Lecture 6.1: Fields and their extensions

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Overview and some history

The quadradic formula is well-known. It gives us the two roots of a degree-2 polynomial $ax^2 + bx + c = 0$:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

There are formulas for cubic and quartic polynomials, but they are *very* complicated. For years, people wondered if there was a quintic formula. Nobody could find one.

In the 1830s, 19-year-old political activist Évariste Galois, with no formal mathematical training proved that no such formula existed.

He invented the concept of a group to solve this problem.

After being challenged to a dual at age 20 that he knew he would lose, Galois spent the last few days of his life frantically writing down what he had discovered.

In a final letter Galois wrote, "*Later there will be, I hope, some people who will find it to their advantage to decipher all this mess.*"

Hermann Weyl (1885–1955) described Galois' final letter as: "*if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind.*" Thus was born the field of group theory!

Arithmetic

Most people's first exposure to mathematics comes in the form of counting.

At first, we only know about the natural numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$, and how to add them.

Soon after, we learn how to subtract, and we learn about negative numbers as well. At this point, we have the integers, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

Then, we learn how to divide numbers, and are introducted to fractions. This brings us to the rational numbers, $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\}$.

Though there are other numbers out there (irrational, complex, etc.), we don't need these to do basic arithmetic.

Key point

To do arithmetic, we need *at least* the rational numbers.

Fields

Definition

A set F with addition and multiplication operations is a field if the following three conditions hold:

- F is an abelian group under addition.
- $F \setminus \{0\}$ is an abelian group under multiplication.
- The distributive law holds: $a(b+c) = ab + ac$.

Examples

- The following sets are fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (prime p).
- The following sets are *not* fields: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_n$ (composite n).

Definition

If F and E are fields with $F \subset E$, we say that E is an extension of F.

For example, $\mathbb{C}$ is an extension of $\mathbb{R}$, which is an extension of $\mathbb{Q}$.

In this chapter, we will explore some more unusual fields and study their automorphisms.

An extension field of $\mathbb{Q}$

Question

What is the smallest extension field F of $\mathbb{Q}$ that contains $\sqrt{2}$?

This field must contain all sums, differences, and quotients of numbers we can get from $\sqrt{2}$. For example, it must include:

$$-\sqrt{2}, \qquad \frac{1}{\sqrt{2}}, \qquad 6+\sqrt{2}, \qquad \left(\sqrt{2}+\frac{3}{2}\right)^3, \qquad \frac{\sqrt{2}}{16+\sqrt{2}}.$$

However, these can be simplified. For example, observe that

$$\left(\sqrt{2}+\frac{3}{2}\right)^3 = (\sqrt{2})^3 + \frac{9}{2}(\sqrt{2})^2 + \frac{27}{4}\sqrt{2} + \frac{27}{8} = \frac{99}{8} + \frac{35}{4}\sqrt{2}.$$

In fact, *all* of these numbers can be written as $a+b\sqrt{2}$, for some $a, b \in \mathbb{Q}$.

Key point

The smallest extension of $\mathbb{Q}$ that contains $\sqrt{2}$ is called "$\mathbb{Q}$ adjoin $\sqrt{2}$," and denoted:

$$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\} = \left\{\frac{p}{q} + \frac{r}{s}\sqrt{2} : p, q, r, s \in \mathbb{Z},\ q, s \neq 0\right\}.$$

$\mathbb{Q}(i)$: Another extension field of $\mathbb{Q}$

Question

What is the smallest extension field F of $\mathbb{Q}$ that contains $i = \sqrt{-1}$?

This field must contain

$$-i, \qquad \tfrac{2}{i}, \qquad 6+i, \qquad \left(i+\tfrac{3}{2}\right)^3, \qquad \tfrac{i}{16+i}\,.$$

As before, we can write all of these as $a+bi$, where $a,b\in\mathbb{Q}$. Thus, the field "$\mathbb{Q}$ adjoin i" is

$$\mathbb{Q}(i)=\{a+bi : a,b\in\mathbb{Q}\}=\left\{\frac{p}{q}+\frac{r}{s}\,i : p,q,r,s\in\mathbb{Z},\ q,s\neq 0\right\}.$$

Remarks

- $\mathbb{Q}(i)$ is much smaller than $\mathbb{C}$. For example, it does *not* contain $\sqrt{2}$.
- $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$, but $\mathbb{Q}(i)$ is not.
- $\mathbb{Q}(\sqrt{2})$ contains all of the roots of $f(x)=x^2-2$. It is called the splitting field of $f(x)$. Similarly, $\mathbb{Q}(i)$ is the splitting field of $g(x)=x^2+1$.

$\mathbb{Q}(\sqrt{2}, i)$: Another extension field of $\mathbb{Q}$

Question

What is the smallest extension field F of $\mathbb{Q}$ that contains $\sqrt{2}$ and $i = \sqrt{-1}$?

We can do this in two steps:

(i) Adjoin the roots of the polynomial $x^2 - 2$ to $\mathbb{Q}$, yielding $\mathbb{Q}(\sqrt{2})$;

(ii) Adjoin the roots of the polynomial $x^2 + 1$ to $\mathbb{Q}(\sqrt{2})$, yielding $\mathbb{Q}(\sqrt{2})(i)$;

An element in $\mathbb{Q}(\sqrt{2}, i) := \mathbb{Q}(\sqrt{2})(i)$ has the form

$$\begin{aligned} & \alpha + \beta i && \alpha, \beta \in \mathbb{Q}(\sqrt{2}) \\ &= (a + b\sqrt{2}) + (c + d\sqrt{2})i && a, b, c, d \in \mathbb{Q} \\ &= a + b\sqrt{2} + ci + d\sqrt{2}i && a, b, c, d \in \mathbb{Q} \end{aligned}$$

We say that $\{1, \sqrt{2}, i, \sqrt{2}i\}$ is a basis for the extension $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$. Thus,

$$\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i : a, b, c, d \in \mathbb{Q}\}$$

In summary, $\mathbb{Q}(\sqrt{2}, i)$ is constructed by starting with $\mathbb{Q}$, and adjoining all roots of $h(x) = (x^2 - 2)(x^2 + 1) = x^4 - x^2 - 2$. It is the splitting field of $h(x)$.

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$: Another extension field of $\mathbb{Q}$

Question

What is the smallest extension field F of $\mathbb{Q}$ that contains $\sqrt{2}$ and $\sqrt{3}$?

This time, our field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, constructed by starting with $\mathbb{Q}$, and adjoining all roots of the polynomial $h(x) = (x^2 - 2)(x^2 - 3) = x^4 - 5x^2 + 6$.

It is not difficult to show that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for this field, i.e.,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\right\}.$$

Like with did with a group and its subgroups, we can arrange the subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ in a lattice.

I've labeled each extension with the degree of the polynomial whose roots I need to adjoin.

Just for fun: What *group* has a subgroup lattice that looks like this?

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash, "2"'] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$