Field Extensions (cont.)

Recall: F: field, $p(x) \in F[x]$ irred.

$K := F[x]/(p(x))$ is an ext. field of F

containing a root θ of p, and $[K:F] = n$.

Def: Let $F \subseteq K$, $\alpha, \beta, \ldots \in K$.

$F(\alpha, \beta, \ldots)$ is the smallest subfield of K

containing F and $\alpha, \beta, \ldots$

Equivalently, $F(\alpha, \beta, \ldots)$ = intersection of all subfields of K w/ this property

Simple ext'n: $E = F(\underset{\text{primitive elt.}}{\alpha})$

Examples:

a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \overset{\text{nontriv.}}{=} \mathbb{Q}(\overbrace{\sqrt{2} + \sqrt{3}}^{\alpha})$ is simple

$\sqrt{2} = \dfrac{\alpha^3 - 9\alpha}{2}$ $\qquad$ $\sqrt{3} = \alpha - \dfrac{\alpha^3 - 9\alpha}{2}$

b) $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots)$ is not simple

Thm: $p(x) \in F[x]$: irred.

Let K: ext'n field of F containing a root α of p.

Then, $F[x]/(p(x)) \cong F(\alpha) \subseteq K$

Pf: Consider the map given by $x + (p) \overset{\varphi}{\mapsto} \alpha$ i.e.

$g(x) + (p(x)) \mapsto g(\alpha)$.

- Well defined: $g(\alpha) = 0$ if $g \in (p)$
- Ring homom.: check the axioms
- Injective: $\ker \varphi$ is an ideal, which for a field is either (0) or $F[x]/(p)$. Not the latter since $1 \mapsto 1$

- Surjective: image is a field containing F and α

$\square$

Cor: Let $E = F(\alpha) \leq K$ w/ $[K:F] = n < \infty$. Then,

a) $\exists$ irred. $p(x) \in F[x]$ s.t. $p(\alpha) = 0$.

b) $\deg p = n$

c) $E \cong F[x]/(p)$

d) E is indep. of the choice of root of p

i.e. if $p(\beta) = 0$, $F(\alpha) \cong F(\beta)$.

Pf: Since $[K:F] = n$, $1, \alpha, \dots, \alpha^n$ are linearly dep. i.e.

$$a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0$$

Let $p(x)$ be an irred. factor of $a_n x^n + \cdots + a_1 x + a_0$

b) This follows from our first theorem today

c) Follows from previous theorem

d) Follows from c)

$\square$

On the other hand, if $[F(\alpha):F] = \infty$, then

$$F(\alpha) \cong F[x] \qquad \text{e.g. } F = \mathbb{Q},$$

$$\frac{p(\alpha)}{q(\alpha)} \longmapsto \frac{p(x)}{q(x)} \qquad \alpha = \underbrace{\pi, e, \ln 2}_{\text{difficult!}}$$

Extension Theorem (skipping this for now!)

Let $\varphi : F \xrightarrow{\sim} F'$ be an isom. of fields.

Let $p(x) \in F[x]$ be irred., and let $p'(x) \in F'[x]$ be the irred. poly obtained by applying φ to the coeffs. of p.

Let α be a root of p (in some extn of F)

Let β be a root of p' (in some extn of F')

Then $\exists$ isom.

$$\sigma : F(\alpha) \xrightarrow{\sim} F'(\beta)$$
$$f \longmapsto \varphi(f) \qquad (\sigma|_F = \varphi)$$
$$\alpha \longmapsto \beta$$

Pf: Let $\tilde{\varphi}$ be the isom.

$$\tilde{\varphi} : F[x] \xrightarrow{\sim} F'[x]$$
$$f \mapsto \varphi(f)$$
$$x \mapsto x$$

Then $\tilde{\varphi}$ maps $(p(x))$ to $(p'(x))$, so it induces an isom

$$F[x]/(p(x)) \xrightarrow{\sim} F'[x]/(p'(x))$$
$$f \overset{\sim}{\longmapsto} \varphi(f) + (p')$$
$$x + (p) \overset{\sim}{\longmapsto} x + (p')$$

Combining this w/ our previous isoms., σ is the map

$$\begin{array}{ccccccc} F(\alpha) & \xrightarrow{\sim} & F[x]/(p(x)) & \xrightarrow{\sim} & F'[x]/(p'(x)) & \xrightarrow{\sim} & F'(\beta) \\ f & \longmapsto & f + (p) & \longmapsto & \varphi(f) + (p') & \longmapsto & \varphi(f) \\ \alpha & \longmapsto & x + (p) & \longmapsto & x + (p') & \longmapsto & \beta \end{array}$$

$\square$

$$\begin{tikzcd} \sigma : F(\alpha) \arrow[r, "\sim"] \arrow[d, dash] & F'(\beta) \arrow[d, dash] \\ \varphi : F \arrow[r, "\sim"] & F' \end{tikzcd}$$

Algebraic Extensions

Summing up,

Thm: $K := F(\alpha)$.

a) If $[K:F] < \infty$, $\exists\, p(x) \in F[x]$ irred.

s.t. $p(\alpha) = 0$ and $K \cong F[x]/(p(x))$

b) If $[K:F] = \infty$, then $K \cong F(x)$ and $\forall p(x) \in F[x]$,

$p(\alpha) \neq 0$.

Def:

In case a), we call α and K/F <u>algebraic</u>

In case b), we call α and K/F <u>transcendental</u>

Prop/def: If α is alg. / F, there exists a unique monic poly. $m_{\alpha,F}(x) \in F[x]$ of min'l degree s.t. $m_{\alpha,F}(x) = 0$. Furthermore, $\deg m_{\alpha,F} = [F(\alpha):F]$

and $\underset{p \in F[x]}{p(\alpha) = 0} \iff p \in (m_{\alpha,F}(x))$

Example: $F = \mathbb{Q}$ $\alpha = \sqrt{2}$

$m_{\alpha,F}(x) = x^2 - 2$

$p(\sqrt{2}) = 0 \iff x - \sqrt{2} \mid p(x)$ in $\mathbb{Q}(\sqrt{2})[x]$
$p \in \mathbb{Q}[x]$
$\iff x^2 - 2 \mid p(x)$ in $\mathbb{Q}[x]$

Pf: Let $I = \{p(x) \in F[x] \mid p(\alpha) = 0\}$. Since $F[x]$ is a PID, let $m_{\alpha,F}(x)$ be a (monic) generator for I. Since I is a prime ideal, p is irred. Now we have

$$F(\alpha) \cong F[x]/(m_{\alpha,F}(x)), \text{ so}$$

$$[F(\alpha) : F] = \deg m_{\alpha,F}.$$

□

Prop: If α alg. $/F$ and $F \subseteq L$, then α is alg. $/L$ and $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$ in $L[x]$.

Pf: $m_{\alpha,F}(x) \in F[x] \subseteq L[x]$, so α is alg. $/L$.

Since $m_{\alpha,F}(\alpha) = 0$, $m_{\alpha,F}$ must therefore be a multiple of $m_{\alpha,L}(x)$. $\square$

Def: K/F is algebraic if every $\alpha \in K$ is alg. $/F$.

Prop: If $[K:F] < \infty$, then K/F is alg.
"finite extn"

Pf: If $\alpha \in K$ is not alg., then $1, \alpha, \alpha^2, \ldots$ are linearly indep. $\square$

Converse doesn't hold

e.g. $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$

K is alg. $/\mathbb{Q}$, but $[K:\mathbb{Q}] = \infty$