MA542 Lecture

Timothy Kohl

Boston University

March 5, 2025

Extension Fields

Definition

A field E is an extension field of a field F if $F \subseteq E$ and the operations in E restricted to F are the same as the operations in F. (i.e. F is subring of E that is also a field).

For example

- $\mathbb{Q}(\sqrt{2})$ is an extension field of $\mathbb{Q}$
- $\mathbb{R}$ is an extension field of $\mathbb{Q}$
- $\mathbb{C}$ is an extension field of $\mathbb{R}$ (and therefore of $\mathbb{Q}$ too)

The construction $\mathbb{Q}[x]/\langle x^2-2\rangle \cong \mathbb{Q}(\sqrt{2})$ motivates the following fundamental result.

Theorem (The Fundamental Theorem of Field Theory)

(Kronecker - 1887)
Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. Then there is an extension field E of F which contains a root of $f(x)$.

PROOF: Given $f(x)$ let $p(x)$ be an irreducible factor of $f(x)$, which exists because $F[x]$ is a UFD.
Let $E = F[x]/\langle p(x)\rangle$ which is a field because $p(x)$ is irreducible, and therefore $\langle p(x)\rangle$ is maximal.
We may view E as an extension field of F as $a \mapsto a + \langle p(x)\rangle$ for each $a \in F$, i.e. $\phi : F \to F[x]/\langle p(x)\rangle$ given by $\phi(a) = a + \langle p(x)\rangle$ is injective (i.e. one-to-one).
So $\phi(F)$ is a subset of E which is isomorphic to F, so we may regard E as an extension field of $\phi(F)$.

An easy example we can give of this is $\mathbb{Q} \mapsto \mathbb{Q}/\langle x^2 - 2\rangle$ where $a \mapsto a + \langle x^2 - 2\rangle \subseteq \mathbb{Q}[x]/\langle x^2 - 2\rangle$, since

$$\{a + \langle x^2 - 2\rangle \mid a \in \mathbb{Q}\} \cong \mathbb{Q}$$

That E contains a root of $f(x)$ can be seen as follows, let $I = \langle p(x)\rangle$ where $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ then let $\alpha = x + I$ and consider $p(\alpha)$ which makes sense since p is a polynomial, so we can plug in the coset $\alpha = x + I$ itself.

Indeed, for any $m \geq 0$, $\alpha^m = (x+I)^m = x^m + I$ and so

$$\begin{aligned}
p(\alpha) &= a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \\
&= a_n(x^n + I) + a_{n-1}(x^{n-1} + I) + \cdots + a_1(x + I) + a_0(1 + I) \\
&= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) + I \\
&= p(x) + I \\
&= 0 + I
\end{aligned}$$

so $\alpha = x + I$ is a root of $p(x)$, where α is an element of $F[x]/\langle p(x)\rangle$, which contains $\phi(F) \cong F$.
For example in $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ we have that

$$(x + \langle x^2 - 2\rangle)^2 - (2 + \langle x^2 - 2\rangle) = (x^2 - 2) + \langle x^2 - 2\rangle = 0 + \langle x^2 - 2\rangle$$

i.e. $x + \langle x^2 - 2\rangle$ is like $\sqrt{2}$.

Examples:

- $\mathbb{Q}[x]/\langle x^2+1\rangle \cong \mathbb{Q}(i)$
- $\mathbb{Q}[x]/\langle x^2-2\rangle \cong \mathbb{Q}(\sqrt{2})$
- $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$
- $\mathbb{Z}_3[x]/\langle x^2+1\rangle$
  an extension field of $\mathbb{Z}_3$ containing a root of $x^2+1=x^2-2$

Before going further, let's take a step *back* and consider what is meant by 'adjoining' a root, such as $\sqrt{2}$, of an irreducible polynomial, like $x^2 - 2$, to a field like $\mathbb{Q}$, and why we write $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Basically, we ask, using the operations of $+$ and $\cdot$, what are all the numbers we can form from combining the elements of the set

$$\mathbb{Q} \cup \{\sqrt{2}\}$$

using these operations?

Specifically, we consider, for each polynomial $f(x) \in \mathbb{Q}[x]$, the numbers $f(\sqrt{2})$, and the question is, can we easily describe this set?

Moreover, is this set of numbers a field?

Well, starting with $\sqrt{2}$, we can multiply it by -1 to get $-\sqrt{2}$, and certainly, for rational numbers a, b we can form the combination $a + b\sqrt{2}$, and since $(\sqrt{2})^2 = 2 \in \mathbb{Q}$ then all higher powers of $\sqrt{2}$ are $\sqrt{2}^{2m} = 2^m$ and $\sqrt{2}^{2m+1} = 2^m\sqrt{2}$.

For example if $f(x) = x^5 + 2x^4 - \frac{3}{2}x^3 + 3x^2 + x + 1$ then

$$
\begin{aligned}
f(\sqrt{2}) &= (\sqrt{2})^5 + 2(\sqrt{2})^4 - \frac{3}{2}(\sqrt{2})^3 + 3(\sqrt{2})^2 + \sqrt{2} + 1 \\
&= 4\sqrt{2} + 2(4) - \frac{3}{2}(2\sqrt{2}) + 3(2) + \sqrt{2} + 1 \\
&= 15 + 2\sqrt{2}
\end{aligned}
$$

and in general for *any* $f(x)$ the value $f(\sqrt{2})$ condenses down to an expression of the form $a + b\sqrt{2}$.
And then we can manually verify that $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ forms a ring, and in fact, a field.

So in general, given $\mathbb{Q}$ and some number α which is the root of a polynomial we can *define*

$$\mathbb{Q}(\alpha) = \{f(\alpha) \mid f(x) \in \mathbb{Q}[x]\}$$

and, later on, we will verify that this is *always* a field extension of $\mathbb{Q}$.

Moreover, although not completely obvious at this moment, the fact that α is the root of some polynomial in $\mathbb{Q}[x]$ is important in determining the 'structure' of $\mathbb{Q}(\alpha)$.

For perspective, (especially with the example of $\mathbb{Q}(\sqrt{2})$ we just explored in mind), consider what $\mathbb{Q}(\pi)$ might look like!

If we look at the example of the extension field $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ the construction of it as $\mathbb{Q}[x]/\langle x^2-2\rangle$ was motivated by the quest to obtain a root of x^2-2.

And in the field $\mathbb{Q}(\sqrt{2})$ we not only have $\sqrt{2}$, but the *other* root of it, namely $-\sqrt{2}$, and similarly $\mathbb{Q}(i)$ contains not only, i, but also $-i$, both of which are the roots of x^2+1.

In the next example, we see a somewhat different situation.

Consider $x^3 - 2 \in \mathbb{Q}[x]$ which we can show is irreducible.

The roots are

$$\sqrt[3]{2},\ \zeta\sqrt[3]{2},\ \zeta^2\sqrt[3]{2}$$

where

$$\zeta = e^{\frac{2\pi}{3}} = \frac{-1+\sqrt{-3}}{2}$$

is a primitive (complex) cube root of unity, namely a root of $\Phi_3(x) = \frac{x^3-1}{x-1} = x^2 + x + 1$.

So, in particular, one of the roots is a real number, while the other two are complex.

So if we construct the field extension of $\mathbb{Q}$ using the quotient $\mathbb{Q}[x]/\langle x^3 - 2\rangle$ we get that $x + \langle x^3 - 2\rangle$ is a 'cube root of 2'.

If we want to match this up with a field obtained by 'adjoining' a root of $x^3 - 2$ to $\mathbb{Q}$ (like we did for $\mathbb{Q}(\sqrt{2})$ where we adjoin $\sqrt{2}$) the question is, *which root*?

i.e. We have $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta\sqrt[3]{2})$, and $\mathbb{Q}(\zeta^2\sqrt[3]{2})$, so are these the *same*?

No, let's see why.

The powers of $\sqrt[3]{2}$ are $1, \sqrt[3]{2}, \sqrt[3]{2}^2$, and since $\sqrt[3]{2}^3 = 2$ then $\sqrt[3]{2}^4 = 2\sqrt[3]{2}$, $\sqrt[3]{2}^5 = 2\sqrt[3]{2}^2$, etc.

The point is that every power of $\sqrt[3]{2}$ is a linear combination of the elements of the set $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$.

As such

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$$

so we can think of $\mathbb{Q}(\sqrt[3]{2})$ as a three dimensional vector space over $\mathbb{Q}$.

Also, we observe that $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.

In contrast, the distinct powers of $\zeta\sqrt[3]{2}$ are $\{1,\zeta\sqrt[3]{2},\zeta^2(\sqrt[3]{2})^2\}$ and the distinct powers of $\zeta^2\sqrt[3]{2}$ are $\{1,\zeta^2\sqrt[3]{2},\zeta(\sqrt[3]{2})^2\}$ and so we have

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a,b,c \in \mathbb{Q}\}$$
$$\mathbb{Q}(\zeta\sqrt[3]{2}) = \{a + b\zeta\sqrt[3]{2} + c\zeta^2(\sqrt[3]{2})^2 \mid a,b,c \in \mathbb{Q}\}$$
$$\mathbb{Q}(\zeta^2\sqrt[3]{2}) = \{a + b\zeta^2\sqrt[3]{2} + c\zeta(\sqrt[3]{2})^2 \mid a,b,c \in \mathbb{Q}\}$$

And we note that $\mathbb{Q}(\zeta\sqrt[3]{2})$ and $\mathbb{Q}(\zeta^2\sqrt[3]{2})$ both contain complex numbers, whereas $\mathbb{Q}(\sqrt[3]{2})$ is a *purely real* field.

Moreover, $\zeta\sqrt[3]{2} \notin \mathbb{Q}(\zeta^2\sqrt[3]{2})$. Why?

Can we find $a, b, c \in \mathbb{Q}$ such that $\zeta\sqrt[3]{2} = a + b\zeta^2\sqrt[3]{2} + c\zeta(\sqrt[3]{2})^2$?

$$\zeta = \frac{-1+\sqrt{-3}}{2} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$
$$\zeta^2 = \frac{-1-\sqrt{-3}}{2} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$$

To simplify things a bit we can multiply both sides by ζ^2 to yield

$$\sqrt[3]{2} = a\zeta^2 + b\zeta\sqrt[3]{2} + c(\sqrt[3]{2})^2$$

which can be rewritten as

$$\sqrt[3]{2}(1 - c\sqrt[3]{2}) = a\zeta^2 + b\zeta(\sqrt[3]{2})$$

where we note that the left hand side is a real number.

So now we have

$$\begin{aligned}\sqrt[3]{2}(1 - c\sqrt[3]{2}) &= a\zeta^2 + b\zeta(\sqrt[3]{2}) \\ &= a(-\zeta - 1) + b\zeta\sqrt[3]{2} \\ &= -a + \zeta(-a + b\sqrt[3]{2}) \\ &= (-\frac{a}{2} - \frac{b\sqrt[3]{2}}{2}) + (-\frac{a\sqrt{3}}{2} + \frac{b\sqrt{3}\sqrt[3]{2}}{2})i\end{aligned}$$

and, as we already observed, the left side is a purely real number, which means

$$(-\frac{a\sqrt{3}}{2} + \frac{b\sqrt{3}\sqrt[3]{2}}{2}) = 0$$

which is impossible since it would imply that $\frac{a}{b} = \sqrt[3]{2}$ for $a, b \in \mathbb{Q}$.

So what we've shown is that $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta\sqrt[3]{2})$ and $\mathbb{Q}(\zeta^2\sqrt[3]{2})$ are all *distinct* extension fields of $\mathbb{Q}$, and each contains exactly one root of $x^3 - 2$ and we can 'diagram' this as follows, indicating the containments.

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[3]{2}) & \mathbb{Q}(\zeta\sqrt[3]{2}) & \mathbb{Q}(\zeta^2\sqrt[3]{2}) \\
& \mathbb{Q} \arrow[ul, dash] \arrow[u, dash] \arrow[ur, dash] &
\end{tikzcd}$$

And, we can actually show that $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\zeta\sqrt[3]{2}) = \mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\zeta^2\sqrt[3]{2}) = \mathbb{Q}$, and $\mathbb{Q}(\zeta\sqrt[3]{2}) \cap \mathbb{Q}(\zeta^2\sqrt[3]{2}) = \mathbb{Q}$.

Moreover, we note that 'adjoining' one of the roots of $x^3 - 2$ to $\mathbb{Q}$ yields a field extension which does **not** contain the other two roots.

This is in contrast with $\mathbb{Q}(\sqrt{2})$ which contains *both* roots of $x^2 - 2$.