Cor An algebraically closed field F has no proper algebraic extension E

Thm Every field F has a unique algebraic closure.

Thm (Fundamental thm. of Alg)
$\mathbb{C}$ is algebraically closed.

Splitting Fields — over what extension field may we factor $p(x) \in F[x]$ into linear factors?

Let F be a field, $p(x) \in F[x]$ non-constant, $\deg(p) = n$

An extension field E of F is a splitting field of $p(x)$ if $\exists\ \alpha_1, \dots, \alpha_n \in E$ s.t. $E = F(\alpha_1, \dots, \alpha_n)$ and

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

$p(x) \in F[x]$ splits in E if it is a product of lin. factors in $E[x]$.

Ex
$$p(x) = x^4 + 2x^2 - 8 \in \mathbb{Q}[x]$$
$$= (x^2 - 2)(x^2 + 4)$$

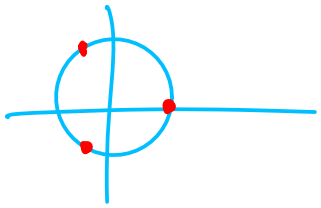
splitting field of $p(x) = \mathbb{Q}(\sqrt{2}, i)$

[Ex] $p(x) = x^3 - 3 \in \mathbb{Q}[x]$

$p(x)$ has a root in $\mathbb{Q}(3^{\frac{1}{3}})$ but this <u>not</u> the splitting field of $p(x)$

$$p(x) = (x - 3^{\frac{1}{3}})(x - 3^{\frac{1}{3}}\rho)(x - 3^{\frac{1}{3}}\rho^2)$$

$$\rho = \frac{-1 + \sqrt{3}i}{3}$$



$\therefore$ splitting field is $\mathbb{Q}(\rho, 3^{\frac{1}{3}})$

Thm Let $p(x) \in F[x]$ be non-constant.
$\exists$ a splitting field E for $p(x)$.

Proof: (sketch)
Induction on $\deg(p(x))$ ← may assume $p(x)$ is irr.

- work for degree 1
- can assume (by induction) that $\exists$ a splitting field for deg $= n-1$ poly.

$\exists$ an extension field K with 1 zero of $p(x)$, say $\alpha \in K$

$$p(x) = (x - \alpha)\, q(x) \qquad \deg(q) = n-1$$

$\therefore$ $p(x)$ splits by induction

∎

Q: Are splitting fields unique?

A: Yes, upto isomorphism, that is given two splitting fields K, L of $p(x) \in F[x]$

$\exists$ a field iso. $\phi: K \xrightarrow{\sim} L$ that preserves F (identity on F)

Lemma 21.32. *Let $\phi : E \to F$ be an isomorphism of fields. Let K be an extension field of E and $\alpha \in K$ be algebraic over E with minimal polynomial $p(x)$. Suppose that L is an extension field of F such that β is root of the polynomial in $F[x]$ obtained from $p(x)$ under the image of ϕ. Then ϕ extends to a unique isomorphism $\bar{\phi} : E(\alpha) \to F(\beta)$ such that $\bar{\phi}(\alpha) = \beta$ and $\bar{\phi}$ agrees with ϕ on E.*

Proof Sketch

- $\phi : E \xrightarrow{\sim} F$

  this gives an isomorphism

  $\phi : E[x] \xrightarrow{\sim} F[x]$

  $a_0 + a_1 x + \cdots a_n x^n \longmapsto \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$

  induce an isc. $E(\alpha) \to F(\beta)$

  $\phi(p(x)) = q(x)$ (minimal poly of β; $p(x)$ minimal)

$$\begin{array}{ccc} E[x]/\langle p(x)\rangle & \xrightarrow[\sim]{\psi} & F[x]/\langle q(x)\rangle \\ \sigma \downarrow \uparrow s & & s \downarrow \uparrow \tau \\ E(\alpha) & \xrightarrow[\sim]{\bar{\phi}} & F(\beta) \\ \downarrow & & \downarrow \\ E & \xrightarrow[\sim]{\phi} & F \end{array}$$

$\phi(\langle p(x)\rangle) = \langle q(x)\rangle$

$a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1} \longmapsto \phi(a_0) + \cdots \phi(a_{n-1})\beta^{n-1}$

Thm $\phi: E \to F$ is an isomorphism of fields $p(x) \in E[x]$ (non-constant), $q(x) = \phi(p(x))$. If K is a splitting field of $p(x)$ and L is a splitting field of $q(x)$ then ϕ extend to an isomorphism $\Psi: K \to L$.

Cor. Let $p(x) \in F[x]$ Then there exists a unique splitting field K of $p(x)$ which is unique up to isomorphism.

$x^2 - 4 = (x+2)(x-2) \Rightarrow$ Splitting field is $\mathbb{Q}$

$x^2 + 4 \Rightarrow$ Splitting field is $\mathbb{Q}(i)$

$x^2 + 2 \Rightarrow$ Splitting field is $\mathbb{Q}(i, \sqrt{2})$

Structure of a finite Field

Prop If F is a finite field $\Rightarrow$ $\text{Char}(F) = p$, p prime

- $\mathbb{Z}/p\mathbb{Z}$ is one such field, are there others?

what about $|F| = n$, $p \mid n$?

Standing Assumption p = a prime in $\mathbb{N}$

Prop If F is a finite field, then $\text{Char}(F) = p$ and $|F| = p^n$ for some $n \in \mathbb{N}$.