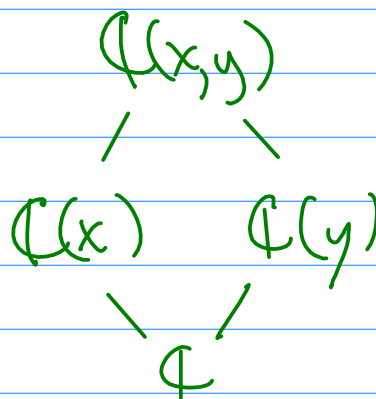


Extension Fields

Def: An extension field E of a field F is a field E which contains F .



We all know the Fundamental Theorem of Algebra

that a ^{nonconstant} polynomial $f(x) \in \mathbb{R}[x]$ has at least one (and hence $n = \deg(f)$ many) root in \mathbb{C} .

Quest: What about other fields?

Ex: $F = \mathbb{Z}_2$, $f(x) = x^2 + x + 1$

$$f(0) = 1 \text{ and } f(1) = 1 \text{ so no roots}$$

Maybe it has roots over some larger field (extension field)?

Theorem: Let F be a field and $f(x) \in F[x]$ be a polynomial which is not constant. Then there exists an extension field E and $\alpha \in E$ with $f(\alpha) = 0$.

Ex: $x^2 + x + 1 \in \mathbb{F}_2[x]$ has a root in \mathbb{F}_4 .

Ex: $x^2 + x + 1 \in \mathbb{Q}[x]$ has a root in \mathbb{C} .

Basic idea: Choose $p(x)$ irreducible in $F[x]$ with $p(x) \mid f(x)$. Then $\langle p(x) \rangle = I$ is a maximal ideal so $(n = \deg p)$

$$\begin{aligned} E &= F[x]/I \\ &= \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} + I \mid a_0, \dots, a_{n-1} \in F\} \\ &= \text{span}_F \{1, x, x^2, \dots, x^{n-1}\} \text{ is a field!} \end{aligned}$$

Obviously $x + I \in E$ satisfies $f(x + I) = 0 + I$.

Algebraic and Transcendental Elements

Def: An element $\alpha \in E \supseteq F$ is algebraic over F if \exists nonzero polynomial $f(x) \in F[x]$ with $f(\alpha) = 0$. An element which is not algebraic is called transcendental.

Special case: $\alpha \in \mathbb{C}$ which is algebraic / \mathbb{Q} is called an algebraic number.

Ex: $\sqrt{2}$, $\sqrt{2} + \sqrt{3}$, i are algebraic #'s

Ex: π , e are not algebraic numbers

Open problem: are $\pi+e$, $\pi-e$, or πe algebraic?

Let E be an extension field of F and $\alpha \in E$.

If α is algebraic, $\exists f(x) \in F[x]$ with $f(\alpha) = 0$.
Let

$I = \{ f(x) \in F[x] \mid f(\alpha) = 0 \}$ ← maximal ideal!
by Euclidean algorithm, $I = \langle p(x) \rangle$.

Def: If α is algebraic, we define the minimal polynomial of α to be the unique polynomial $p(x) \in F[x]$ satisfying

- $p(x)$ is monic
- $p(\alpha) = 0$
- If $q(x) \in F[x]$ satisfies $q(\alpha) = 0$, then $p(x) \mid q(x)$

Notation: $\text{irr}(\alpha, F)$

Ex: $\text{irr}(2, \mathbb{Q}) = x - 2$

$\text{irr}(i, \mathbb{Q}) = x^2 + 1$

$\text{irr}(\sqrt{2} + \sqrt{3}, \mathbb{Q}) = (x^2 - 5)^2 - 24$

Theorem: If $\alpha \in E$ is algebraic, then

$$F[\alpha] = \text{img}(\phi_\alpha) = \{ f(\alpha) \mid f(x) \in F[x] \}$$

is a field.

Proof: $I = \ker(\phi_\alpha) = \langle \text{irr}(\alpha, F) \rangle$ so the evaluation

morphism descends to the quotient to an isomorphism

$$\begin{array}{ccc} F[x] & \longrightarrow & F[\alpha] \\ \downarrow \phi & & \nearrow \\ F[x]/I & & \cong \end{array}$$

Thus $F[\alpha] \cong F[x]/I$ and since I is maximal, $F[\alpha]$ is a field.

□

Def: The subextension field $F(\alpha)$ by $\alpha \in E$ is the smallest subfield of E containing F and α .

Theorem:



