Extensão algébrica

Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos e $\alpha \in \mathbb{E}$. Tome o homomorfismo de anéis $\psi_\alpha : \mathbb{F}[X] \longrightarrow \mathbb{E}$ tal que $\psi_\alpha(X) = \alpha$

Temos duas possibilidades:

(1) ψ_α é injetor. Neste caso, dizemos que α é transcendente sobre $\mathbb{F}$.

(2) ψ_α não é injetor. Neste caso, dizemos que α é algébrico sobre $\mathbb{F}$.

Assuma que α é algébrico. Então como $\mathbb{F}[X]$ é um domínio de ideais principais, $\operatorname{Ker}\psi_\alpha = (p_\alpha(X))$. Podemos assumir que $p_\alpha(X)$ é mônico. Assim, o único polinômio mônico que gera $\operatorname{Ker}\psi_\alpha$ é denominado o polinômio minimal de α sobre $\mathbb{F}$.

Temos que

$$\mathbb{E} \supseteq \mathbb{F}[\alpha] \cong \mathbb{F}[X]/(p_\alpha(X)).$$

Como $\dim \mathbb{F}[\alpha] < \infty$ e $\mathbb{F}[\alpha]$ é domínio, segue que $\mathbb{F}[\alpha]$ é corpo. Assim $(p_\alpha(X))$ é maximal, e portanto,

$p_\alpha(X)$ é irredutível.

Lema. Sejam $\mathbb{E}/\mathbb{F}$ e $\alpha \in \mathbb{E}$. As seguintes afirmações são equivalentes:

(i) α é algébrico sobre $\mathbb{F}$,

(ii) α satisfaz um polinômio não nulo em $\mathbb{F}[X]$,

(iii) $\dim \mathbb{F}[\alpha] < \infty$.

(i) $\Rightarrow$ (ii) Se $\operatorname{Ker} \psi_\alpha = (p_\alpha) \neq 0$, então $p_\alpha(\alpha) = 0$.

(ii) $\Rightarrow$ (i). Se $f(\alpha) = 0$, então $f \in \operatorname{Ker} \psi_\alpha$.

(i) $\Rightarrow$ (iii). já vimos

(iii) $\Rightarrow$ (ii). Se $\dim \mathbb{F}[\alpha] = n < \infty$, então $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ é $\mathbb{F}$-l.d. Daí, existem coef. não todos nulos tais que

$$0 = a_0 + a_1\alpha + \dots + a_n\alpha^n, \quad a_0, a_1, \dots, a_n \in \mathbb{F}.$$

Mas, isso significa que α satisfaz $f(X) = a_0 + a_1X + \dots + a_nX^n$. $\square$

Lema. Sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos, $\alpha \in \mathbb{E}$ algébrico sobre $\mathbb{F}$ e $p(X) \in \mathbb{F}[X]$. As seguintes afirmações são equivalentes:

(i) $p(X)$ é o polinômio minimal de α sobre $\mathbb{F}$,

(ii) $p(X)$ é mônico, irredutível em $\mathbb{F}[X]$, e $p(\alpha) = 0$,

(iii) $p(X)$ é mônico e o polinômio de menor grau que satisfaz $p(\alpha)=0$.

Dem.: (i) $\Rightarrow$ (ii): já vimos.

(ii) $\Rightarrow$ (i). Assuma que $p(X)$ satisfaz as propriedades de (ii). Então $p(X) \in \ker \varphi_\alpha = (p_\alpha(X))$. Então $p(X) = q(X) p_\alpha(X)$. Mas $p(X)$ é irredutível, e portanto, $q(X) \in \mathbb{F}$. Daí $p(X) = p_\alpha(X)$.

(iii) $\Rightarrow$ (i). exercício. $\square$

Notação. O polinômio minimal de α sobre $\mathbb{F}$ é denotado por $\mathrm{Irr}(\alpha, \mathbb{F})$.

Exemplo.

(1) Seja $\mathbb{F}$ um corpo qualquer. Então todo $\alpha \in \mathbb{F}$ é algébrico sobre $\mathbb{F}$. Seu polinômio minimal é $X - \alpha \in \mathbb{F}[X]$.

(2) $\sqrt{2} \in \mathbb{R}$ é algébrico sobre $\mathbb{Q}$.

$$\mathrm{Irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2.$$

$$\mathrm{Irr}(\sqrt{2}, \mathbb{Q}(\sqrt{2})) = X - \sqrt{2}.$$

(3) $\sqrt{1+\sqrt{2}}$ é algébrico sobre $\mathbb{Q}$. Temos que

$$\left(\left(\sqrt{1+\sqrt{2}}\right)^2 - 1\right)^2 = 2.$$

Daí $\sqrt{1+\sqrt{2}}$ satisfaz $(X^2-1)^2-2 \in \mathbb{Q}[X]$.
Portanto, $\sqrt{1+\sqrt{2}}$ é algébrico sobre $\mathbb{Q}$.

(4) $\sqrt{2}+\sqrt{3} \in \mathbb{R}$ é algébrico sobre $\mathbb{Q}$, pois

$$\left(\frac{(\sqrt{2}+\sqrt{3})^2-5}{2}\right)^2 = 6.$$

Então $\sqrt{2}+\sqrt{3}$ satisfaz $X^4-10X^2+1 \in \mathbb{Q}[X]$.

Se α é algébrico sobre $\mathbb{F}$, e se p_α é seu polinômio minimal sobre $\mathbb{F}$, então

$$[\mathbb{F}[\alpha]:\mathbb{F}] = gr(p_\alpha).$$

Então, para mostrar que X^4-10X^2+1 é o polinômio minimal de $\sqrt{2}+\sqrt{3}$ sobre $\mathbb{Q}$, basta mostrar que

$$[\mathbb{Q}[\sqrt{2}+\sqrt{3}]:\mathbb{Q}] = gr(X^4-10X^2+1) = 4.$$

Já vimos que $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Então

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\underbrace{[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]}_{2}.$$

Provemos que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Assuma que

$\mathbb{Q}(\sqrt{2}) \ni \sqrt{3} = a + b\sqrt{2}, \quad a, b \in \mathbb{Q}.$

Então $3 = (a+b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$. Como $\{1, \sqrt{2}\}$ é uma $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$. Daí, vale que

$$\begin{cases} 3 = a^2 + 2b^2 \\ 0 = 2ab \end{cases}$$

Portanto $(a = 0$ e $3 = 2b^2)$ ou $(b = 0$ e $3 = a^2)$.

Mas $3 = 2b^2$ e $3 = a^2$ não possuem solução em $\mathbb{Q}$, uma contradição. Daí $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

Provemos que $X^2 - 3$ é irredutível em $\mathbb{Q}(\sqrt{2})[X]$. Se não fosse, então $X^2 - 3$ teria raiz em $\mathbb{Q}(\sqrt{2})$, o que não ocorre. Daí

$$[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = gr(X^2 - 3) = 2.$$

Daí

$$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Portanto, $gr(Irr(\sqrt{2} + \sqrt{3}, \mathbb{Q})) = 4$. Então $X^4 - 10X^2 + 1$ é o polinômio minimal de $\sqrt{2} + \sqrt{3}$ sobre $\mathbb{Q}$.

Def. Uma extensão de corpos $\mathbb{E}|\mathbb{F}$ é dita ser *algébrica* se todo $\alpha \in \mathbb{E}$ é algébrico sobre $\mathbb{F}$.

Toda extensão $\mathbb{E}/\mathbb{F}$ finita é algébrica. Isso, pois dado $\alpha \in \mathbb{E}$, vale que $[\mathbb{F}(\alpha):\mathbb{F}] \leq [\mathbb{E}:\mathbb{F}] < \infty$. Daí α é algébrica sobre $\mathbb{F}$.

Teorema. Uma extensão $\mathbb{E}/\mathbb{F}$ é finita se e só se existem $\alpha_1, \dots, \alpha_m \in \mathbb{E}$, algébricos sobre $\mathbb{F}$, tais que $\mathbb{E} = \mathbb{F}[\alpha_1, \dots, \alpha_m]$.

Demonstração. Se $\mathbb{E}/\mathbb{F}$ é finita, então todo $\alpha \in \mathbb{E}$ é algébrico sobre $\mathbb{F}$. Daí $\mathbb{E} = \mathbb{F}[\alpha_1, \dots, \alpha_m]$ (por exemplo, se $\alpha_1, \dots, \alpha_m$ é $\mathbb{F}$-base de $\mathbb{E}$).

Agora, assuma que $\mathbb{E} = \mathbb{F}[\alpha_1, \dots, \alpha_m]$, com $\alpha_1, \dots, \alpha_m$ algébricos sobre $\mathbb{F}$. Temos então que $[\mathbb{F}(\alpha_1):\mathbb{F}] < \infty$. Assuma então que, para algum $i \geq 1$, $[\mathbb{F}[\alpha_1, \dots, \alpha_i]:\mathbb{F}] < \infty$. Então α_{i+1} é algébrico sobre $\mathbb{F} \subseteq \mathbb{F}[\alpha_1, \dots, \alpha_i]$. Daí α_{i+1} é algébrico sobre $\mathbb{F}[\alpha_1, \dots, \alpha_i]$. Então

$$[\mathbb{F}[\alpha_1, \dots, \alpha_i][\alpha_{i+1}] : \mathbb{F}[\alpha_1, \dots, \alpha_i]] < \infty.$$

Portanto,

$$[\mathbb{F}[\alpha_1, \dots, \alpha_i, \alpha_{i+1}]:\mathbb{F}] = [\mathbb{F}[\alpha_1, \dots, \alpha_i][\alpha_{i+1}]:\mathbb{F}[\alpha_1, \dots, \alpha_i]] \cdot [\mathbb{F}[\alpha_1, \dots, \alpha_i]:\mathbb{F}] < \infty.$$

$\square$

Teorema. Considere as extensões de corpos $\mathbb{L}/\mathbb{E}/\mathbb{F}$. Então $\mathbb{L}/\mathbb{F}$ é algébrica se e só se $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ são algébricas.

Demonstração. Assuma que $\mathbb{L}/\mathbb{F}$ é algébrica. Então todo $\alpha \in \mathbb{E}$ é algébrico sobre $\mathbb{F}$. Portanto, $\mathbb{E}/\mathbb{F}$ é algébrica. Além disso, dado $\alpha \in \mathbb{L}$, temos que α satisfaz um polinômio em $\mathbb{F}[X] \subseteq \mathbb{E}[X]$. Portanto, α é algébrico sobre $\mathbb{E}$, e $\mathbb{L}/\mathbb{E}$ é algébrica.

Reciprocamente, assuma $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ algébricas. Seja $\alpha \in \mathbb{L}$. Como α é algébrico sobre $\mathbb{E}$, então α satisfaz um polinômio

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{E}[X].$$

Como $f(X) \in \mathbb{F}(a_0, a_1, \ldots, a_{n-1})[X]$, segue que α é algébrico sobre $\mathbb{F}(a_0, a_1, \ldots, a_{n-1})$. Mas $a_0, a_1, \ldots, a_{n-1}$ são algébricos sobre $\mathbb{F}$, e portanto, $[\mathbb{F}(a_0, \ldots, a_{n-1}) : \mathbb{F}] < \infty$. Além disso, $[\mathbb{F}(a_0, \ldots, a_{n-1})[\alpha] : \mathbb{F}(a_0, \ldots, a_{n-1})] < \infty$.

Daí

$$[\mathbb{F}[\alpha] : \mathbb{F}] \leq [\mathbb{F}[a_0, \ldots, a_{n-1}, \alpha] : \mathbb{F}] =$$

$$= [\mathbb{F}[a_0, \ldots, a_{n-1}][\alpha] : \mathbb{F}[a_0, \ldots, a_{n-1}]] \cdot [\mathbb{F}[a_0, \ldots, a_{n-1}] : \mathbb{F}] < \infty.$$

Daí α é algébrico sobre $\mathbb{F}$. Então $\mathbb{L}/\mathbb{F}$ é algébrica. $\square$

Teorema. Seja $\mathbb{M}|\mathbb{F}$ uma extensão de corpos e defina
$$\mathbb{E} = \{\alpha \in \mathbb{M} \mid \alpha \text{ é algébrico sobre } \mathbb{F}\}$$
Então $\mathbb{E}$ é corpo contendo $\mathbb{F}$ e $\mathbb{E}/\mathbb{F}$ é algébrica.

Demonstração. Todo $\alpha \in \mathbb{F}$ é algébrico sobre $\mathbb{F}$, e portanto, $\mathbb{F} \subseteq \mathbb{E}$. Sejam $0 \neq \alpha, \beta \in \mathbb{E}$. Então α e β são algébricos sobre $\mathbb{F}$. Daí $[\mathbb{F}[\alpha, \beta] : \mathbb{F}] < \infty$. Temos $\alpha - \beta, \alpha\beta, \alpha^{-1} \in \mathbb{F}[\alpha, \beta]$, pois $\mathbb{F}[\alpha,\beta]$ é corpo. Portanto, $\alpha-\beta, \alpha\beta, \alpha^{-1}$ são algébricos sobre $\mathbb{F}$, e então, estão em $\mathbb{E}$. Assim, $\mathbb{E}$ é corpo. Por construção, todo elemento de $\mathbb{E}$ é algébrico sobre $\mathbb{F}$, e portanto, $\mathbb{E}/\mathbb{F}$ é algébrica. $\square$

O corpo $\mathbb{E}$ é denominado de fecho algébrico de $\mathbb{F}$ em $\mathbb{M}$.

Obs: (1) Se $\mathbb{L}/\mathbb{F}$ é uma extensão algébrica, então $\mathbb{L} \subset \mathbb{E}$. De fato, todo $a \in \mathbb{L}$ é algébrico sobre $\mathbb{F}$.

(2) Denote $\mathbb{E} = \overline{\mathbb{F}}^{\mathbb{M}}$. Então
$$\overline{\left(\overline{\mathbb{F}}^{\mathbb{M}}\right)}^{\mathbb{M}} = \overline{\mathbb{F}}^{\mathbb{M}} \supseteq \mathbb{F}.$$
Temos que $\overline{\overline{\mathbb{F}}^{\mathbb{M}}}^{\mathbb{M}} / \overline{\mathbb{F}}^{\mathbb{M}}$ e $\overline{\mathbb{F}}^{\mathbb{M}}/\mathbb{F}$ são alg. Portanto, $\overline{\overline{\mathbb{F}}^{\mathbb{M}}}^{\mathbb{M}}/\mathbb{F}$ também é alg. Daí $\overline{\overline{\mathbb{F}}^{\mathbb{M}}}^{\mathbb{M}} \subseteq \overline{\mathbb{F}}^{\mathbb{M}}$. Daí vale a igualdade.

Seja $\alpha = \sum_{n \in \mathbb{N}} \frac{1}{2^{n!}} \in \mathbb{R}$. Tal elemento não está em $\mathbb{Q}$,

Proposição. α é transcendente sobre $\mathbb{Q}$.

Dem.: Assuma o contrário, e portanto, α tem pol. min.

$$f(X) = X^d + a_{n-1} X^{d-1} + \cdots + a_1 X + a_0 \in \mathbb{Q}[X].$$

Existe $D \in \mathbb{Z}$ tal que $Df \in \mathbb{Z}[X]$. Seja

$$\alpha_n = \sum_{i=1}^{n} \frac{1}{2^{i!}} \in \mathbb{Q}.$$

Como $\alpha_n \in \mathbb{Q}$ e f é irredutível sobre $\mathbb{Q}$, $f(\alpha_n) \neq 0$.

Então $Df(\alpha_n) \cdot (2^{n!})^d \in \mathbb{Z} \setminus \{0\}$. Então

$$(*) \quad |D f(\alpha_n) (2^{n!})^d| \geq 1.$$

Por Teorema Fundamental da Álgebra,

$$f(X) = (X - \alpha) \prod_{i=1}^{d-1} (X - \beta_i), \quad \beta_i \in \mathbb{C}.$$

Então

$$|f(\alpha_n)| = |\alpha_n - \alpha| \underbrace{\prod_{i=1}^{d-1} |\alpha_n - \beta_i|}_{} \leq |\alpha_n - \alpha| M.$$

$|\alpha_n - \beta_i| \leq |\alpha_n| + |\beta_i| \leq 2 + C$

Temos
$$|\alpha - \alpha_n| = \sum_{m>n} \frac{1}{2^{m!}} \leq \frac{1}{2^{(n+1)!}} \sum_{i\in\mathbb{N}} \frac{1}{2^i} \leq \frac{2}{2^{(n+1)!}}.$$

Daí
$$|D(2^{n!})^d f(\alpha_n)| \leq \frac{2D(2^{n!})^d}{2^{(n+1)!}} = 2D\left(\frac{2^d}{2^{n+1}}\right)^{(n+1)!}.$$

Daí $D(2^{n!})^d f(\alpha_n) \to 0$ quando $n \to \infty$, o que contradiz $(*)$. $\square$