Aprenda Teoria de Galois (em 24 horas!)

Eduardo Tengan

Suponhamos que você está em uma ilha deserta. De repente, você sente uma vontade irresistível de calcular $\cos\frac{2\pi}{17}$. Como obter

$$\cos\frac{2\pi}{17} = \frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}}{16}$$

utilizando somente cocos, folhas, pedras, galhos, areia e teoria de Galois? É o que aprenderemos a seguir, vendo alguns dos resultados básicos desta teoria. Para simplificar a exposição, enunciaremos vários resultados somente para $\mathbb{Q}$, porém é fácil ver que as provas se estendem ipsis literis para corpos de característica 0.

Para maiores detalhes e outras abordagens, consulte qualquer livro de Álgebra como os listados na bibliografia, em particular o livro (a ser lançado em breve) *Álgebra exemplar*, em coautoria com o professor Sérgio Tadao Martins; uma versão preliminar da parte de grupos encontra-se disponível no site *Open Math Notes* da AMS, em

https://www.ams.org/open-math-notes/omn-view-listing?listingId=110718

1 Glossário

Estrutura	Definição miojo	Exemplos
Conjunto	coleção de objetos, ditos *elementos* do conjunto	$\varnothing$, $\mathbb{N}$ ou $\{a, b, \heartsuit\}$
Grupo	conjunto em que se pode multiplicar e dividir	$(\mathbb{Q}^\times, \cdot)$, $(\mathbb{Z}, +)$, $(S_n, \circ)$ ou $(GL_n(\mathbb{R}), \cdot)$
Grupo abeliano	grupo em que a multiplicação é comutativa	$(\mathbb{R}^\times, \cdot)$ ou $(\mathbb{Z}/n\mathbb{Z}, +)$
Anel	conjunto em que se pode somar, subtrair e multiplicar	$(\mathbb{Z}, +, \cdot)$ ou $(M_n(\mathbb{R}), +, \cdot)$
Anel comutativo	anel com multiplicação comutativa	$(\mathbb{Z}, +, \cdot)$ ou $(\mathbb{R}, +, \cdot)$
Domínio	anel comutativo em que se pode cancelar	$(\mathbb{Z}, +, \cdot)$ ou $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ com p primo
Ideal	subconjunto de múltiplos em um anel	$3\mathbb{Z}$ em $\mathbb{Z}$
Corpo	anel em que se pode dividir por $a \neq 0$	$(\mathbb{Q}, +, \cdot)$ ou $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ com p primo
Morfismo	substituição	$\varphi\colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ com $\varphi(n) =$ paridade de n
Automorfismo	mudança de variáveis	$\varphi\colon \mathbb{C} \to \mathbb{C}$ com $\varphi(z) = \overline{z}$

As definições oficiais destes termos encontram-se no apêndice, juntamente com uma listagem dos enunciados (sem prova) dos principais teoremas.

2 Polinômios simétricos

Seja A um anel comutativo e denote por $A[x_1, \ldots, x_n]$ o anel dos polinômios nas variáveis $x_1, \ldots, x_n$ com coeficientes em A. O primeiro conceito de que necessitaremos é o de **polinômio simétrico**: um polinômio em $A[x_1, \ldots, x_n]$ é simétrico se ele não se altera quando intercambiamos duas de suas variáveis. Provavelmente os polinômios simétricos mais simples são os chamados **polinômios simétricos elementares**:

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ &\vdots \\ s_n &= x_1 \ldots x_{n-1}x_n \end{aligned}$$

Utilizando os polinômios simétricos elementares, é fácil produzir outros polinômios simétricos, tais como $s_2 + s_3$, $s_1^2 s_n$ e, em geral, qualquer polinômio em s_1, s_2, …, s_n. O fato interessante é que esta é a **única** maneira de produzir polinômios simétricos. A demonstração é simples e a reproduzimos aqui.

Em primeiro lugar, ordenamos os monômios segundo uma ordem **grau-lexicográfica**, isto é, diremos que

$$ax_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n} > bx_1^{\beta_1}x_2^{\beta_2}\ldots x_n^{\beta_n} \qquad (a, b \in A,\ \alpha_i, \beta_i \in \mathbb{N})$$

se

(a) o grau $\sum\alpha_i$ do primeiro monômio for maior do que o grau $\sum\beta_i$ do segundo; ou

(b) caso contrário, se os graus forem iguais, o primeiro for lexicograficamente maior do que o segundo (em outras palavras, existe um k tal que $\alpha_i = \beta_i$ para $1 \leqslant i < k$ e $\alpha_k > \beta_k$).

O **termo líder** de um polinômio é o maior de seus monômios (juntamente com seu coeficiente). Por exemplo, o termo líder de

$$\begin{aligned} f(x_1, x_2, x_3) &= 10x_1x_2x_3 + x_1 + x_2 + x_3 \\ &+ 2x_1^2x_2 + 2x_1^2x_3 + 2x_2^2x_1 + 2x_2^2x_3 + 2x_3^2x_1 + 2x_3^2x_2 \end{aligned} \tag{1}$$

é $2x_1^2x_2$. Agora, dado um polinômio simétrico $p(x_1, \ldots, x_n)$, seja $cx_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$ o seu termo líder. Já que p é simétrico, devemos ter $\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_n$. Utilizando os polinômios simétricos elementares, podemos construir outro polinômio simétrico com mesmo termo líder: basta tomar $cs_1^{\alpha_1-\alpha_2}s_2^{\alpha_2-\alpha_3}\ldots s_{n-1}^{\alpha_{n-1}-\alpha_n}s_n^{\alpha_n}$. Agora

$$p - cs_1^{\alpha_1-\alpha_2}s_2^{\alpha_2-\alpha_3}\ldots s_{n-1}^{\alpha_{n-1}-\alpha_n}s_n^{\alpha_n}$$

é um polinômio simétrico com termo líder menor. Repetindo o processo quantas vezes for necessário, obteremos eventualmente 0, ou seja, desta forma teremos escrito p como polinômio em $s_1, s_2, \ldots, s_n$. No exemplo (2) acima, temos

$$f(x_1, x_2, x_3) - 2s_1s_2 = 4x_1x_2x_3 + x_1 + x_2 + x_3$$

com termo líder $4x_1x_2x_3 < 2x_1^2x_2$. Continuando o processo, obtemos finalmente

$$f(x_1, x_2, x_3) = 2s_1s_2 + 4s_3 + s_1$$

A partir da expressão

$$\prod_{1\leqslant i\leqslant n}(x - x_i) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n$$

temos um importante corolário do resultado acima:

Lema 1. *Seja A um domínio. Se $f(x) \in A[x]$, qualquer polinômio simétrico nas raízes de $f(x)$ também pertence a A.*

Por exemplo, como $\dfrac{1\pm\sqrt{5}}{2}$ são raízes de $x^2 - x - 1 \in \mathbb{Z}[x]$, temos que

$$\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n \in \mathbb{Z}$$

para todo $n \in \mathbb{N}$.

3 Extensões algébricas

Seja $L \supseteq K$ uma extensão de corpos. Um elemento $\alpha \in L$ é **algébrico** sobre K se α é raiz de um polinômio não nulo em $K[x]$ (que podemos supor ser mônico, dividindo pelo coeficiente líder). Se $\alpha \in L$ é algébrico, seu **polinômio minimal** sobre K é o polinômio **mônico** $p(x) \in K[x]$ de menor grau para o qual $p(\alpha) = 0$. Cada elemento algébrico $\alpha \in L$ possui um único polinômio minimal sobre K, como consequência do

Teorema 2 (Menor divide)**.** *Seja $L \supseteq K$ uma extensão de corpos e seja $\alpha \in L$ algébrico sobre K. Seja $p(x) \in K[x]$ o polinômio minimal de α sobre K. Dado $q(x) \in K[x]$, temos*

$$q(\alpha) = 0 \iff p(x) \mid q(x)$$

Em particular, o polinômio minimal $p(x) \in K[x]$ de α sobre K pode ser caracterizado como o (único) polinômio mônico irredutível em $K[x]$ que admite α como raiz.

Demonstração. Dividindo $q(x)$ por $p(x)$, obtemos

$$q(x) = a(x)\cdot p(x) + r(x) \qquad \text{com } r(x) = 0 \text{ ou } \deg r(x) < \deg p(x)$$

Substituindo x por α na igualdade acima, concluímos que $r(\alpha) = 0$; sendo $p(x)$ o polinômio minimal de α, não podemos ter $\deg r(x) < \deg p(x)$, logo $r(x) = 0$ e portanto $p(x)$ divide $q(x)$.

Em particular, se um polinômio mônico e irredutível $q(x) \in K[x]$ admite α como raiz, então de $p(x) \mid q(x)$ temos $q(x) = p(x)$, o que prova a caracterização do polinômio minimal acima. □

Dois elementos $\alpha, \alpha' \in L$ algébricos sobre K são ditos **conjugados** sobre K se α, α' possuem o mesmo polinômio minimal sobre K ou, equivalentemente, se são raízes de um mesmo polinômio irredutível em $K[x]$. Por exemplo, $\pm i$ são conjugados sobre $\mathbb{Q}$, assim como $2 \pm \sqrt{3}$. Raízes conjugadas terão um importante papel no que segue.

Dizemos que a extensão $L \supseteq K$ é algébrica se todo elemento de L é algébrico sobre K. Por exemplo, considere (um corpo, prove!)

$$\mathbb{Q}[\sqrt{3}] \stackrel{\text{def}}{=} \mathbb{Q} + \mathbb{Q}\sqrt{3} = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$$

A extensão $\mathbb{Q}[\sqrt{3}] \supseteq \mathbb{Q}$ é algébrica, pois $\alpha = a + b\sqrt{3}$ $(a, b \in \mathbb{Q})$ é raiz do polinômio com coeficientes em $\mathbb{Q}$

$$(x - (a + b\sqrt{3}))(x - (a - b\sqrt{3})) = x^2 - 2ax + a^2 - 3b^2 \in \mathbb{Q}[x]$$

O lema 1 acima possui o seguinte

Corolário 3. *Sejam $M \supseteq L \supseteq K$ extensões de corpos. Se $M \supseteq L$ e $L \supseteq K$ são extensões algébricas, então $M \supseteq K$ também é algébrica (isto é mais difícil de enunciar do que provar!)*

Demonstração. Dado $\alpha \in M$, queremos mostrar que α é algébrico sobre K. Como α é algébrico sobre L, temos que α é raiz de um polinômio

$$\alpha^n + l_{n-1} \cdot \alpha^{n-1} + l_{n-2} \cdot \alpha^{n-2} + \cdots + l_0 = 0 \qquad (l_i \in L)$$

Cada l_i é algébrico sobre K; seja $p_i(x) \in K[x]$ seu polinômio minimal. Considere o produto

$$P(x) = \prod_{l'_{n-1}, l'_{n-2}, \ldots, l'_0} (x^n + l'_{n-1} \cdot x^{n-1} + l'_{n-2} \cdot x^{n-2} + \cdots + l'_0)$$

em que l'_i percorre todas as raízes de $p_i(x)$, i.e., os conjugados de l_i. Obviamente os coeficientes do polinômio $P(x)$ são expressões simétricas das raízes de $p_i(x)$ e portanto pertencem a K. Como $P(\alpha) = 0$ concluímos que α é de fato algébrico sobre K. □

4 Extensões simples

Uma extensão de corpos $L \supseteq K$ é **simples** se $L = K(\alpha)$, ou seja, se L é gerado sobre K por um único elemento $\alpha \in L$. Isto quer dizer que qualquer elemento de $L = K(\alpha)$ é uma função racional (i.e., o quociente de dois polinômios) em α com coeficientes em K. Se, além disso, α é algébrico sobre K, é suficiente utilizar expressões polinomiais:

Teorema 4. *Seja $L \supseteq K$ uma extensão de corpos e seja $\alpha \in L$ algébrico sobre K, com polinômio minimal $p(x) \in K[x]$ de grau d. Então qualquer elemento de $K(\alpha)$ é um polinômio em α com coeficientes em K de grau no máximo $d-1$:*

$$K(\alpha) = K + K\alpha + K\alpha^2 + \cdots + K\alpha^{d-1}$$

Para provar o teorema, basta mostrar que um elemento qualquer

$$f(\alpha)/g(\alpha) \in K(\alpha) \qquad (f, g \in K[x],\ g(\alpha) \neq 0)$$

pode ser escrito como um polinômio em α com coeficientes em K. Daí, se $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$, podemos utilizar recursivamente a relação

$$p(\alpha) = 0 \iff \alpha^d = -a_{d-1}\alpha^{d-1} - \cdots - a_0$$

para reduzir o grau em α até no máximo $d-1$. Sendo $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ os d conjugados de α, a ideia é "racionalizar o denominador" $g(\alpha)$ na expressão acima multiplicando-o pelo produto de seus conjugados, de modo a obter

$$N = \prod_{1 \leqslant i \leqslant d} g(\alpha_i)$$

que é um elemento de K pelo lema 1.
Por exemplo, dado

$$\beta = \frac{7 - 2\sqrt[3]{5}}{1 + \sqrt[3]{5} + 2\sqrt[3]{25}} \in \mathbb{Q}(\sqrt[3]{5})$$

multiplicamos o numerador e denominador desta fração por

$$M \stackrel{\text{def}}{=} (1 + \omega\sqrt[3]{5} + 2\omega^2\sqrt[3]{25})(1 + \omega^2\sqrt[3]{5} + 2\omega\sqrt[3]{25})$$

em que $\omega = e^{2\pi i/3}$, uma raiz cúbica primitiva da unidade. No denominador, obtemos uma expressão simétrica em $\sqrt[3]{5}$, $\omega\sqrt[3]{5}$, $\omega^2\sqrt[3]{5}$, as raízes do polinômio $x^3 - 5 \in \mathbb{Q}[x]$. Após algumas contas, obtemos o número racional

$$N \stackrel{\text{def}}{=} (1 + \sqrt[3]{5} + 2\sqrt[3]{25})(1 + \omega\sqrt[3]{5} + 2\omega^2\sqrt[3]{25})(1 + \omega^2\sqrt[3]{5} + 2\omega\sqrt[3]{25}) = 176$$

Por outro lado, M é uma expressão simétrica em $\omega\sqrt[3]{5}$, $\omega^2\sqrt[3]{5}$, raízes do polinômio

$$\frac{x^3 - 5}{x - \sqrt[3]{5}} = x^2 + \sqrt[3]{5}x + \sqrt[3]{25} \in \mathbb{Q}[\sqrt[3]{5}][x]$$

cujos coeficientes estão no anel $\mathbb{Q}[\sqrt[3]{5}] = \mathbb{Q} + \mathbb{Q}\sqrt[3]{5} + \mathbb{Q}\sqrt[3]{25}$ formado pelas expressões polinomiais em $\sqrt[3]{5}$ com coeficientes em $\mathbb{Q}$. Novamente pelo lema 1, temos $M \in \mathbb{Q}[\sqrt[3]{5}]$ e, de fato, após algumas contas,

$$M = -9 + 19\sqrt[3]{5} - \sqrt[3]{25} \in \mathbb{Q}[\sqrt[3]{5}]$$

Finalmente, obtemos a bonita expressão

$$\beta = \frac{(7 - 2\sqrt[3]{5})M}{N} = \frac{-53 + 151\sqrt[3]{5} - 45\sqrt[3]{25}}{176} \in \mathbb{Q}[\sqrt[3]{5}]$$

A prova do teorema no caso geral é análoga, ou seja, mostramos que

$$\frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha_1)\prod_{2 \leqslant i \leqslant d} g(\alpha_i)}{\prod_{1 \leqslant i \leqslant d} g(\alpha_i)} \in K[\alpha] = K + K\alpha + K\alpha^2 + \cdots + K\alpha^{d-1}$$

observando que o denominador $N = \prod_{1 \leqslant i \leqslant d} g(\alpha_i)$ é uma expressão polinomial simétrica nos conjugados de α, logo pertence a K, enquanto $M = \prod_{2 \leqslant i \leqslant d} g(\alpha_i)$ é simétrica nas raízes de $p(x)/(x - \alpha) \in K[\alpha][x]$, logo pertence a $K[\alpha]$. A prova está **quase** completa. O que está faltando? Falta mostrar que $N \neq 0$! Ou seja, que se $g(\alpha) \neq 0$ então $g(\alpha_i) \neq 0$ para todo $i = 1, 2, \ldots, d$. Mas isto segue do seguinte corolário imediato do menor divide:

Corolário 5 (Conjugados são algebricamente indistinguíveis)**.** *Seja $L \supseteq K$ uma extensão de corpos e sejam $\alpha, \alpha' \in L$ elementos algébricos sobre K, conjugados entre si. Dado $f \in K[x]$, temos*

$$f(\alpha) = 0 \iff f(\alpha') = 0$$

Apesar da aparência inocente, o último corolário é muito importante e nos conduz ao próximo conceito de nosso estudo: imersões.

5 Imersões

Sabendo que

$$\left(\frac{1}{2 - 3i} + 5i + \frac{1}{7}\right) \cdot \frac{(2 + i) \cdot \left(\frac{3}{4} - 5i\right)}{7 + 13i} = \frac{276099 - 158443i}{79352}$$

você pode dizer o valor de

$$\left(\frac{1}{2 + 3i} - 5i + \frac{1}{7}\right) \cdot \frac{(2 - i) \cdot \left(\frac{3}{4} + 5i\right)}{7 - 13i}?$$

É fácil! Como a segunda expressão é conjugada da primeira, não precisamos repetir as contas novamente, a resposta é simplesmente $(276099 + 158443i)/79352$. Este fenômeno merece uma atenção maior. As propriedades do mapa de conjugação

$$\begin{aligned} \tau \colon \mathbb{C} &\to \mathbb{C} \\ a + bi &\mapsto a - bi \qquad\qquad (a, b \in \mathbb{R}) \end{aligned}$$

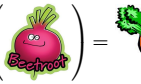
que utilizamos implicitamente no raciocínio acima são

$$\tau(z_1 + z_2) = \tau(z_1) + \tau(z_2) \tag{2}$$
$$\tau(z_1 z_2) = \tau(z_1)\tau(z_2) \tag{3}$$
$$\tau(z) = z \text{ para todo } z \in \mathbb{R} \tag{4}$$

Sejam $L_1 \supseteq K$ e $L_2 \supseteq K$ duas extensões de corpos. Dizemos que uma função $\tau \colon L_1 \hookrightarrow L_2$ é uma K-**imersão** se satisfaz as propriedades (1), (2) e (3′) $\tau(z) = z$ para $z \in K$. Uma K-imersão é sempre injetora (exercício!). Note ainda que se $\alpha \in L_1$ é algébrico sobre K, raiz do polinômio não nulo $f(x) \in K[x]$, então $\tau(\alpha)$ também é raiz de $f(x)$:

$$f(\alpha) = 0 \implies \tau(f(\alpha)) = 0 \implies f(\tau(\alpha)) = 0$$

Em outras palavras temos o **Princípio do Picles**: uma K-imersão conserva raízes de um mesmo polinômio em $K[x]$.

$\tau\left($  $\right) =$ 

Agora estamos prontos para caracterizar as K-imersões de uma **extensão algébrica simples** $L = K(\alpha) \supseteq K$. Como α gera L sobre K, tudo o que precisamos para descrever uma K-imersão $\sigma \colon L \hookrightarrow L'$ é dizer quem é a imagem $\sigma(\alpha) \in L'$ de α. A discussão acima restringe as possibilidades aos conjugados de α. Então por que não tentar definir $\sigma(r(\alpha)) = r(\alpha')$, em que $\alpha' \in L'$ é qualquer conjugado de α em L' e $r(\alpha)$ é uma função polinomial em α (vide teorema 4)? Bem, em primeiro lugar, há várias maneiras de se escrever um elemento de $K(\alpha)$ como expressão polinomial em α (por exemplo $i = i^2 + i + 1 = i^5$), de modo que a função acima pode não estar bem definida. Além disso, ainda precisamos garantir que a função acima é de fato uma K-imersão. Mas graças ao corolário 5, temos que $r(\alpha) = s(\alpha)$ (isto é, α é raiz de $r(x) - s(x) \in K[x]$) se, e só se, $r(\alpha') = s(\alpha')$. Desta forma, podemos de fato definir uma função via

$$\begin{aligned} \sigma \colon L &\hookrightarrow L' \\ r(\alpha) &\mapsto r(\alpha') \end{aligned}$$

Além disso, se temos uma igualdade de expressões polinomiais em α da forma $r(\alpha)s(\alpha) = t(\alpha)$, então $r(\alpha')s(\alpha') = t(\alpha')$, ou seja, σ preserva produto:

$$r(\alpha)s(\alpha) = t(\alpha) \implies \sigma(r(\alpha))\sigma(s(\alpha)) = \sigma(t(\alpha))$$

Analogamente, σ preserva soma. Resumimos este importante resultado, que enunciamos para $K = \mathbb{Q}$ por simplicidade:

Teorema 6 (Picles geral)**.** *Se $\alpha \in \mathbb{C}$ é raiz de um polinômio irredutível $p(x) \in \mathbb{Q}[x]$ de grau d, então existem exatamente d $\mathbb{Q}$-imersões de $\mathbb{Q}(\alpha)$ em $\mathbb{C}$, dadas por $\sigma(\alpha) = \alpha'$, em que α' é qualquer raiz de $p(x)$.*

6 Teorema do elemento primitivo

Tendo em vista a descrição completa das imersões de extensões simples de $\mathbb{Q}$ dada pelo teorema 6, o que podemos dizer sobre outras extensões? Felizmente, podemos reduzir nosso estudo ao caso anterior:

Teorema 7 (Elemento Primitivo)**.** *Seja $L = \mathbb{Q}(\gamma_1, \gamma_2, \ldots, \gamma_n)$ o corpo gerado por elementos $\gamma_i \in \mathbb{C}$ algébricos sobre $\mathbb{Q}$. Então existe um elemento $\theta \in L$ tal que $L = \mathbb{Q}(\theta)$.*

É suficiente provar o resultado para $n = 2$ já que o caso geral segue por indução. Então vamos supor que $L = \mathbb{Q}(\alpha, \beta)$. Sejam $p(x), q(x) \in \mathbb{Q}[x]$ os polinômios minimais de α e β, respectivamente, e $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ e $\beta_1 = \beta, \beta_2, \ldots, \beta_s$ os conjugados destes elementos (com $r = \deg p(x)$ e $s = \deg q(x)$) sobre $\mathbb{Q}$.
Bem, se queremos um único gerador sobre $\mathbb{Q}$ para $L = \mathbb{Q}(\alpha, \beta)$, por que não tentar um elemento da forma $\theta = \alpha + c\beta$ com $c \in \mathbb{Q}^\times$? Neste caso, claramente $\theta \in \mathbb{Q}(\alpha, \beta)$, logo $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$, e para provar a inclusão oposta basta mostrar que $\alpha \in \mathbb{Q}(\theta)$, pois daí $\beta = (\theta - \alpha)/c \in \mathbb{Q}(\theta)$ também, logo $L = \mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\theta)$.
Queremos portanto mostrar que, para algum $c \in \mathbb{Q}^\times$ e θ definido como acima, existe um polinômio $m(x) \in \mathbb{Q}[x]$ tal que $\alpha = m(\theta)$. Neste caso, se θ' é um conjugado de θ, aplicando a $\mathbb{Q}$-imersão dada por $\theta \mapsto \theta'$ à igualdade $\alpha = m(\theta)$, concluímos que $\alpha' \stackrel{\text{def}}{=} m(\theta')$ será um conjugado de α pois imersões preservam conjugados. Mas quem são os conjugados de θ? Podemos encontrar facilmente um polinômio em $\mathbb{Q}[x]$ que admite θ como raiz. Pelo lema 1,

$$t(x) = \prod_{i,j} (x - \alpha_i - c\beta_j) \in \mathbb{Q}[x]$$

Assim, os conjugados de θ formam um subconjunto de $\{\alpha_i + c\beta_j\}$, e seriam exatamente estes elementos se soubéssemos que $t(x)$ é irredutível em $\mathbb{Q}[x]$ (o que, infelizmente, não precisa ocorrer). Ainda assim, é possível construir um polinômio $m(x) \in \mathbb{Q}[x]$ tal que $m(\alpha_i + c\beta_j) = \alpha_i$. Vejamos como.
Escolhemos $c \in \mathbb{Q}$ tal que os rs elementos $\alpha_i + c\beta_j$ são todos distintos entre si. Para construir $m(x) \in K[x]$ tal que $m(\alpha_i + c\beta_j) = \alpha_i$, basta utilizar o **polinômio interpolador de Lagrange** correspondente: para $1 \leqslant u \leqslant r$ e $1 \leqslant v \leqslant s$, considere o polinômio mônico de grau $rs - 1$

$$h_{u,v}(x) \stackrel{\text{def}}{=} \prod_{\substack{(i,j) \neq (u,v) \\ 1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant s}} (x - \alpha_i - c\beta_j)$$

cujas raízes são todos os $\alpha_i + c\beta_j$ com exceção de $\alpha_u + c\beta_v$. Pela escolha de c, temos que $h_{u,v}(\alpha_u + c\beta_v) \neq 0$ enquanto $h_{u,v}(\alpha_i + c\beta_j) = 0$ se $(i, j) \neq (u, v)$. Assim, o polinômio

$$m(x) \stackrel{\text{def}}{=} \sum_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant s}} \frac{h_{i,j}(x)}{h_{i,j}(\alpha_i + c\beta_j)} \cdot \alpha_i$$

satisfaz $m(\alpha_i + c\beta_j) = \alpha_i$; além disso, seus coeficientes são simétricos com relação a $\alpha_1, \alpha_2, \ldots, \alpha_r$ e $\beta_1, \beta_2, \ldots, \beta_s$, logo $m(x) \in \mathbb{Q}[x]$, o que termina a prova.
A prova acima vale para todos os corpos de característica 0, mas em característica positiva existem extensões algébricas finitamente geradas que não são simples. Eis um ponto em que utilizamos uma simplificação da teoria geral ao trabalharmos com o corpo base $\mathbb{Q}$.

Exemplo 8. *O corpo (verifique!)*

$$\begin{aligned}\mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \mathbb{Q} + \mathbb{Q}\sqrt{2} + \mathbb{Q}\sqrt{3} + \mathbb{Q}\sqrt{6} \\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}\end{aligned}$$

pode ser gerado por $\theta = \sqrt{2} + \sqrt{3}$ sobre $\mathbb{Q}$. É claro que $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$; para mostrar a inclusão oposta, observe que

$$\theta^3 = 11\sqrt{2} + 9\sqrt{3} = 9\theta + 2\sqrt{2} \implies \sqrt{2} = \frac{\theta^3 - 9\theta}{2} \in \mathbb{Q}(\theta)$$

Logo $\sqrt{3} = \theta - \sqrt{2} \in \mathbb{Q}(\theta)$ também e portanto $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\theta)$. Os conjugados de θ estão entre $\pm\sqrt{2} \pm \sqrt{3}$. Considere o polinômio

$$\begin{aligned}&(x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}) \\ &= x^4 - 10x^2 + 1 \in \mathbb{Q}[x]\end{aligned}$$

Como ele não tem raízes racionais e nenhum de seus $\binom{4}{2} = 6$ fatores de grau 2 está em $\mathbb{Q}[x]$, concluímos que este polinômio é irredutível em $\mathbb{Q}[x]$ e portanto $\pm\sqrt{2} \pm \sqrt{3}$ são exatamente os conjugados de θ.

Agora que sabemos que toda extensão algébrica finitamente gerada de um corpo K de característica 0 é simples, podemos definir o **grau de uma extensão**: se $L = K(\alpha)$ e o polinômio minimal de α sobre K tem grau d, dizemos que a extensão $L \supseteq K$ tem grau d, em símbolos $d = [L : K]$. Observe que esta noção coincide com a noção usual $[L : K] = \dim_K L$, em que L é visto como um K-espaço vetorial: basta tomar $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ como base. Em particular, a noção de grau está bem definida, isto é, independe da escolha do elemento gerador α. O grau é multiplicativo no seguinte sentido:

Lema 9 (Graus)**.** *Se $E \supseteq L \supseteq K$ são extensões de corpos, então*

$$[E : K] = [E : L][L : K]$$

A demonstração é simples: se ω_i é uma base de E sobre L e τ_j, uma base de L sobre K, é fácil verificar que $\omega_i\tau_j$ é uma base de E sobre K.

7 Automorfismos e Extensões Galoisianas

Dada uma extensão de corpos $L \supseteq K$, um K-**automorfismo** de L é uma K-imersão $\sigma\colon L \to L$ cuja imagem é o próprio L. Em particular, K-automorfismos são bijetores, cujos inversos são também K-automorfismos. Dois K-automorfismos podem ser compostos, originando um novo K-automorfismo, e é fácil ver que o conjunto de todos os K-automorfismos de L formam um grupo com a operação de composição de funções.
De agora em diante, vamos trabalhar no caso em que $K = \mathbb{Q}$ ou um corpo de característica 0, de modo que possamos utilizar todos os resultados anteriores (teoremas 6 e 7). Dada uma extensão algébrica finitamente gerada $L \supseteq K$, há no máximo $[L : K]$ tais K-automorfismos. Se $L = K(\alpha)$ e todos os conjugados de α pertencem a L, então haverá **exatamente** $[L : K]$ automorfismos, dados por $\sigma(\alpha) = \alpha'$, em que α' é um conjugado de α. Se isto ocorrer, diremos que L é uma **extensão galoisiana** de K. Neste caso, denotamos o grupo de K-automorfismos de L por $\mathrm{Gal}(L/K)$. Assim, para uma extensão galoisiana $L \supseteq K$,

$$|\operatorname{Gal}(L/K)| = [L : K]$$

O jeito mais fácil (de fato, o único jeito) de se obter uma extensão galoisiana é acrescentar a K **todas** as raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ de um polinômio $p(x) \in K[x]$; neste caso, qualquer K-imersão de $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ permuta as raízes de $p(x)$, já que $p(\sigma(\alpha_i)) = \sigma(p(\alpha_i)) = 0$. Assim, $\sigma(L) = L$ e portanto σ é um K-automorfismo de L.

Exemplo 10.

- $\mathbb{C} \supseteq \mathbb{R}$ *é Galois e* $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{id, \sigma\}$ *em que id é a identidade e σ é a conjugação complexa.*
- $\mathbb{Q}(\sqrt{3}) = \mathbb{Q} + \mathbb{Q}\sqrt{3} \supseteq \mathbb{Q}$ *é Galois e* $\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{id, \sigma\}$ *em que id é a identidade e $\sigma(\sqrt{3}) = -\sqrt{3}$.*
- $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}$ *é Galois e pelo exemplo 8 temos $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Assim, há 4 automorfismos em $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, que levam $\sqrt{2} + \sqrt{3}$ em seus conjugados $\pm\sqrt{2} \pm \sqrt{3}$. Eles podem ser assim descritos:*

  $$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{id, \sigma, \tau, \sigma \circ \tau\}$$

  em que id é a identidade e

  $$\begin{aligned}\sigma(\sqrt{2}) &= \sqrt{2} & \tau(\sqrt{2}) &= -\sqrt{2} \\ \sigma(\sqrt{3}) &= -\sqrt{3} & \tau(\sqrt{3}) &= \sqrt{3}\end{aligned}$$

  Note que $\sigma^2 \stackrel{\text{def}}{=} \sigma \circ \sigma = id$, $\tau^2 = id$ e $\sigma\tau \stackrel{\text{def}}{=} \sigma \circ \tau = \tau\sigma$. Estas relações determinam o grupo $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ (que é isomorfo ao grupo aditivo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

Exemplo 11 (Extensões ciclotômicas)**.** *Seja p um primo e seja $\zeta_p = e^{2\pi i/p}$, uma raiz primitiva p-ésima da unidade. As $p - 1$ raízes p-ésimas da unidade*

$$\zeta_p, \zeta_p^2, \zeta_p^3, \ldots, \zeta_p^{p-1}$$

são conjugadas entre si sobre $\mathbb{Q}$, pois são raízes do polinômio $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, irredutível em $\mathbb{Q}[x]$ (pelo critério de Eisenstein 105 e o lema de Gauß 104 aplicados a $f(x + 1)$). Assim, $\mathbb{Q}(\zeta_p) \supseteq \mathbb{Q}$ é Galois e cada $a = 1, 2, \ldots, p - 1$ define um $\mathbb{Q}$-automorfismo

$$\begin{aligned}\sigma_a\colon \mathbb{Q}(\zeta_p) &\to \mathbb{Q}(\zeta_p) \\ \zeta_p &\mapsto \zeta_p^a\end{aligned}$$

Logo $|\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = p - 1$. Como

$$(\sigma_a \circ \sigma_b)(\zeta_p) = \sigma_a(\zeta_p^b) = \zeta_p^{ab} \implies \sigma_a \circ \sigma_b = \sigma_{ab \bmod p}$$

temos um isomorfismo de grupos

$$\begin{aligned}(\mathbb{Z}/p\mathbb{Z})^\times &\xrightarrow{\approx} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \\ \overline{a} &\mapsto \sigma_a\end{aligned}$$

Note que $(\mathbb{Z}/p\mathbb{Z})^\times$ é um grupo cíclico, gerado por uma raiz primitiva módulo p. Por exemplo, $(\mathbb{Z}/7\mathbb{Z})^\times = \langle\overline{3}\rangle$ e assim $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = \langle\sigma\rangle$ é um grupo cíclico de ordem 6, gerado pelo $\mathbb{Q}$-automorfismo dado por $\sigma(\zeta_7) = \zeta_7^3$.

Exemplo 12. *Seja $L = \mathbb{Q}(i, \sqrt[4]{5})$. Temos que $L \supseteq \mathbb{Q}$ é Galois (gerado pelas raízes de $x^4 - 5$) e $[L : \mathbb{Q}] = 8$. Você poderá verificar que*

$$\sigma(i) = -i \qquad \rho(i) = i$$
$$\sigma(\sqrt[4]{5}) = \sqrt[4]{5} \qquad \rho(\sqrt[4]{5}) = i\sqrt[4]{5}$$

definem $\mathbb{Q}$-automorfismos de L e que estes dois elementos geram $\mathrm{Gal}(L/\mathbb{Q})$*, mais precisamente*

$$\mathrm{Gal}(L/\mathbb{Q}) = \{id, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$$

Olhando para a ação sobre os geradores i e $\sqrt[4]{5}$ de L sobre $\mathbb{Q}$, é fácil verificar que $\sigma^2 = \rho^4 = id$ e que $\sigma\rho\sigma = \rho^{-1}$. Por exemplo,

$$\sigma\rho\sigma(i) = \sigma\rho(-i) = \sigma(-i) = i = \rho^{-1}(i)$$
$$\sigma\rho\sigma(\sqrt[4]{5}) = \sigma\rho(\sqrt[4]{5}) = \sigma(i\sqrt[4]{5}) = -i\sqrt[4]{5} = \rho^{-1}(\sqrt[4]{5})$$

(verifica-se que $\mathrm{Gal}(L/\mathbb{Q})$ *é isomorfo ao grupo diedral D_4, o grupo de simetrias do quadrado: ρ corresponde a uma rotação de 90° no sentido anti-horário e σ, a uma reflexão com eixo por dois vértices opostos de um quadrado).*

Exemplo 13. *Se $L = \mathbb{Q}(x_1, \ldots, x_n)$ é o* **corpo das funções racionais** *em $x_1, \ldots, x_n$ com coeficientes em $\mathbb{Q}$ e $K = \mathbb{Q}(s_1, s_2, \ldots, s_n)$, o* **subcorpo das funções racionais simétricas***, temos que as permutações das variáveis $x_1, \ldots, x_n$ definem K-automorfismos de L. Além disso, como estas variáveis são as raízes de*

$$\prod_{1 \leqslant i \leqslant n} (x - x_i) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n \in K[x]$$

temos que $L = K(x_1, x_2, \ldots, x_n)$ é uma extensão galoisiana de K. Claramente, $\mathrm{Gal}(L/K) \cong S_n$.

8 Teorema Fundamental

A ideia da teoria de Galois é classificar extensões de corpos através de seus grupos de automorfismos. Vejamos como.
Seja $L \supseteq K$ uma extensão de corpos. Podemos associar, para cada subcorpo intermediário E (isto é, $L \supseteq E \supseteq K$), o subgrupo do grupo de K-automorfismos de L que são também E-automorfismos de L, ou seja, o subgrupo dos automorfismos que fixam cada elemento de E. Reciprocamente, a cada subgrupo H do grupo de automorfismos de L sobre K, associamos o seu **corpo fixo**

$$L^H \stackrel{\text{def}}{=} \{x \in L \mid \sigma(x) = x \quad \forall \sigma \in H\}$$

É natural conjecturar que as duas correspondências acima são inversas uma da outra, o que é verdade se exigirmos que $L \supseteq K$ seja galoisiana. Neste caso, L é uma extensão galoisiana de E e temos que o grupo associado a E é nada mais nada menos do que $\mathrm{Gal}(L/E)$.
Antes de provarmos este fato, vamos deixar registrado o seguinte artifício, que nos ajuda a "criar" elementos no subcorpo fixo por um subgrupo do grupo de Galois.

Lema 14 (Truque das órbitas)**.** *Seja $L \supseteq K$ uma extensão de corpos e seja $G = \mathrm{Aut}(L/K)$ o grupo de K-automorfismos de L. Seja $\theta \in L$ e $H \leqslant G$ um subgrupo finito. Então*

$$f(x) \stackrel{\text{def}}{=} \prod_{\sigma \in H} (x - \sigma(\theta)) \in L^H[x]$$

Em particular, o polinômio minimal de θ sobre L^H divide $f(x)$.

A prova do lema é uma aplicação do "gira-gira": se $\sigma \in H$, então $\tau \mapsto \sigma\tau$ é uma bijeção de H em H, ou seja, aplicando σ ao produto que define $f(x)$, apenas permutamos seus fatores, logo seus coeficientes são invariantes por H.

Teorema 15 (Teorema Fundamental da Teoria de Galois)**.** *Seja $L \supseteq K$ uma extensão galoisiana. Há uma bijeção entre os subcorpos intermediários E de $L \supseteq K$ e os subgrupos de* $\mathrm{Gal}(L/K)$*, dada por*

$$\left\{ \begin{array}{c} \text{subgrupos} \\ H \leqslant \mathrm{Gal}(L/K) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subcorpos intermediários} \\ E \text{ de } L \supseteq K \end{array} \right\}$$
$$H \longmapsto L^H$$
$$\mathrm{Gal}(L/E) \longleftarrow\!\shortmid E$$

Demonstração. Seja E um subcorpo de intermediário de $L \supseteq K$. Começamos mostrando que a associação

$$E \mapsto H \stackrel{\text{def}}{=} \mathrm{Gal}(L/E) \mapsto L^{\mathrm{Gal}(L/E)} = L^H$$

é a identidade. Pela definição, sabemos que $L^H \supseteq E$. Para mostrar a inclusão reversa, escrevemos $L = E(\theta)$ pelo teorema do elemento primitivo 7.
Seja $p(x) \in E[x]$ o polinômio minimal de θ sobre E e sejam $\theta_1 = \theta, \theta_2, \ldots, \theta_r$ as raízes conjugadas de θ, que pertencem a L pois $L \supseteq E$ é uma extensão galoisiana. Os automorfismos em $H = \mathrm{Gal}(L/E)$ são dados por $\sigma_i(\theta) = \theta_i$, $i = 1, 2, \ldots, r$.
Agora, seja $\ell \in L^H$ e escreva $\ell = l(\theta)$ para algum polinômio $l[x] \in E[x]$. Temos

$$\ell = \frac{1}{r} \sum_{\sigma \in H} \sigma(\ell) = \frac{l(\theta_1) + l(\theta_2) + \cdots + l(\theta_r)}{r} \in E$$

que é um elemento de E já que é uma expressão simétrica das raízes θ_i de $p(x) \in E[x]$. Portanto $L^H \subseteq E$, assim, $L^H = E$.
Em seguida, dado um subgrupo $H \leqslant \mathrm{Gal}(L/K)$, devemos mostrar que a associação

$$H \mapsto E \stackrel{\text{def}}{=} L^H \mapsto \mathrm{Gal}(L/L^H) = \mathrm{Gal}(L/E)$$

é a identidade. Claramente $H \subseteq \mathrm{Gal}(L/E)$. Novamente, escrevemos $L = E(\theta)$. Pelo truque das órbitas (lema 135), sabemos que θ é raiz de um polinômio em $E[x]$ de grau $|H|$, logo $|\mathrm{Gal}(L/E)| = [L : E] \leqslant |H|$. Da inclusão anterior, concluímos que $H = \mathrm{Gal}(L/E)$. □

9 Exemplos

Um ditado popular diz

$$1 \text{ exemplo} > 10^3 \text{ palavras}$$

então deixe-me tentar desta maneira.

Exemplo 16. *Seja $\zeta = e^{2\pi i/5}$. Pelo exemplo 11, sabemos que* $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{id, \sigma, \sigma^2, \sigma^3\}$ *em que $\sigma(\zeta) = \zeta^2$ (pois 2 é uma raiz primitiva módulo 5). Os subgrupos de* $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ *são portanto* $\{1\}$, $\{1, \sigma^2\}$ *e* $\{1, \sigma, \sigma^2, \sigma^3\}$*. Os corpos fixos correspondentes estão listados a seguir:*

$$\begin{array}{ccc} \{1\} & \longleftrightarrow & \mathbb{Q}(\zeta) \\ \cap & & \cup \\ \{1, \sigma^2\} & \longleftrightarrow & \mathbb{Q}(\zeta^2 + \zeta^3) \\ \cap & & \cup \\ \{1, \sigma, \sigma^2, \sigma^3\} & \longleftrightarrow & \mathbb{Q} \end{array}$$

Para determinar o polinômio minimal de $\zeta^2 + \zeta^3$ sobre $\mathbb{Q}$, basta utilizar o truque das órbitas; os coeficientes do próximo polinômio são σ-invariantes, logo pertencem a $\mathbb{Q}$:

$$\begin{aligned} \big(x - (\zeta^2 + \zeta^3)\big)\big(x - \sigma(\zeta^2 + \zeta^3)\big) &= \big(x - (\zeta^2 + \zeta^3)\big)\big(x - (\zeta^4 + \zeta)\big) \\ &= x^2 + x - 1 \end{aligned}$$

O polinômio minimal de ζ sobre $\mathbb{Q}(\zeta^2 + \zeta^3)$ é obtido da mesma forma:

$$(x - \zeta)\big(x - \sigma^2(\zeta)\big) = (x - \zeta)\big(x - \zeta^4\big) = x^2 + \big(1 + \zeta^2 + \zeta^3\big)x + 1$$

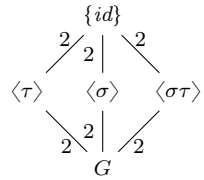
Utilizando estes dois polinômios, juntamente com o fato de $\zeta^2 + \zeta^3 = 2\cos 4\pi/5 < 0$ e $\Im(\zeta) = \operatorname{sen} 2\pi/5 > 0$, podemos calcular

$$\zeta^2 + \zeta^3 = \frac{-1 - \sqrt{5}}{2} \qquad e \qquad \zeta = \frac{\frac{-1+\sqrt{5}}{2} + i\sqrt{\frac{5+\sqrt{5}}{2}}}{2}$$

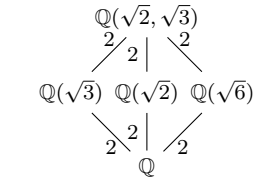
Exemplo 17. *Vimos antes que o grupo de Galois da extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}$ é $G \stackrel{\text{def}}{=} \mathrm{Gal}\big(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\big) = \{id, \sigma, \tau, \sigma\tau\}$ em que σ e τ são dados por*

$$\sigma(\sqrt{2}) = \sqrt{2} \qquad \tau(\sqrt{2}) = -\sqrt{2}$$
$$\sigma(\sqrt{3}) = -\sqrt{3} \qquad \tau(\sqrt{3}) = \sqrt{3}$$

Os subgrupos de G estão representados pelo seguinte reticulado ou diagrama de Haße, em que um traço indica a relação de continência (com subgrupos maiores desenhados abaixo) e os números indicam os índices do subgrupo menor dentro do maior:



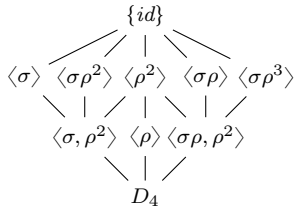
Cada um destes subgrupos corresponde a um subcorpo intermediário, a saber, o subcorpo de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ fixo (ponto a ponto) pelos elementos do subgrupo. O diagrama nos diz que há exatamente 3 subcorpos intermediários diferentes de $\mathbb{Q}$ e $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ e é fácil "chutá-los": $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ e $\mathbb{Q}(\sqrt{6})$. Agora só falta determinar qual corpo corresponde a qual subgrupo, o que também é fácil: σ fixa $\sqrt{2}$, logo fixa $\mathbb{Q}(\sqrt{2})$ também; τ fixa $\sqrt{3}$, logo fixa $\mathbb{Q}(\sqrt{3})$ também; finalmente, $\sigma\tau$ fixa $\sqrt{6}$ e portanto $\mathbb{Q}(\sqrt{6})$. Resumindo, temos o diagrama de corpos (desenhado na ordem da correspondência), em que os números representam os graus das extensões:



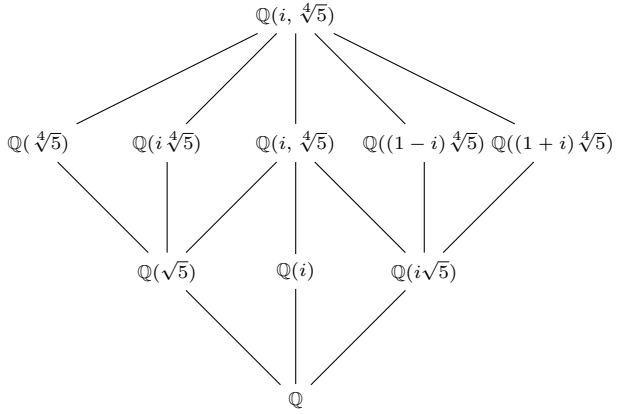
Exemplo 18. *Vimos no exemplo 12 que o grupo de Galois da extensão $\mathbb{Q}(i,\sqrt[4]{5}) \supseteq \mathbb{Q}$ é isomorfo a $D_4 = \langle \rho, \sigma \rangle$, que é gerado pelos $\mathbb{Q}$-automorfismos σ (reflexão) e ρ (rotação) dados por*

$$\sigma(i) = -i \qquad \rho(i) = i$$
$$\sigma(\sqrt[4]{5}) = \sqrt[4]{5} \qquad \rho(\sqrt[4]{5}) = i\sqrt[4]{5}$$

O reticulado de subgrupos de D_4 é ilustrado a seguir (aqui $\langle g \rangle$ é o subgrupo gerado por g):



Os subcorpos intermediários correspondentes são:



É fácil adivinhar vários dos subcorpos acima e, utilizando as descrições explícitas dos automorfismos ρ e σ e os graus das extensões, determinar suas posições corretas no diagrama. Por exemplo, como $[\mathbb{Q}(i\sqrt[4]{5}) : \mathbb{Q}] = 4$ (pois o polinômio minimal de $i\sqrt[4]{5}$ sobre $\mathbb{Q}$ é x^4-5), sabemos que $\mathbb{Q}(i\sqrt[4]{5})$ deve ser colocado no "segundo andar", onde moram todos os corpos intermediários de grau 4 sobre $\mathbb{Q}$. Por outro lado, de

$$\sigma\rho^2(i\sqrt[4]{5}) = \sigma\rho(-\sqrt[4]{5}) = \sigma(-i\sqrt[4]{5}) = i\sqrt[4]{5}$$

vemos que $\mathbb{Q}(i\sqrt[4]{5}) \subseteq \mathbb{Q}(i,\sqrt[4]{5})^{\langle\sigma\rho^2\rangle}$ e comparando graus, concluímos que esta inclusão é uma igualdade.

Os únicos subcorpos "não óbvios" são os fixos por $\langle\sigma\rho\rangle$ e $\langle\sigma\rho^3\rangle$. Mas podemos encontrá-los usando o truque das órbitas. Por exemplo, para o subcorpo fixo por $\langle\sigma\rho\rangle$, temos

$$\sqrt[4]{5} + \sigma\rho(\sqrt[4]{5}) = (1-i)\sqrt[4]{5} \in \mathbb{Q}(i,\sqrt[4]{5})^{\langle\sigma\rho\rangle}$$

Logo, pelo lema de Graus,

$$[\mathbb{Q}\big((1-i)\sqrt[4]{5}\big) : \mathbb{Q}] \mid [\mathbb{Q}(i,\sqrt[4]{5})^{\langle\sigma\rho\rangle} : \mathbb{Q}] = [D_4 : \langle\sigma\rho\rangle] = 4$$

e para concluir que $[\mathbb{Q}\big((1-i)\sqrt[4]{5}\big) : \mathbb{Q}] = 4$, e portanto que $\mathbb{Q}(i,\sqrt[4]{5})^{\langle\sigma\rho\rangle} = \mathbb{Q}\big((1-i)\sqrt[4]{5}\big)$, basta mostrar que $[\mathbb{Q}\big((1-i)\sqrt[4]{5}\big) : \mathbb{Q}] \nmid 2$, ou seja, que $(1-i)\sqrt[4]{5}$ não pertence a nenhuma extensão quadrática de $\mathbb{Q}$. Mas, pelo reticulado de subgrupos de D_4 e a correspondência de Galois, a única extensão quadrática de $\mathbb{Q}$ contida em $\mathbb{Q}(i,\sqrt[4]{5})^{\langle\sigma\rho\rangle}$ é $\mathbb{Q}(i,\sqrt[4]{5})^{\langle\rho^2,\sigma\rho\rangle} = \mathbb{Q}(i\sqrt{5})$. Agora, basta checar que ρ^2 não fixa $(1-i)\sqrt[4]{5}$ para concluir que $\mathbb{Q}(i\sqrt{5}) \neq \mathbb{Q}((1-i)\sqrt[4]{5})$:

$$\rho^2\big((1-i)\sqrt[4]{5}\big) = \rho\big((1-i)i\sqrt[4]{5}\big) = -(1-i)\sqrt[4]{5}$$

10 Gauß e o heptadecágono regular

O próximo exemplo é devido a Gauß; ele mostra que é possível construir o polígono regular de 17 lados apenas com régua e compasso (ver teorema 124 do apêndice).
Seja $\zeta = e^{2\pi i/17}$. Pelo exemplo 11 há um isomorfismo

$$(\mathbb{Z}/17\mathbb{Z})^\times \xrightarrow{\approx} \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$
$$\overline{a} \mapsto (\zeta \mapsto \zeta^a)$$

Assim, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ é gerado pelo $\mathbb{Q}$-automorfismo dado por $\sigma(\zeta) = \zeta^3$, já que 3 é raiz primitiva módulo 17. Há exatamente um único subgrupo de ordem d para cada divisor positivo d de 16:

subgrupos	1	$\leqslant$	$\langle\sigma^8\rangle$	$\leqslant$	$\langle\sigma^4\rangle$	$\leqslant$	$\langle\sigma^2\rangle$	$\leqslant$	$\langle\sigma\rangle = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$
ordens	1		2		4		8		16

Sendo $L_i \overset{\text{def}}{=} \mathbb{Q}(\zeta)^{\langle\sigma^{2^i}\rangle}$ para $i = 0, 1, \ldots, 4$, obtemos portanto uma torre de extensões quadráticas

$$\mathbb{Q}(\zeta) = L_4 \supset L_3 \supset L_2 \supset L_1 \supset L_0 = \mathbb{Q} \qquad ([L_{i+1} : L_i] = 2)$$

Vamos determinar explicitamente estes subcorpos intermediários utilizando o truque das órbitas:

- $L_1 = \mathbb{Q}(\alpha)$ em que

$$\alpha \overset{\text{def}}{=} \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + \zeta^4 + \zeta^{-4} + \zeta^8 + \zeta^{-8}$$
$$= 2\cos\frac{2\pi}{17} + 2\cos\frac{4\pi}{17} + 2\cos\frac{8\pi}{17} + 2\cos\frac{16\pi}{17} > 0$$

  é a soma da σ^2-órbita de ζ (já que $\sigma^2(\zeta) = \zeta^{3^2} = \zeta^9 = \zeta^{-8}$). Como $\alpha \in L_1$ (pois é σ^2-invariante) e como $[L_1 : \mathbb{Q}] = 2$, basta mostrar que $\alpha \notin \mathbb{Q}$ para concluir que $L_1 = \mathbb{Q}(\alpha)$. Mas isto segue do fato de α não ser fixo por σ:

$$\beta \overset{\text{def}}{=} \sigma(\alpha) = \zeta^3 + \zeta^{-3} + \zeta^6 + \zeta^{-6} + \zeta^5 + \zeta^{-5} + \zeta^7 + \zeta^{-7}$$
$$= 2\cos\frac{6\pi}{17} + 2\cos\frac{12\pi}{17} + 2\cos\frac{10\pi}{17} + 2\cos\frac{14\pi}{17} < 0$$

- $L_2 = L_1(\gamma)$ em que

$$\gamma \overset{\text{def}}{=} \zeta + \zeta^{-1} + \zeta^{-4} + \zeta^4 = 2\cos\frac{2\pi}{17} + 2\cos\frac{8\pi}{17} > 0$$

  é a soma da σ^4-órbita de ζ (já que $\sigma^4(\zeta) = \zeta^{3^4} = \zeta^{-4}$). Como $\gamma \in L_2$ por construção e $[L_2 : L_1] = 2$, basta mostrar que $\gamma \notin L_1$ para concluir que $L_2 = L_1(\gamma)$. E, de fato, γ não é σ^2-invariante:

$$\delta \overset{\text{def}}{=} \sigma^2(\gamma) = \zeta^8 + \zeta^{-8} + \zeta^2 + \zeta^{-2} = 2\cos\frac{16\pi}{17} + 2\cos\frac{4\pi}{17} < 0$$

- $L_3 = L_2(\zeta + \zeta^{-1})$. De fato, como $\sigma^8(\zeta) = \zeta^{3^8} = \zeta^{-1}$, σ^8 fixa $\zeta + \zeta^{-1} = 2\cos(2\pi/17)$. Por outro lado,

$$\sigma^4(\zeta + \zeta^{-1}) = \zeta^4 + \zeta^{-4} = 2\cos\frac{8\pi}{17} \neq 2\cos\frac{2\pi}{17} = \zeta + \zeta^{-1}$$

  e portanto $\zeta + \zeta^{-1} \notin L_2$. Assim, $L_3 = L_2(\zeta + \zeta^{-1})$.

Temos portanto uma torre de extensões quadráticas

$$L_4 = \mathbb{Q}(\zeta) \supset L_3 = L_2(\zeta+\zeta^{-1}) \supset L_2 = L_1(\gamma) \supset L_1 = \mathbb{Q}(\alpha) \supset L_0 = \mathbb{Q}$$

Note que todas estas extensões quadráticas são automaticamente Galois e que

$$\mathrm{Gal}(L_{i+1}/L_i) = \{\mathrm{id}, \sigma^{2^i}|_{L_{i+1}}\}$$

Portanto α, γ e $2\cos(2\pi/17) = \zeta + \zeta^{-1}$ são respectivamente as raízes dos polinômios quadráticos

$$f(x) \overset{\text{def}}{=} (x-\alpha)(x-\sigma(\alpha)) = (x-\alpha)(x-\beta) \in \mathbb{Q}[x]$$
$$g(x) \overset{\text{def}}{=} (x-\gamma)(x-\sigma^2(\gamma)) = (x-\gamma)(x-\delta) \in L_1[x]$$
$$h(x) \overset{\text{def}}{=} (x - 2\cos(2\pi/17))(x - \sigma^4(2\cos(2\pi/17))) \in L_2[x]$$

Vamos determinar expressões explícitas para α, γ e $2\cos(2\pi/17)$ resolvendo estas equações. Para isto, utilizaremos diversas vezes a identidade

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{16} = 0 \qquad (*)$$

- Multiplicando $(*)$ por ζ^{-8} obtemos

  $$1 + \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + \cdots + \zeta^8 + \zeta^{-8} = 0 \iff \alpha + \beta = -1$$

  O produto $\alpha\beta$ consiste em uma soma com 64 termos da forma $\zeta^{\pm n}$ com n um dos valores (módulo 17) na seguinte tabela:

$+$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$-\overline{1}$	$-\overline{2}$	$-\overline{4}$	$-\overline{8}$
$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{7}$	$-\overline{6}$	$\overline{2}$	$\overline{1}$	$-\overline{1}$	$-\overline{5}$
$\overline{5}$	$\overline{6}$	$\overline{7}$	$-\overline{8}$	$-\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{1}$	$-\overline{3}$
$\overline{6}$	$\overline{7}$	$\overline{8}$	$-\overline{7}$	$-\overline{3}$	$\overline{5}$	$\overline{4}$	$\overline{2}$	$-\overline{2}$
$\overline{7}$	$\overline{8}$	$-\overline{8}$	$-\overline{6}$	$-\overline{2}$	$\overline{6}$	$\overline{5}$	$\overline{3}$	$-\overline{1}$

  Novamente por $(*)$, $\alpha\beta = -4$. Logo

  $$f(x) = x^2 + x - 4$$

  e assim

  $$\alpha = \frac{-1+\sqrt{17}}{2} \qquad \beta = \frac{-1-\sqrt{17}}{2}$$

  (aqui é necessário utilizar o fato de que $\alpha > 0$ e $\beta < 0$ para decidir quem é quem, pois do ponto de vista algébrico dois conjugados sobre $\mathbb{Q}$ são indistinguíveis).

- Temos $\gamma+\delta=\alpha$. Por outro lado, $\gamma\delta$ é a soma de 16 termos da forma ζ^n com n mod 17 uma entrada na tabela:

$+$	$\overline{1}$	$\overline{4}$	$-\overline{1}$	$-\overline{4}$
$\overline{2}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$-\overline{2}$
$\overline{8}$	$-\overline{8}$	$-\overline{5}$	$\overline{7}$	$\overline{4}$
$-\overline{2}$	$-\overline{1}$	$\overline{2}$	$-\overline{3}$	$-\overline{6}$
$-\overline{8}$	$-\overline{7}$	$-\overline{4}$	$\overline{8}$	$\overline{5}$

  Logo $\gamma\delta=-1$ por $(*)$. Assim,

$$g(x)=x^2-\alpha x-1\in L_1[x]$$

  e como $\gamma>0$ temos

$$\gamma=\frac{\alpha+\sqrt{\alpha^2+4}}{2}=\frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}}{4}$$

- Temos $h(x)=x^2-\gamma x+\nu$ em que

$$\nu\stackrel{\text{def}}{=}\sigma(\gamma)=\zeta^3+\zeta^{-3}+\zeta^{-5}+\zeta^5=2\cos\frac{6\pi}{17}+2\cos\frac{10\pi}{17}>0$$

  Aplicando σ a

$$g(x)=(x-\gamma)(x-\delta)=x^2-\alpha x-1$$

  obtemos que $\nu=\sigma(\gamma)$ e $\sigma(\delta)$ são raízes de $g^\sigma(x)=x^2-\beta x-1\in L_1[x]$ e portanto

$$\nu=\frac{\beta+\sqrt{\beta^2+4}}{2}=\frac{-1-\sqrt{17}+\sqrt{34+2\sqrt{17}}}{4}$$

  Como $\zeta+\zeta^{-1}$ é uma raiz positiva de $h(x)$, temos

$$2\cos\frac{2\pi}{17}=\zeta+\zeta^{-1}=\frac{\gamma+\sqrt{\gamma^2-4\nu}}{2}$$

Finalmente, juntando tudo, obtemos a singela expressão

$$\cos\frac{2\pi}{17}=\frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}}{16}$$

que mostra que o heptadecágono regular é construtível com régua e compasso!

11 Exercícios

1. Escreva $x^2y^2+y^2z^2+z^2x^2$ e $x^3y+xy^3+x^3z+xz^3+y^3z+yz^3$ em termos de polinômios simétricos elementares.
2. Dado um polinômio $f(x)\in K[x]$ com raízes $\alpha_1,\ldots,\alpha_n$, , seu **discriminante** é $\Delta_f\stackrel{\text{def}}{=}\prod_{1\leqslant i<j\leqslant n}(\alpha_i-\alpha_j)^2$, uma expressão simétrica das raízes de f. Mostre que os discriminantes de x^3+px+q, x^4+px^2+r e x^4+qx+r são respectivamente iguais a $-\left(4p^3+27q^2\right)$, $16r\left(p^2-4r\right)^2$ e $-27q^4+256r^3$.
3. Mostre que $\cos 20^\circ$ e $\cos(2\pi/7)$ são algébricos sobre $\mathbb{Q}$. Determine os polinômios minimais sobre $\mathbb{Q}$.
4. Mostre que as seguintes extensões são Galois e determine o grupo de Galois correpondente. Encontre todos os subcorpos intermediários.

   (a) $\mathbb{Q}(\cos 20^\circ)\supseteq\mathbb{Q}$
   (b) $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})\supseteq\mathbb{Q}$
   (c) $\mathbb{Q}(\sqrt{2+\sqrt{2}})\supseteq\mathbb{Q}$
   (d) $\mathbb{Q}(e^{2\pi i/13})\supseteq\mathbb{Q}$

5. Prove: $\cos 3^\circ=\dfrac{2(1+\sqrt{3})\sqrt{5+\sqrt{5}}+(\sqrt{6}-\sqrt{2})(\sqrt{5}-1)}{16}$
6. Seja $f(x)\in K[x]$ e suponha que seu discriminante Δ_f seja um quadrado perfeito no corpo K. Mostre que o grupo de Galois do corpo gerado pelas raízes de f sobre K só contém permutações pares destas raízes.
7. Calcule o grupo de Galois do corpo gerado pelas raízes dos seguintes polinômios sobre $\mathbb{Q}$.

   (a) x^2-x+1
   (b) x^8-2
   (c) x^4-2x^2-2
   (d) x^3+x^2-2x-1
   (e) x^3-3x+1
   (f) x^3-2
   (g) $x^3+27x-4$
   (h) x^3+x+1
   (i) $x^3+3x+14$
   (j) $x^3-21x+7$
   (k) x^3-3x^2+1

8. Mostre que se $p(x)$ é irredutível em $\mathbb{Q}[x]$, seu grupo de Galois (i.e., o grupo de Galois da extensão de $\mathbb{Q}$ gerada por suas raízes) é transitivo: se r e r' são raízes de $p(x)$, existe um automorfismo tal que $\sigma(r)=r'$.
9. Mostre que se um polinômio $f(x)\in\mathbb{Q}[x]$ de grau 3 é tal que o grupo de Galois de seu corpo de raízes sobre $\mathbb{Q}$ é cíclico de ordem 3, então $f(x)$ só tem raízes reais.

12 Apêndice

12.1 Grupos

Definição 19. *Um* **grupo** $(G,\cdot)$ *é um par formado por um conjunto G e uma operação binária, chamada* **produto**,

$$G\times G\to G$$
$$(a,b)\mapsto a\cdot b,$$

que satisfaz os seguintes três axiomas:

(i) (Associatividade) Para quaisquer $a,b,c\in G$, $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

(ii) (Existência de elemento neutro) Existe um elemento $e\in G$ tal que, para todo $a\in G$, $a\cdot e=e\cdot a=a$.

(iii) (Existência de inverso) Dado $a\in G$, existe um elemento $a^{-1}\in G$ tal que $a\cdot a^{-1}=a^{-1}\cdot a=e$.

Se, além dos três axiomas acima, o grupo $(G,\cdot)$ satisfaz

(iv) (Comutatividade) Para quaisquer $a,b\in G$, $a\cdot b=b\cdot a$.

então dizemos que este grupo é **abeliano**[1].

Exemplo 20 (Grupo simétrico)**.** *Seja X um conjunto. Então*

$$S_X=\{f\colon X\to X\mid f\text{ é bijetor}\}$$

juntamente com a operação $\circ$ (composição de funções) é um grupo, chamado de **grupo simétrico**. *Quando $X=\{1,2,\ldots,n\}$, abreviaremos S_X por S_n. Temos $|S_n|=n!$ e S_n é abeliano apenas para $n=1,2$.*
Há várias maneiras de se representar uma permutação. Por exemplo, considere $\pi\in S_5$ dada por

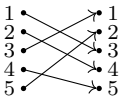
$$\pi(1)=3,\ \pi(2)=4,\ \pi(3)=1,\ \pi(4)=5,\ \pi(5)=2$$

Podemos representar π de uma das seguintes formas:

(a) Notação por matriz 2×5

$$\pi=\begin{pmatrix}1&2&3&4&5\\3&4&1&5&2\end{pmatrix}$$

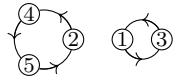
que corresponde pictoricamente a



(b) Notação por produto de ciclos disjuntos

$$\pi=(13)(245)=(245)(13)=(31)(452)=(245)(13)$$

correspondente ao grafo



(c) Notação por matriz de permutação

$$T_\pi=\begin{pmatrix}0&0&1&0&0\\0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&0&1&0\end{pmatrix}$$

Definição 21. *Um grupo G é dito* **cíclico** *se ele puder ser gerado por um único elemento $g\in G$ (em geral, há vários geradores g):*

$$G=\langle g\rangle=g^{\mathbb{Z}}\stackrel{\text{def}}{=}\{g^n\mid n\in\mathbb{Z}\}$$

Definição 22. *Dado um grupo $(G,\cdot)$, um subconjunto $H\subseteq G$ é um* **subgrupo** *de G (notação: $H\leqslant G$) se satisfaz*

(i) $H\neq\varnothing$;

(ii) H é fechado por produto: $a,b\in H\implies a\cdot b\in H$; e

(iii) H é fechado por inverso: $a\in H\implies a^{-1}\in H$.

Note que o subconjunto H faz jus ao nome "subgrupo" visto que, por (ii), a operação $\cdot$ de G se restringe a uma operação binária $\cdot\colon H\times H\to H$ e faz do par $(H,\cdot)$ um legítimo grupo.

Definição 23. *Seja G um grupo e seja $g\in G$.*

[1] em homenagem ao matemático norueguês Niels Henrik Abel (1802–1829), que também dá nome ao prestigioso prêmio Abel.

(a) *a* **ordem** $|G|$ *do grupo* G *é a cardinalidade de* G *(i.e., a quantidade de elementos em* G*).*

(b) *a* **ordem** *do elemento* $g \in G$ *é a ordem do subgrupo cíclico* $\langle g \rangle$*. Equivalentemente, a ordem de* g *é o menor inteiro* $d > 0$ *tal que* $g^d = e$ *(ou infinita se tal* d *não existe).*

Lema 24 (Menor divide)**.** *Sejam* G *um grupo e* $g \in G$ *um elemento com ordem finita* $d > 0$*. Então*

$$g^n = e \iff d \mid n \qquad (n \in \mathbb{Z})$$

Definição 25. *Sejam* G *um grupo e* $H \leqslant G$ *um subgrupo. Um translado à esquerda de* H*, i.e., um subconjunto de* G *da forma*

$$\lambda_g(H) = g \cdot H = \{gh \mid h \in H\} \qquad \text{para algum } g \in G$$

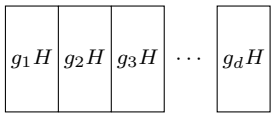
é chamado de **classe lateral à esquerda** *ou* **coclasse à esquerda** *de* H*. Analogamente, uma* **classe lateral à direita** *ou* **coclasse à direita** *de* H *é um subconjunto de* G *da forma* $\rho_g(H) = H \cdot g$ *para algum* $g \in G$*. Denotaremos os conjuntos das coclasses de* H *à esquerda e à direita respectivamente por* $G/H \stackrel{\text{def}}{=} \{g \cdot H \mid g \in G\}$ *e* $H\backslash G \stackrel{\text{def}}{=} \{H \cdot g \mid g \in G\}$*.*

Teorema 26 (Lagrange)**.** *Seja* G *um grupo e seja* $H \leqslant G$ *um subgrupo. Então as classes laterais à esquerda de* H *equiparticionam* G*, i.e.,*

(i) *As classes laterais à esquerda de* H *formam uma partição de* G*.*

(ii) *Quaisquer duas classes laterais à esquerda de* H *têm mesma cardinalidade.*

Em particular, se G *é finito, então* $|G|$ *é um múltiplo de* $|H|$*. Mais precisamente,* $|G| = d \cdot |H|$ *com* $d = |G/H|$*:*



Corolário 27 (também chamado de "Lagrange")**.** *Seja* G *um grupo finito. Então a ordem de qualquer elemento* $g \in G$ *divide* $n = |G|$*. Em particular, para todo* $g \in G$*, temos* $g^n = e$*.*

Definição 28. *Dados dois grupos* $(G, \cdot)$ *e* $(H, *)$*, um* **homomorfismo** *(ou simplesmente* **morfismo***)* $\varphi\colon G \to H$ *é uma função que preserva produtos, i.e.,* $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$ $(a, b \in G)$*.*

Definição 29. *Sejam* G *e* H *dois grupos.*

(i) *Um* **isomorfismo** $\varphi\colon G \to H$ *é um morfismo de grupos bijetor (a função inversa* $\varphi^{-1}\colon H \to G$ *é também um isomorfismo automaticamente). Denotaremos um isomorfismo entre* G *e* H *por* $\varphi\colon G \xrightarrow{\approx} H$*.*

(ii) *Dizemos que* G *e* H *são* **isomorfos** *(notação:* $G \cong H$ *ou* $G \approx H$*) se existe algum isomorfismo entre eles (pode haver mais de um isomorfismo). Intuitivamente, dois grupos isomorfismos são o "mesmo" a menos do nome de seus elementos.*

(iii) *Um* **automorfismo** *de* G *é um isomorfismo* $\varphi\colon G \xrightarrow{\approx} G$*. O conjunto de todos os automorfismos de* G *é denotado*

$$\operatorname{Aut}(G) \stackrel{\text{def}}{=} \{\varphi\colon G \xrightarrow{\approx} G \mid \varphi \text{ é automorfismo }\}$$

e é um grupo com a operação de composição de funções $\circ$*.*

A pré-imagem do subgrupo trivial de H é um subgrupo de G, chamado de **kernel** ou **núcleo** de φ:

$$\ker\varphi \stackrel{\text{def}}{=} \varphi^{-1}(e) = \{g \in G \mid \varphi(g) = e\}$$

Lema 30 (Kernel e injetividade)**.** *Seja* $\varphi\colon G \to H$ *um morfismo de grupos. Então* φ *é injetor se, e só se,* $\ker\phi = \{e\}$*.*

Exemplo 31 (Conjugação)**.** *Seja* G *um grupo e fixe* $g \in G$*. Então*

$$\begin{aligned} \kappa_g\colon G &\to G \\ x &\mapsto gxg^{-1} \end{aligned}$$

é um automorfismo de G*, chamado de* **conjugação** *por* g*.*

Exemplo 32 (Morfismo paridade)**.** *Considere o polinômio*

$$d(x_1, \ldots, x_n) \stackrel{\text{def}}{=} \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)$$

Note que um elemento $\sigma \in S_n$ *age sobre* d*, permutando suas variáveis:* $\sigma(d(x_1, \ldots, x_n)) \stackrel{\text{def}}{=} d(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$*. E como* σ *permuta também os subconjuntos* $\{i, j\} \subseteq \{1, \ldots, n\}$ *de dois elementos, os fatores de* $\sigma(d)$ *são os mesmos de* d *a menos de sinal, logo*

$$\sigma(d) = \prod_{1 \leqslant i < j \leqslant n} (x_{\sigma(i)} - x_{\sigma(j)}) = \pm d$$

Definimos o **morfismo paridade** $\Pi\colon S_n \to \{\pm 1\}$ *por* $\Pi(\sigma) = \sigma(d)/d$*. Denotamos* $\Pi(\sigma)$ *também por* $(-1)^\sigma$ *e dizemos que* σ *é par (respectivamente ímpar) se* $\Pi(\sigma) = 1$ *(respectivamente* $\Pi(\sigma) = -1$*). O núcleo de* Π *é chamado de* **grupo alternante** *e é denotado* A_n*.*

Lema 33 (Critérios de paridade)**.** *Seja* $\sigma \in S_n$*.*

(i) *Uma tranposição* (ij) *é ímpar.*

(ii) *As transposições geram*[2] S_n*. Assim, uma permutação* π *é par (respectivamente ímpar) se* π *é o produto de um número par (respectivamente ímpar) de transposições. Em particular, para um* r*-ciclo* $\sigma = (a_1\, a_2\, a_3\, \ldots\, a_r)$*, temos* $(-1)^\sigma = (-1)^{r+1}$*. Ou seja, ciclos de tamanho par são ímpares e ciclos de tamanho ímpar são pares.*

(iii) *Se* T_σ *é a matriz de permutação correspondente a* σ*,*

$$(-1)^\sigma = \det T_\sigma$$

Definição 34. *Seja* G *um grupo. Um subgrupo* $N \leqslant G$ *é chamado* **normal** *(notação:* $N \trianglelefteqslant G$*) se ele é estável pela conjugação* κ_g *(ver exemplo 31) para qualquer elemento* $g \in G$*, i.e.,*

$$\kappa_g(N) = gNg^{-1} \subseteq N \qquad (g \in G)$$

Seja G um grupo e seja $N \trianglelefteqslant G$ um subgrupo normal. Podemos definir no conjunto das classes laterais $G/N = N\backslash G$ uma operação binária induzida pelo produto em G:

$$g_1N \cdot g_2N \stackrel{\text{def}}{=} g_1g_2N$$

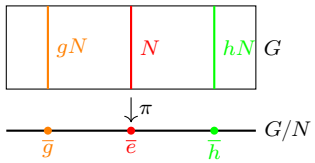
É fácil verifical que esta operação não depende de dos representantes de classe g_i de g_iN. Dizemos que G/N é o **quociente** de G módulo N. Este grupo quociente vem equipado de fábrica com um **morfismo quociente** ou **morfismo de projeção**

$$\begin{aligned} \pi\colon G &\twoheadrightarrow G/N \\ g &\mapsto gN \end{aligned}$$

Claramente π é sobrejetor. Dado $g \in G$, $\pi(g)$ será frequentemente denotado por uma das seguintes notações:

$$\pi(g) = gN = [g] = g \bmod N = \overline{g}$$

Com esta notação podemos por exemplo escrever a definição do produto em G/N como $\overline{g}_1 \cdot \overline{g}_2 = \overline{g_1 \cdot g_2}$ $(g_1, g_2 \in N)$. Intuitivamente, esta construção do grupo quociente corresponde a "igualar" ou "identificar" elementos em uma mesma coclasse gN entre si, de modo que π "comprime" gN em um único "ponto" $\overline{g} \in G/N$ (daí o nome *projeção*):



Teorema 35 (Teorema da Correspondência)**.** *Sejam* G *um grupo e* $N \trianglelefteqslant G$ *um subgrupo normal. Seja* $\pi\colon G \twoheadrightarrow G/N$ *o morfismo de projeção. Então* π *induz uma bijeção entre subgrupos do quociente* G/N *e subgrupos de* G *contendo* N*:*

$$\begin{aligned} \{\overline{H} \leqslant G/N\} &\longleftrightarrow \{H \leqslant G \text{ tais que } N \leqslant H \leqslant G\} \\ \overline{H} &\longmapsto \pi^{-1}(\overline{H}) \\ \pi(H) &\longmapsfrom H \end{aligned}$$

Esta bijeção preserva inclusão e subgrupos normais: dados subgrupos $\overline{H}_i \leqslant G/N$ *e subgrupos correspondentes* $H_i = \pi^{-1}(\overline{H}_i) \leqslant G$ *contendo* N*, temos*

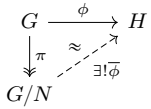
$$\begin{aligned} \overline{H}_1 \leqslant \overline{H}_2 &\iff H_1 \leqslant H_2 \\ \overline{H}_1 \trianglelefteqslant G/N &\iff H_1 \trianglelefteqslant G \end{aligned}$$

Teorema 36 (Propriedade universal do quociente)**.** *Sejam* G *e* H *dois grupos e seja* $N \trianglelefteqslant G$ *um subgrupo normal de* G*. Seja* $\pi\colon G \twoheadrightarrow G/N$ *o morfismo de projeção correspondente. Então dar um morfismo* $\overline{\phi}\colon G/N \to H$ *é equivalente a dar um morfismo* $\phi\colon G \to H$ *que "mata"* N*, i.e., tal que* $\phi(N) = e$*. Ou ainda: dado* $\phi\colon G \to H$ *que "mata"* N*, existe um único morfismo*

$$\begin{aligned} \overline{\phi}\colon G/N &\to H \\ gN &\mapsto \phi(g) \end{aligned}$$

fazendo o seguinte diagrama comutar:

[2] O que é esperado: podemos obter qualquer permutação de n objetos trocando dois objetos de lugar por vez



Teorema 37 (Teorema do Isomorfismo)**.** *Seja $\phi\colon G \to H$ um morfismo de grupos. Então ϕ induz um isomorfismo*

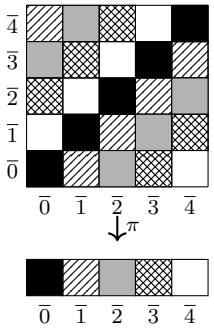
$$\overline{\phi}\colon \frac{G}{\ker\phi} \xrightarrow{\approx} \operatorname{im}\phi$$
$$\overline{g} \mapsto \phi(g)$$

Exemplo 38. *Considere o seguinte morfismo sobrejetor de grupos abelianos aditivos*

$$\pi\colon \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \twoheadrightarrow \mathbb{Z}/5\mathbb{Z}$$
$$(a,b) \mapsto a-b$$

representado graficamente a seguir. O kernel deste morfismo é dado pelos elementos na "diagonal": $\ker\pi = \{(a,a) \in \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \mid a \in \mathbb{Z}/5\mathbb{Z}\}$*. Note que π induz uma bijeção entre classes laterais do kernel e elementos da imagem: as classes laterais são precisamente as "fibras" de π. Cada fibra tem a mesma cardinalidade $|\ker\pi|$ e há tantas fibras quanto elementos na imagem; como as fibras de π particionam $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, temos visivelmente uma "verificação empírica" do teorema do núcleo-imagem:*

$$\underbrace{|\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}|}_{\substack{\text{tamanho do}\\ \text{domínio}}} = 25 = 5 \cdot 5 = \underbrace{|\ker\pi|}_{\substack{\text{tamanho de}\\ \text{cada fibra}}} \cdot \underbrace{|\operatorname{im}\pi|}_{\substack{\text{número}\\ \text{de fibras}}}$$



Definição 39. *Sejam G um grupo e X um conjunto. Uma* **ação de G sobre X** *é um morfismo de grupos $\alpha\colon G \to S_X$. Aqui, como de praxe, S_X denota o grupo simétrico de X. Intuitivamente, α associa a cada $g \in G$ uma bijeção $\alpha(g)\colon X \to X$, que "age" sobre X, permutando seus elementos. Denotamos uma ação de G sobre X por*

$$G \overset{\alpha}{\curvearrowright} X \qquad \text{ou simplesmente} \qquad G \curvearrowright X \quad \text{(deixando } \alpha \text{ subentendido)}$$

e, seguindo a tradição, em vez de $\alpha(g)(x)$ escrevemos simplesmente $g \cdot x$ ($g \in G$, $x \in X$).

A princípio, pode parecer um pouco confuso utilizar um mesmo símbolo $\cdot$ para denotar tanto o produto em G quanto a ação de $g \in G$ sobre um elemento $x \in X$. Mas esta escolha é *proposital*, já que desta forma, temos uma segunda definição equivalente de ação de grupo, dada pelo seguinte

Lema 40. *Dar uma ação $G \curvearrowright X$ equivale a dar uma função*

$$G \times X \to X$$
$$(g,x) \mapsto g \cdot x$$

que satisfaz os seguintes dois mnemônicos axiomas:

(i) (Ação trivial do elemento neutro) Para todo $x \in X$, $1 \cdot x = x$.

(ii) (Associatividade da ação) Para quaisquer $x \in X$, $g,h \in G$, $(g \cdot h) \cdot x = g \cdot (h \cdot x)$

Definição 41. *Seja $G \curvearrowright X$ uma ação de um grupo G sobre um conjunto X. Para um elemento $x \in X$ e um subconjunto $H \subseteq G$, definimos*

(i) a **órbita** *de x (notação: $G \cdot x$) como sendo o subconjunto de X obtido fazendo G agir sobre x:*

$$G \cdot x \overset{\text{def}}{=} \{g \cdot x \in X \mid g \in G\}$$

(ii) o **estabilizador** *ou* **grupo de isotropia** *de x (notação: $\operatorname{Stab}(x)$ ou G_x) como sendo o subgrupo de G que estabiliza x:*

$$G_x = \operatorname{Stab}(x) \overset{\text{def}}{=} \{g \in G \mid g \cdot x = x\}$$

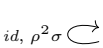
(iii) o **subconjunto fixo** *por H como sendo o subconjunto de X formado pelos pontos em X fixos por todos os elementos de H:*

$$X^H \overset{\text{def}}{=} \{x \in X \mid h \cdot x = x \text{ para todo } h \in H\}$$

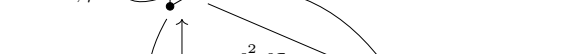
Exemplo 42 (Colorações)**.** *Seja T o triângulo equilátero de vértices $(1,0)$, $(-1/2, \pm\sqrt{3}/2)$ e considere o seu grupo de simetrias, o grupo diedral*

$$D_3 = \{id, \rho, \rho^2, \sigma, \rho\sigma, \rho^2\sigma\}$$

em que ρ denota a rotação no plano de 120° no sentido anti-horário e centro na origem e σ, a reflexão com relação ao eixo x. O grupo D_3 age sobre os vértices de T, permutando-os. O grupo D_3 age também sobre o conjunto X das $2^3 = 8$ colorações dos vértices de T com duas cores, azul e vermelho. Por exemplo,

$\rho^2 \cdot$  $= \sigma \cdot$  $\qquad \operatorname{Stab}\left(\right.$ $\left.\right) = \{id, \rho^2\sigma\}$

Esta ação $D_3 \curvearrowright X$ possui 4 órbitas:



Por exemplo, temos o seguinte diagrama para uma órbita:

Lema 43. *Seja $G \curvearrowright X$ uma ação do grupo G sobre o conjunto X.*

(i) Para qualquer x, $\operatorname{Stab}(x) \leqslant G$.

(ii) **(Fórmula de Mudança de Base)** *Para $g \in G$ e $x \in X$, temos*

$$\operatorname{Stab}(g \cdot x) = g \operatorname{Stab}(x) g^{-1}$$

(iii) As órbitas de $G \curvearrowright X$ formam uma partição do conjunto X.

Teorema 44 (Teorema da Órbita-estabilizador)**.** *Seja $G \curvearrowright X$ uma ação do grupo G sobre o conjunto X. Dado $x \in X$, há uma bijeção entre o conjunto das classes laterais à esquerda de $\operatorname{Stab}(x)$ e a órbita de x:*

$$\psi\colon G/\operatorname{Stab}(x) \to G \cdot x$$
$$g \cdot \operatorname{Stab}(x) \mapsto g \cdot x$$

Logo o tamanho da órbita de x é igual ao índice de seu estabilizador $|G \cdot x| = [G : \operatorname{Stab}(x)]$. Em particular, se G é finito,

$$|G \cdot x| = |G| / |\operatorname{Stab}(x)|$$

(Intuitivamente: o tamanho da órbita de x é igual ao tamanho máximo $|G|$ dividido pelo número de "repetições" $|\operatorname{Stab}(x)|$).

Definição 45. *Seja p um número primo. Um grupo finito G é um* **p-grupo** *se $|G| = p^n$ para algum inteiro $n \geqslant 1$.*

Do teorema de órbita-estabilizador e o fato de as órbitas formarem partição, temos

Teorema 46 (Teorema do Ponto Fixo para p-grupos)**.** *Seja p um primo e seja P um p-grupo. Seja $P \curvearrowright X$ uma ação de P sobre um conjunto finito X. Então*

$$X^P \overset{\text{def}}{=} \{x \in X \mid gx = x \text{ para todo } g \in P\},$$

o conjunto dos pontos fixos desta ação, satisfaz

$$\boxed{|X^P| \equiv |X| \pmod{p}}$$

Em particular, se $p \nmid |X|$ então existe pelo menos um ponto $x \in X$ fixo por todo $g \in P$.

Exemplo 47. *Seja p um número primo e seja P um p-grupo. Seja $Z(P)$ o* **centro** *de P (i.e., o subgrupo formado pelos elementos de P que comutam com todos os elementos de P). Então $Z(P)$ é não trivial. De fato, seja $P \curvearrowright P$ a ação de conjugação (um elemento $g \in P$ age via $x \mapsto gxg^{-1}$). Temos que $Z(P)$ é o conjunto dos pontos fixos de P. Assim, pelo teorema do ponto fixo, $|Z(P)| \equiv |P| \equiv 0 \pmod{p}$. Como $1 \in Z(P)$, $|Z(P)| > 0$ e portanto $|Z(P)| \geqslant p$.*

Teorema 48 (Lema de Burnside)**.** *Sejam G um grupo finito e X um conjunto finito. Dada uma ação $G \curvearrowright X$, o número total de órbitas desta ação é igual ao número médio de pontos fixos por elementos de G:*

$$\text{número de órbitas} = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Demonstração. Podemos contar o número de órbitas associando a cada elemento de $x \in X$ um "peso" inversamente proporcional ao tamanho de sua órbita:

$$\text{número de órbitas} = \sum_{x\in X} \frac{1}{|G\cdot x|} \qquad (*)$$

De fato, dada uma órbita $G\cdot x_1 = \{x_1,\dots,x_n\}$ de tamanho n, cada x_i contribui com peso $1/n$ na soma $(*)$, logo esta órbita contribui com $n\cdot(1/n)=1$ em $(*)$. Pelo teorema da órbita-estabilizador 44, a soma $(*)$ é igual a

$$\sum_{x\in X}\frac{1}{|G\cdot x|} = \sum_{x\in X}\frac{|\operatorname{Stab}(x)|}{|G|} = \frac{1}{|G|}\sum_{x\in X}|\operatorname{Stab}(x)|$$

Assim, para terminar a prova basta mostrar que

$$\sum_{x\in X}|\operatorname{Stab}(x)| = \sum_{g\in G}|X^g| \qquad (**)$$

o que segue de uma contagem dupla, pois ambos os lados contam o número de pares $(g,x)\in G\times X$ tais que $g\cdot x = x$. □

Definição 49. *Seja p um primo e seja G um grupo finito. Seja p^e a maior potência de p que divide $|G|$, i.e., $|G| = p^e m$ com $p\nmid m$. Um p-subgrupo $P\leqslant G$ com $|P|=p^e$ é chamado de um* **p-Sylow** *de G.*

Exemplo 50. *Seja p um primo. Considere o subgrupo $UT_n(\mathbb{F}_p)\leqslant GL_n(\mathbb{F}_p)$ formado pelas matrizes unitriangulares superiores:*

$$UT_n(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ & & \ddots & & \vdots \\ & & & \ddots & * \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \in GL_n(\mathbb{F}_p) \right\}$$

Como cada uma das $n(n-1)/2$ entradas $*$ pode assumir qualquer valor em $\mathbb{F}_p$, $|UT_n(\mathbb{F}_p)| = p^{n(n-1)/2}$. Por outro lado,

$$\begin{aligned} |GL_n(\mathbb{F}_p)| &= (p^n-1)(p^n-p)(p^n-p^2)\dots(p^n-p^{n-1}) \\ &= p^{1+2+\cdots+n-1}\cdot(p^n-1)(p^{n-1}-1)(p^{n-2}-1)\dots(p-1) \\ &= p^{n(n-1)/2}\cdot \text{(número não divisível por } p) \end{aligned}$$

Assim, $UT_n(\mathbb{F}_p)$ é um p-Sylow de $GL_n(\mathbb{F}_p)$.

Teorema 51 (Sylow)**.** *Seja p um primo e seja G um grupo finito cuja ordem é um múltiplo de p, digamos $|G| = p^e m$ com $p\nmid m$.*

(i) G contém ao menos um p-Sylow.

(ii) G contém um subgrupo de ordem p^r para todo $r\leqslant e$; além disso, qualquer p-subgrupo de G está contido em algum p-Sylow.

(iii) Todos os p-Sylows de G são conjugados entre si.

(iv) Seja n_p a quantidade de p-Sylows em G. Então

$$n_p \equiv 1 \pmod p \qquad e \qquad n_p \mid m$$

Exemplo 52. *Mostremos que todo grupo G de ordem 15 é cíclico, ou seja, que G possui pelo menos um elemento de ordem 15. Pelo teorema de Lagrange 27, a ordem de um elemento de G é um divisor de 15. Um elemento de ordem 3 (respectivamente 5) gera um 3-Sylow (respectivamente um 5-Sylow) de G, logo basta encontrar um elemento que não pertence a nenhum 3-Sylow ou 5-Sylow, que terá a ordem desejada 15. Pelos teoremas de Sylow temos $n_3\equiv 1 \pmod 3$ e $n_3 \mid 5$, logo $n_3 = 1$. Da mesma forma, $n_5 = 1$. Sejam P e Q respectivamente os únicos 3-Sylow e 5-Sylow de G. Então $|G\smallsetminus(P\cup Q)| \geqslant 15-3-5 > 0$ e portanto qualquer $g\in G\smallsetminus(P\cup Q)\neq\varnothing$ terá ordem 15.*

12.2 Anéis

Definição 53. *Um* **anel** *é uma tripla $(A,+,\cdot)$ formada por um conjunto A e duas operações binárias*

$$\begin{aligned} +\colon A\times A\to A \quad &(soma) & \cdot\colon A\times A\to A \quad &(produto) \\ (a,b)\mapsto a+b & & (a,b)\mapsto a\cdot b & \end{aligned}$$

satisfazendo os seguintes axiomas:

(i) $(A,+)$ é um grupo abeliano (definição 19), escrito aditivamente;

(ii) $(A,\cdot)$ é um monóide (associatividade e elemento neutro), escrito multiplicativamente.

(iii) (Distributividade à esquerda e à direita) Para quaisquer elementos $a,b,c\in A$, $a\cdot(b+c) = a\cdot b + a\cdot c$ e $(b+c)\cdot a = b\cdot a + c\cdot a$

Se, além dos axiomas acima, o anel $(A,+,\cdot)$ satisfaz

(iv) (Comutatividade do produto) Para quaisquer $a,b\in A$, $a\cdot b = b\cdot a$

dizemos que $(A,+,\cdot)$ é um **anel comutativo**.

Definição 54. *Seja A um anel. Um elemento $u\in A$ é uma* **unidade** *se u possui inverso multiplicativo, i.e., se existe $v\in A$ tal que $uv = vu = 1$. O conjunto de todas as unidades de A*

$$A^\times \stackrel{\text{def}}{=} \{u\in A \mid \exists v\in A \text{ tal que } uv = vu = 1\}$$

forma um grupo multiplicativo $(A^\times,\cdot)$, chamado **grupo das unidades** *de A.*

Exemplo 55 (Inteiros de Gauß)**.** *O anel dos* **inteiros de Gauß** *é o subanel de $\mathbb{C}$ dado por $\mathbb{Z}[i]\stackrel{\text{def}}{=}\mathbb{Z}+\mathbb{Z}i = \{a+bi \mid a,b\in\mathbb{Z}\}$ (um reticulado em $\mathbb{C}$). Definimos a chamada* **função norma** *via (quadrado da distância à origem)*

$$\begin{aligned} N\colon \mathbb{Z}[i] &\to \mathbb{N} \\ z = a+bi &\mapsto |z|^2 = z\overline{z} = a^2+b^2 \qquad (a,b\in\mathbb{Z}) \end{aligned}$$

A principal propriedade da função norma N é ser multiplicativa, já que o mesmo vale para o valor absoluto em $\mathbb{C}$: $N(\alpha\beta) = N(\alpha)N(\beta)$ $(\alpha,\beta\in\mathbb{Z}[i])$. Por isso, a função norma nos ajuda a calcular $\mathbb{Z}[i]^\times$. De fato, se $\alpha\in\mathbb{Z}[i]^\times$ então existe $\beta\in\mathbb{Z}[i]$ tal que

$$\begin{aligned} \alpha\beta = 1 \implies N(\alpha\beta) = N(1) &\iff N(\alpha)N(\beta) = 1 \\ &\iff N(\alpha) = N(\beta) = 1 \end{aligned}$$

já que $N(\alpha), N(\beta)\in\mathbb{N}$. Escrevendo $\alpha = a+bi$ com $a,b\in\mathbb{Z}$ temos que $N(\alpha) = 1 \iff a^2+b^2 = 1$ tem soluções $(a,b) = (\pm1,0)$ ou $(a,b) = (0,\pm1)$, ou seja, $\alpha = \pm1,\pm i$, e todas estas soluções são de fato unidades. Resumindo,

$$\alpha\in\mathbb{Z}[i]^\times \iff N(\alpha) = 1 \iff \alpha\in\{\pm1,\pm i\}$$

e portanto $\mathbb{Z}[i]^\times = \{\pm1,\pm i\}$.

Definição 56. *Seja A um anel. Um elemento $a\in A$ é chamado de*

(i) **nilpotente** *se existe um inteiro $n>0$ tal que $a^n = 0$;*

(ii) **idempotente** *se $a^2 = a$ (e portanto $a^n = a$ para todo inteiro $n>0$). Os elementos 0, 1 são ditos* **idempotentes triviais**.

(iii) **divisor de zero à esquerda** *(respectivamente* **divisor de zero à direita***) se existe $b\neq 0$ em A tal que $ab = 0$ (respectivamente $ba = 0$). Um elemento que é simultaneamente divisor de zero à esquerda e à direita é chamado de* **divisor de zero**.

(note em particular que todo elemento nilpotente $a\in A$ é automaticamente um divisor de zero).

Definição 57. *Um anel comutativo D é um* **domínio de integridade** *ou simplesmente* **domínio** *se $D\neq 0$ (D não é o anel zero) e o único divisor de zero em D é 0, ou seja,*

$$a\cdot b = 0 \implies a = 0 \quad ou \quad b = 0 \qquad (a,b\in D)$$

(ou equivalentemente $a\neq 0$ e $b\neq 0 \implies a\cdot b\neq 0$). Note que, em um domínio D, vale a **regra do cancelamento**

$$\begin{cases} a\neq 0 \\ a\cdot x = a\cdot y \end{cases} \implies x = y \qquad (a,x,y\in D)$$

já que $a\cdot x = a\cdot y \iff a\cdot(x-y) = 0$.

Definição 58. *Um anel A é um*

(i) **anel de divisão** *se $A^\times = A\smallsetminus\{0\}$, ou seja, se $A\neq 0$ e todo elemento não nulo de A é uma unidade.*

(ii) **corpo** *se A é um anel de divisão comutativo.*

O **lema da academia de ginástica** afirma: "Corpo é domínio". Além disso, se $n>0$, temos

$$\boxed{\mathbb{Z}/n\mathbb{Z} \text{ é domínio} \iff n \text{ é primo} \iff \mathbb{Z}/n\mathbb{Z} \text{ é corpo}}$$

Exemplo 59 (Corpos finitos)**.** *Seja p um número primo. O anel dos inteiros módulo p é um corpo finito, que doravante denotaremos por $\mathbb{F}_p \stackrel{\text{def}}{=} \mathbb{Z}/p\mathbb{Z} = \{\overline{0},\overline{1},\overline{2},\dots,\overline{p-1}\}$. Note que $\mathbb{Z}/4\mathbb{Z}$* **não** *é um corpo, já que $\overline{2}$ não é uma unidade neste anel. Existe porém um corpo com 4 elementos, denotado $\mathbb{F}_4$. A ideia é imitar a construção de $\mathbb{C}$ a partir de $\mathbb{R}$, em que um símbolo i satisfazendo $i^2 = -1$ é "acrescentado" a $\mathbb{R}$. Para obter $\mathbb{F}_4$ a partir de $\mathbb{F}_2$, criamos um símbolo α satisfazendo a equação*

$$\alpha^2 = \alpha + \overline{1} \qquad (*)$$

e definimos $\mathbb{F}_4 = \mathbb{F}_2 + \mathbb{F}_2\cdot\alpha = \{\overline{0},\overline{1},\alpha,\overline{1}+\alpha\}$ em que as operações de soma e produto são efetuadas módulo 2, levando-se em conta a relação $(*)$. Por exemplo,

$$\alpha\cdot(\overline{1}+\alpha) = \alpha+\alpha^2 = \alpha+\alpha+\overline{1} = \overline{2}\alpha+\overline{1} = \overline{1}$$

Assim, obtemos as seguintes tabelas de soma e produto e vemos que todo elemento não nulo possui inverso multiplicativo:

$+$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
$\overline{0}$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1}+\alpha$	α
α	α	$\overline{1}+\alpha$	$\overline{0}$	$\overline{1}$
$\overline{1}+\alpha$	$\overline{1}+\alpha$	α	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	α	$\overline{1}+\alpha$
α	$\overline{0}$	α	$\overline{1}+\alpha$	$\overline{1}$
$\overline{1}+\alpha$	$\overline{0}$	$\overline{1}+\alpha$	$\overline{1}$	α

O próximo lema diz essencialmente que "domínios pequenos" são necessariamente corpos.

Lema 60. *Seja D um domínio.*

(i) Se D é finito então D é um corpo.

(ii) Se $K \subseteq D$ é um subcorpo de D e D tem dimensão finita como K-espaço vetorial, então D também é um corpo.

Definição 61. *Sejam A e B dois anéis.*

(i) Um **homomorfismo** *ou* **morfismo de anéis** *é uma função $\varphi\colon A \to B$ que preserva somas, produtos e 1: para quaisquer $a_1, a_2 \in A$, $\varphi(a_1+a_2) = \varphi(a_1)+\varphi(a_2)$, $\varphi(a_1 \cdot a_2) = \varphi(a_1)\cdot\varphi(a_2)$, $\varphi(1_A) = 1_B$. Em outras palavras, φ é simultaneamente um morfismo de grupos entre $(A,+)$ e $(B,+)$ e um morfismo de monóides entre $(A,\cdot)$ e $(B,\cdot)$.*

(ii) Um **isomorfismo** *$\varphi\colon A \xrightarrow{\approx} B$ é um morfismo de anéis que é bijetor; como em grupos, a função inversa $\varphi^{-1}\colon B \xrightarrow{\approx} A$ também é um isomorfismo. Dois anéis A e B são* **isomorfos** *(notação $A \cong B$ ou $A \approx B$) se existe um isomorfismo $\varphi\colon A \xrightarrow{\approx} B$ entre eles (em geral não único).*

(iii) Um **automorfismo** *de um anel A é um isomorfismo $\varphi\colon A \xrightarrow{\approx} A$. O conjunto de todos os automorfismos de A é denotado $\mathrm{Aut}(A)$ e forma um grupo com a operação de composição de funções.*

(iv) O **kernel** *ou* **núcleo** *de um morfismo de anéis $\varphi\colon A \to B$ é o ideal (ver definição 63) $\ker(\varphi) \stackrel{\text{def}}{=} \varphi^{-1}(0) = \{a \in A \mid \varphi(a) = 0\}$.*

Como para grupos, temos que o morfismo de anéis $\varphi\colon A \to B$ é injetor se, e só se, $\ker\varphi = \{0\}$.

Definição 62. *Seja D um domínio D. O "menor corpo"* $\mathrm{Frac}\, D$ *contendo D, o chamado* **corpo de frações** *de D, é o corpo obtido "invertendo-se" os elementos não nulos de D. Precisamente: seja*

$$S = \{(a,b) \mid a,b \in D,\ b \neq 0\},$$

e defina em S a relação $\sim$ por $(a,b) \sim (c,d) \iff ad = bc$. É fácil ver que $\sim$ é uma relação de equivalência; definimos $\mathrm{Frac}\, D = S/\!\sim$. *Por motivos de sanidade psicológica, denotamos a classe de (a,b) pela "fração" a/b, de modo que em* $\mathrm{Frac}\, D$ *temos*

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc \qquad (a,b,c,d \in D,\ b,d \neq 0)$$

Temos que $\mathrm{Frac}\, D$ *é um corpo com as seguintes operações de soma e produto:*

$$\frac{a}{b} + \frac{c}{d} = \frac{a\cdot d + b\cdot c}{b\cdot d} \qquad e \qquad \frac{a}{b}\cdot\frac{c}{d} = \frac{a\cdot c}{b\cdot d}$$

Definição 63. *Dado um anel A, $I \subseteq A$ é um* **ideal à esquerda** *de A se I é fechado por combinações A-lineares à esquerda. Isto é,*

$$a_1, a_2 \in A, \quad x_1, x_2 \in I \Rightarrow a_1x_1 + a_2x_2 \in I.$$

Analogamente se define um **ideal à direita** *de A. Se $I \subseteq A$ é um ideal à esquerda e à direita de A, então I é dito um* **ideal (bilateral)** *de A. Se A for comutativo, denotaremos por*

$$(a_1, \ldots, a_n) \stackrel{\text{def}}{=} A\cdot a_1 + \cdots + A\cdot a_n$$

o ideal (bilateral) gerado por $a_1, \ldots, a_n$. Um ideal da forma (a), gerado por um único elemento a, será chamado de **ideal principal**.

Definição 64. *Seja A um anel. Um A-***módulo à esquerda** *M é um grupo abeliano $(M,+)$ juntamente com uma função $\cdot\colon A \times M \to M$, chamada* **multiplicação escalar**, *satisfazendo os seguintes axiomas:*

(i) (o 1 não faz nada) Para todo $m \in M$, $1 \cdot m = m$.

(ii) (pseudo-associatividade) Para quaisquer $a,b \in A$, $m \in M$, $(a\cdot b)\cdot m = a\cdot(b\cdot m)$.

(iii) (distributividade vetorial) Para quaisquer $a \in A$, $m,n \in M$, $a\cdot(m+n) = a\cdot m + a\cdot n$.

(iv) (distributividade escalar) Para quaisquer $a,b \in A$, $m \in M$, $(a+b)\cdot m = a\cdot m + b\cdot m$.

Se k é um corpo, um k-módulo V é também chamado de **k-espaço vetorial**; *os elementos de V são ditos* **vetores** *enquanto os de k,* **escalares**.

Definição 65. *Seja A um anel e seja M um A-módulo à esquerda.*

(a) Uma **combinação A-linear** *(à esquerda) de $m_1, \ldots, m_r \in M$ é uma expressão da forma*

$$a_1\cdot m_1 + \cdots + a_r\cdot m_r \in M,$$

em que $a_1, \ldots, a_r \in A$. Denotaremos o conjunto de todas as combinações A-lineares à esquerda de $m_1, \ldots, m_r$ por $A\cdot m_1 + \cdots + A\cdot m_r$.

(b) O conjunto $B = \{m_i \in M \mid i \in I\}$ é um **conjunto gerador** *de M se, para todo $x \in M$, existem $i_1, \ldots, i_n \in I$ e $\alpha_1, \ldots, \alpha_n \in A$ tais que*

$$x = \sum_{j=1}^{n} \alpha_j m_{i_j}.$$

Dizemos também que B é **linearmente independente** *(LI) se, para todo subconjunto finito $\{i_1, \ldots, i_n\} \subseteq I$ e elementos $\alpha_1, \ldots, \alpha_n \in A$, temos*

$$\sum_{j=1}^{n} \alpha_j m_{i_j} = 0 \iff \alpha_1 = \ldots = \alpha_n = 0.$$

Se B é um conjunto LI e gerador, dizemos que B é **base** *de M. Se B é um conjunto gerador finito, dizemos que M é* **finitamente gerado**.

Nem todo módulo possui uma base. Por exemplo, o $\mathbb{Z}$-módulo $\mathbb{Z}/4\mathbb{Z}$ não possui base, pois não há subconjuntos LI em $\mathbb{Z}/4\mathbb{Z}$: $4m = \overline{0}$ para todo $m \in \mathbb{Z}/4\mathbb{Z}$. Entretanto, note que $\mathbb{Z}/4\mathbb{Z}$ possui as bases $\{\overline{1}\}$ e $\{\overline{3}\}$ quando visto como um $(\mathbb{Z}/4\mathbb{Z})$-módulo.

Definição 66. *Se o A-módulo à esquerda M possui uma base, dizemos que M é* **livre**.

Exemplo 67. *Todo anel A é um A-módulo à esquerda livre com base $\{1\}$. De modo um pouco mais geral, o módulo A^n é livre com a base canônica $\{e_1, \ldots, e_n\}$, em que $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (1 na i-ésima coordenada).*

Definição 68. *Seja A um anel e seja M um A-módulo à esquerda. Um A-***submódulo** *N de M é um subconjunto $N \subseteq M$ que é fechado por combinações A-lineares à esquerda:*

$$a_1, a_2 \in A, \quad n_1, n_2 \in N \implies a_1\cdot n_1 + a_2\cdot n_2 \in N.$$

Assim, $(N,+)$ é um subgrupo de $(M,+)$ e a multiplicação escalar de M se restringe a N, fazendo de N um A-módulo à esquerda. A definição para módulos à direita é análoga, trocando todas as ocorrências da palavra "esquerda" por "direita".

Exemplo 69. *A partir de uma família de A-módulos $\{M_i\}_{i\in I}$ à esquerda, podemos construir dois novos A-módulos à esquerda:*

(i) o **produto direto** *$\prod_{i\in I} M_i$ que, como conjunto, é igual ao produto cartesiano dos M_i, sendo a soma e o produto escalar feitas componente a componente;*

(ii) a **soma direta** *$\bigoplus_{i\in I} M_i$ que é o submódulo do produto direto cujos elementos são as tuplas $(m_i)_{i\in I}$ "quase nulas", i.e., com $m_i \neq 0$ apenas para um número finito de índices i.*

Em particular, observe que se o conjunto de índices I é finito, então $\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$.

Definição 70. *Seja A um anel e sejam M e N dois A-módulos à esquerda.*

(i) Uma função $f\colon M \to N$ é um **morfismo de A-módulos** *se f é A-linear, i.e., f preserva combinações A-lineares:*

$$f(a_1m_1 + a_2m_2) = a_1f(m_1) + a_2f(m_2) \qquad (a_i \in A,\ m_i \in M)$$

(ii) Dizemos que um morfismo $f\colon M \xrightarrow{\approx} N$ é um **isomorfismo** *se f for bijetor; neste caso, o mapa inverso $f^{-1}\colon N \xrightarrow{\approx} M$ também é um morfismo de A-módulos à esquerda.*

Denotaremos o conjunto de todos os morfismos de A-módulos entre M e N por $\mathrm{Hom}_A(M,N)$.

Definição 71. *Seja A um anel. Dado um ideal bilateral $I \subseteq A$, definimos em A a relação de congruência módulo I via*

$$a \equiv b \pmod{I} \iff a - b \in I \qquad (a,b \in A)$$

(lê-se a é congruente a b módulo I).

Lema 72. *Sejam A um anel e I um ideal bilateral.*

(i) A relação de congruência módulo I é uma relação de equivalência em A: para quaisquer $a,b,c \in A$, temos

(a) (reflexividade) $a \equiv a \pmod{I}$;

(b) (simetria) $a \equiv b \pmod{I} \iff b \equiv a \pmod{I}$;

(c) (transitividade) se $a \equiv b \pmod{I}$ e $b \equiv c \pmod{I}$ então $a \equiv c \pmod{I}$.

(ii) A relação de congruência módulo I é compatível com as operações de soma e produto do anel A, no seguinte sentido:

$$\begin{cases} a \equiv b \pmod{I} \\ c \equiv d \pmod{I} \end{cases} \implies \begin{cases} a + c \equiv b + d \pmod{I} \\ ac \equiv bd \pmod{I} \end{cases}$$

A classe de equivalência do elemento $a \in A$ é o "transladado" $a + I$ de I, que será denotado por uma das seguintes maneiras:

$$a + I = a \bmod I = \overline{a} = [a] \stackrel{\text{def}}{=} \{a + x \mid x \in I\}$$

Denotaremos o conjunto quociente pela relação de equivalência módulo I por

$$A/I \stackrel{\text{def}}{=} \{a + I \mid a \in A\}$$

Podemos dar uma estrutura de anel para o conjunto A/I definindo

$$(a + I) + (b + I) \stackrel{\text{def}}{=} (a + b) + I,$$
$$(a + I) \cdot (b + I) \stackrel{\text{def}}{=} (a \cdot b) + I \qquad (a, b \in A)$$

ou, mais sugestivamente, na notação por barras,

$$\overline{a} + \overline{b} \stackrel{\text{def}}{=} \overline{a + b} \qquad \text{e} \qquad \overline{a} \cdot \overline{b} \stackrel{\text{def}}{=} \overline{a \cdot b} \qquad (a, b \in A)$$

Por (ii) no lema anterior, as operações em A/I estão de fato bem definidas, isto é, não dependem da escolha dos representantes de classe a, b: se $\overline{a} = \overline{c}$ e $\overline{b} = \overline{d}$ então $\overline{a + b} = \overline{c + d}$ e $\overline{a \cdot b} = \overline{c \cdot d}$. O anel A/I é chamado de **anel quociente** de A por I. Os elementos neutros da soma e do produto são respectivamente $\overline{0} = I$ e $\overline{1} = 1 + I$. Intuitivamente, A/I é o anel obtido a partir de A "igualando-se" elementos que diferem por um elemento em I. Em particular, todos os elementos de I são "igualados" a zero. O anel quociente vem equipado de fábrica com um **morfismo quociente** ou **morfismo projeção**, que é o morfismo de anéis sobrejetor dado por:

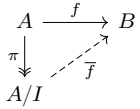
$$\pi \colon A \twoheadrightarrow A/I$$
$$a \mapsto \overline{a}$$

Intuitivamente, π "comprime" todos os elementos de uma mesma classe de equivalência em A em um único ponto de A/I (daí o nome *projeção*).
Como para grupos, temos

Teorema 73 (Correspondência)**.** *Se I é um ideal de A, a projeção $\pi \colon A \to A/I$ estabelece uma bijeção entre ideais de A contendo I e ideais do quociente A/I:*

$$\{\textit{ideais de } A \textit{ que contém } I\} \leftrightarrow \{\textit{ideais de } A/I\}$$
$$J \mapsto J/I = \pi(J)$$
$$\pi^{-1}(J') \hookleftarrow J'$$

Teorema 74 (Propriedade universal do quociente)**.** *Dados um morfismo de anéis $f \colon A \to B$ e um ideal bilateral $I \subseteq \ker(f)$ de A, existe um único morfismo de anéis $\overline{f} \colon A/I \to B$ tal que $\overline{f}(a + I) = f(a)$ para todo $a \in A$, isto é, tal que o diagrama abaixo comuta:*



Aqui, $\pi \colon A \twoheadrightarrow A/I$ é o mapa de projeção $\pi(a) = a + I$. Temos ainda $\ker(\overline{f}) = \ker(f)/I$ e $\operatorname{im}(\overline{f}) = \operatorname{im}(f)$. Assim, f induz um isomorfismo $\overline{f} \colon A/\ker(f) \xrightarrow{\approx} \operatorname{im}(f)$.

Exemplo 75. *O morfismo natural*

$$f \colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}[i]/(2 + i)$$
$$a \mapsto [a]$$

induz um morfismo $\overline{f} \colon \mathbb{Z}/5\mathbb{Z} \xrightarrow{\approx} \mathbb{Z}[i]/(2 + i)$ dado por $\overline{a} \mapsto [a]$ que, como mostraremos a seguir, é um isomorfismo. Primeiro, observe que f é sobrejetor, já que qualquer inteiro de Gauß $a + bi \in \mathbb{Z}[i]$ $(a, b \in \mathbb{Z})$ é congruente a um inteiro módulo $2 + i$: de fato, como

$$2 + i \equiv 0 \pmod{(2 + i)} \iff i \equiv -2 \pmod{(2 + i)}$$

temos $[a + bi] = [a - 2b]$ em $\mathbb{Z}[i]/(2 + i)$. Segundo, $\ker f = 5\mathbb{Z}$: como $5 = (2 + i)(2 - i)$ temos $\ker f \supseteq 5\mathbb{Z}$; reciprocamente,

$$a \in \ker f \iff a = (2 + i) \cdot \gamma \textit{ para algum } \gamma \in \mathbb{Z}[i]$$
$$\implies N(a) = N(2 + i)N(\gamma) \iff a^2 = 5N(\gamma)$$
$$\implies 5 \mid a^2 \textit{ em } \mathbb{Z} \implies 5 \mid a \textit{ em } \mathbb{Z}$$

e portanto $\ker f \subseteq 5\mathbb{Z}$.

Exemplo 76. *Seja $a \in \mathbb{Q}$. Temos um isomorfismo*

$$\overline{f} \colon \frac{\mathbb{Q}[x]}{(x - a)} \xrightarrow{\approx} \mathbb{Q}$$
$$\overline{p(x)} \mapsto p(a)$$

induzido pelo morfismo sobrejetor $f \colon \mathbb{Q}[x] \twoheadrightarrow \mathbb{Q}$ dado pela "avaliação em a": $p(x) \mapsto p(a)$. Para ver isto, note que $\ker f = (x - a)$ do critério da raiz (lema 91).

Definição 77. *Seja A um anel. Um ideal bilateral $I \neq A$ é dito* **maximal** *se satisfaz uma das (logo todas) as seguintes condições equivalentes:*

(i) ele é maximal com relação à inclusão no conjunto dos ideais próprios de A: se $J \subseteq A$ é qualquer ideal de A, então

$$I \subseteq J \implies J = I \textit{ ou } J = A$$

(ii) A/I é um anel **simples**, *isto é, seus únicos ideais são 0 e A/I.*

A equivalência entre (i) e (ii) segue diretamente do teorema da correspondência 73.

Lema 78. *Seja $A \neq 0$ um anel.*

(i) O anel A possui ideais maximais.

(ii) Seja $I \neq A$ um ideal de A. Então I está contido em algum ideal maximal.

Lema 79. *Se A é um anel comutativo, o ideal I de A é maximal se, e somente se, A/I é um corpo.*

Definição 80. *Seja A um anel comutativo. Um ideal $P \subset A$ é* **primo** *se satisfaz uma (logo todas) das seguintes condições equivalentes:*

(i) A/P é um domínio;

(ii) P é um ideal próprio (i.e., $P \neq A$) e, para quaisquer $a, b \in A$,

$$ab \in P \implies a \in P \textit{ ou } b \in P$$

O conjunto de todos os ideais primos de A é chamado de **espectro** *de A e é denotado* $\operatorname{Spec} A$. *De (i) e do lema anterior (juntamente com o lema da academia de ginástica), temos*

$$\boxed{M \textit{ maximal} \implies M \textit{ primo}}$$

Exemplo 81. *Se k é um corpo, então*

$$(x_1), \quad (x_1, x_2), \quad \ldots, \quad (x_1, x_2, \ldots, x_n) \in \operatorname{Spec} k[x_1, \ldots, x_n]$$

já que $k[x_1, x_2, \ldots, x_n]/(x_1, \ldots, x_i) \cong k[x_{i+1}, x_{i+2}, \ldots, x_n]$ são todos domínios. Destes ideais primos, apenas $(x_1, \ldots, x_n)$ é maximal.

Teorema 82 (Teorema Chinês dos Restos)**.** *Seja A um anel comutativo. Sejam $I_1, \ldots, I_n$ ideais de A dois a dois comaximais (i.e., $i \neq j \implies I_i + I_j = A$). Então $I_1 \cap \cdots \cap I_n = I_1 I_2 \cdots I_n$ e o morfismo*

$$\frac{A}{I_1 I_2 \cdots I_n} = \frac{A}{I_1 \cap \cdots \cap I_n} \xrightarrow{\approx} \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}$$
$$a \bmod I_1 \cap \cdots \cap I_n \mapsto (a \bmod I_1, \ldots, a \bmod I_n)$$

é um isomorfismo.

Definição 83. *Seja D um domínio e sejam $a, b \in D$. Escrevemos $a \mid b$ (lê-se a* **divide** *b ou b* **é múltiplo de** *a) se existe $c \in D$ tal que $b = ac$. Em outras palavras, no mundo ideal, "conter é dividir":*

$$\boxed{a \mid b \iff (a) \supseteq (b)}$$

Definição 84. *Seja D um domínio. Dizemos que $a, b \in D$ são* **associados** *se satisfazem uma das (logo todas) seguintes condições equivalentes:*

(i) existe $u \in A^\times$ tal que $a = bu$ (i.e., se a e b diferem multiplicativamente por uma unidade)

(ii) $a \mid b$ e $b \mid a$

(iii) $(a) = (b)$

Definição 85. *Seja D um domínio e seja $\pi \in D$ com $\pi \neq 0$ e $\pi \notin D^\times$.*

(i) Dizemos que π é **irredutível** *se, para $a, b \in D$,*

$$\pi = ab \implies a \in D^\times \textit{ ou } b \in D^\times$$

Ou seja, π é irredutível se só possui fatorações triviais em D: todo divisor de π é associado ou a 1 ou a π.

(ii) Dizemos que π é **primo** *se (π) é um ideal primo, i.e., se*

$$\pi \mid ab \implies \pi \mid a \textit{ ou } \pi \mid b$$

(note que $(\pi) \neq D$ automaticamente pois estamos supondo $\pi \notin D^\times$.)

Em $\mathbb{Z}$, as noções de irredutível e primo se confundem, mas elas são distintas em geral. Por outro lado, temos a seguinte implicação:

Lema 86. *Seja D um domínio e seja $\pi \in D$ com $\pi \neq 0$ e $\pi \notin D^\times$. Se π é primo, então π é irredutível.*

Definição 87. *Um domínio D é dito* **domínio de fatoração única** *(DFU) ou* **domínio fatorial** *se todo elemento não nulo $d \in D$ pode ser escrito como produto de irredutíveis de maneira única a menos da ordem dos fatores e de associados, ou seja,*

(a) (Existência da fatoração) $d = \pi_1\pi_2\dots\pi_m$ *com* π_i *irredutíveis;*

(b) (Unicidade da fatoração) Se $d = \rho_1\rho_2\dots\rho_n$ *é outra fatoração em irredutíveis* ρ_i*, então há a mesma quantidade de fatores* $m = n$ *e existe uma permutação* $\sigma \in S_m$ *tal que* π_i *é associado a* $\rho_{\sigma(i)}$ *para* $i = 1, \dots, m = n$*.*

Lema 88. *Seja* D *um DFU e seja* $\pi \in D$ *com* $\pi \neq 0$ *e* $\pi \notin D^\times$*. Então se* π *é primo se, e só se,* π *é irredutível.*

Definição 89. *Seja* D *um DFU e sejam* $d_1, \dots, d_n \in D$*, não todos iguais a* 0*.*

(i) Um **máximo divisor comum** *(mdc) de* $d_1, \dots, d_n$ *é um divisor comum* d *de* $d_1, \dots, d_n$ *com a propriedade de que se* a *é também um divisor comum de* $d_1, \dots, d_n$ *então* $a \mid d$*.*

(ii) Um **mínimo múltiplo comum** *(mmc) de* $d_1, \dots, d_n$ *é um múltiplo comum* m *de* $d_1, \dots, d_n$ *com a propriedade de que se* a *é também um múltiplo comum de* $d_1, \dots, d_n$ *então* $m \mid a$*.*

Em outras palavras: um mdc (respectivamente mmc) de $d_1, \dots, d_n$ *é um elemento máximo (respectivamente mínimo) com respeito à relação de divisibilidade no conjunto dos divisores comuns (respectivamente múltiplos comuns) de* $d_1, \dots, d_n$*.*

Lema 90 (Critério da raiz racional)**.** *Seja* D *um DFU e seja* $k = \operatorname{Frac} D$*. Dado um polinômio*

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

se $r/s \in K$ *(*$r, s \in D$*,* $s \neq 0$ *e* $\operatorname{mdc}(r, s) = 1$*) é uma raiz de* $f(x)$ *então* $s \mid a_n$ *e* $r \mid a_0$*. Em particular, se* $f(x)$ *é mônico, toda raiz de* $f(x)$ *em* K *pertence a* D*.*

Lema 91 (Critério da raiz)**.** *Seja* K *um corpo e sejam* $f(x) \in K[x]$ *e* $a \in K$*.*

(i) $f(a) \in K$ *é igual ao resto da divisão de* $f(x)$ *por* $x - a$*. Em particular,* $f(a) = 0 \iff x - a \mid f(x)$*.*

(ii) Se $f(x)$ *é não nulo, então* $f(x)$ *possui no máximo* $\deg f(x)$ *raízes em* K*.*

Definição 92. *(i) Um par* (D, ρ) *formado por um domínio* D *e uma função* $\rho\colon D \setminus \{0\} \to \mathbb{N}$ *é chamado de* **domínio euclidiano** *(DE) se* D *possui "divisão euclidiana" com relação ao "tamanho euclidiano"* ρ*, i.e., se dados* $a, b \in D$ *com* $b \neq 0$*, existem* $q, r \in D$ *(quociente e resto, respectivamente) satisfazendo*

$$a = bq + r \qquad \text{com} \quad r = 0 \text{ ou } \rho(r) < \rho(b)$$

Note que não exigimos a unicidade do quociente q *e do resto* r *na definição acima, apenas a existência dos mesmos.*

Na tabela a seguir, resumimos os principais exemplos de DEs e suas respectivas funções "tamanho euclidiano". Aqui, k denota um corpo qualquer e p, um número primo.

Anel	Tamanho Euclidiano
$\mathbb{Z}$	$\rho(a) = \lvert a\rvert$
$k[x]$	grau
$k[\![t]\!]$	valorização t-ádica v_t
$\mathbb{Z}_p$	valorização p-ádica v_p
$\mathbb{Z}[i]$	norma $N(\alpha) = \lvert\alpha\rvert^2$
$\mathbb{Z}[\omega]$	norma $N(\alpha) = \lvert\alpha\rvert^2$

Veremos a seguir que todo DE é um DFU. A aritmética nos DEs da tabela acima é dada por

DE	Grupo de Unidades	Irredutíveis (a menos de associados)
$\mathbb{Z}$	$\{\pm 1\}$	números primos
$k[x]$	$k^\times$	polinômios mônicos irredutíveis
$k[\![t]\!]$	$\{f \in k[\![t]\!] \mid v_t(f) = 0\}$	t
$\mathbb{Z}_p$	$\{f \in \mathbb{Z}_p \mid v_p(f) = 0\}$	p
$\mathbb{Z}[i]$	$\{\pm 1, \pm i\}$	$1 + i$; números primos $p \equiv 3 \pmod 4$; $a \pm bi$ com $a^2 + b^2 = p$ número primo tal que $p \equiv 1 \pmod 4$
$\mathbb{Z}[\omega]$	$\{\pm 1, \pm\omega, \pm\omega^2\}$	$1 - \omega$; números primos $p \equiv 5 \pmod 6$; $a \pm bi$ com $a^2 - ab + b^2 = p$ número primo tal que $p \equiv 1 \pmod 6$

Lema 93. *Seja* (D, ρ) *um DE.*

(i) **(Menor divide)** *Todo ideal de* D *é principal.*

(ii) **(Lema primordial)** *Todo irredutível de* D *é primo.*

Lema 94 (Euclides)**.** *Em um DE* D*, sejam* $a, b \in D$ *com* $b \neq 0$*. Suponha que* $a = bq + r$*. Então* $\operatorname{mdc}(a, b) = \operatorname{mdc}(b, r)$*.*

Definição 95. *Um anel comutativo* A *é dito* **noetheriano** *se satisfaz qualquer uma das seguintes propriedades equivalentes:*

(i) todo ideal $I \subseteq A$ *é finitamente gerado;*

(ii) toda cadeia ascendente de ideais estabiliza, isto é, dada uma cadeia de ideais $I_0 \subseteq I_1 \subseteq I_2 \subset I_3 \subseteq \cdots$ *então* $I_i = I_{i+1}$ *para todo* $i \gg 0$ *suficientemente grande;*

(iii) todo conjunto $\mathcal{S} \neq \varnothing$ *de ideais possui um elemento que é maximal*[3] *em* $\mathcal{S}$ *com relação à inclusão.*

Corpos e DEs são noetherianos pois todos seus ideais são principais (pelo menor divide, 93).

Lema 96. *Seja* D *um domínio noetheriano. Se todo irredutível de* D *for primo então* D *é um DFU.*

Teorema 97 (Teorema da base de Hilbert)**.** *Seja* A *um anel comutativo. Então* A *noetheriano implica* $A[x]$ *noetheriano. Consequentemente, toda álgebra finitamente gerada sobre um anel noetheriano é noetheriana.*

Definição 98. *Seja* A *um anel comutativo. Um* A*-módulo* M *é dito* **noetheriano** *se satisfaz as seguintes condições equivalentes:*

(i) todo submódulo $N \subseteq M$ *é finitamente gerado.*

(ii) toda cadeia ascendente de submódulos estabiliza, isto é, se

$$N_1 \subseteq N_2 \subseteq N_2 \subseteq \cdots$$

é uma cadeia de submódulos de M*, então existe* $i_0 \geqslant 1$ *tal que* $N_i = N_{i_0}$ *para todo* $i \geqslant i_0$*.*

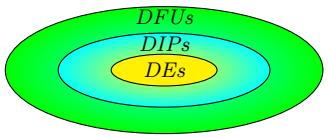
(iii) todo subconjunto $\mathcal{S} \neq \varnothing$ *de submódulos de* M *tem um elemento maximal em* $\mathcal{S}$ *com relação a inclusão.*

Teorema 99. *Seja* A *um anel e seja* M *um* A*-módulo finitamente gerado. Se* A *é noetheriano, então* M *é noetheriano.*

Definição 100. *Um domínio* D *é dito* **domínio de ideais principais** *(DIP) se todo ideal de* D *é principal (i.e., gerado por um único elemento).*

Teorema 101. *Seja* D *um domínio. Então*

$$D \text{ é DE} \implies D \text{ é DIP} \implies D \text{ é DFU}$$



Teorema 102 (Gauß)**.** *Seja* D *um domínio. Então*

$$D \text{ é um DFU} \implies D[x] \text{ é um DFU}$$

Definição 103. *Seja* D *um DFU e seja* $f \in D[x]$ *um polinômio não nulo. Dizemos que* f *é* **primitivo** *se seus coeficientes têm mdc igual a* 1 *(ou mais precisamente, associado a* 1*). Em outras palavras,* f *é primitivo se não existe um irredutível* $\pi \in D$ *que divide todos os seus coeficientes.*

Lema 104 (Lema de Gauß)**.** *Seja* D *um DFU e seja* $K = \operatorname{Frac} D$*.*

(i) Se $f(x), g(x) \in D[x]$ *são primitivos então* $f(x) \cdot g(x)$ *é primitivo.*

(ii) Seja $f(x) \in D[x]$ *um polinômio* **primitivo***. Então*

$$f(x) \text{ irredutível em } K[x] \iff f(x) \text{ irredutível em } D[x]$$

Teorema 105 (Critério de Eisenstein)**.** *Seja* D *um DFU. Seja* $\pi \in D$ *um irredutível e seja* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in D[x]$ *um polinômio* **primitivo** *tal que* $\pi \nmid a_n$*,* $\pi \mid a_i$ *para* $i = 0, 1, \dots, n-1$ *e* $\pi^2 \nmid a_0$*. Então* $p(x)$ *é irredutível em* $D[x]$*, logo pelo lema de Gauß também em* $K[x]$*, em que* $K = \operatorname{Frac} D$*.*

Teorema 106. *Sejam* A *um DIP e* M *um módulo livre de posto* n*, isto é,* $M \cong A^n$*. Se* N *é um submódulo de* M*, então* N *é livre. Mais especificamente, existe uma base* $\{e_1, \dots, e_n\}$ *de* M*, um inteiro não negativo* $k \leqslant n$ *e* $d_1, d_2, \dots, d_k \in A$ *tais que* $\{d_1e_1, d_2e_2, \dots, d_ke_k\}$ *é uma base de* N*.*

Teorema 107. *Seja* A *um DIP e seja* M *um módulo finitamente gerado sobre* A*. Então*

(a) (Fatores invariantes)

$$M \cong A^r \times A/(a_1) \times \cdots \times A/(a_m)$$

para certos inteiros $r, m \geqslant 0$ *e elementos não nulos* $a_1, a_2, \dots, a_m$ *de* A *que não são unidades e que satisfazem* $a_1 \mid a_2 \mid \cdots \mid a_m$*. Os inteiros* r *e* m *são unicamente determinados e os elementos* $a_1, \dots, a_m$ *são unicamente determinados a menos de associados.*

[3] cuidado: note que este elemento maximal em $\mathcal{S}$ não necessariamente é um ideal maximal em A

(b) (Divisores elementares)

$$M \cong A^r \times A/(p_1^{\alpha_1}) \times \cdots \times A/(p_n^{\alpha_n})$$

para um certo inteiro $r \geqslant 0$ e potências de primos (não necessariamente distintos) $p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}$. O inteiro r é unicamente determinado, e as potências de primos são unicamente determinadas a menos de associados.

12.3 Corpos

Dado um corpo K, a **característica** de K, em símbolos $\operatorname{char} K$, é o menor inteiro $n > 0$ tal que

$$n \cdot 1 \stackrel{\text{def}}{=} \underbrace{1 + 1 + \cdots + 1}_{n \text{ vezes}} = 0 \text{ em } K$$

ou $\operatorname{char} K = 0$ se tal inteiro $n > 0$ não existe. Se $\operatorname{char} K > 0$ então $\operatorname{char} K$ é necessariamente um número primo.

Lema 108 (Sonho de todo estudante)**.** *Seja K um corpo com $p = \operatorname{char} K > 0$. Então, para quaisquer $a, b \in K$, $(a+b)^p = a^p + b^p$.*

Definição 109. *Sejam $L \supseteq K$ uma extensão de corpos e $\theta_1, \ldots, \theta_n \in L$. Denotamos por*

(i) $K[\theta_1, \ldots, \theta_n]$ o **subanel** *de L gerado por $\theta_1, \ldots, \theta_n$ sobre K, i.e., o subanel de L (ou mais precisamente a sub-K-álgebra) formado por todas as expressões polinomiais em $\theta_1, \ldots, \theta_n$ com coeficientes em K:*

$$K[\theta_1, \ldots, \theta_n] \stackrel{\text{def}}{=} \{\, f(\theta_1, \ldots, \theta_n) \mid f \in K[x_1, \ldots, x_n] \,\}$$

(ii) $K(\theta_1, \ldots, \theta_n)$ o **subcorpo** *de L gerado por $\theta_1, \ldots, \theta_n$ sobre K, ou seja, o corpo de frações do domínio $K[\theta_1, \ldots, \theta_n]$:*

$$K(\theta_1, \ldots, \theta_n) \stackrel{\text{def}}{=} \operatorname{Frac} K[\theta_1, \ldots, \theta_n]$$

Definição 110. *Seja $L \supseteq K$ uma extensão de corpos. Seja $\theta \in L$.*

(i) Dizemos que θ é **algébrico** *sobre K se existe um polinômio* **não nulo** *$f(x) \in K[x]$ tal que $f(\theta) = 0$. Caso contrário, dizemos que θ é* **transcendente** *sobre K.*

(ii) A extensão $L \supseteq K$ é dita **algébrica** *se todo elemento de L é algébrico sobre K. Caso contrário, dizemos que $L \supseteq K$ é uma extensão* **transcendente**.

Definição 111. *Seja $L \supseteq K$ uma extensão de corpos e seja $\theta \in L$ um elemento algébrico sobre K. O polinômio mônico $m(x) \in K[x]$ de menor grau tal que $m(\theta) = 0$ é chamado de* **polinômio minimal** *de θ sobre K.*

Lema 112 (Menor divide)**.** *Seja $L \supseteq K$ uma extensão de corpos. Seja $\theta \in L$ algébrico sobre K e seja $m(x) \in K[x]$ seu polinômio minimal sobre K. Então*

$$\begin{cases} f(x) \in K[x] \\ f(\theta) = 0 \end{cases} \implies m(x) \mid f(x)$$

Lema 113. *Seja θ um elemento algébrico sobre K e seja $m(x) \in K[x]$ um polinômio mônico. Então $m(x)$ é o polinômio minimal de θ se, e só se, $m(\theta) = 0$ e $m(x)$ é irredutível em $K[x]$.*

Definição 114. *O* **grau** *$[L : K]$ de uma extensão de corpos $L \supseteq K$ é a dimensão de L visto como K-espaço vetorial: $[L : K] \stackrel{\text{def}}{=} \dim_K L$. Dizemos que a extensão $L \supseteq K$ é* **finita** *se $[L : K] < \infty$.*

Lema 115. *Seja k um corpo finito e seja $p = \operatorname{char} k > 0$ (um número primo). Então $|k|$ é uma potência de p.*

Definição 116. *Uma extensão de corpos $L \supseteq K$ é dita uma* **extensão simples** *se L pode ser gerado (como corpo, ver definição 109) por um único elemento sobre K: $L = K(\theta)$ para algum $\theta \in L$.*

Lema 117 (Construindo extensões algébricas simples)**.** *Seja K um corpo qualquer e seja $p(x) \in K[x]$ um polinômio irredutível de grau $d = \deg p(x) > 0$. Então o anel quociente*

$$L \stackrel{\text{def}}{=} K[x]/\big(p(x)\big) = K + K \cdot \overline{x} + \cdots + K \cdot \overline{x}^{d-1}$$

é um corpo. Via o morfismo natural $K \hookrightarrow K[x]/\big(p(x)\big)$, L é uma extensão finita de K de grau $[L : K] = d$ e uma base de L sobre K é $1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{d-1}$.

Corolário 118. *Seja $L \supseteq K$ uma extensão simples de corpos, digamos $L = K(\theta)$ com $\theta \in L$. Se θ é transcendente sobre K, então $L \cong K(x)$. Por outro lado, se θ é algébrico sobre K com polinômio minimal $m(x) \in K[x]$ de grau $d = \deg m(x)$, temos:*

(i) Há um isomorfismo K-linear de anéis

$$\begin{aligned} K[x]/\big(m(x)\big) &\xrightarrow{\approx} K[\theta] \\ \overline{f(x)} &\mapsto f(\theta) \end{aligned}$$

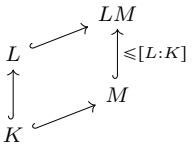
(ii) O subanel de L gerado por θ sobre K é um corpo, logo

$$L = K(\theta) = K[\theta]$$

(iii) A extensão $L \supseteq K$ é finita com $[L : K] = d$; uma base de L sobre K é dada por $1, \theta, \theta^2, \ldots, \theta^{d-1}$.

Teorema 119 (Lema de Graus)**.** *Sejam $M \supseteq L \supseteq K$ extensões de corpos com $[M : L] = n$ e $[L : K] = m$. Se $\tau_1, \ldots, \tau_n$ é uma base de M sobre L e se $\omega_1, \ldots, \omega_m$ é uma base de L sobre K então os mn elementos $\tau_i \omega_j$ com $1 \leqslant i \leqslant n$ e $1 \leqslant j \leqslant m$ formam uma base de M sobre K. Em particular, $[M : K] = [M : L] \cdot [L : K]$.*

Lema 120 (Transporte paralelo)**.** *Sejam K, L, M subcorpos de um corpo Ω. Suponha que $L \supseteq K$ e $M \supseteq K$ com $[L : K] < \infty$. Seja LM o compósito de L e M em Ω (i.e., o menor subcorpo de Ω contendo L e M).*



Então a extensão $LM \supseteq M$ é finita, com $[LM : M] \leqslant [L : K]$. Em particular, se $M \supseteq K$ também é uma extensão finita, então

$$[LM : K] \leqslant [L : K] \cdot [M : K]$$

com igualdade sempre que $\operatorname{mdc}([L : K], [M : K]) = 1$.

Teorema 121 (Critério de algebricidade)**.** *Seja $L \supseteq K$ uma extensão de corpos e seja $\theta \in L$. Então*

$$\theta \text{ é algébrico sobre } K \iff [K(\theta) : K] < \infty$$

Corolário 122 (Algebricidade)**.** *Seja $L \supseteq K$ uma extensão de corpos.*

(i) $L \supseteq K$ finita $\implies$ $L \supseteq K$ algébrica (mas, em geral, a recíproca é falsa).

(ii) O conjunto de todos os elementos de L que são algébricos sobre K forma um subcorpo de L. Em outras palavras,

$$\begin{aligned} &\alpha, \beta \in L \text{ algébricos sobre } K \\ &\implies \alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}\ (\beta \neq 0) \text{ algébricos sobre } K \end{aligned}$$

(iii) (Transitividade) "Algébrico sobre algébrico é algébrico":

$$\begin{cases} M \supseteq L \text{ algébrica e} \\ L \supseteq K \text{ algébrica} \end{cases} \implies M \supseteq K \text{ algébrica}$$

Definição 123. *Um número $\alpha \in \mathbb{R}$ é dito* **construtível** *se $|\alpha|$ é o comprimento de um segmento que pode ser obtido a partir de um segmento de tamanho 1 (o "segmento de referência") utilizando apenas construções com régua (sem marcação) e compasso. Denotaremos o conjunto de todos os números construtíveis por C.*

Teorema 124 (Construtibilidade)**.** *Um número $\alpha \in \mathbb{R}$ é construtível se, e só se, existe uma torre de extensões de corpos*

$$K_0 = \mathbb{Q} \subseteq K_1 \subset K_2 \subset \cdots \subset K_n$$

com $\alpha \in K_n$ e $[K_{i+1} : K_i] = 2$ para todo i. Em particular, se α é construtível então $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é necessariamente uma potência de 2.

Definição 125. *Seja K um corpo e seja $f(x) \in K[x]$ um polinômio de grau $n \geqslant 1$. Um corpo L contendo K é dito um* **corpo de decomposição** *ou* **corpo de raízes** *de $f(x)$ sobre K se $f(x)$ se fatora completamente em fatores lineares em $L[x]$ e L é gerado pelas raízes de $f(x)$ sobre K, i.e., podemos escrever*

$$f(x) = (x - \theta_1) \ldots (x - \theta_n) \qquad (\theta_i \in L)$$

e

$$L = K(\theta_1, \ldots, \theta_n)$$

Em outras palavras, o corpo de raízes de $f(x)$ sobre K é o corpo gerado sobre K por **todas** *as raízes de $f(x)$.*

Definição 126. *Um corpo Ω é dito* **algebricamente fechado** *se satisfaz as seguintes condições equivalentes:*

(i) toda extensão algébrica $L \supseteq \Omega$ é trivial (i.e., $L = \Omega$);

(ii) os únicos polinômios irredutíveis em $\Omega[x]$ são os lineares, i.e., os da forma $ax + b$ ($a, b \in \Omega$ com $a \neq 0$);

(iii) todo polinômio $p(x) \in \Omega[x]$ de grau $n \geqslant 1$ se fatora como um produto de n fatores lineares em $\Omega[x]$;

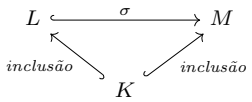
(iv) todo polinômio $p(x)$ não constante em $\Omega[x]$ possui raiz em Ω.

Teorema 127. *Dado um corpo K, existe uma extensão algébrica $K^{\mathrm{alg}} \supseteq K$ com K^{alg} algebricamente fechado, único a menos de K-isomorfismo.*

Definição 128. *Sejam K um corpo e $\theta \in K^{\mathrm{alg}}$. Seja $m(x) \in K[x]$ o polinômio minimal de θ sobre K. As raízes de $m(x)$ em K^{alg} são chamadas de* **conjugados** *de θ sobre K.*

Definição 129. *Sejam $L \supseteq K$ e $M \supseteq K$ duas extensões de corpos.*

(i) Uma **K-imersão** *$\sigma\colon L \hookrightarrow M$ é um morfismo de corpos que satisfaz $\sigma(a) = a$ para todo $a \in K$, ou seja, é uma imersão $\sigma\colon L \hookrightarrow M$ que faz o seguinte diagrama comutar:*



Observe que uma imersão $\sigma\colon L \hookrightarrow M$ é uma K-imersão se, e só se, ela for K-linear.

(ii) Um **K-automorfismo** *$\sigma\colon L \xrightarrow{\approx} L$ é um automorfismo de L que é uma K-imersão (i.e., um automorfismo de L que é K-linear). O conjunto de todos os K-automorfismos de L*

$$\mathrm{Aut}_K(L) \stackrel{\mathrm{def}}{=} \{\sigma\colon L \xrightarrow{\approx} L \mid \sigma \text{ é um } K\text{-automorfismo }\}$$

é um grupo com a operação de composição de funções $\circ$.

Seja $\varphi\colon K \hookrightarrow L$ uma imersão de corpos. Dado um polinômio

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

denotamos por

$$f^{\varphi}(x) \stackrel{\mathrm{def}}{=} \varphi(a_n)\cdot x^n + \varphi(a_{n-1})\cdot x^{n-1} + \cdots + \varphi(a_0) \in L[x]$$

o polinômio obtido aplicando-se φ aos coeficientes de $f(x)$. Note que $\varphi\colon K \hookrightarrow L$ induz um morfismo de anéis

$$\begin{aligned}\varphi\colon K[x] &\to L[x]\\ f(x) &\mapsto f^{\varphi}(x)\end{aligned}$$

que, por simplicidade de notação, ainda denotaremos por φ.
Embora quase uma tautologia, o seguinte *Princípio do Picles* resume toda a ideia central da teoria de Galois: automorfismos preservam raízes conjugadas.

Lema 130 (Princípio do Picles ou Raízes em Conserva)**.** *Seja $\varphi\colon K \hookrightarrow L$ uma imersão de corpos e seja $f(x) \in K[x]$. O morfismo φ conserva raízes: se $\theta \in K$ é raiz de $f(x) \in K[x]$ então $\varphi(\theta) \in L$ é raiz de $f^{\varphi}(x) \in L[x]$:*

$$f(\theta) = 0 \implies f^{\varphi}(\varphi(\theta)) = 0 \qquad (\theta \in L)$$

Em particular, se $L \supseteq K$ é uma extensão algébrica de corpos, então $\sigma \in \mathrm{Aut}_K(L)$ preserva raízes conjugadas sobre K:

$$\sigma\left(\text{  }\right) = \text{}$$

Lema 131 (Lema Fundamental da Teoria de Galois)**.** *Sejam*

- *$\sigma\colon K \xrightarrow{\approx} K'$ um isomorfismo de corpos;*
- *$K(\theta) \supseteq K$ uma extensão simples;*
- *$L' \supseteq K'$ uma extensão qualquer de corpos;*
- *$f(x) \in K[x]$ o polinômio minimal de θ sobre K.*

$$\begin{array}{ccc} K(\theta) & \overset{\tilde{\sigma}}{\dashrightarrow} & L' \\ {\scriptstyle\text{inclusão}}\uparrow & & \uparrow{\scriptstyle\text{inclusão}} \\ K & \xrightarrow[\approx]{\sigma} & K' \end{array}$$

Temos uma bijeção Ξ entre extensões $\tilde{\sigma}\colon K(\theta) \hookrightarrow L'$ de σ e raízes de $f^{\sigma} \in K'[x]$ em L', dada por

$$\begin{aligned}\Xi\colon \left\{ \begin{array}{c} \text{imersões } \tilde{\sigma}\colon K(\theta) \hookrightarrow L' \\ \text{com } \tilde{\sigma}|_K = \sigma \end{array} \right\} &\xrightarrow{\approx} \{\theta' \in L' \mid f^{\sigma}(\theta') = 0\}\\ \tilde{\sigma} &\mapsto \tilde{\sigma}(\theta)\end{aligned}$$

Assim, há tantas imersões $\tilde{\sigma}\colon K(\theta) \hookrightarrow L'$ estendendo σ quanto raízes de f^{σ} em L'.

Definição 132. *Seja K um corpo e seja $L \supseteq K$ uma extensão finita de corpos.*

(i) Um polinômio $f(x) \in K[x]$ é dito **separável** *se não possui raízes múltiplas no fecho algébrico K^{alg} de K.*

(ii) A extensão $L \supseteq K$ é dita **Galois** *ou* **galoisiana** *se L é o corpo de raízes (sobre K) de algum polinômio separável $f(x) \in K[x]$. Para uma extensão Galois $L \supseteq K$, escrevemos $\mathrm{Gal}(L/K)$ no lugar de $\mathrm{Aut}_K(L)$ e chamamos $\mathrm{Gal}(L/K)$ de* **grupo de Galois** *desta extensão.*

(iii) Dado um subgrupo $H \leqslant \mathrm{Aut}_K(L)$, denotamos o subcorpo fixo por H por

$$L^H \stackrel{\mathrm{def}}{=} \{\theta \in L \mid \sigma(\theta) = \theta \text{ para todo } \sigma \in H\}$$

Corolário 133. *Seja $L \supseteq K$ uma extensão finita de corpos. Então*

$$|\mathrm{Aut}_K(L)| \leqslant [L : K]$$

com igualdade se $L \supseteq K$ for Galois.

Teorema 134 (Teorema Fundamental da Teoria de Galois)**.** *Seja $L \supseteq K$ uma extensão finita de corpos Galois. Temos uma bijeção natural*

$$\Gamma\colon \left\{ \begin{array}{c} \text{subgrupos} \\ H \leqslant \mathrm{Gal}(L/K) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subcorpos intermediários} \\ M \text{ de } L \supseteq K \end{array} \right\}$$

$$\begin{aligned} H &\longmapsto L^H\\ \mathrm{Gal}(L/M) &\longmapsfrom M\end{aligned}$$

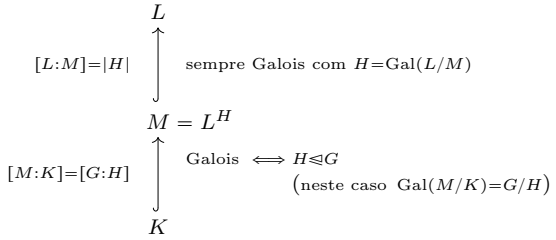
sendo a extensão intermediária "superior" $L \supseteq M$ sempre Galois com $[L : M] = |\mathrm{Gal}(L/M)|$ enquanto a extensão intermediária "inferior" $M \supseteq K$ satisfaz $[M : K] = [\mathrm{Gal}(L/K) : \mathrm{Gal}(L/M)]$ e

$$M \supseteq K \text{ Galois} \iff \mathrm{Gal}(L/M) \trianglelefteq \mathrm{Gal}(L/K)$$

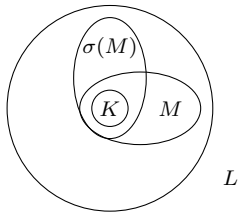
Se $M \supseteq K$ é Galois, temos um isomorfismo natural induzido pela restrição:

$$\begin{aligned}\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) &\xrightarrow{\approx} \mathrm{Gal}(M/K)\\ \overline{\sigma} &\mapsto \sigma|_M\end{aligned}$$

Podemos resumir o teorema pictoricamente da seguinte forma: se $G = \mathrm{Gal}(L/K)$ e $H \leqslant G$ então



Observe que se $L \supseteq K$ é Galois, L sendo corpo de raízes sobre K de um polinômio separável $f(x) \in K[x]$, então L também será corpo de raízes sobre M deste mesmo polinômio $f(x) \in K[x] \subseteq M[x]$, logo a extensão do topo $L \supseteq M$ é sempre Galois.



Lema 135 (Truque das órbitas)**.** *Seja $L \supseteq K$ uma extensão finita de corpos e seja $G = \mathrm{Aut}_K(L)$. Seja $\theta \in L$ e $H \leqslant G$ um subgrupo. Então*

$$f(x) \stackrel{\mathrm{def}}{=} \prod_{\sigma \in H} (x - \sigma(\theta)) \in L^H[x]$$

Em particular, o polinômio minimal de θ sobre L^H divide $f(x)$.

Teorema 136 (Extensões radicais são cíclicas)**.** *Seja K um corpo e seja $r \in \mathbb{N}_{>0}$. Suponha que K contenha todas as raízes r-ésimas da unidade, i.e., que $|\mu_r(K)| = r$. Considere uma extensão radical de K da forma*

$$L \stackrel{\mathrm{def}}{=} K(\beta) \supseteq K \qquad (\alpha \stackrel{\mathrm{def}}{=} \beta^r \in K)$$

com $\beta \neq 0$. Então $L \supseteq K$ é Galois e há um morfismo injetor de grupos

$$\begin{aligned}\mathrm{Gal}(L/K) &\hookrightarrow \mu_r(K)\\ \sigma &\mapsto \sigma(\beta)/\beta\end{aligned}$$

Em particular, $\mathrm{Gal}(L/K)$ é um grupo cíclico cuja ordem divide r.

Lema 137 (Critério da derivada)**.** *Um polinômio $f(x) \in K[x]$ é separável se, e só se, $\mathrm{mdc}(f(x), f'(x)) = 1$. Em particular, se $f(x)$ é irredutível em $K[x]$, então $f(x)$ é separável se, e só se, $f'(x) \neq 0$.*

Corolário 138. *Sejam K um corpo e $f(x) \in K[x]$ um polinômio* **irredutível**

(i) Se $\mathrm{char}\, K = 0$ então $f(x)$ é sempre separável.

(ii) Se $\operatorname{char} K = p > 0$ *então* $f(x)$ *é inseparável se, e só se, existe* $g(x) \in K[x]$ *tal que* $f(x) = g(x^p)$*. Em particular, qualquer polinômio não constante* $f(x) \in K[x]$ *pode ser escrito como* $f(x) = h(x^{p^n})$ *para algum* $n \in \mathbb{N}$ *e algum polinômio separável* $h(x) \in K[x]$*.*

Definição 139. *Dada uma extensão algébrica de corpos* $L \supseteq K$*, diremos que um elemento* $\theta \in L$ *é* **separável** *sobre* K *se seu polinômio minimal sobre* K *for separável. Diremos que* $L \supseteq K$ *é* **separável** *se todo elemento* $\theta \in L$ *for separável; caso contrário, dizemos (surpresa!) que esta extensão é* **inseparável**.

Definição 140. *Dizemos que um corpo* K *é* **perfeito** *se* $\operatorname{char} K = 0$ *ou* $p = \operatorname{char} K > 0$ *e o morfismo de Frobenius*

$$\begin{aligned} \Phi\colon K &\hookrightarrow K \\ \theta &\mapsto \theta^p \end{aligned}$$

é sobrejetor (i.e., todo elemento de K *é uma* p*-ésima potência), logo um automorfismo de* K*.*

Lema 141. *Toda extensão algébrica* $L \supseteq K$ *de um corpo perfeito* K *é separável.*

Teorema 142 (Critério imersivo de separabilidade)**.** *Seja* $\sigma\colon K \hookrightarrow \Omega$ *uma imersão fixada de um corpo* K *em um corpo algebricamente fechado* Ω *(por exemplo, a inclusão de* K *em um fecho algébrico* $\Omega = K^{\mathrm{alg}}$*). Seja* $L \supseteq K$ *uma extensão finita de corpos e seja* $N(L; K; \sigma)$ *o número de imersões* $\tilde{\sigma}\colon L \hookrightarrow \Omega$ *estendendo* σ*, como no diagrama a seguir.*

$$\begin{array}{ccc} L & \overset{\tilde{\sigma}}{\dashrightarrow} & \Omega \\ {\scriptstyle \text{inclusão}}\uparrow & \nearrow_{\sigma} & \\ K & & \end{array}$$

Então $N(L; K; \sigma) \leqslant [L : K]$ *com igualdade se, e só se,* $L \supseteq K$ *é separável.*

Corolário 143. *Sejam* $M \supseteq L \supseteq K$ *extensões algébricas de corpos.*

(i) ("Separável sobre separável é separável")

$$M \supseteq K \text{ é separável} \iff M \supseteq L \text{ e } L \supseteq K \text{ são separáveis}$$

(ii) Se $L = K(\theta_1, \ldots, \theta_n)$ *então* $\theta_1, \ldots, \theta_n$ *são separáveis sobre* K *se, e só se, a extensão* $L \supseteq K$ *é separável. Em particular, o corpo de raízes de um polinômio separável dá origem a uma extensão separável.*

Teorema 144 (Teorema do Elemento Primitivo)**.** *Seja* $L \supseteq K$ *uma extensão finita separável de corpos. Então* $L \supseteq K$ *é uma extensão simples, i.e., existe um elemento* $\theta \in L$ *tal que* $L = K(\theta)$*.*

Definição 145. *Seja* $L \supseteq K$ *uma extensão de corpos de característica* $p > 0$*. Dizemos que* $L \supseteq K$ *é* **puramente inseparável** *se para todo* $\theta \in L$ *existe um* $n \in \mathbb{N}$ *(que depende de* θ*) tal que* $\Phi^n(\theta) = \theta^{p^n} \in K$ *(aqui,* $\Phi\colon L \hookrightarrow L$ *denota o morfismo de Frobenius).*

Lema 146 (Fecho separável)**.** *Seja* $L \supseteq K$ *uma extensão algébrica de corpos de característica* $p > 0$*. O subconjunto* $\tilde{K} \subseteq L$ *dos elementos separáveis sobre* K *forma um subcorpo de* L*. Além disso, a sub-extensão* $L \supseteq \tilde{K}$ *é puramente inseparável:*

$$\begin{array}{c} L \\ \Big\uparrow {\scriptstyle \text{puramente inseparável}} \\ \tilde{K} \\ \Big\uparrow {\scriptstyle \text{separável}} \\ K \end{array}$$

O corpo $\tilde{K}$ *é chamado de* **fecho separável** *de* K *em* L*.*

Definição 147. *Seja* $L \supseteq K$ *uma extensão algébrica e seja* K^{alg} *um fecho algébrico de* L *(e portanto também de* K *pelo corolário 122). A extensão* $L \supseteq K$ *é dita* **normal** *ou* **quase-Galois** *se satisfaz as seguintes condições equivalentes:*

(i) dado um polinômio **irredutível** $f(x) \in K[x]$*, se* $f(x)$ *possui uma raiz* $\theta \in L$*, então* $f(x)$ *se fatora completamente em fatores lineares em* $L[x]$*.*

(ii) L *é fechado por* K*-conjugados: dado* $\theta \in L$*, todos os conjugados (em* K^{alg}*) sobre* K *de* θ *pertencem a* L*.*

(iii) L *é o corpo de raízes de alguma família de polinômios* $S \subseteq K[x]$*.*

Corolário 148 (Ação transitiva sobre conjugados)**.** *Seja* $L \supseteq K$ *uma extensão quase-Galois finita de corpos. Se* $\alpha, \beta \in L$ *são conjugados sobre* K*, então existe* $\sigma \in \operatorname{Aut}_K(L)$ *tal que* $\sigma(\alpha) = \beta$*.*

Teorema 149. *Seja* $L \supseteq K$ *uma extensão finita de corpos. As seguintes condições são equivalentes:*

(a) $L \supseteq K$ *é normal e separável;*

(b) L *é o corpo de raízes sobre* K *de um polinômio separável* $f(x) \in K[x]$*;*

(c) $|\operatorname{Aut}_K(L)| = [L : K]$*.*

Se estas condições são satisfeitas, diremos que $L \supseteq K$ *é uma* **extensão Galois**.

Teorema 150. *Seja* p *um número primo e seja* $n \geqslant 1$ *um inteiro. Então existe um corpo finito* $\mathbb{F}_q$ *com* $q = p^n$ *elementos, único a menos de isomorfismo. Mais precisamente, para cada* $n \in \mathbb{N}$ *positivo, existe um único corpo intermediário* $\mathbb{F}_q$ *de* $\mathbb{F}_p^{\mathrm{alg}} \supset \mathbb{F}_p$ *com* $[\mathbb{F}_q : \mathbb{F}_p] = n$*, a saber, o corpo de raízes do polinômio* $f(x) = x^q - x \in \mathbb{F}_p[x]$*.*

Teorema 151 (Raízes da unidade)**.** *Seja* k *um corpo e seja* G *um subgrupo finito de* $k^\times$ *(i.e.,* G *é um grupo finito de raízes da unidade em* k*, pelo teorema de Lagrange). Então* G *é cíclico.*

Definição 152. *Seja* $L \supseteq K$ *uma extensão finita de corpos. A* **norma** $N_{L/K}\colon L \to K$ *e o* **traço** $\operatorname{Tr}_{L/K}\colon L \to K$ *são os mapas definidos por*

$$N_{L/K}(\beta) = \det(m_\beta) \quad e \quad \operatorname{Tr}_{L/K}(\beta) = \operatorname{Tr}(m_\beta) \qquad (\beta \in L)$$

em que m_β *denota a aplicação* K*-linear de* L *em* L *dada pela multiplicação por* β*:*

$$\begin{aligned} m_\beta\colon L &\to L \\ x &\mapsto \beta x \end{aligned}$$

Lema 153. *Seja* $L \supseteq K$ *uma extensão finita de corpos de grau* $n = [L : K]$*.*

(i) O traço é K*-linear e a norma é multiplicativa: para todo* $\beta_1, \beta_2 \in L$ *e* $\alpha_1, \alpha_2 \in K$*,*

$$\operatorname{Tr}_{L/K}(\alpha_1\beta_1 + \alpha_2\beta_2) = \alpha_1 \operatorname{Tr}_{L/K}(\beta_1) + \alpha_2 \operatorname{Tr}_{L/K}(\beta_2) \qquad e$$
$$N_{L/K}(\beta_1 \cdot \beta_2) = N_{L/K}(\beta_1) \cdot N_{L/K}(\beta_2)$$

Em particular, se $\alpha \in K$ *então*

$$\operatorname{Tr}_{L/K}(\alpha) = n\alpha \qquad e \qquad N_{L/K}(\alpha) = \alpha^n$$

(ii) (Transitividade) Sejam $M \supseteq L \supseteq K$ *extensões finitas de corpos. Temos*

$$\operatorname{Tr}_{M/K} = \operatorname{Tr}_{L/K} \circ \operatorname{Tr}_{M/L} \qquad e \qquad N_{M/K} = N_{L/K} \circ N_{M/L}$$

(iii) Suponha que $L \supseteq K$ *seja separável e sejam* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *as* K*-imersões de* L *em um fecho algébrico* K^{alg} *de* K *(ver 142). Para todo* $\beta \in L$ *temos*

$$\operatorname{Tr}_{L/K}(\beta) = \sum_{1 \leqslant i \leqslant n} \sigma_i(\beta) \qquad e \qquad N_{L/K}(\beta) = \prod_{1 \leqslant i \leqslant n} \sigma_i(\beta)$$

Definição 154. *Seja* K *um corpo e seja* $p(T) \in K[T]$*. Dizemos que* $p(T)$ *é* **solúvel por radicais** *se existe uma torre radical*

$$K_0 \overset{\text{def}}{=} K \subset K_1 \subset K_2 \subset \cdots \subset K_s$$

($K_{i+1} = K_i(\delta_i)$*,* $\delta_i^{r_i} \in K_i$ *para algum* $r_i \in \mathbb{N}_{>0}$*) em que* K_s *contém o corpo de raízes de* $p(T)$ *sobre* K_0*.*

Teorema 155 (Abel-Ruffini)**.** *Sejam* $L = \mathbb{C}(x_1, \ldots, x_n)$ *e* $K = \mathbb{C}(e_1, \ldots, e_n)$*, em que* $e_1, \ldots, e_n$ *denotam os polinômios simétricos elementares nas variáveis* $x_1, \ldots, x_n$*. O polinômio genérico de grau* $n \geqslant 5$

$$\begin{aligned} p(T) &\overset{\text{def}}{=} (T - x_1)(T - x_2)\ldots(T - x_n) \\ &= T^n - e_{n-1}T^{n-1} + \cdots + (-1)^n e_n \in K[T] \end{aligned}$$

não é solúvel por radicais.

Referências

[1] Artin, Algebra

[2] Dummit e Foote, Abstract Algebra

[3] Fraleigh, A First Course in Abstract Algebra

[4] Garcia e Lequain, Álgebra: um Curso de Introdução

[5] Gallian, Abstract Algebra

[6] Hadlock, Field theory and its classical problems

[7] Herstein, Topics in Algebra

[8] Jacobson, Basic Algebra I

[9] Lang, Algebra

[10] Martins e Tengan, Álgebra exemplar

[11] Stewart, Galois Theory