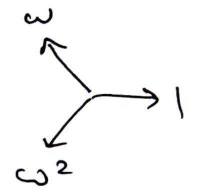
Def A splitting field of $f(x) \in F[x]$ is a field extension E/F in which f splits into a product of linear factors, while f does not split in any proper subfield of E

Example $x^2+1 \in \mathbb{Q}[x]$ splits in $\mathbb{C}$, but its splitting field is $\mathbb{Q}(i)$
$i = \sqrt{-1}$
$(x+i)(x-i)$

$x^3-1 \in \mathbb{Q}[x]$ splits in $\mathbb{C}$ $\quad x^3-1 = (x-1)(x^2+x+1) = (x-1)(x-e^{2\pi i/3})(x+e^{2\pi i/3})$
$\omega = e^{2\pi i/3}$
$= (x-1)(x-\omega)(x-\omega^2)$.



splitting field $\mathbb{Q}(\omega)$

$[\mathbb{Q}(\omega):\mathbb{Q}]=2 \qquad \operatorname{irr}(\omega,\mathbb{Q}) = x^2+x+1$

$1+\omega+\omega^2=0$

Splitting field is a <u>smallest</u> field in which $f(x)$ splits.

Thm Any $f(x) \in F[x]$ has a splitting field

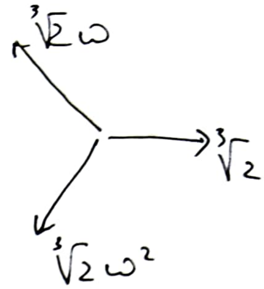
Already proved. Build extension $F \subset E'$ in which f factors $f = c(x-\alpha_1)\dots(x-\alpha_n)$. Now set $E \subset E'$, $E = F(\alpha_1, \dots \alpha_n)$
subfield generated by $\alpha_1 \dots \alpha_n$.

Def An extension $F \subset E$ is <u>simple</u> if $\exists \alpha \in E$, $E = F(\alpha)$

Most finite extensions we will encounter are simple.

$f = x^3 - 2$ irreducible/$\mathbb{Q}$ (Eisenstein criterion).

Splits in $\mathbb{C}$



Splitting field $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) =$

$= \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega) =$

$= \mathbb{Q}(\sqrt[3]{2}, \omega).$

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega) = E$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ since $\deg f = 3$, f irreducible/$\mathbb{Q}$.

$\omega \notin \mathbb{Q}(\sqrt[3]{2})$, since $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, $\omega \notin \mathbb{R}$.

$\Rightarrow$ $x^2 + x + 1$ does not factor in $\mathbb{Q}(\sqrt[3]{2})$ $\Rightarrow$

$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$

$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$

<u>basis:</u> $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$
$1 \quad \alpha \quad \alpha^2$ $\qquad \alpha = \sqrt[3]{2}$

$E/\mathbb{Q}(\sqrt[3]{2})$ has basis $\{1, \omega\}$

$\Rightarrow$ $E/\mathbb{Q}$ has basis - product basis $1, \sqrt[3]{2}, \sqrt[3]{4}$
$\omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega$

$\dim_{\mathbb{Q}} E = 6$

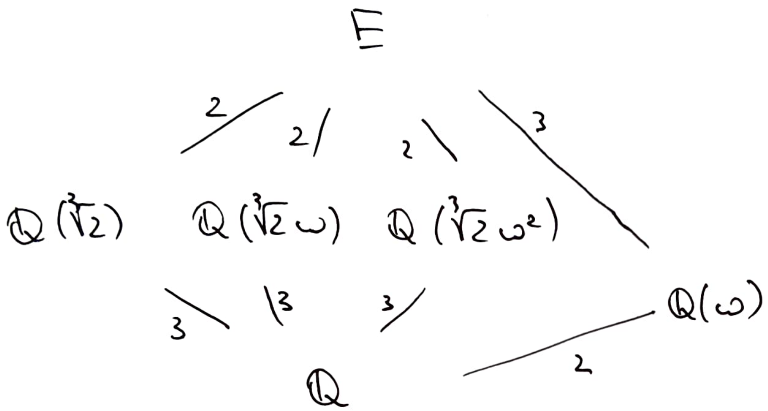
what other subfields does E have? Can choose any root of $x^3 - 2$ to generate an extension of $\mathbb{Q}$ of degree 3.

$(x^2 + x + 1) = (x - \omega)(x - \omega^2)$

x^3-2 has roots $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$. Get 3 subfields, each of dim 3 over $\mathbb{Q}$

$\mathbb{Q}(\sqrt[3]{2}),\ \mathbb{Q}(\sqrt[3]{2}\omega),\ \mathbb{Q}(\sqrt[3]{2}\omega^2)$

exercise: show these two are different subfields.



E is the splitting field of x^3-2

$E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$.

these 3 fields are isomorphic!

$$\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}(\sqrt[3]{2}\omega) \simeq \mathbb{Q}(\sqrt[3]{2}\omega^2) \simeq \mathbb{Q}[x]/(x^3-2)$$ irreducible$/\mathbb{Q}$, add some root.

$$x^3-2 = (x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$$

irreducible in $\mathbb{Q}(\sqrt[3]{2})$. Add its roots, get E.

$$x^3-2 = (x-\sqrt[3]{2}\omega)(x^2+\sqrt[3]{2}\omega x+\sqrt[3]{4}\omega^2 x)$$

coeff. in $\mathbb{Q}(\sqrt[3]{2}\omega)$, irreducible in that field. Add roots, get E.

x^2+x+1 irr. in $\mathbb{Q}$. Add roots, get $\mathbb{Q}(\omega)$. x^3-2 still irreducible $/\mathbb{Q}(\omega)$. Add one root $\to$ get E, two other roots are in the same extension already.

Later we will see these are the only subfields of E. Any other $\beta \in E$, $\beta \notin$ in any of these 4 subfields $\Rightarrow \{1, \beta, \beta^2, \beta^3, \beta^4, \beta^5\}$ is a basis $E/\mathbb{Q}$, $\operatorname{irr}(\beta, \mathbb{Q})$ has degree $\underline{6}$. For instance $\beta = \omega + \sqrt[3]{2}$. Extension is simple.

$$\begin{tikzcd} E \arrow[d, dash] & E \arrow[d, dash] \\ \mathbb{Q}(\sqrt[3]{2}) \arrow[r, "\sigma"] \arrow[d, dash] & \mathbb{Q}(\sqrt[3]{2}\omega) \arrow[d, dash] \\ \mathbb{Q} \arrow[r, phantom, "="] & \mathbb{Q} \end{tikzcd}$$

σ is an isomorphism of fields

σ is identity on $\mathbb{Q}$ $\qquad \sigma(a)=a \ \forall a \in \mathbb{Q}$

$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega$

take root of x^3-2 in $\mathbb{Q}(\sqrt[3]{2})$ to root of x^3-2 in $\mathbb{Q}(\sqrt[3]{2}\omega)$

$$\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}[x]/(x^3-2) \simeq \mathbb{Q}(\sqrt[3]{2}\omega)$$

isomorphism $\qquad$ isomorphism

$\sqrt[3]{2} \longleftrightarrow x \qquad x \longleftrightarrow \sqrt[3]{2}\omega$

composite isomorphism

$$\sqrt[3]{2} \longrightarrow \sqrt[3]{2}\omega$$

$$a+b\sqrt[3]{2}+c\sqrt[3]{4} \longmapsto a+b\sqrt[3]{2}\omega+c\sqrt[3]{4}\omega^2$$

$$(1, \alpha, \alpha^2) \longmapsto (1, \beta, \beta^2)$$

α root of x^3-2 $\qquad$ β root of x^3-2

$\alpha=\sqrt[3]{2}$ $\qquad$ $\beta=\sqrt[3]{2}\omega$

x^2+x+1 is irreducible $/\mathbb{Q}(\sqrt[3]{2})$ and irreducible $/\mathbb{Q}(\sqrt[3]{2}\omega)$.

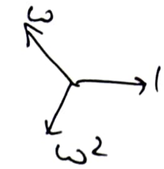
Can extend isomorphism σ by sending a root of x^2+x+1 in $\underbrace{\mathbb{Q}(\sqrt[3]{2})}_{\text{extension } E \text{ of}}$ to a root in $\underbrace{\mathbb{Q}(\sqrt[3]{2}\omega)}_{\text{extension } E \text{ of}}$.

$$\begin{tikzcd} E \arrow[r, dashed, "\tilde{\sigma}"] & E \\ \mathbb{Q}(\sqrt[3]{2}) \arrow[u, dash] \arrow[r, "\sigma"] & \mathbb{Q}(\sqrt[3]{2}\omega) \arrow[u, dash] \\ \mathbb{Q} \arrow[u, dash] \arrow[r, phantom, "="] & \mathbb{Q} \arrow[u, dash] \end{tikzcd}$$

$\tilde{\sigma}$ extends σ

$\tilde{\sigma}(\omega) = \omega$ or $\tilde{\sigma}(\omega) = \omega^2$

$x^2+x+1 = (x-\omega)(x-\omega^2)$



2 extensions, equal to deg of x^2+x+1,
equal to $[E : \mathbb{Q}(\sqrt[3]{2})] = 2$

$$\begin{tikzcd} E \arrow[r, dashed, "\tilde{\sigma}"] & E \\ \mathbb{Q}(\sqrt[3]{2}) \arrow[u, dash] \arrow[r, "\sigma"] & \mathbb{Q}(\sqrt[3]{2}) \text{ or } \mathbb{Q}(\sqrt[3]{2}\omega) \text{ or } \mathbb{Q}(\sqrt[3]{2}\omega^2) \arrow[u, dash] \\ \mathbb{Q} \arrow[u, dash] \arrow[r, phantom, "="] & \mathbb{Q} \arrow[u, dash] \end{tikzcd}$$

$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ (identity) or
$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ or
$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$.

the three σ's are different homomorphisms.
onto different subfields of

for each σ, $\exists$ two extensions to $\tilde{\sigma} : E \to E$
$\tilde{\sigma}$ is an isomorphism of E (automorphism of E).

$\Rightarrow$ we found 6 isomorphisms $E \to E$ (automorphisms of E).

<u>Important</u>! # of automorphisms = degree of extension $E/\mathbb{Q}$.

$$6 = 6$$

E is a <u>splitting field</u> (of x^3-2)

automorphisms are identity on the "base" field $\mathbb{Q}$
(field we start with).

This equality holds in most cases. Need to avoid cases
when irreducible polynomial f has multiple roots, in a larger field.

<u>Def</u> An irreducible $f(x) \in F[x]$ is called <u>separable</u> if $f(x)$ does not have repeated roots in any extension of F.

$Df(x) = f'(x)$ formal derivative

if $f'(x) \not\equiv 0$ (not the zero polynomial), $\deg f' < \deg f$

$\Rightarrow \gcd(f, f') = 1$ since f is irreducible

$\Rightarrow f$ has no repeated roots in any $E \supset F$, otherwise $x - \alpha \mid \gcd(f, f')$.

$\Rightarrow f(x)$ has a repeat root in some E/F if $Df = 0$.

$\Rightarrow \operatorname{char} F = p$ and f has the form

$$f = a_0 + a_1 x^p + a_2 x^{2p} + \dots + a_n x^{np}$$

all powers of x in f have exponent multiple of p.

& f must be irreducible in F.

<u>Remark</u> Not possible if F is finite. Then $\forall a \in F\ \exists b,\ b^p = a$ since Frobenius map is an isomorphism $\phi_p : F \xrightarrow{\sim} F$

$(b^p + c^p) = (b+c)^p$ if $a_0 = b_0^p$, $a_1 = b_1^p$

$$(a_0 + a_1 x^p) = b_0^p + b_1^p x^p = b_0^p + (b_1 x)^p = (b_0 + b_1 x)^p$$

$a_i = b_i^p$

$$a_0 + a_1 x^p + \dots + a_n x^{np} = b_0^p + b_1^p x^p + \dots + b_n^p x^{np} = b_0^p + (b_1 x)^p + \dots + (b_n x^n)^p =$$

$= (b_0 + b_1 x + \dots + b_n x^n)^p \Rightarrow f$ is not irreducible (factors in F)

$f \in F[x]$ not separable $\to$ very special situation, need $\operatorname{char} F = p$ and $\phi_p : F \to F$ not an isomorphism

char p field F is called <u>perfect</u> if $\forall a \in F\ \exists b\ b^p = a$.

$F(t)$ (formal variable) is not perfect

<u>Prop</u> A finite field is perfect.

$f \in F[x]$ is called <u>separable</u> if each irreducible factor of f is separable

$f = f_1(x) \ldots f_r(x)$ each f_i must be separable.

(Rotman Thm 51 page 56)

$\sigma : F[x] \to F'[x]$

<u>Thm</u> Let $\sigma : F \to F'$ be an isomorphism of fields.

$f(x) \in F[x]$ and $f^*(x) = \sigma(f(x)) \in F'[x]$ corr. polyn. $/F'$.

Let $E/_F$ a splitting field of f in F,

$E'/_{F'}$ a splitting field of f^* in F'.

$$\begin{tikzcd} E \arrow[r, dashed, "\tilde{\sigma}"] \arrow[d, dash] & E' \arrow[d, dash] \\ F \arrow[r, "\sigma"] & F' \end{tikzcd}$$

1) There is an isomorphism $\tilde{\sigma} : E \to E'$ extending σ

2) If $f(x)$ is separable, then σ has exactly $[E:F]$ extensions.

<u>Proof</u> 1) <u>Induction on</u> $[E:F]$.

Note for an intermediate field $F \subset B \subset E$, E is splitting field of f over B.

1) $[E:F]=1$ Nothing to prove $E = F, E' = F'$.

Otherwise choose irr. factor $p(x)$, $\deg p \geq 2$.

$f(x), p(x) \in F[x] \longrightarrow f^*(x), p^*(x) \in F'[x]$

$\beta \in E$ root of $p(x)$ in E replace coefficients using isomorphism σ.

$\beta' \in E'$ root of $p^*(x)$

$$\begin{array}{c} E \\ | \\ F[\beta] \leftarrow \text{intermediate field} \\ |\ m = \deg p(x) \\ F \end{array}$$

$[F[\beta]:F] = m = \deg p(x)$

$$\begin{tikzcd} E \arrow[d, dash] & E' \arrow[d, dash] \\ F[\beta] \arrow[r, "\hat{\sigma}"] \arrow[d, dash, "m"'] & F[\beta'] \arrow[d, dash, "m"'] \\ F \arrow[r, "\sigma"] & F' \end{tikzcd}$$

$m = \deg p^*(x) = \deg p(x)$.

fix β : m choices for β' if $p(x)$ (or $p^*(x)$) is <u>separable</u> (always so in char 0)

! m choices for $\hat{\sigma}$, one for each root β' of $p^*(x)$ in E'. # roots $= \deg p(x)$ if p is <u>separable</u>

Now
$$\begin{tikzcd} E \arrow[r, dashed, "\tau"] \arrow[d, dash] & E' \arrow[d, dash] \\ F[\beta] \arrow[r, "\hat{\sigma}"] & F'[\beta'] \end{tikzcd}$$

By induction, can extend $\hat{\sigma}$ to $\tilde{\sigma}$.

$[E : F[\beta]] < [E:F]$ use induction

If f is separable $\Rightarrow$ by induction, # of extensions is the degree $[E : F[\beta]]$

(separable case:)

$$\begin{tikzcd} E \arrow[r, dashed, "\tilde{\sigma}"] \arrow[d, dash, "k"'] & E' \arrow[d, dash] \\ F[\beta] \arrow[r, "\hat{\sigma}"] \arrow[d, dash, "m"'] & F'(\beta') \arrow[d, dash] \\ F \arrow[r, "\sigma"] & F' \end{tikzcd}$$

m choices for $\hat{\sigma}$, $m = \deg p(x)$.

If $[E : F[\beta]] = k$, k choices for $\tilde{\sigma}$ given $\hat{\sigma}$ (by induction)

$\Rightarrow$ km choices for $\tilde{\sigma}$.

$km = [E:F] = [E':F']$.

<u>Corollary</u> if $E \supset F$ is a splitting field of a separable polynomial f,

$[E:F] = \#$ of automorphisms of E/F

$$\begin{tikzcd} E \arrow[r, "\tilde{\sigma}"] \arrow[dr, dash] & E \arrow[d, dash] \\ & F \end{tikzcd}$$

$\tilde{\sigma}$ is identity on F $\quad \tilde{\sigma}(a) = a \ \forall a \in F$.

!! $\boxed{[E:F] = |\mathrm{Aut}(E/F)| \quad \text{if } E \text{ is splitting field of separable polynomial}}$

$\mathrm{Aut}(E/F)$ is called the Galois group of E over F

Denoted $\mathrm{Gal}(E/F) = \mathrm{Aut}(E/F)$.

$\mathbb{F}_p \subset F$ $\quad |F| = p^n$ some n $\quad |F| = q$ $\quad q = p^n$

F - vector space / $\mathbb{F}_p$ of dimension n

$F^* \simeq C_{p^n-1}$ - cyclic group of order $p^n - 1$

$\Rightarrow a^{p^n-1} = 1 \quad \forall a \in F^*$ $\qquad a \in F \Rightarrow a \in F^*$ or $a = 0$

$\Rightarrow a^{p^n} = a \quad \forall a \in F \quad \Leftrightarrow a^q = a$

Take splitting field of polynomial $f = x^q - x$

$f' = q x^{q-1} - 1 = p^n x^{q-1} - 1 = -1$ $\qquad f'$ is constant.

$\gcd(f, f') = 1 \Rightarrow f$ has no multiple roots in any extension of $\mathbb{F}_p$.

$\Rightarrow f$ has exactly q roots ($\deg f = q$) in the splitting field E.

$a \neq 0$ a^{-1} is a root.

If a, b are roots of $f \Rightarrow a+b$, ab are roots of f, $\quad a^q = a$, $b^q = b$

$\underline{(a+b)^q = a+b}$ $\qquad (a+b)^p = a^p + b^p \quad ((a+b)^p)^p = (a^p+b^p)^p = a^{p^2} + b^{p^2} \quad \ldots$

$\Longleftarrow$ $\qquad (a+b)^p{}^p = (a+b)^{p^2}$

$(ab)^q = a^q b^q = ab$.

$\Rightarrow$ roots of f constitute a subfield of $E \Rightarrow \{$roots of $f\} = E$

(extreme case, everything is very compact here)

This only works when we start with a finite field $\mathbb{F}_p$

<u>Prop</u> A field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.

<u>Corollary</u> Up to isomorphism, there is only one field with p^n elements, for any prime p and $n \geq 1$. $\qquad$ Notation: $\mathbb{F}_q = \mathbb{F}_{p^n}$