Chapter 1

Number Fields

A natural way to begin a book about Algebraic Number Theory is by introducing number fields. We will start with a short introduction. Then we'll have a quick refresher on algebraic numbers and minimal polynomials, and finally, we'll define number fields and generalize them.

1 Introduction

Formally, algebraic number fields are finite degree field extensions[1] of the rational numbers. For much of this book we'll work in a more general context of arbitrary (but usually finite) field extensions. However, to get some intuition, we can think of number fields as rational numbers extended by "external" elements.

Example 1.1.1: A typical number field is $\mathbb{Q}(\sqrt{2}) = \left\{m + n\sqrt{2} \mid m, n \in \mathbb{Q}\right\}$. It even has a name - it's called a quadratic field.

It's clearly a field: it's closed under addition and multiplication, and inherits other field properties from $\mathbb{Q}$. It's larger than $\mathbb{Q}$ but much smaller than $\mathbb{R}$.

As we'll see in the next chapter, just as number fields generalize the rational numbers, we can use them to study integers in a more general context - which we'll do in the next chapter. To talk about number fields, it's important to understand the concept of algebraic numbers first[2].

2 Algebraic Numbers

Definition 1.2.1: Algebraic numbers are complex numbers that are roots of a polynomial with coefficients in $\mathbb{Q}$. The set of algebraic numbers is denoted $\overline{\mathbb{Q}}$.

[1] TODO: Explain this in a book about Field and Galois theory

[2] This part will be moved to a book about Field and Galois theory someday

Example 1.2.2:

- 1 is a root of $1 - x$ and $3x - 3$.
- $\frac{1}{2}$ is a root of $2x - 1$ and $x - \frac{1}{2}$.
- $\sqrt{2}$ is a root of $x^2 - 2$ and $x^5 + 2x^4 - 2x^3 - 4x^2$.
- i is a root of $x^2 + 1$.
- π is not a root of any polynomial with rational coefficients.

Definition 1.2.3: A number is algebraic if any such polynomial exist. Since we're working in $\mathbb{Q}$ we can scale the polynomial to be monic (i.e. with 1 as a leading coefficient). The monic polynomial with a smallest degree is called a **minimal polynomial** over $\mathbb{Q}$.

Definition 1.2.4: The **degree** of algebraic number α is denoted $\deg \alpha$ and defined as the degree of its minimal polynomial.

Example 1.2.5: Examples of minimal polynomials:

- The minimal polynomial of 1 is $x - 1$. So $\deg 1 = 1$.
- The minimal polynomial of $\frac{1}{2}$ is $x - \frac{1}{2}$. So $\deg \frac{1}{2} = 1$.
- The minimal polynomial of $\sqrt{2}$ is $x^2 - 2$. So $\deg \sqrt{2} = 2$.
- The minimal polynomial of i is $x^2 + 1$. So $\deg i = 2$.
- The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$. So $\deg \sqrt[3]{2} = 3$.

Definition 1.2.6: If the coefficients of the minimal polynomial are all integers, we call the corresponding algebraic number an **algebraic integer**. Thus 1, i and $\sqrt{2}$ are algebraic integers, while $\frac{1}{2}$ is not. The set of algebraic integers is denoted $\overline{\mathbb{Z}}$.

Definition 1.2.7: Given an algebraic number α with minimal polynomial P of degree n, the n roots of P are called the **Galois conjugates** of α.

Example 1.2.8: Examples of Galois conjugates:

- Galois conjugates of 1 over $\mathbb{Q}$ are $\{1\}$
- Galois conjugates of $\sqrt{2}$ over $\mathbb{Q}$ are $\left\{\sqrt{2}, -\sqrt{2}\right\}$
- Galois conjugates of $\sqrt[3]{2}$ over $\mathbb{Q}$ are $\left\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right\}$ (where ω is a primitive cube root of unity). Note that these conjugates don't lie in $\mathbb{Q}(\sqrt[3]{(2)})$.

There is one more interesting aspect about minimal polynomials and conjugates: conjugates always come together.

Theorem 1.2.9. *Let α be an algebraic number with a minimal polynomial $A(x)$, and let $B(x)$ be another polynomial such that $B(\alpha) = 0$. Then $A(x)$ divides $B(x)$.*

Proof. By the division algorithm for polynomials, we can express $B(x) = A(x)Q(x) + R(x)$, with $\deg R(x) < \deg A(x)$. By substituting α we get $0 = R(\alpha)$. If $R(x)$ is not a zero polynomial, we get a contradiction - α is a root of $R(x)$, which has a degree lower than the degree of the minimal polynomial of α. Hence, $R(x)$ must be a zero polynomial, and thus $B(x) = A(x)Q(x)$ as desired (proving that $A(x)$ divides $B(x)$). □

This has some nice consequences - for example, if we know $a_1, a_2, \ldots a_n$ are conjugates over $\mathbb{Q}$, and that $P(a_1) = 0$, we immediately infer, without further checking, that $P(a_2) = \ldots = P(a_n) = 0$. To reuse a previous example, since $\sqrt{2}$ and $-\sqrt{2}$ are conjugates, if we know that $\sqrt{2}$ is a root of $P(x) = x^5 + 2x^4 - 2x^3 - 4x^2$, we immediately conclude that $-\sqrt{2}$ is also a root.

3 Algebraic properties

Algebraic numbers are just one example of a more generic phenomena. To talk about their properties more generally, we first need to first define a few terms:

Definition 1.3.1: Let A be a field, and L be an extension field of A. An element $x \in L$ is **algebraic** over A if it is the zero of a non-zero polynomial with coefficient in A.

Example 1.3.2: Algebraic numbers are, by definition, algebraic over $\mathbb{Q}$. Algebraic integers are also algebraic over $\mathbb{Q}$ (they are also roots of polynomials with coefficients in $\mathbb{Z}$, but we don't say they're algebraic over $\mathbb{Z}$, because $\mathbb{Z}$ is not a field).

Definition 1.3.3: The **algebraic closure** of A in L is the set of elements of L algebraic over A. If every element of L is algebraic over A we say L is an **algebraic extension** of A.

The algebraic closure of A is often denoted $\overline{A}$. This is why the algebraic closure of $\mathbb{Q}$ - the set of algebraic numbers - is denoted $\overline{\mathbb{Q}}$. For more examples, the algebraic closure of $\mathbb{R}$ is $\mathbb{C}$. The algebraic closure of $\mathbb{C}$ is $\mathbb{C}$.
One last definition worth knowing, even though we won't use often, is:

Definition 1.3.4: A field F is **algebraically closed** if every nonconstant polynomial in $F[x]$ has a root in F.

Clearly, $\mathbb{C}$ is algebraically closed. Another examples of algebraically closed fields include $\overline{\mathbb{Q}}$ and finite fields.

All of the definitions from the previous section carry over - for example we define minimal polynomials and degrees for arbitrary field extension in the same way.

4 Number fields

Having defined algebraic numbers, we can now introduce the concept of number fields. A number field is a field that contains $\mathbb{Q}$ as a subfield, and is generated by adjoining a finite number of algebraic numbers to $\mathbb{Q}$. More formally:

Definition 1.4.1: A **number field** is a finite field extension K of the field of rational numbers $\mathbb{Q}$.

In particular, every finite extension is alebraic.

Remark 1.4.2: $\mathbb{R}$ and $\mathbb{C}$ are not number fields, because they can't be generated by adjoining a *finite* number of elements to $\mathbb{Q}$. In other words, they are not finite extensions of $\mathbb{Q}$.

Example 1.4.3: For example, $\mathbb{Q}(\sqrt{2}) = \left\{\frac{a+b\sqrt{2}}{c+d\sqrt{2}} : a, b, c, d \in \mathbb{Q}\right\}$ is a number field.

Rationalizing the denominator shows that that this is equivalent to $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$. In other words, $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[\sqrt{2}]$. This holds for every algebraic number α (as we prove more generally in Proposition 2.1.7). Therefore, we usually think of elements of $\mathbb{Q}(\alpha)$ as numbers of form $a + b\alpha$ with $a, b \in \mathbb{Q}$.

Definition 1.4.4: The **degree** of a number field K over $\mathbb{Q}$, denoted $[K : \mathbb{Q}]$ is the dimension of K as a vector space over $\mathbb{Q}$.

Example 1.4.5: Number fields as vector spaces:

- The degree of $\mathbb{Q}(\sqrt{2})$ is equal to 2, with basis being $\left\{1, \sqrt{2}\right\}$.
- The degree of $\mathbb{Q}(\sqrt[3]{2})$ is equal to 3, with basis being $\left\{1, \sqrt[3]{2}, \sqrt[3]{4}\right\}$.
- And in general - the degree of $\mathbb{Q}(\alpha)$ is equal to $\deg \alpha$ (Exercise 4).

In the following chapters, we will usually prove results in a more general setting of arbitrary field extensions L/K instead of focusing on number fields which are a special case $(L/\mathbb{Q})$. Nevertheless, we'll sometimes refer to number fields in our examples.

5 Problems

1. Verify that $\mathbb{Q}(\alpha)$ forms a $\mathbb{Q}$-vector space.
2. Find a minimal polynomial of $\sqrt{2} + \sqrt{3}$.
3. Show that $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$ as fields.
4. Show that the degree of $\mathbb{Q}(\alpha)$ is equal to $\deg \alpha$.