Corpos algebricamente fechados

Teorema. Seja $\mathbb{F}$ um corpo. As seguintes afirmações são equivalentes:

(i) todo polinômio em $\mathbb{F}[X]$ de grau não nulo possui raiz em $\mathbb{F}$,

(ii) todo polinômio em $\mathbb{F}[X]$ se fatora como produto de polinômios de grau 1,

(iii) todo polinômio irredutível em $\mathbb{F}[X]$ possui grau 1,

(iv) Se $\mathbb{E}/\mathbb{F}$ é uma extensão algébrica, então $\mathbb{E}=\mathbb{F}$.

(v) Se $\mathbb{E}/\mathbb{F}$ é uma extensão finita, então $\mathbb{E}=\mathbb{F}$.

Dem.: (i) $\Rightarrow$ (ii) Seja $f \in \mathbb{F}[X]$. De (i), existe $\alpha \in \mathbb{F}$ tal que $f(\alpha)=0$. Daí $f = (X-\alpha)\, g(X)$, com $gr(g) < gr\, f$. Por indução no grau do polinômio, obtemos que g é produto de polinômios de grau 1. Portanto, f também é.

(ii) $\Rightarrow$ (iii). Seja $f \in \mathbb{F}[X]$ irredutível. De (ii), segue que $f = f_1 \cdots f_s$, com $gr\, f_i = 1$. Mas f é irredutível, portanto, $s=1$. Daí $gr\, f = 1$.

(iii) $\Rightarrow$ (iv). Sejam $\mathbb{E}/\mathbb{F}$ uma extensão algébrica e $a \in \mathbb{E}$. Então o polinômio minimal de a tem grau 1, por (iii). Daí o polinômio é $X-a$, e portanto $a \in \mathbb{F}$.

Daí $\mathbb{E} = \mathbb{F}$.

(iv) $\Rightarrow$ (v): Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita. Daí $\mathbb{E}/\mathbb{F}$ é algébrica. De (iv), $\mathbb{E} = \mathbb{F}$.

(v) $\Rightarrow$ (i). Seja $f \in \mathbb{F}[X]$ de grau não nulo. Daí, vimos que existe $\mathbb{E} = \mathbb{F}(a)$ tal que $f(a) = 0$. Como $\mathbb{E}/\mathbb{F}$ é finita, temos $\mathbb{E} = \mathbb{F}$. Portanto, $a \in \mathbb{E} = \mathbb{F}$. Daí f possui raiz em $\mathbb{F}$. $\square$

Def. Dizemos que $\mathbb{F}$ é um corpo *algebricamente fechado* se satisfaz uma (portanto todas) as condições do teorema anterior.

Exemplo. $\mathbb{C}$ é algebricamente fechado (Teorema Fundamental da álgebra).

Def. Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos. Dizemos que $\mathbb{E}$ é um *fecho algébrico* de $\mathbb{F}$ se:

(i) $\mathbb{E}$ é algebricamente fechado,

(ii) $\mathbb{E}/\mathbb{F}$ é algébrica.

Proprosição. Seja $\Omega/\mathbb{F}$ uma extensão de corpos, com Ω um corpo algebricamente fechado. Seja $\mathbb{E}$ o fecho algébrico de $\mathbb{F}$ em Ω. Então $\mathbb{E}$ é algebricamente fechado.

Dem.: Já vimos que $\mathbb{E}$ é um corpo e $\mathbb{E}/\mathbb{F}$ é uma extensão algébrica. Seja $f \in \mathbb{E}[X] \subseteq \Omega[X]$. Como Ω é algebricamente fechado, existe $a \in \Omega$ com $f(a) = 0$. Como a satisfaz um polinômio em $\mathbb{E}[X]$, então a é algébrico sobre $\mathbb{E}$. Daí a é algébrico sobre $\mathbb{F}$ ($\mathbb{E}(a)/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ são alg. $\Rightarrow$ $\mathbb{E}(a)/\mathbb{F}$ é alg.) Portanto, $a \in \mathbb{E}$, por construção de $\mathbb{E}$. Então $\mathbb{E}$ é um corpo algebricamente fechado. $\square$

Exemplo. Seja $\mathbb{A} = \{x \in \mathbb{C}$ algébrico sobre $\mathbb{Q}\}$ é um fecho algébrico de $\mathbb{Q}$.

Teorema. Seja $\mathbb{F}$ um corpo. Então $\mathbb{F}$ admite um fecho algébrico.

Dem.: Seja

$$\mathcal{F} = \{\mathbb{E} \text{ corpo} \mid \mathbb{F} \subseteq \mathbb{E} \text{ e } \mathbb{E}/\mathbb{F} \text{ é algébrica}\}.$$

Considere a ordem parcial em $\mathcal{F}$ dada pela inclusão. Além disso, $\mathcal{F} \neq \emptyset$, pois $\mathbb{F} \in \mathcal{F}$. Seja $\mathcal{C} = \{\mathbb{E}_i\}_{i \in I}$ uma cadeia em $\mathcal{F}$. Tome

$$\mathbb{L} = \bigcup_{i \in I} \mathbb{E}_i .$$

Temos que $\mathbb{L}$ é um corpo: Sejam $0 \neq a, b \in \mathbb{L}$. Então, existem $\mathbb{E}_i$, $\mathbb{E}_j$ tais que $a \in \mathbb{E}_i$ e $b \in \mathbb{E}_j$. Como $\mathcal{C}$ é uma cadeia, então $\mathbb{E}_i \subseteq \mathbb{E}_j$ ou $\mathbb{E}_j \subseteq \mathbb{E}_i$. Podemos assumir $\mathbb{E}_i \subseteq \mathbb{E}_j$, a menos de troca de índices. Então $a \in \mathbb{E}_i \subseteq \mathbb{E}_j \ni b$. Como $\mathbb{E}_j$ é corpo,

$$a-b, ab, a^{-1} \in \mathbb{E}_j \subseteq \mathbb{L}.$$

Portanto, $\mathbb{L}$ é corpo. Além disso, por construção, $\mathbb{F} \subseteq \mathbb{L}$. Como $a \in \mathbb{E}_j$ e $\mathbb{E}_j / \mathbb{F}$ é algébrica, segue que a é algébrico sobre $\mathbb{F}$. Portanto, $\mathbb{L}/\mathbb{F}$ é algébrica. Então $\mathbb{L} \in \mathcal{F}$.

Agora, por construção, $\mathbb{E}_i \subseteq \mathbb{L}$, $\forall i \in I$. Daí $\mathbb{L}$ é cota superior de $\mathcal{C}$. Do Lema de Zorn, $\mathcal{F}$ admite um elemento maximal $\overline{\mathbb{F}}$.

Como $\overline{\mathbb{F}} / \mathbb{F}$ é algébrico, bastamostrarmos que $\overline{\mathbb{F}}$ é algebricamente fechado. Seja $\mathbb{M}/\overline{\mathbb{F}}$ uma extensão algébrica. Então, $\mathbb{M}/\mathbb{F}$ é uma extensão algébrica. Portanto, por maximalidade de $\overline{\mathbb{F}}$, segue que $\mathbb{M} = \overline{\mathbb{F}}$. Daí $\overline{\mathbb{F}}$ é um fecho algébrico de $\mathbb{F}$. $\square$

Dado um monomorfismo de corpos $\varphi_0 : \mathbb{F} \to \Omega$ e um polinômio $p(X) = \alpha_0 + \alpha_1 X + \dots + \alpha_m X^m \in \mathbb{F}[X]$, então φ_0 induz um homomorfismo $\mathbb{F}[X] \to \Omega[X]$ via

$$p^{\varphi_0} = \varphi_0(p) = \varphi_0(\alpha_0) + \varphi_0(\alpha_1)X + \dots + \varphi_0(\alpha_m) \in \Omega[X].$$

Proposição. Sejam $\mathbb{F}$ um corpo, Ω um corpo algebricamente fechado e $\varphi_0 : \mathbb{F} \to \Omega$ um monomorfismo de corpos. Seja $\mathbb{E} = \mathbb{F}(a)$ uma extensão de corpos com a algébrico sobre $\mathbb{F}$. Seja $p_a \in \mathbb{F}[X]$ o polinômio minimal de a sobre $\mathbb{F}$. Então, para cada raiz $\omega \in \Omega$ de $p_a^{\varphi_0}$, existe um único monomorfismo $\varphi : \mathbb{E} \to \Omega$ que estende φ_0 e tal que $\varphi(a) = \omega$.

Todo monomorfismo $\mathbb{E} \to \Omega$ que estende φ_0 é construído dessa forma.

Dem.: Identifique $\mathbb{E} \cong \mathbb{F}[X]/(p_a)$, de tal forma que $a \longmapsto X + (p_a)$. Seja ω uma raiz de $p_a^{\varphi_0}$.

$$\begin{tikzcd}
\mathbb{F}[X] \arrow[r, "\psi_\omega"] \arrow[d] & \Omega \\
\mathbb{F}[X]/(p_a) \arrow[ur, dashed] &
\end{tikzcd}$$

Considere o mapa

$$\begin{aligned} \psi_\omega : \mathbb{F}[X] &\longrightarrow \Omega \\ f(X) &\longmapsto f^{\varphi_0}(\omega) \end{aligned}$$

Temos que, por escolha de ω, $\psi_\omega(p_a) = p^{\varphi_0}(\omega) = 0$. Daí $(p_a) \subseteq \operatorname{Ker} \psi_\omega$. Mas (p_a) é maximal, e portanto, $\operatorname{Ker} \psi_\omega = (p_a)$. Daí, conseguimos fatorar ψ_ω da seguinte forma

$$\begin{tikzcd}
\mathbb{F}[X] \arrow[r, "\psi_\omega"] \arrow[d] & \Omega \\
\mathbb{F}[X]/(p_a) \arrow[ur, "\psi'_\omega"'] &
\end{tikzcd}$$

Temos que:

Se $\alpha \in \mathbb{F}$, $\psi'_\omega(\alpha) = \psi_\omega(\alpha) = \varphi_0(\alpha)$;

$$\psi'_\omega(X + (p_a)) = \psi_\omega(X) = \omega.$$

Então ψ'_ω estende φ_0 e satisfaz $\psi'_\omega(a) = \omega$.

Compondo com o iso. $E \cong F[X]/(p_a)$, obtemos $\Psi_\omega : E \to \Omega$.

Vale que Ψ_ω é única: assuma que

$$\varphi' : E \to \Omega$$

estende φ_0 e $\varphi'(a) = \omega$. Então, como $E = F(a)$, um $b \in E$ pode ser escrito como

$$b = g(a), \quad g \in F[X], \; g(X) = \beta_0 + \beta_1 X + \dots + \beta_s X^s$$

Daí

$$\varphi'(b) = \varphi'(g(a)) = \varphi'(\beta_0 + \beta_1 a + \dots + \beta_s a^s) =$$
$$= \varphi'(\beta_0) + \varphi'(\beta_1)\varphi'(a) + \dots + \varphi'(\beta_s)\varphi'(a)^s$$
$$= \varphi_0(\beta_0) + \varphi_0(\beta_1)\omega + \dots + \varphi_0(\beta_s)\omega^s = g^{\varphi_0}(\omega) = \Psi_\omega(b).$$

Portanto, $\varphi' = \Psi_\omega$.

Agora, assuma que $\varphi'' : E \to \Omega$ estende φ_0.
Por um lado, se $p_a = \alpha_0 + \alpha_1 X + \dots + \alpha_r X^r$, então $p_a(a) = 0$. Daí

$$0 = \varphi''(\alpha_0 + \alpha_1 a + \dots + \alpha_r a^r) =$$
$$= \varphi''(\alpha_0) + \varphi''(\alpha_1)\varphi''(a) + \dots + \varphi''(\alpha_r)\varphi''(a)^r$$
$$= \varphi_0(\alpha_0) + \varphi_0(\alpha_1)\varphi''(a) + \dots + \varphi_0(\alpha_r)\varphi''(a)^r$$

$= p_a^{\varphi_0}(\varphi''(a))$.

Portanto, $\varphi''(a)$ é raiz de $p_a^{\varphi_0}$. Daí, φ'' coincide com a única extensão de φ_0 tal que $a \mapsto \omega_0''$, em que $\omega_0'' := \varphi''(a)$ é raiz de $p_a^{\varphi_0}$. $\square$

Observação. Se $\mathbb{F} \subseteq \Omega$, $\varphi_0 = id$, e $\mathbb{E} = \mathbb{F}(a)$, então, provou-se que tem bijeção

$$\begin{pmatrix} \text{monomorfismos } \mathbb{F}(a) \longrightarrow \Omega \\ \text{que são identidade em } \mathbb{F} \end{pmatrix} \longleftrightarrow \begin{pmatrix} \text{raízes (distintas)} \\ \text{de } p_a \text{ em } \Omega \end{pmatrix}.$$

Def. Sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos e $\mathbb{F} \subseteq \Omega$ corpos. Um $\mathbb{F}$-monomorfismo é um monomorfismo $\sigma : \mathbb{E} \longrightarrow \Omega$ tal que $\sigma(\alpha) = \alpha$, $\forall \alpha \in \mathbb{F}$.

Proposição. Sejam $\mathbb{E}/\mathbb{F}$ extensão algébrica, Ω um corpo algebricamente fechado e $\varphi_0 : \mathbb{F} \longrightarrow \Omega$ um monomorfismo de corpos. Então existe monomorfismo $\varphi : \mathbb{E} \longrightarrow \Omega$ que estende φ_0.

Dem.: Seja

$$\mathcal{F} = \{(\mathbb{E}_i, \varphi_i) \mid \mathbb{E}_i/\mathbb{F} \text{ é extensão algébrica}, \mathbb{E}_i \subseteq \mathbb{E}, \text{ e } \varphi_i : \mathbb{E}_i \to \Omega \text{ estende } \varphi_0\}.$$

A família $\mathcal{F}$ é não vazia, pois $(\mathbb{F}, \varphi_0) \in \mathcal{F}$. Considere a ordem parcial $\leq$ em $\mathcal{F}$ dada por:

$(\mathbb{E}_i, \varphi_i) \leq (\mathbb{E}_j, \varphi_j)$ se $\mathbb{E}_i \subseteq \mathbb{E}_j$ e φ_j estende φ_i.

Seja $\mathcal{L} = \{(\mathbb{E}_i, \varphi_i)\}_{i \in I}$ uma cadeia em $\mathcal{F}$. Seja $\mathbb{L} = \bigcup_{i \in I} \mathbb{E}_i$. Do mesmo argumento anterior, $\mathbb{L}$ é um corpo. Além disso, por construção, $\mathbb{F} \subseteq \mathbb{L} \subseteq \mathbb{E}$.

Defina $\varphi : \mathbb{L} \to \Omega$ da seguinte forma: dado $a \in \mathbb{L}$, seja $\mathbb{E}_i \ni a$, $\varphi(a) := \varphi_i(a)$. Está bem definida, pois se $a \in \mathbb{E}_i$ e $a \in \mathbb{E}_j$, então podemos assumir $(\mathbb{E}_i, \varphi_i) \leq (\mathbb{E}_j, \varphi_j)$ (pois $\mathcal{L}$ é cadeia). Daí φ_j estende φ_i, e portanto $\varphi_i(a) = \varphi_j(a)$.

Vale que φ é homomorfismo: dados $a, b \in \mathbb{L}$, existe $\mathbb{E}_i \in \mathcal{L}$ tal que $a, b \in \mathbb{E}_i$ (pois $\mathcal{L}$ é cadeia). Daí

$$\varphi(a+b) = \varphi_i(a+b) = \varphi_i(a) + \varphi_i(b) = \varphi(a) + \varphi(b),$$

$$\varphi(ab) = \varphi_i(ab) = \varphi_i(a)\varphi_i(b) = \varphi(a)\varphi(b).$$

Portanto, φ é hom. Por construção, φ estende φ_0 (pois qualquer φ_i estende φ_0). Daí $(\mathbb{L}, \varphi) \in \mathcal{F}$, e é cota superior para $\mathcal{C}$, por construção. Por Lema de Zorn, existe elemento maximal $(\mathbb{M}, \overline{\varphi}) \in \mathcal{F}$.

Se $\mathbb{M} \neq \mathbb{E}$, então existe $a \in \mathbb{E} \setminus \mathbb{M}$, e extensão algébrica $\mathbb{M}(a)$. Da proposição anterior, existe extensão de $\overline{\varphi}$, $\overline{\overline{\varphi}} : \mathbb{M}(a) \to \Omega$, contradizendo a maximalidade de $(\mathbb{M}, \overline{\varphi})$. Portanto $\mathbb{M} = \mathbb{E}$, e $\overline{\varphi} : \mathbb{E} \to \Omega$ estende $\varphi_0 : \mathbb{F} \to \Omega$. $\square$

Corolário. Quaisquer dois fechos algébricos de um corpo $\mathbb{F}$ são isomorfos.

Dem.: Sejam $\overline{\mathbb{F}}_1$ e $\overline{\mathbb{F}}_2$ fechos algébricos de $\mathbb{F}$. Então, temos $i : \mathbb{F} \to \overline{\mathbb{F}}_2$, e como $\overline{\mathbb{F}}_1 / \mathbb{F}$ é algébrica, existe $j : \overline{\mathbb{F}}_1 \to \overline{\mathbb{F}}_2$, pela prop. anterior. Daí $\overline{\mathbb{F}}_2 / \overline{\mathbb{F}}_1$ é alg. (pois $\overline{\mathbb{F}}_2 / \mathbb{F}$ é alg.) e $\overline{\mathbb{F}}_1$ é alg. fechado. Portanto $j(\overline{\mathbb{F}}_1) = \overline{\mathbb{F}}_2$, e daí j é isomorfismo. $\square$