

Corpos, Extensões Algébricas e Transcendentes, e Corpos de Decomposição

A partir dessa semana, nosso objetivo será estudar extensões de corpos, como o objetivo de entender as raízes de polinômios definidas neles.

Definição 1. Seja F um corpo. Dizemos que $K \subset F$ é um **subcorpo** de F , se K é um corpo com a restrição das operações de F . Dizemos também, neste caso, que F é uma **extensão** (de corpo) de K .

Notação: $F|K$.

Exemplo 1. $\mathbb{C}|\mathbb{R}$ e $\mathbb{R}|\mathbb{Q}$ são extensões de corpos.

Dada uma extensão $F|K$, observe que F pode ser visto como um $\mathbb{K}$ -espaço vetorial.

Definição 2. O **grau** de uma extensão $F|K$, denotado por $[F : K]$, é definido por $[F : K] := \dim_K(F)$.

Definição 3. Se $[F : K] = n < \infty$ dizemos que $F|K$ é uma extensão **finita** de grau n . Caso contrário, $F|K$ é dita extensão **infinita**.

Observe que $[F : K] = 1$ se, e somente se, $F = K$.

Exemplo 2. $\mathbb{C}|\mathbb{R}$ é uma extensão finita de grau 2 e $\mathbb{R}|\mathbb{Q}$ é uma extensão infinita.

Teorema 4. *Sejam $F|K$ e $K|L$ extensões. Então $[F : L] = [F : K][K : L]$. Além disso, $F|L$ é finita se, e somente se, $F|K$ e $K|L$ são finitas.*

Demonstração. Sejam α uma base de F sobre K e β uma base de K sobre L .

Passo 1: $\gamma = \{\alpha_i \beta_j \mid \alpha_i \in \alpha, \beta_j \in \beta\}$ gera F como espaço vetorial sobre L .

Primeiramente, observe que se $v \in F$, então

$$\begin{aligned} v &= \sum a_i \alpha_i && \text{com } a_i \in K \\ &= \sum_j \sum_i b_{ij} \alpha_i \beta_j && \text{com } b_{ij} \in L. \end{aligned}$$

Logo, γ gera F sobre L .

Passo 2: $\gamma = \{\alpha_i \beta_j \mid \alpha_i \in \alpha, \beta_j \in \beta\}$ é L.I.

De fato, se $\sum_j \sum_i b_{ij} \alpha_i \beta_j = 0$, com $b_{ij} \in L$, temos

$$0 = \sum_j \sum_i b_{ij} \alpha_i \beta_j = \sum_i c_i \alpha_i, \quad \text{com } c_i = \sum_j b_{ij} \beta_j \in K.$$

Como α é base temos $c_i = 0$, para todo i . Assim $0 = c_i = \sum_j b_{ij} \beta_j$. E como β é base segue que $b_{ij} = 0$, para todo i e para todo j . E portanto, γ é base de F sobre L .

Passo 3: $F|L$ é finita se, e somente se, $F|K$ e $K|L$ são finitas.

Como cardinalidade de γ é dada pelo produto das cardinalidades de α e β , segue que

$$[F : L] = \#\gamma = (\#\alpha)(\#\beta) = [F : K][K : L]. \quad (1)$$

Por fim, pela equação (1) se uma das extensões é finita, as outras duas também são. $\square$

Na situação do Teorema 4 temos $L \subset K \subset F$, neste caso, $L \subset K \subset F$ é chamada **torre de extensões de corpos** e K é dito **corpo intermediário** da extensão $F|L$.

Exemplo 3. $\mathbb{R}$ é corpo intermediário da extensão $\mathbb{C}|\mathbb{Q}$.

Definição 5. Um elemento α em alguma extensão do corpo F é dito **algébrico** se existe um polinômio não nulo $f \in F[x]$ tal que $f(\alpha) = 0$. Se α não é algébrico sobre F , dizemos que α é **transcendente** sobre F .

Exemplo 4. 1. $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$.

2. π é transcendente sobre $\mathbb{Q}$, mas é algébrico sobre $\mathbb{R}$.

Definição 6. Seja $F|K$ uma extensão. Se todo elemento de F é algébrico sobre K , dizemos que a extensão é **algébrica**.

Teorema 7. *Se $F|K$ é uma extensão finita, então $F|K$ é algébrica.*

Demonstração. Vamos mostrar que todos os elementos de F são algébricos sobre K .

1. Se $\alpha \in K$, então α é algébrico sobre K , uma vez que é raiz de $p(x) = x - \alpha \in K[x]$.
2. Se $\alpha \in F \setminus K$. Seja $n = \dim_K(F) = n$. Os vetores $1, \alpha, \alpha^2, \dots, \alpha^n \in F$ são $n + 1$ vetores em um espaço de dimensão n , logo são linearmente dependentes. Sendo assim, existem $\beta_0, \beta_1, \dots, \beta_n \in K$, não necessariamente todos nulos, tais que

$$\beta_0 + \beta_1\alpha + \dots + \beta_n\alpha^n = 0,$$

ou seja, α é raiz do polinômio não nulo $f(X) = \beta_0 + \beta_1x + \dots + \beta_nx^n \in K[x]$ e portanto α é algébrico sobre K .

□

Observação 8. Note que em uma extensão $F|K$, se $\alpha \in F$ é algébrico sobre K , então existe $p \in K[x]$ tal que $p(\alpha) = 0$, mas para qualquer outro polinômio $g \in K[x]$ tal que p divide g temos $g(\alpha) = 0$. A definição à seguir nos auxilia à associar um único polinômio $p \in K[x]$ à α .

Definição 9. Seja α algébrico sobre K . O **polinômio irredutível minimal** de α sobre F é o polinômio mônico, irredutível de $K[x]$ que possui α como raiz.

Notação: $\text{irr}(\alpha, K)$, $\text{min}(\alpha, K)$ ou ainda $p_{\alpha/K}(x)$.

Proposição 10. $p_{\alpha/K}(x)$ existe e é único.

Demonstração. Se α é algébrico sobre K , por definição existe $f(x) \in K[x]$, tal que $f(\alpha) = 0$. Se f não é mônico, irredutível e minimal, considere $p \in K[x]$ o fator mônico e irredutível de f tal que $p(\alpha) = 0$. Se existem outros polinômios em $K[x]$ com tais propriedades, tome $h \in K[x]$ para ser o de menor grau dentre eles. Aplicando o algoritmo da divisão, temos:

$$p(x) = h(x)q(x) + r(x), \text{ com } r = 0 \text{ ou } \deg r < \deg h.$$

Aplicando em α , segue que $r(\alpha) = 0$, pela minimalidade de h segue que $r = 0$. Logo pela irredutibilidade de p segue que $p(x) = h(x)$. E segue a unicidade. $\square$

Exemplo 5. $p_{\sqrt{2}/\mathbb{Q}}(x) = x^2 - 2$.

Teorema 11. *Seja α algébrico sobre K e seja n o grau de $p_{\alpha/K}(x)$. Então o espaço vetorial gerado sobre K por $\{1, \alpha, \dots, \alpha^{n-1}\}$ é um corpo.*

Demonstração. Basta mostrarmos que L , o espaço vetorial gerado sobre K por $\{1, \alpha, \dots, \alpha^{n-1}\}$ é corpo. Considere o homomorfismo de anéis dado por

$$\begin{aligned} \varphi : K[x] &\rightarrow L \\ f(x) &\mapsto f(\alpha). \end{aligned}$$

PASSO 1: φ está bem definido.

Utilizando o algoritmo da divisão, temos $f(x) = p_{\alpha/K}(x)q(x) + r(x)$, com $\deg r \leq n - 1$. Logo $f(\alpha) = r(\alpha)$, pois $p_{\alpha/K}(\alpha) = 0$.

PASSO 2: φ é sobrejetiva.

Seja $v \in L$, $v = \sum v_i \alpha^i$. Considere $\sum v_i x^i \in K[x]$.

PASSO 3: $\text{Ker } \varphi = \langle p_{\alpha/K}(x) \rangle$.

Temos então, $\text{Ker } \varphi = \{f \in K[x] \mid f(\alpha) = 0\}$, logo $p_{\alpha/K} \in \text{Ker } \varphi$. Aplicando o algoritmo da divisão à qualquer outro $g \in \text{Ker } \varphi$ e $p_{\alpha/K}$, temos

$$g(x) = p_{\alpha/K}(x)q(x) + r(x), \text{ com } r = 0 \text{ ou } \deg r < \deg p_{\alpha/K}.$$

Aplicando em α , segue que $r(\alpha) = 0$, e pela minimalidade de $p_{\alpha/K}$ segue que $r = 0$. Logo $\text{Ker } \varphi = \langle p_{\alpha/K} \rangle$.

PASSO 4: L é corpo.

Como $\langle p_{\alpha/K} \rangle$ é ideal maximal, uma vez que $p_{\alpha/K}$ é irredutível. Temos que $K[x]/\text{Ker } \varphi$ é corpo.

Pelo teorema do isomorfismo, temos $K[x]/\text{Ker } \varphi \simeq \text{Im } \varphi = L$ e segue o resultado. $\square$

O corpo dado pelo Teorema 11 é o "menor" corpo que contém K e α , tal corpo é denotado por $K(\alpha)$, i.e. não existe um corpo L que contenha α , tal que $K \subset L \subset K(\alpha)$. O corpo $K(\alpha)$ é denominado **corpo de adjunção por α** .

Corolário 12. $[K(\alpha) : K] = n$

Demonstração. Primeiramente vamos mostrar que $\mathcal{B} = \{1, \alpha, \dots, \alpha^{n-1}\}$ é L.I.. De fato, se $\mathcal{B}$ não é L.I., então existem $a_0, \dots, a_{n-1} \in K$ não todos nulos tais que $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} = 0$, ou seja, existiria um polinômio $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$, do qual α é raiz, com $\deg f < n$ o que contraria a minimalidade de $p_{\alpha/K}$. $\square$

Sejam α e β algébricos sobre K , então β é algébrico sobre $K(\alpha)$ e $K(\alpha)(\beta)$ é o "menor" corpo que contém K , α e β . Além disso, pelo Teorema 4, temos

$$[K(\alpha)(\beta) : K] = [K(\alpha)(\beta) : K(\alpha)][K(\alpha) : K].$$

De maneira análoga, obtemos $K(\beta)(\alpha)$, que também é o "menor" corpo que contém K , α e β , ou seja, $K(\alpha)(\beta) = K(\beta)(\alpha)$ e por simplicidade denotaremos tal corpo por $K(\alpha, \beta)$.

Indutivamente se $\alpha_1, \dots, \alpha_r$ são algébricos sobre K , obtemos o corpo $K(\alpha_1, \dots, \alpha_r)$ denominado **corpo obtido por adjunção de $\alpha_1, \dots, \alpha_r$ a K** . E novamente pelo Teorema 4, temos

$$[K(\alpha_1, \dots, \alpha_r) : K] = [K(\alpha_1, \dots, \alpha_r) : K(\alpha_1, \dots, \alpha_{r-1})] \cdots [K(\alpha_1) : K].$$

Formalizando temos o seguinte resultado.

Proposição 13. *Se $\alpha_1, \dots, \alpha_r$ são elementos algébricos sobre K , então $K(\alpha_1, \dots, \alpha_r)|K$ é finita e algébrica. Além disso,*

$$[K(\alpha_1, \dots, \alpha_r) : K] = [K(\alpha_1, \dots, \alpha_r) : K(\alpha_1, \dots, \alpha_{r-1})] \cdots [K(\alpha_1) : K].$$

Exemplo 6. Considere $\mathbb{Q}$ e os números i e $\sqrt{3}$. Vamos determinar o corpo de adjunção $\mathbb{Q}(i, \sqrt{3})$. Por Teorema 11 e Proposição 13, temos

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

Como $p_{\sqrt{3}/\mathbb{Q}}(x) = x^2 - 3$, temos

$$\mathbb{Q}(\sqrt{3}) = \{a_0 + a_1\sqrt{3} \mid a_i \in \mathbb{Q}\} \text{ e } [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2.$$

E ainda, como $p_{i/\mathbb{Q}(\sqrt{3})}(x) = x^2 + 1$, temos

$$\mathbb{Q}(i, \sqrt{3}) = \{b_0 + b_1i \mid b_i \in \mathbb{Q}(\sqrt{3})\} \text{ e } [\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2.$$

Portanto,

$$\mathbb{Q}(i, \sqrt{3}) = \{c_0 + c_1i + c_2\sqrt{3} + c_3i\sqrt{3} \mid c_i \in \mathbb{Q}\} \text{ e } [\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = 4.$$

Observação 14. $\mathbb{Q}(i, \sqrt{3}) \neq \mathbb{Q}(i\sqrt{3})$. De fato, $p_{i\sqrt{3}/\mathbb{Q}}(x) = x^2 + 3$, logo temos

$$\mathbb{Q}(i\sqrt{3}) = \{d_0 + d_1i\sqrt{3} \mid d_i \in \mathbb{Q}\} \text{ e } [\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2.$$

Dado um corpo K , veremos à seguir tipos de extensões relacionadas à decomposição de polinômios de $K[x]$.

Teorema 15 (Kronecker). *Sejam K um corpo e $f \in K[x]$ um polinômio de grau ≥ 1 . Então, existe uma extensão $K \subset L$ onde f possui uma raiz.*

Demonstração. Sem perda de generalidade podemos supor que f é irredutível. Neste caso, o ideal (f) é maximal e $E = \frac{K[x]}{(f)}$ é corpo.

Considerando a injeção canônica
$$\begin{array}{ccc} i : K & \rightarrow & E \\ a & \rightarrow & a + (f) \end{array}$$
, sejam $S = E \setminus i(K)$ e

$L = K \sqcup S$. Vamos mostrar L é corpo.

De fato considere $\varphi : L \rightarrow E$, tal que $\varphi(t) = \begin{cases} t, & t \in S \\ i(t), & t \in K. \end{cases}$

Observe que φ é bijetiva. Logo, dados $t, t' \in L$ definimos:

- $t + t' := \varphi^{-1}(\varphi(t) + \varphi(t'))$;
- $t \cdot t' := \varphi^{-1}(\varphi(t) \cdot \varphi(t'))$.

Com tais operações, é fácil ver que L é corpo, com $K \subset L$. Por fim, seja $\alpha \in L$, tal que $\alpha = \varphi^{-1}(x + (f))$, temos $\alpha \in S$ e segue que

$$\begin{aligned} f(\alpha) &= f(\varphi^{-1}(x + (f))) \\ &= f(x + (f)) \\ &= f(x) + (f) \text{ (Prove!)} \\ &= (f) \\ &= 0_E. \end{aligned}$$

Logo, α é uma raiz de f em L .

□

Definição 16. Sejam K é um corpo e $\Lambda = \{f_j\}_{j \in J}$ uma família de polinômios em $K[x]$, todos de grau ≥ 1 . Um corpo L contendo K é dito **corpo de decomposição** dessa família se todo polinômio $f_j \in \Lambda$ possui todas as raízes.

Seja $L|K$ uma extensão de corpos e $\Lambda = \{f_j\}_{j \in J}$ uma família de polinômios em $K[x]$. Seja Z o conjunto de TODAS as raízes dos polinômios em Λ , e suponha que $Z \subseteq L$. Podemos definir $K(Z)$ como o menor corpo de L que contém Z (tome a interseção de todos os subcorpos de L que contém Z). É fácil ver que $K(Z)$ é corpo de decomposição de Λ .

Exemplo 7. Tomando a família $\Lambda = \{f\}$ constituída por um único polinômio $f(x)$. Então, se $\{\alpha_1, \dots, \alpha_n\}$ são as raízes de f em L o corpo dado pela aplicação do Teorema de Kronecker iteradas vezes, então $L = K(\alpha_1, \dots, \alpha_n)$. Neste caso, L é dito **corpo de decomposição de f** .

Nossa próxima pergunta é a seguinte: Será que é possível encontrar uma extensão de corpo K , onde todos os polinômios com coeficientes em K admitem todas as raízes?

Exemplo 8. É claro que $\mathbb{Q}(\sqrt{2})$ é corpo de decomposição de $f(x) = x^2 - 2$.

Definição 17. Seja K um corpo.

1. K é **algebricamente fechado** se *todo* polinômio $f \in K[x]$ de grau ≥ 1 possui uma raiz em K .
2. Um corpo L é dito um **fecho algébrico** para K se $K \subset L$ é uma extensão algébrica e L é algebricamente fechado. **Notação:** $L = \overline{K}$.

É possível mostrar que todo corpo F possui fecho algébrico.

Teorema 18. *Seja F um corpo. Então, existe uma extensão de corpos $F \subset L$, com L algebricamente fechado.*

Se α e β são duas raízes de um polinômio irredutível $f \in K[x]$, o Teorema de 15 garante que os corpos $K(\alpha)$ e $K(\beta)$ são isomorfos, pois ambos isomorfos ao corpo quociente $\frac{K[x]}{(f)}$. Como veremos à seguir, de maneira mais geral temos o seguinte:

1. dois corpos de decomposição de um polinômio $f \in K[x]$ são isomorfos;
2. dois fechos algébricos de um corpo K também são isomorfos.

Para demonstrar tais fatos vamos relembrar alguns fatos a cerca de homomorfismo de corpos.

Sejam F e L corpos e $\sigma : F \rightarrow L$ um homomorfismo, como $\ker(\sigma)$ é um ideal de F temos que σ é o homomorfismo nulo ou σ é necessariamente injetor. Suporemos, daqui em diante, que homomorfismos de corpos são sempre não nulos.

Lema 19. *Seja $K \subset L$ uma extensão de corpos. Se $\tau : L \rightarrow L$ é um homomorfismo de corpos cuja restrição à K é a identidade (dizemos que τ é um **K -homomorfismo**), então τ é isomorfismo.*

Demonstração. Primeiramente observe que uma vez que τ é K -morfismo, dados $g \in K[x]$ e $\alpha \in L$, temos $\tau(g(\alpha)) = g(\tau(\alpha))$, ou seja, τ "comuta" com os polinômios em $K[x]$.

Dado $\beta \in L$ um elemento qualquer, seja $p(x) = p_{\beta/K}(x)$. Considere o conjunto $R = \{\alpha \in L \mid p(\alpha) = 0\}$, temos $R \neq \emptyset$, pois $\beta \in R$ e $\tau(R) \subset R$. Como R é finito e τ é injetora, temos $\tau(R) = R$, logo existe $\gamma \in R$ tal que $\tau(\gamma) = \beta$, o que prova o lema. $\square$

Observação 20. Nas condições do lemma anterior, observe que se L for um corpo de decomposição de $f \in K[x]$, então um isomorfismo $\tau : L \rightarrow L$ é, essencialmente, uma permutação das raízes de f .

No entanto, nem toda permutação das raízes está associada a um isomorfismo. Por exemplo, seja $K = \mathbb{Q}$ e $f(x) = x^4 - x^2 - 1 \in \mathbb{Q}[x]$, cujas raízes são:

$$\alpha_1 = \sqrt{\frac{1+\sqrt{5}}{2}}, \alpha_2 = -\alpha_1, \alpha_3 = \sqrt{\frac{1-\sqrt{5}}{2}}, \alpha_4 = -\alpha_3.$$

Se algum isomorfismo $\tau : L \rightarrow L$ induzisse a permutação $(\alpha_2 \alpha_3)$, então $0 = \tau(\alpha_1 + \alpha_2) = \alpha_1 + \alpha_3$, o que é absurdo.

Proposição 21. *Sejam $K \subset F$ uma extensão algébrica e $\sigma : K \rightarrow L$ um homomorfismo de corpos, com L algébricamente fechado. Se $F = K(\alpha)$, então existe um homomorfismo de corpos $\tau : F \rightarrow L$, tal que $\tau|_K = \sigma$. O homomorfismo τ é dito uma **extensão** de σ .*

Demonstração. Seja $p(x) = p_{\alpha/K}(x)$. Denotaremos por $f^\sigma \in L[x]$ o polinômio obtido pela aplicação de σ coeficiente à coeficiente. Como L é algébricamente fechado, existe $\beta \in L$ raiz de $p^\sigma \in L[x]$. Vamos definir o homomorfismo de corpos $\tau : K(\alpha) \rightarrow L$, por $\tau(g(\alpha)) = g^\sigma(\beta)$, onde $g(x) \in K[x]$.

Temos τ bem definida, pois se $g(\alpha) = h(\alpha)$ para algum $h(x) \in K[x]$, então α é raiz de $t(x) = g(x) - h(x)$. Portanto, p divide t e por conseguinte, p^σ divide t^σ .

Por fim, observe que $\tau|_K = \sigma$, e segue o resultado. $\square$

De maneira geral, é possível provar o seguinte resultado.

Teorema 22. *Sejam $K \subset F$ uma extensão algébrica e $\sigma : K \rightarrow L$ um homomorfismo de corpos, com L algébricamente fechado. Então existe um homomorfismo de corpos $\tau : F \rightarrow L$, tal que $\tau|_K = \sigma$.*

Como toda extensão finita é algébrica, temos:

Corolário 23. *Sejam $K \subset F$ uma extensão finita e $\sigma : K \rightarrow L$ um homomorfismo de corpos, com L algébricamente fechado. Então existe τ uma extensão de σ .*

Ainda como consequência do Teorema 22, temos:

Teorema 24. *Quaisquer dois fechos algébricos de um corpo K são isomorfos.*

Demonstração. Sejam $\overline{K}$ e $\overline{K}'$ dois fechos algébricos de K . Logo, por definição, $K \subset \overline{K}$ é algébrica. Considere a inclusão $i : K \rightarrow \overline{K}'$, pelo Teorema 22, temos que existe um homomorfismo $\tau : \overline{K} \rightarrow \overline{K}'$ tal que $\tau|_K = i$. Vamos mostrar que τ é sobrejetivo e portanto um isomorfismo.

Dado $\beta \in \overline{K}'$, seja $p(x) = p_{\beta/K} \in K[x]$, com $\deg p = n$. Em $\overline{K}$ temos $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. Logo, para cada α_j , temos

$$0 = \tau(p(\alpha_j)) = p(\tau(\alpha_j)) \in \overline{K}'.$$

Logo, $\tau(\alpha_j)$ é raiz de p em $\overline{K}'$, para todo j . Assim, todas as raízes de $p(x)$ são da forma $\tau(\alpha_j)$. Em particular, como β é raiz de $p(x)$, temos que $\tau(\alpha_j) = \beta$, para algum j , o que conclui nossa demonstração. $\square$

Teorema 25. *Sejam K é um corpo e $f \in K[x]$, de grau maior igual a 1. Quaisquer dois corpos de decomposição de f são isomorfos.*

Demonstração. Sejam $K(\alpha_1, \dots, \alpha_n)$, $K(\beta_1, \dots, \beta_n)$ dois corpos de decomposição de f e sejam K_1 e K_2 os fechos algébricos de K em que eles estão contidos, respectivamente. Pelo Teorema 24 existe um isomorfismo $\varphi : K_1 \rightarrow K_2$, segue que $0 = \varphi(f(\alpha_i)) = f(\varphi(\alpha_i))$ para cada i , ou seja, $\varphi(\alpha_i)$ é raiz de f em K_2 . Como φ é isomorfismo, reordenando se necessário, temos $\varphi(\alpha_i) = \beta_i$ para cada i . Portanto, $\varphi|_{K(\alpha_1, \dots, \alpha_n)} : K(\alpha_1, \dots, \alpha_n) \rightarrow K(\beta_1, \dots, \beta_n)$ é um isomorfismo.

Exercícios

1. Prove que $\mathbb{R}|\mathbb{Q}$ é uma extensão infinita de corpos. (Dica: Se fosse finita, o que poderíamos dizer sobre a cardinalidade de $\mathbb{R}$?)
2. Prove que $\mathbb{Q}[i] \simeq \mathbb{Q}(i)$.
3. Considere $S := \{a + b\sqrt{2} + b\sqrt{3} \mid a, b, c \in \mathbb{Q}\} \subset \mathbb{R}$ e $T := \{a + b\sqrt{2} + b\sqrt{3} + c\sqrt{6} \mid a, b, c \in \mathbb{Q}\} \subset \mathbb{R}$. Mostre que S não possui estrutura de corpo com as operações induzidas de $\mathbb{R}$, mas que T possui tal estrutura. Adicionalmente, calcule a dimensão de T como $\mathbb{Q}$ -espaço vetorial.
4. Calcule o grau da extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$. Existe uma relação entre $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ e T do exercício anterior?
5. Podem existir corpos K, L, M tais que $\mathbb{Q} \subseteq K \subseteq M$ e $\mathbb{Q} \subseteq L \subseteq M$ tais que $[K : \mathbb{Q}] = 3$, $[L : \mathbb{Q}] = 4$, $[M : L] = 5$ e $[M : K] = 7$?
6. Prove que $\sqrt{3}$ não está contido em $\mathbb{Q}(\sqrt[5]{3})$.
7. Seja $E|K$ uma extensão de corpos, e $\beta \in E$ um elemento transcendente. Prove que $K[x] \simeq K[\beta]$, como anéis.
8. Determine quais extensões a seguinte nos dão corpos de decomposição.
 - a) $\mathbb{Q} \subseteq \mathbb{C}$ para o polinômio $x^2 + 1 \in \mathbb{Q}[x]$.
 - b) $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$.
 - c) $\mathbb{Q} \subseteq \mathbb{Q}[i\sqrt[4]{5}]$ para o polinômio $x^4 - 5$.
9. Prove que os polinômios $(x^2 - 2x - 2)(x^2 + 1)$ e $x^5 - 3x^3 + x^2 - 3$ possuem corpos de decomposição isomorfos sobre $\mathbb{Q}$. Calcule o grau da extensão do corpo de decomposição e $\mathbb{Q}$.

□