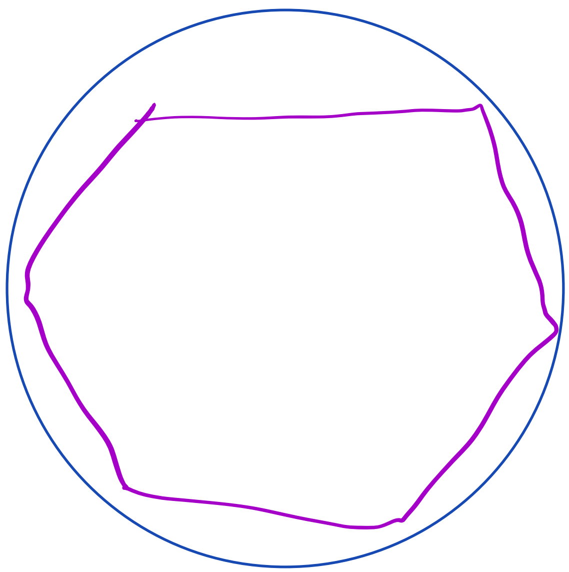
April 28

Last time: splitting field

Today: Finish proof of uniqueness

hexagon inscribing a circle



Let K be a field

Let $f(x) \in K[x]$

<u>Defn</u> We say that $K < L$ is a <u>splitting field</u> if

① $f(x) = a_n(x-\alpha_1)\cdots(x-\alpha_d)$ where $\alpha_i \in L$ (i.e. $f(x)$ splits over K)

② $L = K(\alpha_1, \dots, \alpha_d)$

<u>Thm</u> (Existence) For any K and $f(x) \in K[x]$, $\exists$ splitting field.

<u>Prop</u> (Univ. property of splitting field)

- Let $K < L$ be the splitting field of $f(x) \in K[x]$.
- Let $K \xrightarrow{\sigma} L'$ be another field extension such that $\underline{\sigma(f) \in L'[x]}$ splits

Then $\exists\, \bar{\sigma}: L \to L'$ such that $\bar{\sigma}(a) = \sigma(a)$ $\forall a \in K$.

<u>Picture:</u>

$$\begin{tikzcd} L \arrow[r, dashed, "\exists \bar{\sigma}"] & L' \\ K \arrow[u, "\cup"] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

splitting field of $f \in K[x]$

Assume $\sigma(f)$ splits in L'

<u>Proof:</u> Write $f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_d)$ where $\alpha_i \in L$.

If all $\alpha_i \in K$, then $K = L$ & can take $\bar{\sigma} = \sigma$

Otherwise, let α be a root of $f(x)$ not in K. Then $\exists$ min poly $g(x)$ for α.

$\to$ Know $g(x)$ irred and $f(x) = g(x)h(x)$ for some h

Consider $K \subset K[x]/(f)$

Prop (Univ. property of splitting fields)

- Let $K \subset L$ be the splitting field of $f(x) \in K[x]$.
- Let $K \xrightarrow{\sigma} L'$ be another field extension such that $\sigma(f) \in L'[x]$ splits.

Then $\exists\, \bar{\sigma} : L \to L'$ such that $\bar{\sigma}(a) = \sigma(a)$ $\forall a \in K$.

Picture:

$$\begin{tikzcd} L \arrow[r, dashed, "\exists \bar{\sigma}"] & L' \\ \cup & \\ K \arrow[uur, "\sigma"'] & \end{tikzcd}$$

splitting field of $f \in K[x]$

Assume $\sigma(f)$ splits in L'

Proof: Write $f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_d)$ where $\alpha_i \in L$.

If all $\alpha_i \in K$, then $K = L$ & can take $\bar{\sigma} = \sigma$.

Otherwise, let α be a root of $f(x)$ not in K. Then $\exists$ min poly $g(x)$ for α.

$\to$ Know $g(x)$ irred and $f(x) = g(x)h(x)$ for some h.

Consider $K \subset K[x]/(g) = K(\alpha)$

Picture

$$\begin{tikzcd} L \arrow[rr, dashed, "\bar{\sigma}"] & & L' \\ \cup & & \\ K(\alpha) = K[x]/(g) \arrow[uurr, dashed, "\sigma'"] & & \\ \cup & & \\ K \arrow[uuuurr, "\sigma"'] & & \end{tikzcd}$$

Proof by induction on $|L:K|$.

Goal: Extend σ to σ'.

This suffices by using induction since $|L:K(\alpha)| < |L:K|$ and L splitting field of $f(x) \in K(\alpha)[x]$. $\rightsquigarrow \bar{\sigma}$

Constructing σ': Let's define

$$K[x] \xrightarrow{\psi} L'$$

Since $g \mid f \Rightarrow g(x)$ has a root $\beta \in L'$

Define $\psi(x) = \beta$ or $\psi(g(x)) = g(\beta)$

Then $\operatorname{Ker}\psi = g(x)$

$\to$ Know $g(x)$ irred
and $f(x) = g(x)h(x)$ for some h

Consider $K \subset K[x]/(g) = K(\alpha)$

Picture

$$\begin{tikzcd}
L \arrow[rr, dashed, "\bar{\sigma}"] & & L' \\
K(\alpha) = K[x]/(g) \arrow[u, phantom, "\cup"] \arrow[urr, dashed, "\sigma'"] & & \\
K \arrow[u, phantom, "\cup"] \arrow[uurr, bend right, "\sigma"'] & &
\end{tikzcd}$$

Proof by induction on $|L:K|$.

<u>Goal</u>: Extend σ to σ'.

This suffices by using induction since $|L:K(\alpha)| < |L:K|$ and L splitting field of $f(x) \in K(\alpha)[x]$. $\rightsquigarrow \bar{\sigma}$

Constructing σ': Let's define

$$K[x] \xrightarrow{\psi} L'$$

Since $g \mid f \implies g(x)$ has a root $\beta \in L'$

Define $\psi(x) = \beta$ or $\psi(q(x)) = q(\beta)$

Then $\operatorname{Ker}\psi = g(x)$

Finally, gives

$$\begin{tikzcd}
K[x] \arrow[r, "\psi"] \arrow[d] & L' \\
K[x]/(g) \arrow[ur, dashed, "\exists \sigma'"'] &
\end{tikzcd}$$

since $g \in \ker(\psi)$

$\blacksquare$

Prop (Univ. property of splitting fields)

- Let $K \subset L$ be the splitting field of $f(x) \in K[x]$.
- Let $K \xrightarrow{\sigma} L'$ be another field extension such that $\sigma(f) \in L'[x]$ splits

Then $\exists\, \bar\sigma : L \to L'$ such that
$$\bar\sigma(a) = \sigma(a) \quad \forall a \in K.$$

Picture:

$$\begin{tikzcd} L \arrow[r, dashed, "\exists \bar\sigma"] & L' \\ K \arrow[u, phantom, sloped, "\subset"] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

splitting field of $f \in K[x]$

Assume $\sigma(f)$ splits in L'

Thm (Uniqueness)

Let $\varphi : K \to K'$ isom of fields

Let $f(x) \in K[x]$ & $f' \in K'[x]$ its image

If $K \subset L$ splitting field of f

and $K' \subset L'$ " " f',

Then $\exists$ isom $\bar\varphi : L \to L'$ extending φ.

Picture:

$$\begin{tikzcd} L \arrow[r, dashed, "\exists"] & L' \\ K \arrow[u, phantom, sloped, "\subset"] \arrow[r, "\varphi"] & K' \arrow[u, phantom, sloped, "\subset"] \end{tikzcd}$$

Rmk In special case $K = K'$, shows uniqueness of splitting field

Pf: Proposition gives

$$\begin{tikzcd} L \arrow[r, dashed, "\bar\sigma"] & L' \\ K \arrow[u, phantom, sloped, "\subset"] \arrow[ur, "\sigma"] \arrow[r, "\varphi"] & K' \arrow[u, phantom, sloped, "\subset"] \end{tikzcd}$$

Define $\sigma = \varphi$

So we have $\bar\sigma$! Just need to show it's an isom.

But we know $\bar\sigma : L \to L'$ is injective

$\Longrightarrow |L' : K| \geq |L : K|$

But it's symmetric! ($\varphi^{-1} : K' \to K$)

Same argument applied to $\varphi^{-1} : K' \to K$

gives $|L : K| \geq |L' : K|$

$\Longrightarrow |L : K| = |L' : K| \Rightarrow L \underset{\text{iso}}{\overset{\bar\sigma}{\to}} L'$

Next topics

- normal extensions

Say $K \subset L$ normal field ext

if $\forall f \in K[x]$ such that

$f(x)$ has some root in L, then

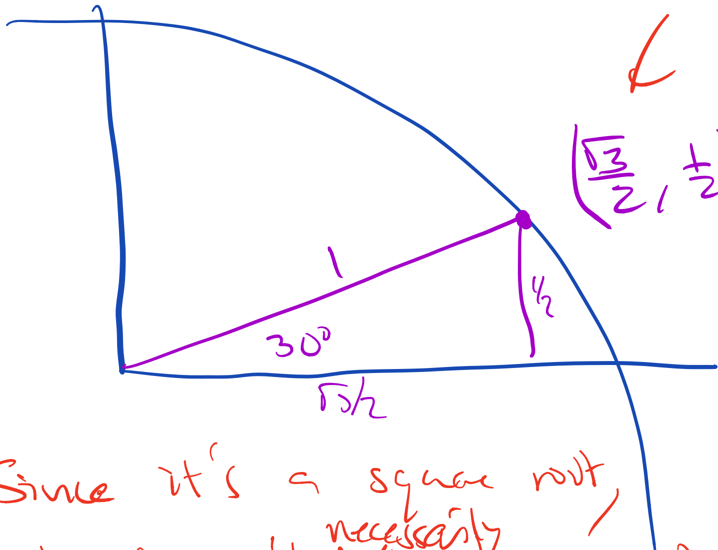
$f(x)$ splits over L.

Prop: Splitting fields are normal.

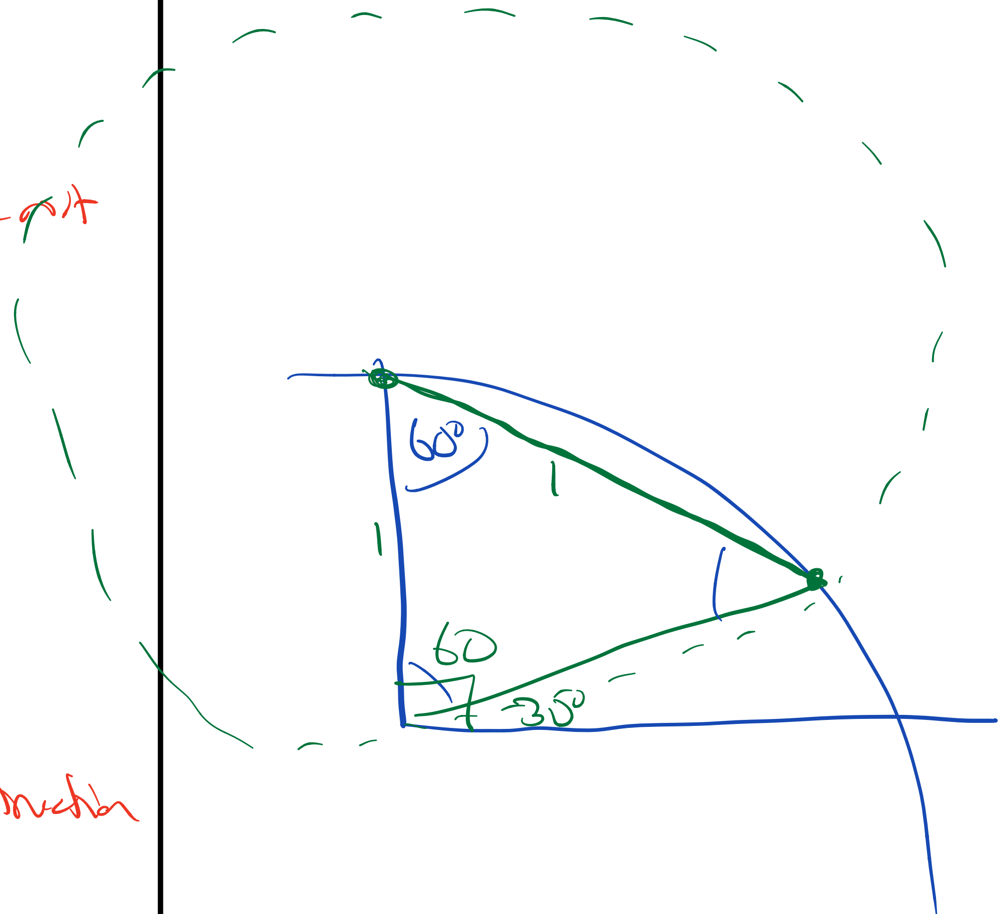
- Fields in char $= p$ & finite fields.

Discussion on HW5

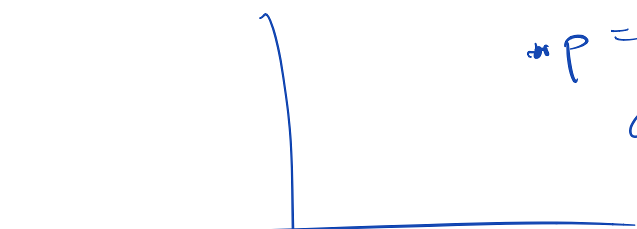
Trisecting 90° angle



square root



Since it's a square root, it doesn't necessarily imply a construction exist



* $p = (a,b)$

  $a,b \in \mathbb{Q}(\sqrt{d})$

  $d \in \mathbb{Z}$

(Hungerford)

It's possible to construct p as intersection point using ruler/compass.