MAT0364–MAT6643
Teoria de Galois

fyyasumura@ime.usp.br
IME–USP
2021

Conteúdo

Prefácio

Tais notas foram originadas do curso Teoria de Galois, ministrado no primeiro semestre de 2021, para o curso de Bacharelado em Matemática do IME–USP.

As referências principais são:

[1] O. Endler, *Teoria de Corpos*
[2] S. Lang, *Algebra*
[3] N. Jacobson, *Basic Algebra I*
[4] Notas de aula da Professora Lucia Ikemoto Murakami.
[5] Notas de aula do Professor Paulo Roberto Brumatti.

0. Revisão: Anel de polinômios

Seja $\mathcal{A}$ um anel (comutativo com 1). Considere o conjunto de todas as sequências

$$(a_0, a_1, a_2, \ldots), \quad a_i \in \mathcal{A},$$

em que no máximo um número finito dos a_i é diferente de 0. Podemos definir as seguintes operações:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_0 + b_2, \ldots),$$
$$(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots),$$

em que

$$c_m = \sum_{i+j=m} a_i b_j, \quad m = 0, 1, 2, \ldots$$

Defina

$$1 := (1, 0, 0, \ldots), \quad X = (0, 1, 0, 0, \ldots).$$

Então

$$\mathcal{A} \cong \{(a, 0, 0, \ldots) \mid a \in \mathcal{A}\} = \{a \cdot 1 \mid a \in \mathcal{A}\},$$

$$X^m = (\underbrace{0, 0, \ldots, 0}_{m \text{ zeros}}, 1, 0, 0, \ldots).$$

Daí, um elemento pode ser escrito da seguinte forma:

$$(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots) = a_0 \cdot 1 + a_1 \cdot X + a_2 \cdot X^2 + \cdots + a_n \cdot X^n.$$

Denota-se tal anel por $\mathcal{A}[X]$ (anel de polinômios em 1 variável com coeficientes no anel $\mathcal{A}$).

Definição 0.1. Dado $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathcal{A}[X]$, com $a_n \neq 0$, dizemos que:

(i) $n = \text{gr}(f)$ é o grau do polinômio,
(ii) a_n é o coeficiente líder,
(iii) dizemos que f é *mônico* se $a_n = 1$.

Lema 0.2. *(a) Se $\mathcal{A}$ é domínio, então* $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.
(b) O anel $\mathcal{A}$ é domínio se, e só se, $\mathcal{A}[X]$ é domínio. □

Definição 0.3. Seja $\mathbb{F}$ um corpo.

(i) Sejam $f, g \in \mathbb{F}[X]$. Dizemos que g divide f se existe $h \in \mathbb{F}[X]$ tal que $f = gh$.
(ii) f é dito ser *irredutível* se $f = gh$, com $g, h \in \mathbb{F}[X]$ implica em $g \in \mathbb{F}$ ou $h \in \mathbb{F}$.

Teorema 0.4. *Seja $\mathbb{F}$ um corpo. Dados $f, g \in \mathbb{F}[X]$, com $g \neq 0$, existem $q, r \in \mathbb{F}[X]$, com $r = 0$ ou $\mathrm{gr}(r) < \mathrm{gr}(g)$, tais que*

$$f(X) = q(X)g(X) + r(X).$$

□

Lema 0.5. *Sejam $f \in \mathbb{F}[X]$ e $\alpha \in \mathbb{F}$. Então $f(\alpha) = 0$ se, e somente se, $(X - \alpha)$ divide f.* □

Todo ideal de $\mathbb{F}[X]$ é principal, isto é, se $I \subseteq \mathbb{F}[X]$ é um ideal, então existe $f(X) \in \mathbb{F}[X]$ tal que

$$I = (f) = f(X) \cdot \mathbb{F}[X] = \{fg \mid g \in \mathbb{F}[X]\}.$$

Se escolhermos f mônico, então o gerador do ideal I é único.

Lema 0.6. *Se $f \in \mathbb{F}[X]$ é irredutível, então (f) é maximal.* □

Todo $f \in \mathbb{F}[X]$ pode ser escrito, de forma única a menos de uma permutação, como

$$f(X) = \alpha p_1(X) \cdots p_m(X),$$

em que $\alpha \in \mathbb{F}$, e $p_1, \ldots, p_m \in \mathbb{F}[X]$ são mônicos e irredutíveis.

Definição 0.7. Dados $f, g \in \mathbb{F}[X]$, o $\mathrm{mdc}(f, g)$ é o polinômio mônico $h \in \mathbb{F}[X]$ tal que:

(i) h divide f e g,
(ii) se $h_0 \in \mathbb{F}[X]$ divide f e g, então h_0 divide h.

Teorema 0.8 (Critério de Eisenstein)**.** *Seja $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ e assuma que existe $p \in \mathbb{Z}$ primo tal que: p divide a_i, $i = 0, 1, \ldots, n-1$, p^2 não divide a_0 e p não divide a_n. Então f é irredutível em $\mathbb{Q}[X]$.* □

1. **Homomorfismos.** Sejam $\mathcal{A}$ e $\mathcal{B}$ aneís (comutativos com 1) e $\psi : \mathcal{A} \to \mathcal{B}$ um homomorfismo de anéis. Então, o mapa $\bar{\psi} : \mathcal{A}[X] \to \mathcal{B}[X]$ definido por

$$\bar{\psi}(a_n X^n + \cdots + a_1 X + a_0) = \psi(a_n) X^n + \cdots + \psi(a_1) X + \psi(a_0)$$

é um homomorfismo de anéis.

Exemplo 0.1. (1) Um polinômio $f \in \mathbb{Z}[X]$ pode ser visto como um polinômio $f \in (\mathbb{Z}/p\mathbb{Z})[X]$. De fato, temos um homomorfismo de anéis $\psi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, que induz $\bar{\psi} : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$.
(2) Um polinômio $f \in \mathbb{Z}[X]$ pode ser visto como um elemento de $\mathbb{Q}[X]$. De fato, temos inclusão de anéis $\mathbb{Z} \to \mathbb{Q}$, que induz inclusão $\mathbb{Z}[X] \to \mathbb{Q}[X]$.

Sejam $\mathcal{A}$ e $\mathcal{B}$ anéis e assuma que $\mathcal{A} \subseteq \mathcal{B}$ é um subanel (e então, $1_{\mathcal{A}} = 1_{\mathcal{B}}$, por convenção). Para cada $b \in \mathcal{B}$, temos um homomorfismo de anéis

$$\psi_b : \mathcal{A}[X] \to \mathcal{B},$$

satisfazendo:

$$\psi_b|_{\mathcal{A}} = \mathrm{Id}_{\mathcal{A}}, \quad \psi_b(X) = b.$$

Este homomorfismo de anéis satisfaz o seguinte: se $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathcal{A}[X]$, então

$$\begin{aligned} \psi_b(f) &= \psi_b(a_n X^n + \cdots + a_1 X + a_0) \\ &= a_n b^n + \cdots + a_1 b + a_0 =: f(b). \end{aligned}$$

Exemplo 0.2. Dado $f(X) = X^2 + 1 \in \mathbb{R}[X]$, e $1 + i \in \mathbb{C}$, então faz sentido calcular $f(1 + i)$. Temos o "esperado", isto é,

$$f(1 + i) = (1 + i)^2 + 1 = 1 + 2i.$$

2. **Quocientes.** Seja $\mathbb{F}$ um corpo e $I \subseteq \mathbb{F}[X]$ um ideal. Então existe $p(X) \in \mathbb{F}[X]$ tal que $I = (p(X))$. Qual a estrutura do quociente $\mathbb{F}[X]/I$?

Seja $\pi : \mathbb{F}[X] \to \mathbb{F}[X]/I$ o homomorfismo de anéis natural, e identifique

$$\begin{aligned} 1 = \pi(1) = 1 + I, \\ y = \pi(X) = X + I. \end{aligned}$$

Então, cada elemento de $\mathbb{F}[X]/I$ é da forma $\pi(f(X))$. Mas, se $f(X) = a_n X^n + \cdots + a_1 X + a_0$, então

$$\begin{aligned} \pi(f(X)) &= \pi(a_n)\pi(X)^n + \cdots + \pi(a_1)\pi(X) + \pi(a_0) \\ &= a_n y^n + \cdots + a_1 y + a_0 = f(y). \end{aligned}$$

Então, os elementos de $\mathbb{F}[X]/I$ são $f(y)$, com $f \in \mathbb{F}[X]$. Temos que

$$f(y) = g(y) \iff f - g \in I \iff p \text{ divide } f - g.$$

Como são as operações do anel quociente? Note que

$$\begin{aligned} f(y) + g(y) &= \pi(f(X)) + \pi(g(X)) = \pi(f(X) + g(X)) \\ &= \pi((f + g)(X)) = (f + g)(y), \\ f(y)g(y) &= \pi(f(X))\pi(g(X)) = \pi(f(X)g(X)) \\ &= \pi(fg(X)) = fg(y). \end{aligned}$$

Portanto, as operações de $\mathbb{F}[X]/I$ são "as mesmas" que as de $\mathbb{F}[X]$, salvo a relação $p(y) = 0$.

O espaço $\mathbb{F}[X]/(p(X))$ é um $\mathbb{F}$-espaço vetorial com base dada pelos elementos $\{1, y, y^2, \ldots, y^{m-1}\}$ (verifique), em que $m = \mathrm{gr}(p)$. Daí, $\dim_{\mathbb{F}} \mathbb{F}[X]/(p(X)) = \mathrm{gr}(p)$.

Exemplo 0.3. Vamos estudar o quociente $\mathbb{Q}[X]/(X^3)$. Pela discussão acima, $\{1, y, y^2, y^3, \cdots\}$ gera $\mathbb{Q}[X]/(X^3)$ como um $\mathbb{Q}$-espaço vetorial. Entretanto,

$$y^3 = 0 \iff X^3 \in (X^3),$$

e portanto, $y^m = 0$ para $m \geq 3$. Daí $\{1, y, y^2\}$ é $\mathbb{Q}$-base de $\mathbb{Q}[X]/(X^3)$.

Exemplo 0.4. Considere $\mathbb{R}[X]/(X^2+1)$. Temos que $f = X^2 + 1$ é irredutível em $\mathbb{R}[X]$ (pois não possui raízes em $\mathbb{R}$). Daí $(X^2 + 1)$ é um ideal maximal, e portanto, $\mathbb{R}[X]/(X^2 + 1)$ é corpo. O quociente é também um $\mathbb{R}$-espaço vetorial de dimensão 2. Seus elementos são

$$\mathbb{R}[X]/(X^2 + 1) = \{a + by \mid a, b \in \mathbb{R}\},$$

em que $y^2 + 1 = 0$ (ou, $y^2 = -1$). Perceba que

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}.$$

Como constrói o isomorfismo?

Note que

$$\psi_i : \mathbb{R}[X] \to \mathbb{C},$$

dado por $\psi_i(f(X)) = f(i)$ é tal que $\mathrm{Im}\, \psi_i = \mathbb{C}$. Além disso, seu núcleo é (X^2+1) (verifique). O Teorema do Isomorfismo garante o isomorfismo entre os corpos.

Agora, existe outro possível homomorfismo entre esses corpos: $\psi_{-i} : \mathbb{R}[X] \to \mathbb{C}$ dado por $\psi_{-i}(f(X)) = f(-i)$ (verifique). Assim, obtemos dois homomorfismos de corpos distintos $\mathbb{R}[X]/(X^2 + 1) \to \mathbb{C}$. Existiriam outros?

Assuma então que temos um isomorfismo $\psi : \mathbb{R}[X]/(X^2 + 1) \to \mathbb{C}$. Então, como $y^2 + 1 = 0$, vale a seguinte relação:

$$0 = \psi(y^2 + 1) = \psi(y)^2 + 1.$$

Isso significa que $\psi(y)$ é raiz do polinômio $X^2 + 1$. Portanto, $\psi(y) \in \{i, -i\}$. Conclui-se que existem exatamente dois homomorfismos (que são isomorfismos de corpos) $\mathbb{R}[X]/(X^2 + 1) \to \mathbb{C}$.

1. Exemplos e mais exemplos

1. **Corpo primo e característica.** Seja $\mathbb{F}$ um corpo. Temos homomorfismo de anéis $\mathbb{Z} \to \mathbb{F}$ que leva 1 em 1. Temos duas possibilidades:

(1) o homomorfismo é injetor. Neste caso, dizemos que $\mathbb{F}$ tem característica 0, e escrevemos $\operatorname{char}\mathbb{F} = 0$ ou $\operatorname{car}\mathbb{F} = 0$. Ainda, $\mathbb{F}$ contém um subanel isomorfo a $\mathbb{Z}$, e portanto, $\mathbb{F}$ contém o menor corpo contendo o $\mathbb{Z}$, que é o corpo dos racionais. Daí, $\mathbb{F}$ contém $\mathbb{Q}$.

(2) o homomorfismo possui um núcleo, gerado por $p\mathbb{Z}$, com $p > 0$. Neste caso, dizemos que $\mathbb{F}$ possui característica p, e escrevemos $\operatorname{char}\mathbb{F} = p$ ou $\operatorname{car}\mathbb{F} = p$. Além disso, nesta situação, $\mathbb{F}$ contém $\{0, 1, \ldots, p-1\} \cong \mathbb{F}_p$ (em que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ é o corpo com p elementos). Daí $\mathbb{F}$ contém uma cópia de $\mathbb{F}_p$.

Definição 1.1. Seja $\mathbb{F}$ um corpo. Seu corpo primo é o menor subcorpo contido em $\mathbb{F}$.

Pelo visto acima, o corpo primo de $\mathbb{F}$ é ou $\mathbb{Q}$, ou algum $\mathbb{F}_p$, dependendo de sua característica.

Observação.

(i) Se $\operatorname{char}\mathbb{F} = p > 0$, então p é primo.

(ii) Além disso, se temos $\mathbb{F} \subseteq \mathbb{E}$, com $\mathbb{E}$ corpo, então $\operatorname{char}\mathbb{F} = \operatorname{char}\mathbb{E}$.

2. **Exemplo: $\mathbb{Q}[i]$.** Denote por $\mathbb{Q}[i]$ o menor subanel de $\mathbb{C}$ contendo $\mathbb{Q}$ e $i \in \mathbb{C}$. Temos que

$$\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

Tal conjunto é um corpo: $\mathbb{Q}[i]$ é um anel comutativo com unidade, e dado $a + bi \neq 0$, temos $a^2 + b^2 \neq 0$. Então

$$(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Existem outras formas de provar que $\mathbb{Q}[i]$ é um corpo, sem explicitamente exibir o inverso de cada elemento.

Temos que $\mathbb{Q} \subseteq \mathbb{Q}[i]$, e ainda, $\mathbb{Q}[i]$ é um $\mathbb{Q}$-espaço vetorial. Temos

$$\dim_{\mathbb{Q}} \mathbb{Q}[i] = 2.$$

Denotaremos $\mathbb{Q}[i]/\mathbb{Q}$, e diremos que $\mathbb{Q}[i]$ é uma *extensão* de $\mathbb{Q}$. O *grau* da extensão é $[\mathbb{Q}[i] : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}[i]$.

Note que o elemento i satisfaz o polinômio $X^2 + 1 \in \mathbb{Q}[X]$. Tal polinômio satisfaz as seguintes propriedades:

(1) $X^2 + 1$ é mônico,

(2) X^2+1 é irredutível em $\mathbb{Q}[X]$.

Por isso, denominaremos X^2+1 como sendo o *polinômio minimal de i sobre* $\mathbb{Q}$. Note que $[\mathbb{Q}[i]:\mathbb{Q}] = \mathrm{gr}(X^2+1)$.

Agora, considere o mapa $\psi_i : \mathbb{Q}[X] \to \mathbb{C}$ tal que $\psi_i(X) = i$. Note que $(X^2+1) \subseteq \ker\psi_i$. Ainda, $\ker\psi_i \neq \mathbb{Q}[X]$ (pois $\psi_i \neq 0$), e (X^2+1) é um ideal maximal de $\mathbb{Q}[X]$ (pois X^2+1 é irredutível em $\mathbb{Q}[X]$). Então, segue que $\ker\psi_i = (X^2+1)$. Além diso, $\mathrm{Im}\,\psi_i = \mathbb{Q}[i]$. Segue que

$$\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}[i].$$

A construção de $\mathbb{Q}[X]/(X^2+1)$ tem a vantagem de ser uma construção abstrata e depende somente do corpo base $\mathbb{Q}$. Para $\mathbb{Q}[i]$, precisou-se da existência de um corpo maior (no caso, os complexos $\mathbb{C}$) e do elemento $i \in \mathbb{C}$.

Agora, $-i$ também é raiz de X^2+1. Então, as mesmas considerações podem ser feitas para obtermos

$$\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}[-i].$$

Entretanto, $\mathbb{Q}[i] = \mathbb{Q}[-i]$. Ou, vale também a seguinte propriedade: $\mathbb{Q}[i]$ contém TODAS as raízes de X^2+1, que são i e $-i$.

Agora, quem é $\mathrm{Aut}(\mathbb{Q}[i])$? Veremos que será mais interessante considerar os automorfismos de $\mathbb{Q}[i]$ que são $\mathbb{Q}$-lineares. Equivalentemente, queremos os automorfismos que fixam os valores de $\mathbb{Q}$. Formalmente, queremos:

$$\begin{aligned}\mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q}) &= \{\psi \in \mathrm{Aut}(\mathbb{Q}[i]) \mid \psi \text{ é } \mathbb{Q}\text{-linear}\} \\ &= \{\psi \in \mathrm{Aut}(\mathbb{Q}[i]) \mid \psi(q) = q, \forall q \in \mathbb{Q}\}.\end{aligned}$$

No caso de $\mathbb{Q}[i]$, é redundante pedir que os automorfismos sejam $\mathbb{Q}$-linear. Isso porque um automorfismo de um corpo automaticamente fixa os elementos do seu corpo primo. Entretanto, tal restrição será fundamental nas construções que desenvolveremos no curso.

Para determinar $\mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q})$, vamos procurar as inclusões (ou seja, homomorfismos não-nulos) $\mathbb{Q}[i] \to \mathbb{C}$ que são $\mathbb{Q}$-lineares.

Sabemos que existe a inclusão identidade $\iota : \mathbb{Q}[i] \to \mathbb{C}$. Agora, se $\sigma \in \mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q})$, então obtemos outra inclusão $\mathbb{Q}[i] \xrightarrow{\sigma} \mathbb{Q}[i] \xrightarrow{\sigma} \mathbb{C}$. Daí

$$|\mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q})| \leq (\text{numero de homomorfismos injetor } \mathbb{Q}[i] \to \mathbb{C}).$$

Como $\mathbb{Q}[i] \cong \mathbb{Q}[X]/(X^2+1)$, vamos estudar os homomorfismos

$$\mathbb{Q}[X]/(X^2+1) \to \mathbb{C}.$$

Então, sejam $\psi : \mathbb{Q}[X]/(X^2+1) \to \mathbb{C}$ não nulo e $x = X + (X^2+1) \in \mathbb{Q}[X]/(X^2+1)$. Daí

$$0 = \psi(x^2+1) = (\psi(x))^2 + 1,$$

portanto, $\psi(x)$ é raiz de X^2+1. Segue que $\psi(x) \in \{i, -i\}$. Então, temos no máximo dois homomorfismos $\mathbb{Q}[X]/(X^2+1) \to \mathbb{C}$, e é elementar verificar que ambas estão bem definidas. Os conjuntos imagens são:

$$\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}[i] \subseteq \mathbb{C},$$
$$\mathbb{Q}[X]/(X^2+1) \cong \mathbb{Q}[-i] \subseteq \mathbb{C}.$$

Então, pelo argumeto apresentado, obtemos a seguinte relação:

(no. de hom. injetor $\mathbb{Q}[i] \to \mathbb{C}$) = (qtd. de raizes distintas de X^2+1).

Agora, para cada $\psi : \mathbb{Q}[i] \to \mathbb{C}$, lembre-se que $\mathbb{Q}[i]$ contém todas as raízes de X^2+1. Isso significa que $\psi(i) \in \mathbb{Q}[i]$, e portanto, $\operatorname{Im}\psi \subseteq \mathbb{Q}[i]$. Como consequência, vale que $\psi \in \operatorname{Aut}(\mathbb{Q}[i]/\mathbb{Q})$. Então $|\operatorname{Aut}(\mathbb{Q}[i]/\mathbb{Q})| = 2$, e $\operatorname{Aut}(\mathbb{Q}[i]/\mathbb{Q}) = \{1, \sigma\}$, em que $\sigma(a+bi) = a - bi$ é a conjugação complexa.

Por fim, assuma que começamos com o corpo $\mathbb{Q}[i]$ e o subgrupo $G = \{1, \sigma\} \subseteq \operatorname{Aut}(\mathbb{Q}[i])$ (na verdade, neste exemplo, vale que $G = \operatorname{Aut}(\mathbb{Q}[i])$). Para recuperar o corpo $\mathbb{Q}$, podemos considerar o corpo fixo por G:

$$\mathbb{Q}[i]^G = \{\alpha \in \mathbb{Q}[i] \mid \psi(\alpha) = \alpha, \forall \psi \in G\} = \mathbb{Q}.$$

Para esse caso especial, a relação acima se traduz em:

$$\mathbb{Q} = \{\alpha \in \mathbb{Q}[i] \mid \bar{\alpha} = \alpha\}.$$

3. **Exemplo: $\mathbb{Q}[\sqrt[3]{2}]$.** Considere o menor subanel de $\mathbb{C}$ contendo $\mathbb{Q}$ e $\sqrt[3]{2}$:

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 \mid a, b, c \in \mathbb{Q}\}.$$

Temos que $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt[3]{2}] = 3$ é finita, e o elemento $\sqrt[3]{2}$ satisfaz um polinômio (por exemplo, $X^3 - 2$).

Temos que $\mathbb{Q}[\sqrt[3]{2}]$ é corpo, pois considere $\psi_{\sqrt[3]{2}} : \mathbb{Q}[X] \to \mathbb{C}$, dado por $\psi_{\sqrt[3]{2}}(X) = \sqrt[3]{2}$. Daí $\operatorname{Im}\psi_{\sqrt[3]{2}} = \mathbb{Q}[\sqrt[3]{2}]$, e $(X^3-2) \subseteq \ker\psi_{\sqrt[3]{2}}$. Além disso, $X^3 - 2$ é irredutível em $\mathbb{Q}[X]$ (por critério de Eisenstein, por exemplo). Daí (X^3-2) é ideal maximal, e portanto, $\ker\psi_{\sqrt[3]{2}} = (X^3-2)$. Segue que

$$\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[X]/(X^3-2)$$

é corpo.

O polinômio X^3-2 é mônico, irredutível em $\mathbb{Q}[X]$ e possui $\sqrt[3]{2}$ como uma de suas raízes. Portanto, X^3-2 será o polinômio minimal de $\sqrt[3]{2}$ sobre $\mathbb{Q}$.

As raízes de X^3-2 em $\mathbb{C}$ são $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ e $\omega^2\sqrt[3]{2}$, em que $\omega \neq \omega^3 = 1$. Daí, vale também:

$$\mathbb{Q}[\omega\sqrt[3]{2}] \cong \mathbb{Q}[X]/(X^3-2) \cong \mathbb{Q}[\omega^2\sqrt[3]{2}] \cong \mathbb{Q}[\sqrt[3]{2}].$$

Porém, esses corpos são distintos. Isso se deve ao fato que $\mathbb{Q}[\sqrt[3]{2}]$ NÃO contém todas as raízes de X^3-2 (de fato, $\mathbb{Q}[\sqrt[3]{2}]$ contém somente a única raiz real).

Vamos calcular $\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})$. Repetindo a ideia do caso $\mathbb{Q}[i]$, nós temos três inclusões $\mathbb{Q}[\sqrt[3]{2}] \to \mathbb{C}$. Porém, os conjuntos imagens são todos distintos. Portanto, a única possibilidade é que $\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = \{1\}$.

Para finalizar, o seu corpo fixo será:

$$\begin{aligned}\mathbb{Q}[\sqrt[3]{2}]^{\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})} &= \{\alpha \in \mathbb{Q}[\sqrt[3]{2}] \mid \psi(\alpha) = \alpha, \forall \psi \in \mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})\} \\ &= \mathbb{Q}[\sqrt[3]{2}].\end{aligned}$$

4. **Exemplo: $\mathbb{Q}[\xi]$, $\xi \neq \xi^5 = 1$.** Seja $\xi \in \mathbb{C}$ de modo que $\xi \neq \xi^5 = 1$. Chamamos tal elemento de uma 5-raiz primitiva da unidade. Note que, se $i \in \{1,2,3,4\}$, então

$$(\xi^i)^5 = (\xi^5)^i = 1.$$

Note também que $X^5-1 = (X-1)(X^4+X^3+X^2+X+1)$. Seja $\Phi_5(X) := X^4+X^3+X^2+X+1$. Então, pelo visto acima, as raízes de $\Phi_5(X)$ são ξ, ξ^2, ξ^3, ξ^4. Além disso, $\Phi_5(X)$ é irredutível em $\mathbb{Q}[X]$ (exercício).

Seja $\mathbb{Q}[\xi] \subseteq \mathbb{C}$ o menor subanel de $\mathbb{C}$ contendo $\mathbb{Q}$ e ξ. Note que as raízes de $\Phi_5(X)$ são $\xi, \xi^2, \xi^3, \xi^4 \in \mathbb{Q}[\xi]$. Assim sendo, sem descrever explicitamente o conjunto $\mathbb{Q}[\xi]$, responda:

(i) $\mathbb{Q}[\xi]$ é corpo?
(ii) $\dim_{\mathbb{Q}} \mathbb{Q}[\xi] = ?$
(iii) Quantos homomorfismos de anéis não-nulo $\mathbb{Q}[\xi] \to \mathbb{C}$ existem?
(iv) $|\mathrm{Aut}(\mathbb{Q}[\xi]/\mathbb{Q})| = ?$

5. **Exemplo: $\mathbb{Q}[\pi]$.** Sabe-se que π é um número transcendente (Lindemann, 1882), ou seja, π não é raiz de um polinômio não-nulo com coeficientes em $\mathbb{Q}$. Considere $\mathbb{Q}[\pi]$ o menor subanel de $\mathbb{C}$ contendo π e $\mathbb{Q}$. Temos que $\dim_{\mathbb{Q}} \mathbb{Q}[\pi] = \infty$. De fato, assuma por absurdo que $\dim_{\mathbb{Q}} \mathbb{Q}[\pi] = n < \infty$. Então 1, π, $\ldots$, π^n são $\mathbb{Q}$-linearmente dependentes. Daí, existem $a_0, a_1, \ldots, a_n \in \mathbb{Q}$, não todos nulos, tais que

$0 = a_0 + a_1\pi + \cdots + a_n\pi^n$. Isso implica que π é raiz do polinômio $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Q}[X]$, uma contradição.

Para descrever $\mathbb{Q}[\pi]$, considere o mapa $\psi_\pi : \mathbb{Q}[X] \to \mathbb{C}$ tal que $\psi_\pi(X) = \pi$. Então $\operatorname{Im}\psi_\pi = \mathbb{Q}[\pi]$, e $\ker\psi_\pi = 0$ (caso contrário, iríamos contradizer a transcendência de π). Do Teorema do Isomorfismo, segue que $\mathbb{Q}[X] \cong \mathbb{Q}[\pi]$. Portanto, $\mathbb{Q}[\pi]$ não é corpo, e

$$\begin{aligned}\mathbb{Q}[\pi] &= \{a_0 + a_1\pi + \cdots + a_n\pi^n \mid n \in \mathbb{N},\, a_0, a_1, \ldots, a_n \in \mathbb{Q}\} \\ &= \{f(\pi) \mid f \in \mathbb{Q}[X]\}.\end{aligned}$$

O menor subcorpo de $\mathbb{C}$ contendo $\mathbb{Q}[\pi]$ é o seu corpo de frações, denotado por $\mathbb{Q}(\pi)$. Temos

$$\mathbb{Q}(\pi) \cong \mathbb{Q}(X) := \text{corpo de frações de } \mathbb{Q}[X].$$

Note que para qualquer outro elemento transcendente $\alpha \in \mathbb{C}$, por mesmo argumento, teríamos que $\mathbb{Q}[\alpha] \cong \mathbb{Q}[X]$. Então, temos infinitos (não-enumerável) monomorfismos $\mathbb{Q}(\pi) \to \mathbb{C}$.

Exercício. Dados $\alpha, \beta \in \mathbb{C}$ transcendentes (sobre $\mathbb{Q}$), o que podemos falar de $\mathbb{Q}[\alpha, \beta]$, o menor subanel de $\mathbb{C}$ contendo $\mathbb{Q}$, α e β?

6. **Exemplo: corpos finitos.** Seja $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ o corpo com 2 elementos, e seja $\mathbb{F}_4$ o $\mathbb{F}_2$-espaço vetorial com base $\{1, y\}$. Então $\mathbb{F}_4 = \{0, 1, y, 1 + y\}$. Considere o produto em $\mathbb{F}_4$ dado por

	0	1	y	$1+y$
0	0	0	0	0
1	0	1	y	$1+y$
y	0	y	$1+y$	1
$1+y$	0	$1+y$	1	y

Temos que $\mathbb{F}_4$ é um corpo. Uma forma de verificar é o seguinte: o polinômio $X^2 + X + 1$ é irredutível em $\mathbb{F}_2[X]$ (pois não possui raízes em $\mathbb{F}_2$). Então $\mathbb{F}_2[X]/(X^2+X+1)$ é um corpo com 4 elementos. Tome $y = X + (X^2 + X + 1)$. Verifica-se que o produto dos elementos em $\mathbb{F}_2[X]/(X^2 + X + 1)$ coincide com os da tabela. Daí

$$\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1).$$

Exercícios.

(1) Construa um corpo com 9 elementos.
(2) Sejam $f_1 = X^3 + X^2 + 1$ e $f_2 = X^3 + X + 1$. Prove que f_1 e f_2 são irredutíveis em $\mathbb{F}_2[X]$. Exiba um isomorfismo de corpos $\mathbb{F}_2[X]/(f_1) \to \mathbb{F}_2[X]/(f_2)$.

7. **Exemplo: Polinômio X^p quando $\operatorname{car}\mathbb{F} = p$.** Seja $\mathbb{F}$ um corpo finito e de característica $p > 0$. Então, dados $a, b \in \mathbb{F}$, vale que (verifique)

$$(a+b)^p = a^p + b^p.$$

Assim, seja $F : \mathbb{F} \to \mathbb{F}$ o mapa definido por $F(a) = a^p$. Temos que

$$F(a+b) = (a+b)^p = a^p + b^p = F(a) + F(b),$$
$$F(ab) = (ab)^p = a^p b^p = F(a)F(b).$$

Daí F é um homomorfismo de anéis. Além disso, $0 = F(a) = a^p$ implica $a = 0$, ou seja, F é um monomorfismo. No caso de $\mathbb{F}$ ser finito, temos então que $\mathbb{F}$ é também sobrejetiva. Assim, dado $a \in \mathbb{F}$, existe $b \in \mathbb{F}$ tal que $a = F(b) = b^p$. Portanto, o polinômio

$$f_a(X) = X^p - a = X^p - b^p = (X-b)^p$$

possui todas as raízes repetidas, e iguais a b.

Agora, considere $\mathbb{E} = \mathbb{F}(Y)$, o corpo de frações do anel de polinômios $\mathbb{F}[Y]$. Considere $f(X) = X^p - Y \in \mathbb{E}[X]$. Temos que não existe $b \in \mathbb{E}$ de modo que $b^p = Y$. Além disso, veremos que o tal polinômio f é irredutível.

Se existir um corpo $\mathbb{L} \supseteq \mathbb{E}$ (na verdade, sempre existe!) em que f possui raiz, então todas as raízes de f serão repetidas. Assim, f é um exemplo de um polinômio irredutível tal que

$$(\text{qtd. de raízes distintas de } f) < \operatorname{gr}(f).$$

8. **Exemplo: $\mathbb{Q}[\sqrt{2}, i]$.** Considere o seguinte subanel de $\mathbb{C}$,

$$\mathbb{Q}[\sqrt{2}, i] = \{a + b\sqrt{2} + ci + d\sqrt{2}i \mid a, b, c, d \in \mathbb{Q}\}.$$

Temos $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}, i] = 4$. Podemos escrever também $\mathbb{Q}[\sqrt{2}, i] = \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}[i]\}$, o que indica que $\mathbb{Q}[\sqrt{2}, i]$ não é somente um $\mathbb{Q}$-espaço vetorial, mas também um $\mathbb{Q}[i]$-espaço vetorial de dimensão 2 (já vimos que $\mathbb{Q}[i]$ é um corpo). Além disso, tal observação evidencia a seguinte fórmula:

$$[\mathbb{Q}[\sqrt{2}, i] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{2}, i] : \mathbb{Q}[i]][\mathbb{Q}[i] : \mathbb{Q}].$$

Seria $\mathbb{Q}[\sqrt{2}, i]$ um corpo?

Dado $0 \neq r \in \mathbb{Q}[\sqrt{2}, i]$, então a multiplicação por r é uma transformação linear $L_r : \mathbb{Q}[\sqrt{2}, i] \to \mathbb{Q}[\sqrt{2}, i]$, $L_r(a) = ra$. Além disso, como $\mathbb{Q}[\sqrt{2}, i]$ é domínio (pois é um subanel de $\mathbb{C}$, que é corpo), segue que L_r é injetora. Como $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}, i] < \infty$, segue que L_r é também sobrejetora. Portanto, existe $s \in \mathbb{Q}[\sqrt{2}, i]$ tal que $rs = L_r(s) = 1$. Isso implica que $r^{-1} = s \in \mathbb{Q}[\sqrt{2}, i]$, ou seja, $\mathbb{Q}[\sqrt{2}, i]$ é corpo.

Qual seria seu grupo de $\mathbb{Q}$-automorfismos?

Temos que $\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}) = \{\eta_0, \eta_1, \eta_2, \eta_3\}$, em que $\eta_0 = \mathrm{Id}$, e

$$\eta_1(a + b\sqrt{2} + ci + d\sqrt{2}i) = a - b\sqrt{2} + ci - d\sqrt{2}i,$$
$$\eta_2(a + b\sqrt{2} + ci + d\sqrt{2}i) = a + b\sqrt{2} - ci - d\sqrt{2}i,$$
$$\eta_3 = \eta_1\eta_2.$$

Em outras palavras, $\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}) = \langle \eta_1, \eta_2 \rangle \cong C_2 \times C_2$. Perceba que cada elemento de $\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q})$ é unicamente descrito por sua ação em $\sqrt{2}$ e em i.

O corpo fixo, neste caso, é (verifique)

$$\mathbb{Q}[\sqrt{2},i]^{\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}} = \mathbb{Q}.$$

Agora, vimos que $\mathbb{Q}[i] \subseteq \mathbb{Q}[\sqrt{2},i]$. Então, conseguiríamos calcular o grupo dos $\mathbb{Q}[i]$-automorfismos, isto é, $\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}[i])$?

Dado $\psi \in \mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}[i])$, temos $\psi(\alpha) = \alpha$, $\forall \alpha \in \mathbb{Q}[i]$. Em particular, $\psi(\alpha) = \alpha$, $\forall \alpha \in \mathbb{Q}$. Daí, obtemos que

$$\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}[i]) \subseteq \mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}).$$

Assim sendo, ψ é unicamente determinado por sua ação sobre $\sqrt{2}$ e sobre i. Necessariamente temos que $\psi(i) = i$, e que $\psi(\sqrt{2}) \in \{sqrt2, -\sqrt{2}\}$. Além disso, as duas possibilidades são possíveis de ocorrer. Assim, o tal grupo de automorfismos possui dois elementos. Mais precisamente, temos que

$$\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}[i]) = \{\eta_0, \eta_1\} = \langle \eta_1 \rangle \cong C_2.$$

Seu corpo fixo é

$$\begin{aligned}\mathbb{Q}[\sqrt{2},i]^{\langle \eta_1 \rangle} &= \{\alpha + \beta\sqrt{2} \in \mathbb{Q}[\sqrt{2},i] \mid \alpha + \beta\sqrt{2} = \eta_1(\alpha + \beta\sqrt{2})\} \\ &= \{\alpha + \beta\sqrt{2} \in \mathbb{Q}[\sqrt{2},i] \mid \alpha + \beta\sqrt{2} = \alpha - \beta\sqrt{2}\} \\ &= \{\alpha \in \mathbb{Q}[i]\} = \mathbb{Q}[i].\end{aligned}$$

Agora, vamos fazer o contrário. Comecemos com o subgrupo $H_2 = \langle \eta_2 \rangle$. Então, o corpo fixo desse subgrupo é (verifique)

$$\mathbb{Q}[\sqrt{2},i]^{\langle \eta_2 \rangle} = \mathbb{Q}[\sqrt{2}].$$

Usando argumentos similares ao caso anterior, obtemos que

$$\mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}[\sqrt{2}]) = \langle \eta_2 \rangle.$$

Por fim, temos um último subcorpo de $\mathbb{Q}[\sqrt{2},i]$, que é $\mathbb{Q}[\sqrt{2}i]$. Temos também um último subgrupo do grupo de autormosfismos, $H_3 = \langle \eta_1\eta_2 \rangle = \langle \eta_3 \rangle$. Ambos estão relacionados por

$$\mathbb{Q}[\sqrt{2},i]^{\langle \eta_3 \rangle} = \mathbb{Q}[\sqrt{2}i], \quad \mathrm{Aut}(\mathbb{Q}[\sqrt{2},i]/\mathbb{Q}[\sqrt{2}i]) = \langle \eta_3 \rangle.$$

Portanto, exibimos uma correspondência biunívoca entre os corpos $\mathbb{F}$, com $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{Q}[\sqrt{2}, i]$, e os subgrupos de $\mathrm{Aut}(\mathbb{Q}[\sqrt{2}, i]/\mathbb{Q})$. Tal correspondência é um caso particular do Teorema Fundamental da Teoria de Galois.

2. Extensão de corpos

Nosso interesse neste curso será estudar simetrias de um corpo, e uma boa forma de o fazer é estudando simetrias em relação a um subcorpo. Para tal propósito, será interessante dizermos como um corpo está incluso num segundo.

Uma noção didática de extensão de corpos é a seguinte:

Definição 2.1. Uma *extensão de corpos* $\mathbb{E}/\mathbb{F}$ é um par de corpos $\mathbb{E}$ e $\mathbb{F}$, com $\mathbb{F} \subseteq \mathbb{E}$.

Reforçamos que vai ser importante como um corpo é subconjunto de um outro corpo, e não somente vê-los como objetos abstratos.

Entretanto, faremos diversas construções em que formalmente um corpo não está contido no outro, porém existe um mapa injetivo entre os corpos. Então, para tais propósitos, a forma correta de definir extensão de corpos é a seguinte:

Definição 2.2. Uma *extensão de corpos* $\mathbb{E}/\mathbb{F}$ é uma tripla $(i, \mathbb{E}, \mathbb{F})$, em que $\mathbb{E}$ e $\mathbb{F}$ são corpos, e $i : \mathbb{F} \to \mathbb{E}$ é um homomorfismo injetor de anéis.

Ressaltamos que o homomorfismo i é a parte mais importante desta definição; pois um corpo $\mathbb{E}$ pode conter diversas cópias do corpo $\mathbb{F}$. Se identificarmos o corpo $\mathbb{F}$ com a imagem $i(\mathbb{F})$, então caímos na primeira definição. Vamos então, usar a Definição 2.1 para extensão de corpos, e sempre identificar o corpo com a sua imagem, se estivermos no caso da Definição 2.2.

Dada uma extensão de corpos $\mathbb{E}/\mathbb{F}$, temos que $\mathbb{E}$ é um espaço vetorial sobre o corpo $\mathbb{F}$. Sendo assim, definimos o seguinte:

Definição 2.3. O *grau* de uma extensão $\mathbb{E}/\mathbb{F}$, denotada por $[\mathbb{E} : \mathbb{F}]$, é a dimensão do espaço $\mathbb{E}$ sobre $\mathbb{F}$. Isto é, $[\mathbb{E} : \mathbb{F}] := \dim_{\mathbb{F}} \mathbb{E}$. Se $[\mathbb{E} : \mathbb{F}] < \infty$, dizemos que a extensão é *finita*. Dizemos que a extensão é quadrática, cúbica, etc... se a extensão tiver grau 2, 3, etc...

Exemplo 2.1.

(1) $\mathbb{C}/\mathbb{R}$ e $[\mathbb{C} : \mathbb{R}] = 2$. Uma base de $\mathbb{C}$ sobre $\mathbb{R}$ é $\{1, i\}$, em que $i^2 = -1$.
(2) $\mathbb{R}/\mathbb{Q}$ e $[\mathbb{R} : \mathbb{Q}] = \infty$ (por que?)
(3) Seja $\mathbb{F}_2$ o corpo com dois elementos (isto é, $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$). Seja $\mathbb{E} = \mathbb{F}_2(X)$ o corpo de frações do anel de polinômios $\mathbb{F}_2[X]$. Então $[\mathbb{E} : \mathbb{F}_2] = \infty$.

    Se tomarmos $\mathbb{F}_2(Y)$ como sendo um outro corpo de frações do anel de polinômios, então claro que $\mathbb{F}_2(Y) \cong \mathbb{E}$. Entretanto, é possível ter outros homomorfismos injetores $\mathbb{F}_2(Y) \to \mathbb{E}$

(não necessariamente sobrejetores)? Nestes casos, quanto seria o grau da extensão $[\mathbb{E} : \mathbb{F}_2(Y)]$?

Teorema 2.4. *Considere extensões de corpos $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$. Então $\mathbb{L}/\mathbb{F}$ é finita se e só se $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ são finitas. Além disso, neste caso, vale*

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

No geral, se $\mathcal{E}$ é uma base de $\mathbb{E}$ sobre $\mathbb{F}$, e se $\mathcal{L}$ é uma base de $\mathbb{L}$ sobre $\mathbb{E}$, então $\{e\ell \mid e \in \mathcal{E}, \ell \in \mathcal{L}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{F}$.

Demonstração. Vamos provar a última afirmação do teorema, que terá como consequência as demais afirmações. Dado $\ell \in \mathbb{L}$, sendo $\mathcal{L}$ uma $\mathbb{E}$-base de $\mathbb{L}$, existem $a_1, \ldots, a_m \in \mathbb{E}$ e $\ell_1, \ldots, \ell_m \in \mathcal{L}$ de modo que

$$\ell = a_1\ell_1 + \cdots + a_m\ell_m.$$

Agora, para cada j, como $\mathcal{E}$ é uma $\mathbb{F}$-base de $\mathbb{E}$, existem $e_{j1}, \ldots, e_{jm_j} \in \mathcal{E}$ e $\alpha_{j1}, \ldots, \alpha_{jm_j} \in \mathbb{F}$ de modo que

$$a_j = \alpha_{j1}e_{j1} + \cdots + \alpha_{jm_j}e_{jm_j}.$$

Daí

$$\ell = \sum_{j=1}^{m}\sum_{i=1}^{m_j} \alpha_{ji}e_{ji}\ell_j.$$

Isso mostra que $\{e\ell \mid e \in \mathcal{E}, \ell \in \mathcal{L}\}$ gera o espaço $\mathbb{L}$ como um espaço vetorial sobre $\mathbb{F}$. Vamos provar que este conjunto é linearmente independente. Para tanto, considere uma $\mathbb{F}$-combinação linear dando zero:

$$0 = \sum_{j=1}^{m}\sum_{i=1}^{m_j} \alpha_{ji}e_{ji}\ell_j = \sum_{j=1}^{m}\left(\sum_{i=1}^{m_j} \alpha_{ji}e_{ji}\right)\ell_j$$

Sendo os elementos $\sum_{i=1}^{m_j} \alpha_{ji}e_{ji} \in \mathbb{E}$ e $\mathcal{L}$ uma $\mathbb{E}$-base, segue que esses são nulos, ou seja, $\sum_{i=1}^{m_j} \alpha_{ji}e_{ji} = 0$. Mas, como cada $\alpha_{ji} \in \mathbb{F}$ e $\mathcal{E}$ é uma $\mathbb{F}$-base, segue que cada $\alpha_{ji} = 0$. Mas isso prova que os coeficientes iniciais são nulos, ou seja, $\{e\ell \mid e \in \mathcal{E}, \ell \in \mathcal{L}\}$ é de fato uma $\mathbb{F}$-base de $\mathbb{L}$. □

2.1. **Subanel gerado.** Sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos e $S \subseteq \mathbb{E}$ um subconjunto. O *subanel* de $\mathbb{E}$, gerado por S sobre $\mathbb{F}$, é o menor subanel de $\mathbb{E}$ contendo $\mathbb{F}$ e S. Denota-se tal subanel por $\mathbb{F}[S]$. No caso em que $S = \{a_1, \ldots, a_m\}$ é finito, denota-se o subanel simplesmente por $\mathbb{F}[a_1, \ldots, a_m]$.

Exemplo 2.2.

(1) $\mathbb{C} = \mathbb{R}[i]$.

(2) Sendo $\pi \in \mathbb{R}$, temos que $\mathbb{Q}[\pi]$ consiste de todos os elementos da forma

$$\alpha_m \pi^m + \alpha_{m-1}\pi^{m-1} + \cdots + \alpha_1 \pi + \alpha_0, \quad \alpha_0, \alpha_1, \ldots, \alpha_m \in \mathbb{Q}.$$

Então $\mathbb{Q}[\pi]$ é isomorfo ao anel de polinômios sobre $\mathbb{Q}$.

Questão 2.1. Por que "o menor subanel contendo tais elementos" existe? (dica: para a existência de um "menor subanel" contendo um subconjunto, é suficiente mostrar que a intersecção de uma família de subanéis ainda é um subanel. Por que?).

Exemplo 2.3. Nestas condições, em que $\mathbb{E}/\mathbb{F}$ e $S \subseteq \mathbb{E}$, mostre que

$$\mathbb{F}[S] = \left\{ \sum_{i=1}^{m} \alpha_i a_{i_1} \cdots a_{i_r} \mid m \in \mathbb{N}, \alpha_i \in \mathbb{F}, a_{i_1}, \ldots, a_{i_r} \in S, r \in \mathbb{N} \right\},$$

ou seja, $\mathbb{F}[S]$ é constituído de todas as somas finitas de produto de elementos de $\mathbb{F} \cup S$.

Neste sentido, será importante para nós o seguinte resultado, e sua consequência:

Lema 2.5. *Seja $\mathcal{R}$ um domínio de integridade comutativo com unidade, contendo um corpo $\mathbb{F}$ como subanel, e assuma que as duas unidades coincidem. Se $\dim_{\mathbb{F}} \mathcal{R} < \infty$, então $\mathcal{R}$ é corpo.*

Demonstração. Por hipótese, temos que $\mathcal{R}$ é um anel comutativo com unidade 1. Então basta provarmos que os elementos não nulos de $\mathcal{R}$ são invertíveis. Seja $r \in \mathcal{R}$ não nulo. Considere o mapa $\varphi_r : \mathcal{R} \to \mathcal{R}$ definido por $\varphi_r(a) = ra$ (multiplicação por r). Então φ_r é uma transformação linear injetiva (pois $\mathcal{R}$ é um domínio). Sendo $\dim_{\mathbb{F}} \mathcal{R} < \infty$, segue que φ_r é sobrejetivo também. Isso significa que existe $s \in \mathcal{R}$ de modo que $1 = \varphi_r(s) = rs$, ou seja, r é invertível em $\mathcal{R}$. □

Corolário 2.6. *Sejam $\mathbb{E}/\mathbb{F}$ e $S \subseteq \mathbb{E}$. Se $\dim_{\mathbb{F}} \mathbb{F}[S]$ é finita, então $\mathbb{F}[S]$ é corpo.*

Demonstração. Por construção, $\mathbb{F}[S]$ é um anel comutativo contendo a mesma unidade de $\mathbb{F}$. Agora, sendo $\mathbb{F}[S]$ um subconjunto do corpo $\mathbb{E}$, segue que $\mathbb{F}[S]$ é um domínio de integridade. Ainda, por hipótese, $\dim_{\mathbb{F}} \mathbb{F}[S] < \infty$. Portanto, estamos na condição do teorema anterior, tomando $\mathcal{R} = \mathbb{F}[S]$. Concluí-se que $\mathbb{F}[S]$ é um corpo. □

Corolário 2.7. *Sejam $\mathbb{E}/\mathbb{F}$ finita e $S \subseteq \mathbb{E}$. Então $\mathbb{F}[S]$ é corpo.* □

2.2. **Subcorpo gerado.** Novamente, sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos e $S \subseteq \mathbb{E}$. O subcorpo gerado por S sobre $\mathbb{F}$, denotado por $\mathbb{F}(S)$, é o menor subcorpo de $\mathbb{E}$ contendo $\mathbb{F}$ e S. Se S for finito, digamos, $S = \{a_1, \ldots, a_m\}$, então denota-se o subcorpo gerado simplesmente por $\mathbb{F}(a_1, \ldots, a_m)$.

Questão 2.2. Por que existe um menor subcorpo?

Exemplo 2.4.

(1) Se $\mathbb{F}[S]$ já é corpo, então vale que $\mathbb{F}[S] = \mathbb{F}(S)$.
De fato, um argumento formal segue: como $\mathbb{F}(S)$ é também um subanel contendo $\mathbb{F}$ e S, segue que, por ser o menor, $\mathbb{F}[S] \subseteq \mathbb{F}(S)$ (esta continência sempre é verdadeira). Agora, como $\mathbb{F}[S]$ é um corpo e contém $\mathbb{F}$ e S, então, por ser o menor, $\mathbb{F}(S) \subseteq \mathbb{F}[S]$. Segue então que vale $\mathbb{F}(S) = \mathbb{F}[S]$.

(2) Seja $\pi \in \mathbb{R}$. Então $\mathbb{Q}(\pi)$ é isomorfo ao corpo de frações do anel de polinômios sobre $\mathbb{Q}$.

Definição 2.8. Uma extensão $\mathbb{E}/\mathbb{F}$ é dita ser *simples* se existe $\alpha \in \mathbb{E}$ de modo que $\mathbb{E} = \mathbb{F}(\alpha)$.

Exemplo 2.5.

(1) $\mathbb{C}/\mathbb{R}$ e $\mathbb{Q}(\pi)/\mathbb{Q}$ são exemplos de extensões simples. Perceba que podemos ter uma uma extensão simples de grau infinito ($[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$).

(2) Seria a extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ simples? Note que

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q} \right\}.$$

Por outro lado, considere o corpo $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Como $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, segue que $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Agora,

$$\sqrt{2} = -\frac{1}{2}\left(\left(\sqrt{2} + \sqrt{3}\right)^2 - 5\right)\left(\sqrt{2} + \sqrt{3}\right) + 3\left(\sqrt{2} + \sqrt{3}\right) \in \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Além disso, $\sqrt{3} = \left(\sqrt{2} + \sqrt{3}\right) - \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Daí obtemos que vale $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, e então, $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ é uma extensão simples.

Vamos finalizar a seção com uma construção. O nome dado para o corpo seguinte não é muito usual, porém a sua construção é bastante conhecida e essencial para a teoria (na verdade, não se preocupe com o nome, mas sim com a construção).

Definição 2.9. Seja $\mathbb{F}$ um corpo e $f(X) \in \mathbb{F}[X]$ um polinômio irredutível. Um *stem field de* $f(X)$ *sobre* $\mathbb{F}$ é um par $(\mathbb{E}, \alpha)$, em que $\mathbb{E}/\mathbb{F}$ é uma extensão de corpos, $\alpha \in \mathbb{E}$, $\mathbb{E} = \mathbb{F}(\alpha)$ e $f(\alpha) = 0$.

A existência de um tal par sempre existe, e a construção é a seguinte: sendo $f(X) \in \mathbb{F}[X]$ um polinômio irredutível, então o quociente $\mathbb{E} := \mathbb{F}[X]/(f(X))$ é um corpo. O elemento $\alpha = X + (f(X))$ é tal que $f(\alpha) = 0$ por construção. Além disso, segue da construção que $\mathbb{E} = \mathbb{F}[\alpha]$. Então o par $(\mathbb{F}[X]/(f(X)), X + (f(X)))$ satisfaz a Definição 2.9. *Exercício.* Prove que o corpo $(\mathbb{E}, \alpha)$ satisfazendo a Definição 2.9 é único, a menos de isomorfismo.

Como consequência, temos o seguinte:

Teorema 2.10. *Sejam $\mathbb{F}$ um corpo e $f(X) \in \mathbb{F}[X]$. Então existe uma extensão finita de corpos $\mathbb{E}/\mathbb{F}$ em que $f(X)$ possui raiz em $\mathbb{E}$.*

Demonstração. Não há nada a fazer se $\mathrm{gr}(f) = 1$. Caso contrário, seja g uma componente irredutível de f. Pela construção anterior, o corpo $\mathbb{E} = \mathbb{F}[X]/(g(X))$ contém uma raiz de g, e portanto, uma raiz de f. □

Como consequência imediata, obtemos o seguinte:

Corolário 2.11. *Sejam $\mathbb{F}$ um corpo e $f(X) \in \mathbb{F}[X]$. Então existe uma extensão de corpos $\mathbb{E}/\mathbb{F}$ em que $f(X)$ possui todas as suas raízes em $\mathbb{E}$.* □

3. Extensão algébrica

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 2.6 que $\mathbb{F}[\alpha]$ é um corpo. Portanto, segue que o polinômio $p_\alpha(X)$ é irredutível em $\mathbb{F}[X]$.

Definição 3.1. 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 3.2. *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 3.3. *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 3.1.

(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 3.4. *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 $\operatorname{gr}(\operatorname{Irr}(\alpha, \mathbb{F})) = [\mathbb{F}[\alpha] : \mathbb{F}]$.*

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 $p_\alpha(X) = \operatorname{Irr}(\alpha, \mathbb{F})$. Temos que $\mathbb{F}[\alpha] \cong \mathbb{F}[X]/(p_\alpha(X))$, e portanto, $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$ é corpo e $[\mathbb{F}[\alpha] : \mathbb{F}] = \operatorname{gr}(p_\alpha(X))$. □

Exemplo 3.2. 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 3.5. *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

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

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 3.6. 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 3.4, 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 3.7. *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 3.4, segue que α é algébrico sobre $\mathbb{F}$. Portanto, $\mathbb{L}/\mathbb{F}$ é algébrico. □

Por fim, temos:

Teorema 3.8. *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 3.5, 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 3.4 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 $[\mathbb{A} : \mathbb{Q}] = \infty$.

4. Corpos algebricamente fechados

Começamos provando as seguintes equivalências:

Teorema 4.1. *Seja $\mathbb{F}$ um corpo. As seguintes afirmações são equivalentes:*

(i) *todo polinômio em $\mathbb{F}[X]$ de grau não nulo possui (pelo menos) uma raiz em $\mathbb{F}$,*
(ii) *todo polinômio em $\mathbb{F}[X]$ se fatora como produto de polinômios de grau 1,*
(iii) *os polinômios irredutíveis de $\mathbb{F}[X]$ possuem 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 $\mathbb{E} = \mathbb{F}$.*

Demonstração. $(i) \Rightarrow (ii)$: Seja $f \in \mathbb{F}[X]$, com $\mathrm{gr}(f) > 0$. Então, de (i), f admite uma raiz $\alpha \in \mathbb{F}$. Segue que $f = (X - \alpha)g(X)$, com $\mathrm{gr}(g) < \mathrm{gr}(f)$. Por indução no grau do polinômio, segue que g é produto de polinômios de grau 1. Portanto, f é produto de polinômios de grau 1.
$(ii) \Rightarrow (iii)$: Seja $f \in \mathbb{F}[X]$ um polinômio irredutível. Então, de (ii), segue que $f = (X - \alpha_1) \cdots (X - \alpha_m)$. Como f é irredutível, necessariamente $m = 1$, e portanto, $\mathrm{gr}(f) = 1$.
$(iii) \Rightarrow (iv)$: Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica. Seja $a \in \mathbb{E}$, e p o seu polinômio minimal sobre $\mathbb{F}$. Por (iii), segue que $\mathrm{gr}(p) = 1$. Portanto, $a \in \mathbb{F}$, e então, $\mathbb{E} = \mathbb{F}$.
$(iv) \Rightarrow (v)$: Se $\mathbb{E}/\mathbb{F}$ é uma extensão finita, então é também uma extensão algébrica. Portanto, de (iv), obtemos que $\mathbb{E} = \mathbb{F}$.
$(v) \Rightarrow (i)$: Seja $f \in \mathbb{F}[X]$ com $\mathrm{gr}(f) > 0$. Então, do Teorema 2.10, existe uma extensão de corpos finita $\mathbb{E}/\mathbb{F}$ de modo que $f(a) = 0$ para algum $a \in \mathbb{E}$. Mas, de (v), segue que $\mathbb{F} = \mathbb{E} \ni a$. Portanto, f admite raiz em $\mathbb{F}$. □

Definição 4.2. Dizemos que $\mathbb{F}$ é um corpo *algebricamente fechado* se satisfaz uma das condições do teorema anterior (e portanto, satisfaz todas as condições).

Exemplo 4.1. $\mathbb{C}$ é um corpo algebricamente fechado. Esse fato é conhecido como o Teorema Fundamental da Álgebra.

Definição 4.3. Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos. Dizemos que $\mathbb{E}$ é um *fecho algébrico* de $\mathbb{F}$ se:

(i) a extensão $\mathbb{E}/\mathbb{F}$ é algébrica,
(ii) $\mathbb{E}$ é um corpo algebricamente fechado.

Provaremos primeiro que, se já sabemos que existe um corpo que é algebricamente fechado Ω contendo $\mathbb{F}$, então um fecho algébrico de $\mathbb{F}$ pode ser tomado como sendo um subcorpo de Ω.

Proposição 4.4. *Seja $\Omega/\mathbb{F}$ uma extensão de corpos. Se Ω é algebricamente fechado, então o fecho de $\mathbb{F}$ em Ω é algebricamente fechado.*

Demonstração. Seja $\mathbb{E} = \{a \in \Omega \mid \ a \text{ é algébrico sobre } \mathbb{F}\}$. Já vimos que $\mathbb{E}$ é um corpo contendo $\mathbb{F}$, e $\mathbb{E}/\mathbb{F}$ é uma extensão algébrica de corpos (Teorema 3.8). Assim, basta mostrarmos que $\mathbb{E}$ é um corpo algebricamente fechado. Seja $f \in \mathbb{E}[X]$ um polinômio de grau não nulo. Então $f \in \Omega[X]$, e portanto, admite uma raiz $a \in \Omega$. Como a satisfaz um polinômio em $\mathbb{E}[X]$, segue que a é algébrico sobre $\mathbb{E}$. Mas então, do Teorema 3.7, segue que a é algébrico sobre $\mathbb{F}$. Assim, da construção, obtemos que $a \in \mathbb{E}$. Portanto, f admite uma raiz em $\mathbb{E}$. Então, $\mathbb{E}$ é um corpo algebricamente fechado. □

Exemplo 4.2. $\mathbb{A} := \{z \in \mathbb{C} \text{ algébrico sobre } \mathbb{Q}\}$ é um corpo algebricamente fechado. Portanto, $\mathbb{A}$ é um fecho algébrico de $\mathbb{Q}$.

Utilizando o Lema de Zorn, provaremos a seguir que todo corpo admite um fecho algébrico, independente da existência de um corpo algebricamente fechado maior.

Teorema 4.5. *Seja $\mathbb{F}$ um corpo. Então $\mathbb{F}$ admite um fecho algébrico.*

Demonstração. Seja

$$\mathscr{F} = \{\mathbb{E} \text{ corpo} \mid \mathbb{F} \subseteq \mathbb{E} \text{ e } \mathbb{E}/\mathbb{F} \text{ é extensão algébrica}\},$$

ordenado por inclusão. A família $\mathscr{F}$ é não vazia, pois $\mathbb{F} \in \mathscr{F}$. Seja $\mathscr{C}$ uma cadeia em $\mathscr{F}$. Provaremos que $\mathscr{C}$ admite uma cota superior em $\mathscr{F}$. Para isso, seja $\mathbb{L} = \bigcup_{\mathbb{E}_i \in \mathscr{C}} \mathbb{E}_i$. Então, $\mathbb{F} \subseteq \mathbb{L}$ por construção. Além disso, dados $0 \neq a, b \in \mathbb{L}$, existem $\mathbb{E}_i, \mathbb{E}_j \in \mathscr{C}$ tais que $a \in \mathbb{E}_i$ e $b \in \mathbb{E}_j$. Sendo $\mathscr{C}$ uma cadeia, segue que $\mathbb{E}_i \subseteq \mathbb{E}_j$ ou $\mathbb{E}_j \subseteq \mathbb{E}_i$. Podemos então supor, a menos de troca de índices, que $\mathbb{E}_i \subseteq \mathbb{E}_j$. Então, vale que $a, b \in \mathbb{E}_j$. Como $\mathbb{E}_j$ é um corpo, segue que $a - b, ab, a^{-1} \in \mathbb{E}_j \subseteq \mathbb{L}$. Portanto, $\mathbb{L}$ é um corpo. Ainda, como $\mathbb{E}_j/\mathbb{F}$ é uma extensão algébrica, segue que a é algébrico sobre $\mathbb{F}$. Daí, $\mathbb{L}/\mathbb{F}$ é uma extensão algébrica. Concluímos que $\mathbb{L} \in \mathscr{F}$. Além disso, por construção, $\mathbb{E}_i \subseteq \mathbb{L}$, para todo $\mathbb{E}_i \in \mathscr{C}$. Provamos então que a cadeia $\mathscr{C}$ admite uma cota superior em $\mathscr{F}$. Portanto, por Lema de Zorn, existe um elemento maximal $\bar{\mathbb{F}} \in \mathscr{F}$. Isso implica, em particular, que $\bar{\mathbb{F}}/\mathbb{F}$ é uma extensão algébrica. Concluiremos o teorema se mostrarmos que $\bar{\mathbb{F}}$ é um corpo algebricamente fechado. Seja então $\mathbb{M}/\bar{\mathbb{F}}$ uma extensão algébrica. Do Teorema 3.7, segue que $\mathbb{M}/\mathbb{F}$ é uma extensão algébrica. Da maximalidade de $\bar{\mathbb{F}}$,

segue que $\mathbb{M} = \bar{\mathbb{F}}$. Portanto, provamos que $\bar{\mathbb{F}}$ satisfaz a condição (iv) do Teorema 4.1, e então $\bar{\mathbb{F}}$ é um corpo algebricamente fechado. $\square$

Nosso próximo passo é garantir a unicidade de um fecho algébrico, a menos de um isomorfismo. Para isso, provaremos um resultado sobre extensão de monomorfismo de corpos, que será útil posteriormente.

Proposição 4.6. *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 algébrica e simples, e seja p_a o polinômio minimal de a sobre $\mathbb{F}$. Então, para cada raiz $\omega \in \Omega$ de $\varphi_0(p_a)$, existe um único homomorfismo de anéis $\varphi : \mathbb{E} \to \Omega$ que estende φ_0 e que satisfaz $\varphi(a) = \omega$. Todo homomorfismo $\mathbb{E} \to \Omega$ que estende φ_0 é construído dessa forma.*

Demonstração. Temos um isomorfismo $\mathbb{E} \cong \mathbb{F}[X]/(p_a)$, de modo que $a \mapsto X + (p_a)$. Seja $\omega \in \Omega$ uma raiz de $\varphi_0(p_a)$. Defina $\psi_\omega : \mathbb{F}[X] \to \Omega$ via $\psi_\omega(f(X)) = \varphi_0(f)(\omega)$, isto é,

$$\psi_\omega(\alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n) = \varphi_0(\alpha_0) + \varphi_0(\alpha_1)\omega + \cdots + \varphi_0(\alpha_n)\omega^n.$$

Como ω é raiz de $\varphi_0(p_a)$, temos que $\ker \psi_\omega \supseteq (p_a)$. Sendo $\psi_\omega \neq 0$ e (p_a) um ideal maximal de $\mathbb{F}[X]$, vale que $\ker \psi_\omega = (p_a)$. Assim, ψ_ω se fatora em

$$\mathbb{F}[X] \longrightarrow \mathbb{F}[X]/(p_a) \xrightarrow{\psi'_\omega} \Omega.$$

Seja $\varphi : \mathbb{E} \to \Omega$ a composição de ψ'_ω com o isomorfismo $\mathbb{E} \to \mathbb{F}[X]/(p_a)$. Então, por construção, vale que

$$\begin{aligned} \varphi(a) &= \psi'_\omega(X + (p_a)) = \psi_\omega(X) = \omega, \\ \varphi(\alpha) &= \psi'_\omega(\alpha) = \varphi_0(\alpha), \quad \forall \alpha \in \mathbb{F}. \end{aligned}$$

Portanto, $\varphi : \mathbb{E} \to \Omega$ é o monomorfismo de corpos requerido. A unicidade vale, pois seja $\varphi' : \mathbb{E} \to \Omega$ um monomorfismo que estende φ_0 e satisfaz $\varphi'(a) = \omega$. Seja $b \in \mathbb{E} = \mathbb{F}(a)$. Então, podemos escrever $b = \beta_0 + \beta_1 a + \cdots + \beta_s a^s$, $\beta_0, \ldots, \beta_s \in \mathbb{F}$. Daí

$$\varphi'(b) = \sum_{i=0}^{s} \varphi'(\beta_i)\varphi'(a^i) = \sum_{i=0}^{s} \varphi_0(\beta_i)\omega^i = \varphi(b).$$

Portanto, $\varphi' = \varphi$.

Agora, seja $\varphi'' : \mathbb{E} \to \Omega$ um monomorfismo de corpos que estende φ_0. Basta provarmos que $\omega' := \varphi''(a)$ é raiz de $\varphi_0(p_a)$. De fato, escreva $p_a = \gamma_0 + \gamma_1 X + \cdots + \gamma_m X^m$. Então

$$\begin{aligned} \varphi_0(p_a)(\omega') &= \varphi_0(\gamma_0) + \varphi_0(\gamma_1)\omega' + \cdots + \varphi_0(\gamma_m)\omega'^m \\ &= \varphi''(\gamma_0 + \gamma_1 a + \cdots + \gamma_m a^m) = \varphi''(0) = 0. \end{aligned}$$

Portanto, φ'' é construído como a única extensão de φ_0 que satisfaz $\varphi''(a) = \omega'$. □

Utilizando novamente o Lema de Zorn, podemos generalizar a proposição anterior no seguinte contexto:

Proposição 4.7. *Sejam $\mathbb{F}$ um corpo, Ω um corpo algebricamente fechado e $\varphi_0 : \mathbb{F} \to \Omega$ um monomorfismo de corpos. Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica. Então existe um monomorfismo de corpos $\varphi : \mathbb{E} \to \Omega$ que é uma extensão de φ_0.*

Demonstração. Seja

$$\mathscr{F} = \{(\mathbb{E}_i, \varphi_i) \mid \mathbb{F} \subseteq \mathbb{E}_i \subseteq \mathbb{E}, \text{ e } \varphi_i : \mathbb{E}_i \to \Omega \text{ estende } \varphi_0\}.$$

A família $\mathscr{F}$ é não vazia, pois $(\mathbb{F}, \varphi_0) \in \mathscr{F}$. Defina a ordem parcial em $\mathscr{F}$ da seguinte forma: $(\mathbb{E}_1, \varphi_1) \leq (\mathbb{E}_2, \varphi_2)$ se $\mathbb{E}_1 \subseteq \mathbb{E}_2$ e φ_2 estende φ_1. Seja $\mathscr{C} = \{(\mathbb{E}_i, \varphi_i)\}_{i \in \mathscr{I}}$ uma cadeia em $\mathscr{F}$. Defina $\mathbb{L} = \bigcup_{i \in \mathscr{I}} \mathbb{E}_i$. Então, por mesma ideia anterior, $\mathbb{L}$ é um corpo. Além disso, por construção, $\mathbb{F} \subseteq \mathbb{L} \subseteq \Omega$. Construa $\bar{\varphi} : \mathbb{L} \to \Omega$ da seguinte forma: dado $a \in \mathbb{L}$, seja $\mathbb{E}_i \ni a$. Então, defina $\bar{\varphi}(a) = \varphi_i(a)$. Tal construção está bem definida, pois se $a \in \mathbb{E}_i$ e $a \in \mathbb{E}_j$, então sendo $\mathscr{C}$ uma cadeia, vale que $(\mathbb{E}_i, \varphi_i) \leq (\mathbb{E}_j, \varphi_j)$ (a menos de trocar os índices). Portanto, $\mathbb{E}_i \subseteq \mathbb{E}_j$, e φ_j estende φ_i. Isso implica que $\varphi_i(a) = \varphi_j(a)$. Agora, dados $a, b \in \mathbb{L}$, existe $\mathbb{E}_i \ni a, b$ (pois $\mathscr{C}$ é cadeia). Então

$$\bar{\varphi}(a+b) = \varphi_i(a+b) = \varphi_i(a) + \varphi_i(b) = \bar{\varphi}(a) + \bar{\varphi}(b),$$
$$\bar{\varphi}(ab) = \varphi_i(ab) = \varphi_i(a)\varphi_i(b) = \bar{\varphi}(a)\bar{\varphi}(b).$$

Portanto, $\bar{\varphi}$ é um homomorfismo de anéis (e portanto, um monomorfismo de corpos). Por construção, $\bar{\varphi}$ estende φ_0. Assim, $(\mathbb{L}, \bar{\varphi}) \in \mathscr{F}$. Além disso, por construção, segue que $(\mathbb{E}_i, \varphi_i) \leq (\mathbb{L}, \bar{\varphi})$, $\forall (\mathbb{E}_i, \varphi_i) \in \mathscr{C}$. Segue que $\mathscr{C}$ admite cota superior em $\mathscr{F}$. Do Lema de Zorn, obtemos que $\mathscr{F}$ admite um elemento maximal $(\mathbb{M}, \varphi)$. Se $\mathbb{M} \neq \mathbb{E}$, então existe $a \in \mathbb{E}$, $a \notin \mathbb{M}$. Então $\mathbb{M}(a)$ á uma extensão própria de $\mathbb{M}$. Como $\mathbb{E}/\mathbb{F}$ é algébrica, segue que a é algébrico sobre $\mathbb{M}$. Da Proposição 4.6, exite $\varphi' : \mathbb{M}(a) \to \Omega$ que estende φ. Daí $(\mathbb{M}(a), \varphi') \in \mathscr{F}$ contradiz a maximalidade de $(\mathbb{M}, \varphi)$. Portanto, $\mathbb{M} = \mathbb{E}$ e $\varphi : \mathbb{E} \to \Omega$ estende $\varphi_0 : \mathbb{F} \to \Omega$. □

Como consequência, prova-se que um fecho algébrico de um corpo é único, a menos de isomorfismo:

Corolário 4.8. *Quaisquer dois fechos algébricos de um mesmo corpo $\mathbb{F}$ são isomorfos.*

Demonstração. Sejam $\bar{\mathbb{F}}_1$ e $\bar{\mathbb{F}}_2$ dois fechos algébricos de $\mathbb{F}$. Então existe monomorfismo de corpos $\iota_0 : \mathbb{F} \to \bar{\mathbb{F}}_2$. Como $\bar{\mathbb{F}}_1/\mathbb{F}$ é uma extensão algébrica, da Proposição 4.7, existe monomorfismo $\iota : \bar{\mathbb{F}}_1 \to \bar{\mathbb{F}}_2$ que estende ι_0. Portanto, temos extensão de corpos $\bar{\mathbb{F}}_2/\bar{\mathbb{F}}_1/\mathbb{F}$. Como $\bar{\mathbb{F}}_2/\mathbb{F}$ é uma extensão algébrica, segue que $\bar{\mathbb{F}}_2/\bar{\mathbb{F}}_1$ é uma extensão algébrica também. Sendo $\bar{\mathbb{F}}_1$ algebricamente fechado, segue que $\iota(\bar{\mathbb{F}}_1) = \bar{\mathbb{F}}_2$. Portanto, ι é um isomorfismo de corpos. □

5. Extensão normal

Começaremos com a seguinte definição, cuja importância ficará clara em breve. Seja Ω um corpo algebricamente fechado contendo um corpo $\mathbb{F}$. Dado $f \in \mathbb{F}[X]$, denote por $\mathscr{R}(f) \subseteq \Omega$ o conjunto das raízes de f em Ω, isto é,

$$\mathscr{R}(f) = \{a \in \Omega \mid f(a) = 0\}.$$

Definição 5.1. Sejam $\mathbb{F}$ um corpo, Ω um corpo algebricamente fechado contendo $\mathbb{F}$, e $\mathscr{S} \subseteq \mathbb{F}[X]$ um conjunto de polinômios. Seja $\mathscr{R}(\mathscr{S}) = \bigcup_{f\in\mathscr{S}} \mathscr{R}(f) \subseteq \Omega$ o conjunto de todas as raízes de todos os $f \in \mathscr{S}$. Um *corpo de raízes* de $\mathscr{S}$ sobre $\mathbb{F}$ (em Ω) é o corpo $\mathbb{L} = \mathbb{F}(\mathscr{R}(\mathscr{S}))$.

No caso em que $\mathscr{S}$ contém um único elemento, digamos $\mathscr{S} = \{f\}$, então dizemos simplesmente que $\mathbb{L}$ é um corpo de raízes de f sobre $\mathbb{F}$.

Exemplo 5.1.

(1) O corpo de raízes de X^2+1 sobre $\mathbb{Q}$ é $\mathbb{Q}(i,-i) = \mathbb{Q}(i)$.

(2) Seja $f = (X^2-2)(X^2-3)$. Suas raízes são $\pm\sqrt{2}, \pm\sqrt{3}$. Então o corpo de raízes de f sobre $\mathbb{Q}$ é $\mathbb{L} = \mathbb{Q}(\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Note que o mesmo $\mathbb{L}$ também é o corpo de raízes de $\mathscr{S} = \{X^2-2, X^2-3\}$ sobre $\mathbb{Q}$.

(3) Sejam $\xi \in \mathbb{C}$ tal que $\xi \neq \xi^3 = 1$. Então um corpo de raízes de X^3-2 sobre $\mathbb{Q}$ é $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2)$. O mesmo coincide com $\mathbb{Q}(\sqrt[3]{2}, \xi)$. De fato, por um lado, $\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2 \in \mathbb{Q}(\sqrt[3]{2}, \xi)$. Mas,

$$\xi = \frac{\sqrt[3]{2}\xi}{\sqrt[3]{2}} \in \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2).$$

Portanto, vale a igualdade de corpos.

(4) Sejam p primo e $\zeta \in \mathbb{C}$ tal que $\zeta \neq \zeta^p = 1$. As raízes de X^p-1 são $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$. Então, o corpo de raízes de X^p-1 sobre $\mathbb{Q}$ é $\mathbb{Q}(1,\zeta,\zeta^2,\ldots,\zeta^{p-1})$. Como $1,\zeta^2,\ldots,\zeta^{p-1} \in \mathbb{Q}(\zeta)$, segue que o corpo de raízes coincide com $\mathbb{Q}(\zeta)$. Note que o tal corpo coincide com a extensão simples de $\mathbb{Q}$ por uma das raízes de X^p-1.

Proposição 5.2. *Sejam $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$ um polinômio de grau $n \geq 1$. Seja $\mathbb{L}$ um corpo de raízes de f sobre $\mathbb{F}$. Então $\mathbb{L}/\mathbb{F}$ é finita e $[\mathbb{L} : \mathbb{F}] \leq n!$.*

Demonstração. Temos que $\mathbb{L} = \mathbb{F}(a_1, \ldots, a_m)$, em que as raízes de f são $\mathscr{R}(f) = \{a_1, \ldots, a_m\}$, em algum corpo algebricamente fechado Ω. Temos que $[\mathbb{F}(a_1) : \mathbb{F}] \leq n$ (coincide com o grau da componente irredutível de f o qual a_1 é raiz). Então $g(X) := \frac{f(X)}{X-a_1} \in \mathbb{F}(a_1)[X]$ é um

polinômio de grau $n-1$. Além disso, o corpo de raízes de g sobre $\mathbb{F}(a_1)$ é o próprio $\mathbb{L}$, por construção. Por indução, $[\mathbb{L} : \mathbb{F}(a_1)] \leq (n-1)!$. Portanto,

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{F}(a_1)][\mathbb{F}(a_1) : \mathbb{F}] \leq n!$$

□

Proposição 5.3. *Sejam $\mathbb{F}$ corpo, $\mathscr{S} \subseteq \mathbb{F}[X]$ e Ω um corpo algebricamente fechado contendo $\mathbb{F}$. O corpo de raízes $\mathbb{L} \subseteq \Omega$ de $\mathscr{S}$ sobre $\mathbb{F}$ é o menor subcorpo de Ω contendo $\mathbb{F}$, e de tal forma todo $f \in \mathscr{S}$ se decompõe como produto de polinômios de grau 1 em $\mathbb{L}[X]$.*

Demonstração. Seja $\mathbb{E} \subseteq \Omega$ um corpo de modo que todo polinômio em $\mathscr{S}$ se fatora como produto de polinômios de grau 1. Então, dado $f \in \mathscr{S}$, podemos escrever

$$f = \alpha(X - a_1) \cdots (X - a_m) \in \mathbb{E}[X].$$

Então $a_1, \ldots, a_m \in \mathbb{E}$, ou seja, $\mathscr{R}(f) \subseteq \mathbb{E}$. Portanto, $\mathscr{R}(\mathscr{S}) \subseteq \mathbb{E}$. Isso implica que $\mathbb{E} \supseteq \mathbb{F}(\mathscr{S}) = \mathbb{L}$. □

Definição 5.4. Sejam $\mathbb{E}_1$ e $\mathbb{E}_2$ corpos contendo um mesmo corpo $\mathbb{F}$. Um $\mathbb{F}$-*homomorfismo* (ou $\mathbb{F}$-monomorfismo) é um mapa $\eta : \mathbb{E}_1 \to \mathbb{E}_2$ tal que $\eta(\alpha) = \alpha$, $\forall \alpha \in \mathbb{F}$. Da mesma forma define-se $\mathbb{F}$-isomorfismo, $\mathbb{F}$-endomorfismo e $\mathbb{F}$-automorfismo.

Notação. Dado um homomorfismo de corpos $\eta : \mathbb{F} \to \mathbb{E}$, e $f \in \mathbb{F}[X]$, denote por $f^\eta = \eta(f)$ (relembre que η induz um homomorfismo de anéis $\mathbb{F}[X] \to \mathbb{E}[X]$).

O próximo resultado mostra que um corpo de raízes não depende do corpo maior em que o mesmo é construído:

Teorema 5.5. *Sejam Ω e Ω' dois corpos algebricamente fechados contendo $\mathbb{F}$, e seja $\mathscr{S} \subseteq \mathbb{F}[X]$. Sejam $\mathscr{R}$ e $\mathscr{R}'$ o conjunto das raízes de todos os $f \in \mathscr{S}$ em Ω e Ω', respectivamente. Sejam $\mathbb{L} = \mathbb{F}(\mathscr{R}) \subseteq \Omega$ e $\mathbb{L}' = \mathbb{F}(\mathscr{R}') \subseteq \Omega'$. Então, existe um $\mathbb{F}$-isomorfismo $\mathbb{L} \to \mathbb{L}'$.*

Demonstração. Por construção, a extensão de corpos $\mathbb{L}/\mathbb{F}$ é algébrica. Então, da Proposição 4.7, a aplicação identidade $\mathbb{F} \to \Omega'$ admite uma extensão $\eta : \mathbb{L} \to \Omega'$. Dado $f \in \mathscr{S}$, temos que $f^\eta = f$, pois η é um $\mathbb{F}$-monomorfismo. Como $\mathbb{L}$ é um corpo de raízes para todos os polinômios em $\mathscr{S}$, segue que

$$f = \alpha(X - a_1) \cdots (X - a_m), \quad a_1, \ldots, a_m \in \mathbb{L}.$$

Assim,

$$f = f^\eta = \alpha(X - \eta(a_1)) \cdots (X - \eta(a_m)).$$

Por um lado, da Proposição 5.3, vale que $\mathbb{L}' \subseteq \operatorname{Im}\eta$. Por outro lado, a mesma conta mostra que $\eta(\mathscr{R}) \subseteq \mathscr{R}'$. Daí $\operatorname{Im}\eta \subseteq \mathbb{F}(\mathscr{R}') = \mathbb{L}'$. Segue que $\operatorname{Im}\eta = \mathbb{L}'$. Conclui-se que $\eta : \mathbb{L} \to \mathbb{L}'$ é um $\mathbb{F}$-isomorfismo. □

Definição 5.6. Seja $\mathbb{L}/\mathbb{F}$ uma extensão algébrica de corpos. A extensão é dita ser *normal* se, para todo $a \in \mathbb{L}$, todas as raízes de $\operatorname{Irr}(a, \mathbb{F})$ (polinômio minimal de a sobre $\mathbb{F}$) estão em $\mathbb{L}$.

Teorema 5.7. *Sejam $\mathbb{L}/\mathbb{F}$ uma extensão de corpos algébrica, e Ω um corpo algebricamente fechado contendo $\mathbb{L}$. As seguintes afirmações são equivalentes:*

(i) *$\mathbb{L}/\mathbb{F}$ é uma extensão normal,*
(ii) *existe $S \subseteq \mathbb{L}$ de modo que $\mathbb{L} = \mathbb{F}(S)$, e, para todo $a \in S$, $\mathbb{L}$ contém todas as raízes de $\operatorname{Irr}(a, \mathbb{F})$,*
(iii) *$\mathbb{L}$ é o corpo de raízes sobre $\mathbb{F}$ de algum conjunto de polinômios em $\mathbb{F}[X]$,*
(iv) *Se $\sigma : \mathbb{L} \to \Omega$ é um $\mathbb{F}$-monomorfismo, então $\operatorname{Im}\sigma = \mathbb{L}$ (portanto, σ é um $\mathbb{F}$-automorfismo de $\mathbb{L}$),*
(v) *se $f \in \mathbb{F}[X]$ é irredutível sobre $\mathbb{F}$, e $\mathbb{L}$ contém uma raiz de f, então $\mathbb{L}$ contém todas as raízes de f.*

Demonstração. $(i) \Rightarrow (ii)$: Pode-se tomar $S = \mathbb{L}$. Por definição, $\mathbb{L}$ contém todas as raízes de todo $a \in \mathbb{L}$. Além disso, $\mathbb{L} = \mathbb{F}(S)$.
$(ii) \Rightarrow (iii)$: Por (ii), $\mathbb{L} = \mathbb{F}(S)$, em que, para todo $a \in S$, $\mathscr{R}(\operatorname{Irr}(a, \mathbb{F})) \subseteq \mathbb{L}$. Seja $\mathscr{S} = \{\operatorname{Irr}(a, \mathbb{F}) \mid a \in S\}$. Defina $\mathscr{R}(\mathscr{S}) \subseteq \Omega$. Como todo elemento de $\mathscr{R}(\mathscr{S})$ pertence a $\mathbb{L}$, obtemos que $\mathscr{R}(\mathscr{S}) \subseteq \mathbb{L}$. Por outro lado, $S \subseteq \mathscr{R}(\mathscr{S})$. Então $\mathbb{L} = \mathbb{F}(S) \subseteq \mathbb{F}(\mathscr{R}(\mathscr{S}))$. Portanto, vale a igualdade e $\mathbb{L}$ é o corpo de raízes de $\mathscr{S}$ sobre $\mathbb{F}$.
$(iii) \Rightarrow (iv)$: Seja $\mathbb{L}$ o corpo de raízes de $\mathscr{S}$ sobre $\mathbb{F}$. Seja $\sigma : \mathbb{L} \to \Omega$ um $\mathbb{F}$-monomorfismo. Para cada $f \in \mathbb{F}[X]$, podemos escrever $f = \alpha(X - a_1) \cdots (X - a_m)$, com $a_1, \ldots, a_m \in \mathbb{L}$. Portanto, $f = f^\eta = \alpha(X - \eta(a_1)) \cdots (X - \eta(a_m))$. Repetindo o argumento na demonstração do Teorema 5.5, obtemos que $\operatorname{Im}\sigma = \mathbb{L}$.
$(iv) \Rightarrow (v)$: Seja $f \in \mathbb{F}[X]$ irredutível e seja $a \in \mathbb{L}$ com $f(a) = 0$. Seja $b \in \Omega$ com $f(b) = 0$. Daí, da Proposição 4.6, existe um $\mathbb{F}$-monomorfismo $\eta_0 : \mathbb{F}(a) \to \Omega$ tal que $\eta_0(a) = b$. Da Proposição 4.7, segue que η_0 admite extensão $\eta : \mathbb{L} \to \Omega$, tal que $\eta(a) = b$. De (iv), segue que $\operatorname{Im}\eta = \mathbb{L}$. Portanto, $b = f(a) \in \mathbb{L}$. Conclui-se que $\mathscr{R}(f) \subseteq \mathbb{L}$.
$(v) \Rightarrow (i)$: Sejam $a \in \mathbb{L}$ e $p_a \in \mathbb{F}[X]$ seu polinômio minimal sobre $\mathbb{F}$. Então p_a é um polinômio irredutível que possui uma raiz em $\mathbb{L}$ (o próprio elemento a). De (v), segue que $\mathscr{R}(p_a) \subseteq \mathbb{L}$. Portanto, $\mathbb{L}/\mathbb{F}$ é extensão normal. □

A seguir, mostraremos exemplos e contra-exemplos de extensões normais.

Proposição 5.8. *Se* $[\mathbb{E}:\mathbb{F}]=2$*, então* $\mathbb{E}/\mathbb{F}$ *é uma extensão normal.*

Demonstração. Seja $a\in\mathbb{E}$. Se $a\in\mathbb{F}$, então seu polinômio minimal é $X-a$. Daí $\mathbb{E}$ contém todas as raízes desse polinômio (que é somente o elemento a). Assuma então que $a\notin\mathbb{F}$. Então, seu polinômio minimal p_a possui grau 2. Daí $p_a=(X-a)g(X)$, com $\mathrm{gr}(g)=1$. Assim, $\mathbb{E}$ possui a única raiz de g. Daí $\mathbb{E}$ possui todas as raízes de p_a. Conclui-se que $\mathbb{E}/\mathbb{F}$ é normal. □

Exemplo 5.2. A propriedade da extensão ser normal não é boa, no seguinte sentido. Sejam $\mathbb{L}/\mathbb{E}/\mathbb{F}$ extensões de corpos. Então, se duas das extensões são normais, não necessariamente a terceira será normal também. Os exemplos seguintes ilustram tal fato:

(1) $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ são extensões normais (pois ambos possuem grau 2). Porém, $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ não é uma extensão normal (pois X^4-2 possui raízes complexas, enquanto que $\mathbb{Q}[\sqrt[4]{2}]\subseteq\mathbb{R}$, por exemplo).

(2) São normais as seguintes extensões: $\mathbb{Q}[\sqrt[3]{2},\xi]/\mathbb{Q}[\sqrt[3]{2}]$ (pois o grau é 2) e $\mathbb{Q}[\sqrt[3]{2},\xi]/\mathbb{Q}$ (pois é o corpo de raízes de X^3-2 sobre $\mathbb{Q}$, conforme exemplo anterior). Porém, $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ não é normal (por que?).

Entretanto, temos o seguinte resultado:

Proposição 5.9. *Sejam* $\mathbb{L}/\mathbb{E}/\mathbb{F}$ *extensões de corpos. Se* $\mathbb{L}/\mathbb{F}$ *é normal, então* $\mathbb{L}/\mathbb{E}$ *é normal.*

Demonstração. Como $\mathbb{L}/\mathbb{F}$ é normal, do Teorema 5.7.(iii), $\mathbb{L}$ é o corpo de raízes sobre $\mathbb{F}$ de algum conjunto $\mathscr{S}\subseteq\mathbb{F}[X]$. Porém, $\mathscr{S}\subseteq\mathbb{F}[X]\subseteq\mathbb{E}[X]$. Por um lado, $\mathbb{L}=\mathbb{F}(\mathscr{R}(\mathscr{S}))\subseteq\mathbb{E}(\mathscr{R}(\mathscr{S}))$. Por outro, $\mathscr{R}(\mathscr{S})\subseteq\mathbb{L}$, e daí $\mathbb{E}(\mathscr{R}(\mathscr{S}))\subseteq\mathbb{L}$. Portanto, $\mathbb{L}$ é o corpo de raízes de $\mathscr{S}$ sobre $\mathbb{E}$. Daí $\mathbb{L}/\mathbb{E}$ é normal. □

5.1. **Fecho normal.** Já vimos que a extensão de corpos $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ não é normal. Isso se deve ao fato de que $\mathbb{Q}(\sqrt[3]{2})$ não contém todas as raízes de X^3-2 (o polinômio minimal de $\sqrt[3]{2}$ sobre $\mathbb{Q}$). Então, é razoável pensar que podemos obter uma extensão normal se considerarmos um corpo contendo $\mathbb{Q}(\sqrt[3]{2})$ e as demais raízes de X^3-2. De fato, tal corpo é uma extensão normal porque a construção coincide com o corpo de raízes de X^3-2 sobre $\mathbb{Q}$. Provaremos que a tal construção pode ser feita para uma extensão algébrica qualquer.

Proposição 5.10. *Sejam $\mathbb{E}/\mathbb{F}$ uma extensão algébrica de corpos, e Ω um corpo algebricamente fechado contendo $\mathbb{E}$. Seja*

$$\mathscr{N} = \{\mathbb{K} \mid \mathbb{E} \subseteq \mathbb{K} \subseteq \Omega,\ \mathbb{L}/\mathbb{F} \text{ é extensão normal}\}.$$

Então $\mathbb{L} := \bigcap_{\mathbb{K}\in\mathscr{N}} \mathbb{K}$ é um corpo e $\mathbb{L}/\mathbb{F}$ é uma extensão normal.

Demonstração. Seja $a \in \mathbb{L}$. Assim, $a \in \mathbb{K}$, $\forall \mathbb{K} \in \mathscr{N}$. Sendo cada $\mathbb{K}/\mathbb{F}$ normal, vale que $\mathscr{R}(\mathrm{Irr}(a,\mathbb{F})) \subseteq \mathbb{K}$, $\forall \mathbb{K} \in \mathscr{N}$. Portanto, $\mathscr{R}(\mathrm{Irr}(a,\mathbb{F})) \subseteq \mathbb{L}$. Daí, $\mathbb{L}/\mathbb{F}$ é normal. □

Assim, o corpo construído na proposição anterior é o menor corpo contendo $\mathbb{E}$ de modo que é uma extensão normal de $\mathbb{F}$. Provamos então a existência do fecho normal, definido a seguir:

Definição 5.11. Sejam $\mathbb{E}/\mathbb{F}$ uma extensão algébrica, e Ω um corpo algebricamente fechado contendo $\mathbb{E}$. O *fecho normal* da extensão $\mathbb{E}/\mathbb{F}$ (em Ω) é o menor subcorpo $\mathbb{L} \subseteq \Omega$ contendo $\mathbb{E}$ de modo que $\mathbb{L}/\mathbb{F}$ é extensão normal. Denota-se tal corpo por $N_\Omega(\mathbb{E}/\mathbb{F})$.

Note que o fecho normal é relativo a uma extensão de corpos, e não a um corpo. Ainda, por definição, vale que $\mathbb{E} \subseteq N_\Omega(\mathbb{E}/\mathbb{F})$, e

$$N_\Omega\left(N_\Omega(\mathbb{E}/\mathbb{F})/\mathbb{F}\right) = N_\Omega(\mathbb{E}/\mathbb{F}).$$

Assim, o fecho normal é uma operação de fecho.

O fecho normal pode ser caracterizado da seguinte forma:

Proposição 5.12. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica.*

(i) *Seja $\mathscr{S} = \{\mathrm{Irr}(a,\mathbb{F}) \mid a \in \mathbb{E}\}$. O fecho normal de $\mathbb{E}/\mathbb{F}$ é o corpo de raízes de $\mathscr{S}$ sobre $\mathbb{F}$.*

(ii) *Assuma que $\mathbb{E} = \mathbb{F}(a_1,\ldots,a_m)$ é finita. Então, o fecho normal de $\mathbb{E}/\mathbb{F}$ é o corpo de raízes de $\{\mathrm{Irr}(a_1,\mathbb{F}),\ldots,\mathrm{Irr}(a_m,\mathbb{F})\}$ sobre $\mathbb{F}$.*

Demonstração. (i) Sejam $\mathbb{L}$ o fecho normal de $\mathbb{E}/\mathbb{F}$, e $a \in \mathbb{E} \subseteq \mathbb{L}$. Portanto, $\mathbb{L} \supseteq \mathscr{R}(\mathrm{Irr}(a,\mathbb{F}))$. Assim, $\mathbb{L}$ contém o corpo de raízes de $\mathscr{S}$ sobre $\mathbb{F}$. Por outro lado, $\mathbb{F}(\mathscr{R}(\mathscr{S}))$ é uma extensão normal de $\mathbb{F}$. Por construção, o mesmo contém $\mathbb{E}$. Assim, como $\mathbb{L}$ é a menor extensão normal de $\mathbb{F}$ contendo $\mathbb{E}$, segue que $\mathbb{L} \subseteq \mathbb{F}(\mathscr{R}(\mathscr{S}))$. Portanto, vale a igualdade.
(ii) Segue os mesmos passos de (i) (exercício). □

5.2. **Monomorfismos.** Para o resto desta seção, assuma que $\mathbb{E}/\mathbb{F}$ é uma extensão algébrica de corpos, e Ω é um corpo algebricamente fechado contendo $\mathbb{E}$.

Definição 5.13. Denota-se

$$\mathrm{Mono}_{\mathbb{F}}(\mathbb{E},\Omega) = \{\mathbb{F}\text{-monomorfismo } \mathbb{E} \to \Omega\},$$
$$\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \{\mathbb{F}\text{-automorfismo de } \mathbb{E}\}.$$

Alguns autores adotam a notação $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = \mathrm{Aut}(\mathbb{E}/\mathbb{F})$, e denominam de o *grupo de Galois* da extensão $\mathbb{E}/\mathbb{F}$.

Munido da composição de funções, $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é um grupo.

Uma vez que $\mathbb{E} \subseteq \Omega$, temos o mapa identidade $\mathbb{E} \to \Omega$. Assim, a composição de um $\mathbb{F}$-automorfismo de $\mathbb{E}$ com a tal inclusão é um $\mathbb{F}$-monomorfismo $\mathbb{E} \to \Omega$. Portanto, podemos ver $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) \subseteq \mathrm{Mono}_{\mathbb{F}}(\mathbb{E},\Omega)$. Reciprocamente, se $\sigma \in \mathrm{Mono}_{\mathbb{F}}(\mathbb{E},\Omega)$ é tal que $\mathrm{Im}\,\sigma = \mathbb{E}$, então σ é um $\mathbb{F}$-automorfismo de $\mathbb{E}$. Daí, um tal σ pode ser visto como um elemento de $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Mas, em geral, os dois conjuntos não coincidem. Entretanto, as extensões normais são caracterizadas como sendo as extensões em que valem a coincidência dos conjuntos. Já demonstramos tal fato (Teorema 5.7, equivalências (i) e (iv)):

Teorema 5.14. *Sejam $\mathbb{L}/\mathbb{F}$ uma extensão algébrica de corpos, e Ω um corpo algebricamente fechado contendo $\mathbb{L}$. Então $\mathbb{L}/\mathbb{F}$ é normal se, e somente se,* $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) = \mathrm{Mono}_{\mathbb{F}}(\mathbb{L},\Omega)$. □

O próximo resultado será importante para nossas construções futuras:

Teorema 5.15. *Seja $\mathbb{L}/\mathbb{F}$ uma extensão normal. Seja $\mathbb{K}$ um corpo intermediário, isto é, $\mathbb{L}/\mathbb{K}/\mathbb{F}$. As seguintes afirmações são equivalentes:*

(i) *$\mathbb{K}/\mathbb{F}$ é uma extensão normal,*
(ii) *$\sigma\mathbb{K} \subseteq \mathbb{K}$, $\forall \sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$.*

Neste caso, temos um homomorfismo de grupos sobrejetor $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) \to \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ *dada por restrição. O seu núcleo é* $\mathrm{Aut}(\mathbb{L}/\mathbb{K})$.

Demonstração. $(i) \Rightarrow (ii)$: Seja $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$. Então podemos ver σ como sendo um $\mathbb{F}$-monomorfismo $\mathbb{L} \to \Omega$. Como $\mathbb{K}/\mathbb{F}$ é normal, segue que $\sigma(\mathbb{K}) = \mathbb{K}$.
$(ii) \Rightarrow (i)$: Seja $\sigma_0 : \mathbb{K} \to \Omega$ um monomorfismo de corpos. Como a extensão $\mathbb{L}/\mathbb{K}$ é algébrica, existe uma extensão $\sigma : \mathbb{L} \to \Omega$ de σ_0. Como $\mathbb{L}/\mathbb{F}$ é normal, vale que $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$. O item (ii) implica que $\sigma(\mathbb{K}) \subseteq \mathbb{K}$. Entretanto, σ restrita a $\mathbb{K}$ coincide com σ_0. Portanto, $\sigma_0(\mathbb{K}) = \mathbb{K}$. Isso implica que $\mathbb{K}/\mathbb{F}$ é normal.

Agora, pela caracterização (ii), o mapa $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) \to \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ é um homomorfismo de grupos bem definido. Seja $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$ tal que a sua restrição $\sigma|_{\mathbb{K}}$ é a identidade de $\mathbb{K}$. Então, $\sigma(a) = a$, $\forall a \in \mathbb{K}$. Isso implica que $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{K})$. Por outro lado, todo $\sigma_0 \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$

admite uma extensão $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$. Como $\sigma_0 = \sigma|_{\mathbb{K}}$, temos que o homomorfismo é sobrejetor. □

Exemplo 5.3. A seguir, exibiremos alguns exemplos de grupo de Galois de alguma extensão, isto é, do grupo $\mathrm{Aut}(\mathbb{L}/\mathbb{F})$.

(1) $\mathrm{Aut}(\mathbb{F}/\mathbb{F}) = \{1\}$.
(2) $\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q}) = \{1, \sigma_i\}$, em que $\sigma_i(a+bi) = a-bi$ é a conjugação complexa.
(3) $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$, em que $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$.
(4) $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$. Isso porque um monomorfismo $\psi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ é tal que $\psi(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2\}$, em que $\xi \neq \xi^3 = 1$. Assim, existe um único monomorfismo $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ cuja imagem coincide com o próprio $\mathbb{Q}(\sqrt[3]{2})$. Portanto, $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ possui um único elemento.

6. Extensão separável

Nosso interesse nesta seção será entender quando um polinômio irredutível possui raízes múltiplas em algum corpo algebricamente fechado. Veremos que tal situação é possível somente em característica positiva.

Definição 6.1. Sejam $\mathbb{F}$ um corpo, $f \in \mathbb{F}[X]$, Ω um corpo algebricamente fechado contendo $\mathbb{F}$, e $a \in \Omega$, com $f(a) = 0$. Dizemos que a *multiplicidade* da raiz a de f é m se $(X-a)^m$ divide f, mas $(X-a)^{m+1}$ não divide f. Se a multiplicidade de uma raiz a é 1, então dizemos que a é uma raiz *simples*. Caso contrário, dizemos que a é uma raiz *múltipla*.

Definição 6.2. Um polinômio f é dito ser *separável* se todas as suas raízes (em algum corpo algebricamente fechado) são simples.

Uma ferramenta prática para estudarmos a multiplicidade de uma raiz é dada pela derivada formal, definida a seguir. Sejam $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$. Escreva $f = \alpha_0 + \alpha_1 X + \cdots + \alpha_m X^m$. A *derivada formal* de f, denotada por f', é, por definição

$$f'(X) = \alpha_1 + 2\alpha_2 X + \cdots + m\alpha_m X^{m-1} = \sum_{i=0}^{m-1} (i+1)\alpha_{i+1} X^i.$$

A propriedade de Leibniz vale para a derivada formal, isto é, se $f, g \in \mathbb{F}[X]$, então

$$(fg)' = f'g + fg'.$$

Outra propriedade interessante é a regra da cadeia:

$$(f(g(X)))' = f'(g(X))g'(X).$$

A verificação de ambas propriedades fica de exercício. Por fim, temos o seguinte, cuja demonstração fica de exercício:

Lema 6.3. *$f' = 0$ se, e somente se, vale um dos seguintes itens:*

1. *ou* $\operatorname{car}\mathbb{F} = 0$ *e* $f \in \mathbb{F}$,
2. *ou* $\operatorname{car}\mathbb{F} = p > 0$ *e* $f = g(X^p)$, *para algum* $g \in \mathbb{F}[X]$ *(ou seja,* $f \in \mathbb{F}[X^p]$*).*

Agora, assuma que $a \in \Omega$ é uma raiz de f. Então $f = (X-a)^m g$, para algum $g \in \Omega[X]$, em que $g(a) \neq 0$, e $m \geq 1$. Então

$$f' = m(X-a)^{m-1} g + (X-a)^m g'.$$

Assumindo, em princípio, que $m > 1$, temos então que $f'(a) = 0$. Por outro lado, se $m = 1$, então $f'(a) = (a-a)g' + g(a) = g(a) \neq 0$. Portanto, acabamos de provar o seguinte critério:

Proposição 6.4. *Seja $a \in \Omega$ uma raiz de $f \in \mathbb{F}[X]$. Então a é raiz múltipla de f se, e somente se, $f'(a) = 0$.* □

De um modo a não se prender a um único elemento $a \in \Omega$, temos o seguinte resultado:

Teorema 6.5. *Seja $f \in \mathbb{F}[X]$. Então f é separável se, e só se,* $\mathrm{mdc}(f, f') = 1$.

Demonstração. Se f não é separável, então $f = (X-a)^2 g$, para algum $g \in \mathbb{F}[X]$. Daí $f' = (X-a)((X-a)g' + 2g)$. Portanto, $\mathrm{mdc}(f, f') \neq 1$. Reciprocamente, assuma que $g(X) := \mathrm{mdc}(f, f') \neq 1$. Então, existe $a \in \Omega$ raiz de g. Daí, $f(a) = f'(a) = 0$. Da Proposição 6.4, segue que a é raiz múltipla da f. Conclui-se que f não é separável. □

Note que o critério $\mathrm{mdc}(f, f') = 1$ pode ser enunciado de forma independente da existência de um corpo maior Ω.

No caso especial em que o polinômio é assumido ser irredutível, obtemos um critério mais simples:

Teorema 6.6. *Seja $f \in \mathbb{F}[X]$ irredutível. Então f é separável se, e somente se, $f' \neq 0$.*

Assim, se f é irredutível e vale um entre (i) ou $\mathrm{car}\,\mathbb{F} = 0$, (ii) ou $\mathrm{car}\,\mathbb{F} = p > 0$ e $f \notin \mathbb{F}[X^p]$, então f é separável.

Demonstração. Assuma que $f' = 0$. Então $\mathrm{mdc}(f, f') \neq 1$. Portanto, do Teorema 6.5, segue que f não é separável. Reciprocamente, assuma que f não é separável. Seja $a \in \Omega$ uma raiz múltipla de f. Então, da Proposição 6.4, segue que $f'(a) = 0$. Isso implica que $f' \in (f)$ (ideal gerado por f em $\mathbb{F}[X]$). Como $\mathrm{gr}(f') < \mathrm{gr}(f)$, segue que $f' = 0$.

A última afirmação do enunciado é válida devido a caracterização de quando $f' = 0$ (Lema 6.3). □

O próximo resultado nos mostra uma caracterização de polinômios irredutíveis que não são separáveis:

Teorema 6.7. *Sejam $\mathbb{F}$ um corpo de característica $p > 0$, e $f \in \mathbb{F}[X]$ irredutível. Então existem $m \geq 0$ e um polinômio irredutível e separável $g \in \mathbb{F}[X]$ tal que $f = g(X^{p^m})$.*

Demonstração. Se f é um polinômio separável, então a conclusão é válida se tomarmos $g = f$ e $m = 0$. Se f não é separável, então, do Teorema 6.6, $f' = 0$. Portanto, do Lema 6.3, $f = g(X^p)$, para algum $g \in \mathbb{F}[X]$. Se $g = g_1 g_2$, então $f = g_1(X^p)g_2(X^p)$. Portanto, como f é irredutível, segue que g é irredutível. Por indução no grau do polinômio, vale que g é separável, ou $g = h(X^{p^m})$, para algum $h \in \mathbb{F}[X]$ irredutível e separável. Portanto, $f = h(X^{p^{m+1}})$. □

Como consequência, obtemos a seguinte propriedade:

Corolário 6.8. *Seja $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$ um polinômio irredutível. Então todas as suas raízes possuem a mesma multiplicidade.*

Demonstração. Exercício. □

Definição 6.9. Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica de corpos. Dizemos que $a \in \mathbb{E}$ é *separável* sobre $\mathbb{F}$ se $\mathrm{Irr}(a, \mathbb{F})$ é um polinômio separável. Dizemos que a extensão $\mathbb{E}/\mathbb{F}$ é *separável* se todo $a \in \mathbb{E}$ é separável sobre $\mathbb{F}$.

Note que $a \in \mathbb{E}$ é separável sobre $\mathbb{F}$ se, e somente se, a é raiz de um polinômio separável em $\mathbb{F}[X]$.

Se $\operatorname{car}\mathbb{F} = p > 0$, então o mapa $F : \mathbb{F} \to \mathbb{F}$ definida por $F(a) = a^p$ é um endomorfismo de corpos (necessariamente injetora). A sua imagem é denotada por $\mathbb{F}^p$.

Definição 6.10. Seja $\mathbb{F}$ um corpo. Dizemos que $\mathbb{F}$ é *perfeito* se $\operatorname{car}\mathbb{F} = 0$, ou se $\operatorname{car}\mathbb{F} = p > 0$ e $\mathbb{F}^p = \mathbb{F}$.

Exemplo 6.1. Seja $\mathbb{F}$ um corpo de característica $p > 0$. Então $\mathbb{K} := \mathbb{F}(X)$ não é perfeito. Seja $\mathbb{E} = \mathbb{F}(X^p) \subseteq \mathbb{K}$. Então, veremos a seguir que a extensão $\mathbb{K}/\mathbb{E}$ não é separável.

Proposição 6.11. *Todo corpo finito e todo corpo algebricamente fechado são perfeitos.*

Demonstração. Seja $\mathbb{F}$ um corpo finito de característica $p > 0$. Então, sendo o mapa $F(a) = a^p$ injetivo e $\mathbb{F}$ finito, vale que F é sobrejetivo. Portanto, $\mathbb{F}^p = \mathbb{F}$.

Agora, seja $\mathbb{F}$ um corpo algebricamente fechado. Dado $a \in \mathbb{F}$, o polinômio $X^p - a$ admite alguma raiz em $\mathbb{F}$, digamos $b \in \mathbb{F}$. Portanto, $b^p = a$. Isso mostra que $\mathbb{F}^p = \mathbb{F}$. □

A seguir, mostraremos a relação entre corpos perfeitos e polinômios e extensões separáveis.

Teorema 6.12. *Seja $\mathbb{F}$ um corpo. As seguintes afirmações são equivalentes:*

(i) *O corpo $\mathbb{F}$ é perfeito.*
(ii) *Todo polinômio irredutível em $\mathbb{F}[X]$ é separável.*
(iii) *Toda extensão algébrica $\mathbb{E}/\mathbb{F}$ é separável.*

Demonstração. Se $\operatorname{car}\mathbb{F} = 0$, então todas as afirmações são válidas. Portanto, assuma que $\operatorname{car}\mathbb{F} = p > 0$.

$(i) \Rightarrow (ii)$: Seja $f \in \mathbb{F}[X]$ um polinômio irredutível. Se f não é separável, então do Teorema 6.6, $f \in \mathbb{F}[X^p]$. Portanto,

$$f(X) = \alpha_0 + \alpha_1 X^p + \alpha_2 X^{2p} + \cdots + \alpha_m X^{mp}.$$

Como $\mathbb{F}$ é perfeito (por (i)), segue que existem $\beta_0, \ldots, \beta_m \in \mathbb{F}$, de modo que $\beta_i^p = \alpha_i$, $i = 0, 1, \ldots, m$. Portanto,

$$f = \beta_0^p + \beta_1^p X^p + \cdots + \beta_m^p X^p = (\beta_0 + \beta_1 X + \cdots + \beta_m X^m)^p .$$

Isso contradiz a irredutibilidade de f. Portanto, f é separável.

$(ii) \Rightarrow (iii)$: Sejam $\mathbb{E}/\mathbb{F}$ uma extensão algébrica, e $a \in \mathbb{E}$. Então, $\mathrm{Irr}(a, \mathbb{F})$ é irredutível. De (ii) segue que o mesmo é separável. Portanto, a extensão $\mathbb{E}/\mathbb{F}$ é separável.

$(iii) \Rightarrow (i)$: Dado $a \in \mathbb{F}$, seja $f = X^p - a$. Se b é uma raiz de f, então $b^p = a$, e portanto, $f = X^p - b^p = (X - b)^p$. Daí, o polinômio minimal p_b de b sobre $\mathbb{F}$ divide $(X - b)^p$. Então, todas as suas raízes são iguais a b. Como a extensão $\mathbb{F}[b]/\mathbb{F}$ é algébrica, de (iii), vale que a mesma é separável. Portanto, p_b é separável. Assim, $p_b = X - b$. Segue que $b \in \mathbb{F}$. Então $\mathbb{F}^p = \mathbb{F}$, ou seja, $\mathbb{F}$ é perfeito. □

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

Lema 6.13. *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 6.14. *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.* □

6.2. **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

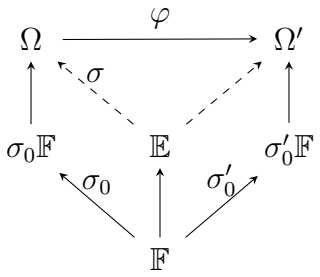
$$\mathrm{Mono}_{\sigma_0}(\mathbb{E}, \Omega) = \{\sigma : \mathbb{E} \to \Omega \text{ extensão de } \sigma_0\}.$$

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 6.15. *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 4.7, 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 6.16. 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 4.6) 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 6.17. *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 4.6, 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 6.18. *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 4.6, 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 6.17, 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 4.6, obtemos que $[\mathbb{F}(a) : \mathbb{F}]_s < [\mathbb{F}(a) : \mathbb{F}]$. Da Proposição 6.17, vale que $[\mathbb{E} : \mathbb{F}(a)]_s \leq [\mathbb{E} : \mathbb{F}(a)]$. Portanto, novamente da Proposição 6.17, 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 6.19. *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 6.20. *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 6.18 e Proposição 6.17, 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 6.18, obtemos que $\mathbb{L}/\mathbb{F}$ é separável. Agora, assuma que as extensões $\mathbb{L}/\mathbb{E}$ e $\mathbb{E}\mathbb{F}$ 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, sendo a extensão $\mathbb{E}/\mathbb{F}$ separável, os elementos $b_0, \ldots, b_m$ são separáveis sobre $\mathbb{F}$. Portanto, do Teorema 6.18, 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 6.21. *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 6.18, 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 5.14, 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 6.17 e da discussão que precede Teorema 5.14, 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 6.22. Uma extensão de corpos $\mathbb{E}/\mathbb{F}$ é dita ser *galoisiana* (ou de Galois) se a extensão é separável e normal.

7. Corpos finitos

Seja $p > 0$ um número primo. Denotaremos por $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ o corpo finito com p elementos. Se $\mathbb{F}$ é um corpo de característica $p > 0$, então $F : \mathbb{F} \to \mathbb{F}$ denota o *homomorfismo de Frobenius*, isto é, $F(a) = a^p$, para cada $a \in \mathbb{F}$. Já vimos que F é um monomorfismo de anéis. Denotaremos por $\bar{\mathbb{F}}_p$ um fecho algébrico de $\mathbb{F}_p$.

Teorema 7.1. *Seja $m \geq 1$. Então existe um corpo $\mathbb{E}$ com exatamente p^m elementos. Tal corpo é único, a menos de um isomorfismo. Ainda mais, as seguintes caracterizações de $\mathbb{E}$ são válidas:*

(1) *$\mathbb{E}$ é o corpo de raízes de $X^{p^m} - X$ sobre $\mathbb{F}_p$.*
(2) *$\mathbb{E}$ é o conjunto das raízes de $X^{p^m} - X$ em $\bar{\mathbb{F}}_p$.*

Demonstração. Seja $f(X) = X^{p^m} - X \in \mathbb{F}_p[X]$. Primeiramente, note que a derivada formal de f é $f' = -1$. Como $\mathrm{mdc}(f, f') = 1$, segue que todas as raízes de f são distintas.

Afirmação 1. Se $\mathbb{E} \subseteq \bar{\mathbb{F}}_p$ é um corpo que possui exatamente p^m elementos, então $\mathbb{E} = \{a \in \bar{\mathbb{F}}_p \mid f(a) = 0\}$.

De fato, o grupo multiplicativo de $\mathbb{E}$ possui exatamente $p^m - 1$ elementos. Portanto, cada $a \in \mathbb{E}^\times$ satisfaz $a^{p^m-1} = 1$. Assim, cada elemento de $\mathbb{E}$ satisfaz $X^{p^m} - X = 0$. Daí, $\mathbb{E}$ consiste das raízes de f.

Afirmação 2. O conjunto $\mathscr{R}(f) = \{a \in \bar{\mathbb{F}}_p \mid f(a) = 0\}$ é um corpo contendo $\mathbb{F}_p$.

De fato, dados $a, b \in \mathscr{R}(f)$, temos que:

- $f(a+b) = (a+b)^{p^m} - (a+b) = f(a) + f(b) = 0$,
- $f(ab) = (ab)^{p^m} - ab = (a^{p^m} - a + a)b^{p^m} - ab = f(a) + af(b) = 0$,
- como $\alpha^p = \alpha$, para cada $\alpha \in \mathbb{F}_p$, segue que $f(\alpha) = 0$. Assim, $\mathbb{F}_p \subseteq \mathscr{R}(f)$.

Portanto, $\mathscr{R}(f)$ é um anel contendo $\mathbb{F}_p$. Como $\mathscr{R}(f)$ é um domínio (pois é subanel do corpo $\bar{\mathbb{F}}_p$), segue que $\mathscr{R}(f)$ é corpo.

Afirmação 3. O corpo de raízes (em $\bar{\mathbb{F}}_p$) de f sobre $\mathbb{F}_p$ possui exatamente p^m elementos.

De fato, pela Afirmação 2, o conjunto $\mathscr{R}(f)$ é um corpo. Além disso, o mesmo é o menor corpo contendo $\mathbb{F}_p$ e as raízes de f. Portanto, $\mathscr{R}(f)$ é o corpo de raízes de f sobre $\mathbb{F}_p$

Portanto, existe um corpo com exatamente p^m elementos. Se $\mathbb{E}'$ é um outro corpo com p^m elementos, então, pela Afirmação 3, $\mathbb{E}'$ é o corpo de raízes de f sobre $\mathbb{F}_p$. Como o corpo de raízes é único, a menos de isomrfismo, segue que $\mathbb{E}'$ é isomorfo a $\mathbb{E}$. □

Se $q = p^m$, denote por $\mathbb{F}_q$ o corpo finito com q elementos. Note que, se m divide n, então $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ (assumindo que ambos são subcorpos de $\bar{\mathbb{F}}_p$).

A seguir, provaremos que o grupo multiplicativo de um corpo finito é cíclico (isto é, é gerado por um único elemento). Como consequência, obteremos a validade do Teorema do Elemento Primitivo para extensões de corpos envolvendo corpos finitos.

Lema 7.2. *Seja G um grupo abeliano finito de ordem n. Assuma que, para todo m dividindo n, $\#\{x \in G \mid x^m = 1\} \leq m$. Então G é cíclico.*

Demonstração. Seja $G_m = \{x \in G \mid o(x) = m\}$ (em que $o(g)$ denota a ordem de g). Se $G_m \neq \emptyset$, então existe $g_m \in G_m$. Daí $\langle g_m \rangle$ é um subgrupo de ordem m. Todos os seus elementos satisfazem $g^m = 1$. Assim, por hipótese, segue que

$$\langle g_m \rangle = \{x \in G \mid x^m = 1\} \supseteq G_m.$$

Obtemos então

$$n = |G| = \sum_{m/n} \#G_m \leq \sum_{m/n} \phi(m) = n,$$

em que $\phi(m) = \#\{1 \leq r \leq m \mid \text{mdc}(r, m) = 1\}$ é a função de Euler. Portanto, todo G_m é não vazio. Em particular, $G_n \neq \emptyset$, ou seja, G é cíclico. □

Teorema 7.3. *Seja $\mathbb{F}$ um corpo finito. Então, seu corpo multiplicativo $(\mathbb{F}^\times, \cdot)$ é um grupo cíclico.*

Demonstração. Seja $G = \mathbb{F}^\times$ o grupo multiplicativo do corpo. Então, para cada m dividindo $|G|$, $\{x \in G \mid x^m = 1\}$ é o conjunto das raízes do polinômio $X^m - 1$. O último possui no máximo m raízes. Portanto, pelo lema anterior, $\mathbb{F}^\times$ é cíclico. □

Corolário 7.4. *Sejam $\mathbb{F}$ um corpo finito e $\mathbb{E}/\mathbb{F}$ uma extensão finita. Então a extensão $\mathbb{E}/\mathbb{F}$ é simples, isto é, existe $a \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(a)$.*

Demonstração. Pelo teorema anterior, $\mathbb{E}^\times = \langle a \rangle$. Portanto, obtemos que $\mathbb{E} = \mathbb{F}(a)$. □

Por fim, vamos calcular o grupo de automorfismos de uma extensão de corpos envolvendo corpos finitos. Começamos com o seguinte:

Teorema 7.5. *Seja $q = p^m$. Então $\text{Aut}(\mathbb{F}_q) = \langle F \rangle$ é um grupo de ordem m, gerado pelo homomorfismo de Frobenius.*

Demonstração. Como $\mathbb{F}_p$ é perfeito, a extensão $\mathbb{F}_q/\mathbb{F}_p$ é separável. Além disso, do Teorema 7.1, a extensão também é normal. Portanto, $\mathbb{F}_q/\mathbb{F}_p$ é galoisiana finita de grau m. Assim, $|\mathrm{Aut}(\mathbb{F}_q)| = |\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)| = m$.

Como o homomorfismo de Frobenius é um homomorfismo de anéis $F : \mathbb{F}_q \to \mathbb{F}_q$, segue que $F \in \mathrm{Aut}(\mathbb{F}_q)$. Ainda, para cada $x \in \mathbb{F}_q$, temos que $F^m(x) = x^{p^m} = x$. Portanto, $F^m = 1$. Assuma que $1 < s \leq m$ é tal que $F^s = 1$. Então todo $x \in \mathbb{F}_q$ satisfaz $0 = F^s(x) - x = x^{p^s} - x$. Isso implica que $\mathbb{F}_q \subseteq \mathbb{F}_{p^s}$. Mas $p^s \leq q$, e portanto, vale a igualdade. Obtemos então que $q = p^s$, ou seja, $s = m$. Segue que $\langle F \rangle$ é um subgrupo com m elementos. Assim, conclui-se que $\mathrm{Aut}(\mathbb{F}_q) = \langle F \rangle$. □

Colecionando os resultados provados, enunciamos o seguinte:

Corolário 7.6. *Seja $\mathbb{E}/\mathbb{F}$ em que $\mathbb{E}$ é finito e de característica $p > 0$. Então $\mathbb{E}/\mathbb{F}$ é galoisiana finita. Ainda mais, se $|\mathbb{F}| = p^m$ e $|\mathbb{E}| = p^n$, então m divide n. O grupo de automorfismos da extensão é $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \langle F^m \rangle$, e sua ordem é $n/m = [\mathbb{E} : \mathbb{F}]$.*

Demonstração. Do teorema anterior, $\mathrm{Aut}(\mathbb{E}) = \langle F \rangle$ possui ordem n. Ainda,

$$\mathbb{E}^{\langle F^m \rangle} = \{x \in \mathbb{E} \mid F^m(x) = x^{p^m} = x\} = \mathbb{F}.$$

Portanto, da correspondência de Galois, $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \langle F^m \rangle$. A ordem do subgrupo é $n/m = [\mathbb{E} : \mathbb{F}]$. □

8. 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.

O caso do corpo finito já foi feito (Corolário 7.4).

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

Teorema 8.1. *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). Do Corolário 7.4, 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 8.2. *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 8.3. *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 8.2. 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). □

9. Teorema Fundamental da Teoria de Galois

Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos, e identifique $\mathbb{F}$ como um subcorpo de $\mathbb{E}$. Relembre que denotamos por $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ como sendo o conjunto dos $\mathbb{F}$-automorfismos de $\mathbb{E}$. Defina $\mathcal{K}$ como o conjunto dos corpos intermediários entre $\mathbb{F}$ e $\mathbb{E}$. Seja $\mathcal{G}$ o conjunto dos subgrupos de $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Mais precisamente:

$$\mathcal{K} = \{\mathbb{K} \text{ corpo} \mid \mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}\},$$
$$\mathcal{G} = \{H \subseteq \mathrm{Aut}(\mathbb{E}/\mathbb{F}) \text{ subgrupo}\}.$$

Temos duas funções entre esses conjuntos:

(1) $\mathcal{K} \to \mathcal{G}$, em que $\mathbb{K} \mapsto \mathrm{Aut}(\mathbb{E}/\mathbb{K}) = \{\sigma \in \mathrm{Aut}(\mathbb{E}) \mid \sigma(\ell) = \ell, \forall \ell \in \mathbb{K}\}$, o conjunto dos $\mathbb{K}$-automorfismos de $\mathbb{E}$,
(2) $\mathcal{G} \to \mathcal{K}$, em que $H \mapsto \mathbb{E}^H := \{a \in \mathbb{E} \mid \sigma(a) = a, \forall \sigma \in H\}$, o *corpo fixo* do subgrupo H.

O objetivo desta seção é estudar as funções definidas acima. Um tal par de mapas é denominado de *conexão de Galois*. O resultado principal é o seguinte: se a extensão $\mathbb{E}/\mathbb{F}$ é galoisiana e finita, então obtemos uma *correspondência de Galois*, isto é, as funções acima são bijeções, e uma é a inversa da outra. Relembre que uma extensão de corpos é dita ser galoisiana se a mesma é separável e normal.

Lema 9.1. *Os mapas definidos acima invertem inclusão. Além disso, sejam $\mathbb{K} \in \mathcal{K}$ e $H \in \mathcal{G}$. Então $\mathbb{K} \subseteq \mathbb{E}^{\mathrm{Aut}(\mathbb{E}/\mathbb{K})}$, e $H \subseteq \mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)$.*

Demonstração. Exercício. □

Teorema 9.2 (Artin)**.** *Seja $H \in \mathcal{G}$ um grupo finito. Então $\mathbb{E}/\mathbb{E}^H$ é uma extensão galoisiana finita. Além disso, $H = \mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)$.*

Demonstração. Seja $a \in \mathbb{E}$, e defina $C_a = \{\sigma(a) \mid \sigma \in H\}$. Temos que $|C_a| \leq |H|$ (pode ocorrer de $\sigma a = \sigma' a$, com $\sigma \neq \sigma'$). Note que cada $\sigma \in H$ induz uma bijeção $\sigma : C_a \to C_a$. Defina o polinômio

$$f_a(X) := \prod_{b \in C_a} (X - b).$$

Para cada $\sigma \in H$, vale que

$$f_a^\sigma = \prod_{b \in C_a} (X - \sigma b) = f_a.$$

Daí, $f_a \in \mathbb{E}^H[X]$. Além disso, por construção, as raízes de f_a são distintas. Portanto, como $f_a(a) = 0$, segue que a é separável sobre $\mathbb{E}^H$. Assim, $\mathbb{E}/\mathbb{E}^H$ é separável. Mais ainda, vale que

$$[\mathbb{E}^H(a) : \mathbb{E}] = \mathrm{gr}(\mathrm{Irr}(a, \mathbb{E}^H)) \leq \mathrm{gr}(f_a) = |C_a| \leq |H|. \tag{9.1}$$

Agora,

$$\mathscr{R}(\mathrm{Irr}(a, \mathbb{E}^H)) \subseteq \mathscr{R}(f_a) = C_a \subseteq \mathbb{E}.$$

Portanto, $\mathbb{E}/\mathbb{E}^H$ é uma extensão normal.

Provemos agora que $[\mathbb{E} : \mathbb{E}^H] \leq |H|$. Assuma que existam $a_1, \ldots, a_s \in \mathbb{E}$, que são $\mathbb{E}^H$-linearmente independentes, com $s > |H|$. Então $\mathbb{L} := \mathbb{E}^H(a_1, \ldots, a_s)$ é uma extensão finita de $\mathbb{E}^H$ tal que $[\mathbb{L} : \mathbb{E}^H] > |H|$. Como $a_1, \ldots, a_s$ são separáveis sobre $\mathbb{E}^H$, segue que $\mathbb{L}/\mathbb{F}$ é separável. Portanto, do Teorema do Elemento Primitivo (Corolário 8.3.(i)), existe $b \in \mathbb{L}$ de modo que $\mathbb{L} = \mathbb{E}^H(b)$. De (9.1), segue que

$$|H| < [\mathbb{L} : \mathbb{E}^H] = [\mathbb{E}^H(b) : \mathbb{E}^H] \leq |H|,$$

uma contradição. Portanto, $\mathbb{E}/\mathbb{E}^H$ é finita, e $[\mathbb{E} : \mathbb{E}^H] \leq |H|$.

Para concluir, note primeiro que, por construção, $H \subseteq \mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)$. Ainda, como $\mathbb{E}/\mathbb{E}^H$ é normal e separável, do Corolário 6.21, vale que $|\mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)| = [\mathbb{E} : \mathbb{E}^H]$. Assim, $|H| \leq |\mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)| = [\mathbb{E} : \mathbb{E}^H] \leq |H|$. Concluímos que $H = \mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)$. □

Corolário 9.3. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana e finita. Então $\mathbb{E}^{\mathrm{Aut}(\mathbb{E}/\mathbb{F})} = \mathbb{F}$.*

Demonstração. Seja $\mathbb{F}' = \mathbb{E}^{\mathrm{Aut}(\mathbb{E}/\mathbb{F})}$. Então, por construção, $\mathbb{F} \subseteq \mathbb{F}'$. Do teorema anterior, temos que

$$[\mathbb{E} : \mathbb{F}'] = |\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}'][\mathbb{F}' : \mathbb{F}].$$

Portanto, $[\mathbb{F}' : \mathbb{F}] = 1$, ou seja, $\mathbb{F}' = \mathbb{F}$. □

Exemplo 9.1. O corolário anterior não é válido se a extensão $\mathbb{E}/\mathbb{F}$ não é galoisiana. Lembre-se que $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$. Portanto,

$$\mathbb{Q}(\sqrt[3]{2})^{\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})} = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}.$$

Precisaremos, num futuro, da seguinte caracterização de extensões galoisianas finitas:

Proposição 9.4. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos. As seguintes afirmações são equivalentes:*

(i) *$\mathbb{E}/\mathbb{F}$ é uma extensão galoisiana finita,*
(ii) *$\mathbb{F} = \mathbb{E}^H$, para algum subgrupo finito $H \subseteq \mathrm{Aut}(\mathbb{E})$,*
(iii) *$\mathbb{E}$ é o corpo de raízes, sobre $\mathbb{F}$, de um polinômio separável $f \in \mathbb{F}[X]$.*

Demonstração. (i)⇒(ii): Pelo corolário anterior, basta tomar $H = \mathrm{Aut}(\mathbb{E}/\mathbb{F})$.
(ii)⇒(iii): do Teorema de Artin (Teorema 9.2), segue que $\mathbb{E}/\mathbb{F}$ é galoisiana e finita. Pelo Teorema do Elemento Primitivo (Corolário 8.3.(i)),

existe $a \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(a)$. Como $\mathbb{E}/\mathbb{F}$ é separável, segue que $\mathrm{Irr}(a, \mathbb{F})$ é um polinômio separável. Como $\mathbb{E}/\mathbb{F}$ é normal, $\mathbb{E}$ contém todas as raízes de $\mathrm{Irr}(a, \mathbb{F})$. Portanto, $\mathbb{E} = \mathbb{F}(a) \subseteq \mathbb{F}(\mathscr{R}(\mathrm{Irr}(a, \mathbb{F}))) \subseteq \mathbb{E}$. Segue que $\mathbb{E}$ é o corpo de raízes do polinômio separável $\mathrm{Irr}(a, \mathbb{F})$ sobre $\mathbb{F}$.
(iii)⇒(i): Sejam $a_1, \ldots, a_s$ as raízes de f. Então $\mathbb{E} = \mathbb{F}(a_1, \ldots, a_s)$ é uma extensão finita de $\mathbb{F}$. Como $\mathbb{E}$ é o corpo de raízes de f sobre $\mathbb{F}$, segue que $\mathbb{E}/\mathbb{F}$ é normal. Como cada a_i é raiz de um polinômio separável (o próprio f), segue que a_i é separável sobre $\mathbb{F}$. Portanto, $\mathbb{E}/\mathbb{F}$ é uma extensão separável. Assim, $\mathbb{E}/\mathbb{F}$ é galoisiana e finita. □

Lema 9.5. *Sejam $H \subseteq \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ um subgrupo e $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Então*

$$\mathbb{E}^{\sigma H \sigma^{-1}} = \sigma \mathbb{E}^H.$$

Demonstração. Dado $\sigma(a) \in \sigma\mathbb{E}^H$, e $\sigma\tau\sigma^{-1} \in \sigma H \sigma^{-1}$, temos que $\tau(a) = a$. Daí,

$$\sigma\tau\sigma^{-1}(\sigma(a)) = \sigma\tau(a) = \sigma(a).$$

Portanto, $\sigma\mathbb{E}^H \subseteq \mathbb{E}^{\sigma H \sigma^{-1}}$. Reciprocamente, dado $a \in \mathbb{E}^{\sigma H \sigma^{-1}}$, escreva $a = \sigma(\sigma^{-1}(a))$. Provemos que $\sigma^{-1}(a) \in \mathbb{E}^H$. Dado $\tau \in H$, temos que

$$\tau(\sigma^{-1}(a)) = \sigma^{-1}(\sigma\tau\sigma^{-1}(a)) = \sigma^{-1}(a).$$

Assim, $a \in \sigma\mathbb{E}^H$. Portanto, vale que $\mathbb{E}^{\sigma H \sigma^{-1}} = \sigma\mathbb{E}^H$. □

Assim, já provamos todas as etapas do nosso resultado principal. Enunciamos da seguinte forma:

Teorema 9.6 (Teorema Fundamental da Teoria de Galois)**.** *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita. Denote por $\mathcal{G}$ o conjunto dos subgrpos de $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$, e $\mathcal{K}$ o conjunto dos corpos $\mathbb{K}$, com $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$. Então, os mapas $\mathbb{K} \in \mathcal{K} \mapsto \mathrm{Aut}(\mathbb{E}/\mathbb{K}) \in \mathcal{G}$ e $H \in \mathcal{G} \mapsto \mathbb{E}^H \in \mathcal{K}$ são inversas uma da outra. Além disso:*

(1) *$H_1 \subseteq H_2$ se, e somente se, $\mathbb{E}^{H_2} \subseteq \mathbb{E}^{H_1}$, para $H_1, H_2 \in \mathcal{G}$.*
(2) *Se $H_1 \subseteq H_2$, então $[\mathbb{E}^{H_1} : \mathbb{E}^{H_2}] = [H_2 : H_1]$.*
(3) *Se $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$, então $\mathbb{K}/\mathbb{F}$ é normal se, e somente se, $\mathrm{Aut}(\mathbb{E}/\mathbb{K})$ é um subgrupo normal de $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Neste caso, $\mathrm{Aut}(\mathbb{K}/\mathbb{F}) \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F})/\mathrm{Aut}(\mathbb{E}/\mathbb{K})$.*

Demonstração. Dado $H \in \mathcal{H}$, o Teorema 9.2 diz que $H = \mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)$. Seja $\mathbb{K} \in \mathcal{K}$. Então, Corolário 6.20 e Proposição 5.9 dizem que $\mathbb{E}/\mathbb{K}$ é uma extensão galoisiana. Daí, o Corolário 9.3 conclui que $\mathbb{K}^{\mathrm{Aut}(\mathbb{E}/\mathbb{K})} = \mathbb{K}$. Portanto, as aplicações são inversas uma da outra.
(1) Segue do enunciado do Lema 9.1, combinado com o fato dos mapas serem uma a inversa da outra.

(2) Do Teorema de Artin, $[\mathbb{E} : \mathbb{E}^{H_i}] = |H_i|$. Além disso,

$$|H_2| = [\mathbb{E} : \mathbb{E}^{H_2}] = [\mathbb{E} : \mathbb{E}^{H_1}][\mathbb{E}^{H_1} : \mathbb{E}^{H_2}] = |H_1|[\mathbb{E}^{H_1} : \mathbb{E}^{H_2}].$$

Portanto, $[\mathbb{E}^{H_1} : \mathbb{E}^{H_2}] = |H_2|/|H_1| = [H_2 : H_1]$.
(3) Seja $H = \mathrm{Aut}(\mathbb{E}/\mathbb{K})$. Do Corolário 9.3, $\mathbb{K} = \mathbb{E}^H$.

Assuma que H é um subgrupo normal, e seja $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Do Lema 9.5, obtemos que $\sigma\mathbb{E}^H = \mathbb{E}^{\sigma H \sigma^{-1}} = \mathbb{E}^H$. Portanto, do Teorema 5.15, $\mathbb{K}/\mathbb{F}$ é uma extensão normal. Reciprocamente, dado $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$, do Lema 9.5, temos

$$\mathbb{E}^{\sigma H \sigma^{-1}} = \sigma\mathbb{E}^H = \mathbb{E}^H.$$

Portanto, $\sigma H \sigma^{-1} = H$. Assim, H é um subgrupo normal de $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$. A conclusão foi provada no Teorema 5.15. □

10. Propriedades de Grupo de Galois

Nesta seção, vamos enunciar e demonstrar algumas ferramentas úteis para calcular o grupo de automorfismos de uma extensão de corpos.

Definição 10.1. Sejam $\mathbb{F}_1$ e $\mathbb{F}_2$ subcorpos de um corpo $\mathbb{E}$. O *compósito* de $\mathbb{F}_1$ e $\mathbb{F}_2$, denotado por $\mathbb{F}_1 \cdot \mathbb{F}_2$, é o menor subcorpo de $\mathbb{E}$ contendo $\mathbb{F}_1$ e $\mathbb{F}_2$. Analogamente define-se o compósito de um número finito de subcorpos de $\mathbb{E}$, denotado por $\mathbb{F}_1 \cdots \mathbb{F}_s$.

Exemplo 10.1. (1) Note que $\mathbb{F}_1 \cdot \mathbb{F}_2 = \mathbb{F}_1(\mathbb{F}_2) = \mathbb{F}_2(\mathbb{F}_1)$.
(2) Como subcorpos de $\mathbb{C}$, vale que $\mathbb{Q}(\sqrt{2}) \cdot \mathbb{Q}(i) = \mathbb{Q}(\sqrt{2}, i)$.
(3) Considere o corpo $\mathbb{C}(X)$, e seus subcorpos $\mathbb{Q}(X)$, e algum $\mathbb{K} \subseteq \mathbb{C} \subset \mathbb{C}(X)$. Então $\mathbb{K} \cdot \mathbb{Q}(X) = \mathbb{K}(X)$.

Proposição 10.2. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita, e sejam $\mathbb{K}_1, \ldots, \mathbb{K}_s$ corpos intermediários, isto é, $\mathbb{F} \subseteq \mathbb{K}_i \subseteq \mathbb{E}$. Seja $\mathbb{K} = \mathbb{K}_1 \cdots \mathbb{K}_s$. Então*

$$\mathrm{Aut}(\mathbb{E}/\mathbb{K}) = \bigcap_{i=1}^{s} \mathrm{Aut}(\mathbb{E}/\mathbb{K}_i).$$

Demonstração. Pela correspondência de Galois, como $\mathbb{K}$ é o menor corpo contendo $\mathbb{K}_1, \ldots, \mathbb{K}_s$, então $\mathrm{Aut}(\mathbb{E}/\mathbb{K})$ é o maior grupo contido em $\mathrm{Aut}(\mathbb{E}/\mathbb{K}_i)$, para cada i. Portanto, vale o resultado. □

Proposição 10.3. *Seja Ω um corpo contendo os corpos $\mathbb{L}, \mathbb{E}, \mathbb{F}$, e assuma que $\mathbb{L} \supseteq \mathbb{F}$, e que $\mathbb{E}/\mathbb{F}$ é galoisiana finita. Então $\mathbb{E}\cdot\mathbb{L}/\mathbb{L}$ e $\mathbb{E}/\mathbb{E}\cap\mathbb{L}$ são galoisianas finitas. Mais ainda:*

(i) *Via restrição de monomorfismo de corpos, vale o isomorfismo de grupos* $\mathrm{Aut}(\mathbb{E} \cdot \mathbb{L}/\mathbb{L}) \cong \mathrm{Aut}(\mathbb{E}/\mathbb{E} \cap \mathbb{L})$.

(ii) $[\mathbb{E} \cdot \mathbb{L} : \mathbb{L}]$ *divide* $[\mathbb{E} : \mathbb{F}]$. *Ainda mais, se* $[\mathbb{L} : \mathbb{F}] < \infty$, *então*

$$[\mathbb{E} \cdot \mathbb{L} : \mathbb{F}] = \frac{[\mathbb{E} : \mathbb{F}][\mathbb{L} : \mathbb{F}]}{[\mathbb{E} \cap \mathbb{L} : \mathbb{F}]}.$$

(iii) $[\mathbb{E} \cdot \mathbb{L} : \mathbb{L}] = [\mathbb{E} : \mathbb{F}]$ *se, e somente se,* $\mathbb{E} \cap \mathbb{L} = \mathbb{F}$. *Neste caso, vale que* $\mathrm{Aut}(\mathbb{E} \cdot \mathbb{L}/\mathbb{L}) \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F})$.

Demonstração. (i) Como $\mathbb{E}/\mathbb{F}$ é galoisiana finita, segue que $\mathbb{E}/\mathbb{E} \cap \mathbb{L}$ é galoisiana finita. Ainda, existe $f \in \mathbb{F}[X]$ separável tal que $\mathbb{E} = \mathbb{F}(\mathscr{R}(f))$. Portanto, $\mathbb{E} \cdot \mathbb{L} = \mathbb{F}(\mathscr{R}(f))(\mathbb{L}) = \mathbb{F}(\mathbb{L})(\mathscr{R}(f)) = \mathbb{L}(\mathscr{R}(f))$. Daí, $\mathbb{E} \cdot \mathbb{L}/\mathbb{L}$ é galoisiana finita.

Dado $\sigma \in \mathrm{Aut}(\mathbb{E} \cdot \mathbb{L}/\mathbb{L})$, denote por $\psi(\sigma) = \sigma|_{\mathbb{E}}$ a sua restrição em $\mathbb{E}$. Dado $a \in \mathbb{E} \cap \mathbb{L} \subseteq \mathbb{L}$, temos que $\sigma(a) = a$. Portanto, $\sigma|_{\mathbb{E}}$ é um $\mathbb{E} \cap \mathbb{L}$-monomorfismo. Agora, a extensão $\mathbb{E}/\mathbb{E} \cap \mathbb{L}$ é normal, e portanto, $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{E}\cap\mathbb{L})$. Isso mostra que o mapa dada por restrição

$\psi : \mathrm{Aut}(\mathbb{E}\cdot\mathbb{L}/\mathbb{L}) \to \mathrm{Aut}(\mathbb{E}/\mathbb{E}\cap\mathbb{F})$ está bem definido. Além disso, o mesmo é um homomorfismo de grupos. Se σ é um $\mathbb{L}$-automorfismo de $\mathbb{E}\cdot\mathbb{L} = \mathbb{L}(\mathbb{E})$ tal que $\sigma|_{\mathbb{E}} = 1_{\mathbb{E}}$, então $\sigma = 1$. Portanto, ψ é injetora.

Por fim, seja $H = \mathrm{Im}\,\psi$. Então, $\mathbb{E}\cap\mathbb{L} \subseteq \mathbb{E}^H \subseteq (\mathbb{E}\cdot\mathbb{L})^{\mathrm{Aut}(\mathbb{E}\cdot\mathbb{L}/\mathbb{L})} \cap \mathbb{E} = \mathbb{E}\cap\mathbb{L}$. Portanto, $H = \mathrm{Aut}(\mathbb{E}/\mathbb{E}\cap\mathbb{L})$. Daí ψ é sobrejetor, e então, um isomorfismo de grupos.

(ii) Do item (i), temos que $[\mathbb{E}\cdot\mathbb{L} : \mathbb{L}] = [\mathbb{E} : \mathbb{E}\cap\mathbb{L}]$. O último divide $[\mathbb{E} : \mathbb{F}]$. Se $[\mathbb{L} : \mathbb{F}] < \infty$, temos então

$$[\mathbb{E}\cdot\mathbb{L} : \mathbb{F}] = [\mathbb{E}\cdot\mathbb{L} : \mathbb{L}][\mathbb{L} : \mathbb{F}] = [\mathbb{E} : \mathbb{E}\cap\mathbb{L}][\mathbb{L} : \mathbb{F}] =$$
$$= [\mathbb{E} : \mathbb{E}\cap\mathbb{L}][\mathbb{L} : \mathbb{F}]\frac{[\mathbb{E}\cap\mathbb{L} : \mathbb{F}]}{[\mathbb{E}\cap\mathbb{L} : \mathbb{F}]} = \frac{[\mathbb{E} : \mathbb{F}][\mathbb{L} : \mathbb{F}]}{[\mathbb{E}\cap\mathbb{L} : \mathbb{F}]}.$$

(iii) Segue dos items (i) e (ii). □

Exemplo 10.2. Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita. Então, a extensão de corpos $\mathbb{E}(X_1,\ldots,X_m)/\mathbb{F}(X_1,\ldots,X_m)$ é galoisina finita. Além disso,

$$\mathrm{Aut}(\mathbb{E}(X_1,\ldots,X_m)/\mathbb{F}(X_1,\ldots,X_m)) \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F}).$$

De fato, basta tomar $\mathbb{L} = \mathbb{F}(X_1,\ldots,X_m)$, e $\Omega = \mathbb{E}(X_1,\ldots,X_m)$ na proposição anterior. Neste caso, temos que $\mathbb{E}\cap\mathbb{L} = \mathbb{F}$.

Exemplo 10.3. Seja Ω um corpo algebricamente fechado e $\mathbb{F}$ o seu corpo primo. Sejam $f \in \mathbb{F}[X]$ um polinômio separável, e $\mathbb{E} \subseteq \Omega$ um corpo. Então

$$\mathrm{Aut}(\mathbb{E}(\mathscr{R}(f))/\mathbb{E}) \cong \mathrm{Aut}(\mathbb{F}(\mathscr{R}(f))/\mathbb{F}(\mathscr{R}(f)) \cap \mathbb{E}).$$

Proposição 10.4. *Seja Ω um corpo contendo $\mathbb{E}_1, \mathbb{E}_2, \mathbb{F}$. Assuma que $\mathbb{E}_1/\mathbb{F}$ e $\mathbb{E}_2/\mathbb{F}$ são galoisianas finitas. Então, $\mathbb{E}_1\cdot\mathbb{E}_2/\mathbb{F}$ é galoisiana finita. Além disso, o mapa*

$$\sigma \in \mathrm{Aut}(\mathbb{E}_1\mathbb{E}_2/\mathbb{F}) \mapsto (\sigma|_{\mathbb{E}_1}, \sigma|_{\mathbb{E}_2}) \in \mathrm{Aut}(\mathbb{E}_1/\mathbb{F}) \times \mathrm{Aut}(\mathbb{E}_2/\mathbb{F})$$

é injetor, e sua imagem é $\{(\sigma_1,\sigma_2) \mid \sigma_1|_{\mathbb{E}_1\cap\mathbb{E}_2} = \sigma_2|_{\mathbb{E}_1\cap\mathbb{E}_2}\}$. Em particular, se $\mathbb{E}_1\cap\mathbb{E}_2 = \mathbb{F}$, então o mapa acima é um isomorfismo.

Demonstração. Temos que, para $i = 1, 2$, existem $f_i \in \mathbb{F}[X]$ separável de modo que $\mathbb{E}_i = \mathbb{F}(\mathscr{R}(f_i))$. Então $\mathbb{E}_1\cdot\mathbb{E}_2 = \mathbb{F}(\mathscr{R}(\{f_1, f_2\}))$. Portanto, $\mathbb{E}_1\cdot\mathbb{E}_2/\mathbb{F}$ é galoisiana finita. Seja

$$H = \{(\sigma_1,\sigma_2) \in \mathrm{Aut}(\mathbb{E}_1/\mathbb{F}) \times \mathrm{Aut}(\mathbb{E}_2/\mathbb{F}) \mid \sigma_1|_{\mathbb{E}_1\cap\mathbb{E}_2} = \sigma_2|_{\mathbb{E}_1\cap\mathbb{E}_2}\}.$$

Por construção, o mapa $\sigma \mapsto (\sigma|_{\mathbb{E}_1}, \sigma|_{\mathbb{E}_2})$ é um homomorfismo de grupos injetor, e sua imagem está contida em H. Provaremos que a cardinalidade de H coincide com a de $\mathrm{Aut}(\mathbb{E}_1\cdot\mathbb{E}_2/\mathbb{F})$. Temos que existem

$[\mathbb{E}_1 : \mathbb{F}]$ $\mathbb{F}$-automorfismos de $\mathbb{E}_1$. Para cada automorfismo σ, existem exatamente $[\mathbb{E}_2 : \mathbb{E}_1 \cap \mathbb{E}_2]$ extensões de $\sigma|_{\mathbb{E}_1 \cap \mathbb{E}_2}$ para $\mathbb{E}_2$. Daí

$$|H| = [\mathbb{E}_1 : \mathbb{F}][\mathbb{E}_2 : \mathbb{E}_1 \cap \mathbb{E}_2] = [\mathbb{E}_1 : \mathbb{F}][\mathbb{E}_2 : \mathbb{E}_1 \cap \mathbb{E}_2]\frac{[\mathbb{E}_1 \cap \mathbb{E}_2 : \mathbb{F}]}{[\mathbb{E}_1 \cap \mathbb{E}_2 : \mathbb{F}]}$$
$$= \frac{[\mathbb{E}_1 : \mathbb{F}][\mathbb{E}_2 : \mathbb{F}]}{[\mathbb{E}_1 \cap \mathbb{E}_2 : \mathbb{F}]} = [\mathbb{E}_1 \cdot \mathbb{E}_2 : \mathbb{F}],$$

em que a última passagem foi utilizada a Proposição 10.3.(ii). Isso conclui o resultado. □

Corolário 10.5. *Sejam $\mathbb{F} \subseteq \mathbb{K}_1, \ldots, \mathbb{K}_m \subseteq \mathbb{E}$ corpos. Assuma que, para cada $i = 1, \ldots, m$, $\mathbb{K}_i/\mathbb{F}$ é galoisiana e finita. Assuma ainda que $\mathbb{K}_i \cap (\mathbb{K}_1 \cdots \mathbb{K}_{i-1} \cdot \mathbb{K}_{i+1} \cdots \mathbb{K}_m) = \mathbb{F}$, para cada i. Então $\mathbb{K}_1 \cdots \mathbb{K}_m/\mathbb{F}$ é galoisiana finita, e*

$$\mathrm{Aut}(\mathbb{K}_1 \cdots \mathbb{K}_m/\mathbb{F}) \cong \mathrm{Aut}(\mathbb{K}_1/\mathbb{F}) \times \cdots \times \mathrm{Aut}(\mathbb{K}_m/\mathbb{F}).$$

□

Por fim, temos a seguinte propriedade a respeito do grupo de automorfismos de uma extensão:

Teorema 10.6. *Sejam $f \in \mathbb{F}[X]$, n a quantidade de raízes distintas de f e $\mathbb{L}$ o corpo de raízes de f sobre $\mathbb{F}$. Então existe um monomorfismo de grupos*

$$\mathrm{Aut}(\mathbb{L}/\mathbb{F}) \to \mathcal{S}_n.$$

Demonstração. Seja $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$. Para cada $u \in \mathscr{R}(f)$, temos que $0 = \sigma(f(u)) = f(\sigma(u))$. Portanto, segue que $\sigma(\mathscr{R}(f)) \subseteq \mathscr{R}(f)$. Sendo σ um monomorfismo e $\mathscr{R}(f)$ finito, obtemos que $\sigma(\mathscr{R}(f)) = \mathscr{R}(f)$. Daí, σ permuta os elementos de $\mathscr{R}(f)$, ou seja, podemos identificar $\sigma \in \mathcal{S}_n$. Tal identificação $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) \to \mathcal{S}_n$ é um homomorfismo de grupos. Além disso, se $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$ é tal que $\sigma(u) = u$, $\forall u \in \mathscr{R}(f)$, então σ é a identidade em $\mathbb{F}(\mathscr{R}(f)) = \mathbb{L}$. Portanto, temos um monomorfismo de grupos $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) \to \mathcal{S}_n$. □

11. Exemplos

1. *Calcule* $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$*, em que* $d \in \mathbb{Z}$ *é livre de quadrados.*

Sabemos que $\mathrm{Irr}(\sqrt{d}, \mathbb{Q}) = X^2 - d$. Assim, sabe-se também que um $\mathbb{Q}$-automorfismo $\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ é totalmente definido pelo elemento $\sigma(\sqrt{d}) \in \{\sqrt{d}, -\sqrt{d}\}$. Portanto, obtemos que $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{Id}, \sigma\} \cong C_2$, em que $\sigma(\sqrt{d}) = -\sqrt{d}$ (e, portanto, $\sigma^2 = \mathrm{Id}$).

2. *Calcule* $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$.

Podemos determinar a estrutura de grupo de $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ de uma forma indireta. Do exemplo anterior, temos que

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2 \cong \mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q}).$$

Ainda, já sabemos que $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(i) = \mathbb{Q}$. Além disso, segue da definição que $\mathbb{Q}(\sqrt{2}) \cdot \mathbb{Q}(i) = \mathbb{Q}(\sqrt{2}, i)$. Portanto, do Corolário 10.5, obtemos que

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q}) \cong C_2 \times C_2.$$

Explicitamente, podemos exibir os elementos e a tábua de multiplicação de $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$. Vamos descrever a extensão $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ via dois elementos, e considere os respectivos polinômios minimais:

$$\begin{array}{c} \mathbb{Q}(\sqrt{2})(i) \\ \Big| \ \mathrm{Irr}(i, \mathbb{Q}(\sqrt{2})) = X^2 + 1 \\ \mathbb{Q}(\sqrt{2}) \\ \Big| \ \mathrm{Irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2 \\ \mathbb{Q} \end{array}$$

Então, da Proposição 4.6, existem dois $\mathbb{Q}$-monomorfismos $\mathbb{Q}(\sqrt{2}) \to \mathbb{C}$, determinados pela imagem de $\sqrt{2}$ (para ser mais preciso, o contradomínio é o próprio $\mathbb{Q}(\sqrt{2})$, pois $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ é normal. Mas não precisamos deste fato aqui). Daí, novamente da Proposição 4.6, cada $\mathbb{Q}$-monomorfismo $\mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ admite exatamente duas extensões para monomorfismos $\mathbb{Q}(\sqrt{2}, i) \to \mathbb{C}$, determinados pela imagem de i. Sendo $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ normal, as tais extensões são $\mathbb{Q}$-automorfismos.

Assim, fica justificado que qualquer elemento $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ é totalmente e bem determinado pelas escolhas $\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$ e

$\sigma(i) \in \{i, -i\}$. Sejam $\sigma_1, \sigma_2 \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ satisfazendo:

$$\sigma_1(\sqrt{2}) = -\sqrt{2}, \quad \sigma_1(i) = i,$$
$$\sigma_2(\sqrt{2}) = \sqrt{2}, \quad \sigma_2(i) = -i.$$

Uma vez que

$$\sigma_1^2(\sqrt{2}) = \sigma_1(-\sqrt{2}) = \sqrt{2}, \quad \sigma_1^2(i) = i,$$

concluimos que $\sigma_1^2 = \mathrm{Id}$. Da mesma forma, $\sigma_2^2 = \mathrm{Id}$. Além disso, $\sigma_1\sigma_2 = \sigma_2\sigma_1$ (exercício: verifique. Para verificar, basta checar que $\sigma_1\sigma_2(\sqrt{2}) = \sigma_2\sigma_1(\sqrt{2})$ e $\sigma_1\sigma_2(i) = \sigma_2\sigma_1(i)$).

Portanto, novamente, obtemos que

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) = \langle \sigma_1, \sigma_2 \rangle \cong C_2 \times C_2.$$

Os subgrupos não triviais de $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ são $\{1\}$, $\langle \sigma_1 \rangle$, $\langle \sigma_2 \rangle$ e $\langle \sigma_1\sigma_2 \rangle$. Seus corpos fixos são (verifique):

$$\mathbb{Q}(\sqrt{2}, i)^{\langle \sigma_1 \rangle} = \mathbb{Q}(i), \quad \mathbb{Q}(\sqrt{2}, i)^{\langle \sigma_2 \rangle} = \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{2}, i)^{\langle \sigma_1\sigma_2 \rangle} = \mathbb{Q}(\sqrt{2}i).$$

3. *Descreva* $\mathrm{Aut}(\mathbb{L}/\mathbb{Q})$*, em que* $\mathbb{L}$ *é o corpo de raízes de* $X^3 - 2$ *sobre* $\mathbb{Q}$.

Sejam $\alpha \in \mathbb{R}$ e $\xi \in \mathbb{C}$ tais que $\alpha^3 = 2$ e $\xi \neq \xi^3 = 1$. Então $\mathscr{R}(X^3 - 2) = \{\alpha, \xi\alpha, \xi^2\alpha\}$. Daí $\mathbb{L} = \mathbb{Q}(\mathscr{R}(X^3 - 2)) = \mathbb{Q}(\alpha, \xi)$. Já vimos que $[\mathbb{L} : \mathbb{Q}] = 6$.

Uma vez que $\mathrm{Aut}(\mathbb{L}/\mathbb{Q}) \subseteq \mathcal{S}_3$ (Teorema 10.6), e $|\mathcal{S}_3| = |\mathrm{Aut}(\mathbb{L}/\mathbb{Q})|$, segue que $\mathrm{Aut}(\mathbb{L}/\mathbb{Q}) \cong \mathcal{S}_3$. Assim, cada $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{Q})$ é unicamente e completamente determinado por uma permutação das raízes $\{\alpha, \xi\alpha, \xi^2\alpha\}$.

Uma descrição explícita pode ser dada da seguinte forma. Analogamente ao exemplo anterior, cada $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{Q})$ fica totalmente determinado pelas escolhas $\sigma(\alpha) \in \{\alpha, \xi\alpha, \xi^2\alpha\}$, e $\sigma(\xi) \in \{\xi, \xi^2\}$. De fato, temos as seguintes extensões simples de corpos:

$$\begin{array}{l} \mathbb{Q}(\alpha)(\xi) \\ \quad \Big| \ \mathrm{Irr}(\xi, \mathbb{Q}(\alpha)) = X^2 + X + 1 \\ \mathbb{Q}(\alpha) \\ \quad \Big| \ \mathrm{Irr}(\alpha, \mathbb{Q}) = X^3 - 2 \\ \mathbb{Q} \end{array}$$

Sejam $\sigma, \tau \in \mathrm{Aut}(\mathbb{L}/\mathbb{Q})$ tais que

$$\sigma(\alpha) = \xi\alpha, \quad \sigma(\xi) = \xi$$
$$\tau(\alpha) = \alpha, \quad \tau(\xi) = \xi^2.$$

Temos que $\sigma^3 = \mathrm{Id}$, de fato,

$$\sigma^3(\alpha) = \sigma^2(\xi\alpha) = \sigma^2(\xi)\sigma^2(\alpha) = \xi\xi^2\alpha = \alpha, \quad \sigma^3(\xi) = \xi.$$

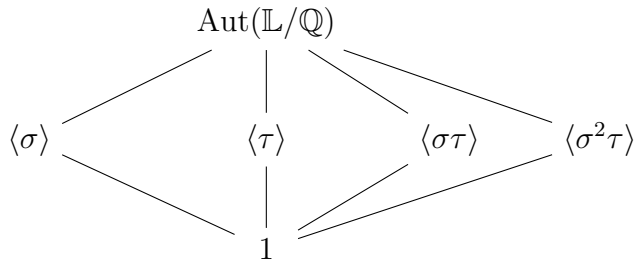
Da mesma forma, $\tau^2 = \mathrm{Id}$. Além disso,

$$\sigma\tau(\alpha) = \sigma(\alpha) = \xi\alpha, \quad \sigma\tau(\xi) = \sigma(\xi^2) = \xi^2,$$
$$\tau\sigma^2(\alpha) = \tau(\xi^2\alpha) = \xi^4\alpha = \xi\alpha, \quad \tau\sigma^2(\xi) = \tau(\xi) = \xi^2.$$

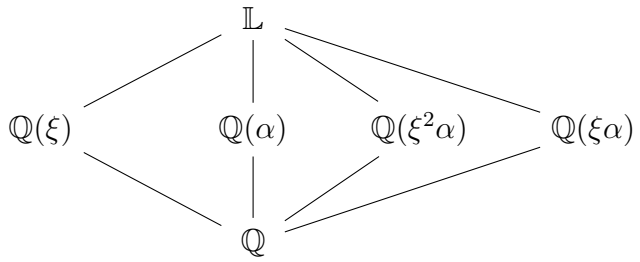
Portanto, $\sigma\tau = \tau\sigma^2$. O subgrupo gerado por σ e τ possui 6 elementos, que coincide com a cardinalidade de $\mathrm{Aut}(\mathbb{L}/\mathbb{F})$. Daí, vale que

$$\mathrm{Aut}(\mathbb{L}/\mathbb{F}) = \langle \sigma, \tau \mid \sigma^3 = \mathrm{Id}, \tau^2 = \mathrm{Id}, \sigma\tau = \sigma^{-1}\tau \rangle \cong \mathcal{S}_3.$$

Os subgrupos de $\mathrm{Aut}(\mathbb{L}/\mathbb{Q})$ são apresentados no seguinte diagrama:



Os subcorpos de $\mathbb{Q}(\sqrt{2}, i)$ (relacione os subgrupos com o respectivo corpo fixo) são:



4. *Determine* $\mathrm{Aut}(\mathbb{L}/\mathbb{Q})$ *em que* $\mathbb{L}$ *é o corpo de raízes de* $X^5 - 1$ *sobre* $\mathbb{Q}$.

Temos $\mathscr{R}(X^5 - 1) = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4\}$, em que $\zeta \neq \zeta^5 = 1$. Podemos, por exemplo, tomar

$$\zeta = e^{\frac{2\pi i}{5}} = \cos\left(\frac{2\pi}{5}\right) + i\mathrm{sen}\left(\frac{2\pi}{5}\right).$$

Temos então $\mathbb{L} = \mathbb{Q}(\mathscr{R}(X^5 - 1)) = \mathbb{Q}(\zeta)$.

$$\begin{array}{c} \mathbb{Q}(\zeta) \\ \Big| \, \mathrm{Irr}(\zeta, \mathbb{Q}) = X^4 + X^3 + X^2 + X + 1 \\ \mathbb{Q} \end{array}$$

Assim, como conjunto, $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, em que $\sigma_i(\zeta) = \zeta^i$. Defina $\sigma = \sigma_2$. Note que $\sigma_1 = \mathrm{Id}$, e

$$\sigma^2(\zeta) = \sigma(\zeta^2) = \zeta^4 = \sigma_4(\zeta).$$

Portanto, $\sigma^2 = \sigma_4$. Da mesma forma, vale que $\sigma^3 = \sigma_3$ e $\sigma^4 = \mathrm{Id}$. Portanto,

$$\mathrm{Aut}(\mathbb{L}/\mathbb{Q}) = \langle \sigma \rangle \cong C_4.$$

O subgrupo $\langle \sigma^2 \rangle$ é o único subgruop não trivial de $\mathrm{Aut}(\mathbb{L}/\mathbb{Q})$. Seu corpo fixo é $\mathbb{Q}(\xi + \xi^{-1})$ (verifique). Uma vez que $\xi + \xi^{-1} = 2\cos(2\pi/5)$, obtemos que o corpo fixo coincide com $\mathbb{Q}(\cos(2\pi/5))$. Assim, temos

$$\begin{array}{ccccc} 1 & \subseteq & \langle \tau^2 \rangle & \subseteq & \mathrm{Aut}(\mathbb{L}/\mathbb{Q}) \\ \mathbb{L} & \supseteq & \mathbb{Q}(\cos(2\pi/5)) & \supseteq & \mathbb{Q}. \end{array}$$

5. *Calcule* $\mathrm{Aut}(\mathbb{L}/\mathbb{Q})$*, em que* $\mathbb{L}$ *é o corpo de raízes de* $X^4 - 3$ *sobre* $\mathbb{Q}$.

Seja $\alpha \in \mathbb{R}$ tal que $\alpha^4 = 3$. Então

$$\mathscr{R}(X^4 - 3) = \{\alpha, i\alpha, -\alpha, -i\alpha\},$$

$\mathbb{L} = \mathbb{Q}(\mathscr{R}(X^4 - 3)) = \mathbb{Q}(\alpha, i)$, e $[\mathbb{L} : \mathbb{Q}] = 8$. Vale a seguinte sequência de extensões simples com os respectivos polinômios minimais:

$$\begin{array}{c} \mathbb{Q}(\alpha)(i) \\ \Big| \, \mathrm{Irr}(i, \mathbb{Q}(\alpha)) = X^2 + 1 \\ \mathbb{Q}(\alpha) \\ \Big| \, \mathrm{Irr}(\alpha, \mathbb{Q}) = X^4 - 3 \\ \mathbb{Q} \end{array}$$

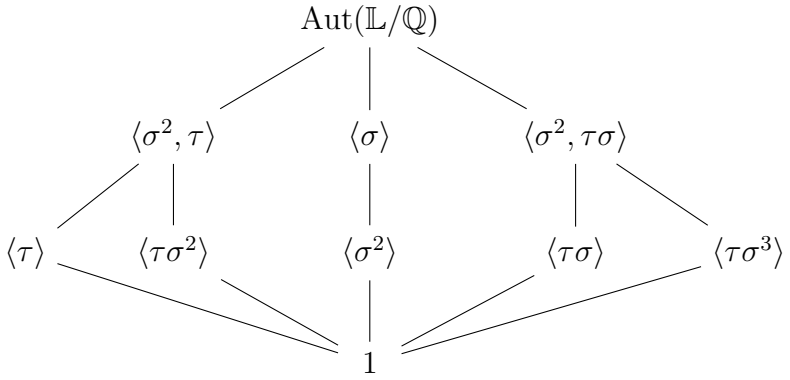
Sejam $\sigma, \tau \mathrm{Aut}(\mathbb{L}/\mathbb{Q})$ tais que

$$\begin{aligned} \sigma(\alpha) &= i\alpha, \quad \sigma(i) = i \\ \tau(\alpha) &= \alpha, \quad \tau(i) = -i. \end{aligned}$$

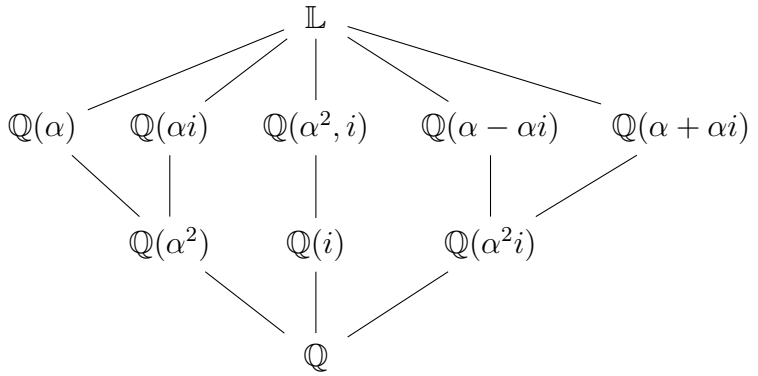
Temos que $\sigma^4 = \mathrm{Id} = \tau^2$, e $\sigma\tau = \sigma^{-1}\tau$ (verifique). Daí, segue que

$$\mathrm{Aut}(\mathbb{L}/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = \mathrm{Id}, \sigma\tau = \sigma^{-1}\tau \rangle \cong \mathcal{D}_4.$$

O grupo $\mathrm{Aut}(\mathbb{L}/\mathbb{Q})$ possui os seguintes subgrupos:



Os respectivos corpos fixos são apresentados a seguir (verifique os detalhes):



Problemas. Seja G um grupo finito.

(1) Existe uma extensão $\mathbb{E}/\mathbb{F}$ que é galoisiana e finita tal que $G \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F})$?

(2) Fixado um corpo $\mathbb{F}$, existe uma extensão de corpos $\mathbb{E}/\mathbb{F}$, que é galoisiana finita, de modo que $G \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F})$? Mais precisamente: quais grupos G podem aparecer como grupo de automorfismos $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$?

(3) Tome $\mathbb{F} = \mathbb{Q}$ no problema anterior anterior.

12. Extensão ciclotômica

Seja $\mathbb{F}$ um corpo. Queremos estudar raízes da unidade, ou seja, raízes do polinômio $X^n - 1$. Se $\operatorname{car}\mathbb{F} = p > 0$ e p divide n, então a derivada de $X^n - 1$ é nula. Portanto, $X^n - 1$ terá raízes repetidas. De fato, neste caso, podemos escrever $X^n - 1 = \left(X^{n/p} - 1\right)^p$. Se $\operatorname{car}\mathbb{F} = p \geq 0$ e p não divide n, então $(X^n - 1)' = nX^{n-1}$ não possui raízes em comum com $X^n - 1$. Portanto, neste caso, $X^n - 1$ é um polinômio separável.

Denote por $W_n(\mathbb{F}) = \{a \in \mathbb{F}^\times \mid a^n = 1\}$. Note que $W_n(\mathbb{F})$ é um subgrupo cíclico e finito de $\mathbb{F}^\times$, de cardinalidade no máximo n. Seja $\mathscr{R}(X^n - 1)$ o conjunto de raízes de $X^n - 1$ num fecho algébrico de $\mathbb{F}$. Note que $W_n(\mathbb{F}) = \mathscr{R}(X^n - 1) \cap \mathbb{F}^\times$.

Denote por $\mathcal{P}_n(\mathbb{F}) = \{a \in \mathbb{F}^\times \mid o(a) = n\}$. Os elementos de $\mathcal{P}_n(\mathbb{F})$ são denominados de *n-raiz primitiva da unidade*. Note que, ou $\mathcal{P}_n(\mathbb{F})$ é vazio, ou possui exatamente $\phi(n)$ elementos.

Proposição 12.1. *Sejam $\mathbb{F}$ um corpo, com $\operatorname{car}\mathbb{F} = p \geq 0$, e $n \in \mathbb{N}$. As seguintes afirmações são equivalentes:*

(i) $|W_n(\mathbb{F})| = n$,
(ii) $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$,
(iii) *p não divide n, e $X^n - 1$ fatora-se completamente em $\mathbb{F}[X]$.*

Neste caso, temos que $W_n(\mathbb{F}) = \langle\xi\rangle$ se e só se $\xi \in \mathcal{P}_n(\mathbb{F})$. Mais ainda

$$W_n(\mathbb{F}) = \bigcup_{d|n} \mathcal{P}_d(\mathbb{F}).$$

Demonstração. $(i) \Rightarrow (ii)$: Seja $\xi \in W_n(\mathbb{F})$ um gerador do grupo. Então $o(\xi) = n$. Portanto, $\xi \in \mathcal{P}_n(\mathbb{F})$.
$(ii) \Rightarrow (iii)$: Se p divide n e existe $\xi \in \mathcal{P}_n(\mathbb{F})$, então $0 = \xi^{p(n/p)} - 1 = (\xi^{n/p} - 1)^p$. Portanto, $o(\xi) \leq n/p < n$, uma contradição. Segue que p não divide n. Por fim, se $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$, então $\langle\xi\rangle = W_n(\mathbb{F})$ possui ordem n. Daí, $\mathbb{F}$ contém todas as raízes de $X^n - 1$.
$(iii) \Rightarrow (i)$: Já vimos que, nesta situação, o polinômio $X^n - 1$ é separável. Se $X^n - 1$ se fatora completamente em $\mathbb{F}[X]$, então as n raízes de $X^n - 1$ estão em $\mathbb{F}$. Portanto, $|W_n(\mathbb{F})| = n$. □

Se $\mathbb{F}$ é algebricamente fechado, então o polinômio $X^n - 1$ se fatora em produto de polinômios de grau 1. Portanto, podemos enunciar o seguinte:

Corolário 12.2. *Sejam $\bar{\mathbb{F}}$ um corpo algebricamente fechado, e $n \in \mathbb{N}$. As seguintes afirmações são equivalentes:*

(i) $|W_n(\bar{\mathbb{F}})| = n$,
(ii) $\mathcal{P}_n(\bar{\mathbb{F}}) \neq \emptyset$,

(iii) $X^n - 1 \in \bar{\mathbb{F}}[X]$ *é um polinômio separável,*
(iv) p *não divide* n.

Em adicional, se $\operatorname{car} \bar{\mathbb{F}} = 0$*, então todas as condições são válidas.* □

Seja $\bar{\mathbb{F}}$ um fecho algébrico de $\mathbb{F}$, e seja $\xi \in \mathcal{P}_n(\bar{\mathbb{F}})$. Considere o corpo $\mathbb{E} = \mathbb{F}(\xi)$. O grupo $W_n(\mathbb{E})$ é isomorfo ao grupo aditivo cíclico $\mathbb{Z}/n\mathbb{Z}$. Um isomorfismo pode ser dado por $\xi^i \in W_n(\mathbb{E}) \mapsto i + nZ \in \mathbb{Z}/n\mathbb{Z}$. Os elementos que geram $\mathbb{Z}/n\mathbb{Z}$ são exatamente as unidades do anel $\mathbb{Z}/n\mathbb{Z}$. Assim, existe bijeção entre $\mathcal{P}_n(\mathbb{E})$ e $(\mathbb{Z}/n\mathbb{Z})^\times$. Note então que $\mathcal{P}_n(\mathbb{E}) = \{\xi^i \mid 1 \leq i \leq n, \operatorname{mdc}(n,i) = 1\}$. Mais ainda, sabe-se que $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Por construção, $\mathbb{E}$ é o corpo de raízes de $X^n - 1$ sobre $\mathbb{F}$. Portanto, $\mathbb{E}/\mathbb{F}$ é galoisiana finita. Seja $\sigma \in \operatorname{Aut}(\mathbb{E}/\mathbb{F})$. Então a restrição $\sigma|_{W_n(\mathbb{E})} : W_n(\mathbb{E}) \to W_n(\mathbb{E})$ é um isomorfismo de grupos. Isso significa que $\sigma(\xi) \in \mathcal{P}_n(\mathbb{E})$. Portanto, temos um mapa

$$\sigma \in \operatorname{Aut}(\mathbb{E}/\mathbb{F}) \mapsto \sigma \in \operatorname{Aut}(W_n(\mathbb{E})) \mapsto i + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times,$$

em que $\sigma(\xi) = \xi^i$. Como $\sigma \in \operatorname{Aut}(\mathbb{E}/\mathbb{F})$ é totalmente definido pelo elemento $\sigma(\xi)$, segue que o mapa $\operatorname{Aut}(\mathbb{E}/\mathbb{F}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ é injetora.

Combinando essas observações, acabamos de provar o seguinte:

Teorema 12.3. *Seja* $\mathbb{F}$ *um corpo de característica* $p \geq 0$*, em que* p *não divide* n*. Seja* $\xi \in \bar{\mathbb{F}}$ *uma* n*-ésima raiz primitiva da unidade. Então:*

(1) $\mathbb{F}(\xi)/\mathbb{F}$ *é galoisiana finita,*
(2) $\operatorname{Aut}(\mathbb{F}(\xi)/\mathbb{F})$ *é isomorfo a um subgrupo de* $(\mathbb{Z}/n\mathbb{Z})^\times$*, e portanto,* $[\mathbb{F}(\xi) : \mathbb{F}]$ *divide* $\phi(n)$*,*
(3) $[\mathbb{F}(\xi) : \mathbb{F}] = \phi(n)$ *se, e somente se,* $\operatorname{Aut}(\mathbb{F}(\xi)/\mathbb{F}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

□

A extensão $\mathbb{F}(\xi)/\mathbb{F}$ é denominada de a *n-ésima extensão ciclotômica* de $\mathbb{F}$. Vamos estudar a extensão ciclotômica no caso de $\mathbb{F} = \mathbb{Q}$. Para isso, precisaremos do seguinte resultado elementar (demonstração fica de exercício):

Lema 12.4 (Lema de Gauss)**.** *Seja* $f \in \mathbb{Z}[X]$ *mônico, e assuma que* $g, h \in \mathbb{Q}[X]$ *sejam mônicos de modo que* $f = gh$*. Então* $g, h \in \mathbb{Z}[X]$*.*

□

Teorema 12.5. *Seja* $\xi \in \mathcal{P}_n(\mathbb{C})$*. Então* $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n)$*. Além disso, vale o isomorfismo* $\operatorname{Aut}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Demonstração. Seja p um número primo que não divide n. Sejam $f_1 = \operatorname{Irr}(\xi, \mathbb{Q})$, e $f_2 = \operatorname{Irr}(\xi^p, \mathbb{Q})$. Vamos provar que $f_1 = f_2$. Caso contrário, como ambos dividem $X^n - 1$, temos que $X^n - 1 = f_1(X) f_2(X) g(X)$.

Do Lema de Gauss, segue que $g(X) \in \mathbb{Z}[X]$. Como ξ é raiz de $f_2(X^p)$, temos que $f_2(X^p) = f_1(X)h(X)$, para algum $h(X) \in \mathbb{Q}[X]$. Novamente do Lema de Gauss, vale que $h \in \mathbb{Z}[X]$.

Seja $\pi : \mathbb{Z} \to \mathbb{F}_p$ o homomorfismo canônico. Além disso, para cada $z \in \mathbb{Z}$, temos que $\pi(z^p) = \pi(z)^p = \pi(z)$. Portanto, temos que

$$f_1^\pi(X)h^\pi(X) = \pi(f_2(X^p)) = (f_2^\pi(X))^p.$$

Isso significa que $d(X) := \text{mdc}(f_1^\pi, f_2^\pi) \neq 1$. Portanto, $(d(X))^2$ divide $f_1^\pi f_2^\pi g^\pi = \pi(X^n - 1)$. Mas $\pi(X^n - 1)$ é separável, uma contradição. Conclui-se então que $f_1 = f_2$.

Como $\text{mdc}(p, n) = 1$, segue que $\xi^p \in \mathcal{P}_n(\mathbb{C})$. Repetindo o argumento para outros primos não dividindo n, obtemos que $\text{Irr}(\zeta, \mathbb{Q}) = \text{Irr}(\xi, \mathbb{Q})$, para qualquer $\zeta \in \mathcal{P}_n(\mathbb{C})$. Portanto, $\text{gr}(\text{Irr}(\xi, \mathbb{Q})) \geq \phi(n)$. Do teorema anterior, segue que $\text{gr}(\text{Irr}(\xi, \mathbb{Q})) = \phi(n)$. □

Seja $\Phi_n(X) = \text{Irr}(\xi, \mathbb{Q})$. Então, a demonstração do teorema anterior garante que $\Phi_n(X) = \prod_{\zeta \in \mathcal{P}_n(\mathbb{C})}(X - \zeta)$ é um polinômio de grau $\phi(n)$. Denominamos $\Phi_n(X)$ de o *n-ésimo polinômio ciclotômico*. Mais ainda, temos que

$$X^n - 1 = \prod_{\zeta \in W_n(\mathbb{C})} (X - \zeta) = \prod_{d|n} \left(\prod_{\zeta \in \mathcal{P}_d(\mathbb{C})} (X - \zeta) \right) = \prod_{d|n} \Phi_d(X).$$

Como $X^n - 1$ e cada $\Phi_d(X)$ é um polinômio mônico em $\mathbb{Q}[X]$, o Lema de Gauss garante que cada $\Phi_d(X) \in \mathbb{Z}[X]$. Mais ainda, a fórmula anterior permite calcular $\Phi_n(X)$ recursivamente. De fato,

$$\Phi_n(X) = \frac{X^n - 1}{\prod\limits_{\substack{d|n \\ d \neq n}} \Phi_d(X)}.$$

Exemplo 12.1.

(1) $\Phi_1(X) = X - 1$.

(2) Se p é primo, então

$$\Phi_p = \frac{X^p - 1}{\Phi_1(X)} = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

(3) $\Phi_6(X) = \dfrac{X^6 - 1}{\Phi_1(X)\Phi_2(X)\Phi_3(X)} = X^2 - X + 1.$

A construção dos polinômios $\Phi_n(X)$ podem ser feitas sobre qualquer corpo. O que pode ocorrer é que os mesmos não necessariamente são irredutíveis sobre um corpo qualquer.

Sobre um corpo primo finito, temos os seguintes resultados:

Teorema 12.6. *Sejam $n \in \mathbb{N}$ e p um primo não dividindo n. Seja $\bar{\mathbb{F}}_p$ um fecho algébrico de $\mathbb{F}_p$, e seja $\xi \in \mathcal{P}_n(\bar{\mathbb{F}}_p)$. Então $[\mathbb{F}_p(\xi) : \mathbb{F}_p] = o(p + n\mathbb{Z})$, a ordem do elemento $p + n\mathbb{Z}$ em $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Demonstração. Da estrutura de corpos finitos, sabemos que $|\mathbb{F}_p(\xi)| = p^m$, em que $m = [\mathbb{F}_p(\xi) : \mathbb{F}_p] = |\mathrm{Aut}(\mathbb{F}_p(\xi))|$. Além disso, $\mathrm{Aut}(\mathbb{F}_p(\xi)/\mathbb{F}_p) = \langle F \rangle$, em que $F : a \in \mathbb{F}_p(\xi) \mapsto a^p \in \mathbb{F}_p(\xi)$. Temos ainda

$$\begin{aligned} o(F) &= \min\{r > 0 \mid \xi = F^r = \mathrm{Id}\} \\ &= \min\{r > 0 \mid \xi = F^r(\xi) = \xi^{p^r}\} \\ &= \min\{r > 0 \mid p^r \equiv 1 \pmod{n}\} = o(p + n\mathbb{Z}). \end{aligned}$$

□

Para cada n não múltiplo de p, seja

$$\Psi_n(X) = \prod_{\xi \in \mathcal{P}_n(\bar{\mathbb{F}}_p)} (X - \xi).$$

Note que $\mathbb{F}_p[X] \ni X^n - 1 = \prod_{d|n} \Psi_d(X)$. Além disso, vale o seguinte:

Corolário 12.7. *Seja $\pi : \mathbb{Z} \to \mathbb{F}_p$ a projeção canônica. Então*

(i) *$\Psi_n = \Phi_n^\pi$, para cada n não múltiplo de p,*
(ii) *Seja $r = \phi(n)/o(p+n\mathbb{Z})$. Então Ψ_n é o produto de r polinômios mônicos e irredutíveis de grau $o(p + n\mathbb{Z})$, distintos dois a dois em $\mathbb{F}_p[X]$.*

Demonstração. (i) Temos que $\Psi_1(X) = X - 1 = \pi(X - 1) = \Phi_1^\pi(X)$. Assumindo, por indução, que $\Psi_d(X) = \Phi_d^\pi(X)$, para todo $d < n$, temos que

$$\prod_{d|n} \Psi_d(X) = X^n - 1 = \pi(X^n - 1) = \pi\left(\prod_{d|n} \Phi_d(X)\right) = \Phi_n^\pi\left(\prod_{\substack{d|n \\ d \neq n}} \Psi_d(X)\right).$$

Portanto, $\Phi_n^\pi(X) = \Psi_n(X)$.
(ii) Seja $\xi \in \mathcal{P}_n(\bar{\mathbb{F}}_p)$. Então, do teorema anterior, $\mathrm{gr}\,\mathrm{Irr}(\xi, \mathbb{F}_p) = o(p + n\mathbb{Z})$. Como Ψ_n é um polinômio separável e é o produto de alguns $\mathrm{Irr}(\xi, \mathbb{F}_p)$, o resultado segue. □

Olhando para os casos extremos no item (ii) do corolário anterior, obtemos o seguinte:

Corolário 12.8. *Seja n não múltiplo do primo p. Então*

(i) *$\Psi_n(X)$ se fatora completamente como produto de polinômios de grau 1 em $\mathbb{F}_p[X]$ se, e somente se, $p \equiv 1 \pmod{n}$.*

(ii) $\Psi_n(X)$ *é irredutível em* $\mathbb{F}_p[X]$ *se, e somente se,* $(\mathbb{Z}/n\mathbb{Z})^\times = \langle p + n\mathbb{Z} \rangle$.

□

Finalmente, para um corpo qualquer, podemos combinar a Proposição 10.3 e os resultados para $\mathbb{Q}$ e $\mathbb{F}_p$ para descrever o grupo de Galois de uma extensão ciclotômica:

Teorema 12.9. *Seja* $\mathbb{F}$ *um corpo,* $\mathbb{F}_0 \subseteq \mathbb{F}$ *seu corpo primo, e* $\bar{\mathbb{F}} \supseteq \mathbb{F}$ *um fecho algébrico. Assuma que* $\operatorname{car} \mathbb{F}$ *é zero ou não divida* $n \in \mathbb{N}$. *Seja* $\xi \in \mathcal{P}_n(\bar{\mathbb{F}})$. *Então*

$$\operatorname{Aut}(\mathbb{F}(\xi)/\mathbb{F}) \cong \operatorname{Aut}(\mathbb{F}_0(\xi)/\mathbb{F} \cap \mathbb{F}_0(\xi)) \subseteq \operatorname{Aut}(\mathbb{F}_0(\xi)/\mathbb{F}_0).$$

Em particular, $\operatorname{Aut}(\mathbb{F}(\xi)/\mathbb{F})$ *é um grupo abeliano.* □

13. Extensão cíclica

13.1. **Norma e traço.** Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita de corpos, e seja $\{a_1, \ldots, a_n\}$ uma $\mathbb{F}$-base de $\mathbb{E}$. Para cada $\alpha \in \mathbb{E}$, fica bem definido uma $\mathbb{F}$-transformação linear $\mathbb{E} \to \mathbb{E}$ via multiplicação por α. Mais precisamente, existem $\alpha_{ij} \in \mathbb{F}$ tais que

$$\alpha a_i = \sum_{j=1}^{n} \alpha_{ij} a_j, \quad i = 1, \ldots, n.$$

Seja $A = (\alpha_{ij})_{(i,j)}$. Define-se o *traço* e a *norma* do elemento α sobre $\mathbb{E}/\mathbb{F}$ pela fórmula:

$$\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\alpha) := \mathrm{tr}(A) = \sum_{i=1}^{n} \alpha_{ii}, \quad \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha) = \det A.$$

O *polinômio característico* do elemento α é, por definição, o polinômio característico da matriz A. Mais precisamente, define-se

$$F(\alpha, \mathbb{E}/\mathbb{F}) = \det(x\mathrm{Id} - A).$$

As seguintes propriedades ficam de exercício:

Lema 13.1. *Sejam $[\mathbb{E} : \mathbb{F}] = n$ e $\alpha \in \mathbb{E}$.*

(i) $\mathrm{tr}_{\mathbb{E}/\mathbb{F}}$ *é $\mathbb{F}$-linear, e* $\mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha\beta) = \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha)\mathscr{N}_{\mathbb{E}/\mathbb{F}}(\beta)$.

(ii) *Se* $F(\alpha, \mathbb{E}/\mathbb{F}) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_1 X + \alpha_0$, *então*

$$\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\alpha) = -\alpha_{n-1}, \quad \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha) = (-1)^n \alpha_0.$$

(iii) α *é raiz de* $F(\alpha, \mathbb{E}/\mathbb{F})$.

(iv) $F(\alpha, \mathbb{F}(\alpha)/\mathbb{F}) = \mathrm{Irr}(\alpha, \mathbb{F})$.

(v) *Se* $\mathbb{L}/\mathbb{E}/\mathbb{F}$, *então* $F(\alpha, \mathbb{L}/\mathbb{F}) = F(\alpha, \mathbb{E}/\mathbb{F})^{[\mathbb{L}:\mathbb{E}]}$. *Ainda,*

$$\mathrm{tr}_{\mathbb{L}/\mathbb{F}}(\alpha) = [\mathbb{L} : \mathbb{E}]\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\alpha), \quad e \quad \mathscr{N}_{\mathbb{L}/\mathbb{F}}(\alpha) = \big(\mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha)\big)^{[\mathbb{L}:\mathbb{E}]}.$$

(vi) $F(\alpha, \mathbb{E}/\mathbb{F}) = \mathrm{Irr}(\alpha, \mathbb{F})^{[\mathbb{E}:\mathbb{F}(\alpha)]}$.

(vii) *Se* $\mathrm{Irr}(\alpha, \mathbb{F}) = \mathrm{Irr}(\beta, \mathbb{F})$, *então* $\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\alpha) = \mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\beta)$, *e* $\mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha) = \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\beta)$.

(viii) *Se* $\mathbb{E}/\mathbb{F}$ *é separável e finita e* $\Omega \supseteq \mathbb{F}$ *é algebricamente fechado, então*

$$\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\alpha) = \sum_{\sigma \in \mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega)} \sigma(\alpha), \quad \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha) = \prod_{\sigma \in \mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega)} \sigma(\alpha).$$

Nomenclatura. Dizemos que uma extensão $\mathbb{E}/\mathbb{F}$ é *cíclica* se o mesmo é galoisiana finita e $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é um grupo cíclico. Da mesma forma, dizemos que $\mathbb{E}/\mathbb{F}$ é *abeliano*, *solúvel*, etc, se o grupo $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é abeliano, solúvel, etc.

13.2. **Extensão cíclica.** O objetivo desta seção é estudar as extensões da forma $X^n - a$, em que $a \in \mathbb{F}^\times$. Começamos com o seguinte:

Lema 13.2. *Assuma que $X^n - a = (X - a_1)\cdots(X - a_n)$ é a fatoração em polinômios de grau 1 em $\Omega[X]$. Então*

$$\{a_j a_1^{-1} \mid j = 1, 2, \ldots, n\} = W_n(\Omega).$$

Em adicional, se $\operatorname{car}\mathbb{F} = p \geq 0$ não divide n, então $X^n - a$ é separável. Ainda mais, dados quaisquer $\xi \in \mathcal{P}_n(\Omega)$ e $\alpha \in \mathscr{R}(X^n - a)$, segue que

$$X^n - a = (X - \alpha)(X - \xi\alpha)(X - \xi^2\alpha)\cdots(X - \xi^{n-1}\alpha).$$

Demonstração. Temos que $a_j^n = a$, para cada j. Portanto, $(a_j a_1^{-1})^n = a_j^n (a_1^n)^{-1} = aa^{-1} = 1$. Daí $a_j a_1^{-1} \in W_n(\Omega)$. Reciprocamente, dado $w \in W_n(\Omega)$, temos que $(a_1 w)^n = a_1^n w^n = a$. Ou seja, $a_1 w \in \mathscr{R}(X^n - a)$.

Agora, assuma que $\operatorname{car}\mathbb{F}$ é zero ou $\operatorname{car}\mathbb{F} = p > 0$ não divide n. Então $(X^n - a)' = nX^{n-1} \neq 0$ possui somente o 0 como raiz. Segue que $\operatorname{mdc}(X^n - a, nX^{n-1}) = 1$, e então, $X^n - a$ é separável. A última afirmação segue de $W_n(\Omega) = \langle\xi\rangle$, para qualquer $\xi \in \mathcal{P}_n(\Omega)$. □

O próximo resultado diz que, se $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$, então a extensão de corpos $\mathbb{F}(\mathscr{R}(X^n - a))/\mathbb{F}$ é cíclica. Relembre que, a hipótese $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$ implica que $\operatorname{car}\mathbb{F}$ não divide n (ou é zero).

Teorema 13.3. *Sejam $\mathbb{F}$ um corpo tal que $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$ e $a \in \mathbb{F}^\times$. Seja $\mathbb{E} = \mathbb{F}(\mathscr{R}(X^n - a))$. Então:*

(i) *$\mathbb{E} = \mathbb{F}(\alpha)$, para qualquer $\alpha \in \mathscr{R}(X^n - a)$.*
(ii) *$[\mathbb{E} : \mathbb{F}]$ divide n. Ainda, $\operatorname{Aut}(\mathbb{E}/\mathbb{F})$ é isomorfo a um subgrupo de $W_n(\mathbb{F})$.*
(iii) *$[\mathbb{E} : \mathbb{F}] = n$ se e só se $\operatorname{Aut}(\mathbb{E}/\mathbb{F}) \cong W_n(\mathbb{F})$, e se e só se $X^n - a$ é irredutível em $\mathbb{F}[X]$.*

Demonstração. (i) Como $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$, o resultado segue do lema anterior.
(ii) Sejam $\xi \in \mathcal{P}_n(\mathbb{F})$ e $\alpha \in \mathscr{R}(X^n - a)$. Do lema anterior, temos então que $\mathscr{R}(X^n - a) = \{a, \xi a, \cdots, \xi^{n-1}a\}$. Para cada $\sigma \in \operatorname{Aut}(\mathbb{E}/\mathbb{F})$, temos que $\sigma(\mathscr{R}(X^n - a)) = \mathscr{R}(X^n - a)$. Portanto, $\sigma(\alpha) = \xi^j\alpha$, para algum j. Assim, temos um mapa

$$\psi : \sigma \in \operatorname{Aut}(\mathbb{E}/\mathbb{F}) \mapsto \frac{\sigma(\alpha)}{\alpha} = \xi^j \in W_n(\mathbb{F}).$$

Provemos que ψ é um homomorfismo de grupos. Dados $\sigma_1, \sigma_2 \in \operatorname{Aut}(\mathbb{E}/\mathbb{F})$ tais que $\sigma_i(\alpha) = \xi^{j_i}\alpha$, temos que

$$(\sigma_1 \circ \sigma_2)(\alpha) = \sigma_1(\xi^{j_2}\alpha) = \xi^{j_2}\xi^{j_1}\alpha.$$

Portanto, $\psi(\sigma_1\sigma_2) = \psi(\sigma_1)\psi(\sigma_2)$. Agora, seja $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ tal que $\psi(\sigma) = 1$. Então $\sigma(\alpha) = \alpha$. Isso implica que $\sigma = \mathrm{Id}_{\mathbb{F}(\alpha)}$. Daí $\sigma = 1$. Concluí-se que ψ é injetora, e portanto, $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é isomorfo a um subgrupo de $W_n(\mathbb{F})$. Por consequência, $[\mathbb{E} : \mathbb{F}] = |\mathrm{Aut}(\mathbb{E}/\mathbb{F})|$ divide $|W_n(\mathbb{F})| = n$.
(iii) Por (i), $\mathbb{L}$ é uma extensão simples de $\mathbb{F}$ por qualquer $\alpha \in \mathscr{R}(X^n - a)$. Assim, $[\mathbb{E}, \mathbb{F}] = n$ implica que $n = \mathrm{gr}(\mathrm{Irr}(\alpha, \mathbb{F}))$. Portanto, $\mathrm{Irr}(\alpha, \mathbb{F}) = X^n - a$. Reciprocamente, se $X^n - a$ é irredutível, então $X^n - a = \mathrm{Irr}(\alpha, \mathbb{F})$, e daí $[\mathbb{E} : \mathbb{F}] = n$.

Além disso, de (ii), ocorre que $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) \cong W_n(\mathbb{F})$ se e só se $n = |\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$. □

Em particular, temos o seguinte resultado:

Corolário 13.4. *Assuma que* $\mathrm{car}\,\mathbb{F}$ *é zero ou um primo que não divide* n. *Sejam* $\bar{\mathbb{F}}$ *um fecho algébrico de* $\mathbb{F}$, *e* $a \in \mathbb{F}^\times$ *e* $\xi \in \mathcal{P}_n(\bar{\mathbb{F}})$. *Seja* $\mathbb{L} = \mathbb{F}(\mathscr{R}(X^n - a))$. *Então*

(i) $\mathbb{L}/\mathbb{F}$ *é galoisiana finita, e* $\mathbb{L} = \mathbb{F}(\xi, \alpha)$, *para qualquer* $\alpha \in \mathscr{R}(X^n - a)$,
(ii) $\mathrm{Aut}(\mathbb{L}/\mathbb{F}(\xi))$ *é cíclico, e sua ordem divide* n,
(iii) $\mathbb{F}(\xi)/\mathbb{F}$ *é galoisiana finita, e* $\mathrm{Aut}(\mathbb{F}(\xi)/\mathbb{F})$ *é abeliano.*

Portanto, $\mathrm{Aut}(\mathbb{L}/\mathbb{F})$ *é solúvel.*

Demonstração. O corpo $\mathbb{E} = \mathbb{F}(\xi)$ é tal que $\mathcal{P}_n(\mathbb{E}) \neq \emptyset$. Portanto, (i) e (ii) seguem do teorema anterior. O item (iii) foi provado no Teorema 12.9. A conclusão final segue da correspondência de Galois (Teorema 9.6.(3)). □

Para provar a recíproca do Teorema 13.3, precisaremos do seguinte:

Teorema 13.5 (Artin)**.** *Seja* S *um grupo e* $\sigma_1, \ldots, \sigma_m$ *homomorfismos* $S \to \mathbb{F}^\times$ *dois a dois distintos. Então* $\{\sigma_1, \ldots, \sigma_m\}$ *é um conjunto* $\mathbb{F}$*-linearmente independente.*

Demonstração. Provaremos por indução em m, em que a base $m = 1$ é imediata. Sejam $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$ e considere a combinação linear $\alpha_1\sigma_1 + \cdots + \alpha_m\sigma_m = 0$. Portanto,

$$\alpha_1\sigma_1(a) + \cdots + \alpha_m\sigma_m(a) = 0, \quad \forall a \in S. \tag{13.2}$$

Como $\sigma_1 \neq \sigma_m$, existe $b \in S$ tal que $\sigma_1(b) \neq \sigma_m(b)$. Assim, por (13.2), temos que, $\forall a \in S$,

$$0 = \alpha_1\sigma_1(ba) + \cdots + \alpha_m\sigma_m(ba) = \alpha_1\sigma_1(b)\sigma_1(a) + \cdots + \alpha_m\sigma_m(b)\sigma_m(a).$$

Multiplicando (13.2) por $\sigma_m(b)$ e subtraindo da equação acima, obtemos que, $\forall a \in S$,

$$0 = \alpha_1(\sigma_1(b) - \sigma_m(b))\sigma_1(a) + \cdots + \alpha_{m-1}(\sigma_{m-1}(b) - \sigma_m(b))\sigma_{m-1}(a).$$

Isso implica que

$$\alpha_1(\sigma_1(b) - \sigma_m(b))\sigma_1 + \cdots + \alpha_{m-1}(\sigma_{m-1}(b) - \sigma_m(b))\sigma_{m-1} = 0,$$

em que cada $\alpha_i(\sigma_i(b) - \sigma_m(b)) \in \mathbb{F}$. Por indução, $\{\sigma_1, \ldots, \sigma_{m-1}\}$ é um conjunto $\mathbb{F}$-linearmente independente. Portanto, $\alpha_i(\sigma_i(b) - \sigma_m(b)) = 0$, para todo i. Como $\sigma_1(b) - \sigma_m(b) \neq 0$, temos que $\alpha_1 = 0$. Portanto, novamente por indução, obtemos que $\alpha_2 = \cdots = \alpha_m = 0$. Daí, $\{\sigma_1, \ldots, \sigma_m\}$ é $\mathbb{F}$-linearmente independente. □

Corolário 13.6 (Dedekind)**.** *Sejam $\sigma_1, \ldots, \sigma_m \in \mathrm{Aut}(\mathbb{F})$ dois a dois distintos. Então $\{\sigma_1, \ldots, \sigma_m\}$ é um conjunto $\mathbb{F}$-linearmente independente.* □

Teorema 13.7 (90 de Hilbert)**.** *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita de corpos tal que $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$ é cíclica. Seja $a \in \mathbb{E}$.*

(i) *$\mathscr{N}_{\mathbb{E}/\mathbb{F}}(a) = 1$ se, e somente se, existe $b \in \mathbb{E}$ tal que $a = b/\sigma(b)$.*
(ii) *$\mathrm{tr}_{\mathbb{E}/\mathbb{F}}\, a = 0$ se, e só se, existe $b \in \mathbb{E}$ tal que $a = b - \sigma(b)$.*

Demonstração. ($\Leftarrow$) Como $\sigma(b)$ e b possuem o mesmo polinômio minimal, segue que $\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(b) = \mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\sigma(b))$ e $\mathscr{N}_{\mathbb{E}/\mathbb{F}}(b) = \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\sigma(b))$. Portanto, vale a volta.
(i)($\Rightarrow$): Seja $a \in \mathbb{E}$ tal que $\mathscr{N}_{\mathbb{E}/\mathbb{F}}(a) = 1$. Do Teorema de Dedekind, $\sigma^0, \sigma^1, \ldots, \sigma^{m-1}$ são $\mathbb{E}$-linearmente independentes. Então, existe $c \in \mathbb{E}$ tal que

$$b := c + a\sigma(c) + (a\sigma(a))\sigma^2(c) + \cdots + (a\sigma(a)\cdots\sigma^{n-2}(a))\sigma^{n-1}(c) \neq 0.$$

Note que $\sigma(b) = b/a$, pois $1 = \mathscr{N}_{\mathbb{E}/\mathbb{F}}(a) = a\sigma(a)\cdots\sigma^{n-1}(a)$ e $\sigma^n = \mathrm{Id}$. Portanto, $a = b/\sigma(b)$.
(ii)($\Rightarrow$): Pelo Teorema de Dedekind, existe $c \in \mathbb{E}$ tal que

$$0 \neq \sigma^0(c) + \sigma(c) + \cdots + \sigma^{n-1}(c) = \mathrm{tr}_{\mathbb{E}/\mathbb{F}}(c).$$

Seja

$$b := \frac{1}{\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(c)} \left(\sum_{i=1}^{n} \left(\sum_{j=0}^{i-1} \sigma^j(a) \right) \sigma^i(c) \right).$$

Note que $\sigma(b) = b - a$, pois $\sigma^n = \mathrm{Id}$ e $\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(a) = a + \sigma(a) + \cdots + \sigma^{n-1}(a) = 0$. Portanto, $b - \sigma(b) = a$. □

Teorema 13.8. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana cíclica de grau n, $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$, e assuma que $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$. Então, existe $a \in \mathbb{F}^\times$ tal*

que $X^n - a$ é irredutível em $\mathbb{F}[X]$ e $\mathbb{E} = \mathbb{F}(\mathscr{R}(X^n - a))$. Além disso, $\mathbb{E} = \mathbb{F}(\alpha)$, $\forall \alpha \in \mathscr{R}(X^n - a)$.

Demonstração. Seja $\xi \in \mathcal{P}_n(\mathbb{F})$. Então $\mathscr{N}_{\mathbb{E}/\mathbb{F}}(\xi) = 1$. Do Teorema 90 de Hilbert, existe $\alpha \in \mathbb{E}$ tal que $\xi = \alpha/\sigma(\alpha)$. Portanto, $\sigma^j(\alpha) = \xi^{-j}\alpha$, para cada j. Segue que $\alpha, \xi^{-1}\alpha, \ldots, \xi^{n-1}\alpha$ são raízes distintas de $\operatorname{Irr}(\alpha, \mathbb{F})$. Daí, $n \leq \operatorname{gr}\operatorname{Irr}(\alpha, \mathbb{F}) \leq [\mathbb{E} : \mathbb{F}] = n$. Portanto, vale a igualdade. Por fim, $\sigma\alpha^n = \alpha^n$. Portanto, $a := \alpha^n \in \mathbb{E}^{\langle\sigma\rangle} = \mathbb{F}$. Agora, α é raiz de $X^n - a$, e $\operatorname{gr}(X^n - a) = n = \operatorname{gr}(\operatorname{Irr}(\alpha, \mathbb{F}))$. Segue que $X^n - a = \operatorname{Irr}(\alpha, \mathbb{F})$ é um polinômio irredutível.

As últimas consequências seguem dos fatos de que $\mathscr{R}(X^n - a) = \{\xi^j\alpha \mid j = 0, \ldots, n-1\} \subseteq \mathbb{E}$, e $[\mathbb{F}(\alpha) : \mathbb{F}] = \operatorname{gr}\operatorname{Irr}(\alpha, \mathbb{F}) = [\mathbb{E} : \mathbb{F}]$. □

Assim, temos uma caracterização de extensões cíclicas de grau n de um corpo $\mathbb{F}$, desde que $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$. Portanto, excluímos o caso em que $\operatorname{car}\mathbb{F} = p > 0$ e p divide n.

Então, até o fim desta subseção, vamos direcionar os nossos estudos para o caso faltante. A conclusão será que, essencialmente, o polinômio $X^p - X - a$ terá as propriedades que queremos, e por isso, será um substituto do polinômio $X^p - a$.

Vamos estudarmos as extensões cíclicas de grau p, em que $\operatorname{car}\mathbb{F} = p > 0$. Da caracterização de grupos solúveis finitos (veja abaixo), seguirá que esse caso é suficiente para os nossos propósitos.

Neste sentido, temos o seguinte:

Teorema 13.9 (Artin-Schreier)**.** *Seja $\operatorname{car}\mathbb{F} = p > 0$. Para todo $a \in \mathbb{F}$, o polinômio $f = X^p - X - a$ é separável e*

$$\mathscr{R}(f) = \{\alpha, \alpha + 1, \ldots, \alpha + p - 1\},$$

para qualquer $\alpha \in \mathscr{R}(f)$. Além disso, as seguintes afirmações são equivalentes:

(i) *f é irredutível em $\mathbb{F}[X]$,*
(ii) *$a \notin \{b^p - b \mid b \in \mathbb{F}\}$,*
(iii) *$\mathscr{R}(f) \cap \mathbb{F} = \emptyset$.*

Nestas condições, seja $\mathbb{E} = \mathbb{F}(\mathscr{R}(f))$. Então $\mathbb{E}/\mathbb{F}$ é uma extensão galoisiana de grau p, e $\operatorname{Aut}(\mathbb{E}/\mathbb{F})$ é cíclico de ordem p. Além disso, $\mathbb{E} = \mathbb{F}(\alpha)$, $\forall \alpha \in \mathscr{R}(f)$.

Demonstração. Assuma que $\alpha \in \mathscr{R}(f)$. Então, para qualquer $i \in \{0, 1, \ldots, p-1\}$, temos que

$$f(\alpha+i) = (\alpha+i)^p - (\alpha+i) - a = \alpha^p + i^p - \alpha - i - a = f(\alpha) + i - i = 0.$$

Portanto, $\{\alpha, \alpha + 1, \ldots, \alpha + p - 1\} \subseteq \mathscr{R}(f)$. Como f possui grau p, segue que os dois conjuntos coincidem. Em particular, f é separável.

$(i) \Rightarrow (ii)$: se $a = b^p - b$, para algum $b \in \mathbb{F}$, então $f(b) = b^p - b - a = 0$. Portanto, f não é irredutível em $\mathbb{F}[X]$.
$(ii) \Rightarrow (iii)$: Se existe $b \in \mathscr{R}(f) \cap \mathbb{F}$, então $0 = f(b) = b^p - b - a$. Portanto, $a = b^p - b$ está no conjunto definido em (ii).
$(iii) \Rightarrow (i)$: Assuma que $f = gh$, com $g \in \mathbb{F}[X]$ mônico e $1 \leq \mathrm{gr}(g) < p$. Escreva $g(X) = X^q + b_{q-1}X^{q-1} + \cdots + b_1X + b_0$. Então, existem $1 \leq j_1 < j_2 < \cdots < j_q \leq p-1$ tais que $g(X) = (X - \alpha - j_1) \cdots (X - \alpha - j_q)$. Portanto, $b_{q-1} = -\sum_{\ell=1}^{q}(\alpha + j_\ell) = -q\alpha - r \in \mathbb{F}$. Daí, $\alpha = -q^{-1}(b_{q-1} + r) \in \mathbb{F} \cap \mathscr{R}(f)$.

Para finalizar, da caracterização de $\mathscr{R}(f)$, segue que $\mathbb{E} = \mathbb{F}(\alpha)$ para qualquer $\alpha \in \mathscr{R}(f)$. Da Proposição 4.6, temos que $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \{\sigma_0, \sigma_1, \ldots, \sigma_{p-1}\}$, em que $\sigma_i(\alpha) = \alpha + i$. Além disso, note que $\sigma_0 = \mathrm{Id}_{\mathbb{E}}$ e $\sigma_i = \sigma_1^i$. Portanto, $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é cíclico, e gerado por σ_1. □

A recíproca do Teorema 13.3, na situação em que grau da extensão coincide com a característica do corpo, pode ser enunciada da seguinte forma:

Teorema 13.10. *Seja* $\mathrm{car}\,\mathbb{F} = p > 0$*, e assuma que* $\mathbb{E}/\mathbb{F}$ *é uma extensão cíclica de grau* p*. Denote* $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$*. Então, existe* $a \in \mathbb{F}$ *tal que* $f = X^p - X - a$ *é irredutível em* $\mathbb{F}[X]$ *e* $\mathbb{E} = \mathbb{F}(\mathscr{R}(f))$*. Neste caso,* $\mathbb{E} = \mathbb{F}(\alpha)$*,* $\forall \alpha \in \mathscr{R}(f)$*.*

Demonstração. Temos que $\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(-1) = p(-1) = 0$. Portanto, do Teorema 90 de Hilbert, existe $\alpha \in \mathbb{E}$ tal que $-1 = \alpha - \sigma(\alpha)$. Ou seja, $\sigma(\alpha) = \alpha + 1$. Daí $\sigma^j(\alpha) = \alpha + j$, para cada j. Os elementos $\alpha, \alpha+1, \ldots, \alpha+p-1$ são dois a dois distintos, e são raízes de $\mathrm{Irr}(\alpha, \mathbb{F})$. Portanto,

$$n \leq \mathrm{gr}(\mathrm{Irr}(\alpha, \mathbb{F})) \leq [\mathbb{E} : \mathbb{F}] = n.$$

Segue que $\mathrm{gr}(\mathrm{Irr}(\alpha, \mathbb{F})) = n$. Seja $a = \alpha(\alpha + 1) \cdots (\alpha + p - 1) = \prod_{j=0}^{n-1} \sigma^j(\alpha)$. Então, $\sigma(a) = a$. Daí $a \in \mathbb{E}^{\langle\sigma\rangle} = \mathbb{F}$. Segue que

$$\mathrm{Irr}(\alpha, \mathbb{F}) = \prod_{i=0}^{p-1}(X - \alpha - i) = X^p - X - a \in \mathbb{F}[X],$$

e portanto, $X^p - X - a$ é irredutível. As demais conclusões seguem do Teorema de Artin-Schreier. □

14. Solubilidade via radicais

14.1. **Revisão: Grupos solúveis.** Nesta subseção vamos relembrar a definição e algumas propriedades envolvendo grupos solúveis. Enunciaremos os resultados sem prová-los.

Definição 14.1. Seja G um grupo. Então G é *solúvel* se existe uma sequência de subgrupos

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = 1,$$

tal que, para todo $i = 1, \ldots, m$, $G_i \triangleleft G_{i-1}$ (ou seja, G_i é um subgrupo normal de G_{i-1}), e G_{i-1}/G_i é abeliano.

Teorema 14.2. *Seja G um grupo finito. Então G é solúvel se, e somente se, existe uma sequência de subgrupos*

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = 1,$$

tal que, para todo $i = 1, \ldots, m$, $G_i \triangleleft G_{i-1}$, e G_{i-1}/G_i é cíclico de ordem prima.

Teorema 14.3. *Sejam G um grupo e $H \subseteq G$ um subgrupo.*

(i) *Se G é solúvel, então H é solúvel.*
(ii) *Assuma que H é normal. Então G é solúvel se, e somente se, H e G/H são solúveis.*

Teorema 14.4. *Para $n \geq 5$, o grupo simétrico $\mathcal{S}_n$ não é solúvel.*

14.2. **Solubilidade via radicais em característica zero.** Vamos descrever formalmente o significado de ser possível caracterizar as raízes de um polinômio via operações do corpo e "extração de raízes".

Definição 14.5. Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos de característica zero. Dizemos que a extensão $\mathbb{E}/\mathbb{F}$ é *radical* se existe uma sequência de subcorpos

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_m = \mathbb{E}$$

satisfazendo a seguinte condição. Para cada $i = 0, 1, \ldots, m-1$, $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$, para algum $d_i \in \mathbb{F}_{i+1}$ tal que existe $n_i \in \mathbb{N}$ com $d_i^{n_i} \in \mathbb{F}_i$.

Definição 14.6. Seja $f \in \mathbb{F}[X]$ um polinômio separável. Dizemos que f é *solúvel por radicais* se existe uma extensão radical $\mathbb{E}/\mathbb{F}$ tal que $\mathbb{E} \supseteq \mathscr{R}(f)$.

A seguir, vamos definir o grupo de Galois de um polinômio separável:

Definição 14.7. Seja $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$ um polinômio separável. O *Grupo de Galois* do polinômio f é o grupo $G_f = \mathrm{Aut}(\mathbb{F}(\mathscr{R}(f))/\mathbb{F})$.

O resultado principal desta subseção é o seguinte:

Teorema 14.8. *Seja $\mathbb{F}$ um corpo de característica zero e $f \in \mathbb{F}[X]$ um polinômio separável. Então f é solúvel por radicais se, e somente se, o grupo de Galois G_f é solúvel.*

Antes de demonstrarmos o tal teorema, precisaremos dos seguintes resultados:

Lema 14.9. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão separável finita e radical. Então existe uma extensão $\mathbb{L}/\mathbb{E}$ tal que $\mathbb{L}/\mathbb{F}$ é galoisiana finita e radical.*

Demonstração. Do Teorema do Elemento Primitivo (Corolário 8.3.(i)), existe $a \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(a)$. Seja $\mathbb{L} = \mathbb{F}(\mathrm{Irr}(a, \mathbb{F}))$. Então $\mathbb{L}/\mathbb{F}$ é galoisiana finita, e $\mathbb{L}$ é uma extensão de $\mathbb{E}$ ($\mathbb{L}$ é o fecho normal da extensão $\mathbb{E}/\mathbb{F}$).

Da definição de extensão radical, denote

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \mathbb{F}_m = \mathbb{E},$$

e sejam $d_i \in \mathbb{E}$ tais que $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$, com $d_i^{n_i} \in \mathbb{F}_i$. Denote $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) = \{\sigma_1, \ldots, \sigma_s\}$, e assuma que $\sigma_1 = \mathrm{Id}_{\mathbb{L}}$. Defina indutivamente:

$$\begin{aligned} &\mathbb{E}_0 = \mathbb{E}, \\ &\mathbb{E}_j = \sigma_j(\mathbb{E}) \cdot \mathbb{E}_{j-1}, \quad j \geq 1. \end{aligned}$$

Note que $\mathscr{R}(\mathrm{Irr}(a, \mathbb{F})) \subseteq \mathbb{E}_s$. Portanto, $\mathbb{E}_s = \mathbb{L}$. Ainda, por construção, temos que

$$\mathbb{F} \subseteq \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \cdots \subseteq \mathbb{E}_s = \mathbb{L}.$$

Note que, para $i \geq 1$, temos

$$\begin{aligned} \mathbb{E}_{i-1} \subseteq \mathbb{E}_{i-1}(\sigma_i(d_1)) \subseteq \cdots \subseteq \mathbb{E}_{i-1}(\sigma_i(d_1), \sigma_i(d_2), \ldots, \sigma_i(d_m)) \\ = \mathbb{E}_{i-1} \cdot \sigma_i(\mathbb{E}) = \mathbb{E}_i. \end{aligned} \tag{14.3}$$

Além disso,

$$\sigma_i(d_j)^{n_j} \in \sigma_i(\mathbb{F}_j) = \sigma_i(\mathbb{F}(d_1, \ldots, d_{j-1})) \subseteq \mathbb{E}_{i-1}(\sigma_i(d_1), \ldots, \sigma_i(d_{j-1})).$$

Portanto, a extensão $\mathbb{E}_i/\mathbb{E}_{i-1}$ é radical. Concatenando as torres dadas por (14.3), para cada $i = 1, \ldots, s$, e a torre de $\mathbb{E}/\mathbb{F}$, obtemos que $\mathbb{L}/\mathbb{F}$ é radical. □

Lema 14.10. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita e solúvel de grau n. Assuma que $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$. Então $\mathbb{E}/\mathbb{F}$ é uma extensão radical.*

Demonstração. Como $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é solúvel e finito, existe uma sequência de subgrupos

$$\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_m = \{1\}$$

tal que $H_i \triangleleft H_{i-1}$ e H_{i-1}/H_i é cíclico de ordem prima. Da correspondência de Galois, obtemos sequência de corpos

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_m = \mathbb{E},$$

em que $\mathbb{F}_i = \mathbb{E}^{H_i}$. Como $\mathrm{Aut}(\mathbb{E}/\mathbb{F}_i) = H_i \triangleleft H_{i-1} = \mathrm{Aut}(\mathbb{E}/\mathbb{F}_{i-1})$, temos que $\mathbb{F}_i/\mathbb{F}_{i-1}$ é galoisiana finita. Ainda, $\mathrm{Aut}(\mathbb{F}_i/\mathbb{F}_{i-1}) \cong H_{i-1}/H_i$ é cíclico de ordem prima p. Como $\emptyset \neq \mathcal{P}_n(\mathbb{F}) \subseteq \mathcal{P}_n(\mathbb{F}_{i-1})$ e p divide n, segue que $\mathcal{P}_p(\mathbb{F}_{i-1}) \neq \emptyset$. Portanto, do Teorema 13.8, segue que existe $d_{i-1} \in \mathbb{F}_i$ tal que $\mathbb{F}_i = \mathbb{F}_{i-1}(d_{i-1})$, e $d_{i-1}^{n_{i-1}} \in \mathbb{F}_{i-1}$. Assim, $\mathbb{E}/\mathbb{F}$ é radical. □

Lema 14.11. *Seja $\mathbb{E}/\mathbb{F}$ galoisiana finita e radical, e escreva*

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_m = \mathbb{E}.$$

Sejam $d_i \in \mathbb{E}$ e $n_i \in \mathbb{N}$ tais que $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$ e $d_i^{n_i} \in \mathbb{F}_i$. Seja $n = \mathrm{mmc}(n_1, \ldots, n_m)$, e assuma que $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$. Então $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é solúvel.

Demonstração. Da correspondência de Galois, temos

$$\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\},$$

em que $H_i = \mathrm{Aut}(\mathbb{E}/\mathbb{F}_i)$. Como n_i divide n, segue que $\mathcal{P}_{n_i}(\mathbb{F}_i) = \mathcal{P}_{n_i}(\mathbb{F}) \neq \emptyset$. Portanto, do Teorema 13.3, temos que $\mathbb{F}_{i+1} = \mathbb{F}_i(\mathscr{R}(X^{n_i} - d_i^{n_i}))$, $\mathbb{F}_{i+1}/\mathbb{F}_i$ é galoisiana finita e $\mathrm{Aut}(\mathbb{F}_{i+1}/\mathbb{F}_i)$ é cíclica. Portanto, da correspondência de Galois, segue que $H_{i+1} \triangleleft H_i$ e $H_i/H_{i+1} \cong \mathrm{Aut}(\mathbb{F}_{i+1}/\mathbb{F}_i)$ é abeliana (de fato, é cíclica). Portanto, $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é solúvel. □

Agora temos todos os passos para demonstrarmos o Teorema 14.8.

Demonstração do Teorema 14.8. Assuma que $G_f = \mathrm{Aut}(\mathbb{F}(\mathscr{R}(f))/\mathbb{F})$ é solúvel. Sejam $\bar{\mathbb{F}}$ um fecho algébrico de $\mathbb{F}$, $n = [\mathbb{F}(\mathscr{R}(f)) : \mathbb{F}]$, $\xi \in \mathcal{P}_n(\bar{\mathbb{F}})$ e $\mathbb{E} = \mathbb{F}[\xi]$. Da Proposição 10.3, temos que

$$\mathrm{Aut}(\mathbb{E}(\mathscr{R}(f))/\mathbb{E}) \cong \mathrm{Aut}(\mathbb{F}(\mathscr{R}(f))/\mathbb{E} \cap \mathbb{F}(\mathscr{R}(f))) \subseteq \mathrm{Aut}(\mathbb{F}(\mathscr{R}(f))/\mathbb{F}).$$

Portanto, $\mathrm{Aut}(\mathbb{E}(\mathscr{R}(f))/\mathbb{E})$ é solúvel. Do Lema 14.10, sabe-se que $\mathbb{E}(\mathscr{R}(f))/\mathbb{E}$ é radical. Como $\mathbb{E} = \mathbb{F}(\xi)$ e $\xi^n \in \mathbb{F}$, segue que $\mathbb{E}(\mathscr{R}(f))/\mathbb{F}$ é radical. Portanto, f é solúvel via radicais.

Reciprocamente, assuma que f é solúvel via radicais. Então, existe $\mathbb{E}/\mathbb{F}$ finita e radical tal que $\mathscr{R}(f) \subseteq \mathbb{E}$. Do Lema 14.9, existe uma extensão $\mathbb{L}/\mathbb{E}$ tal que $\mathbb{L}/\mathbb{F}$ é galoisiana finita e radical. Da definição de extensão radical, escreva

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_m = \mathbb{L},$$

e sejam $d_i \in \mathbb{L}$ e $n_i \in \mathbb{N}$ tais que $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$ e $d_i^{n_i} \in \mathbb{F}_i$. Sejam $n = \text{mmc}(n_1, \ldots, n_m)$, $\bar{\mathbb{F}}$ o fecho algébrico de $\mathbb{F}$, e $\xi \in \mathcal{P}_n(\bar{\mathbb{F}})$. A extensão $\mathbb{L}(\xi)/\mathbb{F}(\xi)$ é radical, pois a torre seguinte satisfaz a definição:

$$\mathbb{F}(\xi) = \mathbb{F}_0(\xi) \subseteq \mathbb{F}_1(\xi) \subseteq \cdots \subseteq \mathbb{F}_m(\xi) = \mathbb{L}(\xi).$$

Então, segue do Lema 14.11, que $\text{Aut}(\mathbb{L}(\xi)/\mathbb{F}(\xi))$ é solúvel. Por Teorema 12.9, $\mathbb{F}(\xi)/\mathbb{F}$ é galoisiana e $\text{Aut}(\mathbb{F}(\xi)/\mathbb{F})$ é abeliano (e, portanto, solúvel). Daí, da correspondência de galois (Teorema 9.6.(3)), $\text{Aut}(\mathbb{F}(\xi)/\mathbb{F}) \cong \text{Aut}(\mathbb{L}(\xi)/\mathbb{F})/\text{Aut}(\mathbb{L}(\xi)/\mathbb{F}(\xi))$. Assim, $\text{Aut}(\mathbb{L}(\xi)/\mathbb{F})$ é solúvel (Teorema 14.3.(ii)).

Por fim, como $G_f \cong \text{Aut}(\mathbb{L}(\xi)/\mathbb{F})/\text{Aut}(\mathbb{L}(\xi)/\mathbb{F}(\mathscr{R}(f)))$, segue que G_f é solúvel. □

15. Extensão transcendente

Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos. Relembre que dizemos que um elemento $t \in \mathbb{E}$ é transcendente sobre $\mathbb{F}$ se $\mathbb{F}[t] \cong \mathbb{F}[X]$.

Definição 15.1. Dizemos que uma extensão de corpos $\mathbb{E}/\mathbb{F}$ é *transcendente* se a extensão não é algébrica.

Então, uma extensão de corpos $\mathbb{E}/\mathbb{F}$ é transcendente se e só se existe (pelo menos) um elemento $t \in \mathbb{E}$ que é transcendente sobre $\mathbb{F}$.

Definição 15.2. Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos. Dizemos que $t_1, \ldots, t_m \in \mathbb{E}$ são *algebricamente dependentes* sobre $\mathbb{F}$ se existe um polinômio não nulo $f \in \mathbb{F}[X_1, \ldots, X_m]$ tal que $f(t_1, \ldots, t_m) = 0$. Dizemos que os mesmos são *algebricamente independentes* se não forem algebricamente dependentes.

Equivalentemente, pode-se caracterizar a propriedade de ser algebricamente independente da seguinte maneira. Dados $t_1, \ldots, t_m \in \mathbb{E}$, fica bem definido o mapa

$$\psi_{(t_1,\ldots,t_m)} : \mathbb{F}[X_1, \ldots, X_m] \to \mathbb{E},$$

tal que $\psi_{(t_1,\ldots,t_m)} = f(t_1, \ldots, t_m)$. Dizemos que $t_1, \ldots, t_m$ são algebricamente independentes se $\psi_{(t_1,\ldots,t_m)}$ é um monomorfismo de anéis.

Definição 15.3. Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos. Um conjunto $M \subseteq \mathbb{E}$ é dito ser *algebricamente independente* sobre $\mathbb{F}$ se, para todo subconjunto finito $\{t_1, \ldots, t_m\} \subseteq M$, os elementos $t_1, \ldots, t_m$ são algebricamente independentes sobre $\mathbb{F}$.

Neste sentido, temos a seguinte propriedade de conjunto algebricamente independente:

Lema 15.4. *Sejam $\mathbb{E}/\mathbb{F}$ uma extensão de corpos e $M, N \subseteq \mathbb{E}$. Então, as seguintes afirmações são equivalentes:*

(1) *$M \cap N = \emptyset$ e $M \cup N$ é algebricamente independente sobre $\mathbb{F}$.*
(2) *M é algebricamente independente sobre $\mathbb{F}$, e N é algebricamente independente sobre $\mathbb{F}(M)$.*

Demonstração. (i)⇒(ii): Como $M \subseteq M \cup N$, obtemos que M é algebricamente independente sobre $\mathbb{F}$. Assuma que N não é algebricamente independente sobre $\mathbb{F}(M)$. Então, existem $t_1, \ldots, t_n \in N$ e $0 \neq f \in \mathbb{F}(M)[X_1, \ldots, X_n]$ tais que $f(t_1, \ldots, t_n) = 0$. Escreva

$$f = \sum_{I=(i_1,\ldots,i_n)} \frac{\alpha_I}{\beta_I} X_1^{i_1} \cdots X_n^{i_n},$$

em que $\alpha_I, \beta_i \in \mathbb{F}(M)$, e somente um número finito dos α_I é não nulo. Sejam $s_1, \ldots, s_m \in M$ todos os elementos que efetivamente aparecem em pelo menos um dos α_I ou β_I. Daí, $f \in \mathbb{F}(s_1, \ldots, s_m)[X_1, \ldots, X_n]$. Multiplicando por todos os β_I, podemos então assumir que

$$f \in \mathbb{F}[s_1, \ldots, s_m][X_1, \ldots, X_n].$$

Portanto, obtemos que $\{s_1, \ldots, s_m, t_1, \ldots, t_n\} \subseteq M \cup N$ é algebricamente dependente sobre $\mathbb{F}$, uma contradição.
(ii)⇒(i): Assuma que existem $s_1, \ldots, s_m \in M$, $t_1, \ldots, t_n \in N$, e um polinômio $0 \neq f \in \mathbb{F}[X_1, \ldots, X_{n+m}]$ tais que $f(s_1, \ldots, s_m, t_1, \ldots, t_n) = 0$. Se $n = 0$, então obtemos que M é algebricamente dependente sobre $\mathbb{F}$. Assuma então $n > 0$ e defina

$$g(X_1, \ldots, X_n) = f(s_1, \ldots, s_m, X_1, \ldots, X_n) \in \mathbb{F}(s_1, \ldots, s_m)[X_1, \ldots, X_n].$$

Então $g \neq 0$ e $g(t_1, \ldots, t_n) = 0$. Portanto, N é algebricamente dependente sobre $\mathbb{F}(M)$. □

Como consequência, se N possui um único elemento, então o lema anterior pode ser enunciado da seguinte forma:

Lema 15.5. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos, $M \subseteq \mathbb{E}$ um conjunto algebricamente independente sobre $\mathbb{F}$ e $t \in \mathbb{E}$, $t \notin M$. Então $M \cup \{t\}$ é algebricamente independente sobre $\mathbb{F}$ se, e somente se, t é transcendente sobre $\mathbb{F}(M)$.* □

Definição 15.6. Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos. Uma *base de transcendência* da extensão $\mathbb{E}/\mathbb{F}$ é um conjunto $M \subseteq \mathbb{E}$ algebricamente independente sobre $\mathbb{F}$, tal que $\mathbb{E}/\mathbb{F}(M)$ é algébrica.

Observação. Seja M uma base de transcendência da extensão de corpos $\mathbb{E}/\mathbb{F}$. Então, o grau da extensão $[\mathbb{E} : \mathbb{F}(M)]$ não é um invariante. Por exemplo, seja $\mathbb{E} = \mathbb{F}(t)$, em que t é transcendente sobre $\mathbb{F}$. Então $M_1 = \{t\}$ e $M_2 = \{t^2\}$ são bases de transcendência de $\mathbb{E}/\mathbb{F}$. Porém, $[\mathbb{E} : \mathbb{F}(M_1)] = 1$ e $[\mathbb{E} : \mathbb{F}(M_2)] = 2$.

A família $\mathscr{M}(\mathbb{E}/\mathbb{F})$ dos subconjuntos de $\mathbb{E}$ que são algebricamente independentes sobre $\mathbb{F}$ é parcialmente ordenado via inclusão. Seja $M \subseteq \mathbb{E}$ um conjunto algebricamente independente. Então, note que M é uma base de transcendência da extensão $\mathbb{E}/\mathbb{F}$ se e só se M é um elemento maximal da família $\mathscr{M}(\mathbb{E}/\mathbb{F})$.

Lema 15.7. *Sejam $\mathbb{E}/\mathbb{F}$ uma extensão de corpos, $M_0 \subseteq \mathbb{E}$ um conjunto algebricamente independente, e $S \subseteq \mathbb{E}$ tal que $\mathbb{E}/\mathbb{F}(S)$ é uma extensão algébrica. Então, existe $S' \subseteq S$ tal que $S' \cap M_0 = \emptyset$ e $S' \cup M_0$ é uma base de transcendência de $\mathbb{E}/\mathbb{F}$.*

Demonstração. Considere a família

$$\mathscr{M} = \{S_0 \subseteq S \mid \ S_0 \cap M_0 = \emptyset \text{ e } M_0 \cup S_0 \text{ é alg. independente}\}.$$

Sendo M_0 algebricamente independente, temos que $\emptyset \in \mathscr{M}$. Por Lema de Zorn (por que podemos aplicar?) existe um elemento maximal $S' \subseteq S$. Por construção, $S' \cap M_0 = \emptyset$. Se $S' \cup M_0$ não é uma base de transcendência, então existe $t \in \mathbb{E}$ que é transcendente sobre $\mathbb{F}(S' \cup M_0)$. Portanto, do Lema 15.5, $S' \cup \{t\} \in \mathscr{M}$, contradizendo a maximalidade de S'. □

Como consequência, temos que qualquer conjunto algebricamente independente pode ser completada para uma base de transcendência:

Corolário 15.8. *Seja $S \subseteq \mathbb{E}$ um conjunto algebricamente independente. Então existe uma base de transcendência M de $\mathbb{E}/\mathbb{F}$ que contém S.* □

Finalmente, mostraremos que a cardinalidade de uma base de transcendência finita é uma constante. Para isso, temos a seguinte observação:

Lema 15.9. *Sejam M uma base de transcendência de $\mathbb{E}/\mathbb{F}$, e $N \subseteq M$. Então $M \setminus N$ é uma base de transcendência de $\mathbb{E}/\mathbb{F}(N)$.*

Demonstração. Temos que $\mathbb{E}$ é algébrico sobre $\mathbb{F}(M) = \mathbb{F}(N)(M \setminus N)$. Além disso, do Lema 15.4, segue que $M \setminus N$ é algebricamente independente sobre $\mathbb{F}(N)$. Portanto, $M \setminus N$ é uma base de transcendência de $\mathbb{E}/\mathbb{F}(N)$. □

Teorema 15.10. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos que admite uma base de transcendência com $m < \infty$ elementos. Então toda base de transcendência de $\mathbb{E}/\mathbb{F}$ admite m elementos.*

Demonstração. Sejam M e S bases de transcendência de $\mathbb{E}/\mathbb{F}$, em que M possui m elementos. Por simetria do argumento, basta mostrarmos que a cardinalidade de S é $\leq m$. A demonstração será feita por indução em m, com a base $m = 0$ sendo válida pelo Lema 15.5.

Seja $s \in S$. Então, do Lema 15.7, existe $M_0 \subseteq M$ tal que $M_0 \cap \{s\} = \emptyset$ e $M_0 \cup \{s\}$ é uma base de transcendência de $\mathbb{E}/\mathbb{F}$. Como $s \notin M_0$ e s é algébrico sobre $\mathbb{F}(M)$, obtemos que $M_0 \neq M$, ou seja, $|M_0| \leq |M| - 1$. Por Lema 15.9, $S \setminus \{s\}$ e M_0 são bases de transcendência de $\mathbb{E}/\mathbb{F}(s)$. Assim, por hipótese de indução, obtemos que

$$|S| - 1 = |S \setminus \{s\}| \leq |M_0| \leq |M| - 1.$$

Portanto, $|S| \leq m$. □

O teorema anterior garante que a seguinte definição de grau de transcendência está bem posto.

Definição 15.11. Sejam $\mathbb{E}/\mathbb{F}$ uma extensão de corpos, e $M \subseteq \mathbb{E}$ uma base de transcendência da extensão. Dizemos que o *grau de transcendência* de $\mathbb{E}/\mathbb{F}$ é a cardinalidade de M, se a mesma for finita, e ∞ caso contrário. Denotamos o grau da transcendência da extensão por $\operatorname{gr}\operatorname{tr}(\mathbb{E}/\mathbb{F})$.

Neste sentido, temos o seguinte resultado:

Corolário 15.12. *Seja $\mathbb{E}/\mathbb{F}$ um corpo com $\operatorname{gr}\operatorname{tr}(\mathbb{E}/\mathbb{F}) = r < \infty$.*

(i) *Todo conjunto de $\mathbb{E}$ que é algebricamente independente sobre $\mathbb{F}$ possui no máximo r elementos. Em particular, um conjunto algebricamente independente é uma base de transcendência se, e somente se, o conjunto possui r elementos.*

(ii) *Todo subconjunto $S \subseteq \mathbb{E}$ tal que $E/\mathbb{F}(S)$ é algébrica possui no mínimo r elementos. Em particular, S é uma base de transcendência se, e só se, S possui exatamente r elementos.* □

Lema 15.13. *Sejam $\mathbb{L}/\mathbb{E}/\mathbb{F}$ extensões de corpos, N uma base de transcendência de $\mathbb{L}/\mathbb{E}$, e M uma base de transcendência de $\mathbb{E}/\mathbb{F}$. Então $M \cap N = \emptyset$ e $M \cup N$ é uma base de transcendência de $\mathbb{L}/\mathbb{F}$.*

Demonstração. Sendo $\mathbb{E}/\mathbb{F}(M)$ extensão de corpos e N algebricamente independente sobre $\mathbb{E}$, obtemos que N é algebricamente independente sobre $\mathbb{F}(M)$. Daí, do Lema 15.4, $M \cup N$ é algebricamente independente sobre $\mathbb{F}$, e $M \cap N = \emptyset$. Agora, todo elemento de $\mathbb{E}$ é algébrico sobre $\mathbb{F}(M)$. Além disso, $\mathbb{E}(N) = \mathbb{F}(N)(\mathbb{E})$, e $\mathbb{F}(M \cup N) = \mathbb{F}(M)(N)$. Conclui-se que a extensão $\mathbb{E}(N)/\mathbb{F}(M \cup N)$ é algébrica. Como $\mathbb{L}/\mathbb{E}(N)$ e $\mathbb{E}(N)/\mathbb{F}(M \cup N)$ são algébricas, segue que $\mathbb{L}/\mathbb{F}(M \cup N)$ é algébrica. Portanto, $M \cup N$ é uma base de transcendência de $\mathbb{L}/\mathbb{F}$. □

Como consequência do teorema anterior, obtemos a seguinte propriedade aditiva do grau de transcendência.

Corolário 15.14. *Sejam $\mathbb{L}/\mathbb{E}/\mathbb{F}$ extensões de corpos. Então*

$$\operatorname{gr}\operatorname{tr}(\mathbb{L}/\mathbb{F}) = \operatorname{gr}\operatorname{tr}(\mathbb{L}/\mathbb{E}) + \operatorname{gr}\operatorname{tr}(\mathbb{E}/\mathbb{F})$$

Tal fórmula continua válida para graus de transcendência infinita. □