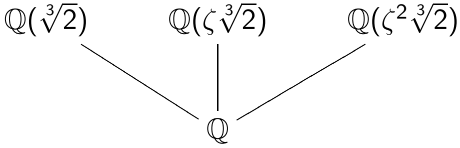
MA542 Lecture

Timothy Kohl

Boston University

March 7, 2025

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.



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.

So the question is, which of these *is* $\mathbb{Q}[x]/\langle x^3-2\rangle$?
We can answer this as follows:

Theorem

The three extension fields $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta\sqrt[3]{2})$, *and* $\mathbb{Q}(\zeta^2\sqrt[3]{2})$ *are all isomorphic to* $\mathbb{Q}[x]/\langle x^3-2\rangle$.

Proof.

If $I=\langle x^3-2\rangle$ and we let $r_i=\zeta^i\sqrt[3]{2}$ for $i=0,1,2$ then define:

$$\psi_i : \mathbb{Q}[x]/I \rightarrow \mathbb{Q}(r_i) \text{ by}$$
$$\psi_i(a+bx+cx^2+I)=a+br_i+cr_i^2$$

and verify that this is 1-1, onto, and a homomorphism, i.e. $\psi_i((f(x)+I)+(g(x)+I))=\psi_i(f(x)+I)+\psi_i(g(x)+I)$ and $\psi_i((f(x)+I)(g(x)+I))=\psi_i(f(x)+I)\psi_i(g(x)+I)$ which is a relatively easy exercise. □

So the point is, all three fields $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta\sqrt[3]{2})$, and $\mathbb{Q}(\zeta^2\sqrt[3]{2})$ are isomorphic to $\mathbb{Q}[x]/\langle x^3-2\rangle$ and therefore to each other as well, even though they are *distinct* extension fields of $\mathbb{Q}$.

So the contrast between these three fields, none of which contains all three roots, as compared with $\mathbb{Q}(\sqrt{2})$, which contains both roots of x^2-2 motivates the following definition.

Definition

Let E be an extension field of F and let $f(x) \in F[x]$.

We say that $f(x)$ splits in E if $f(x)$ can be factored into a product of linear factors in $E[x]$.

We say that E is the/a splitting field of $f(x)$ if it splits in E but in **no proper subfield** of E.

So for example, since $x^2 - 2 \in \mathbb{Q}[x]$ splits as $(x - \sqrt{2})(x + \sqrt{2}) \in \mathbb{R}[x]$ then we say $x^2 - 2$ splits in $\mathbb{R}$.

However, we don't *need* all of $\mathbb{R}$ so to speak since $x^2-2=(x-\sqrt{2})(x+\sqrt{2}) \in \mathbb{Q}(\sqrt{2})[x]$, and $\mathbb{Q}(\sqrt{2})$ is *a* splitting field of x^2-2 since there is no subfield of $\mathbb{Q}(\sqrt{2})$ wherein x^2-2 factors.

Indeed, since $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$ then any subfield of $\mathbb{Q}(\sqrt{2})$ that splits x^2-2 *must* contain both $\sqrt{2}$ and $-\sqrt{2}$ which means it contains $\mathbb{Q}(\sqrt{2})$ so $\mathbb{Q}(\sqrt{2})$ is the smallest subfield of itself which contains these roots and is therefore a splitting field.

Splitting Fields

As mentioned earlier, the polynomial $x^2 - 2 \in \mathbb{Q}[x]$ splits in a field like $\mathbb{R}$, but that $\mathbb{Q}(\sqrt{2})$ is the splitting field in that it is the 'minimal' or 'smallest' extension of $\mathbb{Q}$ that contains the roots of $x^2 - 2$.

In particular, $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ but is *not* irreducible in $\mathbb{Q}(\sqrt{2})[x]$ since, in $\mathbb{Q}(\sqrt{2})[x]$ it equals $(x - \sqrt{2})(x + \sqrt{2})$.

And the field extension of $\mathbb{Q}$ given by Kronecker's theorem, $\mathbb{Q}[x]/\langle x^2 - 2\rangle$, is isomorphic to $\mathbb{Q}(\sqrt{2})$.

In contrast, for $x^3 - 2 \in \mathbb{Q}[x]$, the field $\mathbb{Q}[x]/\langle x^3 - 2\rangle$ is isomorphic to all three fields $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta\sqrt[3]{2})$, $\mathbb{Q}(\zeta^2\sqrt[3]{2})$, but each contains only one root of $x^3 - 2$.

So what about a splitting field for $x^3 - 2$?

It splits in $\mathbb{C}$ but this is not minimal at all.

Since the roots are $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$, and $\zeta^2\sqrt[3]{2}$ then any splitting field (over $\mathbb{Q}$) must contain these three roots.

Recall that

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

So if $E/\mathbb{Q}$ is a splitting field for $x^3 - 2$ then it contains

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

so it must contain, for example

$$\frac{\zeta\sqrt[3]{2}^2}{\sqrt[3]{2}^2} = \zeta$$

as well as $\dfrac{\zeta^2\sqrt[3]{2}}{\sqrt[3]{2}} = \zeta^2$ etc.

But $\mathbb{Q}(\zeta\sqrt[3]{2})$ and $\mathbb{Q}(\zeta^2\sqrt[3]{2})$ *don't* contain ζ, and clearly $\mathbb{Q}(\sqrt[3]{2})$ doesn't either since ζ is complex and $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.

The powers of ζ are $\{1, \zeta, \zeta^2\}$ since $\zeta^3 = 1$.

However, we must make an important observation. Since ζ is a root of $x^2 + x + 1$ then

$$\begin{aligned} \zeta^2 + \zeta + 1 = 0 \\ \downarrow \\ \zeta^2 = -\zeta - 1 \end{aligned}$$

i.e. ζ^2 is a linear combination of $1, \zeta$.

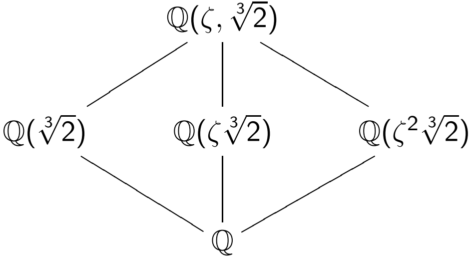
As such we note then that $\mathbb{Q}(\zeta) = \{a + b\zeta \mid a, b \in \mathbb{Q}\}$.

What we end up with is that (the) splitting field of $x^3 - 2$ over $\mathbb{Q}$ is the field

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

namely the $\mathbb{Q}$ span of $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \zeta, \zeta\sqrt[3]{2}, \zeta\sqrt[3]{2}^2\}$.

And we can see that this field is an extension field of $\mathbb{Q}(\sqrt[3]{2})$,$\mathbb{Q}(\zeta\sqrt[3]{2})$, and $\mathbb{Q}(\zeta^2\sqrt[3]{2})$, which are all extension fields of $\mathbb{Q}$, which we can diagram.



Now, $\mathbb{Q}(\zeta, \sqrt[3]{2})$ contains all the roots of $x^3 - 2$, but is there a proper subfield $E \subseteq \mathbb{Q}(\zeta, \sqrt[3]{2})$ which contains all the roots?

No, and the reason is that, as we saw, any such field must contain ζ and $\sqrt[3]{2}$ and therefore must contain $\mathbb{Q}(\zeta, \sqrt[3]{2})$ which means it must *equal* $\mathbb{Q}(\zeta, \sqrt[3]{2})$.

So does this same idea work for an arbitrary polynomial $f(x) \in F[x]$?

Theorem

Given $f(x) \in F[x]$, then there exists a splitting field E containing F for $f(x)$.

Proof.

We use induction on $n = deg(f(x))$. If $deg(f(x)) = 1$ then $f(x) = ax + b$ and so $\alpha = \frac{-b}{a}$ is the root of $f(x)$ and $\alpha \in F$, so F is the splitting field of $f(x)$.
Now say $deg(f(x)) > 1$ then there exists an extension field field $F(a_1)$ which contains (at least) one root of $f(x)$, and so, in $F(a_1)[x]$ we have $f(x) = (x - a_1)g(x)$ where now $deg(g(x)) = n - 1$, and so, inductively, we can assume that there is a field E (which is an extension of $F(a_1)$) which is a splitting field of $g(x)$ but then E is a splitting field (over F) of $f(x)$. □

Here is a somewhat alternative way of thinking about $\mathbb{Q}(\zeta, \sqrt[3]{2})$ as a splitting field of $x^3 - 2$.

Since $\mathbb{Q}(\sqrt[3]{2})$ contains at least one root of $x^3 - 2$ then in $\mathbb{Q}(\sqrt[3]{2})$, $x^3 - 2 = (x - \sqrt[3]{2})g(x)$, where

$$
\begin{aligned}
g(x) &= (x - \zeta\sqrt[3]{2})(x - \zeta^2\sqrt[3]{2}) \\
&= x^2 - (\zeta + \zeta^2)\sqrt[3]{2}x + \sqrt[3]{2}^2 \\
&= x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2
\end{aligned}
$$

and so the field extension of $\mathbb{Q}(\sqrt[3]{2})$ which contains the other two roots is $\mathbb{Q}(\sqrt[3]{2})(\zeta)$.

And $\mathbb{Q}(\sqrt[3]{2})(\zeta)$ is described as follows:

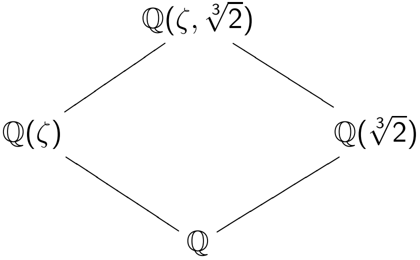
$$\mathbb{Q}(\sqrt[3]{2})(\zeta) = \{a + b\zeta \mid a, b \in \mathbb{Q}(\sqrt[3]{2})\}$$

i.e. $a = a_0 + a_1\sqrt[3]{2} + a_1\sqrt[3]{2}^2$ and $b = b_0 + b_0\sqrt[3]{2} + b_2\sqrt[3]{2}^2$ where $a_i, b_j \in \mathbb{Q}$, i.e.

$$\begin{aligned} a + b\zeta &= (a_0 + a_1\sqrt[3]{2} + a_1\sqrt[3]{2}^2) + (b_0 + b_0\sqrt[3]{2} + b_2\sqrt[3]{2}^2)\zeta \\ &= a_0 + a_1\sqrt[3]{2} + a_1\sqrt[3]{2}^2 + b_0\zeta + b_0\sqrt[3]{2}\zeta + b_2\zeta\sqrt[3]{2}^2 \end{aligned}$$

which is exactly what a typical element of $\mathbb{Q}(\zeta, \sqrt[3]{2})$ looks like, i.e. $\mathbb{Q}(\sqrt[3]{2})(\zeta) = \mathbb{Q}(\zeta, \sqrt[3]{2})$, and we arrive at this by first extending $\mathbb{Q}$ to get $\mathbb{Q}(\sqrt[3]{2})$ and then extend $\mathbb{Q}(\sqrt[3]{2})$ to get $\mathbb{Q}(\sqrt[3]{2})(\zeta)$.

We also note, that $\mathbb{Q}(\zeta, \sqrt[3]{2})$ is equally $\mathbb{Q}(\zeta)(\sqrt[3]{2})$, namely extend $\mathbb{Q}$ by ζ and then extend $\mathbb{Q}(\zeta)$ to get $\mathbb{Q}(\zeta)(\sqrt[3]{2})$.



We saw earlier that $\mathbb{Q}(\sqrt[3]{2})$ consists of expressions of the form $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$ where $a, b, c \in \mathbb{Q}$ since $\sqrt[3]{2}^3 = 2$ so that all higher powers of $\sqrt[3]{2}$ can be expressed as linear combinations of $1, \sqrt[3]{2}, \sqrt[3]{2}^2$.

This is precisely due to the fact that $\sqrt[3]{2}$ is a root of $x^3 - 2$, and we also saw that $\mathbb{Q}(\sqrt[3]{2})$ is isomorphic to $\mathbb{Q}[x]/\langle x^3 - 2\rangle$.

If we let $I = \langle x^3 - 2\rangle$ we note that $x^3 - 2 + I = 0 + I$, namely that $x^3 + I = 2 + I$ and that the distinct cosets of I in $\mathbb{Q}[x]/I$ are of the form $a + bx + cx^2 + I$, and so one makes the correspondence

$$a + bx + cx^2 + I \leftrightarrow a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$$

So in general, we have the following

Theorem

Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a root of $p(x)$ in some extension field E of F then

$$F(a) \cong F[x]/\langle p(x)\rangle$$

where, if $deg(p(x)) = n$ then every element of $F(a)$ is of the form $c_0 + c_1 a + \cdots + c_{n-1}a^{n-1}$ where $c_0, \ldots, c_{n-1} \in F$.

The proof of this is basically from looking at $F[x]/\langle p(x)\rangle$ and realizing that the distinct cosets are of the form $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$.

We also have this basic fact, which we saw exemplified in the $x^3 - 2$ case.

Corollary

Let F be a field and let $p(x) \in F[x]$ be irreducible. If a is a root of $p(x)$ in some extension field E of F and if b is a root of $p(x)$ in some (other) extension field E' of F then $F(a) \cong F(b)$.

Proof.

$F(a) \cong F[x]/\langle p(x)\rangle$ and $F(b) \cong F[x]/\langle p(x)\rangle$. □

We can actually give the isomorphism directly, namely let $\phi : F(a) \to F(b)$ be given by $\phi(c_0 + c_1 a + \cdots + c_{n-1}a^{n-1}) = c_0 + c_1 b + \cdots + c_{n-1}b^{n-1}$ which derives from simply defining $\phi(a) = b$ and $\phi(c) = c$ for $c \in F$.

We should point out that for $\phi : F(a) \to F(b)$ one has that $\phi\big|_F = id$, the identity, which is not insignificant.

Another consequence of this is that if $p(x)$ is irreducible in $F[x]$ and a is a root of $p(x)$ in some extension field of E of F then $F(a)$ consists of all F-linear combinations of $\{1, a, a^2, \ldots, a^{n-1}\}$ where $n = deg(p(x))$ which means that $F(a)$ is not just a field, but also a F-vector space, and , as a vector space, $dim_F(F(a)) = n$.

The other important corollary is this.

Corollary

Let F be a field and let $p(x) \in F[x]$ be irreducible, then any two splitting fields of $p(x)$ over F are isomorphic.