Section 29 - Extension fields

Def If E, F are fields with F a subfield of E, say E is extension field of F

Examples: $\mathbb{C}$ is extension field of $\mathbb{R}$.
$\mathbb{R}$ —— " —— $\mathbb{Q}$

Thm (Kronecker): Let F be a field, $f(x) \in F[x]$ non constant. Then there exists an extension field E of F s.t. $f(x)$ has a zero in E, i.e. an $\alpha \in E$ s.t $f(\alpha)=0$.

Proof Write

$$f(x) = p(x) q_1(x) \cdots q_m(x)$$

where $p(x)$ & $q_i(x)$ are irreducible.
Enough to find E, α s.t. $p(\alpha)=0$, since $p(\alpha)=0 \Rightarrow f(\alpha)=0$.

$p(x)$ irreducible $\Rightarrow \langle p(x) \rangle \subset F[x]$ maximal ideal

$$\Rightarrow E = F[x]/\langle p(x) \rangle \text{ is a field.}$$

Remains to show: (1) E is extension field of F
(2) $p(x)$ has a zero $\alpha \in E$

(1): $\exists$ homomorphisms $\iota : F \to F[x]$, $\iota(a) = a$ (constant polynomial)

$\gamma : F[x] \to F[x]/\langle p(x) \rangle = E$, $\gamma(g(x)) = g(x) + \langle p(x) \rangle$

Def Let $\psi = \gamma \circ \iota : F \to E$

$$\psi(a) = a + \langle p(x) \rangle$$

$\ker \psi \subset F$ is an ideal $\Rightarrow \ker \psi = \begin{cases} \{0\} \text{ or} \\ F \end{cases}$.

$\psi(1) = 1 + \langle p(x) \rangle \neq 0 + \langle p(x) \rangle$
$\Rightarrow \ker \psi \neq F$, so $\ker \psi = 0$.

Hence ψ injective, $F \simeq \psi[F] \leq E$.

(2) Let $\alpha = x + \langle p(x)\rangle$. Then, if $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, have

$$p(\alpha) = a_n\alpha^n + \cdots + a_0 = a_n(x+\langle p(x)\rangle)^n + a_{n-1}(x+\langle p(x)\rangle)^{n-1} + \cdots + a_0$$

$$= (a_n x^n + \langle p(x)\rangle) + (a_{n-1}x^{n-1} + \langle p(x)\rangle) + \cdots + (a_0 + \langle p(x)\rangle)$$

$$= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) + \langle p(x)\rangle = p(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle = 0.$$

□

Example • $f(x) = x^2+1 \in \mathbb{R}[x]$. x^2+1 irreducible over $\mathbb{R}$, get a field extension

$$\mathbb{R} \leq E = \mathbb{R}[x]/\langle x^2+1\rangle, \qquad \alpha = x + \langle x^2+1\rangle \in E$$

$$\& \; f(\alpha) = 0.$$

We'll see $E \simeq \mathbb{C}$.

• $f(x) = x^2-2 \in \mathbb{Q}[x]$. Get a field extension

$$\mathbb{Q} \leq E = \mathbb{Q}[x]/\langle x^2-2\rangle \qquad \alpha = x + \langle x^2-2\rangle \in E$$

$$f(\alpha) = 0.$$

We'll see $E \simeq \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \leq \mathbb{C}$.

• $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$, $f(0) = f(1) = 1 \Rightarrow f(x)$ irreducible

$$\rightsquigarrow \quad \mathbb{Z}_2 \leq E = \mathbb{Z}_2[x]/\langle x^2+x+1\rangle, \qquad \& \; \alpha = x + \langle x^2+x+1\rangle$$

$$f(\alpha) = 0$$

Algebraic & transcendental elements

Let $F \leq E$ be a field extension. An $\alpha \in E$ is *algebraic over F* if there is a $0 \neq f(x) \in F[x]$ s.t. $f(\alpha) = 0$. Otherwise α is *transcendental over F*.

Examples: If $\alpha \in F$, then α is algebraic over F, take $f(x) = x - \alpha$.

• $\sqrt{2} \in \mathbb{R} \geq \mathbb{Q}$ is algebraic over $\mathbb{Q}$ $\quad (f(x) = x^2 - 2)$

$i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ $\quad (f(x) = x^2 + 1)$

$e, \pi \in \mathbb{R}$ are transcendental over $\mathbb{Q}$.

Def An element $\alpha \in \mathbb{C}$ algebraic over $\mathbb{Q}$ is an *algebraic number*

— " — transcendental — " — *transcendental number*

The irreducible polynomial for α

Thm Let $F \leq E$ be field extension. Let $\alpha \in E$ be algebraic over F.

There is an irreducible $p(x) \in F[x]$ s.t. $p(\alpha) = 0$.

- $p(x)$ is unique up to multiplying by element of F
- $p(x)$ has minimal degree among all $0 \neq f(x)$ s.t $f(\alpha) = 0$
- If $f(x) \in F[x]$ is s.t. $f(\alpha) = 0$, then $p(x)$ divides $f(x)$.

Example: $\mathbb{Q} \leq \mathbb{R}$, $\sqrt[3]{2} \in \mathbb{R}$. Take $p(x) = x^3 - 2$.

Unique up to rescaling: Could take $2(x^3-2)$, $\frac{3}{5}(x^3-2)$, ...

Minimal degree: $f(x) \in \mathbb{Q}[x]$, if $f(\sqrt[3]{2}) = 0$ then $\deg f \geq 3$, and x^3-2 divides $f(x)$.

Proof: Evaluation homomorphism $\phi_\alpha : F[x] \longrightarrow E$

$$\phi_\alpha(f(x)) = f(\alpha).$$

$f(\alpha) = 0 \iff \phi_\alpha(f(x)) = 0 \iff f(x) \in \ker \phi_\alpha$.

$\ker \phi_\alpha$ is an ideal in $F[x]$

Ideals in $F[x]$ are principal, so $\ker \phi_\alpha = \langle p(x) \rangle$ for some $p(x) \in F[x]$.

$f(\alpha) = 0 \iff f(x) \in \langle p(x) \rangle \iff f(x) = q(x)p(x) \Rightarrow$ $\deg f \geq \deg p$, $p(x)$ divides $f(x)$.

$p(x)$ is irreducible: If $p(x)$ reducible, then $p(x) = r(x)q(x)$, $\deg r, \deg q < \deg p$.

$$p(\alpha) = 0 \Rightarrow r(\alpha)q(\alpha) = 0 \Rightarrow r(x) \in \langle p(x) \rangle \text{ or } q(x) \in \langle p(x) \rangle.$$

But $r(x) \in \langle p(x) \rangle \Rightarrow \deg r \geq \deg p$, contradiction.

~~**Def** Let $E \geq F$, $\alpha \in F$ as above.~~

~~Given $p(x) = a_n x^n + \cdots + a_0$ ...~~

Def Let $F \leq E$ be field extension. The irreducible polynomial of α, written $\mathrm{irr}(\alpha, F)$, is the unique monic irreducible polynomial in $F[x]$ s.t. $f(x) = 0$.

Example. $\text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, since $x^2 - 2$ is monic, irreducible over $\mathbb{Q}$ & $(\sqrt{2})^2 - 2 = 0$.

- $\text{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$.

(Note that $x^2 - 2$ is reducible over $\mathbb{R}$).

- $\text{irr}(\sqrt{2} + \sqrt{3}, \mathbb{Q}) = ?$ Let $\alpha = \sqrt{2} + \sqrt{3}$.

$$\alpha^2 = 4 + 2\sqrt{6} + 9 = 13 + 2\sqrt{6}$$

$$\alpha^2 - 13 = 2\sqrt{6}$$

$$(\alpha^2 - 13)^2 = 4(6) = 24$$

$$\alpha^4 - 26\alpha^2 + 145 = 0$$

$x^4 - 26x^2 + 145$ is irreducible by the Eisenstein criterion for $p = 5$,

so $\text{irr}(\sqrt{2} + \sqrt{3}, \mathbb{Q}) = x^4 - 26x^2 + 145$.

The degree of α over F is $\deg(\alpha, F)$ = degree of $\text{irr}(\alpha, F)$.

Examples: $\deg(\sqrt{2}, \mathbb{Q}) = 2$, $\deg(\sqrt{2}, \mathbb{R}) = 1$, $\deg(\sqrt{2} + \sqrt{5}, \mathbb{Q}) = 4$.