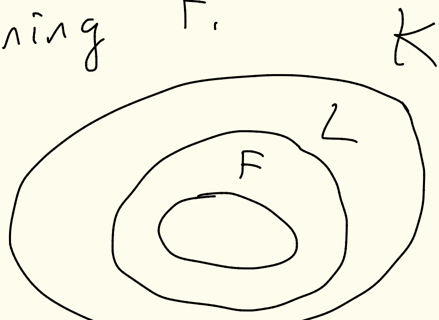
Math 5402

4/8/20

13.4 - Splitting fields and algebraic closures

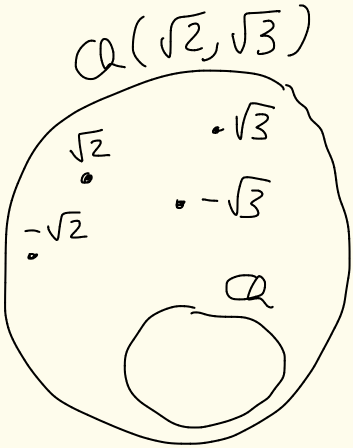
Def: An extension field K of a field F is called a *splitting field* for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield L of K containing F.



Ex: What is the splitting field of $f(x) = (x^2-2)(x^2-3)$ over $\mathbb{Q}$?

The roots of $f(x)$ are $x = \pm\sqrt{2}, \pm\sqrt{3}$.

So the splitting field of f is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.



$$
\begin{tikzcd}
\mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[d, dash, "4"] \\
\mathbb{Q}
\end{tikzcd}
$$

In $\mathbb{Q}(\sqrt{2},\sqrt{3})[x]$, f factors completely into
$f(x) = (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$

Ex: Find the splitting field for x^3-2 over $\mathbb{Q}$.

roots of x^3-2 are:

$$2^{1/3},\ 2^{1/3}\omega,\ 2^{1/3}\omega^2$$

where

$$\omega = e^{\frac{2\pi i}{3}} = \cos\left(\tfrac{2\pi}{3}\right)+i\sin\left(\tfrac{2\pi}{3}\right) = -\frac{1}{2}+i\frac{\sqrt{3}}{2}$$

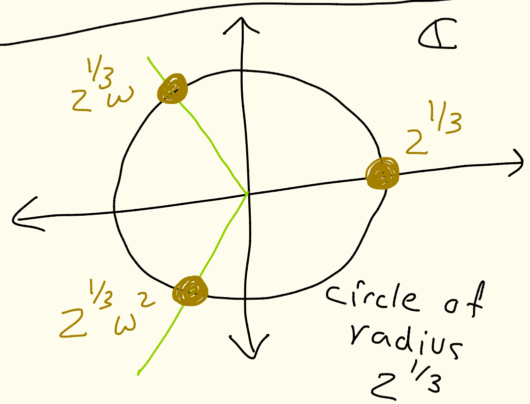
$$\left(\omega^2 = -\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)$$

$a \in \mathbb{R}$, $a>0$

x^n-a has roots:

$$a^{1/n}\left(e^{\frac{2\pi i}{n}}\right)^k, \quad k=0,1,2,\ldots,n-1$$

$$e^{i\theta} = \cos(\theta)+i\sin(\theta)$$



Is $\mathbb{Q}(2^{1/3})$ the splitting field?

$$[\mathbb{Q}(2^{1/3}):\mathbb{Q}] = 3 \longleftarrow m_{2^{1/3},\mathbb{Q}}(x) = x^3-2$$

(irreducible by Eisenstein $p=2$)

$$\mathbb{Q}(2^{1/3}) = \{\underbrace{a + b(2^{1/3}) + c(2^{1/3})^2}_{\text{these are all in } \mathbb{R}} \,/\, a,b,c \in \mathbb{Q}\}$$

So, $\mathbb{Q}(2^{1/3}) \subseteq \mathbb{R}$.

Thus, $2^{1/3}\omega,\ 2^{1/3}\omega^2 \notin \mathbb{Q}(2^{1/3})$.

The splitting field is

$$\mathbb{Q}(2^{1/3},\ 2^{1/3}\omega,\ 2^{1/3}\omega^2)$$

$$\boxed{\begin{aligned} \omega &= -\frac{1}{2} + i\frac{\sqrt{3}}{2} \\ \omega^2 &= -\frac{1}{2} - i\frac{\sqrt{3}}{2} \end{aligned}}$$

<u>Claim:</u>

$$\mathbb{Q}(2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2) = \mathbb{Q}(2^{1/3}, i\sqrt{3})$$

<u>pf:</u> $\mathbb{Q}(2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2) \subseteq \mathbb{Q}(2^{1/3}, i\sqrt{3})$ is clear since $2^{1/3}, \omega \in \mathbb{Q}(2^{1/3}, i\sqrt{3})$.

Why is $\mathbb{Q}(2^{1/3}, i\sqrt{3}) \subseteq \mathbb{Q}(2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2)$?

Because $2^{1/3} \in \mathbb{Q}(2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2)$ and

$$2(2^{1/3})^2(2^{1/3}\omega) + 1$$

$$= 2(2^{1/3})^2\left(2^{1/3}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\right) + 1$$

$$= \sqrt{3}\, i$$

So, $\sqrt{3}\, i \in \mathbb{Q}(2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2)$.

$\boxed{\text{Claim}}$

So the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is

$$\mathbb{Q}(2^{1/3}, \sqrt{3}\, i)$$

$$
\begin{tikzcd}
\mathbb{Q}(2^{1/3}, \sqrt{3}i) \arrow[d, dash, "2"] \arrow[dd, dash, bend right=60, "6"'] \\
\mathbb{Q}(2^{1/3}) \arrow[d, dash, "3"] \\
\mathbb{Q}
\end{tikzcd}
$$

$m_{\sqrt{3}i, \mathbb{Q}(2^{1/3})}(x) = x^2 + 3$

$\sqrt{3}i$ is a root of x^2+3

and $\underbrace{\sqrt{3}i, -\sqrt{3}i}_{\text{in } \mathbb{C} \setminus \mathbb{R}} \notin \underbrace{\mathbb{Q}(2^{1/3})}_{\mathbb{Q}(2^{1/3}) \subseteq \mathbb{R}}$

$m_{2^{1/3}, \mathbb{Q}}(x) = x^3 - 2$

(irreducible over $\mathbb{Q}$ by Eisenstein with $p=2$)

basis for $\mathbb{Q}(2^{1/3})$ over $\mathbb{Q}$: $1, 2^{1/3}, 2^{2/3}$

basis for $\mathbb{Q}(2^{1/3}, \sqrt{3}i)$ over $\mathbb{Q}(2^{1/3})$: $1, \sqrt{3}i$

basis for $\mathbb{Q}(2^{1/3}, \sqrt{3}i)$ over $\mathbb{Q}$:

$1, 2^{1/3}, 2^{2/3}, \sqrt{3}i, 2^{1/3}\sqrt{3}i, 2^{2/3}\sqrt{3}i$

$\mathbb{Q}(2^{1/3}, \sqrt{3}i) = \{a + b2^{1/3} + c2^{2/3} + d\sqrt{3}i + e2^{1/3}\sqrt{3}i + f2^{2/3}\sqrt{3}i \mid a,b,c,d,e,f \in \mathbb{Q}\}$

<u>Theorem:</u> For any field F, if $f(x) \in F[x]$, then there exists an extension K of F which is the splitting field for $f(x)$.

<u>proof:</u>

<u>step 1:</u> We first show that there exists an extension E of F over which $f(x)$ splits completely into linear factors. We do this by induction on the degree n of f.

If $n=1$, then $f(x) = ax+b \in F[x]$. So its only root $-\frac{b}{a}$ is already in F. So, $E = F$.

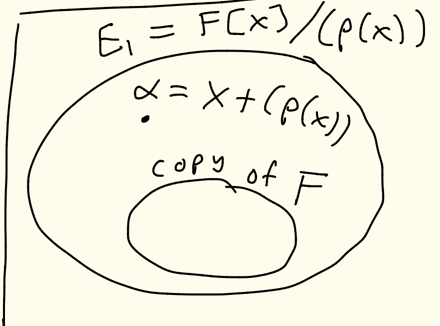
Suppose $n>1$ and the theorem is true for all polys of degree less than n.

If the irreducible factors of $f(x)$ over F all have degree 1 then again F is the splitting field of $f(x)$ and $E = F$.

If this isn't the case then $f(x) = p(x)h(x)$ where $p(x), h(x) \in F[x]$ and $p(x)$ is irreducible over F of degree at least 2.

h(x) could be any poly including 1 or a constant

By a previous theorem (Thm 3 in book) there exists an extension E_1 of F containing a root α of $p(x)$.

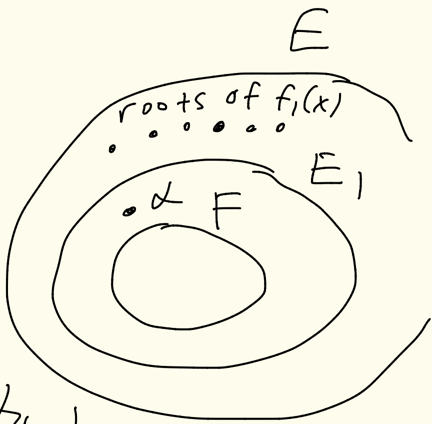


Then,

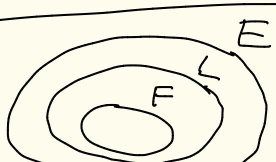
$$f(x) = (x-\alpha) f_1(x)$$

where $f_1(x) \in E_1[x]$ and $\deg(f_1) < n$.

By the induction hypothesis (or keep repeating this process) applied to $f_1(x)$ we get an extension E of E_1 where $f_1(x)$ factors completely into linear factors.



So, $f(x) = (x-\alpha) f_1(x)$ will factor completely into linear factors in E (since $\alpha \in E$ too).



step 2: To get a splitting field let K be the intersection of all subfields L of E where L contains F and $f(x)$ factors completely into linear factors over L.

Then K is a splitting field for $f(x)$ $\square$