2. Extensões algébricas

2.1. **Extensões algébricas.** Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos, considere o anel de polinômios $\mathbb{F}[X]$ e tome $\alpha \in \mathbb{E}$. Então, temos um homomorfismo de anéis bem definido

$$\psi_\alpha : \mathbb{F}[X] \to \mathbb{E},$$

de modo que $\psi_\alpha(1) = 1$ e $\psi_\alpha(X) = \alpha$. Relembre que este homomorfismo pode ser descrito da maneira seguinte: dado $f(X) \in \mathbb{F}[X]$, vale que $\psi_\alpha(f(X)) = f(\alpha)$ (substituição de X por α no polinômio f, e cálculos feitos em $\mathbb{E}$).

A primeira observação, bastante importante é o seguinte: a imagem de ψ_α é exatamente $\mathbb{F}[\alpha]$. Além disso, temos duas possibilidades:

1. ψ_α é um homomorfismo injetor. Neste caso, dizemos que α é um elemento *transcendente* sobre $\mathbb{F}$. Então, segue que $\mathbb{F}[\alpha]$ é isomorfo ao anel de polinômios $\mathbb{F}[X]$.
2. ψ_α não é injetor. Neste caso, dizemos que α é um elemento *algébrico* sobre $\mathbb{F}$. Então seu núcleo $\ker \psi_\alpha \neq 0$. Assim sendo, segue que

$$\mathbb{F}[\alpha] \cong \mathbb{F}[X]/\ker \psi_\alpha.$$

Agora, como $\mathbb{F}[X]$ é um domínio de ideais principais, existe um único polinômio mônico $p_\alpha(X)$ que gera o núcleo, isto é, $\ker \psi_\alpha = (p_\alpha(X))$. Já vimos que

$$\dim_{\mathbb{F}} \mathbb{F}[\alpha] = \dim_{\mathbb{F}} \mathbb{F}[X]/(p_\alpha(X)) < \infty.$$

Assim, sendo $\mathbb{F}[\alpha] \subseteq \mathbb{E}$ um domínio, segue do Corolário 1.6 que $\mathbb{F}[\alpha]$ é um corpo. Portanto, segue que o polinômio $p_\alpha(X)$ é irredutível em $\mathbb{F}[X]$.

Definição 2.1. Sejam $\mathbb{E}/\mathbb{F}$ e $\alpha \in \mathbb{E}$. O elemento α é dito ser *algébrico* sobre $\mathbb{F}$ se o mapa ψ_α não é injetor. O único polinômio mônico $p_\alpha(X)$ que gera seu núcleo é denominado *polinômio mínimo* (ou *polinômio minimal*) de α sobre $\mathbb{F}$.

Note as seguintes equivalentes formas de definir elemento algébrico:

Lema 2.2. *Sejam $\mathbb{E}/\mathbb{F}$ e $\alpha \in \mathbb{E}$. As afirmações seguintes são equivalentes:*

(i) *α é algébrico sobre $\mathbb{F}$,*
(ii) *existe $f(X) \in \mathbb{F}[X]$ não nulo de modo que $f(\alpha) = 0$,*
(iii) *existe $m > 0$ e $a_0, a_1, \ldots, a_m \in \mathbb{F}$ de modo que*

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m = 0$$

(iv) $\dim_{\mathbb{F}} \mathbb{F}[\alpha] < \infty$.

Demonstração. Exercício. □

Da mesma forma, existem diversas formas de definir o polinômio mínimo:

Lema 2.3. *Sejam $\mathbb{E}/\mathbb{F}$, $\alpha \in \mathbb{E}$ um elemento algébrico sobre $\mathbb{F}$ e $p(X) \in \mathbb{F}[X]$. As afirmações seguintes são equivalentes:*

(i) *o polinômio $p(X)$ 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 tal que $p(\alpha) = 0$,*

Demonstração. Denote por $\psi_\alpha : \mathbb{F}[X] \to \mathbb{E}$ a função substituição (isto é, definimos $\psi_\alpha(X) = \alpha$). Seja p_α o polinômio minimal de α sobre $\mathbb{F}$.
$(i) \iff (ii)$: seja $p(X)$ satisfazendo (ii). Então, como $p(\alpha) = 0$, segue que $p \in \ker \psi_\alpha = (p_\alpha)$. Portanto, p_α divide p. Sendo p irredutível e ambos mônicos,

obtemos que $p = p_\alpha$. Reciprocamente, já vimos que o polinômio minimal satisfaz as propriedades (ii).
$(i) \iff (iii)$: seja $p(X)$ satisfazendo (iii). Então, como $p(\alpha) = 0$, por mesmo argumento anterior, segue que p_α divide p. Como $p_\alpha(\alpha) = 0$ e o grau de p é o menor que anula α, temos que $\mathrm{gr}(p) \leq \mathrm{gr}(p_\alpha)$. Entretanto, essas afirmações implicam que $p = p_\alpha$. □

Notação. Usualmente, denota-se o polinômio mínimo de α sobre $\mathbb{F}$ por $\mathrm{Irr}(\alpha, \mathbb{F})$.

Exemplo 2.1.

(1) Todo elemento $\alpha \in \mathbb{F}$ é algébrico sobre $\mathbb{F}$. Seu polinômio minimal é $X - \alpha$.
(2) Dado $\alpha \in \mathbb{Q}$, $\alpha > 0$, e $m \in \mathbb{N}$, um elemento $y \in \mathbb{R}$ tal que $y^m = \alpha$ é algébrico sobre $\mathbb{Q}$. De fato, tal elemento é raiz de $X^m - \alpha \in \mathbb{Q}[X]$.
(3) O elemento $\sqrt{1+\sqrt{2}}$ é algébrico sobre $\mathbb{Q}$. De fato, seja $\alpha = \sqrt{1+\sqrt{2}}$. Então, note que
$$(\alpha^2 - 1)^2 = 2,$$
ou seja, α satisfaz o polinômio $X^4 - 2X^2 - 1$.
(4) O elemento $\sqrt{2} + \sqrt{3}$ é algébrico sobre $\mathbb{Q}$. De fato,
$$\left(\frac{(\sqrt{2}+\sqrt{3})^2 - 5}{2}\right)^2 = 6,$$
e daí $\sqrt{2} + \sqrt{3}$ satisfaz o polinômio $X^4 - 10X^2 + 1$.

Provemos a seguinte observação:

Proposição 2.4. *Sejam $\mathbb{E}/\mathbb{F}$ e $\alpha \in \mathbb{E}$. Então α é algébrico sobre $\mathbb{F}$ se e só se $\mathbb{F}[\alpha]/\mathbb{F}$ é uma extensão finita. Neste caso, vale que $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$ e $\mathrm{gr}\,(\mathrm{Irr}(\alpha, \mathbb{F})) = [\mathbb{F}[\alpha] : \mathbb{F}]$.*

Demonstração. Temos que $[\mathbb{F}[\alpha] : \mathbb{F}] < \infty$ se e só se o homomorfismo $\psi_\alpha : \mathbb{F}[X] \to \mathbb{F}[\alpha]$ não é injetor (caso contrário, $\dim_{\mathbb{F}} \mathbb{F}[\alpha] = \dim \mathbb{F}[X] = \infty$). O último ocorre se e só se α é algébrico sobre $\mathbb{F}$.

Agora, assuma que α é algébrico sobre $\mathbb{F}$. Seja $p_\alpha(X) = \mathrm{Irr}(\alpha, \mathbb{F})$. Temos que $\mathbb{F}[\alpha] \cong \mathbb{F}[X]/(p_\alpha(X))$, e portanto, $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$ é corpo e $[\mathbb{F}[\alpha] : \mathbb{F}] = \mathrm{gr}(p_\alpha(X))$. □

Exemplo 2.2. Provaremos que $X^4 - 10X^2 + 1$ é o polinômio minimal de $\sqrt{2}+\sqrt{3}$ sobre $\mathbb{Q}$. Vimos que tal elemento satisfaz tal polinômio, por exemplo anterior. Então, a conclusão é obtida se mostrarmos que o grau do polinômio minimal de $\sqrt{2}+\sqrt{3}$ sobre $\mathbb{Q}$ é exatamente 4. E isso equivale a mostrar que $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$. Por um lado, como $\sqrt{2}+\sqrt{3}$ satisfaz um polinômio de grau 4, vale que $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] \leq 4$. Entretanto, já vimos que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Além disso, vale que
$$4 \geq [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{2}.$$
Assim, basta mostrarmos que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, o que implicaria $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] > 1$. Assuma então que
$$\sqrt{3} = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$
Então $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. Sendo $\{1, \sqrt{2}\}$ uma $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$, segue que $3 = a^2 + 2b^2$ e $2ab = 0$. Portanto, $a = 0$ ou $b = 0$, e sabe-se que as equações

$a^2 = 3$ e $2b^2 = 3$ não possuem solução em $\mathbb{Q}$ (por que?). Isso é uma contradição, e portanto, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

Perceba que, ao mostrar que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, provamos também que $X^2 - 3$ é o polinômio minimal de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$.

Provaremos a seguinte descrição de extensões finitas:

Teorema 2.5. *Uma extensão $\mathbb{E}/\mathbb{F}$ é finita se e só se existem $\alpha_1, \ldots, \alpha_m \in \mathbb{E}$ algébricos sobre $\mathbb{F}$ de modo que $\mathbb{E} = \mathbb{F}[\alpha_1, \ldots, \alpha_m]$.*

Demonstração. Assuma que $\mathbb{E}/\mathbb{F}$ é finita. Então, todo $\alpha \in \mathbb{E}$ é algébrico sobre $\mathbb{F}$, uma vez que $[\mathbb{F}[\alpha] : \mathbb{F}] < [\mathbb{E} : \mathbb{F}] < \infty$. Assim, existem $\alpha_1, \ldots, \alpha_m \in \mathbb{E}$ algébricos sobre $\mathbb{F}$ de modo que $\mathbb{E} = \mathbb{F}[\alpha_1, \ldots, \alpha_m]$ (por exemplo, pode-se tomar $\{\alpha_1, \ldots, \alpha_m\}$ como sendo uma $\mathbb{F}$-base de $\mathbb{E}$).

Reciprocamente, assuma que $\mathbb{E} = \mathbb{F}[\alpha_1, \ldots, \alpha_m]$, com $\alpha_1, \ldots, \alpha_m \in \mathbb{E}$ algébricos sobre $\mathbb{F}$. Então, da proposição anterior, $[\mathbb{F}[\alpha_1] : \mathbb{F}] < \infty$. Agora, assuma que, para algum $i \geq 1$, $[\mathbb{F}[\alpha_1, \ldots, \alpha_i] : \mathbb{F}] < \infty$. Temos que α_{i+1} satisfaz um polinômio em $\mathbb{F}[X] \subseteq \mathbb{F}[\alpha_1, \ldots, \alpha_i][X]$. Portanto, α_{i+1} é algébrico sobre $\mathbb{F}[\alpha_1, \ldots, \alpha_i]$. Segue que $[\mathbb{F}[\alpha_1, \ldots, \alpha_i][\alpha_{i+1}] : \mathbb{F}[\alpha_1, \ldots, \alpha_i]] < \infty$. Daí

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

Assim, por indução, $[\mathbb{E} : \mathbb{F}] = [\mathbb{F}[\alpha_1, \ldots, \alpha_m] : \mathbb{F}] < \infty$. □

Estamos interessados no seguinte tipo de extensão:

Definição 2.6. Uma extensão de corpos $\mathbb{E}/\mathbb{F}$ é dito ser *algébrica* se todo $\alpha \in \mathbb{E}$ é algébrico sobre $\mathbb{F}$.

Da Proposição 2.4, obtemos que toda extensão finita é algébrica. Entretanto, existem extensões algébricas que não são finitas (qual?).

As extensões algébricas constituem uma classe boa de extensões, no seguinte sentido:

Teorema 2.7. *Considere as extensões de corpos $\mathbb{L}/\mathbb{E}/\mathbb{F}$. Então $\mathbb{L}/\mathbb{F}$ é algébrico se e só se $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ são algébricos.*

Demonstração. Assuma que $\mathbb{L}/\mathbb{F}$ é algébrico. Então, por definição, todo elemento $\alpha \in \mathbb{E} \subseteq \mathbb{L}$ é algébrico sobre $\mathbb{F}$, e portanto, $\mathbb{E}/\mathbb{F}$ é algébrico. Além disso, dado $\alpha \in \mathbb{L}$, como α é algébrico sobre $\mathbb{F}$, segue que α satisfaz um polinômio em $\mathbb{F}[X] \subseteq \mathbb{E}[X]$. Portanto α é algébrico sobre $\mathbb{E}$, e daí, $\mathbb{L}/\mathbb{E}$ é algébrico.

Reciprocamente, assuma que $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ são algébricos. Se $\alpha \in \mathbb{L}$, então α satisfaz algum polinômio $f(X) = a_0 + a_1X + \cdots + a_mX^m \in \mathbb{E}[X]$. Tal polinômio está em $\mathbb{F}[a_0, a_1, \ldots, a_m]$, e então α é algébrico sobre $\mathbb{F}[a_0, a_1, \ldots, a_m]$. Portanto, $[\mathbb{F}[a_0, a_1, \ldots, a_m][\alpha] : \mathbb{F}[a_0, a_1, \ldots, a_m]] < \infty$. Agora, $a_0, a_1, \ldots, a_m$ são algébricos sobre $\mathbb{F}$, e portanto, do teorema anterior, $[\mathbb{F}[a_0, a_1, \ldots, a_m] : \mathbb{F}] < \infty$. Daí,

$$[\mathbb{F}[\alpha] : \mathbb{F}] \leq [\mathbb{F}[a_0, a_1, \ldots, a_m, \alpha] : \mathbb{F}] < \infty.$$

Da Proposição 2.4, segue que α é algébrico sobre $\mathbb{F}$. Portanto, $\mathbb{L}/\mathbb{F}$ é algébrico. □

Por fim, temos:

Teorema 2.8. *Seja $\mathbb{M}/\mathbb{F}$ uma extensão de corpos. Defina*

$$\mathbb{E} = \{x \in \mathbb{M} \text{ } \textit{algébrico sobre} \text{ } \mathbb{F}\}.$$

Então $\mathbb{E}$ é um corpo contendo $\mathbb{F}$, e $\mathbb{E}/\mathbb{F}$ é uma extensão algébrica.

Demonstração. Como todo elemento de $\mathbb{F}$ é algébrico sobre $\mathbb{F}$, segue por definição que $\mathbb{F} \subseteq \mathbb{E}$. Sejam $\alpha, \beta \in \mathbb{E}$. Então, do Teorema 2.5, segue que $[\mathbb{F}[\alpha, \beta] : \mathbb{F}] < \infty$. Como $\alpha\beta, \alpha - \beta, \alpha^{-1} \in \mathbb{F}[\alpha, \beta]$ (a última, se $\alpha \neq 0$), segue da Proposição 2.4 que todos esses elementos são algébricos sobre $\mathbb{F}$, e portanto, estão em $\mathbb{E}$. Isso implica que $\mathbb{E}$ é um corpo. Por construção, todo elemento de $\mathbb{E}$ é algébrico sobre $\mathbb{F}$. □

O conjunto $\mathbb{E}$ do teorema anterior é usualmente denominado de o *fecho algébrico de* $\mathbb{F}$ *em* $\mathbb{M}$.

Exercício. Seja $\mathbb{A} = \{x \in \mathbb{C} \text{ algébrico sobre } \mathbb{Q}\}$. Mostre que $\mathbb{A}/\mathbb{Q}$ é uma extensão algébrica com $[\mathbb{A} : \mathbb{Q}] = \infty$.