MATH5645: Algebraic Number Theory

Gerald Huang

Contents

Field extensions

Much of our algebraic number theory studies come from the study of algebraic number fields (a concept discussed in Chapter 1). However, before discussing such a concept, we revisit another concept usually taught at an undergraduate abstract algebra course (MATH3711 or MATH3521) – fields and their extensions.

To build up the concept of an *extension*, we shall look at a few examples (and non-examples) of fields. In short, a field is some algebraic structure that allows us to add, subtract, multiply and divide elements.

Example 0.0.1. The set of real numbers $\mathbb{R}$ with its standard addition and multiplication operations form a field.

Example 0.0.2. The set of natural numbers $\mathbb{N}$ with its standard addition and multiplication operations do NOT form a field. We have no notion of "subtraction" in this group. So it seems like we at least need the negative numbers.

Example 0.0.3. The set of integers $\mathbb{Z}$ with its standard addition and multiplication operations do NOT form a field. We have no notion of "division" in this ring. So even the negative and positive integers are not enough for a field. However, if we include fractions, then we do indeed get a field.

Example 0.0.4. The set of rational numbers $\mathbb{Q}$ with its standard addition and multiplication operations form a field.

0.1 Subfields

Before we begin discussions of an extension, we also briefly discuss the notion of a *subfield*. Much like groups, there may be fields that contain other fields. For example, the field $\mathbb{Q}$ is contained in $\mathbb{R}$ which is contained in $\mathbb{C}$ (with respect to the same standard addition and multiplication operations). We formalise this concept in the following definition.

Definition 0.1.1. Let E and F be fields with respect to the same addition and multiplication operations, and suppose that $E \subset F$. Then we say that F is an *extension* or *extension field* of E or equivalently F/E is a *field extension*.

So in the previous example, $\mathbb{R}$ is an extension field of $\mathbb{Q}$ and $\mathbb{C}$ is an extension field of $\mathbb{R}$. The reason why we call this an *extension* is because we primarily start with a field and add some new elements to create a bigger field. This bigger field *extends* the smaller field.

This is especially useful when we talk about polynomial reducibility. Of course, irreducibility depends on what field we talk about. For example, $p(x) = x^2 + 1$ is irreducible over $\mathbb{R}$. However, it can be factored into $p(x) = (x + i)(x - i)$ over $\mathbb{C}$.

So one natural question is: what elements would we want to add into our field $\mathbb{Q}$ for certain polynomials to be reducible?

0.2 Irreducibility over fields

Consider the field of rational numbers, $\mathbb{Q}$. This does not have any irrational numbers and so polynomials such as $p(x) = x^2 - 2 \in \mathbb{Q}[x]$ has no solutions. However, if we were to "add" in the element $\sqrt{2}$, then p can be reduced. The problem is, $\sqrt{2}$ is not the only element we'd have to add to maintain that field structure. We'd have to add in any linear combination of rational numbers with $\sqrt{2}$. This allows us to "add" and "subtract" elements without any issue. What about multiplication and division?

To reason why this is no longer an issue, we look at a few examples. For notation purposes, I will call this new "field" $\mathbb{Q}_{\sqrt{2}}$; we will define it using proper notation later. If $1 + \sqrt{2} \in \mathbb{Q}_{\sqrt{2}}$, then so must its inverse which is $(1 + \sqrt{2})^{-1}$. However, we see that

$$\begin{aligned}(1+\sqrt{2})^{-1} &= \frac{1}{1+\sqrt{2}} \\ &= \frac{1-\sqrt{2}}{(1+\sqrt{2})(1-\sqrt{2})} \\ &= \frac{1-\sqrt{2}}{1-2} \\ &= \sqrt{2}-1 \in \mathbb{Q}_{\sqrt{2}}.\end{aligned}$$

So it looks like we're okay in this regard. Let's demonstrate that it's okay more generally. Let $a, b \in \mathbb{Q}$. Then the inverse of $(a + b\sqrt{2})$ is $(a + b\sqrt{2})^{-1}$ but we see that

$$\begin{aligned}(a+b\sqrt{2})^{-1} &= \frac{1}{a+b\sqrt{2}} \\ &= \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} \\ &= \frac{a-b\sqrt{2}}{a^2-2b^2} \\ &= \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}_{\sqrt{2}}.\end{aligned}$$

So it appears that $\mathbb{Q}_{\sqrt{2}}$ forms a field. We'll formalise the notation a bit now.

Let $a, b \in \mathbb{Q}$. We define the following field by "adjoining" the element $\sqrt{2}$,

$$\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}.$$

Observe that, if m is *square-free* (m has no perfect square divisors), then we have

$$\mathbb{Q}(\sqrt{m}) = \left\{a + b\sqrt{m} : a, b \in \mathbb{Q}\right\}.$$

If m was not square-free, then write $m = a^2 \cdot b$. Then $\mathbb{Q}(\sqrt{m}) \cong \mathbb{Q}(\sqrt{b})$ since we can write

$$x \in \mathbb{Q}(\sqrt{m}) \implies x = y + z\sqrt{m} = y + z\sqrt{a^2 \cdot b} = y + az\sqrt{b} \in \mathbb{Q}(\sqrt{b}).$$

Chapter 1

Algebraic Numbers and Algebraic Integers

Algebraic number theory is primarily concerned with the study of algebraic number fields. This chapter focuses on building some language to then describe these algebraic structures. To motivate this idea, we begin with a discussion on extension fields.

Suppose that we have two fields, E and F, and suppose that $F \subseteq E$ is a subfield of E. Then we say that E is an *extension* of F or equivalently, E/F is an *extension field*. For example,

1.1 Algebraic number fields and the ring of integers

1.2 Norms and traces

1.3 Embeddings in $\mathbb{C}$

1.4 Discriminants

Chapter 2

Ideals and prime decomposition in rings of integers

2.1 Factorisation of ideals

2.2 Chinese Remainder Theorem

2.3 Splitting of primes