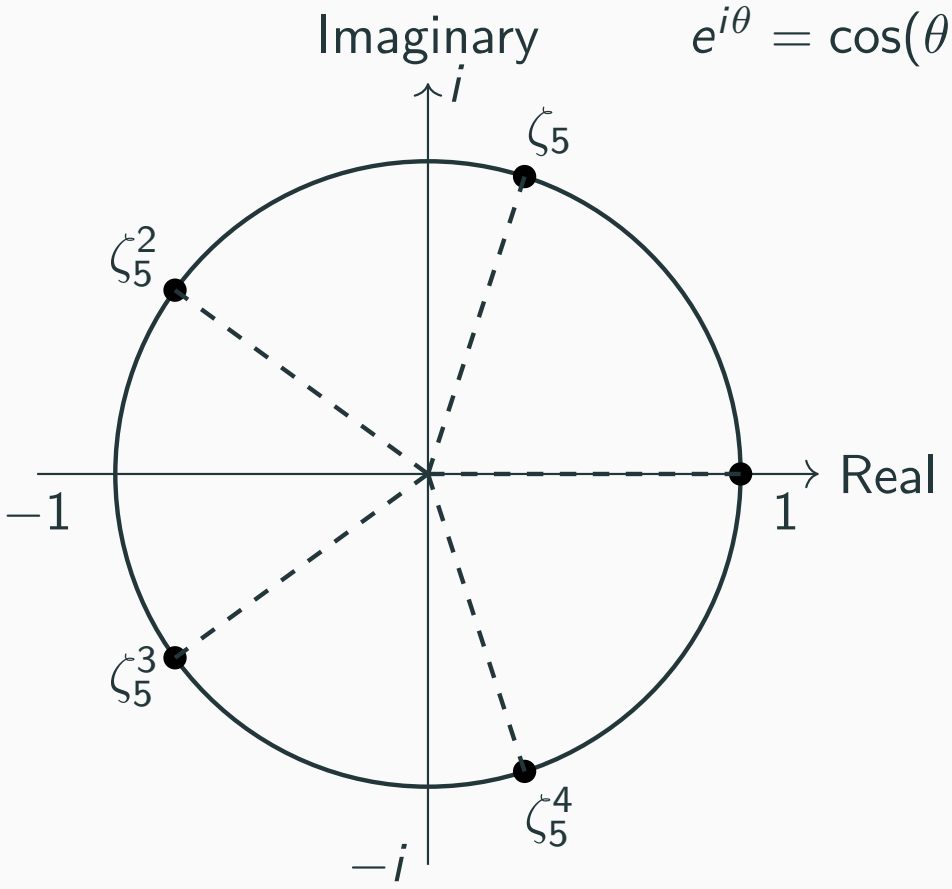
If this polynomial is in $\mathbb{Z}[x]$, then $2a \in \mathbb{Z}$. Hence $a \in \mathbb{Z}$ or a is half an odd integer. If $a \in \mathbb{Z}$, then necessarily $b \in \mathbb{Z}$. But, if $a = \frac{a_0}{2}$, then we could have $b = \frac{b_0}{2}$. If $a_0^2 - b_0^2 d \equiv 0 \bmod 4$, then we see that $a^2 - b^2 d \in \mathbb{Z}$. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \bmod 4$ and $\mathbb{Z}[\sqrt{d}]$ otherwise.

To summarize,

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\frac{1+\sqrt{d}}{2} : a, b \in \mathbb{Z}\right\} & \text{for } d \equiv 1 \bmod 4 \\ \mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\} & \text{otherwise.} \end{cases}$$

Cyclotomic Number Fields

Let ζ_n be a primitive n^{th} root of unity, a root of $x^n - 1$ but with $\zeta_n^k \neq 1$ for $1 \leq k < n$. The number field $\mathbb{Q}(\zeta_n)$ is called the n^{th} *cyclotomic field*. The word cyclotomic comes from "circle dividing". To see this, let's consider the 5^{th} roots of unity in the complex plane:



The Ring of Integers in a Cyclotomic Field

With a little work, we can show that the ring of integers of the n^{th} cyclotomic field $\mathbb{Q}(\zeta_n)$ is simply $\mathbb{Z}[\zeta_n]$.

For an explicit example, consider a fifth root of unity $e^{2\pi i/5} = \zeta_5$. We have seen that this satisfies the polynomial $x^5 - 1 = 0$. However, the *minimal polynomial* of ζ_5 is actually $x^5 - 1/x - 1 = x^4 + x^3 + x^2 + x + 1$.

The fifth cyclotomic field $\mathbb{Q}(\zeta_5)$ has a $\mathbb{Q}$-basis given by powers of ζ_5:

$$\mathbb{Q}(\zeta_5) = \left\{ r_0 + r_1\zeta_5 + r_2\zeta_5^2 + r_3\zeta_5^3 : r_i \in \mathbb{Q} \right\},$$

and the ring of integers has a $\mathbb{Z}$-basis that is also given by powers of ζ_5:

$$\mathbb{Z}[\zeta_5] = \left\{ a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3 : a_i \in \mathbb{Z} \right\}.$$

In particular, every element of $\mathbb{Q}(\zeta_5)$ that satisfies a monic polynomial with integer coefficients can be written as $a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3$ with the a_i in $\mathbb{Z}$.

Another Historical Interlude

Perhaps the first person to focus on cyclotomic fields and their rings of integers was Ernst Kummer. Kummer's work lead Dedekind towards general the definition of a ring.

Figure 3: Ernst Kummer (1810-1893)

Fermat's Last Theorem

The motivation for Kummer was a brilliant attack on Fermat's last theorem.

Fermat's last theorem states that the equation $x^n + y^n = z^n$ has no non-trivial integer solutions for $n > 2$. It suffices to prove this for $n = 4$ and $n = p$, an odd prime. Pierre de Fermat himself did the $n = 4$ case.

Suppose there was a solution $x^p + y^p = z^p$. Kummer (actually it was Gabriel Lamé first) realized that in $\mathbb{Z}[\zeta_p]$ one could use polynomial factorization $x^p - 1 = \prod_{i=1}^{p}(x - \zeta_p^i)$ to obtain the factorization

$$x^p + y^p = \prod_{i=1}^{p} \left(x + \zeta_p^i y\right) = z^p.$$

Using the fact that $\mathbb{Z}[\zeta_p]$ shares many properties with $\mathbb{Z}$, Kummer could derive a contradiction in many cases.

Monogenicity

Returning to our saunter through rings of integers. We start to notice that all the rings of integers we have met have a particularly nice form. They all look like $\mathbb{Z}[\beta]$ for some β.

With this in mind, we make the following definition: Let $\mathbb{Q}(\alpha)$ be a number field. If the ring of integers of $\mathbb{Q}(\alpha)$ has the form $\mathbb{Z}[\beta]$ for some $\beta \in \mathbb{Q}(\alpha)$, then we say $\mathbb{Q}(\alpha)$ is *monogenic*. (The ring of integers has "one generator.") In this case, we call β a *monogenerator*. We also say that $\mathcal{O}_{\mathbb{Q}(\alpha)}$ admits a *power integral basis*. Explicitly,

$$\mathcal{O}_{\mathbb{Q}(\alpha)} = \left\{ a_0 + a_1\beta + a_2\beta^2 + \cdots a_{n-1}\beta^{n-1} : a_i \in \mathbb{Z} \right\}.$$

If $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial of β, then we say $f(x)$ is a *monogenic polynomial*.

A natural first hope after the examples we've seen is that every number field is monogenic!

“All that glistens is not gold.”

Does this always happen? When one is learning (or discovering) algebraic number theory, they might be tempted to think every extension of $\mathbb{Q}$ is monogenic. It works for the first two families of number fields we encounter, so maybe we expect it always happens.

Expectation is the root of all heartache.

- William Shakespeare

A Couple of Ideas Before the Example

If $K = \mathbb{Q}(\alpha)$ is a number field with ring of integers $\mathcal{O}_K$, then I can take any $\beta \in \mathcal{O}_K$ and consider $\mathbb{Z}[\beta]$. When $\mathbb{Z}[\beta]$ is big enough, we call it an *order*. The *index* $\left[\mathcal{O}_K : \mathbb{Z}[\beta]\right]$ measure how far away $\mathbb{Z}[\beta]$ is from being the full ring of integers. For example, $\mathbb{Z}[3\sqrt{2}]$ is not the full ring of integers of $\mathbb{Q}(\sqrt{2})$. The index $\left[\mathbb{Z}[\sqrt{2}] : \mathbb{Z}[3\sqrt{2}]\right]$ is 3.

We mentioned that number rings, the rings of integers of number fields, share many properties with the integers. One of the most important properties is unique factorization. Not all number rings have unique factorization into prime numbers, but all number rings have unique factorization into *prime ideal numbers* (a.k.a. *prime ideals*). For example, 7 is no longer a prime number in $\mathbb{Z}[\sqrt{2}]$. However, $7 = (3 + \sqrt{2})(3 - \sqrt{2})$, and these two elements of $\mathbb{Z}[\sqrt{2}]$ are primes!

Dedekind-Kummer Factorization

Theorem (Dedekind building on work of Kummer)

Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ with α denoting a root. If $p \in \mathbb{Z}$ is a prime that does not divide $\left[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]\right]$, then the factorization of p in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ mirrors the factorization of $f(x)$ in $\mathbb{F}_p[x]$. That is,

$$f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \bmod p \quad \textit{and} \quad p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

For example, consider $\mathbb{Q}(\alpha)$ where α is a root of $f(x) = x^3 - x^2 - 2x - 8$. Take my word that 59 does not divide $\left[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]\right]$. You can check that

$$f(x) \equiv (x + 30)(x + 39)(x + 48) \bmod 59.$$

Thus 59 factors into three primes $\mathfrak{l}_1\mathfrak{l}_2\mathfrak{l}_3$ in the ring of integers of $\mathbb{Q}(\alpha)$.

Dedekind-Kummer Factorization

Theorem (Dedekind building on work of Kummer)

Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ with α denoting a root. If $p \in \mathbb{Z}$ is a prime that does not divide $\left[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]\right]$, then the factorization of p in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ mirrors the factorization of $f(x)$ in $\mathbb{F}_p[x]$:

$$f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \bmod p \quad \textit{and} \quad p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Again, consider $\mathbb{Q}(\alpha)$ where α is a root of $f(x) = x^3 - x^2 - 2x - 8$. Dedekind computed the factorization $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Working the other direction, if this field is monogenic, there is a cubic polynomial $g(x)$ and root β such that 2 does not divide $\left[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\beta]\right]$. We see that $g(x) \equiv (x-a)(x-b)(x-c) \bmod 2$, where a, b, and c are distinct elements of $\mathbb{Z}/2\mathbb{Z}$...

Since $\mathbb{Z}/2\mathbb{Z}$ only has two distinct elements, Dedekind has constructed a non-monogenic field!

Common Index Divisors

One can generalize Dedekind's example: If a prime $p < n$ splits completely in an extension $K/\mathbb{Q}$ of degree n, then K is not monogenic. [**?**] builds on these ideas to show the following.

Theorem

Fix a prime p. The prime p divides $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ for every algebraic integer θ generating K over $\mathbb{Q}$ if and only if there is an integer f such that the number of prime ideal factors of $p\mathcal{O}_K$ with inertia degree f is greater than the number of monic irreducibles of degree f in $\mathbb{F}_p[x]$.

Any p satisfying this theorem is called a *common index divisor*. The terms 'essential discriminant divisor' and 'inessential discriminant divisor' also appear in the literature.

Other Obstructions

It turns out that common index divisors are not the only obstruction to monogeneity:

Example: [**?**, Chapter 2.2.6] Consider the number field given by $K = \mathbb{Q}\left(\sqrt[3]{7 \cdot 5^2}\right) = \mathbb{Q}\left(\sqrt[3]{5 \cdot 7^2}\right)$. The elements $\left\{1, \sqrt[3]{7 \cdot 5^2}, \sqrt[3]{7^2 \cdot 5}\right\}$ form an integral basis for $\mathcal{O}_K$. For any fixed prime p, one can find $\alpha \in \mathcal{O}_K$ such that $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is not divisible by p; however, K is not monogenic.

In fact, the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ can be described with a form, called the *index form*. In the example above it is $5X_1^3 - 7X_2^3$. We can consider it modulo 7 to see that there are no values for which the form is ± 1.

The Lay of the Land

Gras [**?**] has shown that, with the exception of the maximal real subfields of cyclotomic fields, abelian extensions of $\mathbb{Q}$ of prime degree greater than or equal to 5 are not monogenic. Generally, Gras [**?**] has shown that almost all abelian extensions of $\mathbb{Q}$ with degree coprime to 6 are not monogenic. Bhargava, Shankar, and Wang [**?**] have shown that the density of monic, irreducible polynomials $f(x) \in \mathbb{Z}[x]$ such that a root θ of $f(x)$ yields a power basis for the ring of integers of $\mathbb{Q}(\theta)$ is $\frac{6}{\pi^2} = \zeta(2)^{-1} \approx 60.79\%$. In the same paper, they also show that the density of monic integer polynomials with square-free discriminants is

$$\prod_p \left(1 - \frac{1}{p} + \frac{(p-1)^2}{p^2(p+1)}\right) \approx 35.82\%.$$

Note that these polynomials are a subset of the monic, irreducible polynomials $f(x) \in \mathbb{Z}[x]$ such that a root θ yields a power basis for the ring of integers of $\mathbb{Q}(\theta)$.

Which and How Many Number Fields are Monogenic?

Rough Folklore Conjecture: Counted appropriately, number fields of degree greater than two are very seldom monogenic.

Thank You!

Figure 4: QR Code for My Website

References i