

1 Extensões normais, separáveis e Galoisianas

A Teoria de Galois é um dos avanços mais impressionantes da matemática moderna. Com seu estudo de raízes de polinômios, Evariste Galois foi capaz de construir os fundamentos para uma teoria que foi capaz de resolver não só o problema da solubilidade de equações polinômiais por meio de radicais, mas também, de forma surpreendente problemas muito antigos da geometria clássica grega, isto é, o problema da duplicação do cubo, quadratura do círculo e trissecção do ângulo.

Nesta semana discutiremos o grupo de Galois de uma extensão de corpos, e provaremos o teorema fundamental da teoria de Galois.

Enunciaremos aqui o seguinte lema que foi provado nas notas da semana passada, mas será utilizado aqui novamente.

Lema 1. *Seja $K \subset L$ uma extensão de corpos. Se $\tau : L \rightarrow L$ é um homomorfismo de corpos cuja restrição à K é a identidade (dizemos que τ é um **K -morfismo**), então τ é isomorfismo.*

Teremos a seguinte caracterização.

Teorema 2. *Sejam $K \subset L$ uma extensão algébrica e $\overline{K}$ um fecho algébrico de K , contendo L . São equivalentes:*

1. *L é corpo de decomposição de algum polinômio em $f \in K[x]$.*
2. *Todo K -morfismo $\sigma : L \rightarrow \overline{K}$, verifica $\sigma(L) = L$.*
3. *Se um polinômio irreduzível em $K[x]$ possui uma raiz em L , então ele possui todas as raízes em L .*

Demonstração. (1) $\Rightarrow$ (2) Sabemos que $L = K(Z)$, onde Z é o conjunto das raízes de algum polinômio $f \in K[x]$. Então dado $\alpha \in Z$, temos $f(\alpha) = 0$ para algum $f \in \Lambda$ e mais,

$$0 = \sigma(f(\alpha)) = f(\sigma(\alpha)),$$

ou seja, $\sigma(Z) \subset Z$. Logo, $\sigma(L) \subset L$ e pelo Lema 1 temos $\sigma(L) = L$.

(2) $\Rightarrow$ (3) Seja $f \in K[x]$ um polinômio irreduzível que possui uma raiz $\alpha \in L$. Seja $\beta \in \bar{K}$ outra raiz de f . Como f é irreduzível sabemos que existe um K -isomorfismo $\theta : K(\alpha) \rightarrow K(\beta)$, com $\theta(\alpha) = \beta$. Assim, existe $\sigma : L \rightarrow \bar{K}$, tal que $\sigma|_K = \theta$. Então por (2), temos $\sigma(L) = L$, donde $\sigma(\alpha) = \theta(\alpha) = \beta$ e então $\beta \in L$.

(3) $\Rightarrow$ (1) Seja Λ a família dos polinômios $p_{\alpha/K} \in K[x]$ para todo $\alpha \in L$. Então $K \subset L$ é algébrica e tomando $f = \prod p_{\alpha/K}$, (1) é imediato. □

Definição 3. Uma extensão $K \subset L$ satisfazendo uma das condições equivalentes do Teorema 2 é dita **normal**.

Observação 4. Se $K \subset L \subset F$ é uma torre de extensões com $K \subset L$ e $L \subset F$ normais, a extensão $K \subset F$ não é necessariamente normal. De fato, sejam $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$ e $F = \mathbb{Q}(\sqrt{\sqrt{2}}) = \mathbb{Q}(\sqrt[4]{2})$. Temos L corpo de decomposição para $x^2 - 2 \in \mathbb{Q}[x]$ e F corpo de decomposição para $x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$, mas F possui não todas as raízes de $x^4 - 2 \in \mathbb{Q}[x]$. No entanto, temos o seguinte resultado.

Relembraremos agora a definição de característica de um corpo, que já discutimos na seção de anéis, mas que terá um papel importante a partir de agora.

Definição 5. Seja K um corpo. Chamamos de **característica de K** o menor inteiro m tal que $m \cdot a = 0$ para todo $a \in K$, e denotamos $\text{char}(K) = m$. Caso este inteiro não exista diremos que K possui característica zero, e escreveremos $\text{char}(K) = 0$.

Definição 6. Sejam k um corpo de característica 0 e $f(x) \in k[x]$, com $\deg f = n \geq 1$. Dizemos que α é uma **raiz de multiplicidade m** de f se $(x - \alpha)^m$ divide f mas $(x - \alpha)^{m+1}$ não divide f . Se $m = 1$ diremos que α é uma raiz simples. Diremos que $f(x)$ é **separável** se toda raiz de $f(x)$ num fecho algébrico, $\bar{k}$, de k é simples, isto é, $f(x)$ tem exatamente n raízes em $\bar{k}$.

Para a prova do seguinte resultado, precisaremos da noção de *derivada* de um polinômio. Se K é um corpo, e $f \in K[x]$, com $f(x) = \sum_{i=0}^n a_i x^i$ definimos a **derivada (formal)** de f como sendo $f'(x) = \sum_{i=1}^n i a_i x^{i-1}$. É importante notar fácil ver que a operação de derivada formal não tem nada a ver com os limites que aprendemos em cálculo, por isso o uso da palavra formal. Também é fácil ver que a operação de derivada assim definida satisfaz todas as propriedades para derivadas de soma e produto que estamos acostumados, bem como a regra de Leibniz. Utilizando essas propriedades, podemos provar a seguinte proposição.

Proposição 7. *Sejam K um corpo de característica 0 e $f \in K[x]$. Então α é uma raiz de multiplicidade m de f se, e somente se α for raiz de $f^{(m+1)}$ e não for raiz de $f^{(m+2)}$. Em particular, α é simples se, e somente se α não é raiz de f' .*

Proposição 8. *Sejam K um corpo e $P \in K[x]$ um polinômio irredutível, mônico de graus n . Então as seguintes afirmações são verdadeiras:*

- Se $\text{char}(K) = 0$, então $P(x)$ é separável.
- Se $\text{char}(K) = p$ com p primo, então existem um inteiro positivo μ e $G(x) \in K[x]$ tal que $P(x) = G(x^{p^\mu})$.

Demonstração. Provaremos apenas o primeiro item. Seja $\alpha \in \overline{K}$ uma raiz de f . Note que como f é mônico e irredutível, segue da definição que f é o polinômio minimal de α . Suponha que α é um raiz de P com multiplicidade $m \geq 2$, então pela Proposição 7, $P'(\alpha) = 0$. Como $\text{char}(K) = 0$, temos que o grau de f é $n - 1$ que tem α como raiz, assim P divide P' o que é absurdo pois o grau de f é n . $\square$

Definição 9. Sejam $K \subset L$ uma extensão de corpos e α um elemento algébrico sobre K . Dizemos que α é **separável sobre K** se seu polinômio minimal, $p_{\alpha/K}(x)$, for separável. Quando a extensão $K \subset L$ for algébrica, dizemos que ela é separável se todo $\alpha \in L$ for separável sobre K .

IMPORTANTE: Dados uma extensão de corpos $L|K$ e $\alpha \in L$ algébrico sobre K temos, pela proposição anterior, que se $ch(K) = 0$ então α é separável e portanto qualquer extensão algébrica sobre um corpo de característica zero é separável.

Dada uma extensão finita de corpos $K \subset L$ de grau n , nem sempre é verdade que L possui um elemento de grau n sobre K . É claro que isso sempre ocorre se $L = K(\alpha)$ para algum elemento $\alpha \in L$. O seguinte teorema nos ajudará a entender quando é possível encontrar tal elemento.

Teorema 10 (Teorema do elemento primitivo). *Seja $K \subset L$ uma extensão finita de corpos. Então existe um elemento $\alpha \in L$ tal que $L = K(\alpha)$ se, e somente se, o número de corpos F intermediários na extensão $K \subset F \subset L$ é finito. Tal elemento α é dito **elemento primitivo** da extensão $K \subset L$.*

Demonstração. ($\Rightarrow$) Suponha que existe $\alpha \in L$ tal que $L = K(\alpha)$. Como $K \subset L$ é uma extensão finita, segue que é algébrica, e assim seja $p_{\alpha/K} \in K[x]$ o polinômio minimal de α sobre K . Seja F um corpo intermediário da extensão, ou seja, $K \subset F \subset L$ e seja $p_{\alpha/F}$ o polinômio minimal de α sobre F .

Sejam $\{a_1, \dots, a_m\} \in F$ os coeficiente de $p_{\alpha/F}$, e $F' = K(a_1, \dots, a_m)$ o corpo de adjunção. Então, o polinômio minimal de α sobre F' , $p_{\alpha/F'}$, coincide com $p_{\alpha/F}$, como $F' \subset F$, temos a cadeia de extensões $F' \subset F \subset L$ e então:

$$[L : F'] = [L : F][F : F']$$

Como $p_{\alpha/F'} = p_{\alpha/F}$ temos que $[L : F'] = [L : F]$, logo $[F : F'] = 1$ o que implica que $F = F'$.

Isto é, o polinômio minimal de cada corpo intermediário na extensão $K \subset F \subset L$ define um ÚNICO corpo intermediário.

Como $[L : K] = [L : F][F : K]$, segue que $\deg p_{\alpha/K} \geq \deg p_{\alpha/F}$, pelo algoritmo da divisão de Euclides em $K[x]$ temos que existem $q, r \in K[x]$ com $p_{\alpha/K}(x) = p_{\alpha/F}(x)q(x) + r(x)$ com $r = 0$ ou $\deg r < \deg p_{\alpha/F}$. Como $p_{\alpha/K}(\alpha) = r(\alpha) = 0$, temos pela minimalidade do polinômio minimal que $r = 0$ e assim $p_{\alpha/F}$ divide $p_{\alpha,K}$. **Assim, o polinômio minimal de todo**

corpo intermediário na extensão $K \subset F \subset L$ divide o $p_{\alpha/K}$

Por fim, como um polinômio admite apenas um número finito de divisores mônicos, temos que existe um número finito de classes de isomorfismos de corpos intermediários na extensão.

($\Leftarrow$) Assuma que o número de corpos F intermediários na extensão $K \subset F \subset L$ é finito.

Se K é finito, e como $K \subset L$ é finita segue que L também é finito. Assim, L^* (o grupo dos elementos não nulos de L) é um grupo cíclico, e portanto existe $\alpha \in L$ tal que $L^* = \{1, \alpha, \dots, \alpha^n\}$, logo $L = K(\alpha)$.

Assuma então K infinito. Neste caso, L também é infinito. Sejam $\{\beta_1, \dots, \beta_n\}$ uma base de L sobre K . Assim, temos que $L = K(\beta_1, \dots, \beta_n)$. Se provarmos que uma extensão gerada por quaisquer dois elementos pode ser gerada por um único elemento, podemos proceder de forma indutiva para obter nosso resultado.

Desta forma, assuma que $L = K(a, b)$ com $a, b \in L$. Considere os elementos da forma $\{a + fb\}$ com $f \in K \setminus \{0\}$. Como K é infinito por hipótese, temos que $\{a + fb\}_{f \in K}$ é infinito, mas como temos que existe um número finito de extensões intermediárias $K \subset F \subset L$, então existem $f_1, f_2 \in K$ tal que $K(a + f_1b) = K(a + f_2b) =: F$.

Vamos mostrar que $L = K(a, b) = K(\alpha)$, com $\alpha := a + f_1b$.

Como $a + f_1b$ e $a + f_2b$ estão em F , segue que $a + f_1b - (a + f_2b) \in F$, logo $(f_1 - f_2)b \in F$, e portanto $b \in F$. Ademais como $f_1 \in K \subset F$ segue que $f_1b \in F$ e portanto $a \in F$. Logo $L = K(a, b) \subseteq F$ e portanto $L = F = K(\alpha)$. $\square$

Com as mesmas ideias do teorema anterior é possível provar que

Corolário 11. *Seja $K \subset L$ uma extensão finita de corpos. Se L é separável sobre K então esta extensão admite elemento primitivo, isto é, existe $\alpha \in L$ tal que $L = K(\alpha)$.*

A seguinte proposição será útil em nossos estudos, mas não a demonstraremos aqui.

Proposição 12. *Seja L o corpo de decomposição de um polinômio $f \in F[x]$. Seja $h \in F[x]$ irredutível, de modo que $\alpha, \beta \in L$ são duas raízes distintas de h . Então existe um isomorfismo de $\varphi : L \rightarrow L$ tal que $\varphi(\alpha) = \beta$ e $\varphi(b) = b$ para todo $b \in L$.*

Começaremos agora a definir nossos principais objetos de estudo.

Proposição 13. *Seja $K \subset L$ uma extensão de corpos. O conjunto $\text{Gal}(L/K)$ definido como*

$$\text{Gal}(L/K) := \{\sigma : L \rightarrow L; \sigma \text{ automorfismo}, \sigma(a) = a \forall a \in K\}$$

tem estrutura de grupo, chamado grupo de Galois de $K \subset L$

Demonstração. É claro que o morfismo identidade $1_L : L \rightarrow L$ está em $\text{Gal}(L/F)$. Vamos mostrar que $\text{Gal}(L/K)$ é fechado para a composição. Sejam $\sigma, \tau \in \text{Gal}(L/K)$, temos que $\sigma \circ \tau : L \rightarrow L$ é um automorfismo e para todo $a \in K$, temos $\sigma \circ \tau(a) = \sigma(\tau(a)) = a$. $\square$

Para computarmos o grupo de Galois de uma extensão de corpos, precisamos entender como os elementos de $\text{Gal}(L/F)$ se comportam. Para isso, a seguinte proposição será muito útil.

Proposição 14. *Seja $K \subset L$ uma extensão de corpos, e $\sigma \in \text{Gal}(L/F)$. Então:*

- a) Se $h \in K[x]$ é um polinômio não constante tal que $h(\alpha) = 0$ com $\alpha \in L$, então $h(\sigma(\alpha)) = 0$.*
- b) Se $L = K(\alpha_1, \dots, \alpha_n)$, então σ é unicamente determinado pelos seus valores em $\alpha_1, \dots, \alpha_n$.*

Demonstração. Para o item a) temos que como σ preserva adição, multiplicação e é a identidade nos coeficientes de um polinômio em $K[x]$, segue que

$$0 = \sigma(0) = \sigma(h(\alpha)) = h(\sigma(\alpha))$$

e portanto $\sigma(\alpha) \in L$ também é raiz de h .

Para o item *b*), note que $L = K[\alpha_1, \dots, \alpha_n]$, e como $K(\alpha_1, \dots, \alpha_n)$ é uma extensão de K , qualquer $\beta \in L$ pode ser escrito como $\beta = h(\alpha_1, \dots, \alpha_n)$ para algum polinômio $h \in K[x_1, \dots, x_n]$. Como σ preserva adição, multiplicação e é a identidade nos coeficientes de um polinômio em $K[x]$, segue

$$\sigma(\beta) = \sigma(h(\alpha_1, \dots, \alpha_n)) = h(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$$

logo segue que $\sigma : L \rightarrow L$ é unicamente determinado por $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$. $\square$

Esta proposição nos leva ao primeiro resultado estrutural sobre a estrutura de $\text{Gal}(L/F)$.

Corolário 15. *Seja $K \subset L$ uma extensão finita de corpos. Então $|\text{Gal}(L/K)| < \infty$.*

Demonstração. Como $K \subset L$ é uma extensão finita, segue que $L = K(\alpha_1, \dots, \alpha_n)$, onde cada $\alpha_i \in L$ é algébrico sobre K . Agora suponha que $\sigma \in \text{Gal}(L/K)$. Segue que σ é unicamente determinado pelos valores nos α_i . Adicionalmente, seja $p_i \in K[x]$ o polinômio minimal de α_i . Pela parte *a*) da Proposição 14 temos que existe no máximo $\deg p_i$ possibilidades para $\sigma(\alpha_i)$ (uma vez que $\sigma(\alpha_i)$ é raiz de p_i), de onde vem o resultado. $\square$

Corolário 16. *Seja $K \subset L$ uma extensão finita de corpos com $L = K(\alpha_1, \dots, \alpha_n)$, onde cada $\alpha_i \in L$ é algébrico sobre K . Então $|\text{Gal}(L/K)| \leq \prod \deg p_{\alpha_i, K}$, onde $p_{\alpha_i, K}$ é o polinômio minimal de α_i sobre K .*

Exemplo 1. Considere a extensão $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt[3]{2})$. O polinômio mínimo de $\sqrt[3]{2}$ é $x^3 - 2$. As raízes de $x^3 - 2$ são $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, onde $\omega = e^{\frac{2\pi i}{3}}$. Como $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ não são reais, segue da Proposição 14 que se $\sigma \in \text{Gal}(L/\mathbb{Q})$, então $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, como σ é unicamente determinado por $\sqrt[3]{2}$, temos que $\sigma = I_L$. Assim $\text{Gal}(L/\mathbb{Q}) = \{I_L\}$.

Exemplo 2. Seja $F = K(t)$, com K corpo de característica p e t uma variável. Seja $f(x) = x^p - t \in F[x]$. Seja $\alpha \in \overline{F}$ uma raiz de f , onde $\overline{F}$ denota o fecho algébrico de F . Afirmamos que α é a única raiz de f em $\overline{F}$, e

portanto possui multiplicidade p . De fato, Se α é raiz de f , segue que $\alpha^p = t$, e como $(x - \alpha)^p = x^p - \alpha^p = x^p - t$, segue que α é a única raiz de f , e que f é irredutível sobre F . Seja $L = F(\alpha)$. Como α é a única raiz de f , temos, argumentando de maneira análoga ao caso anterior que $\text{Gal}(L/F) = \{I_F\}$.

Exemplo 3. Seja $\tau : \mathbb{C} \rightarrow \mathbb{C}$ a conjugação complexa. É claro que τ é um automorfismo de $\mathbb{C}$ que fixa $\mathbb{R}$. Logo $\text{Gal}(\mathbb{C}/\mathbb{R})$ possui pelo menos dois elementos. Como $\mathbb{C} = \mathbb{R}(i)$, e como $x^2 + 1$ é o polinômio minimal de i sobre $\mathbb{R}$, segue do Corolário 16 que $|\text{Gal}(\mathbb{C}/\mathbb{R})| \leq 2$ e portanto $|\text{Gal}(\mathbb{C}/\mathbb{R})| = 2$, mais precisamente $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{1_{\mathbb{C}}, \tau\} \simeq \mathbb{Z}/2\mathbb{Z}$.

Sejam $K \subset L_1$ e $K \subset L_2$ duas extensões finitas de corpos, uma pergunta natural que surge é qual a relação entre $\text{Gal}(L_1/K)$ e $\text{Gal}(L_2/K)$. No caso em que $L_1 \simeq L_2$ temos a seguinte proposição.

Proposição 17. *Sejam $K \subset L_1$ e $K \subset L_2$ duas extensões finitas de corpos, com $L_1 \simeq L_2$, tal que o isomorfismo fixa K . Então $\text{Gal}(L_1/K) \simeq \text{Gal}(L_2/K)$.*

Demonstração. Seja $\varphi : L_1 \rightarrow L_2$, um isomorfismo de corpos, tal que $\varphi(k) = k$ para todo $k \in K$. Defina $\Psi : \text{Gal}(L_1/K) \rightarrow \text{Gal}(L_2/K)$ tal que para todo $\sigma \in \text{Gal}(L_1/K)$, $\Psi(\sigma) = \varphi \circ \sigma \circ \varphi^{-1}$. É fácil ver que Ψ define um isomorfismo de grupos. $\square$

Lembre-se que o corpo de decomposição de um polinômio é único a menos de isomorfismo, assim, a proposição anterior nos permite fazer a seguinte definição.

Definição 18. Sejam K um corpo e $f \in K[x]$. Seja L o corpo de decomposição de f . Diremos que o **grupo de Galois de f** é o grupo $\text{Gal}(L/K)$, que será denotado por $\text{Gal}(f, K)$

Nosso próximo objetivo será relacionar o grau de f com a ordem de $\text{Gal}(f, K)$.

Lembre-se que dizemos que um polinômio f é dito separável se possui raízes distintas no seu corpo de decomposição. Essa foi a situação considerada por Galois.

Agora provaremos o primeiro resultado principal da Teoria de Galois

Teorema 19. *Se L é o corpo de decomposição de um polinômio separável f em $K[x]$, então o grupo de Galois de $K \subset L$ tem ordem $|\text{Gal}(L/K)| = [L : K]$*

Sejam $\{\alpha_1, \dots, \alpha_n\}$ as distintas raízes de f . Então $L = K(\alpha_1, \dots, \alpha_n)$.

Afirmção 1: Cada α_i é separável sobre K Como $p_{\alpha_i, K}$ divide f , se $p_{\alpha_i, K}$ não fosse separável, isto é, tivesse raízes múltiplas, f também teria, contradição.

Portanto $L|K$ é separável, e pelo Teorema do Elemento primitivo, temos que existe $\beta \in L$ tal que $L = K(\beta)$. Seja $p_{\beta, K}$ o polinômio minimal de β sobre K . Temos que $[L : K] = \deg p_{\beta, K}$.

Afirmção 2: $|\text{Gal}(L/K)| = \deg p_{\beta, K}$

Seja $m = \deg p_{\beta, K}$. Como $p_{\beta, K}$ é polinômio minimal de β , por definição ele é mônico e irredutível, e portanto todas as suas raízes são distintas. Como $\beta \in L$, e L é corpo de decomposição, segue que todas as raízes de $p_{\beta, K}$ estão contidas em L . Sejam $\beta, \beta_2, \dots, \beta_m$ as raízes de $p_{\beta, K}$. Pelo Proposição 12, para cada $i \in \{2, \dots, m\}$ existe um automorfismo $\sigma_i : L \rightarrow L$ tal que σ_i fixa K e $\sigma_i(\beta) = \beta_i$. Como cada $\beta_i \neq \beta_j$ para $i \neq j$, temos que $\sigma_i \neq \sigma_j$ e portanto $|\text{Gal}(L/K)| \geq m$. (NÃO ESQUEÇA DE CONTAR O MORFISMO IDENTIDADE)

Como $L = K(\beta)$, dado $\sigma \in \text{Gal}(L/K)$, pela Proposição 14 temos que σ é unicamente determinado pelo valor $\sigma(\beta) \in \{\beta_2, \dots, \beta_m\}$, portanto $\sigma = \sigma_i$ para algum i , e então $|\text{Gal}(L/K)| = m$.

Exemplo 4. Seja $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. L é corpo de decomposição de $f = (x^2 - 2)(x^2 - 3)$, com $f \in \mathbb{Q}[x]$. Então pelo Teorema anterior temos que $|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 4$. Como $\text{Gal}(L/\mathbb{Q})$ não tem nenhum elemento de ordem 4, uma vez que $\sigma^2 = I_L$ para todo $\sigma \in \text{Gal}(L/\mathbb{Q})$, temos que $\text{Gal}(L/\mathbb{Q})$ é o grupo de Klein.

É importante observar que as hipóteses do corpo L ser o corpo de decomposição de algum polinômio, e de a extensão ser separável não podem ser retiradas. No exemplo 1 note que $\mathbb{Q}(\sqrt[3]{2})$ não é corpo de decomposição, e que no Exemplo 2, L não é separável.

Nosso próximo objetivo será estudar com mais detalhes o grupo de Galois de um polinômio.

Seja f um polinômio separável em $K[x]$, e L um corpo de decomposição para f . Nós interpretaremos $\text{Gal}(L/K)$ em termos das permutações das raízes de f .

Proposição 20. *Sejam f um polinômio separável em $K[x]$ de grau n e L um corpo de decomposição para f . Existe um monomorfismo de grupos $\varphi : \text{Gal}(L/K) \rightarrow S_n$, onde S_n denota o grupo de permutações de n elementos.*

Demonstração. Seja $f = c(x - \alpha_1) \cdots (x - \alpha_n)$. Com $c \neq 0$. Dado $\sigma \in \text{Gal}(L/K)$, temos que $\sigma(\alpha_i)$ também é uma raiz de f , então $\sigma(\alpha_i) = \alpha_{\tau(i)}$ para algum $\tau(i) \in \{1, \dots, n\}$, note que $\tau(i)$ é unicamente determinado, uma vez que $\alpha_1, \dots, \alpha_n$ são distintos. Note também que $\tau : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ é injetivo, e portanto bijetiva (por se tratar de função de conjuntos finito). Segue que $\tau \in S_n$ e temos então definido o mapa $\varphi : \text{Gal}(L/K) \rightarrow S_n$. Este mapa é claramente um homomorfismo de grupos, e como $L = K(\alpha_1, \dots, \alpha_n)$, segue da Proposição 14 b) que φ é injetivo. $\square$

Corolário 21. *Sejam f um polinômio separável em $K[x]$ de grau n e L um corpo de decomposição para f . Então $[L : K]$ divide $n!$*

Demonstração. Segue do fato que podemos ver $\text{Gal}(L/K)$ como subgrupo de S_n , e portanto pelo Teorema de Lagrange temos que $|\text{Gal}(L/K)|$ divide $|S_n| = n!$ como pelo Teorema 19 $|\text{Gal}(L/K)| = [L : K]$ temos o resultado. $\square$

Além disso, a seguinte proposição se faz útil no estudo da estrutura de grupo de Galois de uma extensão.

Proposição 22. *Seja $K \subset F \subset L$ uma torre de extensões tal que $K \subset L$ e $K \subset F$ são normais. Então $\text{Gal}(L/F)$ é um subgrupo normal de $\text{Gal}(L/K)$ e ademais temos que*

$$\text{Gal}(L/K)/\text{Gal}(L/F) \simeq \text{Gal}(F/K)$$

Nosso próximo objetivo será relacionar subgrupos de um grupo de Galois de uma extensão $L|K$ com subcorpos intermediários desta extensão. Seja $K \subset F \subset L$ uma torre de extensão finita de corpos e H um subgrupo de $\text{Gal}(L/K)$. Definimos

$$\Gamma(F) := \{\alpha \in \text{Aut}(L); \alpha(a) = a \forall a \in F\}$$

$$\Phi(H) := \{x \in L; \alpha(x) = x \forall \alpha \in H\}$$

Começaremos com o seguinte resultado

Proposição 23. *Seja $L|K$ uma extensão de corpos. Então as seguintes afirmações são verdadeiras.*

- a) *Para cada torre de extensão de corpos $L|F|K$, temos que $\Gamma(F)$ é um subgrupo de $\text{Gal}(L/K)$.*
- b) *Para cada subgrupo H de $\text{Gal}(L/K)$, temos que $\Phi(H)$ é um subcorpo na torre de extensões $K \subset \Phi(H) \subset L$*

Demonstração. (a) Temos que $\Gamma(F)$ é não vazio pois $I_L \in \Gamma(F)$. Além disso, é fácil ver que a composta de dois automorfismos que fixam F também fixa F , e se $\sigma \in \Gamma(F)$, então $\sigma^{-1} \in \Gamma(F)$, uma vez que $\sigma^{-1} \in \text{Aut}(L)$, e como $\sigma(a) = a$ para todo $a \in F$, temos que $\sigma^{-1}(a) = a$ para todo $a \in F$.

(b) Temos que $\Phi(H)$ é não vazio pois $1_L \in \Phi(H)$. É claro que $\Phi(H)$ é um corpo, e como $H \leq \text{Gal}(L/K)$ temos que $\Phi(H) \supset K$, ademais se H for um subgrupo próprio, teremos que $K \subset \Phi(H)$ propriamente. $\square$

Nosso objetivo será entender quando Φ e Γ são inversos um para o outro.

Apesar de a demonstração do seguinte resultado ser uma tautologia, é importante enunciá-lo, pois ele nos ajudará na demonstração do teorema principal.

Proposição 24. *Seja $K \subset F \subset L$ uma torre de extensão de corpos, e $H \leq \text{Gal}(L/K)$ um subgrupo. Então temos*

- a) $F \subseteq \Phi(\Gamma(F));$
- b) $H \subseteq \Gamma(\Phi(H)).$

Veremos que será possível obter a igualdade dos conjuntos acima, em um tipo especial de extensão. Usaremos a seguinte definição.

Definição 25. Uma extensão de corpos $L|K$ é dita **de Galois** ou **Galoisiana** se $L|K$ for separável e normal.

Lembre-se que uma extensão é dita normal se ela é o corpo de decomposição de algum polinômio.

Exemplo 5. $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ é de Galois uma vez que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é o corpo de decomposição de $f(x) = (x^2 - 2)(x^2 - 3)$ e portanto a extensão é normal e como a característica de $\mathbb{Q}$ é zero segue que a extensão é separável.

Exemplo 6. Note que $\mathbb{Q}(\sqrt[3]{2})$ não é normal sobre $\mathbb{Q}$ e portanto $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ não é Galois.

Usaremos a seguinte terminologia. Sejam $L|K$ uma extensão de corpos e um homomorfismo $\sigma : L \rightarrow L$ que fixa K , chamaremos σ de K -homomorfismo. Analogamente, se $L|F|K$ é uma torre de extensões, e $\sigma : F \rightarrow L$ é um monomorfismo que fixa K então chamaremos σ de K -monomorfismo.

Precisaremos do seguinte resultado sobre extensões separáveis.

Lema 26. *Seja $K \subset L$ uma extensão separável de corpos tal que $[K(u) : K] \leq n$ para cada $u \in L$. Então existe $\alpha \in L$ tal que $L = K(\alpha)$ e portanto a extensão $K \subset L$ é finita com $[L : K] \leq n$*

Demonstração. Pela hipótese podemos tomar $\alpha \in L$ tal que $[K(\alpha) : K] = \max\{[K(u) : K]\}$; Suponha que existe $a \in L \setminus K(\alpha)$. Como $L|K$ é separável, pelo teorema do elemento primitivo temos que existe $\beta \in L$ tal que $K(\beta) = K(\alpha, a)$. Mas então $[K(\beta) : K] = [K(\alpha, a) : K] = [K(\alpha, a) : K(\alpha)][K(\alpha) : K]$ e portanto $[K(\beta) : K] > [K(\alpha) : K]$ uma contradição. $\square$

Teorema 27. *Sejam L um corpo e G um subgrupo de $\text{Aut}(L)$, tal que $|G| = n$ e $F = \Phi(G)$. Então $F \subset L$ é Galoisiana de grau n e $\text{Gal}(L/\Phi(G)) = G$.*

Demonstração. Escreva $G = \{\sigma_1, \dots, \sigma_n\}$, e tome $\beta \in L$. Podemos supor, depois de rearranjar se necessário, que $\{\sigma_1(\beta), \dots, \sigma_n(\beta)\} = \{\sigma_1(\beta), \dots, \sigma_r(\beta)\}$ com $r \leq n$, e $\sigma_i(\beta) \neq \sigma_j(\beta)$ para $i \neq j$. Como G é finito, temos que para todo $\sigma \in G$, $\sigma \circ \sigma_i = \sigma_j$ para algum $j \in \{1, \dots, r\}$, assim $\sigma(\{\sigma_1(\beta), \dots, \sigma_r(\beta)\}) = \{\sigma_1(\beta), \dots, \sigma_r(\beta)\}$

Considere o polinômio $f(x) = \prod_{i=1}^r (x - \sigma_i(\beta))$. E para todo $\sigma \in G$ temos

$$\sigma(f(x)) = \prod_{i=1}^r (x - \sigma\sigma_i(\beta)) = \prod_{i=1}^r (x - \sigma_i(\beta)) = f(x)$$

segue que $f \in \Phi(G)[x]$, uma vez que todo $\sigma \in G$ fixa os coeficiente de f . Como f não possui raízes repetidas, e f se anula em β , temos que o polinômio minimal de β sobre $\Phi(G)$, denotado por $p_{\beta, \Phi(G)}$ também não possui raízes repetidas uma vez $p_{\beta, \Phi(G)}$ divide f , então $[\Phi(G)(\beta) : \Phi(G)] \leq r \leq n$ e como β é arbitrário, segue que $\Phi(G) \subset L$ é separável. Assim, pelo Lema 26, existe $\alpha \in L$ tal que $L = \Phi(G)(\alpha)$ e $[L : \Phi(G)] \leq n$. Como todo automorfismo de $\Phi(G)(\alpha)$ está unicamente determinado pelo seu valor em α pela Proposição 14 segue que $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ para todo $i \neq j$. Assim $f(x) = \prod_{i=1}^n (x - \sigma_i(\alpha))$ possui grau n e $[L : \Phi(G)] \leq n$ segue que f é o polinômio minimal de α , e assim L é corpo de decomposição para f e $[L : \Phi(G)] = n = |G|$. Como $G \subset \text{Gal}(L/\Phi(G))$ e pelo Teorema 19 temos que $[L : \Phi(G)] = |\text{Gal}(L/\Phi(G))|$, segue que $G = \text{Gal}(L/\Phi(G))$. $\square$

Estamos agora em posição de provar nosso resultado principal destas notas.

Teorema 28 (Fundamental da Teoria de Galois). *Sejam $K \subset L$ uma extensão de Galois. Então para todo corpo intermediário na extensão $K \subset F \subset L$ temos que $\Phi(\Gamma(F)) = F$ e que para todo subgrupo $H \leq \text{Gal}(L/K)$ temos $\Gamma(\Phi(H)) = H$.*

Demonstração. Seja $H \leq \text{Gal}(L/K)$ temos que $K \subset \Phi(H) \subset L$ é uma torre de extensões de corpos, e por definição, temos

$$\Gamma(\Phi(H)) := \{\alpha \in \text{Aut}(L); \alpha(a) = a \forall a \in \Phi(H)\} = \text{Gal}(L/\Phi(H))$$

e pelo teorema anterior temos que $\text{Gal}(L/\Phi(H)) = H$. Portanto $\Gamma(\Phi(H)) = H$.

Seja $K \subset F \subset L$ um torre de extensão de corpos. Como $K \subset L$ é de

Galois, segue que $F \subset L$ é de Galois, assim pelo Teorema 19, temos que

$$[L : F] = |\text{Gal}(L/F)| = |\Gamma(F)|$$

Pela Proposição 24, temos que $F \subseteq \Phi(\Gamma(F)) \subset L$; Logo pelo teorema das torres de extensões segue que

$$[L : F] = [L : \Phi(\Gamma(F))][\Phi(\Gamma(F)) : F]$$

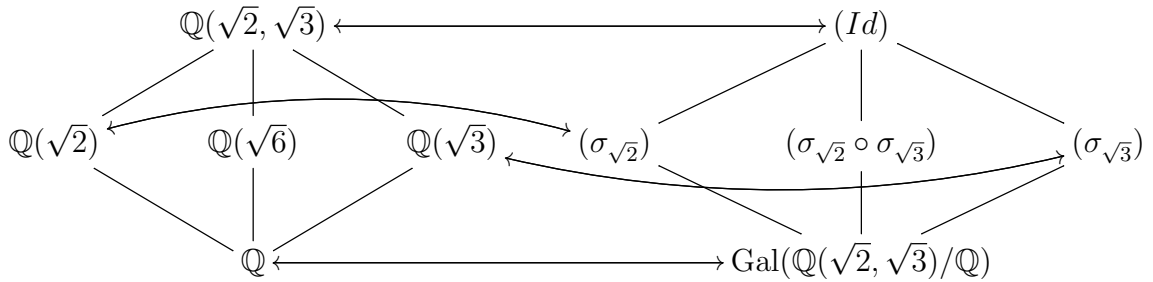
Como $[L : \Phi(\Gamma(F))] = |\Gamma(F)|$, temos que $[\Phi(\Gamma(F)) : F] = 1$ e portanto $\Phi(\Gamma(F)) = F$. $\square$

Temos o seguinte corolário.

Corolário 29. *Seja $K \subset L$ um extensão de Galois. Então existe uma bijeção entre:*

$$\begin{array}{ccc} \{\text{Corpos intermediários de } K \subset L\} & \rightleftharpoons & \{\text{Subgrupos de } \text{Gal}(L/K) \subset L\} \\ F & \mapsto & \Gamma(F) \\ \Phi(H) & \longleftarrow & H \end{array}$$

Exemplo 7. De posse do corolário anterior, podemos calcular todas os corpos intermediários em uma extensão. Por exemplo, considere a extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$. Vemos do diagrama a seguir que os únicos corpos entre $\mathbb{Q}$ e $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ são $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ e $\mathbb{Q}(\sqrt{6})$.



O diagrama da esquerda acima é conhecido como reticulado da extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$, e o da direita o reticulado do grupo $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$.

Exercícios

1. Seja K um corpo e $f \in K[x]$. Prove que f é separável se, e somente se $\text{mdc}(f, f') = 1$;
2. Seja $F|K$ uma extensão de corpos. Prove que se $[F : K] = 2$ então $F|K$ é normal.
3. Sejam F um corpo de característica positiva p e $a \in F$ e f seu polinômio mínimo, e $K = F[a]$. Então f é separável se, e somente se, $K = F[a^p]$.
4. Prove que $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$ é normal.
5. Prove que $\mathbb{Q}(\sqrt{2}(1+i))|\mathbb{Q}$ não é normal.
6. Conclua que se $F|K|L$ é uma torre de extensões, então $F|L$ pode não ser normal mesmo que $F|K$ e $K|L$ sejam normais.
7. Prove que o grupo de Galois de $x^4 - 5$ sobre $\mathbb{Q}$ é isomorfo à D_4 .
8. Prove que o grupo de Galois de $(x^2 - 3)(x^2 + 1)(x^3 - 6)$ sobre $\mathbb{Q}$ é isomorfo a $S_3 \times \mathbb{Z}_2$. (Sugestão: Use o Corolário ??).
9. Calcule todos os corpos intermediários da extensão do corpo de decomposição do polinômio $x^4 - 5$ sobre $\mathbb{Q}$, bem como seu reticulado.
10. Spoiler: Veremos como calcular muitos mais exemplos de grupos de Galois de polinômios com as técnicas que aprenderemos na próxima semana.
11. O exercícios que deverão ser entregues dessa lista são: 6 e 7.