Previously, given irred $f(x) \in F[x]$, the field $F[x]/(f)$ contains a root θ of f.

Today: adjoin <u>all</u> the roots of f to F.

Recall: $f(\alpha) = 0 \Leftrightarrow x - \alpha \mid f(x)$

and $F[x]$ is a UFD, so f factors into $\leq \deg f$ irreducibles, and all factors are unique up to units, so f has $\leq n$ roots.

Def: The ext'n field K of F is a splitting field for $f(x) \in F[x]$ if

a) f factors into linear factors ("splits completely") in $K[x]$ (equivalently: K contains $n := \deg f$ roots of f, counting multiplicity)

b) If $F \subseteq L \subsetneq K$, F does not split completely in $L[x]$.

E.g: a) $\mathbb{Q}(\sqrt{2})$ is the splitting field for $x^2 - 2 \in \mathbb{Q}[x]$:

$$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$$

$\mathbb{R}$ is not (since $\mathbb{Q}(\sqrt{2})$ is smaller)

b) $\mathbb{Q}(\sqrt[3]{2})$ is <u>not</u> the splitting field of $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ since $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ but f has two nonreal roots.

$$f(x) = x^3 - 2 = (x - \sqrt[3]{2})\underbrace{(x^2 + \sqrt[3]{2}\,x + (\sqrt[3]{2})^2)}_{\text{irred.}} \in \mathbb{Q}(\sqrt[3]{2})[x]$$

Fix: adjoin a (primitive) root of unity:

Let $\zeta := \zeta_3 = e^{2\pi i/3}$

Then, $\zeta^3 = 1$

in general, can take ζ_n to be any nth root of 1 that is not a dth root of 1 for $d < n$.

Then $f(\sqrt[3]{2}) = f(\zeta \sqrt[3]{2}) = f(\zeta^2 \sqrt[3]{2}) = 0$.

Let $K = \mathbb{Q}(\sqrt[3]{2}, \zeta)$. Then,

$$f(x) = (x - \sqrt[3]{2})(x - \zeta\sqrt[3]{2})(x - \zeta^2\sqrt[3]{2}) \in K[x]$$

So f splits completely over K. If f splits over $L \subseteq K$ then $\sqrt[3]{2}$, $\zeta\sqrt[3]{2} \in L$, so $\zeta \in L$ and $K = L$.

Thm: Let $f(x) \in F[x]$. $\exists$ a field extension K/F s.t. K is a splitting field for F

Remark: K is unique up to isom., so we will often talk about <u>the</u> splitting field $\mathrm{Sp}\, f := \mathrm{Sp}_F f$ of f over F.

Pf: Induction on $n := \deg f$. Let f_1: irred. factor of f, $L := F[x]/(f_1(x))$. Then f has a root $\theta_1 \in L$, so

$$f(x) = (x-\theta_1)\underbrace{f_2(x)}_{\deg = n-1} \in L[x].$$

By induction, there is a splitting field K for f_2 over L.

$$f(x) = (x-\theta_1)f_2(x) = (x-\theta_1)(x-\theta_2)\cdots(x-\theta_n) \in K[x].$$

Thus, $F(\theta_1, \theta_2, \dots, \theta_n)$ is a splitting field for f over F. $\square$

Cor: If K is a/the splitting field for $f(x) \in F[x]$, then $[K:F] \leq (\deg f)!$

(see Midterm 1 Problem 2b

Pf: Induction.

$$[K:F] = \underbrace{[K:F(\overset{\substack{\text{root}\\ \text{of } f\\ \downarrow}}{\theta})]}_{\substack{\leq (n-1)! \\ \text{by inductive} \\ \text{hyp.}}} \underbrace{[F(\theta):F]}_{\substack{\leq n \\ (= n \text{ if} \\ f \text{ irred.})}} \leq n!$$

$\square$

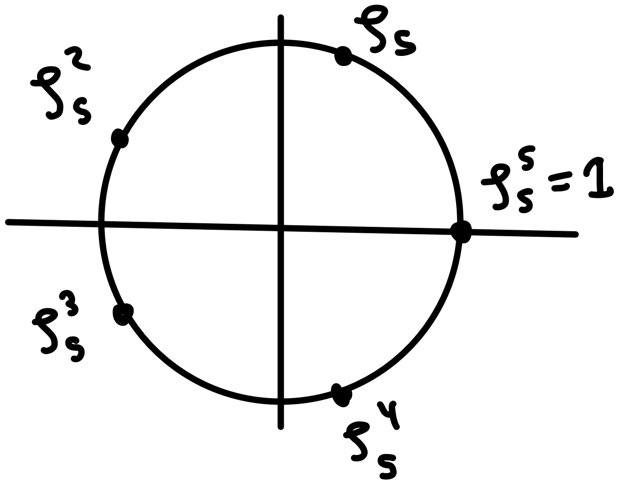
Remarks:

a) "Most" polys. have $[K:F] = n!$

b) $n! = |S_n|$. Seems like a random fact, but this will be highly relevant!

usually $\zeta_n = e^{2\pi i/n}$

Def/Ex: Let ζ_n be a primitive nth root of 1.
The field $\mathbb{Q}(\zeta_n)$ is the <u>cyclotomic field</u> of nth roots of 1



$$x^n - 1 = (x-1)(x-\zeta_n)(x-\zeta_n^2)\cdots(x-\zeta_n^{n-1})$$
$$= (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

and $1, \zeta_n, \ldots, \zeta_n^{n-1} \in \mathbb{Q}(\zeta_n)$

So $\mathbb{Q}(\zeta_n)$ is the splitting field for $x^n - 1$

$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq n-1$ w/ equality iff p: prime (HW3 #4)

Ex: $f(x) = x^p - 2 \in \underbrace{\mathbb{Q}[x]}_{\text{default}}$, p: prime

$$f(x) = (x - \sqrt[p]{2})(x - \zeta_p \sqrt[p]{2}) \cdots (x - \zeta_p^{p-1} \sqrt[p]{2})$$

unique pos. real
pth root of 2

Splitting field: $S_p(x^p - 2) = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$

Composite ext'n:

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}][\mathbb{Q}(\zeta_p) : \mathbb{Q}]$$

Tower Law:

$$p = [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}]$$

$$p-1 = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}]$$

coprime

So

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1)$$

If time: uniqueness of splitting fields
(see D&F Thm 13.8, 13.27)

Thm: Let $\varphi : F \xrightarrow{\sim} F'$ be an isom. of fields.
Let $f(x) \in F[x]$, and $f'(x)$ be the image of f in $F'[x]$ under φ (mapping x to itself)

a) Suppose f is irred. Let α be a root of f, β be a root of f'. Then $\exists$ $F(\alpha) \xrightarrow{\sim} F'(\beta)$ sending $F \xrightarrow{\varphi} F'$

$$\alpha \longmapsto \beta$$

b) Let K be a splitting field for f over F
K' be a splitting field for f' over F'
Then $\exists$ $K \xrightarrow{\sim} K'$ sending $F \xrightarrow{\varphi} F'$

Pf: a) $$F(\alpha) \cong F[x]/(f) \cong F'[x]/(f') \cong F'(\beta)$$

b) Induction. Choose a root $\alpha \in K$ of some irred. factor p of f and a root $\beta \in K'$ of $p' := \varphi(p)$.

By part a), $F(\alpha) \cong F'(\beta)$, so let $E := F(\alpha)$, $E' := F'(\beta)$.

Now if $g = \frac{f}{x-\alpha}$, $g' = \frac{f'}{x-\beta}$, we have the same situation as b) but w/ g, g', E, E' replacing f, f', F, F'.

By the inductive hypothesis, $\exists\ K \xrightarrow{\sim} K$

sending $E \xrightarrow{\sim} E'$

sending $F \xrightarrow{\sim} F'$.

$\square$

Cor: $Sp_F f$ is unique up to isom.

$\square$