Grupos e Corpos

Prof. Lucas Calixto

Aula 9 - Extensões de corpos

De agora em diante, as letras $\mathbb{F}$, $\mathbb{E}$, $\mathbb{K}$, ... denotarão corpos

Dado um poli $f(x) \in \mathbb{F}[x]$, queremos encontrar um corpo $\mathbb{E}$ que contenha as raízes de f. Nesse caso

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \text{ em } \mathbb{E}[x]$$

Exemplo: $f(x) = x^4 - 5x + 6 \in \mathbb{Q}(x)$ se escreve como $(x^2 - 2)(x^2 - 3)$ em $\mathbb{Q}[x]$

Assim, se queremos achar raízes de $f(x)$ precisamos de um corpo maior do que $\mathbb{Q}$

Por exemplo,

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3}) \text{ em } \mathbb{R}[x]$$

Note: não precisamos de todo $\mathbb{R}$ para conseguir raízes de $f(x)$. De fato, tome

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

Então, $f(x)$ tem raíz em $\mathbb{Q}(\sqrt{2})$ e

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})(x^2 - 3) \text{ em } \mathbb{Q}(\sqrt{2})[x]$$

A ideia será estudar esse tipo de corpo para polinômios em $\mathbb{F}[x]$

Extensões de corpos

Se $\mathbb{F} \subset \mathbb{E}$ dizemos que $\mathbb{E}$ é uma extensão de $\mathbb{F}$ (ou $\mathbb{F}$ é um subcorpo de $\mathbb{E}$)

Exemplo: Tome $\mathbb{F} = \mathbb{Q}(\sqrt{2})$ e $\mathbb{E} = \mathbb{Q}(\sqrt{2}+\sqrt{3}) =$ o menor corpo que contem $\mathbb{Q}$ e $\sqrt{2}+\sqrt{3}$. Note que $\frac{1}{\sqrt{2}+\sqrt{3}} = \sqrt{2}-\sqrt{3} \in \mathbb{E}$. Logo,

$$(\sqrt{2}+\sqrt{3}) \pm (\sqrt{2}-\sqrt{3}) = \sqrt{2}, \sqrt{3} \in \mathbb{E} \Rightarrow \mathbb{Q} \subset \mathbb{F} \subset \mathbb{E}$$

Essa conta $\Rightarrow \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) =$ o menor corpo que contem $\mathbb{Q}$, $\sqrt{2}$ e $\sqrt{3}$

Teorema: Seja $p(x) \in \mathbb{F}[x]$ poli não constante. Então existe extensão $\mathbb{E} \supset \mathbb{F}$ tal que $p(x)$ tem raiz em $\mathbb{E}$

Prova: Podemos assumir $p(x) = b_0 + b_1 x + \cdots + b_k x^k$ irredutível

$\mathbb{E} = \mathbb{F}[x]/\langle p(x) \rangle = \{a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + \langle p(x) \rangle \mid a_i \in \mathbb{F}\}$ é tal corpo

Notação: $\overline{a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}} = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + \langle p(x) \rangle$

Note:

$$\begin{aligned}
\overline{a_0 + a_1x + \cdots + a_{k-1}x^{k-1}} &= a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + \langle p(x)\rangle \\
&= (a_0 + \langle p(x)\rangle) + (a_1 + \langle p(x)\rangle)(x + \langle p(x)\rangle) + \cdots + (a_{k-1} + \langle p(x)\rangle)(x^{k-1} + \langle p(x)\rangle) \\
&= (a_0 + \langle p(x)\rangle) + (a_1 + \langle p(x)\rangle)(x + \langle p(x)\rangle) + \cdots + (a_{k-1} + \langle p(x)\rangle)(x + \langle p(x)\rangle)^{k-1} \\
&= \bar{a}_0 + \bar{a}_1\bar{x} + \cdots + \bar{a}_{k-1}\bar{x}^{k-1}
\end{aligned}$$

Logo, $\mathbb{E} = \{\bar{a}_0 + \bar{a}_1\bar{x} + \cdots + \bar{a}_{k-1}\bar{x}^{k-1} \mid a_i \in \mathbb{F}\}$. **Obs:** não confundam $\bar{x}$ (que é um elemento de $\mathbb{E}$) com x (que continua sendo uma variável)

- $\mathbb{F} \subset \mathbb{E}$: e fácil ver que o homomorfismo

$$\phi : \mathbb{F} \to \mathbb{E}, \quad \phi(a) = \bar{a}$$

permite identificarmos $\mathbb{F}$ com $\phi(\mathbb{F}) \subset \mathbb{E}$

- $\bar{x} \in \mathbb{E}$ é raiz de $p(x) \in \mathbb{E}[x]$: (note que $\bar{x}$ é elemento de $\mathbb{E}$ e x é variável e portanto $x \notin \mathbb{E}$)

$$\begin{aligned}
p(\bar{x}) &= \bar{b}_0 + \bar{b}_1\bar{x} + \cdots + \bar{b}_k\bar{x}^k \\
&= b_0 + b_1x + \cdots + b_kx^k + \langle p(x)\rangle \\
&= 0 + \langle p(x)\rangle = \bar{0} \text{ em } \mathbb{E}
\end{aligned}$$

Exemplo: $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ é irredutível

$\Rightarrow \mathbb{E} = \mathbb{Z}_2[x]/\langle p(x)\rangle = \{\bar{a} + \bar{b}\bar{x} \mid a, b \in \mathbb{Z}_2\} = \{\bar{0}, \bar{b}\bar{x}, \bar{1}, \bar{1} + \bar{x}\}$ é corpo

Considerando $p(x) \in \mathbb{E}[x]$, temos $p(\bar{x}) = 0$ em $\mathbb{E}$

Exemplo: $p(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$ não é irredutível

$p(x) = (x^2 + x + 1)(x^3 + x + 1)$ é fatoração em irredutíveis (pq?)

Em $\mathbb{E}_1 = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$, $\alpha_1 = x + \langle x^2 + x + 1\rangle$ é raiz de $p(x)$

$\Rightarrow p(x) = (x - \alpha_1)(x - \alpha_2)(x^3 + x + 1)$ em $\mathbb{E}_1[x]$ (aqui, $\alpha_2 = (1 + x) + \langle x^2 + x + 1\rangle$)

Em $\mathbb{E}_2 = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$, $\beta_1 = x + \langle x^3 + x + 1\rangle$ é raiz de $p(x)$

$\Rightarrow p(x) = (x - \beta_1)(x - \beta_2)(x^2 + x + 1)$ em $\mathbb{E}_2[x]$. Quem é β_2?

Note: $|\mathbb{E}_1| = 4$ e $|\mathbb{E}_2| = 8$

Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão

Um elemento $\alpha \in \mathbb{E}$ é algébrico sobre $\mathbb{F}$ se $p(\alpha) = 0$ para algum $p(x) \in \mathbb{F}[x]$

Um elemento $\alpha \in \mathbb{E}$ é transcendental sobre $\mathbb{F}$ se α não é algébrico sobre $\mathbb{F}$

Se todo $\alpha \in \mathbb{E}$ é algébrico sobre $\mathbb{F}$, dizemos que a extensão $\mathbb{F} \subset \mathbb{E}$ é algébrica

O menor subcorpo de $\mathbb{E}$ que contem $\mathbb{F}$ e elementos $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$ será denotado por $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$

Se $\exists\ \alpha \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(\alpha)$, dizemos que a extensão $\mathbb{F} \subset \mathbb{E}$ é simples

Exemplo: • $\sqrt{2}, i \in \mathbb{C}$ são algébricos sobre $\mathbb{Q}$, já que são, respetivamente, raízes dos polis $x^2 - 2$ e $x^2 + 1$ em $\mathbb{Q}[x]$

• π e e são transcendentais sobre $\mathbb{Q}$ (a demonstração não é trivial)

Fato: números transcendentais são difíceis de achar, mas os números algébricos que são raros (os algébricos tem cardinalidade $\aleph_0 = |\mathbb{N}|$, enquanto que os transcendentais tem cardinalidade $\aleph_1 = |\mathbb{R}|$)

Exemplo: $\alpha = \sqrt{2+\sqrt{3}}$ é algébrico sobre $\mathbb{Q}$. De fato,

$$\alpha^2 = 2+\sqrt{3} \Rightarrow \alpha^2 - 2 = \sqrt{2} \Rightarrow \alpha^4 - 4\alpha^2 + 4 = 3 \Rightarrow \alpha^4 - 4\alpha^2 + 1 = 0$$

Logo, α é raiz de $p(x) = x^4 - 4x^2 + 1 \in \mathbb{Q}[x]$

Teorema: Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão, e $\alpha \in \mathbb{E}$. Então, α é transcendental sobre $\mathbb{F}$ se e só se $\mathbb{F}(\alpha) \cong \mathbb{F}(x)$ (lembre: $\mathbb{F}(x)$ é o corpo de frações do domínio integral $\mathbb{F}[x]$)

Prova: Tome $\phi_\alpha : \mathbb{F}[x] \to \mathbb{E}$, $\phi_\alpha(f(x)) = f(\alpha)$ (homomorfismo de avaliação em α)

α é transcendental $\Leftrightarrow \ker(\phi_\alpha) = \{0\} \Leftrightarrow \phi_\alpha$ é injetora

Logo, α é transcendental $\Leftrightarrow F[x] \cong \operatorname{im}\phi_\alpha$ e portanto $F(x) \cong Q(\operatorname{im}\phi_\alpha) =$ corpo de frações do domínio $\operatorname{im}\phi_\alpha$. Lembrem,

$$Q(\operatorname{im}\phi_\alpha) = \{f(\alpha)g(\alpha)^{-1} \mid f(x), g(x) \in \mathbb{F}[x],\ g(x) \neq 0\} \subset \mathbb{E}$$

Afirmamos que $Q(\operatorname{im}\phi_\alpha) = F(\alpha)$

$\phi_\alpha(x) = \alpha \in Q(\operatorname{im}\phi_\alpha)$, $\phi_\alpha(a) = a \in Q(\operatorname{im}\phi_\alpha)\ \forall a \in \mathbb{F} \Rightarrow \mathbb{F}(\alpha) \subset Q(\operatorname{im}\phi_\alpha)$

Por outro lado, $f(\alpha), g(\alpha) \in \mathbb{F}(\alpha)$ para todos $f(x), g(x) \in \mathbb{F}[x] \Rightarrow f(\alpha)g(\alpha)^{-1} \in \mathbb{F}(\alpha)$

$\Rightarrow Q(\operatorname{im}\phi_\alpha) \subset \mathbb{F}(\alpha) \Rightarrow Q(\operatorname{im}\phi_\alpha) = \mathbb{F}(\alpha) \Rightarrow \mathbb{F}(x) \cong \mathbb{F}(\alpha)$

Teorema: Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão, e $\alpha \in \mathbb{E}$ algébrico sobre $\mathbb{F}$. Então existe único poli monico irredutível em $\mathbb{F}[x]$ de grau mínimo tal que $p(\alpha) = 0$. Além disso, se $f(x) \in \mathbb{F}[x]$ é tal que $f(\alpha) = 0$, então $p(x) \mid f(x)$.

Prova: Tome $\phi_\alpha : \mathbb{F}[x] \to \mathbb{E}$, $\phi_\alpha(f(x)) = f(\alpha)$

α algébrico $\Rightarrow \ker \phi_\alpha \neq 0$. Seja $p(x) \in \mathbb{F}[x]$ único poli mônico com $\text{gr}(p(x)) > 0$ tal que $\ker \phi_\alpha = \langle p(x) \rangle$

$p(x)$ redutível $\Leftrightarrow p(x) = g(x)q(x)$ com $\text{gr}(g(x)) > 0$ e $\text{gr}(q(x)) > 0 \Leftrightarrow \langle p(x) \rangle \subsetneq \langle g(x) \rangle$ e $\langle p(x) \rangle \subsetneq \langle q(x) \rangle$. Logo, $p(\alpha) = 0 \Rightarrow g(\alpha) = 0$ ou $q(\alpha) = 0$

Se $g(x) = 0 \Rightarrow g(x) \in \ker \phi_\alpha = \langle p(x) \rangle \Rightarrow \langle g(x) \rangle \subset \langle p(x) \rangle$ (contradição)

Logo, $p(x)$ é irredutível

Se $f(\alpha) = 0$, então $f(x) \in \ker \phi_\alpha = \langle p(x) \rangle \Rightarrow p(x) \mid f(x)$

Note: o poli $p(x) \in \mathbb{F}[x]$ do teorema tem grau mínimo dentre os polis que tem α como raiz. Esse é chamado poli minimal de α sobre $\mathbb{F}$ e será denotado por $m_\alpha(x)$. O grau de $m_\alpha(x)$ é chamado de grau de α sobre $\mathbb{F}$

Exemplo: Os polis $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ e $g(x) = x^4 - 4x^2 + 1 \in \mathbb{Q}[x]$ são os polis minimais de $\sqrt{2}$ e $\sqrt{2+\sqrt{3}}$, respetivamente.

Teorema: Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão, e $\alpha \in \mathbb{E}$ algébrico sobre $\mathbb{F}$. Então $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/\langle m_\alpha(x)\rangle$.

Prova: Pelo Teorema anterior, vemos que $\mathbb{F}[x]/\langle m_\alpha(x)\rangle \cong \operatorname{im}\phi_\alpha$. Logo, $\operatorname{im}\phi_\alpha$ é corpo de $\mathbb{E}$ que contem $\mathbb{F}$ e $\alpha \Rightarrow F(\alpha) \subset \operatorname{im}\phi_\alpha$

Por outro lado, $\operatorname{im}\phi_\alpha = \{f(\alpha) \mid f(x) \in \mathbb{F}[x]\}$ está obviamente contido em $F(\alpha)$

Portanto, $\mathbb{F}[x]/\langle m_\alpha(x)\rangle \cong \operatorname{im}\phi_\alpha = \mathbb{F}(\alpha)$

Corolário Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão, $\alpha \in \mathbb{E}$ algébrico sobre $\mathbb{F}$. Então, todo elemento $\beta \in \mathbb{F}(\alpha)$ pode ser unicamente expresso como

$$\beta = a_0 + a_1\alpha + \cdots + a_n\alpha^{n-1}, \quad a_i \in \mathbb{F} \text{ e } n = \operatorname{gr}(m_\alpha(x))$$

Prova: Segue da formula que dá o isomorfismo $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/\langle m_\alpha(x)\rangle$

Corolário: Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão, $\alpha \in \mathbb{E}$ algébrico sobre $\mathbb{F}$. Então $\mathbb{F}(\alpha)$ é um $\mathbb{F}$-espaço vetorial com base $\{1, \ldots, \alpha^{n-1}\}$, onde $n = \operatorname{gr}(m_\alpha(x))$. Em particular, $\dim_{\mathbb{F}} \mathbb{F}(\alpha) = n$.

Se $\mathbb{F} \subset \mathbb{E}$ é uma extensão e $\mathbb{E}$ é um espaço vetorial de dimensão n sobre $\mathbb{F}$, dizemos que a extensão $\mathbb{F} \subset \mathbb{E}$ é finita de grau n e escrevemos $[\mathbb{E} : \mathbb{F}] = n$

Corolário: Se $\mathbb{F} \subset \mathbb{E}$ é uma extensão, $\alpha \in \mathbb{E}$ algébrico sobre $\mathbb{F}$, então $[\mathbb{F}(\alpha) : \mathbb{F}] = \text{gr}(m_\alpha(x))$

Exemplo: $[\mathbb{Q}(\sqrt{2} : \mathbb{Q})] = 2$ e $[\mathbb{C} : \mathbb{R}] = 2$

Teorema: Se $\mathbb{F} \subset \mathbb{E}$ é uma extensão finita, então $\mathbb{E}$ é algébrico sobre $\mathbb{F}$

Prova: Suponha $[\mathbb{E} : \mathbb{F}] = n$ e tome $\alpha \in \mathbb{E}$. Então $1, \alpha, \ldots, \alpha^n$ é LD

$\Rightarrow$ existe expressão $a_0 1 + a_1\alpha + \cdots + a_n\alpha^n = 0$ com algum $0 \neq a_i \in \mathbb{F}$

$\Rightarrow f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x] \setminus \{0\}$ e $f(\alpha) = 0 \Rightarrow \alpha$ é algébrico sobre $\mathbb{F}$

Exercício: Mostre que a reciproca do Teorema não vale (dica: tome $\mathbb{E} = \{\alpha \in \mathbb{R} \mid \alpha \text{ é algébrico sobre } \mathbb{Q}\}$, mostre que $\mathbb{E}$ é corpo e que $[\mathbb{E} : \mathbb{Q}] = \infty$)

Teorema: Suponha que $\mathbb{F} \subset \mathbb{E}$ e $\mathbb{E} \subset \mathbb{K}$ são extensões finitas. Então, $\mathbb{F} \subset \mathbb{K}$ é finita e

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$$

Prova: Exercício de álgebra linear. Basta mostrar que se $\{\alpha_1, \ldots, \alpha_n\}$ é base de $\mathbb{E}$ sobre $\mathbb{F}$ e $\{\beta_1, \ldots, \beta_m\}$ é base de $\mathbb{K}$ sobre $\mathbb{E}$, então $\{\alpha_i\beta_j \mid i = 1, \ldots, n,\ j = 1, \ldots, m\}$ é base de $\mathbb{K}$ sobre $\mathbb{F}$.

Corolário: Suponha que $\mathbb{F}_1 \subset \mathbb{F}_2,\ \mathbb{F}_2 \subset \mathbb{F}_3, \cdots, \mathbb{F}_{n-1} \subset \mathbb{F}_n$ são extensões finitas. Então, todas as extensões $\mathbb{F}_i \subset \mathbb{F}_j$ com $i < j$ são finitas, e vale

$$[\mathbb{F}_j : \mathbb{F}_i] = [\mathbb{F}_j : \mathbb{F}_{j-1}] \cdots [\mathbb{F}_{i+1} : \mathbb{F}_i]$$

Corolário: Suponha $\mathbb{F} \subset \mathbb{E}$ é uma extensão, $\alpha \in \mathbb{E}$ algébrico sobre $\mathbb{F}$. Então, $\mathrm{gr}(m_\beta(x)) \mid \mathrm{gr}(m_\alpha(x))$ para qualquer $\beta \in \mathbb{F}(\alpha)$

Prova: Note que: • $\mathbb{F} \subset \mathbb{F}(\beta)$ e $\mathbb{F}(\beta) \subset \mathbb{F}(\alpha)$

• $[\mathbb{F}(\beta) : \mathbb{F}] = \mathrm{gr}(m_\beta(x))$ e $[\mathbb{F}(\alpha) : \mathbb{F}] = \mathrm{gr}(m_\alpha(x))$

Como

$$\mathrm{gr}(m_\alpha(x)) = [\mathbb{F}(\alpha) : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{F}(\beta)][\mathbb{F}(\beta) : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{F}(\beta)]\,\mathrm{gr}(m_\beta(x))$$

o resultado segue.

Exemplo: Vamos analisar a extensão $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}+\sqrt{5})$. Como no exemplo do slide 7, vemos que $m(x) = x^4 - 16x^2 + 4 \in \mathbb{Q}[x]$ é poli que tem $\sqrt{3}+\sqrt{5}$ como raiz. Eisenstein implica que $m(x)$ é irredutível e portanto minimal de $\sqrt{3}+\sqrt{5}$. Logo,

$$[\mathbb{Q}(\sqrt{3}+\sqrt{5}) : \mathbb{Q}] = 4$$

Por outro lado,

$$[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}],$$

onde já sabemos que $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$

$[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 1 \Rightarrow \mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3}) \Rightarrow [\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ o que é uma contradição pois $\mathbb{Q}(\sqrt{3}+\sqrt{5}) \subset \mathbb{Q}(\sqrt{3},\sqrt{5})$

Logo, $[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2$, pois $x^2 - 5 \in \mathbb{Q}(\sqrt{3})[x]$ é zero em $\sqrt{5}$

Assim, $[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$

Note: $\mathbb{Q}(\sqrt{3},\sqrt{5})$ é $\mathbb{Q}$-esp vet de dimensão 4 e contem o subespaço vet $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ cuja dimensão sobre $\mathbb{Q}$ também é 4. Logo, $\mathbb{Q}(\sqrt{3}+\sqrt{5}) = \mathbb{Q}(\sqrt{3},\sqrt{5})$

Mais ainda, temos que $\{1, \sqrt{3}, \sqrt{5}, \sqrt{3}\sqrt{5}\}$ é base de $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ sobre $\mathbb{Q}$

Exemplo: Vamos analisar a extensão $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{5}, i\sqrt{5})$, onde $\sqrt[3]{5}$ é a raiz cúbica real de 5 (ou seja, a raiz real do poli $x^3 - 5$)

$i\sqrt{5} \notin \mathbb{Q}(\sqrt[3]{5}) \Rightarrow [\mathbb{Q}(\sqrt[3]{5}, i\sqrt{5}) : \mathbb{Q}(\sqrt[3]{5})] = 2$, já que $i\sqrt{5}$ é raiz de $x^2 + 5 \in \mathbb{Q}[x]$

Temos também que $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ (pq?)

Assim, $[\mathbb{Q}(\sqrt[3]{5}, i\sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5}, i\sqrt{5}) : \mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 6$

Por outro lado, $i\sqrt[6]{5}$ é raiz de $x^6 + 5 \in \mathbb{Q}[x]$, que é irredutível por Eisenstein

Logo, $[\mathbb{Q}(i\sqrt[6]{5}) : \mathbb{Q}] = 6$. Como $\mathbb{Q}(i\sqrt[6]{5}) \subset \mathbb{Q}(\sqrt[3]{5}, i\sqrt{5})$, temos $\mathbb{Q}(\sqrt[3]{5}, i\sqrt{5}) = \mathbb{Q}(i\sqrt[6]{5})$

Note: • $\{1, i\sqrt{5}\}$ é base de $\mathbb{Q}(\sqrt[3]{5}, i\sqrt{5})$ sobre $\mathbb{Q}(\sqrt[3]{5})$

• $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$ é base de $\mathbb{Q}(\sqrt[3]{5})$ sobre $\mathbb{Q}$

$\Rightarrow \{1, i\sqrt{5}, \sqrt[3]{5}, (\sqrt[3]{5})^2, i\sqrt[3]{5}\sqrt{5}, i(\sqrt[3]{5})^2\sqrt{5}\}$ é base de $\mathbb{Q}(\sqrt[3]{5}, i\sqrt{5})$ sobre $\mathbb{Q}$

Obs: Esses exemplos mostram que podemos ter extensões simples de $\mathbb{F}$ que a primeira vista são da forma $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$, e sendo assim, parecem ser não simples. Esse também foi o caso de $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ no slide 3

Teorema: Suponha que $\mathbb{F} \subset \mathbb{E}$ seja uma extensão. São equivalentes:

1. A extensão $\mathbb{F} \subset \mathbb{E}$ é finita
2. Existem $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$ algébricos sobre $\mathbb{F}$ tais que $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$
3. Existe uma cadeia de corpos

$$\mathbb{F} \subset \mathbb{F}(\alpha_1) \subset \cdots \subset \mathbb{F}(\alpha_1, \ldots, \alpha_n) = \mathbb{E},$$

onde cada $\mathbb{F}(\alpha_1, \ldots, \alpha_i)$ é algébrico sobre $\mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})$.

Prova: (1) $\Rightarrow$ (2) : Se $\{\alpha_1, \ldots, \alpha_n\}$ é base de $\mathbb{E}$ sobre $\mathbb{F}$, então $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$. De fato, é óbvio que $\mathbb{F}(\alpha_1, \ldots, \alpha_n) \subset \mathbb{E}$, e que qualquer $\mathbb{F}$-combinação linear dos elementos $\alpha_1, \ldots, \alpha_n$ está em $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$. Logo, $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$. Como a extensão $\mathbb{F} \subset \mathbb{E}$ é finita, cada α_i é algébrico sobre $\mathbb{F}$.

(2) $\Rightarrow$ (3) Óbvio

(3) $\Rightarrow$ (1) α_i algébrico sobre $\mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})$

$$\Rightarrow [\mathbb{F}(\alpha_1, \ldots, \alpha_i) : \mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})] = \mathrm{gr}(m_{\alpha_i}(x)),$$

onde $m_{\alpha_i}(x)$ é o poli minimal de α_i em $\mathbb{F}(\alpha_1, \ldots, \alpha_{i-1})[x]$. Logo,

$$[\mathbb{E} : \mathbb{F}] = \mathrm{gr}(m_{\alpha_1}(x)) \cdots \mathrm{gr}(m_{\alpha_n}(x)) < \infty$$

Lista de exercícios:

Cap 21 : 1, 2, 4, 5, 9, 10, 12, 13, 14, 15, 20, 21, 22, 25, 26, 27