TEORIA DE GALOIS — NOTAS DE CURSO

NIVALDO MEDEIROS

Resumo. Estas são notas para o curso de Álgebra III, bacharelado em Matemática, da Universidade Federal Fluminense. São uma introdução, algo sucinta, da teoria básica de extensões de corpos e da correspondência de Galois, ênfase em extensões finitas, que formam o núcleo da segunda parte do curso. Procurei escrevê-las em seções curtas, de até três páginas, que correspondem aproximadamente a cada uma das aulas. Estão em elaboração e pedem sua compreensão, paciência.

Quaisquer observações, considerações, recomendações, sugestões, correções (tradução: estou realmente pedindo ajuda!) são muito bem-vindas. Para contribuir ou encontrar versões mais recentes, dê uma espiada em

www.professores.uff.br/nmedeiros

24 março 2016
N.

≈≈

Sumário

Anéis são comutativos, com unidade e exigimos $1 \neq 0$. O anel dos inteiros módulo n é denotado por $\mathbb{Z}_n$. Letras gregas $(\sigma, \tau, \rho, \dots)$ indicam homomorfismos. Um homomorfismo de anéis $\sigma\colon A \to B$, por definição, satisfaz: $\sigma(u+v) = \sigma(u) + \sigma(v)$, $\sigma(u\cdot v) = \sigma(u)\cdot\sigma(v)$ e $\sigma(1_A) = 1_B$.

Em geral, k, E, F denotam corpos; elementos de um corpo serão denotados por u, v, w. Corpos com um número finito ℓ de elementos são denotados por $\mathbb{F}_\ell$. Até a Seção 11 apenas subcorpos dos números complexos são considerados. A palavra: simplicidade.

Escrevo $|S|$ para indicar a cardinalidade do conjunto S.

Para grupos, D_n é o grupo diedral das simetrias de um polígono regular de n lados, e portanto possui $2n$ elementos; C_n é o grupo cíclico de ordem n.

Em anéis de polinômios, as indeterminadas são sempre denotadas por x, x_1, x_2, etc, em letras minúsculas, como por exemplo em $k[x]$ e $k[x_1, \dots, x_n]$.

Não utilizo "$\supset$" para indicar inclusões estritas e logo $F \supset k$ permite que F seja eventualmente igual a k. Idem para "$\subset$" .

Primeira Parte

1. O começo

Nestas notas tratamos do problema de encontrar raízes de polinômios. Para iniciar a conversa, vamos pensar apenas em polinômios cujos coeficientes são números reais.

Em primeiro lugar, consideramos a questão da *existência* de raízes. Tendo resolvido isso, a pergunta seguinte é: como *determiná-las*?

A primeira questão tem uma resposta satisfatória, cuja primeira demonstração foi assunto da tese de doutorado de Gauss:

Teorema Fundamental da Álgebra. *Todo polinômio não-constante com coeficientes complexos possui uma raiz nos números complexos.*

Passamos então à questão seguinte: gostaríamos de uma fórmula ou, pelo menos, um algoritmo para encontrar essas raízes. Embora não seja possível determiná-las exatamente para um polinômio escolhido ao sabor do acaso, bons algoritmos existem e hoje em dia temos bons computadores que rapidamente nos fornecem boas *aproximações*, com precisão a nosso bel prazer; mas este é tema mais afim da Análise Numérica do que da Álgebra.

Nossa busca aqui é em outra direção: procuramos fórmulas exatas. Tais fórmulas existem para polinômios de grau pequeno e são bem conhecidas. Façamos um passeio breve.

1.1. **Equações lineares e quadráticas.** Começamos com polinômios lineares. Não há muito a dizer aqui: uma equação

$$ax + b = 0 \qquad (a \neq 0)$$

possui apenas uma solução, a saber, $x = -b/a$.

Os babilônios possuíam métodos para resolver algumas equações quadráticas já em 1600 a.C., assunto que hoje é tema de longas listas de exercícios no ensino médio... Procuramos resolver

$$ax^2 + bx + c = 0 \qquad (a \neq 0). \tag{1}$$

Completamos o quadrado ou, de maneira equivalente, perfazemos a substituição $x = y - b/2a$, obtendo

$$a(y - \frac{b}{2a})^2 + b(y - \frac{b}{2a}) + c = ay^2 - by + \frac{b^2}{4a} + by - \frac{b^2}{2a} + c = ay^2 - \frac{b^2}{4a} + c$$

ou seja, para resolvermos a equação (1) basta resolvermos

$$ay^2 - \frac{b^2}{4a} + c = 0$$

e isso, espero que estejamos de acordo, é algo que sabemos fazer: as soluções são $y = \pm\frac{\sqrt{b^2-4ac}}{2a}$. Substituindo agora o valor de x, reobtemos a familiar

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{2}$$

Eis a nossa *fórmula*. Em retrospectiva, o que fizemos foi transmutar (1) em uma equação mais simples, da forma $y^2 - u = 0$, que declaramos saber resolver. Esta é a estratégia que seguiremos adiante.

1.2. **Equações cúbicas.** Métodos para resolver equações cúbicas são, quando comparadas ao caso quadrático, recentes. Fórmulas remontam a Scipione del Ferro, Niccolo Fontana (Tartaglia), Cardano, em versões que datam do séc. XVI. Consideramos agora

$$ax^3 + bx^2 + cx + d = 0 \qquad (a \neq 0). \tag{3}$$

Tome $x = y - b/3a$. Como exercício: esta substituição elimina o termo de grau 2; somos levados a $ay^3 + ry + s = 0$. Dividindo por a, chegamos a

$$y^3 + py + q = 0 \tag{4}$$

com $p = r/a$ e $q = s/a$. Podemos supor p, q ambos não-nulos, pois caso contrário a solução já está em nosso alcance.

Para resolver (4), escrevemos uma raiz como uma soma

$$y = u + v \tag{5}$$

com u, v ambos não-nulos. Não há nenhum mal nisso, mas não parece haver bem algum... Seja como for, substituindo em (4),

$$\begin{aligned}&(u+v)^3 + p(u+v) + q\\ &= u^3 + v^3 + q + (3uv + p)(u+v)\end{aligned}$$

e logo para encontrar uma raiz é *suficiente* que

$$\begin{cases} u^3 + v^3 = -q \\ 3uv = -p \end{cases} \tag{6}$$

e, passe de mágica, temos um sistema que podemos resolver. Da segunda equação obtemos $v = -p/3u$ e substituindo na primeira,

$$u^3 - \frac{p^3}{27u^3} + q = 0$$

ou equivalentemente

$$u^6 + qu^3 - \frac{p^3}{27} = 0.$$

Tomando $z = u^3$, vem

$$z^2 + qz - \frac{p^3}{27} = 0$$

uma equação quadrática, com a qual já sabemos lidar: $z = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$. Escolhendo

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \qquad \text{vem de (6) que} \qquad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Para obter as outras soluções, tomamos uma raiz cúbica da unidade, o número complexo

$$\omega = e^{2\pi i/3} = \cos(2\pi/3) + i\,\mathrm{sen}(2\pi/3)$$

que satisfaz $\omega^3 = 1$. Note que $\omega \notin \mathbb{R}$. Agora convido você a verificar que se se o par (u, v) é uma solução de (6), então os pares $(\omega u, \omega^2 v)$ e $(\omega^2 u, \omega v)$ também são soluções de (6). Seguem daí as expressões para as raízes de (4):

$$\begin{aligned} y_1 &= u + v \\ y_2 &= \omega u + \omega^2 v \\ y_3 &= \omega^2 u + \omega v \end{aligned} \tag{7}$$

Como todo polinômio real de grau ímpar tem uma raiz real, vem que se $p, q \in \mathbb{R}$, então pelo menos uma destas três raízes sempre é um número real.

A expressão para as raízes de $x^3 + px + q = 0$:

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \tag{8}$$

é uma fonte de surpresas. Por exemplo

$$f = x^3 + 3x - 14$$

tem 2 como raiz e logo $f = (x-2)(x^2+2x+7)$. As outras raízes são $-1 \pm i\sqrt{6}$, que não são números reais. Assim, segue de (8) que

$$\sqrt[3]{7 + \sqrt{50}} + \sqrt[3]{7 - \sqrt{50}} = 2 \tag{9}$$

que é sempre meio desconcertante à primeira vista. E para os que gostam desse tipo de coisas, identidades parecidas em grau superior podem ser obtidas de maneira similar; por exemplo,

$$\sqrt[5]{712 + \sqrt{506945}} + \sqrt[5]{712 - \sqrt{506945}} = 4.$$

1.3. **Equações de grau superior.** Fórmulas para raízes de equações de grau 4 foram descobertas não muito depois da solução da cúbica, e são devidas a Ferrari, Descartes, Euler, Lagrange, entre outros. Como é de se esperar, são um pouco mais complicadas, mas tem uma característica em comum com as fórmulas para graus 2 e 3: as raízes são descritas em termos de *radicais* aplicados aos coeficientes. Convido você a dar uma olhada nas notas de aula da profa. Maria Lúcia Villela [Vilella] aqui da UFF ou em [Stillwell94].

Naturalmente, o sucesso levou os matemáticos a buscarem soluções similares para as equações de grau 5. Lagrange tinha um método que unificava a obtenção de todas as fórmulas para grau ≤ 4, mas seu método não produzia resultados para as quínticas. Instalou-se a dúvida: tais fórmulas para equações de grau 5 de fato existem?

Ruffini fez tentativas entre 1799 e 1813, obtendo avanços, mas sem sucesso; e Abel publicou um artigo com a primeira demonstração da impossibilidade em 1824, resultado por

vezes referido como o *teorema de Abel–Ruffini*. Entretanto a teoria definitiva foi estabelecida por Évariste Galois (1811–1832), publicada postumamente em 1846. A problema, dito de maneira precisa, é o seguinte: dada uma equação polinomial

$$a_r x^r + \cdots + a_1 x + a_0 = 0$$

como determinar se é possível encontrar uma expressão para as raízes que envolvam somente as operações $+, -, \times, \div, \sqrt[\star]{\cdot}$ aplicadas sucessivamente aos coeficientes? Quando isto acontece, dizemos que o polinômio é *solúvel por radicais*. Para equações quadráticas, cúbicas e quárticas isto sempre ocorre, mas não em geral!

A compreensão das técnicas para demonstrar isto é o assunto do nosso curso: para cada polinômio sobre o corpo k associa-se um grupo finito, o seu *grupo de Galois*. O teorema de Galois é: *um polinômio é solúvel por radicais se e somente se seu grupo de Galois possui uma propriedade especial* — o nome técnico é *solúvel*. Verificar se dado grupo é solúvel ou não, é relativamente simples.

Um exemplo concreto. O polinômio $x^5 - 4x + 2$, de grau 5, não é solúvel por radicais: não existe uma fórmula para expressar suas raízes utilizando apenas as operações aritméticas elementares e raízes $\star$-ésimas aplicadas aos coeficientes. Veja o Exemplo 10.7.

2. Permutar é preciso

2.1. **Newton em simétricos.** Nosso problema é buscar expressões para raízes de um polinômio em termos dos seus coeficientes. Caminhamos aqui no sentido contrário: dadas as raízes, o que podemos dizer sobre os coeficientes?

Sejam $u_1, \ldots, u_n$ indeterminadas sobre um corpo k. Consideramos o *polinômio geral*

$$f = (x - u_1)(x - u_2)\cdots(x - u_n)$$

onde x é uma outra indeterminada sobre k. Expandindo,

$$f = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^j s_j x^{n-j} + \cdots + (-1)^n s_n$$

vem que os coeficientes de f são dados por:

$$\begin{aligned}
s_1 &= u_1 + \cdots + u_n \\
s_2 &= \sum_{i<j} u_i u_j = u_1u_2 + u_1u_3 + \cdots + u_{n-1}u_n \\
s_3 &= \sum_{i<j<k} u_i u_j u_k \qquad\qquad \ldots \\
s_r &= \sum_{i_1<\cdots<i_r} u_{i_1}\cdots u_{i_r} \qquad\qquad \ldots \\
s_n &= u_1 \cdots u_n
\end{aligned} \tag{10}$$

expressões que de fato tem uma forma muito particular: se fazemos qualquer permutação das variáveis $u_1, \ldots, u_n$, estes polinômios não se alteram.

Um polinômio f em $k[u_1, \ldots, u_n]$ é *simétrico* se $f(u_1, \ldots, u_n) = f(u_{\sigma(1)}, \ldots, u_{\sigma(n)})$ para qualquer permutação σ em S_n. Dizendo de outra forma, os polinômios simétricos são os polinômios *invariantes* pela ação do grupo de permutações S_n.

Os polinômios $s_1, \ldots, s_n$ são os exemplos fundamentais, e são denominados *simétricos elementares*. Outros exemplos:

$$a^2 + b^2 + c^2, \quad 4a^3 + 4b^3 + 4c^3 + 7ab + 7ac + 7bc + 12abc$$

são simétricos em a, b, c.

Teorema 2.1 (Newton)**.** *Todo polinômio simétrico* $p(u_1, \ldots, u_n)$ *pode ser escrito como um polinômio nos polinômios simétricos elementares* $s_i = s_i(u_1, \ldots, u_n)$.

De maneira precisa: Seja k *um corpo. Dado um polinômio simétrico* $p \in k[u_1, \ldots, u_n]$*, existe um único polinômio* $h \in k[t_1, \ldots, t_n]$ *tal que* $p = h(s_1, \ldots, s_n)$.

Demonstração. [BMST10] Definimos uma relação de ordem total nos polinômios simétricos em n variáveis. Primeiro, comparamos monômios. Escrevemos

$$a u_1^{e_1} \cdots u_n^{e_n} \succ b u_1^{f_1} \cdots u_n^{f_n}$$

se

(1) $e_1 + \cdots + e_n > f_1 + \cdots + f_n$;
(2) ou $e_1 + \cdots + e_n = f_1 + \cdots + f_n$ e $(e_1, \ldots, e_n)$ é lexicograficamente maior que $(f_1, \ldots, f_n)$, isto é, existe i tal que $e_1 = f_1, \ldots, e_{i-1} = f_{i-1}$ mas $e_i > f_i$.

Para polinômios $p, q \in k[u_1, \ldots, u_n]$, escrevemos $p \succ q$ se o maior monômio de p (seu *termo inicial*) é maior do que o maior monômio de q. Note que em um polinômio simétrico, seu termo inicial $a u_1^{e_1} \cdots u_n^{e_n}$ é tal que $e_1 \geq e_2 \geq \cdots \geq e_n$.

A demonstração do teorema é por indução com relação à ordem total acima definida, sendo a base da indução constituída pelos polinômios constantes (que são simétricos), para os quais o resultado é trivialmente verdadeiro. Agora, dado um polinômio simétrico p com termo inicial $a u_1^{e_1} \cdots u_n^{e_n}$, considere o polinômio simétrico

$$a s_1^{e_1 - e_2} s_2^{e_2 - e_3} \cdots s_{n-1}^{e_{n-1} - e_n} s_n^{e_n}$$

cujo termo inicial é

$$a u_1^{e_1 - e_2} (u_1 u_2)^{e_2 - e_3} \cdots (u_1 u_2 \cdots u_{n-1})^{e_{n-1} - e_n} (u_1 u_2 \cdots u_n)^{e_n} = a u_1^{e_1} \cdots u_n^{e_n}$$

ou seja, o mesmo de p. Assim

$$p \succ p - a s_1^{e_1 - e_2} \cdots s_{n-1}^{e_{n-1} - e_n} s_n^{e_n}.$$

Como o polinômio $p - a s_1^{e_1 - e_2} \cdots s_{n-1}^{e_{n-1} - e_n} s_n^{e_n}$ é simétrico, pela hipótese de indução ele pode ser escrito em função de polinômios simétricos elementares. Logo o mesmo vale para p, como desejado. □

Eis alguns exemplos:

$$u_1^2 + \cdots + u_n^2 = s_1 - 2s_2$$
$$u_1^3 + \cdots + u_n^3 = s_1^3 - 3s_1s_2 + 3s_3$$
$$u_1^4 + \cdots + u_n^4 = s_1^4 - 4s_1^2s_2 + 4s_1s_3 + 2s_2^2 - 4s_4.$$

O teorema de Newton é o pilar sobre o qual residem as aplicações da teoria dos grupos (permutações) no estudo algébrico das raízes de polinômios.

Vejamos como funciona. Suponha que $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ é um polinômio com coeficientes em $\mathbb{Q}$ e que os u_i's não são indeterminadas, mas sim as raízes complexas do polinômio f. Então os coeficientes de f são dados pelos polinômios simétricos elementares avaliados nas raízes: $a_j = (-1)^j s_j(u_1, \ldots, u_n)$; ou seja, são *sempre* obtidos através das equações (10). Isto para equações quadráticas

$$f = x^2 - (u_1 + u_2)x + u_1u_2$$

não é nada além da frase: *o termo linear é a soma das raízes com sinal trocado e o termo constante é produto das raízes.*

A principal observação é que, pelo Teorema de Newton, *qualquer expressão simétrica* nas raízes $u_1, \ldots, u_n$ é expressa em termos dos coeficientes de f, *mesmo que não saibamos explicitamente quais são as raízes*! E podemos usar isto para determinar relações, isto é, equações envolvendo as raízes; se as temos em número suficiente, podemos resolver e daí escrever as raízes em termos dos coeficientes. Se o nome do jogo é simetria, o nome do jogador é: Lagrange.

2.2. **Discriminantes.** Nossa próxima obsessão é procurar por expressões simétricas nas raízes. Entre muitas, há uma particularmente notável, o *discriminante*: se $u_1, \ldots, u_n$ são as raízes de $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x]$, observe que

$$\prod_{i<j}(u_i - u_j)$$

é invariante por *permutações pares*, mas tem seu sinal trocado por uma permutação ímpar. Logo seu quadrado,

$$\operatorname{disc} f := \prod_{i<j}(u_i - u_j)^2$$

é invariante por qualquer permutação e portanto, pelo Teorema de Newton, pertence ao corpo k. Uma conexão importante é que o discriminante pode ser obtido via a *matriz de Vandermonde*: $\operatorname{disc} f = \det(V(u_1, \ldots, u_n))^2$, onde

$$V(u_1, \ldots, u_n) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ u_1 & u_2 & \cdots & u_n \\ u_1^2 & u_2^2 & \cdots & u_n^2 \\ \vdots & & & \vdots \\ u_1^{n-1} & u_2^{n-1} & \cdots & u_n^{n-1} \end{pmatrix}$$

Vejamos o singelo caso das equações quadráticas. Tome $f = x^2 + bx + c$. Então

$$\Delta = \operatorname{disc} f = (u_1 - u_2)^2 = (u_1 + u_2)^2 - 4u_1u_2 = b^2 - 4c.$$

Eis que temos um sistema linear em função dos coeficientes de f

$$\begin{aligned} u_1 + u_2 &= -b \\ u_1 - u_2 &= \sqrt{\Delta} \end{aligned}$$

e ao resolvê-lo obtemos, mais uma vez,

$$u_1, u_2 = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Exercício 2.2. Para cúbicas:

$$\operatorname{disc}(x^3 + px + q) = -4p^3 - 27q^2 \tag{11}$$

Compare com as expressões que aparecem na fórmula de Cardano (8).

2.3. **Lagrange em cúbicas.** Considerar apenas o discriminante não é suficiente para encontrar fórmulas para raízes em grau superior a dois. O método de Lagrange (que foi expandido amplamente por Galois) consiste em encontrar mais expressões simétricas para as raízes, na tentativa de "capturar suas simetrias".

Considere $f = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ e sejam $u_1, u_2, u_3 \in \mathbb{C}$ suas raízes. Tome $\omega = e^{2\pi i/3} = -1/2 + \sqrt{3}i/2$ uma raiz cúbica da unidade. Lagrange nos convida a considerar

$$u = (u_1 + \omega u_2 + \omega^2 u_3)^3.$$

Como $\omega^3 = 1$, segue que este elemento é invariante pelas permutações pares de S_3, mas as permutações ímpares o levam a

$$v = (u_1 + \omega^2 u_2 + \omega u_3)^3$$

Assim, embora u e v não sejam invariantes separadamente, qualquer expressão simétrica envolvendo ambos o é. Em particular, $u + v$ e $u \cdot v$ são invariantes e, pelo Teorema de Newton, podem ser escritos em termos dos coeficientes a, b, c. Com algum trabalho (a relação $1 + \omega + \omega^2 = 0$ pode ajudar) encontramos

$$\begin{aligned} u + v &= -2a^3 + 9ab - 27c \\ u \cdot v &= a^6 - 9a^4b + 27a^2b^2 - 27b^3. \end{aligned}$$

Definimos um polinômio auxiliar

$$r(x) = x^2 - (u + v)x + u \cdot v$$

conhecido como a *resolvente de Lagrange*; seus coeficientes pertencem *ao mesmo corpo* dos coeficientes de f, são números racionais. Seu grau é menor do que o de f, e portanto sabemos resolvê-lo, encontrando os valores de u e v.

Finalmente, para obter as raízes, acrescentamos a equação linear correspondente ao coeficiente de x^2 às duas que já possuímos e obtemos o sistema

$$\begin{aligned} u_1 + u_2 + u_3 &= -a \\ u_1 + \omega u_2 + \omega^2 u_3 &= \sqrt[3]{u} \\ u_1 + \omega^2 u_2 + \omega u_3 &= \sqrt[3]{v} \end{aligned}$$

Resolvendo, expressamos as raízes em termos de radicais nos coeficientes do polinômio f. Notável!

Exercício 2.3. Tomando $a = 0, b = p$ e $c = q$, encontre u e v, resolva o sistema acima e recupere as soluções em (7), obtidas pelo método de Cardano.

Exercício 2.4. Se f é uma cúbica e r é sua resolvente, então $-27\,\mathrm{disc}(f) = \mathrm{disc}(r)$.

3. EXTENSÕES DE CORPOS

3.1. **Corpos.** Um *corpo* é um anel onde todo elemento não-nulo é invertível. Os exemplos mais familiares:

- O conjunto dos números racionais $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$;
- Os números reais $\mathbb{R}$;
- Os números complexos $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$;
- Para $p \in \mathbb{Z}$ primo, o anel $\mathbb{Z}_p$ dos inteiros módulo p.

Uma *extensão de corpos* consiste simplesmente de dois corpos k e F, onde k é um subcorpo de F. Escrevemos $F \supset k$. O *corpo de base* de extensão é o corpo k. São exemplos: $\mathbb{R} \supset \mathbb{Q}$, $\mathbb{C} \supset \mathbb{R}$, $\mathbb{C} \supset \mathbb{Q}$.

Estamos interessados no comportamento *relativo* e não absoluto: estudamos propriedades do par F, k e não somente de um dos corpos.

Exercício 3.1. Mostre que o conjunto

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

é um corpo que contém $\mathbb{Q}$.

3.2. **Adjunção.** Dada uma extensão de corpos $F \supset k$, temos um processo para criar corpos intermediários entre k e F: se $S \subset F$ é um subconjunto qualquer, a *adjunção* $k(S)$ é, por definição, o menor subcorpo de F contendo k e S. Quando $S = \{u_1, \ldots, u_n\}$ é um conjunto finito, denotamos $k(S)$ por $k(u_1, \ldots, u_n)$.

O caso mais simples é o da adjunção de um único elemento, que consideramos agora. Tomemos $u \in F$. Pense bem: qualquer corpo contendo k e u deve conter todas as potências de u, bem como combinações lineares envolvendo essas potências digamos: $a_n u^n + \cdots + a_1 u + a_0$, com os a_i's em k; ou seja, polinômios de $k[x]$ avaliados em u. Além disso, todas as frações de elementos desse tipo deve estar presentes, um vez que um corpo contém inversos de elementos não-nulos. De fato,

$$\left\{ \frac{f(u)}{g(u)} \mid f, g \in k[x],\ g(u) \neq 0 \right\} \tag{12}$$

já forma um corpo, como você está convidado a verificar no exercício abaixo. Este é então $k(u)$, o menor subcorpo de F contendo $k \cup \{u\}$.

Exercício 3.2. Mostre o conjunto definido em (12) é de fato um subcorpo de F. Em seguida, prove que $\mathbb{Q}(\sqrt{2})$ coincide com o corpo definido no primeiro exercício.

O caso de um número finito de elementos é similar:

$$k(u_1, \ldots, u_n) = \left\{ \frac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)} \mid f, g \in k[x_1, \ldots, x_n],\ g(u_1, \ldots, u_n) \neq 0 \right\}. \tag{13}$$

Não há mistério algum em adjunções sucessivas:

Exercício 3.3. Mostre que $k(u, v) = (k(u))(v)$.

Quando S é um conjunto possivelmente infinito, $k(S)$ é ainda conjunto das frações de polinômios avaliados em elementos de S, com uma ressalva: usamos apenas um número finito indeterminadas para cada polinômio, mas permitimos que este número fique arbitrariamentre grande.

Exercício 3.4. Seja $i = \sqrt{-1} \in \mathbb{C}$. Então $\mathbb{C} = \mathbb{R}(i)$ e $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

3.3. **Álgebra Linear.** Seja $F \supset k$ uma extensão de corpos. Evidentemente podemos somar elementos de F e também realizar produtos de elementos de F com elementos de k. Sendo operações dos corpos k e F, elas se comportam decentemente: são comutativas, associativas, possuem elemento neutro, vale a distributividade, etc. Ou seja, F possui a estrutura de espaço vetorial, com o corpo k fazendo o papel dos "escalares".

Sim, é um ponto de vista mais abstrato do que o usual. Os escalares são o corpo de base da extensão e portanto podem variar. Isto, provavelmente, é bem diferente do que você aprendeu no seu primeiro curso de Álgebra Linear, onde os escalares são sempre os números reais.

A boa notícia é essencialmente todos os conceitos e resultados do seu saudoso curso ainda são válidos aqui, sem custo, mesmas demonstrações. São exemplos: independência linear, geradores, bases, dimensão, etc. Entretanto, estes conceitos agora tem que ser tomados relativamente ao corpo de base: assim, falamos de k-independência linear, k-bases, transformações k-lineares, etc.

Este ponto de vista é extremamente útil no caminho que iremos percorrer. De qualquer modo, um aviso: a intuição geométrica tem que ser adaptada.

Exemplo 3.5. O corpo $\mathbb{Q}(\sqrt{2})$ é um $\mathbb{Q}$-espaço vetorial de dimensão dois: os "vetores" 1 e $\sqrt{2}$ formam uma $\mathbb{Q}-$base. De fato, formam um conjunto de geradores, como visto nos Exercícios 3.1 e 3.2; e são linearmente independentes sobre $\mathbb{Q}$, visto que se $a, b \in \mathbb{Q}$ são tais que $a + b\sqrt{2} = 0$, então $a = b = 0$, pois $\sqrt{2}$ não é um número racional. Escrevemos $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$. Para pensar: quanto vale $\dim_{\mathbb{Q}(\sqrt{2})} \mathbb{Q}(\sqrt{2})$?

É uma situação curiosa, não? Ambos os corpos $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}$ estão contidos na reta $\mathbb{R}$. Um desenho ingênuo seria: um monte de pontos desconexos contidos na reta real... E pode piorar: os corpos k e F podem ter um número finito de elementos.

O *grau* de uma extensão $F \supset k$ é simplesmente a dimensão de F como k-espaço vetorial e a denotamos $[F : k]$. Assim, o grau é a cardinalidade de qualquer k-base de F. Uma extensão é dita *finita* se o seu grau é finito, *infinita* caso contrário.

Exercício 3.6. $[F : k] = 1$ se e somente se $F = k$.

Exercício 3.7. Qual a dimensão de $\mathbb{R}$ como espaço vetorial sobre $\mathbb{Q}$?

3.4. **O grau em torres de extensões.** Seja $F \supset k$ uma extensão de corpos. Seja E um corpo intermediário, $F \supset E \supset k$ (neste caso dizemos que temos uma *torre* de extensões). Como vimos, tanto F quanto E têm uma estrutura de k-espaço vetorial; mas podemos também considerar F como um espaço vetorial tendo E como corpo de escalares. Este tipo de situação é nova, não? Há uma relação entre os graus de todas estas extensões.

Teorema 3.8 (Multiplicatividade do grau)**.** *Dada uma torre* $k \subset E \subset F$*, a extensão* $k \subset F$ *é finita se e somente se as extensões* $k \subset E$ *e* $E \subset F$ *são finitas. Precisamente: se* $u_1, \ldots, u_m$ *é uma base de* E *sobre* k *e* $v_1, \ldots, v_n$ *é uma base de* F *sobre* E*, então* $u_i v_j$*,* $i = 1, \ldots, m, j = 1, \ldots, n$ *é uma base de* F *sobre* k*. Em particular:*

$$[F : k] = [F : E][E : k].$$

Demonstração: Se $F \supset k$ é uma extensão finita, então $E \supset k$ é finita pois E é um subespaço vetorial de F; e $F \supset E$ é também finita, uma vez que E contém k.

Reciprocamente, dado $v \in F$, escreva $v = \sum b_j v_j$, com $b_j \in E$ para cada j. Em seguida, expressamos cada b_j em termos da base de E sobre k, digamos $b_j = \sum_i a_{ij} u_i$ $(a_{ij} \in k)$, e obtemos

$$v = \sum_j (\sum_i a_{ij} u_i) v_j = \sum_{i,j} a_{ij} u_i v_j$$

e portanto os mn elementos $u_i v_j$ geram F como um k-espaço vetorial. Afirmamos que estes elementos são linearmente independentes. De fato, dados $a_{ij} \in k$,

$$\begin{aligned}
0 &= \textstyle\sum_{i,j} a_{ij} u_i v_j \iff \\
0 &= \textstyle\sum_j (\sum_i a_{ij} u_i) v_j \iff \\
0 &= \textstyle\sum_i a_{ij} u_i, \quad \text{para } j = 1, \ldots, n \iff \\
0 &= a_{ij}, \quad \text{para } j = 1, \ldots, n,\ i = 1, \ldots, m.
\end{aligned}$$

□

É sugestivo utilizar diagramas para representar extensões de corpos. Assim, na situação do enunciado do teorema:

$$\begin{array}{c} F \\ \Big| {\scriptstyle n} \\ E \\ \Big| {\scriptstyle m} \\ k \end{array}$$

e o grau de $F \supset k$ é $m \cdot n$.

4. EXTENSÕES ALGÉBRICAS

Seja $F \supset k$ uma extensão de corpos. Um elemento $u \in F$ é *algébrico sobre* k se existe um polinômio $f \in k[x]$ não-nulo que tenha u como raiz. Se não é algébrico, u é chamado *transcendente* sobre k. Sem dúvida o caso de maior interesse é $k = \mathbb{Q}$, quando falamos simplesmente de *números algébricos* ou *números transcendentes*.

Assim, $\sqrt{2}$, $\sqrt[3]{5}$, i e $e^{2\pi i/3}$ são números algébricos, pois são raízes de x^2-2, x^3-5, x^2+1 e x^3-1, respectivamente. Outro exemplo: $\sqrt[4]{2}$ é algébrico sobre $\mathbb{Q}(\sqrt{2})$, pois é raiz de $x^2-\sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$. Por fim, π é algébrico sobre $\mathbb{R}$; e é também algébrico sobre $\mathbb{Q}(\pi)$, pois é raiz do polinômio $x-\pi$.

Seja $u \in F$ algébrico sobre k. Dentre os polinômios não-nulos em $k[x]$ que tem u com raiz, há aqueles cujo grau é mínimo. Se p é um destes, então multiplicando-o por constante adequada obtemos um polinômio *mônico* (isto é, o coeficiente do seu termo de mais alto grau é 1). Estas propriedades determinam unicamente p, como veremos a seguir; ele é chamado o *polinômio minimal* de u sobre k, simbolizado $p_{u,k}$.

Exemplo 4.1.

(1) Uma das raízes do polinômio x^2-2 é $\sqrt{2}$. Como $\sqrt{2} \notin \mathbb{Q}$, ele é de fato o polinômio minimal.
(2) O polinômio $f = x^3-5$ tem $u = \sqrt[3]{5}$ como raiz e é, de fato, o seu polinômio minimal sobre os racionais; com efeito, seja $p = p_{u,\mathbb{Q}}$. Realizamos a divisão euclidiana e obtemos $f = qp + r$ com $r = 0$ ou $\operatorname{grau} r < \operatorname{grau} f$. Como $f(u) = p(u) = 0$, vem que $r(u) = 0$ e logo devemos ter $r = 0$, pela minimalidade do grau de p. Sendo f irredutível em $\mathbb{Q}[x]$ (Eisenstein), vem que q é uma constante. Como f e p são mônicos, $q = 1$, ou seja, $p = f$.
(3) Os polinômios minimais de i e $e^{2\pi i/3}$ sobre os racionais são, respectivamente, x^2+1 e x^2+x+1.
(4) O polinômio minimal de $\sqrt[4]{2}$ sobre $\mathbb{Q}$ é x^4-2; já sobre $\mathbb{Q}(\sqrt{2})$ é $x^2-\sqrt{2}$.

Exercício 4.2. Prove que um polinômio minimal $p_{u,k}$ é irredutível em $k[x]$.

Teorema 4.3. *Seja $F \supset k$ uma extensão de corpos, $u \in F$ algébrico sobre k e $p \in k[x]$ seu polinômio minimal. Então:*

(a) *Dado $f \in k[x]$, então $f(u) = 0$ se e somente se p divide f. Em particular, p é o único polinômio mônico irredutível em $k[x]$ que tem u como raiz.*
(b) *Seja n o grau de p. Então $1, u, u^2, \ldots, u^{n-1}$ é uma base de $k(u)$ sobre k.*

Demonstração: Provemos o item (a). Realizamos a divisão euclidiana de f por p e encontramos polinômios $q, r \in k[x]$ tais que

$$f = qp + r$$

onde $r = 0$ ou $\operatorname{grau} r < \operatorname{grau} p$. Como $f(u) = p(u) = 0$, temos $r(u) = 0$ e logo devemos ter $r = 0$, pela minimalidade do grau de p. Assim p divide f. O item (a) agora se segue do Exercício 4.2.

Para o item (b), tome uma combinação linear $a_0 + a_1u + \cdots + a_{n-1}u^{n-1} = 0$ sobre k. Então todos os a_i's são nulos, pois caso contrário $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ seria um polinômio de grau menor que do que o de p e que anula u. Portanto $1, u, \ldots, u^{n-1}$ é um conjunto linearmente independente sobre k.

Mostrar que eles formam um conjunto de geradores requer um pouco mais de trabalho. Um elemento v em $k(u)$ se escreve como $f(u)/g(u)$, com $f, g \in k[x]$ e $g(u) \neq 0$. Do item (a) vem que p não divide g e logo $\mathrm{mdc}(p, g) = 1$, pois p é irredutível. Assim, existem $s, t \in k[x]$ tais que

$$sp + tg = 1$$

e como $p(u) = 0$, temos que $t(u) = 1/g(u)$. Logo $h = ft$ é um polinômio com coeficientes em k e tal que $v = h(u)$. Dividindo h por p, obtemos $h = qp + r$, onde $r = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in k[x]$. Mais uma vez, como $p(u) = 0$, obtemos $v = r(u)$ o que conclui a demonstração. □

Do teorema: se um polinômio mônico e irredutível anula u, então ele é o seu polinômio minimal. Se temos a boa fortuna de utilizar algum critério indireto para determinar a irredutibilidade (Eisenstein, por exemplo), determinamos então o polinômio minimal e daí o grau da extensão envolvida. Além disso, para elementos algébricos sobre k não necessitamos de frações para descrever o corpo $k(u)$:

Exercício 4.4. Se u é algébrico sobre k, então $k(u) = k[u]$ onde $k[u] := \{f(u) \mid f \in k[x]\}$. O que você tem a dizer sobre a recíproca?

Uma extensão $F \supset k$ é *algébrica* se todo elemento de F é algébrico sobre k.

Proposição 4.5. *Toda extensão finita é algébrica.*

Demonstração. Suponha $F \supset k$ finita, digamos de grau n. Então, dado $u \in F$, os $n + 1$ elementos $1, u, u^2, \ldots, u^n$ são necessariamente k-linearmente dependentes, ou seja, existem $a_0, \ldots, a_n \in k$ não todos nulos tais que u é raiz do polinômio $a_0 + a_1x + \cdots + a_nx^n \in k[x]$. □

Exercício 4.6. Uma extensão $k(u) \supset k$ é finita se e somente se u é algébrico sobre k.

Exercício 4.7. Uma extensão algébrica é necessariamente finita?

Para motivar o próximo resultado considere a seguinte situação: $\sqrt{2}$ e $\sqrt{3}$ são números algébricos e não é difícil mostrar que $u = \sqrt{2} + \sqrt{3}$ é também um número algébrico. De fato, $u^2 - 5 = 2\sqrt{6}$ e logo $u^4 - 10u^2 + 1 = 0$. É natural perguntar se $x^4 - x^2 + 1$ é o polinômio minimal de u sobre $\mathbb{Q}$.

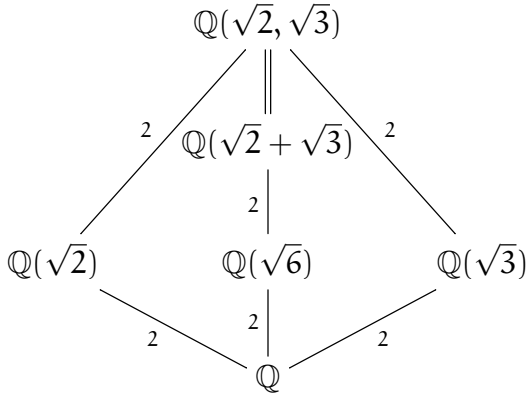
Exercício 4.8. Vamos calcular o grau da extensão $Q(u) \supset \mathbb{Q}$. As ferramentas: multiplicatividade do grau em extensões e o item (b) do Teorema 4.3. Vale a pena acompanhar o argumento via o diagrama abaixo.

(1) Mostre que $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ e logo $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.
(2) Note que temos uma torre de extensões

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Mostre agora que $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}(\sqrt{6})$.

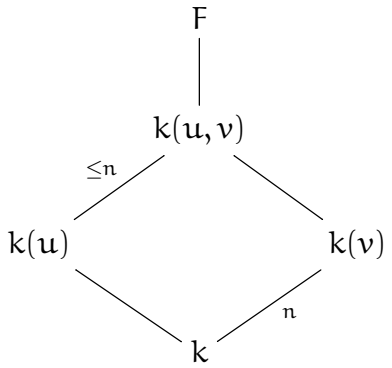
(3) Conclua que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ e daí que $x^4 - 10x^2 + 1$ é o polinômio minimal de $\sqrt{2}+\sqrt{3}$ sobre $\mathbb{Q}$.



Esse foi um exemplo simples. Se você se tentar provar que $\sqrt[57]{75} + \sqrt[75]{57}$ é um número algébrico tentando encontrar o polinômio que o anule, rapidamente se convencerá de que não é um bom negócio. Há uma outra maneira.

Proposição 4.9. *A soma, diferença, produto e quociente de elementos algébricos são elementos algébricos.*

Demonstração: Sejam $u, v \in F$ algébricos sobre k. Pelo Exercício 4.6, as extensões $k(u) \supset k$ e $k(u,v) \supset k(u)$ são finitas; pela multiplicatividade dos graus, $k(u,v) \supset k$ é também uma extensão finita e logo algébrica, pela Proposição 4.5. Portanto, $u \pm v$, $u \cdot v$ e u/v $(v \neq 0)$ são algébricos sobre k, uma vez que pertencem a $k(u,v)$.



□

Exercício 4.10. No diagrama acima: $[k(u,v) : k(u)] \leq [k(v) : k]$.

Vem do legado de Cantor que os números algébricos foram um conjunto enumerável, e portanto são "poucos". Por outro lado, não sabemos muitos exemplos explícitos de números transcendentes. Até 1844 a sua existência era uma questão em aberto, quando Liouville mostrou que números cuja expansão decimal contém cadeias cada vez maiores de

zeros são transcendentes, como por exemplo $\sum_{n=0}^{\infty} 10^{-n!}$. Determinar se um dado número é transcendente ou não é uma questão bem mais difícil. Hermite demonstrou que e é transcendente em 1873, usando métodos analíticos; e Lindermann provou que π é um número transcendente em 1882, baseando-se nas ideias de Hermite. Uma demonstração elegante pode ser encontrada em [Rowen95, Appendix A].

5. EXTENSÕES SEPARÁVEIS

Esta é uma seção curta. Seu objetivo é responder ao seguinte "desafio": como determinar se um polinômio tem raízes repetidas *sem* fatorá-lo?

Tome k um subcorpo de $\mathbb{C}$. Seja $u \in \mathbb{C}$ uma raiz de um polinômio $f \in k[x]$. Da divisão euclidiana vem que $f = (x-u)g$ ou seja, $x-u$ divide f. Dizemos que u é uma raiz *simples* se $(x-u)^2 \nmid f$. Para detectar raízes simples buscamos ajuda do Cálculo.

Escreva $f = a_n x^n + \cdots + a_1 x + a_0$, com os coeficientes em k. Tomando-se a derivada da função definida por f, obtemos um polinômio

$$f' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$$

que ainda tem coeficientes em k. Se $f, g \in k[x]$, então

$$(f+g)' = f' + g' \qquad \text{e} \qquad (f\cdot g)' = f'\cdot g + f\cdot g'.$$

Agora:

Exercício 5.1. u é raiz simples de $f \iff f(u) = 0$ mas $f'(u) \neq 0$.

Por definição, um polinômio $f \in k[x]$ é *separável* se todas as suas raízes são simples, ou seja, não possui raízes "repetidas". De maneira equivalente, se f possui grau n, então f é separável se e somente se f possui n raízes distintas em $\mathbb{C}$. Observe que a noção de separabilidade diz respeito somente ao polinômio em questão e independe do corpo onde ele se encontra; note o contraste com a noção de irredutibilidade.

Usando o critério da derivada, temos uma resposta para a questão do início da seção:

Proposição 5.2. *Seja k um subcorpo de $\mathbb{C}$. Um polinômio $f \in k[x]$ é separável se e somente se* $\operatorname{mdc}(f, f') = 1$. *Em particular, se f é irredutível em $k[x]$, então f é separável.*

Demonstração. A primeira afirmação do enunciado decorre imediatamente do Exercício 5.1, pois se $d = \operatorname{mdc}(f, f') \in k[x]$, então as raízes de d em $\mathbb{C}$ são raízes tanto de f como de f'. Finalmente, se f é irredutível, então f não divide f' já que $\operatorname{grau} f' = \operatorname{grau} f - 1$. □

Um elemento de uma extensão F de um corpo k é *separável* sobre k se seu polinômio mínimo sobre k é separável. A extensão é *separável* se todos seus elementos são separáveis sobre o corpo de base.

Para subcorpos dos complexos toda extensão é separável, em virtude da Proposição 5.2. Isto, porém, não vale para um corpo arbitrário. A palavra-chave aqui é *característica zero*. Veja a seção sobre característica para mais informações.

Exercício 5.3. Se $F \supset k$ é separável e E é um corpo intermediário, então $F \supset E$ e $E \supset k$ são separáveis.

6. EXTENSÕES NORMAIS

Nesta seção estudamos homomorfismos em extensões de corpos que fixam o corpo de base. Este caminho nos leva ao encontro de um tipo particular de extensões, conhecidas como normais, que examinamos com detalhe.

Mais uma vez, consideramos somente subcorpos dos números complexos.

Começamos com um aquecimento:

Exercício 6.1. Seja $\sigma\colon A \to B$ um homomorfismo de anéis. Se A é um corpo, então σ é injetivo.

Seja $F \supset k$ uma extensão de corpos. Tome u um elemento de F e seja f um polinômio não-nulo em $k[x]$ que tenha u como raiz. Seja $\sigma\colon F \to \mathbb{C}$ um homomorfismo com uma propriedade especial: suponha que $\sigma(a) = a$ para todo $a \in k$. Então $\sigma(u)$ é também uma raiz de f. Isto é muito simples: se $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, então

$$\begin{aligned} 0 = f(u) \implies 0 &= \sigma(f(u)) = \sigma(a_n u^n + a_{n-1}u^{n-1} + \cdots + a_0) \\ &= \sigma(a_n)\sigma(u)^n + \sigma(a_{n-1})\sigma(u)^{n-1} + \cdots + \sigma(a_0) \\ &= a_n\sigma(u)^n + a_{n-1}\sigma(u)^{n-1} + \cdots + a_0 \\ &= f(\sigma(u)) \end{aligned} \tag{14}$$

Seja $S \subset \mathbb{C}$ o conjunto das raízes de f. Como todo homomorfismo de corpos é injetor e S é finito, segue que σ induz uma permutação em S. Está aberto o caminho que nos levará ao grupo de Galois. (Incidentalmente, fica justificado porque escolhemos $\mathbb{C}$ como contra-domínio: lá encontramos todas as raízes.)

Sejam F, F' extensões de um corpo k. Um k-*homomorfismo* $\sigma\colon F \to F'$ é um homomorfismo que estende a identidade de k, isto é, $\sigma|_k = \mathrm{id}_k$, isto é, $\sigma(a) = a$ para todo $a \in k$. Representamos essa situação em um diagrama:

$$\begin{array}{ccc} F & \xrightarrow{\sigma} & F' \\ \big| & & \big| \\ k & \xrightarrow{\mathrm{id}} & k \end{array}$$

Dizemos que σ é um k-*endomorfismo* se aplica F em si mesmo, ou seja, $\sigma(F) \subset F$; e um k-*automorfismo* de F é um k-isomorfismo, ou seja, $\sigma(F) = F$.

Os k-automorfismos de F com a operação de composição formam um grupo, que é denotado por $\mathrm{Gal}_k(F)$ ou também $\mathrm{Aut}_k(F)$.

Exercício 6.2. A aplicação $\mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ dada por $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ é um homomorfismo.

Exercício 6.3. Suponha $F = k(u_1, \ldots, u_n)$. Mostre que todo k-homomorfismo fica completamente determinado pela sua ação nos geradores de F. Precisamente: se $\sigma, \sigma'\colon F \to F'$ são k-homomorfismos, e $\sigma(u_i) = \sigma'(u_i)$ para $i = 1, \ldots, n$, então $\sigma = \sigma'$ (ou seja: $\sigma(v) = \sigma'(v), \forall v \in F$). Em particular,

$$\sigma(F) = k(\sigma(u_1), \ldots, \sigma(u_n)).$$

(Sugestão: utilize a descrição da equação (13))

Exercício 6.4. Se k é um subcorpo de $\mathbb{C}$, então $k \supset \mathbb{Q}$ (pois $1 \in k$). E vale também que todo homomorfismo $\sigma\colon k \to \mathbb{C}$ é um $\mathbb{Q}$-homomorfismo (pois $\sigma(1) = 1$).

Para encurtar referências no futuro: os k-*conjugados* de um elemento $u \in F$ são simplesmente as raízes (em $\mathbb{C}$) do seu polinômio minimal sobre k.

A equação (14) tem consequências interessantes. Um k-homomorfismo $F \to \mathbb{C}$ permuta k-conjugados; se todos eles já estão em F, temos uma aplicação de F em si mesmo, ou seja, um endomorfismo.

Definição 6.5. Sejam $f \in k[x]$ um polinômio e $S \subset \mathbb{C}$ o conjunto de todas as raízes de f, isto é, $S = \{u \in \mathbb{C} \mid f(u) = 0\}$. O *corpo de decomposição de* f *sobre* k é o corpo $k(S)$. O *grupo de Galois de* f *sobre* k é o grupo de automorfismos desta extensão: $\mathrm{Gal}_k f := \mathrm{Gal}_k k(S)$.

Uma extensão finita $F \supset k$ é *normal* se F é o corpo de decomposição de algum polinômio não-nulo em $k[x]$.

Exemplo 6.6.

(1) $\mathbb{Q}(\sqrt{2})$ é normal sobre $\mathbb{Q}$.
(2) Se $\omega = e^{2\pi i/n} \in \mathbb{C}$ é uma raiz n-ésima da unidade, então $\mathbb{Q}(\omega)$ é o corpo de decomposição de $x^n - 1$, pois suas raízes são $1, \omega, \ldots, \omega^{n-1}$. Logo $\mathbb{Q}(\omega) \supset \mathbb{Q}$ é normal.
(3) A extensão $\mathbb{C} \supset \mathbb{R}$ é normal.
(4) O corpo $\mathbb{Q}(\sqrt[4]{2}, i)$ é normal sobre $\mathbb{Q}$, pois é o corpo de decomposição de $x^4 - 2$, cujas raízes são $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$.

Exercício 6.7. Toda extensão de grau 2 é normal.

Manfredo Perdigão do Carmo é um excelente professor e geômetra, famoso por palestras memoráveis e frases de efeito. Uma delas:

> *Uma boa definição deve estar grávida de teoremas.*

Assim seja.

Proposição 6.8. *Se uma extensão* $F \supset k$ *é normal, então todo* k*-homomorfismo* $F \to \mathbb{C}$ *é um endomorfismo.*

Demonstração. Escrevemos $F = k(u_1, \ldots, u_r)$ onde os u_i's são as raízes de $f \in k[x]$. Então (14) nos diz que um k-homomorfismo $\sigma\colon F \to \mathbb{C}$ permuta estas raízes e, em particular, $\sigma(u_i) \in F$ para cada $i = 1, \ldots, r$. O resultado agora segue do Exercício 6.3. □

Assim, para extensões normais, homomorfismos que fixam o corpo de base não vão a lugar algum: tudo acontece dentro da própria extensão.

Há mais surpresas. Antes, um resultado auxiliar.

Lema 6.9. *Seja* $F \supset k$ *uma extensão algébrica. Então todo* k*-endomorfismo de* F *é um automorfismo.*

Demonstração: Dado u em F, seja $S = \{\,k\text{-conjugados de } u\,\} \cap F$. Então um k-endomorfismo σ leva o conjunto S em si mesmo; e, sendo injetor e S finito, induz uma bijeção em S. Portanto existe $v \in S$ tal que $\sigma(v) = u$. Concluímos que $F = \sigma(F)$. □

Eis a conclusão do que provamos até aqui, enunciada como um teorema e não como corolário, devido à sua importância.

Teorema 6.10. *Se $F \supset k$ é uma extensão normal, então todo k-homomorfismo $F \to \mathbb{C}$ é de fato um automorfismo.*

7. Extensões, agora de homomorfismos

Seja $F \supset k$ uma extensão algébrica. Buscamos descrever os k-homomorfismos $\sigma\colon F \to \mathbb{C}$, isto é, as extensões da identidade de k ao corpo F. Se $u \in F$, vem da equação (14) que σ leva u em algum dos seus k-conjugados. Nossa questão é sobre existência: dado $v \in \mathbb{C}$ um k-conjugado de u, é possível estender a identidade de modo que $u \mapsto v$?

A resposta é positiva, e podemos generalizar: de fato, podemos estender não somente a identidade, mas qualquer homomorfismo.

Dados $\lambda\colon k \to k'$ e um polinômio $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ em $k[x]$, definimos

$$f^\lambda = \lambda(a_n)x^n + \lambda(a_{n-1})x^{n-1} + \cdots + \lambda(a_0) \in k'[x]$$

que é o polinômio obtido aplicando-se λ aos coeficientes de f. Sejam agora $u \in F$ uma raiz de f, F' uma extensão de k' e $\sigma\colon F \to F'$ e um homomorfismo que estende λ. Então $\sigma(u)$ é uma raiz do polinômio transformado f^λ. A conta é a mesma de (14):

$$\begin{aligned} 0 = \sigma(0) &= \sigma(a_n u^n + a_{n-1}u^{n-1} + \cdots + a_0) \\ &= \sigma(a_n)\sigma(u)^n + \sigma(a_{n-1})\sigma(u)^{n-1} + \cdots + \sigma(a_0) \\ &= f^\lambda(\sigma(u)) \end{aligned} \tag{15}$$

uma vez que $\sigma(a) = \lambda(a)$ para todo $a \in k$. Um diagrama:

$$\begin{array}{ccc} F & \xrightarrow{\sigma} & F' \\ \big| & & \big| \\ k & \xrightarrow{\lambda} & k' \end{array}$$

Exercício 7.1.

$$(f+g)^\lambda = f^\lambda + g^\lambda \qquad \text{e} \qquad (f\cdot g)^\lambda = f^\lambda \cdot g^\lambda. \tag{16}$$

Em particular, se λ é um isomorfismo, então f é irredutível em $k[x]$ se e somente se f^λ é irredutível em $k'[x]$.

Eis a almejada descrição de extensões de homomorfismos em extensões finitas.

Teorema 7.2 (Extensão)**.** *Sejam $k(u) \subset \mathbb{C}$ uma extensão finita de um corpo k, p o polinômio minimal de u sobre k, $\lambda\colon k \to \mathbb{C}$ um homomorfismo e $v_1, \ldots, v_r \in \mathbb{C}$ as distintas raízes de p^λ. Então λ possui exatamente r extensões $\sigma_i\colon k(u) \to \mathbb{C}$, dadas por $u \mapsto v_i$.*

Demonstração: Toda extensão de λ leva u em uma raiz de p^λ, como vimos em (15).

Reciprocamente, denote $k' = \lambda(k)$ e seja v uma das raízes de $p^\lambda \in k'[x]$. Pelo Teorema 4.3, cada elemento de $k(u)$ pode ser escrito como $f(u)$ para algum f em $k[x]$. Então a aplicação $\sigma\colon k(u) \to k'(v)$ dada por

$$\sigma(f(u)) = f^\lambda(v)$$

está de fato bem definida: se $f, g \in k[x]$ são tais que $f(u) = g(u)$, então $(f-g)(u) = 0$ e logo p divide $f-g$; segue daí que p^λ divide $(f-g)^\lambda$ e portanto $f^\lambda(v) = g^\lambda(v)$. Finalmente, as igualdades em (16) mostram que σ é um homomorfismo, que evidentemente estende λ. A prova está terminada. □

Corolário 7.3. *É sempre possivel estender homomorfismos em extensões finitas.*

Demonstração. Dada $k \subset F$ finita, temos uma torre

$$k = F_0 \subset F_1 \subset \cdots \subset F_r = F$$

onde $F_i = F_{i-1}(u_i)$ com u_i algébrico sobre F_{i-1}. Agora basta aplicar o Teorema 7.2 sucessivamente a cada passo da torre. □

Depois de lavoura feita com tanto cuidado, hora de colhermos frutos.

Corolário 7.4. *Se $F \supset k$ é normal e E é um corpo intermediário, então todo k-homomorfismo $E \to \mathbb{C}$ se estende a um k-automorfismo de F.*

Demonstração. Segue imediatamente do Corolário 7.3 e do Teorema 6.10. □

É fácil construir extensões normais. Decidir se uma dada extensão é normal é uma outra estória...

Suponha que F é uma extensão normal de k. Dado $u \in F$, seja $v \in \mathbb{C}$ um k-conjugado de u. Do Teorema 7.2 existe um k-homomorfismo $k(u) \to \mathbb{C}$ que leva $u \mapsto v$; pelo Corolário 7.4, podemos estendê-lo a um k-automorfismo de F e logo $v \in F$. Um resumo do que acabamos de mostrar:

Corolário 7.5. *Se $F \supset k$ é normal, então os k-conjugados de elementos de F estão em F.*

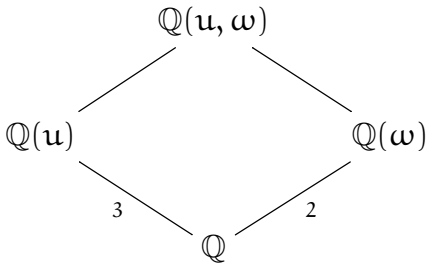
Temos assim um critério para mostrar que uma extensão *não* é normal. Por exemplo, $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ não é uma extensão normal, pois os $\mathbb{Q}$-conjugados de $\sqrt[4]{2}$ são $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$; os dois últimos não são números reais e logo não pertencem ao corpo $\mathbb{Q}(\sqrt[4]{2})$.

Exercício 7.6. A extensão $\mathbb{Q}(\sqrt[3]{2}, i) \supset \mathbb{Q}$ não é normal.

Vamos calcular nosso primeiro grupo de Galois.

Exemplo 7.7. Sejam $u = \sqrt[3]{2}$ e $\omega = e^{2\pi i/3} \in \mathbb{C}$ uma raiz cúbica da unidade. O polinômio minimal de u sobre $\mathbb{Q}$ é $f = x^3 - 2$, e suas raízes são $u, \omega u$ e $\omega^2 u$. O corpo de decomposição de f sobre $\mathbb{Q}$ é $F = \mathbb{Q}(u, \omega u, \omega^2 u) = \mathbb{Q}(u, \omega)$. Então $F \supset \mathbb{Q}$ é uma extensão normal cujo

grau é 6, uma vez que $\omega \notin \mathbb{Q}(u)$.



Repetimos o *modus operandi* da prova do Corolário 7.3 para descrever os automorfismos de $G = \mathrm{Gal}_{\mathbb{Q}} f$. Pelo Teorema 7.2 existem exatamente três $\mathbb{Q}$-homomorfismos

$$\sigma_i \colon \mathbb{Q}(u) \to \mathbb{C} \qquad i = 0, 1, 2$$

dados por $u \mapsto \omega^i u$. Como $F = \mathbb{Q}(u)(\omega)$ e o polinômio minimal de ω sobre $\mathbb{Q}(u)$ é $p = x^2 + x + 1$, vem do Teorema de Extensão que cada σ_i se estende a exatamente a dois homomorfismos $\sigma_{ij} \colon F \to \mathbb{C}$, $j = 1, 2$, dados por $\omega \mapsto \omega^j$ (note que $p^{\sigma_i} = p$). Como $[F : \mathbb{Q}] = 6$, estas são todas as possíveis extensões. Agora, $F \supset \mathbb{Q}$ é normal e daí cada σ_{ij} é de fato um automorfismo, pelo Teorema 6.10. Em resumo,

$$G = \{\sigma_{0,1}, \sigma_{0,2}, \sigma_{1,1}, \sigma_{1,2}, \sigma_{2,1}, \sigma_{2,2}\}$$

e cada automorfismo $\sigma_{ij} \colon F \to F$ fica definido pela sua ação no par u, ω (Exercício 6.3), segundo a tabela abaixo:

$$\begin{array}{lll}
\sigma_{0,1} : & u \mapsto u, & \omega \mapsto \omega \\
\sigma_{0,2} : & u \mapsto u, & \omega \mapsto \omega^2 \\
\sigma_{1,1} : & u \mapsto \omega u, & \omega \mapsto \omega \\
\sigma_{1,2} : & u \mapsto \omega u, & \omega \mapsto \omega^2 \\
\sigma_{2,1} : & u \mapsto \omega^2 u, & \omega \mapsto \omega \\
\sigma_{2,2} : & u \mapsto \omega^2 u, & \omega \mapsto \omega^2
\end{array}$$

Para um grupo de ordem 6, há apenas duas possibilidades: ou é cíclico, isomorfo a C_6, ou é isomorfo ao grupo S_3 de permutações de 3 elementos. E agora?

Comparemos os automorfismos $\sigma_{2,1}\sigma_{1,2}$ e $\sigma_{1,2}\sigma_{2,1}$. Mais uma vez, basta calcular a composição no par u, ω; temos

$$\begin{aligned}
(\sigma_{2,1}\sigma_{1,2})(u) &= \sigma_{2,1}(\omega u) = \sigma_{2,1}(\omega)\sigma_{2,1}(u) = \omega(\omega^2 u) = u \\
(\sigma_{2,1}\sigma_{1,2})(\omega) &= \sigma_{2,1}(\omega^2) = \omega^2
\end{aligned}$$

e logo $\sigma_{2,1}\sigma_{1,2} = \sigma_{0,2}$; por outro lado,

$$\begin{aligned}
(\sigma_{1,2}\sigma_{2,1})(u) &= \sigma_{1,2}(\omega^2 u) = \sigma_{1,2}(\omega)^2\sigma_{1,2}(u) = (\omega^2)^2(\omega u) = \omega^2 u \\
(\sigma_{1,2}\sigma_{2,1})(\omega) &= \sigma_{1,2}(\omega) = \omega^2
\end{aligned}$$

ou seja $\sigma_{1,2}\sigma_{2,1} = \sigma_{2,2}$. Assim G não é abeliano e, consequentemente, $G \cong S_3$. □

Exercício 7.8. Calcule as ordens dos elementos do grupo G no exemplo acima.

Exercício 7.9. Mostre que $\mathrm{Gal}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Z}_2$. Note que $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ mas o grupo de automorfismos tem ordem 2... Qual a origem da discrepância?

Para terminar esta seção, recorde que se um grupo G *age* em um conjunto S, então cada elemento de G induz uma permutação dos elementos de S. A ação é *transitiva* se cada órbita é igual ao próprio conjunto S, isto é: dados $u, v \in S$, existe $\sigma \in G$ tal que $\sigma(u) = v$.

Proposição 7.10. *Seja f um polinômio irredutível em $k[x]$, de grau n. Então $\mathrm{Gal}_k f$ é isomorfo a um subgrupo de S_n que age transitivamente nas raízes de f.*

Demonstração. Seja $S \subset \mathbb{C}$ o conjunto das raízes de f e $F = k(S)$ o corpo de decomposição de F. Como f é separável (Proposição 5.2), temos $|S| = n$. Como vimos, cada elemento de $\mathrm{Gal}_k f$ define uma permutação em S e logo temos um homomorfismo $\mathrm{Gal}_k f \to S_n$; este homomorfismo é injetor, pois $\sigma = \mathrm{id}_F$ se e somente se $\sigma(u) = u$ para todo $u \in S$. Finalmente, escolha $u, v \in S$. Pelo Teorema 7.2 existe um k-homomorfismo $k(u) \to \mathbb{C}$ levando $u \mapsto v$, que se estende a um automorfismo de F (Corolário 7.4). Logo a ação é transitiva. □

8. Teoria de Galois

8.1. **A correspondência de Galois.** Seja $F \supset k$ uma extensão de corpos e tome $G = \mathrm{Gal}_k F$ o grupo de automorfismos desta extensão. Um elemento $u \in F$ é um *ponto fixo* de um automorfismo $\sigma \in G$ se $\sigma(u) = u$.

A cada corpo intermediário $k \subset E \subset F$ fica associado a um subgrupo de G, a saber

$$\mathrm{Gal}_E F = \{\sigma \in G \mid \sigma(u) = u,\ \forall u \in E\}$$

o subgrupo dos automorfismos que estendem a identidade de E; dizendo de outra forma, são os k-automorfismos de F para os quais todos os elementos de E são pontos fixos. Reciprocamente, seja H um subgrupo de G. Definimos

$$F^H = \{u \in F \mid \sigma(u) = u,\ \forall \sigma \in H\}$$

o conjunto dos pontos fixos por *todos* os automorfismos pertencentes a H. Este é corpo intermediário na extensão $F \supset k$: de fato, como só consideramos k-automorfismos, ele contém k; e se $u, v \in F^H$, então

$$\sigma(u + v) = \sigma(u) + \sigma(v) = u + v \qquad (\forall \sigma \in H)$$

donde $u + v \in F^H$. Uma conta análoga funciona para $u - v$, $u \cdot v$ e u/v. Denominamos F^H o *corpo fixo* por H.

A *correspondência de Galois* é o par de aplicações

$$\begin{array}{ccc} \left\{\begin{array}{c}\text{corpos intermediários}\\ \text{de } F \supset k\end{array}\right\} & & \{\text{subgrupos de } G\} \\ E & \longmapsto & \mathrm{Gal}_E F \\ F^H & \longleftarrow & H \end{array} .$$

A correspondência de Galois reverte inclusões, como você deve verificar. Em geral, estas aplicações não desfrutam de outras propriedades emocionantes, como serem injetoras ou

sobrejetoras ou inversas uma da outra. Ainda assim, sucessivas aplicações fazem crescer o corpo ou grupo com o qual começamos:

Exercício 8.1. Dado um corpo intermediário E, tome $H = \mathrm{Gal}_E F$. Então para

$$E \mapsto H \mapsto F^H$$

vale que $E \subset F^H$. Reciprocamente, dado um subgrupo H, seja $E = F^H$. Então para

$$H \mapsto E \mapsto \mathrm{Gal}_E F$$

tem-se que $H \subset \mathrm{Gal}_E F$. Encontre exemplos onde não valem as inclusões opostas.

8.2. **Extensões galoisianas.**

Definição 8.2. Uma extensão é *galoisiana* (ou *de Galois*) se é normal e separável.

Mais uma vez: como estamos considerando apenas subcorpos dos complexos, nossas extensões são automaticamente separáveis e logo, aqui, uma extensão é galoisiana se e somente se é normal.

É instrutivo acompanhar a demonstração da proposição a seguir pelo Exemplo 7.7.

Proposição 8.3. *Se $F \supset k$ é galoisiana finita, então $|\mathrm{Gal}_k F| = [F : k]$.*

Demonstração. Escreva $F = k(u_1, \ldots, u_s)$, onde os u_i's são algébricos sobre k. Construímos a torre

$$k = F_0 \subset F_1 \subset \cdots \subset F_s = F$$

onde $F_i = F_{i-1}(u_i)$. Seja p_i o polinômio minimal de u_i sobre F_{i-1}. Temos

$$|\{\text{raízes de } p_i \text{ em } \mathbb{C}\}| = \operatorname{grau} p_i = [F_i : F_{i-1}]$$

onde a igualdade da esquerda vem do fato de que cada p_i é separável (Proposição 5.2). Segue então do Teorema 7.2 que um homomorfismo possui exatamente $[F_i : F_{i-1}]$ extensões no i-ésimo passo da torre. Assim, se começamos com a identidade de k, podemos estendê-la a $F \to \mathbb{C}$ por exatamente $[F_1 : F_0] \cdots [F_s : F_{s-1}] = [F : k]$ maneiras distintas. Como a extensão é normal, segue do Teorema 6.10 que todas estas extensões são automorfismos, o que termina a demonstração. □

Veremos a seguir que as extensões galoisianas finitas são exatamente aquelas para as quais a correspondência de Galois é bem comportada, ou seja, as aplicações da correspondência de Galois são de fato bijeções.

Lema 8.4. *Se $F \supset k$ uma extensão separável tal que $[k(u) : k] \leq n$ para cada $u \in F$, então a extensão é finita e vale $[F : k] \leq n$.*

Demonstração: Seja v em F escolhido de forma que $[k(v) : k]$ seja máxima. É suficiente mostrar que $F \subset k(v)$.

Tome $u \in F$. Como $k(u, v) \supset k$ é finita e separável, existe um elemento w tal que $k(u, v) = k(w)$ (um *elemento primitivo*; veja o Teorema 13.1). Então as desigualdades

$$[k(v) : k] \leq [k(u, v) : k] = [k(w) : k] \leq [k(v) : k]$$

são de fato igualdades e portanto $u \in k(v)$, como queríamos. □

Apresentamos agora o principal resultado desta seção, o célebre *Teorema Fundamental da Teoria de Galois*, devido a Emil Artin:

Teorema 8.5 (Artin)**.** *Sejam* F *um corpo e* G *um subgrupo* ***finito*** *qualquer do grupo de automorfismos de* F*. Então* $F \supset F^G$ *é uma extensão galoisiana de grau* $|G|$*, cujo grupo de Galois é* G*.*

Demonstração: Denote $k = F^G$. Dado $u \in F$, seja $S \subset F$ o conjunto das diferentes imagens de u pelos elementos de G, digamos $S = \{u = u_1, \ldots, u_r\}$. Observe que $r \leq |G|$. Defina $f = \prod_i (x - u_i)$, um polinômio em $F[x]$, de grau r.

Cada elemento de G induz uma permutação no conjunto S das raízes. Como os coeficientes de f são os polinômios simétricos elementares (10) nos u_i's, segue-se que cada um destes coeficientes é fixado por todos os elementos de G, ou seja, pertencem ao corpo fixo por G. Assim f é de fato um polinômio em $k[x]$, que tem u como raiz.

Em suma, mostramos que todo elemento de F é raiz de um polinômio separável em $k[x]$ cujas raízes estão em F, ou seja, $F \supset k$ é separável e normal. Agora, como $G \subset \mathrm{Gal}_k F$, temos

$$|G| \leq |\mathrm{Gal}_k F| = [F : k] \leq |G|$$

onde a igualdade vem da Proposição 8.3 e a desigualdade da direita segue do Lema 8.4, já que $[k(u) : k] \leq \operatorname{grau} f \leq |G|$ para cada $u \in F$. Portanto as desigualdades acima são de fato igualdades, concluindo a demonstração do teorema. □

Corolário 8.6. *Se* $F \supset k$ *é uma extensão galoisiana finita, então a correspondência de Galois é uma bijeção. De modo preciso, as aplicações*

$$\begin{array}{ccc} \left\{\begin{array}{c}\textit{corpos intermediários}\\ \textit{de } F \supset k\end{array}\right\} & & \{\textit{subgrupos de } \mathrm{Gal}_k F\} \\ E & \longmapsto & \mathrm{Gal}_E F \\ F^H & \longleftarrow & H \end{array}$$

são a inversa uma da outra. Além disso, $|H| = [F : F^H]$ *e* $[F^H : k] = (\mathrm{Gal}_k F : H)$*.*

Demonstração: Tome E um corpo intermediário e seja $H = \mathrm{Gal}_E F$. Como a extensão $F \supset E$ é galoisiana finita, vem da Proposição 8.3 que $|H| = [F : E]$; agora, pelo Exercício 8.1,

$$F \supset F^H \supset E$$

e como $[F : F^H] = |H|$ (Teorema de Artin), temos que a inclusão da direita é de fato uma igualdade, como desejado.

Por outro lado, sendo $\mathrm{Gal}_k F$ finito, segue do Teorema de Artin que $\mathrm{Gal}_{F^H} F = H$ para todo subgrupo H, o que prova que a correspondência de Galois é de fato uma bijeção. Para as igualdades do final do enunciado, já verificamos a primeira; e a segunda é consequência do bom e velho Teorema de Lagrange da teoria de grupos. □

Um diagrama, mil palavras: para extensões $F \supset k$ galoisianas finitas,

$$\begin{array}{ccc} F & & \{\mathrm{id}\} \\ \Big| {\scriptstyle |H|} & & \Big| \\ F^H = E & \longleftrightarrow & H = \mathrm{Gal}_E F \\ \Big| {\scriptstyle (G:H)} & & \Big| \\ k & & G \end{array}$$

Exemplo 8.7. Seja $\omega = e^{2\pi i/5} = \cos(2\pi/5) + i\,\mathrm{sen}(2\pi/5) \in \mathbb{C}$ uma raiz 5-ésima da unidade, isto é, $\omega^5 = 1$. As raízes do polinômio $x^5 - 1$ são $1, \omega, \ldots, \omega^4$. Temos $x^5 - 1 = (x-1)p$, onde $p = x^4 + \cdots + x + 1$. Pelo critério de Eisenstein, p é irredutível em $\mathbb{Q}[x]$, pois 5 é um número primo. Logo a extensão $\mathbb{Q}(\omega) \supset \mathbb{Q}$ é galoisiana de grau 4; os $\mathbb{Q}$-conjugados de ω são $\omega, \ldots, \omega^4$.

Seja G o grupo de automorfismos desta extensão. Cada automorfismo $\sigma \in G$ deve permutar as raízes de p e fica completamente determinado pela sua imagem $\sigma(\omega)$. Logo $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ onde $\sigma_j(\omega) = \omega^j$. Note que $\sigma_1 = \mathrm{id}$; e aplicando sucessivamente σ_2, obtemos

$$\omega \mapsto \omega^2 \mapsto \omega^4 \mapsto \omega^8 = \omega^3 \mapsto \omega^6 = \omega$$

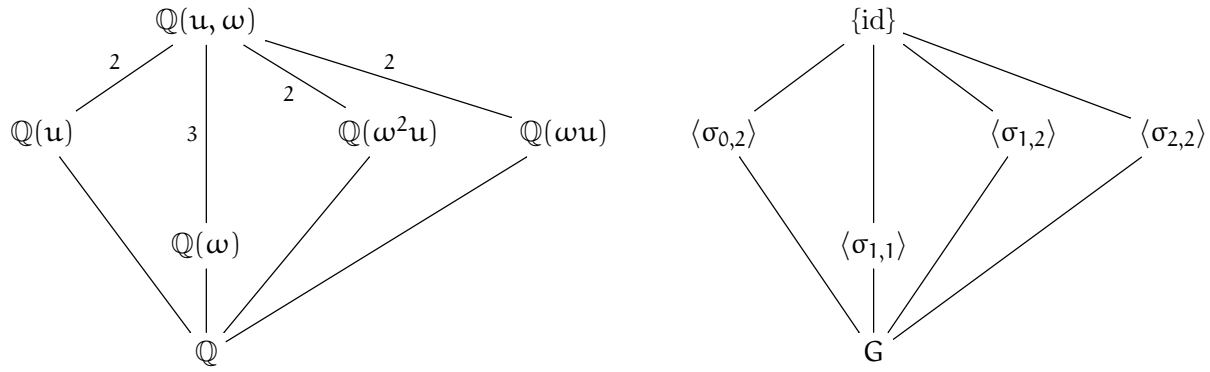
e logo σ_2 tem ordem 4. Portanto $G = \langle \sigma_2 \rangle$ é isomorfo a $\mathbb{Z}_4$.

Sendo cíclico de ordem 4, o grupo G possui um único subgrupo próprio, que tem ordem 2, a saber $H = \langle \sigma_2^2 \rangle = \langle \sigma_4 \rangle$. Daí, pela correspondência de Galois, a extensão $\mathbb{Q}(\omega) \supset \mathbb{Q}$ possui apenas um subcorpo intermediário não-trivial, o corpo fixo por H. Para determiná-lo, tome $u = \omega + \omega^{-1}$. Note que $\sigma_4(u) = u$ e portanto $u \in \mathbb{Q}(\omega)^H$. Como $\omega^{-1} = \bar{\omega}$ é o conjugado complexo de ω, vem que $u \in \mathbb{R}$ e daí $\mathbb{Q}(\omega) \supset \mathbb{Q}(u)$ é uma extensão de grau 2, pois $\omega \notin \mathbb{Q}(u)$ e ω é raiz de um polinômio quadrático em $\mathbb{Q}(u)[x]$, a saber $(x - \omega)(x - \bar{\omega}) = x^2 - ux + 1$. A correspondência de Galois é bem simples:

$$\begin{array}{ccc} \mathbb{Q}(\omega) & & \{\mathrm{id}\} \\ \Big| {\scriptstyle 2} & & \Big| \\ \mathbb{Q}(\omega + \omega^{-1}) & \longleftrightarrow & H \\ \Big| {\scriptstyle 2} & & \Big| \\ \mathbb{Q} & & G \end{array}$$

Exemplo 8.8. Revisitamos agora o Exemplo 7.7, usando a mesmo notação ali estabelecida. Vimos que o corpo F de decomposição do polinômio $x^3 - 2$ é uma extensão de grau 6 sobre $\mathbb{Q}$, e cujo grupo de Galois sobre é isomorfo ao grupo simétrico S_3. O grupo S_3 possui exatamente 3 subgrupos de ordem 2, a saber $\langle \sigma_{0,2} \rangle, \langle \sigma_{1,2} \rangle, \langle \sigma_{2,2} \rangle$ e exatamente um subgrupo de ordem 3. Da correspondência de Galois vem que existem exatamente 3 subcorpos intermediários E tais que $[F : E] = 2$; como $\mathbb{Q}(u), \mathbb{Q}(\omega^2 u)$ e $\mathbb{Q}(\omega u)$ são extensões de grau 3 de $\mathbb{Q}$, distintos entre si, estes são os corpos em questão. O subcorpo restante é $\mathbb{Q}(\omega)$

que fica associado ao subgrupo gerado por $\sigma_{1,1}$, que é um elemento de ordem 3 de G. Eis o diagrama que descreve a correspondência:



Exercício 8.9. Mostre que o diagrama do exemplo anterior está correto, isto é, que $\mathbb{Q}(\omega^{3-i}u)$ é corpo fixo por $\langle\sigma_{i,2}\rangle$, para $i = 0, 1, 2$.

Exercício 8.10. Um caso em que a extensão não é normal: descreva a correspondência de Galois para $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$.

Duas extensões E, E' de um corpo k são chamadas *conjugadas* se existe um k-isomorfismo $E \to E'$. Recorde que dois subgrupos H, H' de um grupo G são *conjugados* se existe $\sigma \in G$ tal que $H' = \sigma H \sigma^{-1}$.

Lema 8.11. *Seja $F \supset k$ uma extensão galoisiana finita. Então dois corpos intermediários E e E' são conjugados se e somente se $\mathrm{Gal}_E F$ e $\mathrm{Gal}_{E'} F$ são subgrupos conjugados em $\mathrm{Gal}_k F$.*

Demonstração: Começamos com a seguinte

Afirmação: *Dado $\sigma \in \mathrm{Gal}_k F$, então $\mathrm{Gal}_{\sigma(E)} F = \sigma(\mathrm{Gal}_E F)\sigma^{-1}$.*
De fato,

$$\begin{aligned}
\tau \in \mathrm{Gal}_{\sigma(E)} F &\iff \tau(\sigma(u)) = \sigma(u), \forall u \in E \\
&\iff (\sigma^{-1}\tau\sigma)(u) = u, \forall u \in E \\
&\iff \sigma^{-1}\tau\sigma \in \mathrm{Gal}_E F \\
&\iff \tau \in \sigma(\mathrm{Gal}_E F)\sigma^{-1}.
\end{aligned}$$

Seja agora $\lambda\colon E \to E'$ um k-isomorfismo. Como $F \supset k$ é uma extensão finita e normal, estendemos λ um k-automorfismo $\sigma\colon F \to F$. Então $\sigma(E) = E'$ e da Afirmação segue-se que $\mathrm{Gal}_E F$ e $\mathrm{Gal}_{E'} F$ são conjugados.

Reciprocamente, se $\mathrm{Gal}_E F$ e $\mathrm{Gal}_{E'} F$ são conjugados, então decorre da Afirmação que $\mathrm{Gal}_{E'} F = \mathrm{Gal}_{\sigma(E)} F$ para algum $\sigma \in \mathrm{Gal}_k F$. Como $F \supset k$ é galoisiana finita, vem da correspondência de Galois que $E' = \sigma(E)$, o que termina a prova. □

Teorema 8.12 (Segundo Teorema Fundamental)**.** *Seja $F \supset k$ uma extensão galosiana finita e E um corpo intermediário. Então a extensão $E \supset k$ é normal se e somente se*

$\mathrm{Gal}_E F$ *é um subgrupo normal de* $\mathrm{Gal}_k F$. *Nesse caso,*

$$\mathrm{Gal}_k E \cong \frac{\mathrm{Gal}_k F}{\mathrm{Gal}_E F}.$$

Demonstração: Pelo Lema 8.11:

$$\mathrm{Gal}_E F \text{ é normal em } \mathrm{Gal}_k F \iff \sigma(E) = E, \quad \forall \sigma \in \mathrm{Gal}_k F$$

e a condição do lado direito é válida se e somente se $E \supset k$ é uma extensão normal: você está oficialmente convidado a verificar. Isto prova a primeira afirmação do teorema.

Por outro lado, se $E \supset k$ é uma extensão normal, então a restrição de um k-automorfismo de F ao corpo E induz de fato um automorfismo (Teorema 6.10). Temos portanto um homomorfismo de grupos

$$|_E \colon \mathrm{Gal}_k F \to \mathrm{Gal}_k E$$

que é sobrejetor, uma vez que todo k-automorfismo de E se estende a um k-automorfismo de F (Corolário 7.4); seu núcleo evidentemente é $\mathrm{Gal}_E F$, pois estes são os automorfismos que fixam E. Segue do Teorema dos Homomorfismos que vale o isomorfismo do enunciado. □

Traduzindo em um diagrama: para extensões $F \supset k$ galoisianas,

$$\begin{array}{ccc} F & & \{\mathrm{id}\} \\ | & & | \\ E & & H \\ \text{normal} | & \iff & | \text{normal} \\ k & & G \end{array} \qquad (\textit{e nesse caso } \mathrm{Gal}_k E \cong G/H)$$

Exemplo 8.13. Denote $E = \mathbb{Q}(\sqrt[4]{2})$ e $F = \mathbb{Q}(\sqrt[4]{2}, i)$. Então $F \supset \mathbb{Q}$ é uma extensão normal. O seu grupo G de automorfismos não é abeliano: de fato, como $E \supset \mathbb{Q}$ não é normal, vem do Teorema 8.12 que o subgrupo $H = \mathrm{Gal}_E F$ não é normal em G.

Exercício 8.14. No exemplo anterior, mostre que $|G| = 8$ e que $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(i)$ é cíclico de ordem 4. Mais ainda, encontre σ, τ em G tais que

$$G = \langle \sigma, \tau \rangle, \quad \sigma^4 = 1, \quad \tau^2 = 1 \quad \text{e} \quad \tau\sigma = \sigma^3\tau$$

(estas são as relações necessárias para demonstrar que $G \cong D_4$, o grupo das simetrias de um quadrado).

Exemplo 8.15. Um exemplo mais longo, para o qual você está escalado(a) para preencher os detalhes.Tome $u = \sqrt{2}$, $v = \sqrt[3]{5}$ e $\omega = e^{2\pi i/3}$ uma raiz cúbica da unidade. Considere $F = \mathbb{Q}(u, v, w)$. Então $F \supset \mathbb{Q}$ é galoisiana, de grau $2 \cdot 3 \cdot 2 = 12$, graus correspondentes à torre

$$\mathbb{Q} \subset \mathbb{Q}(u) \subset \mathbb{Q}(u, v) \subset \mathbb{Q}(u, v, \omega) = F.$$

Os elementos do grupo de Galois G da extensão podem ser descritos da seguinte maneira:

$$G = \{\sigma_{ijk} \mid i = 0, 1,\ j = 0, 1, 2,\ k = 1, 2\}$$

onde σ_{ijk} fica dado por $(u, v, \omega) \mapsto ((-1)^i u, \omega^j v, \omega^k)$.

Seja n_2 o número de subgrupos de G com ordem $2^2 = 4$. Pelos teoremas de Sylow, temos

$$n_2 \equiv 1 \pmod 2 \quad \text{e} \quad n_2 \mid 3$$

e logo $n_2 = 1$ ou $n_2 = 3$. Como decidir? Olhamos para a extensão: temos pelo menos 3 subcorpos intermediários distintos E tais que $[F : E] = 4$, a saber: $\mathbb{Q}(v), \mathbb{Q}(\omega v)$ e $\mathbb{Q}(\omega^2 v)$. Estes, de fato, são os únicos pois pela correspondência de Galois, obtemos três subgrupos de G com ordem 4 e logo $n_2 = 3$. Novamente pelos teoremas de Sylow, os três grupos correspondentes a esses corpos são conjugados e segue daí pelo Lema 8.11 que esses três corpos são conjugados.

Também pelos teoremas de Sylow, G possui exatamente um subgrupo de ordem 3, que é normal em G; decorre da correspondência de Galois que existe exatamente um subcorpo intermediário K com $[F : K] = 3$. Uma inspeção rápida nos leva a $K = \mathbb{Q}(u, \omega)$. Note que $K \subset \mathbb{Q}$ é normal, como previsto pelo segundo Teorema Fundamental.

É natural tentar caracterizar o grupo G. Existem exatamente 5 grupos de ordem 12 não isomorfos entre si. Dois deles são abelianos ($\mathbb{Z}_{12}$ e $\mathbb{Z}_2 \times \mathbb{Z}_6$), que estão fora. Restam A_4, D_6 e $\mathbb{Z}_3 \rtimes \mathbb{Z}_4 \ldots$ □

Exercício 8.16. No exemplo anterior, encontre os subgrupos G_1, G_2 e G_3 associados aos corpos $\mathbb{Q}(v), \mathbb{Q}(\omega v)$ e $\mathbb{Q}(\omega^2 v)$ e determine elementos $g \in G$ tais que $gG_i g^{-1} = G_j$ para cada i, j.

9. RAÍZES DA UNIDADE

Seja $n \geq 1$ um inteiro. Um elemento ω em um corpo F é uma *raiz n-ésima da unidade* se $\omega^n = 1$, ou seja, se é uma raiz do polinômio $x^n - 1$. A ordem de qualquer raiz n-ésima da unidade como elemento do grupo multiplicativo F^* é, portanto, um divisor de n; a raiz é dita *primitiva* se sua ordem é igual a n.

O conjunto $U_n(F)$ das raízes n-ésimas é um subgrupo finito do grupo multiplicativo de um corpo, sendo portanto cíclico e cuja ordem divide n; vale que $|U_n(F)| = n$ se e somente se F possui uma raiz n-ésima primitiva.

Exemplo 9.1. É claro que $U_1(F) = \{1\}$ e $U_2(F) = \{\pm 1\}$ para qualquer corpo F. Considere $n \geq 3$. Para os números complexos, temos $U_n(\mathbb{C}) \cong \mathbb{Z}_n$ e uma raiz primitiva da unidade é $e^{2\pi i/n} = \cos(2\pi/n) + i\,\mathrm{sen}(2\pi/n)$. Já para os números racionais ou reais, $U_n(\mathbb{Q}) = U_n(\mathbb{R}) = \{1\}$ ou $\{\pm 1\}$ caso n seja par ou ímpar, respectivamente.

Recordemos alguns fatos sobre grupos cíclicos. Se G é cíclico de ordem n, então $G \cong \mathbb{Z}_n$. Se g é um gerador de G, então g^a é um outro gerador se e somente se $\mathrm{mdc}(a, n) = 1$ e logo G possui exatamente $\phi(n)$ geradores, onde ϕ é a função de Euler. Um automorfismo de G leva um gerador em outro gerador, sendo portanto da forma $g \mapsto g^a$ com $\mathrm{mdc}(a, n) = 1$. Segue daí que $\mathrm{Aut}(G) \cong \mathbb{Z}_n^*$.

Proposição 9.2. *Tome k um subcorpo dos números complexos e $\omega \in \mathbb{C}$ uma raiz n-ésima primitiva da unidade. Então a extensão $k(\omega) \supset k$ é galosiana e seu grupo de Galois é um subgrupo de $\mathbb{Z}_n^*$, sendo portanto abeliano.*

Demonstração. Como $k(\omega)$ é o corpo de decomposição do polinômio $x^n - 1$, a extensão $k(\omega) \supset k$ é normal e logo galoisiana. Seja σ um automorfismo desta extensão. A restrição de σ ao grupo das unidades $U = U_n(k(\omega))$ induz um automorfismo deste grupo. Como brinde, ganhamos um homomorfismo $\mathrm{Gal}_k k(\omega) \hookrightarrow \mathrm{Aut}(U) \cong \mathbb{Z}_n^*$ dado pela restrição, $\sigma \mapsto \sigma|_U$; este homomorfismo é injetor, pois $\sigma = \mathrm{id}$ se e somente se $\sigma(\omega) = \omega$.

Uma descrição mais concreta: como σ induz um automorfismo de U, temos $\sigma(\omega) = \omega^a$ onde $\mathrm{mdc}(a, n) = 1$. Por outro lado, como um k-automorfismo de $k(\omega)$ fica determinado pela sua imagem em ω, vem que σ fica determinado este expoente, e denotamos $a_\sigma = a$. O homomorfismo $\mathrm{Gal}_k k(\omega) \to \mathbb{Z}_n^*$ fica dado por $\sigma \mapsto \bar{a}_\sigma$. Note que $\sigma\tau \mapsto \bar{a}_\sigma \bar{a}_\tau$, pois $(\sigma\tau)(\omega) = \sigma(\omega^{a_\tau}) = \omega^{a_\sigma a_\tau}$. □

Temos uma descrição mais precisa quando o corpo de base são os números racionais.

Teorema 9.3. *Sejam $n \geq 1$ e $\omega \in \mathbb{C}$ uma raiz n-ésima primitiva da unidade. Então $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$. Consequentemente,* $\mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\omega) \cong \mathbb{Z}_n^*$.

Demonstração. Começamos com um resultado auxiliar.

Afirmação: *Se ω é uma raiz n-ésima primitiva da unidade, f seu polinômio minimal sobre $\mathbb{Q}$ e p é um primo tal que $p \nmid n$, então*

$$f(\omega^p) = 0.$$

De fato, como f divide $x^n - 1$, existe $h \in \mathbb{Q}[x]$ mônico tal que

$$x^n - 1 = fh$$

Pelo Lema de Gauss, $f, h \in \mathbb{Z}[x]$. Assuma que a Afirmação não valha, ou seja, $f(\omega^p) \neq 0$. Então $h(\omega^p) = 0$, o que significa que ω é uma raiz de $h(x^p)$. Como f é o polinômio minimal de ω, temos $h(x^p) = fg$ para algum polinômio g e, como anteriormente, temos $g \in \mathbb{Z}[x]$. Considerando essa igualdade módulo p, temos

$$\bar{h}(x^p) = \bar{h}^p = \bar{f}\bar{g} \qquad \text{em } \mathbb{Z}_p[x]$$

e como $\mathbb{Z}_p[x]$ é um domínio fatorial, segue-se que $\bar{f}$ e $\bar{h}$ possuem um fator comum. Mas $x^n - \bar{1} = \bar{f}\bar{h}$ temos uma contradição, pois o polinômio $x^n - \bar{1}$ é separável uma vez que $p \nmid n$. Logo nossa Afirmação vale.

Passemos à prova de que cada raiz n-ésima primitiva é uma raiz de f. Com efeito, tome m com $\mathrm{mdc}(m, n) = 1$ e decomponha $m = p_1 \cdots p_r$ como produto de primos, não necessariamente distintos. Dado que nenhum dos p_i's divide n, segue da Afirmação que $f(\omega^{p_1}) = 0$ e daí $p_{\omega^{p_1},\mathbb{Q}}$ divide f; portanto estes polinômios são iguais, pois são irredutíveis. Agora, tome $\omega_1 = \omega^{p_1}$; esta é uma raiz n-ésima primitiva da unidade, e com o mesmo argumento provamos que $p_{\omega_1,\mathbb{Q}} = p_{\omega_1^{p_2},\mathbb{Q}}$. Assim prosseguindo, concluímos que os polinômios minimais de ω e ω^m coincidem.

Em resumo, provamos que $\mathrm{grau}\, f \geq \phi(n)$. A outra desigualdade e a última afirmação do enunciado seguem da Proposição 9.2. □

Dado um inteiro n positivo, o n-*ésimo polinômio ciclotômico* é o polinômio minimal, sobre k, de uma raiz n-ésima primitiva. Quando $k = \mathbb{Q}$, o denotamos por Φ_n; vimos no Teorema 9.3 que este polinômio tem grau $\phi(n)$.

Exercício 9.4. As raízes de Φ_n são exatamente as raízes n-ésimas primitivas da unidade.

Exemplo 9.5. Se p é um número primo, então $\Phi_p = x^{p-1} + x^{p-2} + \cdots + x + 1$, pois este polinômio divide $x^p - 1$ e é irredutível sobre os racionais (troque $x \mapsto x + 1$ e use Eisenstein). Se n não é um número primo, encontrar Φ_n dá um pouco mais de trabalho. Por exemplo, $\Phi_6 = x^2 - x + 1$ e há pelo menos duas maneiras de verificar isto. Uma delas vem do exercício acima: tomando $\omega = e^{2\pi i/6}$, basta multiplicar $(x - \omega)(x - \omega^{-1})$ (note que $\omega^{-1} = \bar{\omega}$). A outra é recursiva, descrita pelo exercício abaixo.

Exercício 9.6. Prove que $x^n - 1 = \prod_{d|n} \Phi_d$ em $\mathbb{Q}[x]$, onde d percorre os divisores de n. Sugestão: agrupe as raízes n-ésimas de unidade de acordo com sua ordem e observe que para um divisor d de n existem exatamente $\phi(d)$ raízes d-ésimas primitivas da unidade em $\mathbb{C}$. A partir daí fique de olho no Exercício 9.4.

Uma extensão $F \supset k$ é *ciclotômica* se F é o corpo de decomposição do polinômio $x^n - 1$ para algum n.

Para $\omega_n = e^{2\pi i/n}$, vimos que $\mathbb{Q}(\omega_n) \supset \mathbb{Q}$ tem grupo de Galois $\mathbb{Z}_n^*$. No Exemplo 8.7 descrevemos o caso $n = 5$ com detalhe: vimos ali que o grupo de Galois é cíclico, isomorfo a $\mathbb{Z}_4 \cong \mathbb{Z}_5^*$. De fato, vale o seguinte (veja [GL02]):

Teorema 9.7. *O grupo $\mathbb{Z}_n^*$ é cíclico se e somente se $n = 2, 4, p^r$ ou $2p^r$, onde p é um primo ímpar.*

Exemplo 9.8. Analisamos agora o caso $\omega = e^{2\pi i/8}$, uma raiz 8-ésima primitiva da unidade.

A extensão $\mathbb{Q}(\omega) \supset \mathbb{Q}$ é galoisiana e tem grau 4, vide Teorema 9.3. Logo seu grupo de automorfismos também tem ordem 4, digamos $G = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$. Os índices foram escolhidos dessa maneira porque cada σ_j é definido por $\omega \mapsto \omega^j$, uma vez que um automorfismo permuta as raízes primitivas da unidade (que são as raízes do polinômio minimal de ω, pelo Exercício 9.4). Temos

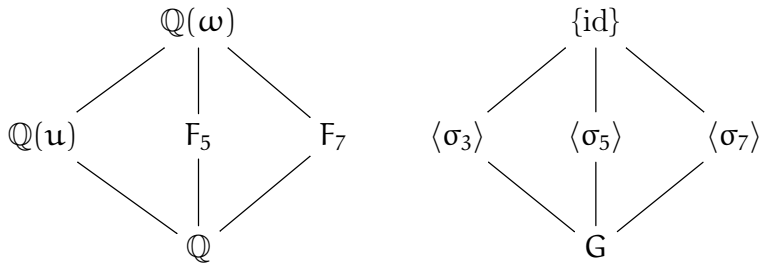
$$\sigma_3^2 = \sigma_5^2 = \sigma_7^2 = \mathrm{id}$$

pois

$$\omega^{3^2} = \omega^{5^2} = \omega^{7^2} = 1 \quad \text{uma vez que} \quad 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8.$$

Logo não existem elementos de ordem 4 e portanto $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, como previsto pelo Teorema 9.7. Os corpos fixos correspondentes aos subgrupos $\langle\sigma_3\rangle, \langle\sigma_5\rangle, \langle\sigma_7\rangle$ são todos os subcorpos intermediários não-triviais da extensão, e os apelidamos F_3, F_5, F_7.

Como encontrar esses corpos? Para grupos cíclicos $\langle\sigma\rangle$ há um truque clássico: basta acompanhar a ação de σ no gerador da extensão e tomar a soma. Por exemplo, como σ_3 leva $\omega \mapsto \omega^3 \mapsto \omega$, vem que $u = \omega + \omega^3$ é fixado por este automorfismo e logo $\mathbb{Q}(u) \subset F_3$; e como $[F_3 : \mathbb{Q}] = [G : \langle\sigma_3\rangle] = 2$ e $u \notin \mathbb{Q}$ (desenhe!), obtemos $F_3 = \mathbb{Q}(u)$.



Exercício 9.9. Encontre os outros dois corpos fixos no exemplo anterior. Se estiver de bom humor, descreva a correspondência de Galois para $\mathbb{Q}(e^{2\pi i/9})$; restando algum fôlego, faça para $\mathbb{Q}(e^{2\pi i/12})$.

10. SOLUBILIDADE POR RADICAIS

Estamos em condições de resolver o problema levantado no início destas notas: decidir quando um polinômio tem suas raízes expressas em termos das operações $+, -, \times, \div, \sqrt[n]{\cdot}$ aplicadas aos coeficientes. Nossa estratégia é reformular o problema em termos de extensões de corpos e em seguida resolvê-lo via a correspondência de Galois.

Como motivação, considere os exemplos:

Exemplo 10.1.

(1) Tome $f = x^4 - 6x^2 + 7 \in \mathbb{Q}[x]$. Suas raízes são $\pm\sqrt{3 \pm \sqrt{2}}$. Para obtê-las, consideramos a torre de extensões

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(\sqrt{3+\sqrt{2}}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3+\sqrt{2}})(\sqrt{3-\sqrt{2}})$$

obtidas adjuntando-se uma raiz de um elemento da extensão anterior. O último corpo da torre, contém todas as raízes de f. Note que todo elemento deste corpo se escreve como somas, produtos e quocientes de raízes quadradas sucessivamente aplicadas a números racionais.

(2) Tome $f = x^3 + 3x - 14 = (x-2)(x^2+2x+7)$. Suas raízes são $2, -1 \pm i\sqrt{6}$ e pertencem à extensão

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{-6})$$

onde $\sqrt{-6}$ é uma raiz do polinômio x^2+6. Por outro lado, se utilizamos as fórmulas de Cardano em (7), as raízes se escrevem como

$$u + v, \quad \omega u + \omega^2 v \quad \text{e} \quad \omega^2 u + \omega v$$

onde $u = \sqrt[3]{7+\sqrt{50}}$, $v = \sqrt[3]{7-\sqrt{50}}$ e $\omega = e^{2\pi i/3}$ é uma raiz cúbica da unidade. Considere a torre de extensões

$$\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\omega)(\sqrt{50}) \subset \mathbb{Q}(\omega, \sqrt{50})(\sqrt[3]{7+\sqrt{50}})$$

que são obtidas adjuntando-se sucessivamente raízes quadradas e cúbicas de elementos da extensão anterior. Mais uma vez, o maior corpo da torre contém todas as raízes do polinômio f (note que $u+v = 2$, veja (9)). Um destino, vários caminhos.

Dado a em um corpo k, uma *raiz n-ésima de a* é um elemento u em alguma extensão de k tal que $u^n = a$. Escrevemos $u = \sqrt[n]{a}$. Um aviso sobre a simbologia: ao contrário da convenção para números reais (onde $\sqrt[n]{a}$ denota a única raiz positiva de $x^n - a$), no nosso contexto $\sqrt[n]{a}$ é sempre ambíguo e indica qualquer uma das raízes de $x^n - a$.

Uma extensão $F \supset k$ é *radical* se pode ser decomposta em uma torre

$$k = F_0 \subset F_1 \subset \cdots \subset F_r = F$$

de modo que cada corpo é obtido adjuntando-se uma raiz $\star$-ésima de um elemento do corpo anterior, isto é: $F_i = F_{i-1}(\sqrt[n_i]{a_i})$ onde $a_i \in F_{i-1}$ e os n_i's são inteiros positivos.

Um artifício, tão simples quanto útil: se todos os n_i's são iguais entre si, digamos $n_1 = \cdots = n_r = n$, a extensão é dita n-*radical*; e de fato toda extensão radical é m-radical para algum m: basta tomar $m = n_1 \cdots n_r$.

Um polinômio $f \in k[x]$ é *solúvel por radicais* se existe uma extensão radical $F \supset k$ tal que f se decompõe em F (note: não pedimos aqui que F seja o corpo de decomposição de f, mas apenas um corpo no qual f se fatore linearmente).

Exercício 10.2. Se $F \supset E$ e $E \supset k$ são radicais, então $F \supset k$ é radical.

Antes de provar o teorema de Galois, precisamos de dois resultados auxiliares. O primeiro descreve o grupo de Galois em extensões obtidas adjuntando-se raízes.

Lema 10.3. *Suponha k é um subcorpo de $\mathbb{C}$ e que k contém uma raiz n-ésima primitiva da unidade. Dado $a \in k$, a extensão $k(\sqrt[n]{a}) \supset k$ é galosiana com grupo de Galois cíclico.*

Demonstração. Seja $\omega \in k$ uma raiz n-ésima primitiva e denote $u = \sqrt[n]{a}$. Temos que $x^n - a$ é um polinômio em $k[x]$ que possui n raízes distintas, a saber $u, \omega u, \ldots, \omega^{n-1}u$ e portanto a extensão $k(u) \supset k$ é normal — e logo galoisiana.

Um automorfismo σ desta extensão fica determinado pela sua ação em u. Daí, como $\sigma(u) = \omega^{a_\sigma}u$ para algum $a_\sigma \in \{0, \ldots, n-1\}$, o expoente a_σ determina σ. Definindo

$$\mathrm{Gal}_k\, k(u) \to \mathbb{Z}_n \qquad (a \mapsto \bar{a}_\sigma)$$

obtemos um homomorfismo, pois $\sigma\tau \mapsto \bar{a}_\sigma + \bar{a}_\tau$, já que $\sigma\tau(u) = \sigma(\omega^{a_\tau}u) = \omega^{a_\sigma + a_\tau}u$. Finalmente, se $\sigma \mapsto \bar{0}$, então $\sigma(u) = u$ e logo $\sigma = \mathrm{id}$, e portanto nosso homomorfismo é injetor. Isto termina a prova. □

Eis o segundo, de natureza puramente técnica.

Lema 10.4. *Considere uma extensão $F \supset k$ (de subcorpos de $\mathbb{C}$) n-radical. Então existe um corpo $N \supset F$ tal que a extensão $N \supset k$ é normal e n-radical.*

Demonstração. Por hipótese, existe uma torre

$$k = F_0 \subset F_1 \subset \cdots \subset F_r = F$$

tal que $F_i = F_{i-1}(u_i)$ e onde u_i é raiz de $x^n - a_{i-1} \in F_{i-1}[x]$.

Podemos supor que k contém uma raiz n-ésima primitiva da unidade (adjunte caso seja necessário). Então $k(u_1)$ é o corpo de decomposição de $x^n - a_0$, e portanto $F_1 \supset k$ é uma extensão normal. Tome $f_1 = \prod_\sigma (x^n - \sigma(a_1))$ onde σ percorre o grupo de automorfismos

$\mathrm{Gal}_k F_1$. Então cada σ fixa cada um dos coeficientes de f_1, o que mostra que $f_1 \in k[x]$; e adjuntando as raízes de f_1 sucessivamente ao corpo F_1, obtemos um corpo R, que é uma extensão n-radical de F_1. Logo $R \supset k$ é uma extensão normal (é dada pelo corpo de decomposição de f_1) e n-radical. Assim prosseguindo, obtemos a extensão $N \supset F \supset k$ desejada. □

Recorde que um grupo G é *solúvel* se existe uma cadeia de subgrupos

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{\mathrm{id}\}$$

tal que cada quociente G_{i-1}/G_i é um grupo abeliano.

Proposição 10.5. *Seja N um subgrupo normal de um grupo G. Então G é solúvel se e somente se N e G/N são solúveis.*

Teorema 10.6 (Galois)**.** *Suponha que k é um subcorpo de $\mathbb{C}$. Dado $f \in k[x]$, seja F o corpo de decomposição de f. Então f é solúvel por radicais se, e somente se, $\mathrm{Gal}_k F$ é um grupo solúvel.*

Demonstração. Suponha que f é solúvel por radicais. Então existe uma extensão n-radical $R \supset k$ tal que $R \supset F$. Seja $\omega = e^{2\pi i/n} \in \mathbb{C}$ uma raiz n-ésima primitiva da unidade. Então $R(\omega)$ também é uma extensão n-radical de k. Pelo Lema 10.4, existe $N \supset R(\omega)$ tal que $N \supset k$ é normal e n-radical.

Temos então uma torre de corpos (começamos adjuntando a raiz da unidade)

$$k = N_0 \subset k(\omega) = N_1 \subset N_2 \subset \cdots \subset N_r = N$$

onde $N_i = N_{i-1}(\sqrt[n]{a_i})$ e $a_i \in N_{i-1}$ para $i \geq 2$.

Sejam $G = \mathrm{Gal}_k N$ e $G_i = \mathrm{Gal}_{N_i} N$. Da correspondência de Galois, obtemos uma cadeia de subgrupos

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = \{\mathrm{id}\}$$

onde cada subgrupo é de fato normal no seguinte, uma vez que $N_{i-1} \subset N_i$ é uma extensão normal e tendo em vista o Teorema 8.12. Do mesmo teorema vem que G_{i-1}/G_i é isomorfo a $\mathrm{Gal}_{N_{i-1}} N_i$, e este grupo é abeliano: para $i = 1$ isto segue da Proposição 9.2, pois $N_1 \supset k$ é ciclotômica; para $i \geq 2$, vem do Lema 10.3 que o grupo de Galois de $N_i \supset N_{i-1}$ é cíclico, pois o corpo de base destas extensões contém uma raiz n-ésima primitiva da unidade.

Logo G é um grupo solúvel. Finalmente: como $F \supset k$ é normal, mais uma vez lançamos mão do Teorema 8.12 para concluir $\mathrm{Gal}_k F \cong G/\mathrm{Gal}_F N$, que é um grupo solúvel pela Proposição 10.5. Terminamos assim esta parte da demonstração.

A recíproca requer algo mais, aguarde em uma versão futura destas notas. □

Exemplo 10.7. Considere $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Afirmamos que o seu grupo de Galois é isomorfo ao grupo S_5 de permutações de 5 elementos.

Com efeito, sejam F o corpo de decomposição de f sobre $\mathbb{Q}$ e $G = \mathrm{Gal}_{\mathbb{Q}} F$. Como vimos na Proposição 7.10, podemos ver G como um subgrupo de S_5. Como f é irredutível, temos que $[\mathbb{Q}(u) : \mathbb{Q}] = 5$ para qualquer raiz u de f. Isso nos diz que 5 divide $[F : \mathbb{Q}] = |G|$; vem

do Teorema de Cauchy que G contém um elemento de ordem 5 e logo possui um 5-ciclo (se p é primo, todo elemento de ordem p de S_p é um p-ciclo).

Por outro lado, uma análise com derivadas e convexidade lá dos nossos bons tempos de Cálculo mostram que f possui exatamente duas raízes complexas não-reais, que são conjugadas entre si. Daí, se $\tau\colon \mathbb{C} \to \mathbb{C}$ é a conjugação complexa, então τ troca essas duas raízes e fixa as outras três; ou seja, $\tau|_F$, visto como um elemento de G, é uma transposição — note que a restrição de τ a F de fato define um automorfismo, pois $F \supset \mathbb{Q}$ é normal.

Em resumo, G é um subgrupo de S_5 que contém um 5-ciclo e uma transposição e logo $G = S_5$ (se p é primo, então S_p é gerado por um p-ciclo e uma transposição). Como S_5 não é um grupo solúvel, vem do Teorema 10.6 que o polinômio f não é solúvel por radicais. □

Do lado positivo da força, é claro que existem equações quínticas solúveis por radicais. Eis um exemplo interessante, explicado em detalhe em [BSW02, p. 29]:

$$x^5 + 15x + 12 = 0$$

tem como uma de suas soluções

$$\sqrt[5]{\frac{-75 + 21\sqrt{10}}{125}} + \sqrt[5]{\frac{-75 - 21\sqrt{10}}{125}} + \sqrt[5]{\frac{225 + 72\sqrt{10}}{125}} + \sqrt[5]{\frac{225 - 72\sqrt{10}}{125}}$$

e as outras raízes tem expressão similar.

Exercício 10.8. Os polinômios $x^5 - 20x^2 + 20, x^5 + x - 1$ e $x^5 - 2ax + a$ $(a \geq 2)$ também tem S_5 como grupo de Galois e portanto não são solúveis por radicais sobre $\mathbb{Q}$.

Exercício 10.9. A construção do Exemplo 10.7 generaliza-se com facilidade: Se p é um primo e f é um polinômio irredutível em $\mathbb{Q}[x]$ de grau p com exatamente duas raízes complexas não-reais, então $\mathrm{Gal}_{\mathbb{Q}} f \cong S_p$, o grupo de permutações de p elementos.

Você consegue encontrar um exemplo para $p = 7$?

Segunda Parte

11. corpos algebricamente fechados

11.1. **O fecho algébrico.** *Todo polinômio não constante com coeficientes complexos possui uma raiz em* $\mathbb{C}$. Este é o famoso Teorema Fundamental da Álgebra. Apresentamos abaixo (Teorema 11.7) uma demonstração, mais algébrica, que faz uso da correspondência de Galois e da teoria de grupos.

Uma consequência é que todo polinômio em $\mathbb{C}[x]$ se decompõe totalmente, isto é, pode ser escrito na forma $c(x-z_1)\cdots(x-z_n)$ onde $c, z_1, \ldots, z_n$ são números complexos.

Se k é um corpo qualquer, não necessariamente contido em $\mathbb{C}$, o que podemos dizer? Nossa questão é: dado um polinômio em $k[x]$, existe um corpo que contenha todas suas raízes? Mais ambiciosamente: existe um corpo que contenha todas as raízes de *todos* os polinômios de $k[x]$?

A resposta é... sim!

Teorema 11.1 (Kronecker)**.** *Dado um polinômio* p *com coeficientes em um corpo* k*, existe uma extensão finita* $F \supset k$ *na qual* p *de decompõe totalmente.*

Demonstração: Podemos supor que p é irredutível em $k[x]$ (caso não seja, consideramos um fator irredutível de p). Considere o ideal $(p) \subset k[x]$ dos múltiplos de p e seja $F = k[x]/(p)$ o anel quociente. Afirmamos que F é de fato um corpo. Com efeito, seja $f \in k[x]$ tal que $\bar{f} \neq \bar{0}$. Então p não divide f e, sendo p irredutível, $\mathrm{mdc}(p, f) = 1$. Logo existem $g, h \in k[x]$ tais que $gp + fh = 1$, ou seja, $\bar{f}\bar{h} = \bar{1}$. Assim $\bar{f}$ é invertível em F.

O homomorfismo $k \to F$ dado por $a \mapsto \bar{a}$ é injetivo e logo F contém uma cópia isomorfa de k. Finalmente, $\bar{x}$ é uma raiz de p, pois $p(\bar{x}) = \bar{p} = \bar{0}$ em F. Esta extensão é finita, uma vez que $F = k(\bar{x})$.

Tendo encontrado em F uma raiz u de p, fatoramos $p = (x-u)g$ com $g \in F[x]$, e construímos uma extensão finita de F que contenha uma raiz de g; assim prosseguindo, em um número finito de etapas obtemos uma extensão de k contendo todas as raízes de p. □

Se temos uma coleção finita de polinômios, então uma aplicação sucessiva do teorema de Kronecker nos fornece uma extensão com todas as raízes desses polinômios. A demonstração para uma coleção infinita é mais elaborada, necessariamente envolve o Lema de Zorn e, sorrateiramente, a omitimos; consulte [Lang02], [Morandi96].

Um corpo F é *algebricamente fechado* se cada polinômio não-constante em $F[x]$ possui uma raiz em F. O corpo dos números complexos é um exemplo. Um *fecho algébrico* de um corpo k é um corpo algebricamente fechado F tal que a extensão $F \supset k$ é algébrica.

Fechos algébricos sempre existem e são, essencialmente, únicos:

Teorema 11.2. *Seja* k *um corpo qualquer. Então* k *possui um fecho algébrico. Ainda, se* F *e* F' *são dois deles, então existe um* k*-isomorfismo* $F \to F'$*.*

Dada a unicidade, usualmente denotamos um fecho algébrico de k por $\bar{k}$.

Exemplo 11.3. O corpo $\mathbb{C}$ é um fecho algébrico do corpo $\mathbb{R}$ dos números reais. Porém, $\mathbb{C}$ não é um fecho algébrico de $\mathbb{Q}$, já que a extensão é transcendente. De fato, $\bar{\mathbb{Q}} \subset \mathbb{C}$ é o conjunto de todos os números algébricos.

Exercício 11.4. Mostre que $\bar{\mathbb{Q}}$ é enumerável. O que você tem a dizer sobre a dimensão de $\bar{\mathbb{Q}}$ como espaço vetorial sobre $\mathbb{Q}$?

Exercício 11.5. Se $\mathbf{F}$ é um corpo algebricamente fechado contendo k e

$$A = \{u \in \mathbf{F} \mid u \text{ é algébrico sobre } k\},$$

então A é também é algebricamente fechado e logo A é um fecho algébrico de k.

11.2. **O teorema fundamental da álgebra.** Como uma aplicação da teoria de Galois, provamos agora que todo polinômio complexo não-constante possui uma raiz complexa.

A prova que apresentamos aqui repousa sobre um fato topológico: a reta real é conexa (suspeito que qualquer prova deva envolver esse fato, ainda que indiretamente — apreciaria muito se você puder me dizer algo mais profundo a respeito), o que implica que todo polinômio real de grau ímpar possui uma raiz real.

Para polinômios de grau pequeno não há muito a fazer.

Exercício 11.6. Todo polinômio de grau 2 com coeficientes complexos possui uma raiz em $\mathbb{C}$. Em particular, não existem extensões de $\mathbb{C}$ de grau 2.

Teorema 11.7. *O corpo dos números complexos é algebricamente fechado.*

Demonstração: Suponha que u é algébrico sobre $\mathbb{C}$ e seja N o fecho normal da extensão $\mathbb{C}(u) \supset \mathbb{R}$. Então $N \supset \mathbb{R}$ é uma extensão galoisiana finita. Seja G seu grupo de Galois.

Sejam H o 2-subgrupo de Sylow de G e $F = N^H$ o seu corpo fixo. O índice $[G : H]$ é igual ao grau da extensão $F \supset \mathbb{R}$, e logo um número ímpar. Portanto, dado $v \in F$, o seu o polinômio mínimo sobre $\mathbb{R}$ tem também grau ímpar e consequentemente, pelo Teorema do Valor Intermediário, possui uma raiz em $\mathbb{R}$. Isso mostra que $v \in \mathbb{R}$. Concluímos $F = \mathbb{R}$, ou seja, $H = G$, e logo $|G|$ é uma potência de 2.

Afirmamos que $|G| = 2$: caso contrário, tomaríamos um subgrupo não-trivial dentro do 2-grupo G de índice 2 e teríamos, pela correspondência de Galois, uma extensão de grau 2 de $\mathbb{C}$, contradição com o resultado do Exercício 11.6.

Finalmente, segue da nossa afirmação que $N = \mathbb{C}$ e daí que $u \in \mathbb{C}$, demonstrando portanto que $\mathbb{C}$ é algebricamente fechado. □

12. A CARACTERÍSTICA DE UM CORPO

Entre todos os anéis, o dos números inteiros possui uma propriedade muito especial: para um anel k qualquer, sempre existe o homomorfismo *canônico* $\varphi\colon \mathbb{Z} \to k$, dado por

$$n \mapsto n \cdot 1_k = \pm 1_k \pm \cdots \pm 1_k \quad (|n| \text{ vezes}).$$

O núcleo e a imagem deste homomorfismo são objetos interessantes. O núcleo é um ideal de $\mathbb{Z}$ e logo da forma $p\mathbb{Z}$ para algum inteiro $p \geq 0$. O número p é chamado a *característica*

do anel k, que denotamos por $\operatorname{car} k$. De maneira equivalente e talvez mais compreensível, a característica de k é o menor inteiro positivo p tal que

$$1_k + \cdots + 1_k = 0 \qquad (p \text{ vezes}) \tag{17}$$

sendo que $\operatorname{car} k = 0$ se isso não acontece.

Há restrições para os possíveis valores de p quando k é um domínio. De fato, nesse caso a imagem também é um domínio. Agora, pelo Teorema dos Homomorfismos, vale $\varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ e, como sabemos, este quociente é um domínio se e somente se p é zero ou um número primo. Isso acontece em particular no nosso contexto, nos casos em que k é um corpo, o que voltamos a assumir de agora em diante.

Essas duas situações, característica zero e positiva, dividem os corpos em classes bem distintas. Por um lado, suponha que k tenha característica zero. Então φ é injetivo e logo $\varphi(\mathbb{Z}) \cong \mathbb{Z}$. Tomando o corpo de frações, concluímos que k contém uma cópia isomorfa do corpo $\mathbb{Q}$ dos números racionais. Assim, todo corpo de característica zero possui um número infinito de elementos. Se, por outro lado, $\operatorname{car} k = p > 0$, então k contém um corpo com p elementos, a saber, $\varphi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$. Aqui pode acontecer que k seja finito ou infinito.

O *corpo primo* k_0 do corpo k é por definição o seu menor subcorpo, isto é, a interseção de todos os subcorpos de k. Passamos agora a caracterizar todos os possíveis corpos primos.

Seja $F \subset k_0 \subset k$ o corpo de frações da imagem do homomorfismo $\varphi\colon \mathbb{Z} \to k_0$ acima, agora com contra-domínio em k_0. Sendo F um subcorpo de k, temos, por definição, que $k_0 \subset F$ e logo $F = k_0$. Assim, os únicos corpos primos existentes, a menos de isomorfismos, são $\mathbb{Q}$ e $\mathbb{Z}/p\mathbb{Z}$, para p primo. De agora em diante batizamos o único corpo com p elementos por $\mathbb{F}_p$. Resumindo:

Proposição 12.1. *A característica de um corpo k é zero ou um número primo. Quando $\operatorname{car} k = 0$, o corpo contém uma cópia isomorfa do corpo $\mathbb{Q}$ dos números racionais; se $\operatorname{car} k = p > 0$, então k contém uma cópia isomorfa de $\mathbb{F}_p$.*

Exemplo 12.2.

(1) Qualquer subcorpo de $\mathbb{C}$ tem característica zero.
(2) Dado um primo $p > 0$, seja F o corpo de frações do anel de polinômios $\mathbb{F}_p[x]$. Em outras palavras, os elementos de F são frações da forma f/g de polinômios em $\mathbb{F}_p[x]$ com $g \neq 0$. Então F é um corpo com um número infinito de elementos e com característica p.

12.1. **Corpos finitos.** Um corpo é *finito* se possui um número finito de elementos. Os corpos finitos são particularmente importantes em aplicações, como criptografia, códigos corretores de erros, processamento de imagens e muitas outras.

Um corpo finito F necessariamente possui característica positiva, uma vez que não contém uma cópia de $\mathbb{Q}$. Então $F \supset \mathbb{F}_p$, onde $p = \operatorname{car} F$ é um número primo. Em particular F é um $\mathbb{F}_p$-espaço vetorial de dimensão finita, digamos n. Temos assim um isomorfismo de espaços vetoriais $(\mathbb{F}_p)^n = \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ e em particular o corpo F possui p^n elementos. Acabamos de mostrar que a cardinalidade de qualquer corpo finito é uma potência de um número primo. Por exemplo, não existem corpos com 10 ou 36 elementos.

O conjunto F^* das unidades de F é um grupo multiplicativo, de ordem $p^n - 1$. Dado $a \in F^*$, segue do teorema de Lagrange que sua ordem divide $p^n - 1$ e logo $a^{p^n-1} = 1$. Incluindo o zero, temos que todo elemento de F é uma das raízes de $x^{p^n} - x$, que são em número $\leq p^n$. Mas esta é a cardinalidade de F; a conclusão é que existem de fato p^n raízes, que são exatamente os elementos de F.

Reciprocamente, vamos mostrar que todo corpo finito pode ser construído desta maneira. Sejam dados um número primo p e um inteiro $n \geq 1$. Tome $\mathbf{F}$ um fecho algébrico de $\mathbb{F}_p$. Sendo p primo, p divide $\binom{p}{i}$ para cada $i = 1, \ldots, p-1$ e logo

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

para quaisquer $a, b \in \mathbf{F}$. Indutivamente, obtemos

$$(a+b)^{p^r} = a^{p^r} + b^{p^r} \qquad (r \geq 0). \tag{18}$$

Seja $S \subset \mathbf{F}$ o conjunto das raízes do polinômio $x^{p^n} - x$. Dados $a, b \in S$, segue de (18) $a+b \in S$ e, evidentemente $-a, ab$ e $1/a$ $(a \neq 0)$ são elementos de S. E como $0, 1$ também estão em S, temos que S é um subcorpo de $\mathbf{F}$. Finalmente, $x^{p^n} - x$ é um polinômio separável (tome a derivada), e logo suas raízes são distintas duas a duas, o que mostra $|S| = p^n$.

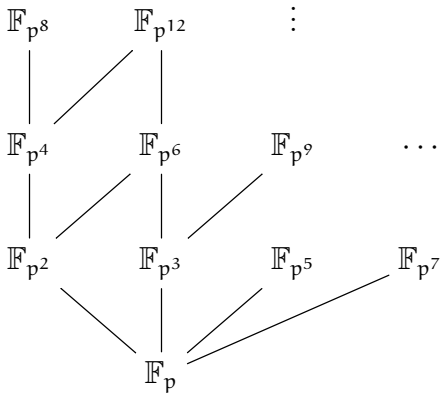
Eis o resumo de todo nosso bate-papo.

Teorema 12.3. *Se F é um corpo finito, então $|F| = p^n$, onde p é a característica de F. Reciprocamente, dados p primo, $n \geq 1$ e fixado um fecho algébrico de $\mathbb{F}_p$, então existe exatamente um único corpo finito com p elementos, denotado $\mathbb{F}_{p^n}$, que é dado pelas raízes do polinômio $x^{p^n} - x$. Finalmente,*

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n.$$

Demonstração. Basta provar a última afirmação do teorema. Se $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ é uma extensão de grau a, então do isomorfismo de espaços vetoriais $\mathbb{F}_{p^n} \cong (\mathbb{F}_{p^m})^a$ vem que $p^n = (p^m)^a$, donde $n = ma$. Reciprocamente: se $m \mid n$, então $x^{p^m} - x$ divide $x^{p^n} - x$ e daí vem que $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. □

Eis um diagrama que ilustra o reticulado formado pelos corpos finitos:



13. O TEOREMA DO ELEMENTO PRIMITIVO

Seja $F \supset k$ uma extensão de corpos. Dizemos que u é um *elemento primitivo* da extensão se $F = k(u)$. Seu pressentimento está correto: nem toda extensão admite um elemento primitivo. Mas isto ocorre em uma situação bem geral, um resultado muito útil.

Teorema 13.1 (Elemento primitivo)**.** *Seja $F \supset k$ uma extensão finita e separável. Então existe $w \in F$ tal que $F = k(w)$.*

Demonstração: A prova se divide em dois casos. No primeiro, supomos que k é um corpo finito. Então F é também um corpo finito e logo basta tomar w como um gerador do grupo multiplicativo F^* (que é cíclico).

Assuma k infinito. Começamos com o caso em que F é gerado por apenas dois elementos, digamos $F = k(u, v)$. Sejam $f, g \in k[x]$ os polinômios minimais de u, v sobre k e $\{u = u_1, \ldots, u_r\}$ e $\{v = v_1, \ldots, v_s\}$ as raízes desses polinômios. Escolha $c \in k$ tal que

$$u + cv \neq u_i + cv_j$$

para todo i e todo $j \geq 2$, ou seja, escolha c fora do conjunto finito

$$\{(u_i - u)/(v - v_j) \mid i = 1, \ldots, r,\ j = 2, \ldots, s\}.$$

Tome $w = u + cv$. Então v é uma raiz dos polinômios $g(x)$ e $f(w - cx)$, que estão em $k(w)[x]$. Seja h o polinômio minimal de v sobre $k(w)$. Então h divide tanto $g(x)$ como $f(w - cx)$; por outro lado, segue da escolha de c que v é a única raiz comum de $g(x)$ e $f(w - cx)$ e, como h é separável, obtemos $h = x - v$. Concluímos que v e a posteriori u, estão em $k(w)$, o que termina este caso.

Para o caso geral: como $F \supset k$ é uma extensão finita, temos $F = k(u_1, \ldots, u_n)$ onde cada u_i é algébrico sobre k e perfazemos indução sobre o número n de geradores, aplicando o caso anterior: $k \subset k(u_1, u_2) \subset k(u_1, u_2, u_3) = k(w, u_3) \subset \cdots$. Convido você a preencher os detalhes. □

A demonstração fornece um método para encontrar um elemento primitivo.

Exercício 13.2. Encontre elementos primitivos para as extensões $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ e $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ sobre os números racionais.

Há ainda uma outra variante, devida a Steinitz, em termos dos corpos intermediários.

Teorema 13.3. *Uma extensão é finita e separável se e somente se possui um número finito de corpos intermediários.*

Demonstração. □

≈≈

14. DEPOIS DO HORIZONTE

Há ótimas referências para aprender mais sobre o assunto. A lista apresentada abaixo não é completa e acredito que qualquer tentativa nesse sentido seria vã. Alguns comentários sobre as escolhas que fiz.

Emil Artin [Artin66] é *o* clássico, um primor em simplicidade e elegância; Serge Lang (um aluno de Artin) [Lang02] é semi-enciclopédico; Patrick Morandi [Morandi96] é moderno, bem escrito, apontando conexões com tópicos mais avançados; John Stillwell [Stillwell94] é ligeiro e me agrada bastante pela simplicidade e eficiência, e ainda traz consigo algo de história; David Cox [Cox12] é recente, com viés computacional, de rara riqueza em exemplos e construções clássicas. O artigo da Wikipedia [Wiki] é quase obrigatório: é a ponta de um novelo que traz prazer ao puxar, seja pela matemática, seja por aprender mais da tragédia que pairou, insistente, sobre a curta vida de Galois.

Enfim, minha predileção recai sobre *Galois Theory*, de Ian Stewart [Stewart03] e *Algebra*, de Michael Artin [Artin91], duas delícias explícitas de leitura.

REFERÊNCIAS

[Artin66] E. Artin, *Galois Theory*, Notre Dame Mathematical Lectures Number 2, 1966.
[Artin91] M. Artin, *Algebra*, Prentice-Hall, 1991.
[BSW02] B.C. Berndt, B.K. Spearman and K.S. Williams, *Commentary on a unpublished lecture by G.N. Watson on solving the quintic*. Mathematical Intelligencer 4(24), 1 5–33, 2002.
[Cox12] D. Cox, *Galois Theory*, 2nd. edition, John Wiley & Sons, 2012.
[GL02] A. Garcia, Y. Lequain, *Elementos de álgebra*, Projeto Euclides, IMPA, 2002.
[Herstein75] I. Herstein, *Topics in Algebra*, 1975.
[Kaplansky69] I. Kaplansky, *Fields and Rings*, University of Chicago Press, 1969.
[Lang02] S. Lang, *Algebra*, GTM 211 (Revised third ed.), Springer-Verlag, 2002.
[Morandi96] P. Morandi, *Field and Galois Theory*, GTM 167, Springer-Verlag, 1996.
[BMST10] F. Brochero, C. Gustavo Moreira, N. Saldanha, E. Tengan, *teoria dos números*, IMPA, 2010.
[Rotman98] J. Rotman, *Galois Theory*, (New York, 1998).
[Rowen95] L. Rowen, *Algebra: Groups, Rings, and Fields*, A. K. Peters, Ltd., 1995.
[Galois] E. Galois, *Œuvres Mathématiques*, Journal de Liouville, 1846.
[Stewart03] I. Stewart, *Galois Theory*, Chapman & Hall, 2003.
[Stillwell94] J. Stillwell, *Elements of Algebra*, UTM, Springer, 1994.
[Tignol88] J.-P. Tignol, *Galois' Theory of Algebraic Equations*, Longman, New York, 1988.
[Vilella] M. L. Vilella, *Notas de aula para o curso de Álgebra III*, UFF, 2010.
[Wiki] Wikipedia, *Évariste Galois*: pt.wikipedia.org/wiki/Évariste_Galois