Def. A splitting field of \( f(x) \in F[x] \) is a field extension \( E/F \) in which \( f(x) \) splits into a product of linear factors, while \( f(x) \) 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 \( \mathbb{Q}(i) \)

\[ (x+i)(x-i) \]

\( x^3 - 1 \in \mathbb{Q}[x] \) splits in \( \mathbb{C} \)

\[ x^3 = (x-\omega)(x+\omega + \omega^2) = (x-e^{\frac{2\pi i}{3}})(x+e^{\frac{2\pi i}{3}}) \]

\[ \omega = e^{\frac{2\pi i}{3}} \]

\[ \omega^2 + \omega + 1 = 0 \]

Splitting field is \( \mathbb{Q}(\omega) \)

\[ [\mathbb{Q}(\omega) : \mathbb{Q}] = 2 \]

\[ m(\omega, \mathbb{Q}) = x^2 + x + 1 \]

Then any \( f(x) \in F[x] \) has a splitting field

Already proved. Build extension \( FCE \) in which \( f(x) \) factors

\[ f = c(x-a_1) \cdots (x-a_n) \]

Now set \( ECE' \), \( F = F(d_1, \ldots, d_n) \)

subfield generated by \( d_1, \ldots, d_n \).

Def. An extension \( FCE \) is simple if \( \exists x \in E \), \( E = F(x) \).

Most finite extensions we will encounter are simple.
$d = x^3 - 2$ irreducible (Eisenstein criterion).

Splitting 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.

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

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

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

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

Basis: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has basis \{1, $\sqrt[3]{2}$, $\sqrt[3]{4}$\}

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

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

$\sqrt[3]{2} \in \mathbb{Q} = 6$

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

$(x^3 - x + 1) = (x - \omega)(x - \omega^2)$
\( x^3 - 2 \) has roots \( \sqrt[3]{2}, \sqrt[3]{2} \omega, \sqrt[3]{2} \omega^2 \). Get 3 subfields, each of degree 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 are different subfields.

\[ E \]

\[ \begin{array}{ccc}
2 & / & 2 \\
\mathbb{Q}(\sqrt[3]{2}) & \mathbb{Q}(\sqrt[3]{2} \omega) & \mathbb{Q}(\sqrt[3]{2} \omega^2) \\
3 & / & 3 \\
\mathbb{Q} & & \mathbb{Q}(\omega) \\
\end{array} \]

Here 3 fields are isomorphic!

\[ \mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2} \omega) \cong \mathbb{Q}(\sqrt[3]{2} \omega^2) \cong \mathbb{Q}[x]/(x^3 - 2) \text{ irreducible over } \mathbb{Q}, \text{ contains } \text{ all } \sqrt[3]{2}. \]

\[ x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2} x + \sqrt[3]{4}) \text{ irreducible in } \mathbb{Q}(\sqrt[3]{2}). \text{ Add its roots, get } E. \]

\[ x^3 - 2 = (x - \sqrt[3]{2} \omega)(x^2 + \sqrt[3]{2} \omega x + \sqrt[3]{4} \omega^2 x) \text{ coeff. in } \mathbb{Q}(\sqrt[3]{2} \omega), \text{ irreducible in that field. Add roots, get } E. \]

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

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

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

$\phi$ is an isomorphism of fields

$\phi$ is identity on $\mathbb{Q}$

$\forall a \in \mathbb{Q}$

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

The roots of $x^3 - 2$ do not exist in $\mathbb{Q}(\sqrt[3]{2})$

in $\mathbb{Q}(\sqrt[3]{2})$

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

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

isomorphism

isomorphism

$\sqrt[3]{2} \mapsto x$

$x \mapsto \sqrt[3]{2} \omega$

composite isomorphism

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

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

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

The root of $x^3 - 2$

The root of $x^3 - 2$

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

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

Can extend isomorphism $\phi$ by sending a root of $x^3 + x + 1$ in $\mathbb{Q}(\sqrt[3]{2})$ extension $E$ of $\mathbb{Q}(\sqrt[3]{2})$.
\[ E \rightarrow \overline{E} \rightarrow E \]

\[ \overline{E} = \overline{E} \]

\[ \overline{Q}(\sqrt[3]{2}) \] maps to \( Q(\sqrt[3]{2}) \) or \( Q(\sqrt[3]{2} \omega) \) or \( Q(\sqrt[3]{2} \omega^2) \)

\[ b(\sqrt[3]{2}) = \sqrt[3]{2} \text{ (identity)}, \quad \omega \quad b(\sqrt[3]{2}) = \sqrt[3]{2} \omega \text{ or} \]

\[ b(\sqrt[3]{2}) = \sqrt[3]{2} \omega^2. \]

The three \( b \)'s are different homomorphisms onto different subfields of \( E \).

For each \( b \), \( E \) has extensions to \( \overline{E} : E \rightarrow E \).

\( \overline{E} \) is an isomorphism of \( E \) (automorphism of \( E \)).

\( \implies \) We found \( 3 \) isomorphisms \( E \rightarrow E \) (automorphism of \( E \)).

**Important!** \# of automorphisms = degree of extension \( E/\mathbb{Q} \).

\[ 6 \]

\( E \) is a splitting field (of \( x^3 - 2 \)).

The 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.
Def. An irreducible $f(x) \in \mathbb{F}[x]$ is called separable if $f(x)$ does not have repeated roots in any extension of $\mathbb{F}$.

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

If $f'(x) \neq 0$ (not the zero polynomial), then $\deg f' < \deg f$

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

$\Rightarrow \mathbb{F}$ has no repeated roots in any $\mathbb{E} \in \mathbb{F}$, otherwise $x - a \mid \gcd(f, f')$.

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

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

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

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

$\Rightarrow f$ must be irreducible in $\mathbb{F}$.

Remark. Not possible if $\mathbb{F}$ is finite. Then $\forall a \in \mathbb{F}$, $b^p = a$ since Frobenius map is an isomorphism $b : \mathbb{F} \rightarrow \mathbb{F}$

$$(b^p + c^p) = (b + c)^p$$

If $a_0 = b_0^p$, $a_1 = b_1^p$

$$(a_0 + a_1 x^p) = b_0^p + b_1^p x^p = b_0^p + \left(b_1 x)^p = (b_0 + b_1 x)^p.$$
$f \in F[x]$ is called \underline{separable} if each irreducible factor of $f$ is separable.

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

(Fromman, Thm 5.1 page 56)

Let $\delta : F \rightarrow F'$ be an isomorphism of fields.

$f(x) \in F[x]$ and $f^\delta(x) = \delta(f(x)) \in F'[x]$ on poly. $F'$.

Let $E/f$ a splitting field of $f$ in $F$, $E'/f'$ a splitting field of $f^\delta$ in $F'$.

1) There is an isomorphism $\delta : E \rightarrow E'$ extending $\delta$.

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

\underline{Proof:}

1) \underline{Induction on $[E : F]$.}

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

1) $[E : F] = 1$ No more do prove $E = F, E' = F'$.

Consider algebraic factor $p(x)$, deg $p \geq 2$.

$f(x), p(x) \in F[x] \rightarrow f^\delta(x), p^\delta(x) \in F'[x]$

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

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

$\left\{ \begin{array}{c}
\forall \beta \in E, \exists \beta' \in E' \text{ root of } p^\delta(x) \\
\forall \alpha \in B, \exists \alpha' \in B' \end{array} \right.$

$m = \text{deg } p(x) \rightarrow m = \text{deg } p^\delta(x) \rightarrow m = \text{deg } p(x)$.

$m_1 = \text{deg } p^\delta(x) \rightarrow m_1 = \text{deg } p(x)$.

$m = \text{deg } p(x)$ is \underline{separable}.

1 m choices for $\beta$, m choices for each root $\beta'$ of $p^\delta(x)$ in $E'$.

$\delta : F \rightarrow F'$ is \underline{separable}.
Now \( E \rightarrow E' \)
\[
F(\beta) \overset{\sigma}{\rightarrow} F'(\beta')
\]
By induction, can extend \( \sigma \) to \( \sigma' \).
If \( \sigma \) is separable \( \Rightarrow \)

\[
[E:F(\beta)] < [E:F] \text{ use induction.}
\]
by induction, \# of extensions is the degree \( [E:F(\beta)] \)

\[
E \overset{\sigma}{\rightarrow} E'
\]
\[
\begin{align*}
F(\beta) & \overset{\sigma}{\rightarrow} F'(\beta') \\
m & \overset{\sigma}{\rightarrow} m
\end{align*}
\]

Galliany: if \( E \supseteq F \) is a splitting field of a separable polynomial \( p \),
\[
[E:F] = \# \text{ of automorphisms of } E/F
\]

\[
E \overset{\sigma}{\rightarrow} E
\]
\[
\sigma \text{ is identity on } F \quad \sigma(a) = a \quad \forall a \in F.
\]

\[
\begin{array}{c|c|c}
[E:F] & \# \text{ Aut } (E/F) & \text{if } E \text{ is splitting field of separable polynomial} \\
\hline
1 & |\text{Aut } (E/F)| & \text{if } E \text{ is splitting field of separable polynomial}
\end{array}
\]

\[\text{Aut } (E/F) \text{ is called the Galois group of } E \supseteq F\]

\[\text{Denoted } \text{Gal } (E/F) = \text{Aut } (E/F)\].
$\mathbb{F}_p \subset \mathbb{F}$  $|\mathbb{F}| = p^n$ some $n$  $|\mathbb{F}| = q \Rightarrow q = p^n$

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

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

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

$\Rightarrow a^q = a \ \forall a \in \mathbb{F} \Rightarrow a^q = a$

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

$f' = qx^{q-1} - 1 = p^nx^{q-1} - 1 = -1$  $\Rightarrow f'$ is constant.

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

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

If $a, b$ are roots of $f$  $\Rightarrow ab$ is a root.

$a^q = a  \Rightarrow a^{q-1} = 1$  $\Rightarrow a$ is a root of $f'$.

$\Rightarrow a^p = a^q = a$  $\Rightarrow ab$ is a root of $f'$.

$ab^{p} = (ab)^p = (a^p)(b^p) = (a^q)(b^p) = a^p b^p$

$\Rightarrow ab^p = a^p b = ab$

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

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

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

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