7. Extensão separável (Parte II)

7.1. **Polinômio inseparável.** Começaremos mostrando a existência de polinômios irredutíveis não separáveis (e, portanto, a existência de uma extensão não separável).

Lema 7.1. *Sejam $\mathbb{F}$ um corpo de característica $p > 0$, $a \in \mathbb{F}$, e $f = X^p - a$. Então, ou f é irredutível sobre $\mathbb{F}$, ou f possui raiz em $\mathbb{F}$ (tal raiz tem multiplicidade p).*

Demonstração. Assuma que $X^p - a$ não é irredutível em $\mathbb{F}[X]$. Portanto, existe $g \in \mathbb{F}[X]$, com $1 \leq \mathrm{gr}(g) < p$, tal que $X^p - a = g(X)h(X)$, para algum $h \in \mathbb{F}[X]$. Seja $\Omega = \bar{\mathbb{F}}$ o fecho algébrico de $\mathbb{F}$, e seja $b \in \Omega$ uma raiz de f. Daí $b^p = a$. Portanto,

$$f = X^p - a = X^p - b^p = (X - b)^p.$$

Assim, todas as raízes de f são repetidas, e iguais a b. Daí, o mesmo vale para g. Assim, $g = (X - b)^m$, para algum $1 \leq m < p$. Portanto, $b^m \in \mathbb{F}$. Além disso, $a = b^p \in \mathbb{F}$ também. Como $\mathrm{mdc}(m, p) = 1$, existem $r, s \in \mathbb{Z}$ tais que $mr + ps = 1$. Portanto,

$$\mathbb{F} \ni (b^m)^r (b^p)^s = b^{mr+ps} = b.$$

Assim, f admite uma raiz em $\mathbb{F}$ de multiplicidade p. □

Corolário 7.2. *Seja $\mathbb{F}$ um corpo não perfeito de característica $p > 0$, e seja $a \in \mathbb{F} \setminus \mathbb{F}^p$. Então $X^p - a$ é um polinômio irredutível em $\mathbb{F}[X]$ e não separável.* □

7.2. **Grau separável e monomorfismos.** Sejam $\mathbb{E}/\mathbb{F}$ uma extensão, Ω um corpo, e $\sigma_0 : \mathbb{F} \to \Omega$ um monomorfismo. Denota-se

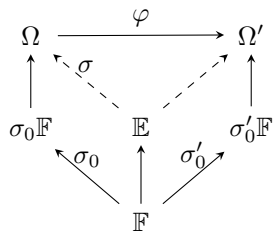
$$\mathrm{Mono}_{\sigma_0}(\mathbb{E}, \Omega) = \{\sigma : \mathbb{E} \to \Omega \text{ extensão de } \sigma_0\}.$$

No caso especial em que $\mathbb{F} \subseteq \Omega$, e $\sigma : \mathbb{F} \to \Omega$ é a função identidade, então denotamos $\mathrm{Mono}_{\sigma}(\mathbb{E}, \Omega)$ por $\mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega)$.

Lema 7.3. *Sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos, Ω, Ω' corpos algebricamente fechados, e $\sigma_0 : \mathbb{F} \to \Omega$ e $\sigma_0' : \mathbb{F} \to \Omega'$ monomorfismos. Assuma que $\Omega/\sigma_0\mathbb{F}$ e $\Omega'/\sigma_0'\mathbb{F}$ são extensões algébricas. Então*

$$|\mathrm{Mono}_{\sigma_0}(\mathbb{E}, \Omega)| = |\mathrm{Mono}_{\sigma_0'}(\mathbb{E}, \Omega')|.$$

Demonstração. Temos um monomorfismo de corpos $\sigma_0' \circ \sigma_0^{-1} : \sigma_0\mathbb{F} \to \sigma_0'\mathbb{F} \hookrightarrow \Omega'$. Portanto, por Proposição 3.7, existe um monomorfismo $\varphi : \Omega \to \Omega'$ que estende $\sigma_0' \circ \sigma_0^{-1}$. Como Ω é algebricamente fechado, segue que φ é um isomorfismo. Seja $\sigma \in \mathrm{Mono}_{\sigma_0}(\mathbb{E}, \Omega)$.



Seja $\sigma' : \mathbb{E} \to \Omega'$, definida por $\sigma' = \varphi \circ \sigma$. Dado $\alpha \in \mathbb{F}$, temos que

$$\sigma'(\alpha) = \varphi \circ \sigma(\alpha) = \varphi(\underbrace{\sigma_0(\alpha)}_{\in \sigma_0\mathbb{F}}) = \sigma_0' \circ \sigma_0^{-1}(\sigma_0(\alpha)) = \sigma_0'(\alpha).$$

Portanto, σ' estende σ_0'. Daí, obtemos um mapa $\sigma \in \mathrm{Mono}_{\sigma_0}(\mathbb{E}, \Omega) \mapsto \sigma' \in \mathrm{Mono}_{\sigma_0'}(\mathbb{E}, \Omega')$. Da mesma forma, dado $\sigma' \in \mathrm{Mono}_{\sigma_0'}(\mathbb{E}, \Omega')$, temos que $\varphi^{-1} \circ \sigma' \in \mathrm{Mono}_{\sigma_0}(\mathbb{E}, \Omega)$; e um mapa é o inverso do outro. Portanto, existe uma bijeção entre os conjuntos. Então, vale que $|\mathrm{Mono}_{\sigma_0}(\mathbb{E}, \Omega)| = |\mathrm{Mono}_{\sigma_0'}(\mathbb{E}, \Omega')|$. □

O lema anterior justifica que a próxima definição está bem definida.

Definição 7.4. Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica de corpos, e Ω um corpo algebricamente fechado contendo $\mathbb{F}$. O *grau separável* da extensão $\mathbb{E}/\mathbb{F}$ é

$$[\mathbb{E} : \mathbb{F}]_s := |\mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega)|.$$

Considere uma extensão de corpos algébrica e simples $\mathbb{E} = \mathbb{F}(a)$. Então, já vimos (Proposição 3.6) que $|\mathrm{Mono}_{\mathbb{F}}(\mathbb{F}(a), \Omega)|$ coincide com a quantidade distinta de raízes de $\mathrm{Irr}(a, \mathbb{F})$. Portanto, vale que $[\mathbb{F}(a) : \mathbb{F}]_s = [\mathbb{F}(a) : \mathbb{F}]$ se, e somente se, a é separável sobre $\mathbb{F}$. Os próximos resultados provarão que tal afirmação vale para uma extensão finita qualquer $\mathbb{E}/\mathbb{F}$.

Proposição 7.5. *Sejam $\mathbb{L}/\mathbb{E}/\mathbb{F}$ extensões algébricas de corpos. Então*

$$[\mathbb{L} : \mathbb{F}]_s = [\mathbb{L} : \mathbb{E}]_s [\mathbb{E} : \mathbb{F}]_s.$$

Além disso, se $\mathbb{E}/\mathbb{F}$ é finita, então $[\mathbb{E} : \mathbb{F}]_s \leq [\mathbb{E} : \mathbb{F}]$.

Demonstração. Seja $\{\sigma_i\}$ o conjunto dos $\mathbb{F}$-monomorfismos $\mathbb{E} \to \Omega$. Tal conjunto tem cardinalidade $[\mathbb{E} : \mathbb{F}]_s$. Cada um dos σ_i admite $[\mathbb{L} : \mathbb{E}]_s$ extensões $\bar{\sigma}_{ij} : \mathbb{L} \to \Omega$. Todos os monomorfismos $\bar{\sigma}_{ij}$ são distintos, e construímos um total de $[\mathbb{L} : \mathbb{E}]_s [\mathbb{E} : \mathbb{F}]_s$ monomorfismos. Além disso, se $\sigma : \mathbb{L} \to \Omega$ é um $\mathbb{F}$-monomorfismo, então σ é uma extensão da sua restrição $\sigma|_{\mathbb{E}} : \mathbb{E} \to \Omega$. Portanto, tal σ coincide com algum $\bar{\sigma}_{ij}$. Assim, provamos a fórmula $[\mathbb{L} : \mathbb{F}]_s = [\mathbb{L} : \mathbb{E}]_s [\mathbb{E} : \mathbb{F}]_s$.

Agora, assuma que $\mathbb{E} = \mathbb{F}(a_1, \ldots, a_m)$. Da Proposição 3.6, temos que o número de $\mathbb{F}$-monomorfismos $\mathbb{F}(a_1) \to \Omega$ é igual ao número de raízes distintas de $\mathrm{Irr}(a_1, \mathbb{F})$. Portanto, vale que $[\mathbb{F}(a_1) : \mathbb{F}]_s \leq [\mathbb{F}(a_1) : \mathbb{F}]$. Assumindo, por indução, que $[\mathbb{F}(a_1)(a_2, \ldots, a_m) : \mathbb{F}(a_1)]_s \leq [\mathbb{F}(a_1)(a_2, \ldots, a_m) : \mathbb{F}(a_1)]$, obtemos

$$\begin{aligned}[\mathbb{E} : \mathbb{F}]_s &= [\mathbb{F}(a_1)(a_2, \ldots, a_m) : \mathbb{F}(a_1)]_s [\mathbb{F}(a_1) : \mathbb{F}]_s \\ &\leq [\mathbb{F}(a_1)(a_2, \ldots, a_m) : \mathbb{F}(a_1)][\mathbb{F}(a_1) : \mathbb{F}] = [\mathbb{E} : \mathbb{F}].\end{aligned}$$

□

Teorema 7.6. *Sejam $\mathbb{F}$ um corpo, e $\mathbb{E} = \mathbb{F}(a_1, \ldots, a_m)$ uma extensão finita de $\mathbb{F}$. As seguintes afirmações são equivalentes:*

(i) *$\mathbb{E}/\mathbb{F}$ é uma extensão separável,*
(ii) *os elementos $a_1, \ldots, a_m$ são separáveis sobre $\mathbb{F}$,*
(iii) *$[\mathbb{E} : \mathbb{F}]_s = [\mathbb{E} : \mathbb{F}]$.*

Demonstração. $(i) \Rightarrow (ii)$: A extensão $\mathbb{E}/\mathbb{F}$ é separável. Assim, por definição, os elementos $a_1, \ldots, a_m$ são separáveis sobre $\mathbb{F}$.
$(ii) \Rightarrow (iii)$: Assuma, por indução, que dado $i \geq 0$, vale $[\mathbb{F}(a_1, \ldots, a_i) : \mathbb{F}]_s = [\mathbb{F}(a_1, \ldots, a_i) : \mathbb{F}]$. Sendo a_{i+1} separável sobre $\mathbb{F}$, segue que a_{i+1} é raiz de um polinômio separável em $\mathbb{F}[X] \subseteq \mathbb{F}(a_1, \ldots, a_i)[X]$. Portanto, a_{i+1} é separável sobre $\mathbb{F}(a_1, \ldots, a_i)$. Da Proposição 3.6, o número de $\mathbb{F}(a_1, \ldots, a_i)$-monomorfismos $\mathbb{F}(a_1, \ldots, a_i)(a_{i+1}) \to \Omega$ é igual a quantidade de raízes distintas do polinômio minimal de a_{i+1} sobre $\mathbb{F}(a_1, \ldots, a_i)$. Como o elemento é separável, segue que

$[\mathbb{F}(a_1,\ldots,a_i)(a_{i+1}):\mathbb{F}(a_1,\ldots,a_i)]_s = [\mathbb{F}(a_1,\ldots,a_i)(a_i):\mathbb{F}(a_1,\ldots,a_i)]$. Portanto, por indução e da Proposição 7.5, vale que

$$\begin{aligned}[\mathbb{F}(a_1,\ldots,a_i,a_{i+1}):\mathbb{F}]_s &= [\mathbb{F}(a_1,\ldots,a_i)(a_{i+1}):\mathbb{F}(a_1,\ldots,a_i)]_s[\mathbb{F}(a_1,\ldots,a_i):\mathbb{F}]_s \\ &= [\mathbb{F}(a_1,\ldots,a_i)(a_{i+1}):\mathbb{F}(a_1,\ldots,a_i)][\mathbb{F}(a_1,\ldots,a_i):\mathbb{F}] \\ &= [\mathbb{F}(a_1,\ldots,a_i,a_{i+1}):\mathbb{F}]\end{aligned}$$

$(iii) \Rightarrow (i)$: Assuma que a extensão $\mathbb{E}/\mathbb{F}$ não é separável. Então, existe um elemento $a \in \mathbb{E}$ que não é separável sobre $\mathbb{F}$. Da Proposição 3.6, obtemos que $[\mathbb{F}(a):\mathbb{F}]_s < [\mathbb{F}(a):\mathbb{F}]$. Da Proposição 7.5, vale que $[\mathbb{E}:\mathbb{F}(a)]_s \leq [\mathbb{E}:\mathbb{F}(a)]$. Portanto, novamente da Proposição 7.5, obtemos que

$$[\mathbb{E}:\mathbb{F}]_s = [\mathbb{E}:\mathbb{F}(a)]_s[\mathbb{F}(a):\mathbb{F}]_s < [\mathbb{E}:\mathbb{F}(a)][\mathbb{F}(a):\mathbb{F}] = [\mathbb{E}:\mathbb{F}].$$

Assim, $[\mathbb{E}:\mathbb{F}]_s \neq [\mathbb{E}:\mathbb{F}]$. □

Corolário 7.7. *Sejam $\mathbb{E} = \mathbb{F}(S)$ uma extensão de corpos. Então $\mathbb{E}/\mathbb{F}$ é separável se, e somente se, todo $a \in S$ é separável sobre $\mathbb{F}$.*

Demonstração. Se $\mathbb{E}/\mathbb{F}$ é separável, então, por definição, todo $a \in S$ é separável sobre $\mathbb{F}$. Reciprocamente, seja $a \in \mathbb{F}(S)$. Então, existem $a_1,\ldots,a_m \in S$ tais que $a \in \mathbb{F}(a_1,\ldots,a_m)$. Por hipótese, os elementos $a_1,\ldots,a_m$ são separáveis sobre $\mathbb{F}$. Assim, do teorema anterior, a extensão $\mathbb{F}(a_1,\ldots,a_m)/\mathbb{F}$ é separável. Portanto, o elemento $a \in \mathbb{F}(a_1,\ldots,a_m)$ é separável sobre $\mathbb{F}$. Como a afirmação vale para todo $a \in \mathbb{F}(S)$, segue que a extensão $\mathbb{F}(S)/\mathbb{F}$ é separável. □

Utilizando as propriedades do grau separável, pode-se provar que as extensões separáveis formam uma classe boa de extensões:

Corolário 7.8. *Sejam $\mathbb{L}/\mathbb{E}/\mathbb{F}$ extensões de corpos. Então $\mathbb{L}/\mathbb{F}$ é separável se, e somente se, $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ são separáveis.*

Demonstração. Assuma que $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ são separáveis e finitos. Combinando Teorema 7.6 e Proposição 7.5, obtemos.

$$[\mathbb{L}:\mathbb{F}]_s = [\mathbb{L}:\mathbb{E}]_s[\mathbb{E}:\mathbb{F}]_s = [\mathbb{L}:\mathbb{E}][\mathbb{E}:\mathbb{F}] = [\mathbb{L}:\mathbb{F}].$$

Portanto, novamente do Teorema 7.6, obtemos que $\mathbb{L}/\mathbb{F}$ é separável. Agora, assuma que as extensões $\mathbb{L}/\mathbb{E}$ e $\mathbb{EF}$ são separáveis, mas não necessariamente são finitas. Seja $a \in \mathbb{L}$. Então, como a é separável sobre $\mathbb{E}$, $\mathrm{Irr}(a,\mathbb{E}) = b_0 + b_1X + \cdots + b_mX^m \in \mathbb{E}[X]$ é um polinômio separável. Como $\mathrm{Irr}(a,\mathbb{E}) \in \mathbb{F}(b_0,b_1,\ldots,b_m)[X]$, segue que a é separável sobre $\mathbb{F}(b_0,\ldots,b_m)$. Portanto, a extensão $\mathbb{F}(b_0,\ldots,b_m,a)/\mathbb{F}(b_0,\ldots,b_m)$ é separável. Ainda, como a extensão $\mathbb{E}/\mathbb{F}$ é separável, os elementos $b_0,\ldots,b_m$ são separáveis sobre $\mathbb{F}$. Portanto, do Teorema 7.6, obtemos que $\mathbb{F}(b_0,\ldots,b_m)/\mathbb{F}$ é uma extensão separável. Do caso finito provado no início da demonstração, segue que $\mathbb{F}(b_0,\ldots,b_m,a)/\mathbb{F}$ é separável. Portanto, a é separável sobre $\mathbb{F}$. Sendo a afirmação válida para todo $a \in \mathbb{L}$, obtemos que a extensão $\mathbb{L}/\mathbb{F}$ é separável.

Reciprocamente, assuma que $\mathbb{L}/\mathbb{F}$ é separável. Assim, para todo $a \in \mathbb{E} \subseteq \mathbb{L}$, vale que $\mathrm{Irr}(a,\mathbb{F})$ é um polinômio separável. Portanto, $\mathbb{E}/\mathbb{F}$ é separável. Agora, se $a \in \mathbb{L}$, então a satisfaz o polinômio separável $\mathrm{Irr}(a,\mathbb{F}) \in \mathbb{F}[X] \subseteq \mathbb{E}[X]$. Portanto, a é separável sobre $\mathbb{E}$. Daí $\mathbb{L}/\mathbb{E}$ é separável. □

Corolário 7.9. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita de corpos. Então $\mathbb{E}/\mathbb{F}$ é separável e normal se, e somente se, $|\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = [\mathbb{E}:\mathbb{F}]$.*

Demonstração. Do Teorema 7.6, a extensão $\mathbb{E}/\mathbb{F}$ é separável se, e somente se, $[\mathbb{E} : \mathbb{F}] = |\mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega)|$. Como consequência do Teorema 5.5, a extensão $\mathbb{E}/\mathbb{F}$ é normal se, e somente se, $|\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = |\mathrm{Mono}_{\mathbb{F}}(\mathbb{F}, \Omega)|$. Portanto, se a extensão $\mathbb{E}/\mathbb{F}$ é separável e normal, vale que $|\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$. Reciprocamente, da Proposição 7.5 e da discussão que precede Teorema 5.5, vale que $|\mathrm{Aut}(\mathbb{E}/\mathbb{F})| \leq |\mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega)| \leq [\mathbb{E} : \mathbb{F}]$. Portanto, a igualdade $|\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$ implica também que essas quantidades coincidem com $|\mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega)|$. Usando as equivalências enunciadas nas duas primeiras frases, obtemos que $\mathbb{E}/\mathbb{F}$ é normal e separável. □

Estaremos interessados nas extensões finitas que são normal e separável. Daremos um nome especial para tais extensões:

Definição 7.10. Uma extensão de corpos $\mathbb{E}/\mathbb{F}$ é dita ser *galoisiana* (ou de Galois) se a extensão é separável e normal.

7.3. **Teorema do Elemento Primitivo.** Relembre que uma extensão de corpos $\mathbb{E}/\mathbb{F}$ é dita ser simples se existe $a \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(a)$. Um tal elemento a é denominado um *elemento primitivo*. Os próximos resultados concernem determinar condições para que uma extensão finita de corpos seja simples. Tais resultados são conhecidos como Teorema do Elemento Primitivo.

Começaremos com o caso de corpo finito. Para isso, precisamos de um resultado que envolve somente teoria de grupos.

Lema 7.11. *Seja G um grupo abeliano finito, e assuma que, pra todo d dividindo $|G|$, $|\{x \in G \mid x^d = 1\}| \leq d$. Então G é cíclico.*

Demonstração. Exercício (ou, encontre e leia uma demonstração). □

Proposição 7.12. *Seja $\mathbb{F}$ um corpo finito. Então uma extensão de corpos $\mathbb{E}/\mathbb{F}$ finita é simples.*

Demonstração. Seja $G = \mathbb{E}^\times$ o grupo multiplicativo do corpo. Então, para cada d dividindo $|G|$, $\{x \in G \mid x^d = 1\}$ é o conjunto das raízes do polinômio $X^d - 1$. O último possui no máximo d raízes. Portanto, pelo lema anterior, $\mathbb{E}^\times$ é cíclico, ou seja, $\mathbb{E}^\times = \langle\gamma\rangle$. Portanto, vale que $\mathbb{E} = \mathbb{F}[\gamma]$. □

Obs. A proposição anterior também prova que o grupo multiplicativo de um corpo finito é cíclico.

O próximo resultado é o enunciado mais geral no sentido de existência de um elemento primitivo.

Teorema 7.13. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita de corpos. Então $\mathbb{E}/\mathbb{F}$ é simples se, e só se, existe um número finito de corpos entre $\mathbb{F}$ e $\mathbb{E}$.*

Demonstração. Se $\mathbb{F}$ é finito e $\mathbb{E}/\mathbb{F}$ é uma extensão finita, então o corpo $\mathbb{E}$ também é finito. Portanto, é verdade que existe um número finito de corpos entre $\mathbb{F}$ e $\mathbb{E}$ (pois, existe um número finito de subconjuntos). Da Proposição 7.12, segue que a extensão também é simples. Portanto, o enunciado do teorema é válido para corpos finitos. Assuma então que $\mathbb{F}$ é um corpo infinito.

Assuma que existe um número finito de corpos entre $\mathbb{F}$ e $\mathbb{E}$. É suficiente provar que o resultado é válido para $\mathbb{E} = \mathbb{F}(a_1, a_2)$. De fato, assumindo que provamos pra tal caso, e por indução, obtemos

$$\mathbb{E} = \mathbb{F}(a_1, a_2, \ldots, a_m) = \mathbb{F}(c, a_3, \ldots, a_m) = \mathbb{F}(c').$$

Considere os corpos $\mathbb{F}(a_1 + \lambda a_2)$, com $\lambda \in \mathbb{F}$. Como $\mathbb{F}$ é infinito, temos uma família infinita de corpos. Mas, como existe um número finito de corpos entre $\mathbb{F}$ e $\mathbb{E}$, podemos encontrar $\lambda \neq \lambda'$ de modo que $\mathbb{F}(a_1 + \lambda a_2) = \mathbb{F}(a_1 + \lambda' a_2)$. Assim, $a_1 + \lambda' a_2 \in \mathbb{F}(a_1 + \lambda a_2)$. Daí

$$\mathbb{F}(a_1 + \lambda a_2) \ni \frac{1}{\lambda - \lambda'} \left((a_1 + \lambda a_2) - (a_1 + \lambda' a_2) \right) = a_2.$$

Isso implica que $\mathbb{F}(a_1 + \lambda a_2) \ni (a_1 + \lambda a_2) - \lambda a_2 = a_1$. Portanto, $\mathbb{F}(a_1, a_2) \subseteq \mathbb{F}(a_1 + \lambda a_2)$. Por outro lado, $a_1 + \lambda a_2 \in \mathbb{F}(a_1, a_2)$. Então, $\mathbb{F}(a_1 + \lambda a_2) \subseteq \mathbb{F}(a_1, a_2)$. Daí vale a igualdade, provando o que queria.

Reciprocamente, assuma que $\mathbb{E} = \mathbb{F}(a)$. Provaremos que o número de corpos intermediários é menor ou igual ao número de divisores mônicos de $\mathrm{Irr}(a, \mathbb{F})$. Seja $\mathbb{L}$ um corpo intermediário, ou seja, $\mathbb{E}/\mathbb{L}/\mathbb{F}$. Sabe-se que $\mathrm{Irr}(a, \mathbb{L})$ divide $\mathrm{Irr}(a, \mathbb{F})$. Portanto, temos um mapa

$$\Psi : \{\mathbb{L} \mid \mathbb{E}/\mathbb{L}/\mathbb{F}\} \to (\text{divisores mônicos de } \mathrm{Irr}(a, \mathbb{F}))$$
$$\Psi(\mathbb{L}) = \mathrm{Irr}(a, \mathbb{L}).$$

Denote por $\mathrm{Irr}(a, \mathbb{L}) = b_0 + b_1 X + \cdots + b_s X^s$, e seja $\mathbb{L}' = \mathbb{F}(b_0, b_1, \ldots, b_s)$. Como $b_0, \ldots, b_s \in \mathbb{L}$, temos que $\mathbb{L}' \subseteq \mathbb{L}$. Além disso, $\mathrm{Irr}(a, \mathbb{L}) \in \mathbb{L}'[X]$. Como $\mathbb{L}' \subseteq \mathbb{L}$, a redutibilidade de $\mathrm{Irr}(a, \mathbb{L})$ em $\mathbb{L}'[X]$ implicaria na redutibilidade do mesmo em $\mathbb{L}[X]$. Portanto, $\mathrm{Irr}(a, \mathbb{L}) = \mathrm{Irr}(a, \mathbb{L}')$. Isso implica que $[\mathbb{E} : \mathbb{L}] = [\mathbb{E} : \mathbb{L}']$. Assim, como

$$[\mathbb{E} : \mathbb{L}'] = [\mathbb{E} : \mathbb{L}][\mathbb{L} : \mathbb{L}'],$$

segue que $[\mathbb{L} : \mathbb{L}'] = 1$, ou seja, $\mathbb{L} = \mathbb{L}'$. Isso implica que a função Ψ é injetiva. Como o conjunto de divisores mônicos de $\mathrm{Irr}(a, \mathbb{F})$ é finita (pois $\mathbb{F}[X]$ é domínio de fatoração única), segue que o conjunto dos corpos intermediários entre $\mathbb{F}$ e $\mathbb{E}$ é finito. □

Teorema 7.14. *Seja $\mathbb{E} = \mathbb{F}[a_1, a_2, \ldots, a_m]$ uma extensão finita, em que $a_2, \ldots, a_m$ são separáveis sobre $\mathbb{F}$ (a_1 não precisa ser separável sobre $\mathbb{F}$). Então $\mathbb{E}/\mathbb{F}$ é simples.*

Demonstração. Repetindo as considerações iniciais da demonstração do teorema anterior, podemos nos restringir no caso em que $\mathbb{F}$ é infinito, e $\mathbb{E} = \mathbb{F}(a, b)$, em que b é separável sobre $\mathbb{F}$. Sejam p_a e p_b os polinômios minimais de a e b sobre $\mathbb{F}$, respectivamente. Seja Ω um fecho algébrico de $\mathbb{F}$, $a_1 = a, a_2, \ldots, a_r \in \Omega$ as raízes de p_a, e $b_1 = b, b_2, \ldots, b_s \in \Omega$ as raízes de p_b. Como p_b é separável, temos que $p_b = (X - b)(X - b_2) \cdots (X - b_s)$.

Para cada i, j, em que $(i, j) \neq (1, 1)$, defina $f_{ij} = (a - a_i) + (b - b_j)X$. Como $\mathbb{F}$ é infinito, existe $\gamma \in \mathbb{F}$ tal que $f_{ij}(\gamma) \neq 0$, para todo i, j. Como $a + \gamma b \in \mathbb{F}(a, b)$, temos que $\mathbb{F}(a + \gamma b) \subseteq \mathbb{F}(a, b)$. Provaremos que vale a inclusão contrária. Defina o polinômio

$$g(X) = p_a(a + \gamma b - \gamma X) \in \mathbb{F}(a + \gamma b)[X].$$

Temos que $g(b) = p_a(a) = 0$. Além disso, se $j \neq 1$ e dado qualquer i, então $0 \neq f_{ij}(\gamma) = a_i - a + b_j\gamma - b\gamma$. Portanto,

$$a_i \neq a + b\gamma - b_j\gamma.$$

Daí, $g(b_j) = p_a(a + b\gamma - b_j\gamma) \neq 0$, pois as únicas raízes de p_a são $a_1, \ldots, a_r$. Assim, a única raiz comum em Ω de $g(X)$ e p_b é b. Então, calculando em $\Omega[X]$, vale que $\mathrm{mdc}(g, p_b) = X - b$. Por outro lado, o mdc entre polinômios é independente de extensão de corpos. Portanto, $\mathrm{mdc}(g, p_b) = X - b$ em $\mathbb{F}(a + \gamma b)[X]$. Assim,

obtemos que $b \in \mathbb{F}(a+\gamma b)$. Daí, $\mathbb{F}(a+\gamma b) \ni (a+\gamma b) - \gamma b = a$. Conclui-se então que $\mathbb{F}(a,b) \subseteq \mathbb{F}(a+\gamma b)$. Isso termina a prova do teorema. □

É interessante listarmos alguns casos especiais em que uma extensão finita é simples:

Corolário 7.15. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita. Então:*

(i) *Se $\mathbb{E}/\mathbb{F}$ é separável, então $\mathbb{E}/\mathbb{F}$ é simples.*
(ii) *Se $\mathbb{F}$ é perfeito, então $\mathbb{E}/\mathbb{F}$ é simples.*
(iii) *Se $\operatorname{car}\mathbb{F} = 0$, então $\mathbb{E}/\mathbb{F}$ é simples.*
(iv) *Se $\mathbb{F}$ é finito, então $\mathbb{E}/\mathbb{F}$ é simples.*

Demonstração. O (i) é um caso particular do Teorema 7.14. Os items (iii) e (iv) são um caso particular de (ii), pois todo corpo de característica zero e todo corpo finito são perfeitos. Para (ii), seja $\mathbb{E}/\mathbb{F}$ uma extensão finita, em que $\mathbb{F}$ é perfeito. Então, a mesma é algébrica. Portanto, do Teorema 6.12, segue que a extensão é separável. Daí, o resultado segue de (i). □