Extensões de Corpos:

Def: Uma extensão de corpos E/F é uma inclusão de corpos $F \hookrightarrow E$.
O grau de extensão E/F é a dimensão de E como F-esp. vetorial e é denotado $[E:F]$ (eventualmente infinito).

Exemplos: 1. $\mathbb{C}/\mathbb{R}$ é uma extensão de corpos tq. $[\mathbb{C}:\mathbb{R}] = 2$.

2. $\mathbb{R}/\mathbb{Q}$ é uma extensão de corpos com $[\mathbb{R}:\mathbb{Q}]$ é infinito não contável.

3. $K \equiv$ corpo, $K(X)/K$ é uma extensão de grau infinito.

Prop. Se $L \supset E \supset F$ são extensões de corpos, então $[L:F] < \infty$ sse $[L:E] < \infty$ e $[E:F] < \infty$ e temos

$$[L:F] = [L:E][E:F]$$

Exemplo: Se $f \in K[X]$ é irredutível então $K \hookrightarrow E := K[X]/\langle f \rangle$ é uma extensão de corpos de grau

$$[E:K] = \deg f.$$

Exemplo: $\mathbb{C} = \mathbb{R}[X]/\langle X^2+1 \rangle$

Notação: Dada uma extensão de corpos E/K e $S \subset E$ denota-se por $K[S] \subset E$ o subanel de E gerado por S e K.

NB: $K[S]/K$ é extensão de anéis.

Recorde-se $K[S]/K$ é extensão integral entre

$$K \text{ corpo} \Rightarrow K[S] \text{ é corpo}$$

Em particular, se S é t.q. $K[S]$ tem dimensão finita (/K), então $K[S]$ é um corpo.

Exemplos: 1. $\mathbb{C} = \mathbb{R}[i]$ é um corpo

2. $\mathbb{Q}[\sqrt[n]{2}] \subset \mathbb{R}$ é um corpo

Notação: Se $S \subset E$ e E/k extensão então $k(S) \subset E$ denota o subcorpo gerado por k e S.

NB: Se $k[S]$ tem dimensão finita $/k$ então $k(S) = k[S]$.

Def: Se E/k é extensão de corpos, tq. $E = k(\alpha)$, para algum $\alpha \in E$, diz-se que a extensão E/k é simples.

Exemplo: $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$ logo $\mathbb{C}/\mathbb{R}$ é extensão simples.

Def: Seja E/K extensão de corpos e seja $\alpha \in E$. Se α é integral sobre K, diz-se que α é algébrico $/K$. Caso contrário, diz-se que α é transcendente $/K$.

Exemplos: 1. $i = \sqrt{-1} \in \mathbb{C}$ é algébrico $/\mathbb{R}$.

2. $\sqrt[n]{2} \in \mathbb{R}$ é algébrico $/\mathbb{Q}$

3. $\pi \in \mathbb{R}$ é transcendente $/\mathbb{Q}$.

NB: $\alpha \in E$ algébrico $/K \iff$

$$K(\alpha) = K[\alpha]$$

Def: Se E/K é extensão de corpos integral, diz-se que E/K é algébrica. Caso contrário, diz-se transcendente.

Exemplos: 1. $\mathbb{C}/\mathbb{R}$ é algébrica

2. $\mathbb{R}/\mathbb{Q}$ é transcendente.

NB: Se E/k é extensão de corpos tq. $[E:k] < \infty$, então E/k é algébrica.

Prop: E/k é extensão finita se é algébrica e é f.g. como k-álgebra.

Dem: exercício. ∎

Def: Um corpo Ω diz-se <u>algebricamente fechado</u> se $\forall f \in \Omega[X]$

$\exists \alpha_1, \ldots, \alpha_n \in \Omega$ e $\exists a \in \Omega$ tq.

$$f = a \prod_{i=1}^{n} (X - \alpha_i)$$

Exemplo: $\mathbb{C}$ é algebricamente fechado.

Def: Se Ω / K é extensão algébrica tq. Ω é algebricamente fechado, diz-se que Ω é um fecho algébrico de K.

Exemplo: $\mathbb{C}$ é um fecho algébrico de $\mathbb{R}$.

Prop: Se Ω / k é extensão algébrica e $\forall f \in k[X]$ f tem fatorização em polinómios de grau 1, então Ω é um fecho algébrico de k.

Dem: exercício. □

Notação: Se $f = a(X-\alpha_1)\cdots(X-\alpha_n)$ também se diz que f se decompõe em Ω.

Prop: Se E/k é extensão algébrica e R/k é subextensão de anéis, então R é um corpo.

Dem: $\alpha \in R \Rightarrow k[\alpha]$ é um

k-esp. vet. de dimensão finita
logo é corpo. $\therefore \alpha^{-1} \in R$.

□

Def: Se E/k e E'/k são extensões de corpos, um homomorfismo de extensões entre E/k e E'/k é um hom. de corpos $\varphi: E \to E'$ tq. $\varphi|_k = 1_k$.

Notação: $\hom_k(E, E')$ ou $\hom(E/k, E'/k)$

Se $E' = E$ e φ é iso., diz-se que φ é um automorfismo:

$\varphi \in \mathrm{Aut}(E/k)$

Exemplo: $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{1_{\mathbb{C}}, \sigma\}$

onde $\sigma : \mathbb{C} \to \mathbb{C}$; $z \mapsto \overline{z}$

Prop: Seja $k(\alpha)/k$ uma extensão simples e seja E/k outra extensão. Então

i. Se α é transcendente $/k$, $\exists$ bijeção

$$\hom(k(\alpha)/k, E/k) \longleftrightarrow \{\beta \in E \mid \beta \text{ transc. } /k\}$$
$$\varphi \longmapsto \varphi(\alpha)$$

ii. Se α é algébrico $/k$, com polinómio mínimo $f \in k[X]$, então $\exists$ bij.

$$\hom(k(\alpha)/k, E/k) \hookrightarrow \{\text{raízes de } f \text{ em } E\}$$

Dem i. $k(\alpha) \simeq k(X)$

ii. $k[\alpha] = k(\alpha) \simeq k[X]/\langle \varphi \rangle$ ☒

Exemplo: $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) \simeq \{\pm i\}$;

$\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{1_{\mathbb{C}}, \sigma\}$ t.q. $\sigma(z) = \bar{z}$.

Exemplo: $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \{1_{\mathbb{Q}(\sqrt{2})}, \sigma\}$

onde $\sigma(n + m\sqrt{2}) := n - m\sqrt{2}$.

Extensões de Decomposição:

Def: Seja E/K uma extensão e seja $f \in K[X]$ tq. f se decompõe em $E[X]$. Se $E = K[\alpha_1, \dots, \alpha_n]$, diz-se que E/K é uma extensão de decomposição de f.

Exemplos: 1. $\mathbb{C}/\mathbb{R}$ é extensão de decomposição $f = X^2+1 \in \mathbb{R}[X]$.

2. $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ é extensão de decomposição de $f = X^2-2 \in \mathbb{Q}[X]$.

Prop: Todo o polinómio $f \in K[X]$ tem uma extensão de decomposição E_f / K t.q.

$$[E_f : K] \leq (\deg f)!$$

Dem: Por indução em $\deg f$.

Seja $g \in K[X]$ um fator irredutível de f. Seja $E_1 := K[X]/\langle g \rangle$.

Temos

$$f = (X - \alpha_1) f_1 \text{ em } E_1[X]$$

Por hipótese de indução f_1 tem ext. de decomposição E_{f_1} / E_1 t.q.

$$[E_{f_1} : K] = [E_{f_1} : E_1][E_1 : K]$$
$$\leq (\deg f_1)! \deg g$$
$$\leq (\deg f - 1)! \deg f$$
$$= (\deg f)!$$

□

Exemplo: $f = X^p - 1/(X-1)$ ($p \in \mathbb{N}$ primo)

$f = X^{p-1} + X^{p-2} + \cdots + 1$. Seja $\omega \in \mathbb{C}$ raiz de f, então $\omega^2, \ldots, \omega^{p-1}$ são raízes de f, logo f decompõe-se em $\mathbb{Q}(\omega) \subset \mathbb{C}$.

$\therefore \mathbb{Q}(\omega)/\mathbb{Q}$ é extensão de decomposição de f em grau $= \deg f$.

(exercício: $f \in \mathbb{Q}[X]$ é irredutível
sugestão: Aplicar Eisenstein a $f(X+1)$)

Questão: Será a extensão de decomp. única a menos de isomorfismo?

Prop: Sejam $f \in k[X]$, E/k gerada por raízes de f e F/k outra extensão onde f se decompõe.

Então

(a) $\hom(E/k, F/k) \neq \emptyset$

(b) $|\hom(E/k, F/k)| \leq [E:k]$

com igualdade se f tem $\deg f$ raízes distintas.

Dem: Sejam $\alpha_1, \dots, \alpha_r \in E$ raízes de f t.q. $E = K[\alpha_1, \dots, \alpha_r]$. Seja $g_1 \in K[X]$ o polinómio mínimo de α_1 / K

Temos

$$1 \leq |\hom(K[\alpha_1]/K, F/K)| \leq \deg g_1$$

com igualdade à direita se as raízes de g_1 em F são todas distintas

...

(exercício)

□

Cor: Sejam E/k e F/k extensões t.q. $[E:k] < \infty$, então

(a) $|\hom(E/k, F/k)| \leq [E:k]$

(b) $\exists\ L/k$ t.q. $[L:k] < \infty$

e

$$|\hom(E/k, L/k)| \neq \emptyset$$

Dem: Seja $f \in k[X]$ t.q. E/k é gerada por raízes de f.

Seja L/F uma extensão de decomposição de $f \in k[X]$. Pela prop.

$$1 \leq \hom(E/k, L/k) \leq [E:k]$$

Como $\hom(E/k, F/k) \subset \hom(E/k, L/k)$ ∎

Cor: As extensões de decomp. são únicas a menos de iso.

Dem: Sejam E_1/k e E_2/k ext. de decomp. de $f \in k[X]$.

$\Rightarrow \exists \varphi \in \hom(E_1/k, E_2/k)$

φ é 1-1 pq é hom. de corpos.

Como E_1/k e E_2/k são gerados por raízes de f, φ é sobrejetiva. $\square$

Raízes Múltiplas:

Prop: Sejam $f, g \in K[X]$ e seja $E \supset K$.

Temos

$$\mathrm{mdc}_{K[X]}(f,g) = \mathrm{mdc}_{E[X]}(f,g).$$

Em particular, se f, g são entre si em $K[X]$ também o são em $E[X]$.

Dem: Denotemos os mdc's por r_K e r_E. Temos $r_K \mid r_E$ em $E[X]$.

Sejam $a, b \in K[X]$ tq.

$$r_K = af + bg,$$

logo $r_E \mid r_K$ em $E[X]$.

□

NB: Podemos escrever $r = \text{mdc}(f,g)$ indep. da extensão.

Cor: Se $p(x), q(x) \in K[x]$ são irredutíveis não associados, então $p(x)$ e $q(x)$ não têm raízes comuns em nenhuma extensão de K.

Def: Diz-se que $f \in K[x]$ tem raízes múltiplas se isso é verdade numa extensão de decomposição de f. Caso contrário, diz-se que f tem raízes simples.

NB: A indep. do dpo. de ext. de decomposição garante a def.

é indep. da extensão.

Exemplo: $K = \mathbb{F}_p(T)$, $f = X^p - T$ $\in K[X]$. Seja $E/_K$ uma extensão onde f tem uma raiz $\alpha \in E$. Então

$$f = X^p - T = X^p - \alpha^p = (X-\alpha)^p \in E[X]$$

$\therefore$ f tem raízes múltiplas.

Exercício: $f \in K[X]$ é irredutível.

Def: $f = \sum_i a_i X^i \in K[X]$

Define-se a derivada f' tq.

$$f' := \sum_i i a_i X^{i-1}$$

Prop: Seja $f \in k[X]$ tq. $\deg f > 0$ e f é irred. ASASE:

(a) f tem raiz múltipla;

(b) $\text{mdc}(f, f') \neq 1$

(c) $\text{char}(k) = p > 0$ e $\exists g \in k[X]$:

$$f(X) = g(X^p)$$

(d) todas as raízes de f são múltiplas.