Splitting Fields: K/F is a splitting field for $f(x) \in F[x]$ if

(a) $f(x)$ factors into linear terms in $K[x]$. ("splits completely")

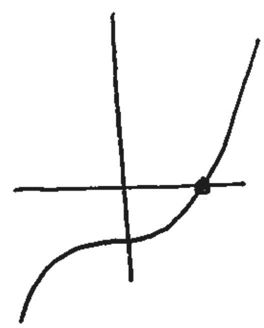
(b) $f(x)$ does not split completely in any $F \subseteq L \subsetneq K$.

Ex: $\mathbb{Q}(\sqrt{2})$ is the splitting field for $x^2 - 2$ in $\mathbb{Q}[x]$, as $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. [Note: $\mathbb{R}$ is not a splitting field.]

Q: What is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$ (inside $\mathbb{C}$)?

Note: $\mathbb{Q}(\sqrt[3]{2})$ is not big enough:

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



Let $\rho = e^{2\pi i/3}$ so that $\rho^3 = 1$. Then $f(\rho\sqrt[3]{2}) = f(\rho^2\sqrt[3]{2}) = 0$

So over $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$ have

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \rho \cdot \sqrt[3]{2})(x - \rho^2 \cdot \sqrt[3]{2})$$

In fact, K is a splitting field: As $\mathbb{C}[x]$ is a UFD, any field $\subseteq \mathbb{C}$ where $x^3 - 2$ splits completely must contain $\sqrt[3]{2}$ and $\rho \cdot \sqrt[3]{2}$ and hence also ρ.

<u>Thm</u>: Let $f(x) \in F[x]$. Then $\exists$ an extension K/F which is a splitting field for f.

<u>Pf</u>: Induct on $\deg f$. Let f_1 be an irred. factor of f, and set $L = F[x]/(f_1(x)) = F(\theta_1 = x + (f_1(x)))$

Then $f(\theta) = 0$, so $f(x) = (x - \theta_1) f_2(x)$ in $L[x]$.

By induction, $\exists K/L$ in which f_2 splits completely as

$$(x - \theta_2)(x - \theta_3) \cdots (x - \theta_n)$$

Then $F(\theta_1, \ldots, \theta_n)$ is a splitting field for f.

[Again, no smaller field works since $K[x]$ is a UFD.] ▨

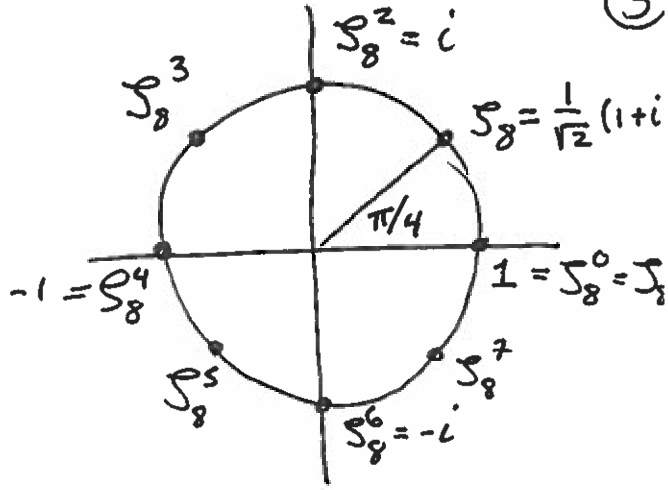
<u>Cor</u>: If K is a splitting field for $f(x) \in F[x]$ then

$$[K : F] \le (\deg f)!$$

For a random polynomial in $\mathbb{Z}[x]$, $[K : \mathbb{Q}] = (\deg f)!$ with prob $\longrightarrow 1$. [Next, here is an example with opposite behavior]

<u>Ex</u>: $x^n - 1$ in $\mathbb{Q}[x]$ has splitting field $\mathbb{Q}(\zeta_n) \subseteq \mathbb{C}$ where $\zeta_n = e^{2\pi i/n}$

Specifically,



$$1, \zeta_n, \zeta_n^2, \zeta_n^3, \dots, \zeta_n^{n-1}$$

are <u>distinct</u> roots of $X^n - 1$ and hence

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

Thus $\mathbb{Q}(\zeta_n)$ is the splitting field, and $[\mathbb{Q}(\zeta_n):\mathbb{Q}] \leq n-1$. ← will calculat later.

These <u>Cyclotomic Fields</u> are a central example in number theory. In 19th century, F.L.T. was "proved" using the (false) "fact" that $\mathbb{Z}[\zeta_n]$ is a UFD.

Actually, $\mathbb{Z}[\zeta_{23}]$ is <u>not</u> a UFD! Lead to introduction of ideals.

<u>Ex</u>: $R = \mathbb{Z}[\sqrt{-5}]$ $\qquad \overbrace{6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})}^{\text{all irreducibles}}$

<u>Goal</u>: Enlarge R to S which is a UFD.

<u>Not so crazy</u>: $\mathbb{Z}[\sqrt{-3}]$ is not a UFD, but $\mathbb{Z}[\rho = \frac{1}{2}(1+\sqrt{-3})]$ is.

Idea: Given $s \in S$, consider all multiples of s which are in R, i.e. $(s) \cap R$. Closed under $+$, mult by elts of R, that is, an ideal. Consider

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

$$(p_1 p_2)(p_3 p_4) \quad (p_1 p_3)(p_2 p_4)$$ ← Assuming simplist possibility

Then $(p_1) \cap R \supseteq (2, 1+\sqrt{-5})$. So define

$$\left.\begin{array}{ll} P_1 = (2, 1+\sqrt{-5}) & P_2 = (2, 1-\sqrt{-5}) \\ P_3 = (3, 1+\sqrt{-5}) & P_4 = (3, 1-\sqrt{-5}) \end{array}\right\}$$ Turns out, these are all prime ideals in $\mathbb{Z}[\sqrt{-5}]$

Also $(6) = P_1 P_2 P_3 P_4$ as ideals, and this factorization into prime ideals is unique. Same is true for e.g. ideals in $\mathbb{Z}[\zeta_n]$.