Seja $\mathbb{K}$ uma extensão de corpos $\mathbb{L}$ & $S \subseteq \mathbb{K}$ um subconjunto $\neq$ vazio.

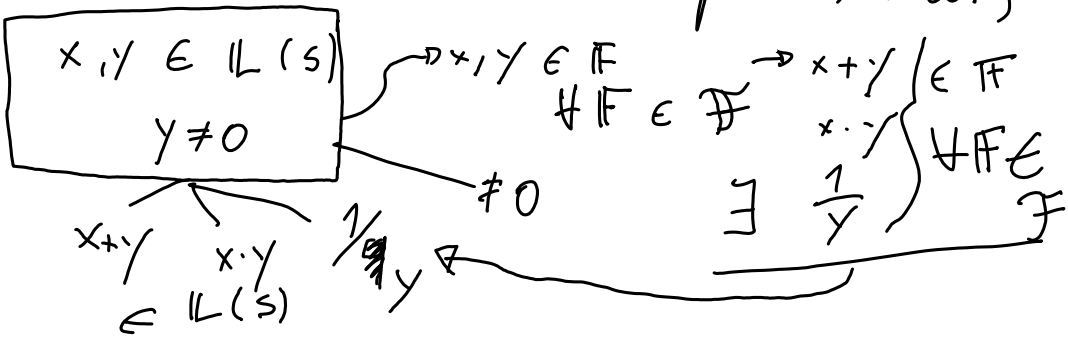
Considere a família

$$\mathcal{F} = \left\{ \mathbb{F} \;\middle|\; \begin{array}{l} i)\ \mathbb{F} \text{ é subcorpo de } \mathbb{K} \\ ii)\ \mathbb{L} \subseteq \mathbb{F} \\ iii)\ S \subset \mathbb{F} \end{array} \right\}$$

$$\mathbb{L}(S) := \bigcap_{\mathbb{F} \in \mathcal{F}} \mathbb{F}$$

AF: $\mathbb{L}(S)$ é um subcorpo de $\mathbb{K}$

(exercício – como em álgebra linear)



Caso $S = \{\alpha\}$ é unitário

Denotemos $\mathbb{L}(S)$ por $\mathbb{L}(\alpha)$

Distingue isto de $\mathbb{L}[\alpha] = \{w \in \mathbb{K} \mid w$ é c.l. de potências de $\alpha\}$

$= \mathrm{Im}(\psi_\alpha)$

Lema

Seja $\alpha \in \mathbb{K}$ & $\mathbb{K} \mid_{\mathbb{L}}$ extensão de corpo.

Então

(a) $\mathbb{L}(\alpha) = \mathbb{L}[\alpha] \iff \alpha$ é algébrico sobre $\mathbb{L}$

(b) $\mathbb{L}[\alpha] \subsetneq \mathbb{L}(\alpha)$

~~$\iff$~~ $\iff$

α é transcendente sobre $\mathbb{L}$

Neste caso $\mathbb{L}(\alpha) = \{x/y \mid x, y \in \mathbb{L}[\alpha]\ y \neq 0\}$

Prova

Vimos que se $\alpha \in \Lambda_{\mathbb{L}}(\mathbb{K}) = \{w \in \mathbb{K} \mid w \text{ é algébrica sobre } \mathbb{L}\}$

$\Rightarrow \ker(\psi_\alpha) = \chi_\alpha \mathbb{L}[x]$ & χ_A é irredutível & $\dfrac{\mathbb{L}[x]}{\ker(\psi_\alpha)} \cong \mathbb{K}[\alpha]$

é corpo, pois $\ker(\psi_\alpha)$ é ideal maximal.

Sempre $\mathbb{L}[\alpha] \subseteq \mathbb{L}(\alpha)$

b) $\ker(\psi_\alpha) = \{0\} \iff$

$\mathbb{L}[\alpha] \cong \mathbb{L}[x] \subsetneq \mathbb{L}(x) = \left\{ \dfrac{f(x)}{g(x)} \;\middle|\; f, g \in \mathbb{L}[x] \right\}$

Teorema (Steiner)

Seja $\mathbb{F}$ um corpo finito ou $\mathbb{F} = \mathbb{Q}$ & seja $\mathbb{K}$ uma extensão de $\mathbb{F}$ com $[\mathbb{K}:\mathbb{F}] = n \in \mathbb{N}$. Então $\exists \alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{L}(\alpha)$.

mas ainda $\partial(\chi_\alpha) = n$.

Uma extensão do tipo $\mathbb{L}(\alpha)$ é dita uma extensão simples & α é chamado elemento primitivo da extensão

Exemplo

$\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$\mathbb{L} = \mathbb{Q}$

$S = \{\sqrt{2}, \sqrt{3}\}$

$\mathbb{K} = \mathbb{L}(S)$

$[\mathbb{K} : \mathbb{L}] = ?$

$\mathbb{F}(\sqrt{3}) = \mathbb{K}$

$\mathbb{F} = \mathbb{L}(\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ } $x^2 - 3$ anula $\sqrt{3}$

$\mathbb{L}$

$[\mathbb{F} : \mathbb{L}] = 2$ $\quad x^2 - 2$ $\quad \mathbb{Q}(\sqrt{2})$

$\mathbb{Q}$

$\mathbb{F}(\sqrt{3})$
|
$\mathbb{F}$

$x^2 - 3$ anula $\sqrt{3}$ $\longrightarrow$ $[\mathbb{F}(\sqrt{3}) : \mathbb{F}] = 2$ (22

$$[\mathbb{K} : \mathbb{L}] = [\mathbb{K} : \mathbb{F}][\mathbb{F} : \mathbb{L}]$$
$$= 2 \times 2$$
$$= 4$$

Por Steiner $\exists\, \alpha \in \mathbb{K}$ t.q. $\mathbb{K} = \mathbb{Q}(\alpha)$
$= \mathbb{Q}[\alpha]$

ACHAR um α:

$\alpha = \sqrt{2} + \sqrt{3}$ serve?

Se servir, então todo $x \in \mathbb{K}$ é C.L., com coeficientes de α.

Basta fazer isto para $\sqrt{2}$ & $\sqrt{3}$

$$\begin{cases} \alpha^2 = 5 + 2\sqrt{2}\sqrt{3} \\ \alpha = \sqrt{2} + \sqrt{3} \end{cases}$$

$$\alpha^2 = 5 + 2\sqrt{2}(\alpha - \sqrt{2})$$

$$\alpha^2 = 5 + 2\sqrt{2}\,\alpha - 4$$

$$\alpha^2 = 1 + 2\sqrt{2}\cdot\alpha$$

$$2\sqrt{2}\cdot\alpha = \alpha^2 - 1$$

$$\boxed{\sqrt{2} = \frac{\alpha}{2} - \frac{1}{2}\cdot\alpha^{-1}}$$

$$\alpha^2 - 5 = 2\sqrt{6}$$

$$(\alpha^2 - 5)^2 = 24$$

$$\alpha^4 - 10\alpha^2 + 25 = 24$$

$$\boxed{\alpha^4 - 10\alpha^2 + 1 = 0}$$ (ainda não vimos como provar irracionalidade)

$$1 = 10\alpha^2 - \alpha^4$$

$$1 = \alpha(10\alpha - \alpha^3)$$

$$\boxed{\alpha^{-1} = 10\alpha - \alpha^3}$$

$$\sqrt{2} = \frac{\alpha}{2} - \frac{1}{2}(10\alpha - \alpha^3)$$

$$\boxed{\sqrt{2} = -9/2\,\alpha + 1/2\,\alpha^3}$$

$\sqrt{3} = \alpha - \sqrt{2}$

$$\boxed{\sqrt{3} = \frac{11}{2}\alpha - \frac{1}{2}\alpha^3}$$

$\sqrt{6} = \sqrt{2} \cdot \sqrt{3} = (\quad) \cdot (\quad)$

CAMINHO GERAL Provar que o polinômio $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ é irredutível:

Lema:

$\mathbb{K} = \mathbb{Q}(\alpha)$

$n = [\mathbb{K} : \mathbb{Q}]$, $\mathbb{F} = \mathbb{Q}$

Então o grupo $AUT(\mathbb{K}|\mathbb{F}) =$

$$\{ \varphi : \mathbb{K} \to \mathbb{K} \mid \varphi \text{ é isomorfismo de } \mathbb{K} \text{ e } \varphi(x) = x \ \forall x \in \mathbb{F} \}$$

Prova $K = \mathbb{Q}(\alpha)$, $\alpha = \sqrt{2} + \sqrt{3}$

$\mathbb{F} = \mathbb{Q}$

$w \in \mathbb{K} \Rightarrow \exists \ \lambda_1, \dots, \lambda_n \in \mathbb{F}$ t.q.

$w = \lambda_0 + \lambda_1 \alpha + \dots + \lambda_n \alpha^n$

$\{1, \alpha, \alpha^2, \alpha^3\}$ é $\mathbb{Q}$-base de $\mathbb{K}$

$\alpha^4 = 1 + 10\alpha^2$

$\alpha^5 = \alpha + 10\alpha^3$

$\alpha^6 = \alpha^2 + 10\alpha^4$

$= \alpha^2 + 10(1 + 10\alpha^2)$

$= 10 + 11\alpha^2$

$\{1, \alpha, \dots, \alpha^{n-1}\}$ é $\mathbb{F}$-base de $\mathbb{K} = \mathbb{F}(\alpha)$ $\mathbb{K}|\mathbb{F}$

$\varphi \in \mathrm{Aut}(\mathbb{F}|\mathbb{K})$ Lembre $\lambda_i \in \mathbb{F}$ & Logo

$\boxed{\varphi(\lambda_i) = \lambda_i \ \forall i}$

Daí $\varphi(w) = \lambda_0 + \lambda_1 \varphi(\alpha) + \dots +$

$+ \lambda_{n-1}[\varphi(\alpha)]^{n-1}$ ✓

Para saber $\varphi(w)$ importa saber somente o valor de $\boxed{\varphi(\alpha)}$ Logo φ é completamente determinado pelo seu valor

sobre α (ou seja $\varphi(\alpha)$)

Lembre $\alpha^4 - 10\alpha^2 - 1 = 0$

ou seja α é raiz do polinômio

$$f(x) = x^4 - 10x^2 - 1$$

$\varphi(\alpha) = \varphi(0) = \varphi(\alpha^4 - 10\alpha^2 - 1) \Rightarrow$

$\varphi(\alpha)$ é raiz de $f(x) = x^4 - 10x^2 - 1$

$0 = [\varphi(\alpha)]^4 - 10[\varphi(\alpha)]^2 - 1$

Logo as raizes complexas $\tilde{n}$ servem.

$f' = 4x^3 - 20x$ ou seja $\varphi(\alpha)$ é raiz da f onde $f' = 4$ temos no máximo 4 escolhas para $\varphi(\alpha)$

Logo

No gráfico α substitui x

$\alpha^4 - 10\alpha^2 - 1 = 0$

$-\alpha \quad 0 \quad \sqrt{5} \quad \alpha$

$\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{R}$

tem 4 aut $\Rightarrow$ distintos $\pm\alpha$ raizes

$x^4 - 10x - 1$

$f(x) = a_0 + a_1 x + \dots + x^m$

$a_i \in \mathbb{R}$

& $\beta \in \mathbb{C}$

$f(\beta) = 0$

b

$f(\bar{\beta}) = 0$

pois $0 = \bar{0} = \overline{f(\beta)} = \overline{a_0 + \dots + \beta^m}$

$= a_0 + \dots + (\bar{\beta})^n$

$= f(\bar{\beta})$

$(x - \beta)(x - \bar{\beta})$ divide f

$x^2 - (\beta + \bar{\beta}) \cdot x + \beta\bar{\beta} =$

$= x^2 - \underbrace{2\mathrm{Re}(\beta)}_{\in \mathbb{R}} x + \underbrace{|\beta|^2}_{\in \mathbb{R}} \in \mathbb{R}[x]$

$f = (x^2 - 2\mathrm{Re}(\beta)x + |\beta|^2) \cdot q(x)$

$q(x) \in \mathbb{R}[x]$

Logo $\partial f \geq 3$

$\Rightarrow f$ é redutível sobre $\mathbb{R}$ #

outra forma

$\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$\mathbb{Q}(\sqrt{2})(\sqrt{3})$

$\mathbb{Q}(\sqrt{2})$ $\}$ $\{1, \sqrt{3}\}$

$\mathbb{Q}$ $\{1, \sqrt{2}\}$ é base

B base é?

$B = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} = \sqrt{2}\cdot\sqrt{3}$

é base de $\mathbb{K}/\mathbb{F}$

só basta saber $\varphi(\sqrt{2})$ & $\varphi(\sqrt{3})$

$(\sqrt{2})^2 = 2$

$\varphi(\sqrt{2})^2 = \varphi(2) = 2$

$\Rightarrow \varphi(\sqrt{2}) = \pm\sqrt{2}$

$(\sqrt{3})^2 = 3$

$|\varphi(\sqrt{3})|^2 = \varphi(3) = 3$

$\varphi(\sqrt{3}) = \pm\sqrt{3}$

φ_0 $\quad \sqrt{2} \longrightarrow +\sqrt{2}$
$\quad \sqrt{3} \longrightarrow +\sqrt{3}$

φ_1 $\quad \sqrt{2} \longrightarrow -\sqrt{2}$
$\quad \sqrt{3} \longrightarrow +\sqrt{3}$ $\quad Id$

φ_2 $\quad \sqrt{2} \longrightarrow +\sqrt{2}$
$\quad \sqrt{3} \longrightarrow -\sqrt{3}$

φ_3 $\quad \sqrt{2} \longrightarrow -\sqrt{2}$
$\quad \sqrt{3} \longrightarrow -\sqrt{3}$

XV $\quad \mathbb{Z}[i] = \{ n + m\sqrt{-1} \mid n, m \in \mathbb{Z} \}$

α è invertibile $\iff \exists$

$\beta \in \mathbb{Z}[i]$ t.q.

$\alpha\beta = 1$

XIII

$p = 3$

$\frac{21}{84} = \frac{3 \cdot 7}{3^4} = \frac{1}{3^3} \cdot 7 = 3^{-3} \cdot 7$

$\| \quad p^{-3} \cdot 7$

$\nu(\alpha) = -3$

$\beta = \frac{21}{84} = 3\frac{7}{84} = p \cdot \frac{7}{84}$

$\nu(\beta) = 1$

$\text{dist}(\alpha, 0) = \left(\frac{1}{2}\right)^{-\nu(\alpha - 0)} = \left(\frac{1}{2}\right)^{-\nu(\alpha)}$

$= \frac{1}{2}^{-(-3)} = 1/8$

$\text{dist}(\beta, 0) = \frac{1}{2}^{-\nu(\beta)} = \frac{1}{2}^{-(1)} = 2$

XII $R = \{ \frac{n}{m} \mid p \nmid m \}$

$\frac{n}{m}, \frac{a}{b} \in R$

$\frac{n}{m} + \frac{a}{b} = \frac{nb + am}{mb}$

$\frac{n}{m} \cdot \frac{a}{b} = \frac{na}{mb}$ — $p \nmid mb$

$0 = \frac{0}{1}$ $p \nmid 1$

$\alpha = \frac{n}{m} \in R$ e $\alpha^{-1} \in R$

candidato de α^{-1} é $\frac{m}{n}$

daí $p \nmid n$

$I = \{ \frac{n}{m} \in R \mid p \mid n \}$

$\frac{n}{m}, \frac{a}{b} \in I$

$\frac{n}{m} + \frac{a}{b} = \frac{nb + ma}{mb}$ $\quad p \mid (nb + ma)$

$\frac{c}{d} \in R \quad \frac{c}{d} \cdot \frac{n}{m} = \frac{c \cdot n}{dm} \quad - p \mid cn$

$J \lhd R$

$\alpha = \frac{a}{b} \in J \neq R$

$p \mid a \Rightarrow \alpha \in I$

$\Downarrow$

$J \subseteq I$

$p \nmid a \Rightarrow \alpha^{-1} \in R$

Dar $\alpha^{-1} \cdot \alpha = 1 \in J$

$\forall x \in R \quad x = 1 \cdot x \in J \Rightarrow J = R$