ÁLGEBRA MINIMAL PARA A GRADUAÇÃO

Teoremas e definições

1. Grupos e ações

1.1. Definição. Um conjunto G munido de uma operação binária $\cdot : G\times G \to G$, $\cdot : (g_1, g_2) \mapsto g_1 \cdot g_2$, é dito um *grupo* se são válidos os axiomas seguintes:

GA. $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ para todos $g_1, g_2, g_3 \in G$ (a multiplicação é *associativa*).
G1. Existe $e \in G$ tal que $e \cdot g = g \cdot e = g$ para todo $g \in G$ (existe um elemento *neutro*; tal elemento é necessariamente único).
GI. Para todo $g \in G$, existe $g' \in G$ tal que $g \cdot g' = g' \cdot g = e$ (todo elemento $g \in G$ possui seu *inverso*; o inverso de todo elemento de G é necessariamente único).

Podemos usar outros sinais para a operação: $+$, $\oplus$, $\odot$, $*$, $\star$, $\circ$, ... Usando a notação *multiplicativa,* normalmente denotamos o elemento neutro por 1 e o inverso de g por g^{-1}. (Note que $1^{-1} = 1$ e $(g^{-1})^{-1} = g$.) Na notação *aditiva,* envolvendo $+$, é melhor denotar o elemento neutro por 0 e o inverso de g por $-g$. Assim, os axiomas no caso aditivo tornam-se $(g_1+g_2)+g_3 = g_1+(g_2+g_3)$, $0+g = g+0 = g$, $g + (-g) = (-g) + g = 0$.

O "número" de elementos do grupo G (finito ou infinito) se chama a *ordem* de G.

1.2. Observação. A associatividade da operação possibilita omitir parênteses em produtos. Por exemplo, no lugar de $a \cdot \big(b \cdot (c \cdot d)\big)$ ou de $\big((a \cdot b) \cdot c\big) \cdot d$, podemos escrever simplesmente $a \cdot b \cdot c \cdot d$, pois

$$\big((a \cdot b) \cdot c\big) \cdot d = [\text{tomando em } \mathbf{GA}\ g_1 = a \cdot b,\ g_2 = c,\ g_3 = d] = (a \cdot b) \cdot (c \cdot d) = \\ = [\text{tomando em } \mathbf{GA}\ g_1 = a,\ g_2 = b,\ g_3 = c \cdot d] = a \cdot \big(b \cdot (c \cdot d)\big).$$

1.3. Observação. $(g_1 \cdot g_2 \cdot \ldots \cdot g_n)^{-1} = g_n^{-1} \cdot \ldots \cdot g_2^{-1} \cdot g_1^{-1}$.

1.4. Observação. Sejam $f_1 : M_1 \to M_2$ e $f_2 : M_2 \to M_3$ funções entre conjuntos. A operação de *composição* ou *composta* $f_2 \circ f_1 : M_1 \to M_3$, definida por $(f_2 \circ f_1)m_1 := f_2(f_1 m_1)$ para todo $m_1 \in M_1$ é associativa (quando definida). Isto é: se $f_1 : M_1 \to M_2$, $f_2 : M_2 \to M_3$ e $f_3 : M_3 \to M_4$ são funções entre conjuntos, então $(f_3 \circ f_2) \circ f_1 = f_3 \circ (f_2 \circ f_1)$.

Denotemos por 1_M a função *idêntica* $1_M : M \to M$, $1_M : m \mapsto m$. Seja $f : M_1 \to M_2$ qualquer função. Então $1_{M_2} \circ f = f = f \circ 1_{M_1}$.

Uma função $b : M_1 \to M_2$ é *bijetora* se e só se existe uma função $b' : M_2 \to M_1$ tal que $b \circ b' = 1_{M_2}$ e $b' \circ b = 1_{M_1}$. Para toda função b, esta *inversa* b' é única, se existir; denotâmo-la por b^{-1}.

1.5. Exemplos. 1. Seja M um conjunto. Então o conjunto $\Sigma M = \{b : M \to M \mid b \text{ é uma bijeção}\}$ munido da operação composta $\circ$ é um grupo chamado *grupo simétrico* de M ou *grupo das permutações* de M. Por exemplo, se $M = \{1, 2, 3, 4, 5\}$, podemos exibir os elementos de $\Sigma_5 := \Sigma M$ na forma do tipo $\binom{12345}{23145}$. Calculando, obtemos $\binom{12345}{23145} \cdot \binom{12345}{54321} = \binom{12345}{54132} \neq \binom{12345}{43521} = \binom{12345}{54321} \cdot \binom{12345}{23145}$. Isto significa que o grupo Σ_5 não é comutativo. É fácil verificar que $\binom{12345}{23145}^{-1} = \binom{12345}{31245}$.

1.5.2. Seja $G = 0$ ou $G = \mathbb{Z}$ ou $G = \mathbb{Q}$ ou $G = \mathbb{R}$ ou $G = \mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$ ou $G = \mathbb{C}$. Então $(G, +)$ é um grupo, onde $+$ é a adição usual de números.

1.5.3. Seja p um número primo e seja $G := \{q \in \mathbb{Q} \mid q$ admite a forma de fração de números inteiros com o denominador não divisível por $p\}$. Então $(G, +)$ é um grupo, onde $+$ é a adição usual.

1.5.4. Seja $G = 1$ ou $G = \{1, -1\}$ ou $G = \{1, -1, i, -i\}$ ou $G = \mathbb{Q}^* := \mathbb{Q} \setminus 0$ ou $G = \mathbb{R}^* := \mathbb{R} \setminus 0$ ou $G = \mathbb{R}^{>0} := \{r \in \mathbb{R} \mid r > 0\}$ ou $G = \mathbb{C}^* = \mathbb{C} \setminus 0$ ou $G = \mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$. Então $(G, \cdot)$ é um grupo, onde $\cdot$ é a multiplicação usual de números.

1.5.5. Sejam G_1 e G_2 grupos. Definimos em $G_1 \times G_2$ a operação $(g_1, g_2) \cdot (g_1', g_2') := (g_1 \cdot g_1', g_2 \cdot g_2')$. Então $(G_1 \times G_2, \cdot)$ é um grupo chamado *produto cartesiano* ou *produto direto* de G_1 e G_2.

1.5.6. Seja $A = \mathbb{Z}$ ou $A = \mathbb{Z}[i]$ ou $A = \mathbb{Q}$ ou $A = \mathbb{R}$ ou $A = \mathbb{C}$. O conjunto $G = \operatorname{Matr}_{m\times n} A$ de todas as $m \times n$-matrizes com coeficientes em A munido da adição usual de matrizes é um grupo $(G, +)$.

1.5.7. O conjunto $\operatorname{GL}_n A := \{M \in \operatorname{Matr}_{n\times n} A \mid \det M \neq 0\}$, onde $A = \mathbb{Q}$ ou $A = \mathbb{R}$ ou $A = \mathbb{C}$, munido da multiplicação usual de matrizes é um grupo chamado de *grupo linear*.

1.5.8. O conjunto $\operatorname{O}_n A := \{M \in \operatorname{Matr}_{n\times n} A \mid M$ é ortogonal$\}$, onde $A = \mathbb{Q}$ ou $A = \mathbb{R}$ ou $A = \mathbb{C}$ munido da multiplicação usual de matrizes é um grupo chamado de *grupo ortogonal*. (Uma matriz quadrada M se chama *orthogonal* se $MM^t = M^tM = 1$.)

1.5.9. Seja $M = \{v_1, v_2, \ldots, v_n\}$ o conjunto de todos os vértices de um polígono regular P_n no plano. Façamos

$$\operatorname{D}_n := \big\{\sigma \in \Sigma M \mid \operatorname{dist}(v_i, v_j) = \operatorname{dist}(\sigma v_i, \sigma v_j) \text{ para todos } i, j\big\},$$

onde "dist" denota distância entre dois pontos. Em outras palavras, D_n é conjunto de todas as simetrias de P_n. Obtemos o grupo *diedral* $(\operatorname{D}_n, \circ)$, onde $\circ$ é a composta usual de simetrias.

1.6. Definição. Seja G um grupo e seja $H \subset G$. Dizemos que H é um *subgrupo* de G e escrevemos $H \leqslant G$ se são válidas as seguintes propriedades:

SG1. $1 \in H$.
SGM. $h_1, h_2 \in H \Rightarrow h_1 \cdot h_2 \in H$.
SGI. $h \in H \Rightarrow h^{-1} \in H$.

Assim, um subgrupo é um subconjunto fechado relativamente às operações do grupo: a escolha da unidade, a multiplicação e a operação de tomar inverso. Note que qualquer subgrupo é um grupo: a operação é a induzida.

Todo grupo G contém subgrupos $1 \leqslant G$ (*trivial*) e $G \leqslant G$. Um subgrupo diferente destes se chama subgrupo *próprio*.

1.7. Critério. *Seja G um grupo e seja $\varnothing \neq H \subset G$. Então*

$$H \leqslant G \Leftrightarrow \textbf{SG. } h_1, h_2 \in H \Rightarrow h_1 \cdot h_2^{-1} \in H.$$

1.8. Observação. Seja G um grupo. A interseção $H = \bigcap\limits_{i\in I} H_i$ de qualquer família de subgrupos $H_i \leqslant G$, $i \in I$, é um subgrupo. Em particular, $\langle S\rangle := \bigcap\limits_{S\subset H\leqslant G} H$ é o subgrupo mínimo que contém um dado subconjuto $S \subset G$. O subgrupo $\langle S\rangle$ é dito o subgrupo *gerado* por S e S se chama conjunto de *geradores* de $\langle S\rangle$. Quando $G = \langle S\rangle$ dizemos que G é *gerado* por S ou que os elementos de S são *geradores* de G. Qualquer grupo que admite apenas um gerador se chama grupo *cíclico*. A *ordem* de $g \in G$ é simplesmente a ordem de $\langle g\rangle$.

1.9. Lema. *Seja G um grupo e seja $S \subset G$. Então*

$$\langle S\rangle = \{s_1^{\varepsilon_1} \cdot s_2^{\varepsilon_2} \cdot \ldots \cdot s_n^{\varepsilon_n} \mid n \geqslant 0,\ \varepsilon_i = \pm 1,\ s_i \in S\},$$

onde $s^{+1} = s$ e, para $n = 0$, o produto apresentado é 1 (por definição).

Seja G um grupo e seja $g \in G$. Para $0 < n \in \mathbb{N}$, denotemos $g^n := \underbrace{g \cdot \ldots \cdot g}_{n \text{ vezes}}$, $g^{-n} := (g^{-1})^n$ e $g^0 := 1$. Assim, g^m é definido para todo $m \in \mathbb{Z}$. São válidas as relações $g^m \cdot g^n = g^{m+n}$ e $(g^m)^n = g^{mn}$ para todos $m, n \in \mathbb{Z}$. Além disso, $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

1.20. Definição. Seja $h : G_1 \to G_2$ uma função entre grupos. Dizemos que h é um *homomorfismo* se

HG. $h(g \cdot g') = hg \cdot hg'$ para todos $g, g' \in G_1$.

É fácil provar que $h1 = 1$ e que $hg^{-1} = (hg)^{-1}$.

A *imagem* $hG_1 := \{hg \mid g \in G_1\}$ e o *núcleo* $h^{-1}1 = \{g \in G_1 \mid hg = 1\}$ de qualquer homomorfismo são subgrupos em G_2 e G_1, respectivamente. A composta de dois homomorfismos é um homomorfismo. A inclusão $H \hookrightarrow G$ de um subgrupo $H \leqslant G$ é um homomorfismo. Note que as imagem e imagem inversa de qualquer subgrupo por qualquer homomorfismo são subgrupos.

1.21. Lema. *Seja $h : G_1 \to G_2$ um homomorfismo entre grupos. Então h é injetivo se e só se o núcleo de h é trivial, $h^{-1}1 = 1$.*

1.22. Exemplos. 10. O grupo $(\mathbb{Z}, +)$ é cíclico: $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$. A função $\mathbb{Z} \to \langle g \rangle$, $m \mapsto g^m$, é um homomorfismo sobrejetivo entre grupos cíclicos.

1.22.11. $|\ | : \mathbb{C}^* \to \mathbb{R}^{>0}$, $|\ | : z \mapsto |z|$, é um homomorfismo.

1.22.12. $\exp : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$, $\exp : r \mapsto e^r$, é um homomorfismo.

1.22.13. $\exp 2\pi i - : (\mathbb{R}, +) \to (\mathbb{S}^1, \cdot)$, $\exp 2\pi i - : r \mapsto e^{2\pi i r}$, é um homomorfismo, onde $\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$.

1.22.14. As raízes n-ésimas da unidade (relativamente a multiplicação usual de números complexos) formam um grupo cíclico de ordem n.

1.22.15. Seja $A = \mathbb{Q}$ ou $A = \mathbb{R}$ ou $A = \mathbb{C}$, então $\det : \mathrm{GL}_n A \to A^*$, $\det : M \mapsto \det M$, é um homomorfismo.

1.22.16. Seja $A = \mathbb{Z}$ ou $A = \mathbb{Z}[i]$ ou $A = \mathbb{Q}$ ou $A = \mathbb{R}$ ou $A = \mathbb{C}$, então $\mathrm{tr} : (\mathrm{Matr}_{m \times n} A, +) \to (A, +)$, $\mathrm{tr} : M \mapsto \mathrm{tr}\, M$, é um homomorfismo.

1.23. Definição. Seja G um grupo e seja M um conjunto. Dizemos que G *age sobre* M (*à esquerda*; de maneira semelhante podemos definir *ação à direita*) e escrevemos $G \curvearrowright M$ (para a ação à direita, escrevemos $M \curvearrowleft G$) se é definida uma operação $G \times M \to M$, $(g, m) \mapsto g \cdot m$, que satisfaz os seguintes axiomas:

AG1. $1 \cdot m = m$ para todo $m \in M$.
AGA. $(g_1 \cdot g_2) \cdot m = g_1 \cdot (g_2 \cdot m)$ para todos $g_1, g_2 \in G$ e $m \in M$.

Note que ação de G sobre M não é nada mais do que um homomorfismo $h : G \to \Sigma M$, pois, a partir de uma acão $G \curvearrowright M$, podemos definir $(hg)m := g \cdot m$ e, reciprocamente, qualquer homomorfismo $h : G \to \Sigma M$ define uma ação: $g \cdot m := (hg)m$ (no caso de ação à direita, deve-se considerar um antihomomorfismo $h : G \to \Sigma M$, isto é, uma função que satisfaz a identidade $h(g_1 \cdot g_2) = hg_2 \cdot hg_1$ para todos $g_1, g_2 \in G$).

Usando a associatividade **AGA**, podemos omitir os parêntesis nas fórmulas do tipo $(g_1 \cdot g_2) \cdot (g_3 \cdot m)$. Além disso, $g \cdot m_1 = m_2$ implica $g^{-1} \cdot m_2 = m_1$.

Toda ação $G \curvearrowright M$ define uma relação de equivalência em M:

$$m_1 \sim m_2 \Leftrightarrow \exists g \in G,\ m_2 = g \cdot m_1.$$

As classes desta equivalência se chamam *órbitas* da ação. Toda órbita tem a forma $Gm := \{g \cdot m \mid g \in G\}$ para qualquer seu representante $m \in M$. Denotemos por $G\backslash M$ o conjunto de todas as G-órbitas de M (para a ação $M \curvearrowleft G$, o conjunto de todas as órbitas é denotado por M/G). Temos uma função sobrejetiva $\pi : M \to G\backslash M$, $\pi : m \mapsto [m]$, que leva todo elemento $m \in M$ para a sua órbita $[m] := Gm$.

Quando existe exatamente uma órbita da ação, a ação é dita *transitiva.*

Seja $m \in M$. O subconjunto $\operatorname{Stab}_G m := \{g \in G \mid g \cdot m = m\}$ é um subgrupo de G chamado de *estabilizador* de m em G.

Dados um homomorfismo de grupos $h : G_1 \to G_2$ e uma ação $G_2 \curvearrowright M$, obtemos uma ação $G_1 \curvearrowright M$ *induzida* pelo homomorfismo: $g_1 \cdot m := (hg_1) \cdot m$. Em particular, a ação $G \curvearrowright M$ induz uma ação $H \curvearrowright M$ para cada subgrupo $H \leqslant G$.

1.24. Teorema. *Seja $G \curvearrowright M$ uma ação de um grupo sobre um conjunto. Então, para $m_1, m_2 \in M$ de uma mesma órbita (digamos $g \cdot m_1 = m_2$), os estabilizadores $\operatorname{Stab}_G m_1$ e $\operatorname{Stab}_G m_2$ são conjugados, isto é, $g \cdot \operatorname{Stab}_G m_1 \cdot g^{-1} = \operatorname{Stab}_G m_2$. Em particular, as ordens de $\operatorname{Stab}_G m_1$ e de $\operatorname{Stab}_G m_2$ são iguais.*

A cardinalidade de uma órbita Gm se calcula pela fórmula $|Gm| = |G|/|\operatorname{Stab}_G m|$.

Além disso, $|M| = \sum_{[m] \in G\backslash M} |G|/|\operatorname{Stab}_G m|$, onde $[m]$ percorre todas as órbitas $[m] \in G\backslash M$.

1.25. Exemplos. 17. Todo grupo G age sobre si mesmo pela multiplicação à esquerda: a ação $G \curvearrowright G$ é definida pela regra $g \cdot m$ para $g, m \in G$. Essa ação é transitiva e $\operatorname{Stab}_G m = 1$ para todo $m \in G$. Como esta ação define um homomorfismo $h : G \to \Sigma G$, é fácil provar o teorema de Cayley utilizando o Lema 1.21: *Todo grupo finito é um subgupo de um grupo simétrico.*

1.25.18. Seja G um grupo e seja $H \leqslant G$ um subgrupo de G. A ação do Exemplo 1.25.17 define a ação $H \curvearrowright G$ cujas órbitas Hg são ditas *classes laterais* (*à direita*) de H em G. Pelo Teorema 1.24, o número das classes laterais, dito o *índice* de H em G e denotado por $|G : H|$, é igual a $|G|/|H|$, pois o fato que $\operatorname{Stab}_G m = 1$ para a ação $G \curvearrowright G$ implica o fato que $\operatorname{Stab}_H m = 1$ para a ação $H \curvearrowright G$. Esta afirmação é o teorema de Lagrange: $|G| = |G : H| \cdot |H|$. Em particular, vemos que ordem de subgrupo divide ordem de grupo.

1.25.19. Podemos identificar o grupo Σ_{n-1} com o subgrupo de Σ_n formado por todas as permutações que preservam n. Mais detalhadamente, considerando a ação natural $G \curvearrowright M$, onde $G := \Sigma_n$ e $M := \{1, \ldots, n\}$, vemos que o subgrupo $\operatorname{Stab}_G n$ (o estabilizador de n) é, de fato, Σ_{n-1}. As classes laterais à esquerda de Σ_{n-1} em Σ_n têm a descrição seguinte: A classe "número i" é formada por todas as permutações que levam n para i.

1.25.20. É fácil ver que a ordem de $g \in G$ é o menor número natural $0 < n \in \mathbb{N}$ tal que $g^n = 1$ (ou ∞ se não existem tais números naturais). Usando o algoritmo Euclidiano, podemos demonstrar que $g^m = 1$ implica que $|g|$ divide m. Pelo teorema de Lagrange, $g^{|G|} = 1$. Em particular, todo grupo de ordem prima é cíclico.

1.25.21. No conjunto $\mathbb{Z}/n\mathbb{Z}$ de números inteiros módulo n, a mutiplicação é bem definida pela regra $\overline{a} \cdot \overline{b} := \overline{ab}$. O conjunto $G = \left\{\overline{a} \mid 0 \leqslant a < n,\ \operatorname{mdc}(a, n) = 1\right\}$ de φn elementos é um grupo relativamente à multiplicação, pois é formado por todos os elementos de $\mathbb{Z}/n\mathbb{Z}$ que possuem inversos multiplicativos. Pelo Exemplo 1.25.20, $a^{\varphi n} \equiv_n 1$ se $\operatorname{mdc}(a, n) = 1$.

1.26. Definição. Seja G um grupo e seja $N \leqslant G$ um subgrupo de G. Dizemos que N é um subgrupo *normal* de G se N é estável relativamente às conjugações por todos os elementos de G, isto é, $g \cdot n \cdot g^{-1} \in N$ para todo $n \in N$ e todo $g \in G$, ou seja, $N^G \subset N$. Neste caso, usamos a notação $N \lhd G$. Um subgrupo $N \leqslant G$ é normal se e só se $gN = Ng$ para todo $g \in G$. Definindo $g_1N \cdot g_2N := (g_1 \cdot g_2)N$, obtemos a estrutura de grupo em G/N. Assim, multiplicando as classes, usamos quaisquer seus representantes. O conjunto G/N munido desta operação se chama grupo *quociente* de G por N. A função $\pi : G \to G/N$, $\pi : g \mapsto gN$ é um homomorfismo de grupos chamado *canônico.*

1.27. Teorema (de homomorfismo)**.** *Seja $h : G_1 \to G_2$ um homomorfismo de grupos. Denotemos por $N := h^{-1}1$ o seu núcleo. Então $N \lhd G_1$ e existe um único homomorfismo $h_0 : G_1/N \to G_2$ tal que $h_0 \circ \pi = h$. Este h_0 é injetivo. Além disso, o homomorfismo h estabelece uma correspondência bijetora entre os subgrupos de G_1 que contêm o núcleo N e os subgrupos da imagem hG_1. Esta correspondência*

preserva a inclusão de subgrupos e leva os subgrupos normais de G_1 (que contêm N) exatamente para os subgrupos normais de hG_1.

Sejam G_1 e G_2 grupos. Um homomorfismo $h : G_1 \to G_2$ se chama *monomorfismo* (*epimorfismo, isomorfismo*) se a função h é injetora (sobrejetora, bijetora, respectivamente). É fácil verificar que a bijeção inversa a um isomorfismo também é um homomorfismo (e, portanto, um isomorfismo). Grupos isomorfos têm as mesmas propriedades algébricas. Todo monomorfismo é, de fato, um subgrupo. (Melhor dizer que todo monomorfismo é um isomorfismo com um subgrupo.) Assim, o Teorema 1.27 pode ser lido da maneira seguinte: *Todo homomorfismo entre grupos pode ser decomposto em um epimorfismo e um monomorfismo. Todo epimorfismo é, de fato, o homomorfimo canônico do quociente do grupo por um subgrupo normal* (*o núcleo do homomorfismo*). *O homomorfismo canônico produz uma correspondência* ...

Qualquer isomorfismo de um grupo G com si mesmo se chama *automorfismo* de G. Denotemos por $\operatorname{Aut} G$ o conjunto de todos os automorfismos de G. Assim, $\operatorname{Aut} G \leqslant \Sigma G$. Para dois grupos G_1 e G_2, denotemos por $\operatorname{Hom}(G_1, G_2)$ o conjunto de todos os homomorfismos de G_1 para G_2. Qualquer homomorfismo de um grupo G para si mesmo se chama *endomorfismo* de G. Denotemos por $\operatorname{End} G$ o conjunto de todos os endomorfismos de G. Assim, $\operatorname{End} G = \operatorname{Hom}(G, G)$.

1.28. Observação. Seja G um grupo. A interseção $N = \bigcap_{i \in I} N_i$ de qualquer família $N_i \lhd G$, $i \in I$, de subgrupos normais de G é um subgrupo normal. Em particular, $(S) := \bigcap_{S \subset N \lhd G} N$ é o subgrupo normal mínimo que contém $S \subset G$. O subgrupo normal (S) é dito o subgrupo normal de G *gerado* por S.

1.29. Lema. *Seja G um grupo e seja $S \subset G$. Então*

$$(S) = \{s_1^{g_1} \cdot s_2^{g_2} \cdot \ldots \cdot s_n^{g_n} \mid n \geqslant 0,\ g_i \in G,\ s_i \in S \cup S^{-1}\},$$

onde $s^g := g \cdot s \cdot g^{-1}$, $S^{-1} := \{s^{-1} \mid s \in S\}$ e, para $n = 0$, o produto apresentado é 1 (por definição).

1.30. Exemplos. 22. Qualquer grupo G age sobre si mesmo por conjugação: a ação é definida pela regra $g \star m := g \cdot m \cdot g^{-1}$. Na verdade, esta ação define não apenas um homomorfismo $h : G \to \Sigma G$, mas um homomorfismo $h : G \to \operatorname{Aut} G$, pois, neste caso, G age sobre si mesmo por automorfismos: $g \star (m_1 \cdot m_2) = (g \star m_1) \cdot (g \star m_2)$, ou seja, $(m_1 \cdot m_2)^g = m_1^g \cdot m_2^g$. A imagem de h é o grupo $\operatorname{Int} G \leqslant \operatorname{Aut} G$ dos automorfismos chamados *internos*. Pelo Teorema 1.27, temos $\operatorname{Int} G \simeq G/CG$ (o símbolo $\simeq$ se lê como "é isomorfo a"), onde $CG := \{c \in G \mid c \cdot g = g \cdot c \text{ para todo } g \in G\}$ é o *centro* de G. Além disso, $\operatorname{Int} G \lhd \operatorname{Aut} G$.

Agindo G sobre o conjunto G, o grupo G age sobre os subconjuntos de G. Em particular, G age pela conjugação sobre os subgrupos de G. Os subgrupos da mesma órbita são ditos *conjugados*. Um subgrupo é normal se e só se sua órbita consiste em um só elemento.

1.30.23. O grupo Σ_n é gerado por todas as transposições. É possível provar que a paridade do número de transposições envolvidas na decomposição de toda permutação independe da escolha da decomposição. Assim, obtemos um homomorfismo "paridade" ou "sinal" (de uma permutação) $p : \Sigma_n \to \{1, -1\}$ que é sobrejetivo para $n > 1$, cujo núcleo se chama o grupo *alternado* e é denotado por A_n.

1.30.24. Consideremos $G = (\mathbb{R}, +)$ e $N = \mathbb{Z}$. Então $N \lhd G$ (pois G é comutativo) e $G/N \simeq \mathbb{S}^1$, onde $\mathbb{S}^1$ é a circunferência unitária de números complexos munida da multiplicação usual. Este fato é uma consequência do Teorema 1.27 e do Exemplo 1.22.13.

1.30.25. Consideremos a circunferência unitária $\mathbb{S}^1$ como um subgrupo de $\mathbb{C}^*$. Então $\mathbb{S}^1 \lhd \mathbb{C}^*$ (pois $\mathbb{C}^*$ é comutativo) e $\mathbb{C}^*/\mathbb{S}^1 \simeq \mathbb{R}^{>0}$. Este fato é uma consequência do Teorema 1.27 e do Exemplo 1.22.11. Na verdade, $\mathbb{C}^* \simeq \mathbb{R}^{>0} \times \mathbb{S}^1$. (Este fato não é nada mais do que a forma trigonométrica dos números complexos.)

1.30.26. Note que um subgrupo de um subgrupo é um subgrupo, mas um subgrupo normal de um subgrupo normal não é necessariamente um subgrupo normal. Sejam $N = \left\{\binom{1234}{1234}, \binom{1234}{2143}, \binom{1234}{3412}, \binom{1234}{4321}\right\}$

e $N_0 = \left\{\binom{1234}{1234}, \binom{1234}{2143}\right\}$. É fácil verificar[1] que $N \lhd \Sigma_4$, que N e N_0 são subgrupos e que N é abeliano. Portanto, temos $N_0 \lhd N \lhd S_4$. Mas $\binom{1234}{1324} \cdot \binom{1234}{2143} \cdot \binom{1234}{1324} = \binom{1234}{3412} \notin N_0$. Consequentemente, $N_0 \not\lhd \Sigma_4$.

1.30.27. Seja G um grupo e seja $H \leqslant G$ um subgrupo. Sabemos que H age sobre G pela multiplicação à esquerda e que as H-órbitas dessa ação são as classes laterais à direita de H em G, estas têm a forma Hg, $g \in G$. Além disso, G age sobre si mesmo à direita pela multiplicação à direita. Estas ações comutam. Logo, G age à direita sobre o conjunto $H\backslash G := \{Hg \mid g \in G\}$ de todas as classes laterais à direita de H em G $\big($pela regra $(Hg)\cdot g' = H(gg')\big)$. Assim, obtemos um antihomomorfismo $h : G \to \Sigma(H\backslash G)$.

1.30.28. Todo subgrupo e toda imagem por um homomorfismo de um grupo cíclico é um grupo cíclico.

1.30.29. Seja $\sigma \in \Sigma_n$. O subgrupo $\langle\sigma\rangle$ gerado por σ age sobre $M := \{1, 2, \ldots, n\}$. Portanto, temos a decomposição $M = O_1 \sqcup O_2 \sqcup \cdots \sqcup O_r$ de M em $\langle\sigma\rangle$-órbitas. Toda $\langle\sigma\rangle$-órbita O_i tem a forma $O_i = \{m, \sigma m, \sigma^2 m, \ldots, \sigma^{k_i-1}m\}$, onde $m \in O_i$ e $\sigma^{k_i}m = m$. Assim, podemos decompor qualquer permutação σ em produto de ciclos $\sigma = (i_{11}i_{12}\ldots i_{1k_1})\cdot(i_{21}i_{22}\ldots i_{2k_2})\cdot\ldots\cdot(i_{r1}i_{r2}\ldots i_{rk_r})$, onde $M = \{i_{11}, i_{12}, \ldots, i_{1k_1}\} \sqcup \{i_{21}, i_{22}, \ldots, i_{2k_2}\} \sqcup \cdots \sqcup \{i_{r1}, i_{r2}, \ldots, i_{rk_r}\}$ é a decomposição de M em $\langle\sigma\rangle$-órbitas e $(a_1a_2\ldots a_k)$ denota a permutação (ciclo) que leva a_1 para a_2, a_2 para a_3, …, a_k para a_1 e faz nada com os outros elementos de M. Na decomposição apresentada, podemos omitir os ciclos de comprimento 1 (pois são iguais a 1). Obviamente, a decomposição obtida é única a menos da ordem de ciclos (eles comutam entre si) e a menos da escolha do primeiro elemento em cada ciclo.

1.30.30. Seja N um grupo e suponhamos que um outro grupo G age sobre N por automorfismos. Isto significa que é dado um homomorfismo $h : G \to \operatorname{Aut} N$. No conjunto $H := N \times G$, definimos a estrutura de grupo pela regra

$$(n_1, g_1)\cdot(n_2, g_2) = \big(n_1 \cdot (hg_1)n_2, g_1 \cdot g_2\big).$$

Definimos também homomorfismos $j : N \to H$, $j : n \mapsto (n, 1)$, e $\pi : H \to G$, $\pi : (n, g) \mapsto g$. É fácil ver que $N' = \big\{(n, 1) \mid n \in N\big\}$ e $G' = \big\{(1, g) \mid g \in G\big\}$ são subgrupos de H isomorfos a N e a G, respectivamente. Além disso, $N \lhd H$ (N é o núcleo de π) e, para $n' = (n, 1) \in N'$ e $g' = (1, g) \in G'$, temos $n'^{g'} = (hg)n$. (Em outras palavras, dentro de H, a ação de G sobre N por automorfismos tornou-se a ação por automorfismos internos de H realizados por elementos de G' que é uma cópia de G.)

Apliquemos esta construção para o caso em que N é o grupo cíclico de ordem n, G é o grupo cíclico de ordem 2, $G = \langle g\rangle$, e a ação de G sobre N é dada pela formula $(hg)n := n^{-1}$. Obtemos o grupo diedral D_n do Exemplo 1.5.9.

Se $N \lhd G$ e $H \leqslant G$, então o conjunto $NH := \{n\cdot s \mid n \in N, s \in S\}$ é um subgrupo em G que contém N. Temos $N \lhd NH \leqslant G$ e $N \cap H \lhd H$.

1.31. Teorema (de isomorfismo)**.** *Seja G um grupo, seja $N \lhd G$ e seja $H \leqslant G$. Então $NH/N \simeq H/(N \cap H)$.*

1.32. Teorema. *Seja G um grupo e sejam $N_1, N_2 \lhd G$ subgrupos normais tais que $N_1 \subset N_2$. Então $(G/N_1)/(N_2/N_1) \simeq G/N_2$, onde $N_2/N_1 \lhd G/N_1$ denota a imagem de N_2 com relação ao homomorfismo canônico $\pi : G \to G/N_1$.*

Um grupo finito cuja ordem é potência de um número primo p se chama *p-grupo.*

Seja G um grupo finito e seja $p > 1$ um número primo tal que $|G| = p^k m$, onde $k > 0$ e $\operatorname{mdc}(p, m) = 1$. Um subgrupo $H \leqslant G$ é dito *p-subgrupo (de Sylow)* se $|H| = p^i$ para algum i (para $i = k$).

---

[1] Agindo sobre $M = \{1, 2, 3, 4\}$, o grupo Σ_4 age sobre o conjunto P de todas as $2 + 2$-partições de M : isto é, $P = \big\{\{1, 2\} \sqcup \{3, 4\}, \{1, 3\} \sqcup \{2, 4\}, \{1, 4\} \sqcup \{2, 3\}\big\}$. Assim, obtemos um homomorfismo $h : \Sigma_4 \to \Sigma P \simeq \Sigma_3$. Podemos verificar que N é o núcleo de h (além disso, h é um epimorfismo).

1.33. Teorema (de Sylow)**.** *Seja G um grupo finito e seja p um divisor primo de $|G|$, isto é, $|G| = p^k m$, $k > 0$, $\mathrm{mdc}(p, m) = 1$. Então*

- *Para todo $0 \leqslant j \leqslant k$, existe um p-sugrupo $H \leqslant G$ tal que $|H| = p^j$.*
- *Para quaisquer p-subgrupo de Sylow $P \leqslant G$ e p-subgrupo $H \leqslant G$, existe $g \in G$ tal que $H \subset P^g$. Em particular, qualquer p-subgrupo está contido em um p-subgrupo de Sylow e todos os p-subgrupos de Sylow são conjugados.*
- *O número de p-subgrupos de Sylow é igual a 1 módulo p.*
- *O centro de qualquer p-grupo não-trivial não é trivial.*

Demonstração. Para $1 \leqslant j \leqslant k$, façamos $M_j := \{X \subset G \mid |X| = p^j\}$. O grupo G age sobre M_j pela multiplicação à esquerda, $G \curvearrowright M_j$. Seja $X \in M_j$. Então $(\mathrm{Stab}_G X)X = X$. Isto significa que X é a união de alguma coleção de $\mathrm{Stab}_G X$-classes laterais à direita. Portanto, $|\mathrm{Stab}_G X|$ divide $|X|$, implicando que $|\mathrm{Stab}_G X| = p^i$ para algum $0 \leqslant i \leqslant j$. A órbita de X tem $|G|/|\mathrm{Stab}_G X| = p^{k-i}m = p^{j-i}l$ elementos, onde $l := p^{k-j}m$. Suponhamos que, para todo $X \in M_j$, o i correspondente seja sempre menor do que j. Isto implica que $|M_j|$ é divisível por pl. Por outro lado, $|M_j| = \frac{n!}{p^j!(n-p^j)!} = l \cdot \frac{(n-1)!}{(p^j-1)!(n-p^j)!}$, mas p não divide $\frac{(n-1)!}{(p^j-1)!(n-p^j)!}$ (mostre isto![2]). Uma contradição. Consequentemente, $|\mathrm{Stab}_G X| = p^j$ para algum $X \in M_j$.

Seja $P \leqslant G$ um p-subgrupo de Sylow e seja $H \leqslant G$ um p-subgrupo. O grupo H age pela multiplicação à esquerda sobre o conjunto G/P de todas as P-classes laterais à esquerda: $h \cdot gP = hgP$. A órbita de gP para esta ação tem $|H|/|\mathrm{Stab}_H gP|$ elementos. Se não existe uma órbita de um só elemento, então $|G/P|$ é divisível por p, o que é impossível. Portanto, $HgP = gP$ para algum $g \in G$. Isto implica $Hg \subset gP$ e, logo, $H \subset P^g$.

Seja M o conjunto de todos os p-subgrupos de Sylow e seja $P \in M$. O grupo P age sobre M pela conjugação. Para qualquer $Q \in M$, a P-órbita de Q tem $|P|/|\mathrm{Stab}_P Q|$ elementos. É suficiente demonstrar que existe uma única P-órbita de um só elemento. Para tal órbita $\{Q\}$, temos $\mathrm{Stab}_P Q = P$, ou seja, $Q^p = Q$ para todo $p \in P$. Consideremos o conjunto $F = \{g \in G \mid Q^g = Q\}$. É fácil ver que $Q \subset F \leqslant G$. Além disso, $P \leqslant F$. Em outras palavras, P e Q são p-subgrupos de Sylow do grupo F. Pela afirmação acima, eles são conjugados em F, implicando $P = Q^f$ para algum $f \in F$. Pela definição de F, $Q^f = Q$. Portanto, $P = Q$.

Seja G um p-grupo. Ele age sobre si mesmo pela conjugação. A classe $[g]$ de conjugação de $g \in G$ tem $|G|/|\mathrm{Stab}_G g|$ elementos, onde $\mathrm{Stab}_G g = \{x \in G \mid g^x = g\}$ é o *centralizador* de g. É claro que $\mathrm{Stab}_G g = G$ se e só se $g \in CG$. Se o centro CG é trivial, então existe somente uma classe de um só elemento. Para qualquer outra classe K, p divide $|K|$. Isto contradiz o fato de que p divide $|G|$ ∎

1.34. Observação. Seja G um grupo finitamente gerado, $G = \langle g_1, \ldots, g_n \rangle$, e seja $h : G \to H$ um homomorfismo de grupos. Então a imagem $hG \leqslant H$ é finitamente gerada, $hG = \langle hg_1, \ldots, hg_n \rangle$.

2. Grupos abelianos

Um grupo A cuja multiplicação é comutativa ($a_1a_2 = a_2a_1$ para todos $a_1, a_2 \in A$) é dito *abeliano*. Nessa seção, lidamos somente com os grupos abelianos e, principalmente, com finitamente gerados.

Normalmente usaremos a notação aditiva. Assim, o elemento neutro é 0, o inverso (*oposto* para a notação aditiva) de a é $-a$. Em vez de potências inteiras, utilizamos *múltiplos*: na para $n \in \mathbb{Z}$ e $a \in A$. Nessa notação, $0a = 0$, $(m \pm n)a = ma \pm na$, $(nm)a = n(ma)$ para todos $m, n \in \mathbb{Z}$ e $a \in A$ (a fórmula $a - b := a + (-b)$ introduz a subtração). Pela comutatividade, para todo $n \in \mathbb{Z}$, $n : A \to A$, $n : a \mapsto na$, é um endomorfismo de A. Assim, é válida a distributividade $n(a_1 \pm a_2) = na_1 \pm na_2$

[2] Denotando por $O_p a$ o expoente do primo p em a, observe que $O_p(a!) = [a/p] + O_p([a/p]!)$. Agora, de $[[a/p^s]/p] = [a/p^{s+1}]$, segue que $O_p(a!) = [a/p] + [a/p^2] + [a/p^3] + \ldots$ Resta verificar que $[(n-1)/p^s] = [(p^j - 1)/p^s] + [(n-p^j)/p^s]$ para todo $s > 0$ se p^j divide n e $j > 0$. Para isto, considere os casos $s < j$ e $s \geqslant j$.

para todos $n \in \mathbb{Z}$ e $a_1, a_2 \in A$. Se o grupo A é gerado por $g_1, \dots g_n \in A$, em vez de $A = \langle g_1, \dots, g_n \rangle$, escrevemos $A = \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_n$.

2.1. Observação. Podemos caracterizar a soma direta (= produto cartesiano) de dois grupos em termos internos: $A = A_1 \oplus A_2$ significa que temos dois subgrupos $A_1, A_2 \leqslant A$ tais que $A_1 + A_2 = A$ e $A_1 \cap A_2 = 0$. Nessa situação, todo elemento $a \in A$ admite uma única forma $a = a_1 + a_2$ com $a_1 \in A_1$ e $a_2 \in A_2$.

2.2. Definição. Seja L um grupo e sejam $b_1, \dots, b_n \in L$. O grupo L é dito *livre* finitamente gerado com a *base* $b_1, \dots, b_n$ se, para todo $l \in L$, existem únicos $c_1, \dots, c_n \in \mathbb{Z}$ tais que $l = c_1b_1 + \cdots + c_nb_n$. Neste caso, claramente, $L \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ vezes}}$ é a soma direta, onde o isomorfismo é dado pela regra $l \mapsto (c_1, \dots, c_n)$. Também podemos escrever $L = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_n$.

2.3. Observação. Suponhamos que $\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{m \text{ vezes}} \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ vezes}}$. Então $m = n$. O fato vale, pois, para $L := \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{m \text{ vezes}}$, o grupo $L/2L$ tem 2^m elementos. Portanto o número de elementos da base, chamado *posto* do grupo livre, é uma característica do grupo independente da escolha da base.

2.4. Definição. Seja A um grupo. Então $\mathrm{T}\,A := \{a \in A \mid \exists n \in \mathbb{Z}, n \neq 0, na = 0\} \leqslant A$ é o subgrupo de *torsão.* No caso em que $\mathrm{T}\,A = 0$, dizemos que A é um grupo *sem torsão.* É facil verificar que $A/\mathrm{T}\,A$ é um grupo sem torsão.

2.5. Lema. *Seja $h : A \to L$ um epimorfismo do grupo A para um grupo livre finitamente gerado L. Então existe um subgrupo $L' \leqslant A$ tal que $A = h^{-1}0 \oplus L'$ e h estabelece um isomorfismo entre L' e L.*

Demonstração. Seja $b_1, \dots, b_n \in L$ uma base de L. Para alguns $a_1, \dots, a_n \in A$, temos $ha_i = b_i$. Façamos $L' = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$. Se, para alguns $c_1, \dots, c_n \in \mathbb{Z}$, temos $c_1a_1 + \cdots + c_na_n \in h^{-1}0$, então $c_1b_1 + \cdots + c_nb_n = 0$ implicando $c_1 = \cdots = c_n = 0$. Isto significa que L' é livre com a base $a_1, \dots, a_n$ e que $h^{-1}0 \cap L' = 0$.

Seja $a \in A$. Então $ha = c_1b_1 + \cdots + c_nb_n$ para alguns $c_1, \dots, c_n \in \mathbb{Z}$. Daí, $h\big(a - \sum_i c_ia_i\big) = 0$. Em outras palavras, $a \in h^{-1}0 + L'$. Assim, obtemos $h^{-1}0 + L' = A$ ∎

2.6. Lema. *Qualquer subgrupo de um grupo livre finitamente gerado é um grupo livre finitamente gerado.*

Demonstração. Seja $H \leqslant \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_n = L$. Usamos indução sobre n. Consideremos o homomorfismo de projeção $\pi : L \to \mathbb{Z}b_n$. Então $\pi^{-1}0 = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_{n-1} = L'$ é livre de posto $n-1$. Temos o epimorfismo induzido $\pi|_H : H \to \pi H \leqslant \mathbb{Z}b_n$. Qualquer subgrupo de $\mathbb{Z} \simeq \mathbb{Z}b_n$ é livre (de posto 1 ou de posto 0). Pelo Lema 2.5, $H \simeq (\pi|_H)^{-1}0 \oplus \pi H$. Resta observar que, pela hipótese de indução, $(\pi|_H)^{-1}0 = L' \cap H \leqslant L'$ é livre finitamente gerado ∎

2.7. Proposição. *Seja A um grupo finitamente gerado. Então $A = \mathrm{T}\,A \oplus L$, onde L é um grupo livre finitamente gerado e $\mathrm{T}\,A$ é finito.*

Demonstração. Se conseguimos provar que $A/\mathrm{T}\,A$ é um grupo livre (pela Observação 1.34, ele é finitamente gerado), então, pelo Lema 2.5, obtemos a decomposição desejada. Agora, pela Observação 1.34, sendo a imagem de A finitamente gerada, $\mathrm{T}\,A$ é finitamente gerado. Isto implica que $\mathrm{T}\,A$ é finito, pois os geradores de $\mathrm{T}\,A$ são periódicos. Sabemos que $A/\mathrm{T}\,A$ é um grupo finitamente gerado sem torsão. Portanto, podemos supor que A é sem torsão e precisamos apenas provar que A é livre.

Entre os geradores $g_1, \dots, g_n \in A$, escolhemos um subconjunto maximal, por exemplo, $g_1, \dots, g_m$, com a propriedade de ser $\mathbb{Z}$-linearmente independentes, isto é, $\sum_{i=1}^{m} c_ig_i \Rightarrow c_i = 0$ para todo i, onde

$c_1, \dots, c_m \in \mathbb{Z}$. Obviamente, $L = \mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_m$ é um grupo livre com a base $g_1, \dots, g_m$. Para todo $m < j \leqslant n$, os geradores $g_1, \dots, g_m, g_j$ são $\mathbb{Z}$-linearmente dependentes. Portanto, $c_1g_1 + \cdots + c_mg_m + k_jg_j = 0$, onde nem todos os $c_1, \dots, c_m, k_j \in \mathbb{Z}$ são nulos. É claro que $k_j \neq 0$ (caso contrário, encontramos uma dependência $\mathbb{Z}$-linear entre $g_1, \dots, g_m$). Façamos $k := k_{m+1}k_{m+2} \dots k_n \neq 0$. De $k_jg_j \in L$ e de $g_1, \dots, g_m \in L$, segue que $kg_i \in L$ para todo gerador g_i de A. Daí concluímos que $kA \subset L$. Para o grupo sem torsão, a multiplicação por k, um inteiro não-nulo, $k : a \mapsto ka$, é um monomorfismo. Logo, $A \simeq kA$ e, pelo Lema 2.6, concluímos que A é um grupo livre finitamente gerado assim obtendo a decomposição desejada ■

Agora é claro que, para entender a estrutura de grupos abelianos finitamente gerados, precisamos apenas estudar os grupos finitos. Para isto, vamos precisar do seguinte

2.8. Lema. *Sejam $m_1, \dots, m_k \in \mathbb{Z}$ tais que $\operatorname{mdc}(m_1, \dots, m_k) = d$. Então existem $t_1, \dots, t_k \in \mathbb{Z}$ tais que $t_1m_1 + \cdots + t_km_k = d$.*

Demonstração. O fato que a divide b pode ser escrito como $\mathbb{Z}a \supset \mathbb{Z}b$. Portanto, o fato que d é um divisor comum dos m_i's é equivalente a $\mathbb{Z}d \supset \mathbb{Z}m_i$ para todo i. Daí, $\mathbb{Z}d \supset \mathbb{Z}m_1 + \cdots + \mathbb{Z}m_k$. Sabemos que o subgrupo $\mathbb{Z}m_1 + \cdots + \mathbb{Z}m_k \leqslant \mathbb{Z}$ é gerado por um elemento: $\mathbb{Z}m_1 + \cdots + \mathbb{Z}m_k = \mathbb{Z}g$, $g \in \mathbb{Z}$. Isto implica que $s_1m_1 + \cdots + s_km_k = g$ para alguns $s_1, \dots, s_k \in \mathbb{Z}$. O fato que $\mathbb{Z}g \supset \mathbb{Z}m_i$ significa que g divide m_i. Supondo que d é o maior divisor comum, concluímos que g divide d, isto é, $\mathbb{Z}g \supset \mathbb{Z}d$. Logo, $\mathbb{Z}g = \mathbb{Z}d$, ou seja, $d = \pm g$ ■

2.9. Definição. Se p é um número primo e A é um grupo, $\mathrm{T}_p A := \{a \in A \mid \exists n \in \mathbb{N},\ p^n a = 0\} \leqslant A$. Caso $\mathrm{T}_p A = A$, chamamos A de *p-grupo*.

2.10. Proposição. *Seja A um grupo finito. Então $A = \mathrm{T}_{p_1} A \oplus \cdots \oplus \mathrm{T}_{p_k} A$ para alguns números primos $p_1, \dots, p_k$ distintos dois a dois.*

Demonstração. Seja $|A| =: n = p_1^{r_1} \dots p_k^{r_k}$, onde $\mathbb{N} \ni p_1, \dots p_k$ são números primos distintos dois a dois. Façamos $m_i := n/p_i^{r_i}$. Obviamente, $\operatorname{mdc}(m_1, \dots, m_k) = 1$. Pelo Lema 2.8, otemos $t_1, \dots, t_k \in \mathbb{Z}$ tais que $t_1m_1 + \cdots + t_km_k = 1$. Seja $a \in A$. Então $a = 1a = (t_1m_1 + \cdots + t_km_k)a = t_1m_1a + \cdots + t_km_ka = a_1 + \cdots + a_k$, onde $a_i := t_im_ia \in \mathrm{T}_{p_i} A$, pois $p_i^{r_i}a_i = p_i^{r_i}t_im_ia = t_ina = 0$ (pelo teorema de Lagrange, sabemos que $|A|a = 0$ para todo $a \in A$). Portanto, $A = \mathrm{T}_{p_1} A + \cdots + \mathrm{T}_{p_k} A$.

Sejam $a_i \in \mathrm{T}_{p_i} A$ tais que $a_1 + \cdots + a_k = 0$. Precisamos provar que $a_i = 0$. Fixamos um índice i. Para todo $j \neq i$, p_j divide m_i. Para um $m \in \mathbb{N}$ suficientemente grande e para todo $j \neq i$, $m_i^m a_j = 0$, pois $a_j \in \mathrm{T}_{p_j} A$. Multiplicando a igualdade $a_1 + \cdots + a_k = 0$ por m_i^m, concluímos que $m_i^m a_i = 0$. Mas o período (= ordem para a notação aditiva) de a_i é uma potência de p_i e p_i é coprimo com m_i. Isto implica que $a_i = 0$. Portanto, $A = \mathrm{T}_{p_1} A \oplus \cdots \oplus \mathrm{T}_{p_k} A$ ■

2.11. Proposição. *Seja A um p-grupo finito. Então $A = C_1 \oplus \cdots \oplus C_s$, onde C_j é um grupo cíclico de ordem p^{k_j} e $1 \leqslant k_1 \leqslant \cdots \leqslant k_s$. Os números $k_1, \dots, k_s$ independem da escolha de uma decomposição de A na soma direta do tipo indicado.*

Demonstração. Usamos a indução sobre $|A|$. Seja $a \in A$ o elemento de maior ordem, $|a| = p^k$. Aplicando a hipótese de indução para o grupo $\overline{A} = A/\mathbb{Z}a$, para alguns $b_1, \dots b_{s-1} \in A$, obtemos uma decomposição $\overline{A} = \mathbb{Z}\overline{b}_1 \oplus \cdots \oplus \mathbb{Z}\overline{b}_{s-1}$, onde $|\overline{b}_j| = p^{k_j}$ (no grupo $\overline{A}$) e $1 \leqslant k_1 \leqslant \cdots \leqslant k_{s-1}$.

2.12. Lema. *Para todo $\overline{b} \in \overline{A}$, existe um $b' \in A$ tal que $|b'| = |\overline{b}|$ e $\overline{b}' = \overline{b}$.*

Demonstração. Sejam $|b| = p^u$ e $|\overline{b}| = p^v$ (é claro que $u \geqslant v$). Logo, $p^vb \in \mathbb{Z}a$. Portanto, $p^vb = ma$ para algum $m \in \mathbb{Z}$ e $m = p^tn$, onde $\operatorname{mdc}(p, n) = 1$. Se $t \geqslant v$, então $p^v(b - p^{t-v}na) = 0$ e $b' := b - p^{t-v}na$ é o desejado. Se $t < v$, então $0 = p^ub = p^{u-v}p^vb = p^{u-v}p^tna = p^{u+t-v}na$. Sendo $\operatorname{mdc}(p, n) = 1$, os elementos a e na têm o mesmo período, p^k. Logo, $u + t - v \geqslant k$ implicando $u > k$, pois $t < v$. Uma contradição com a escolha de a ■

Continuação da demonstração da Proposição 2.11. Pelo Lema 2.12, podemos supor que $|b_j| = |\overline{b}_j|$ para todo $j < s$. Façamos $b_s := a$ e $k_s := k$. Claramente, $1 \leqslant k_1 \leqslant \cdots \leqslant k_{s-1} \leqslant k_s$. Vamos mostrar que $A = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_{s-1} \oplus \mathbb{Z}b_s$. Seja $x \in A$. Então $\overline{x} = c_1\overline{b}_1 + \cdots + c_{s-1}\overline{b}_{s-1}$ para alguns $c_1, \ldots, c_{s-1} \in \mathbb{Z}$. Em outras palavras, $x \in c_1b_1 + \cdots + c_{s-1}b_{s-1} + \mathbb{Z}b_s$ implicando $A = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_{s-1} + \mathbb{Z}b_s$. Se $c_1b_1 + \cdots + c_{s-1}b_{s-1} + c_sb_s = 0$, então $c_1\overline{b}_1 + \cdots + c_{s-1}\overline{b}_{s-1} = \overline{0}$. Daí concluímos que $c_j\overline{b}_j = \overline{0}$ para todo $j < s$. De $|b_j| = |\overline{b}_j|$ segue que $c_jb_j = 0$ para todo $j < s$. Logo, $c_sb_s = 0$ também.

Para provar a unicidade dos $k_1, \ldots, k_s$, usamos a indução sobre $|A|$. Suponhamos que $C_1 \oplus \cdots \oplus C_s \simeq C'_1 \oplus \cdots \oplus C'_{s'}$, onde os C_i's e C'_j's são grupos cíclicos, $|C_i| = p^{k_i}$, $|C'_j| = p^{k'_j}$, $1 \leqslant k_1 \leqslant \cdots \leqslant k_s$ e $1 \leqslant k'_1 \leqslant \cdots \leqslant k'_{s'}$. Então $p(C_1 \oplus \cdots \oplus C_s) \simeq p(C'_1 \oplus \cdots \oplus C'_{s'})$. Observando que $p(C_1 \oplus \cdots \oplus C_s) = (pC_1) \oplus \cdots \oplus (pC_s)$ e que pC_i é um grupo cíclico de ordem p^{k_i-1}, o resultado segue pela hipótese de indução ∎

2.13. Teorema. *Todo grupo finitamente gerado é a soma direta de grupos cíclicos que são infinitos ou p-grupos (em geral, com vários p's). Nessa decomposição, o número de grupos cíclicos de ordem dada independe da escolha da decomposição na soma direta.*

Demonstração. A primeira afirmação segue pelas Proposições 2.7, 2.10 e 2.11.

Para a segunda, observamos que um isomorfismo $A \simeq A'$ induz isomorfismos $\mathrm{T}\,A \simeq \mathrm{T}\,A'$ e $A/\mathrm{T}\,A \simeq A'/\mathrm{T}\,A'$. O número de grupos cíclicos infinitos na decomposição é igual ao posto do grupo livre $A/\mathrm{T}\,A \simeq A'/\mathrm{T}\,A'$ que é bem definido pela Observação 2.1. O isomorfismo $\mathrm{T}\,A \simeq \mathrm{T}\,A'$ induz isomorfismos $\mathrm{T}_p\,A \simeq \mathrm{T}_p\,A'$ para todo número primo p. Resta aplicar a Proposição 2.11 ∎

2.14. Critério. *Seja L um grupo e sejam $b_1, \ldots, b_n \in L$. Então L é um grupo livre com base $b_1, \ldots, b_n$ se e só se, para todo grupo A e para qualquer função $f : \{b_1, \ldots, b_n\} \to A$, existe um único homomorfismo $h : L \to A$ tal que $hb_i = fb_i$ para todo i.*

2.15. Observação. Sejam A_1 e A_2 grupos. Então $\mathrm{Hom}(A_1, A_2)$ munido da operação definida pela regra $(h_1 + h_2) : a_1 \mapsto h_1a_1 + h_2a_1$, $a_1 \in A_1$, é um grupo. Sejam A_1, A_2, A_3 grupos. Então a composição $\circ : \mathrm{Hom}(A_2, A_3) \times \mathrm{Hom}(A_1, A_2) \to \mathrm{Hom}(A_1, A_3)$ é aditiva em todo argumento, isto é, $(h_2 + h'_2) \circ h_1 = h_2 \circ h_1 + h'_2 \circ h_1$ e $h_2 \circ (h_1 + h'_1) = h_2 \circ h_1 + h_2 \circ h'_1$ para todos $h_1, h'_1 \in \mathrm{Hom}(A_1, A_2)$ e $h_2, h'_2 \in \mathrm{Hom}(A_2, A_3)$.

2.16. Observação. Podemos caracterizar a soma direta $A := A_1 \oplus \cdots \oplus A_m$ através de homomorfismos. Temos homomorfismos de projeções $\pi_i : A \to A_i$, $\pi_i : a_1 + \cdots + a_i + \cdots + a_m \mapsto a_i$, e homomorfosmos de injeções $j_i : A_i \to A$. Eles satisfazem as seguintes identidades: $\pi_i \circ j_i = 1_{A_i}$, $\pi_k \circ j_i = 0$ para $k \neq i$, $j_1 \circ \pi_1 + \cdots + j_m \circ \pi_m = 1_A$.

2.17. Observação. Sejam $A := A_1 \oplus \cdots \oplus A_m$ e $A' := A'_1 \oplus \cdots \oplus A'_{m'}$. Denotamos por π_i e j_i projeções e injeções para A e por π'_k e j'_k projeções e injeções para A'. Então podemos descrever $\mathrm{Hom}(A, A')$ na forma matricial

$$\mathrm{Hom}(A, A') \simeq \begin{bmatrix} \mathrm{Hom}(A_1, A'_1) & \ldots & \mathrm{Hom}(A_m, A'_1) \\ \vdots & \ddots & \vdots \\ \mathrm{Hom}(A_1, A'_{m'}) & \ldots & \mathrm{Hom}(A_m, A'_{m'}) \end{bmatrix},$$

onde a (i, k)-componente da "matriz" que corresponde ao homomorfismo $h \in \mathrm{Hom}(A, A')$ é igual a $\pi'_i \circ h \circ j_k$. Nessa identificação a soma das matrizes corresponde à soma de homomorfismos. Seja $A'' := A''_1 \oplus \cdots \oplus A''_{m''}$. Identificando como acima os homomorfismos de $\mathrm{Hom}(A', A'')$ com $m'' \times m'$-matrizes, podemos ver que, na forma matricial, a composição $\circ : \mathrm{Hom}(A', A'') \times \mathrm{Hom}(A, A') \to \mathrm{Hom}(A, A')$ é a multiplicação "usual" de "matrizes".

3. Anéis e módulos

3.1. Definição. Seja $(A,+)$ um grupo abeliano munido de uma operação binária $\cdot : A \times A \to A$, $\cdot : (a_1, a_2) \mapsto a_1 \cdot a_2$, chamada *multiplicação.* Então $(A,+,\cdot)$ se chama *anel* (*associativo*) se são válidos os axiomas seguintes:

AA. $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$ para todos $a_1, a_2, a_3 \in A$.
AD. $(a_1 + a_2) \cdot a_3 = (a_1 \cdot a_3) + (a_2 \cdot a_3)$ e $a_1 \cdot (a_2 + a_3) = (a_1 \cdot a_2) + (a_1 \cdot a_3)$ para todos $a_1, a_2, a_3 \in A$.

Um anel A é *com unidade* se existe $e \in A$ um elemento neutro respectivamente à multiplicação.

A1. Existe $e \in A$ tal que $e \cdot a = a \cdot e = a$ para todo $a \in A$.

Usualmente denotamos a unidade por 1. Um anel A se chama *comutativo* se

AC. $a_1 \cdot a_2 = a_2 \cdot a_1$ para todos $a_1, a_2 \in A$.

Nossos anéis serão associativos e com uninade, mas não necessariamente comutativos.

3.2. Exemplos. 1. Seja $(M,+)$ um grupo abeliano. Então, pela Observação 2.15, $\big(\mathrm{End}(M,+),+,\circ\big)$ é um anel (normalmente não-comutativo).

3.2.2. $(\mathbb{Z},+,\cdot)$ é um anel com unidade, entretanto $(2\mathbb{Z},+,\cdot)$ é um "anel sem unidade".

3.2.3. $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ é um anel finito (o anel de números inteiros módulo n).

3.2.4. $\big(\mathbb{Z}[i],+,\cdot\big)$ é um anel (o anel de números inteiros de Gauss).

3.2.5. Seja A um anel. Então o conjunto $\mathrm{Matr}_{n\times n} A$ de $n \times n$-matrizes com coeficientes em A munido das operações "usuais" é um anel (normalmente não-comutativo).

3.2.6. Seja C um conjunto e seja A um anel. Então $\mathrm{Func}(C,A) = \{f : C \to A\}$ é um anel. As operações são definidas pelas regras seguintes: $(f_1 + f_2)c := f_1 c + f_2 c$, $(f_1 \cdot f_2)c := f_1 c \cdot f_2 c$.

3.3. Exercício. Prove que em qualquer anel $0 \cdot a = a \cdot 0 = 0$ e $(-a_1) \cdot a_2 = -(a_1 \cdot a_2) = a_1 \cdot (-a_2)$.

3.4. Definição. Seja A um anel. Um subgrupo aditivo $S \leqslant A$ é dito *subanel* se

SA1. $1 \in S$.
SAM. $s_1, s_2 \in S \Rightarrow s_1 \cdot s_2 \in S$.

Obviamente, qualquer subanel sendo munido das operações induzidas é um anel.

3.5. Definição. Sejam A_1 e A_2 anéis. Um homomorfismo $h : (A_1,+) \to (A_2,+)$ de grupos abelianos é dito *homomorfismo* de anéis se

HA1. $h1 = 1$.
HAM. $h(a_1 \cdot a_1') = (ha_1) \cdot (ha_1')$ para todos $a_1, a_1' \in A_1$.

A inclusão de um subanel em seu anel é um homomorfismo de anéis. Claramente, a composição de dois homomorfismos de anéis (se é definida) é um homomorfismo de anéis. Note que a imagem e a imagem inversa de qualquer subanel por qualquer homomorfismo são subanéis.

3.6. Definição. Seja $(M,+)$ um grupo abeliano e seja A um anel. Seja dada uma operação binária (também chamada *multiplicação*) $\cdot : A \times M \to M$, $\cdot : (a,m) \mapsto a \cdot m$, tal que são válidos os axiomas seguintes:

M1. $1 \cdot m = m$ para todo $m \in M$.
MA. $(a_1 \cdot a_2) \cdot m = a_1 \cdot (a_2 \cdot m)$ para todos $a_1, a_2 \in A$ e $m \in M$.
MDA. $(a_1 + a_2) \cdot m = (a_1 \cdot m) + (a_2 \cdot m)$ para todos $a_1, a_2 \in A$ e $m \in M$.
MDM. $a \cdot (m_1 + m_2) = (a \cdot m_1) + (a \cdot m_2)$ para todos $a \in A$ e $m_1, m_2 \in M$.

Então dizemos que M é um A-*módulo* (*à esquerda*) e escrevemos ${}_A M$. (De modo semelhante podemos definir A-*módulo à direita,* escrevendo M_A.)

Note que o conceito de A-módulo pode ser visto em termos de homomorfismo de anéis $h : A \to \mathrm{End}(M,+)$, onde $(ha)m := a \cdot m$, e vice versa: qualquer homomorfismo de anéis $h : A \to \mathrm{End}(M,+)$ define sobre M uma estrutura de A-módulo pela regra $a \cdot m := (ha)m$.

3.7. Exemplos. 7. Todo grupo abeliano pode ser considerado como um $\mathbb{Z}$-módulo.

3.7.8. Seja A um anel. Denotando $M := (A,+)$, a multiplicação em A define uma ação de A sobre M, tornando M um A-módulo. Essa ação induz um homomorfismo de anéis $h : A \to \mathrm{End}(A,+)$, $(ha_1)a_2 := a_1 \cdot a_2$. De fato, h identifica A com um subanel em $\mathrm{End}(A,+)$, pois o núcleo de h é nulo: $ha = 0 \Rightarrow (ha)1 = 0 \Rightarrow a \cdot 1 = 0 \Rightarrow a = 0$.

3.7.9. Seja ${}_AM$ um A-módulo. Então todos os endomorfismos do A-módulo ${}_AM$ formam um anel $\mathrm{End}_A M$.

3.8. Definição. Seja ${}_AM$ um A-módulo. Um subgrupo $S \leqslant_A M$ é dito *submódulo,* se

SM. $a \in A$ e $s \in S \Rightarrow a \cdot s \in S$.

Qualquer submódulo, sendo munido da operação induzida, é um A-módulo. Escrevemos ${}_AS \leqslant_A M$.

3.9. Definição. Seja A um anel e sejam ${}_AM_1$ e ${}_AM_2$ A-módulos. Um homomorfismo $h : M_1 \to M_2$ de grupos abelianos é dito *homomorfismo* de A-módulos, se

HM. $h(a \cdot m_1) = a \cdot (hm_1)$ para todos $a \in A$ e $m_1 \in_A M_1$.

A inclusão de um submódulo no seu módulo é um homomorfismo de módulos. A composição de dois homomorfismos de A-módulos (se é definida) é um homomorfismo de A-módulos. A imagem e a imagem inversa de qualquer submódulo por qualquer homomorfismo de A-módulos são submódulos. Em particular, o núcleo de um homomorfismo é um submódulo.

3.10. Definição. Seja A um anel e seja $I \leqslant (A,+)$ um subgrupo aditivo. Dizemos que I é um *ideal* (*bilateral*) em A, denotando $I \lhd A$, se

IE. $a \in A$ e $i \in I \Rightarrow a \cdot i \in I$ (*ideal à esquerda,* denotado $I \lhd_l A$).
ID. $i \in I$ e $a \in A \Rightarrow i \cdot a \in I$ (*ideal à direita,* denotado $I \lhd_r A$).

Seja $h : A_1 \to A_2$ um homomorfismo de anéis. Então $h^{-1}0 \lhd A_1$.

Considerando A como A-módulo (vide o Exemplo 3.7.8), podemos ver que os submódulos de ${}_AA$ são exatamente os ideais à esquerda de A.

3.11. Exercício. Quando um ideal é um subanel?

Note que a intersecção de qualquer família de subanéis (ideais bilaterais, ideais à esquerda, ideais à direita, submódulos) é um subanel (ideal bilateral, ideal à esquerda, ideal à direita, submódulo). Isto permite introduzir o conceito de geradores e provar as afirmações análogas aos Lemas 1.9 e 1.29 para subanéis, ideais bilaterais, ideais à esquerda, ideais à direita, submódulos. Por exemplo, seja ${}_AM$ um A-módulo e sejam $g_1, \ldots, g_n \in M$. Então $Ag_1 + \cdots + Ag_n := \{a_1g_1 + \cdots + a_ng_n \mid a_1, \ldots, a_n \in A\}$ é o submódulo gerado por $g_1, \ldots, g_n$.

Seja $I \lhd A$ um ideal em um anel. No grupo quociente A/I, a regra $(a_1 + I) \cdot (a_2 + I) := (a_1 \cdot a_2) + I$ corretamente define uma multiplicação. Assim, A/I é um anel chamado anel *quociente* de A por I e a função $\pi : A \to A/I$, $\pi : a \mapsto a + I$, é um homomorfismo de anéis, chamado *canônico.* Obviamente, I é o núcleo de π.

Seja ${}_AM$ um A-módulo e seja ${}_AS \leqslant_A M$ um submódulo. No grupo quociente M/S, a regra $a \cdot (m + S) := (a \cdot m) + S$ corretamente define uma estrutura de A-módulo. Assim, M/S é um A-módulo chamado módulo *quociente* de M por S e a função $\pi : M \to M/S$, $\pi : m \mapsto m + S$, é um homomorfismo de A-módulos, chamado *canônico.* Além disso, ${}_AS$ é o núcleo de π.

3.12. Teoremas de homomorfismo. 1. *Seja $h : A_1 \to A_2$ um homomorfismo de anéis. Denotamos por $I = h^{-1}0$ o seu núcleo. Então $I \lhd A_1$ e existe um único homomorfismo $h' : A_1/I \to A_2$ tal que $h' \circ \pi = h$. Este h' é injetivo. Além disso, o homomorfismo h estabelece uma correspondência bijetora entre os subanéis (ideais, ideais à esquerda, ideais à direita) de A_1 que contêm o núcleo I e os subanéis (ideais, ideais à esquerda, ideais à direita) da imagem hA_1. A correspondência preserva inclusão.*

3.12.2. *Seja A um anel e seja $h : {}_AM_1 \to {}_AM_2$ um homomorfismo de A-módulos. Denotamos por $S = h^{-1}0$ o seu núcleo. Então ${}_AS$ é um submódulo em ${}_AM_1$ e existe um único homomorfismo $h' : M_1/S \to M_2$ tal que $h' \circ \pi = h$. Este h' é monomorfismo. Além disso, o homomorfismo h estabelece uma correspondência bijetora entre os submódulos de ${}_AM_1$ que contêm o núcleo ${}_AS$ e os submódulos da imagem hM_1. A correspondência preserva inclusão.*

3.12.3. *Seja A um anel, seja $I \lhd A$ e seja $S \leqslant A$ um subanel. Então $I + S$ é um subanel em A, $I \lhd I + S$, $I \cap S \lhd S$ e $(I + S)/I \simeq S/(I \cap S)$.*

3.12.4. *Seja ${}_AM$ um A-módulo e sejam ${}_AS, {}_AN \leqslant {}_AM$ submódulos. Então $(S+N)/S \simeq N/(S\cap N)$.*

3.12.5. *Seja A um anel e sejam $I_1, I_2 \lhd A$ tais que $I_1 \subset I_2$. Então $(A/I_1)/(I_2/I_1) \simeq A/I_2$, onde $(I_2/I_1) \lhd (A/I_1)$ denota a imagem de I_2 com relação ao homomorfismo canônico $\pi : A \to A/I_1$.*

3.12.6. *Seja ${}_AM$ um A-módulo e sejam ${}_AS_1 \leqslant {}_AS_2 \leqslant {}_AM$ submódulos. Então, denotando por $(S_2/S_1) \leqslant (M/S_1)$ a imagem de S_2 com relação ao homomorfismo canônico $\pi : M \to M/S_1$, temos $(M/S_1)/(S_2/S_1) \simeq M/S_2$.*

4. Anéis comutativos, domínios, corpos

Nessa seção, lidamos somente com anéis comutativos.

É fácil provar que, neste caso, vale o *binômio* de Newton:

$$(a+b)^n = \sum_{i=0}^{n} \frac{n!}{i! \cdot (n-i)!} a^i b^{n-i},$$

onde, por definição, $a^k := \underbrace{a \cdot \ldots \cdot a}_{k \text{ vezes}}$ para $k > 0$ e $a^0 := 1$.

4.1. Definição. Um anel D se chama *domínio* se

D1. $1 \neq 0$ em D.

D0. $d_1 \cdot d_2 = 0 \Rightarrow d_1 = 0$ ou $d_2 = 0$ para todos $d_1, d_2 \in D$.

Um anel K se chama *corpo* se $1 \neq 0$ em K e todo elemento $0 \neq k \in K$ possui um inverso multiplicativo, isto é, um $k' \in K$ tal que $k \cdot k' = 1$. Tal inverso é único e é denotado por k^{-1}. É fácil ver que qualquer corpo é um domínio.

4.2. Exemplos. 1. O anel $\mathbb{Z}/4\mathbb{Z}$ não é um domínio, pois possui *divisores de zero*: $\overline{2} \cdot \overline{2} = \overline{0}$, mas $\overline{2} \neq \overline{0}$.

4.2.2. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$ são corpos.

4.2.3. Seja D um domínio. Então $D[x]$, o anel de polinômios numa variável x com coeficientes em D, também é um domínio. Qualquer $d \in D$ define um homomorfismo "de substituição" de d no lugar da variável, isto é, $|_{x=d} : D[x] \to D$, $f \mapsto f(d)$.

4.3. Lema. *Seja K um anel com $1 \neq 0$. Então K é um corpo se e só se K não possui ideais próprios.*

Demonstração. Seja K um corpo e seja $0 \neq I \lhd K$. Então existe $0 \neq i \in I$. Sendo K um corpo, existe $i^{-1} \in K$ tal que $i^{-1} \cdot i = 1$. Para todo $k \in K$, temos $k = (k \cdot i^{-1}) \cdot i \in I$. Portanto, $I = K$.

Seja K um anel sem ideais próprios. Se $0 \neq k \in K$, então $0 \neq k \in Kk \lhd K$. Portanto, $Kk = K \ni 1$ e $k' \cdot k = 1$ para algum $k' \in K$.

4.4. Exercício. Prove que qualquer domínio finito é um corpo.

4.5. Definição-Lema. *Seja A um anel e seja $I \lhd A$.*

Dizemos que I é um ideal primo *de A (notação $I \lhd_p A$) se é satisfeita uma das seguintes equivalentes condições*:

- *A/I é um domínio.*
- *$I \neq A$ e $a_1 \cdot a_2 \in I \Rightarrow a_1 \in I$ ou $a_2 \in I$.*

Dizemos que I é um ideal maximal *de A (notação $I \lhd_m A$) se é válida uma das seguintes equivalentes propriedades*:

- *A/I é um corpo.*
- *$I \neq A$ e não existe ideais de A entre I e A, isto é, $J \lhd A$ com $I \subset J \subset A$ implica $I = J$ ou $J = A$.*

4.6. Exemplos. 4. Seja $p \in \mathbb{Z}$ um número primo. Então $\mathbb{Z}p \lhd_m \mathbb{Z}$ pois a inclusão $\mathbb{Z}a \supset \mathbb{Z}b$ significa que a divide b. Portanto, $\mathbb{Z}/p\mathbb{Z}$ é um corpo finito. O denotamos por $\mathbb{F}_p$.

4.6.5. Seja D um domínio. No conjunto de "frações formais" $F = \big\{(a,d) \mid a \in D,\ 0 \neq d \in D\big\}$, definimos uma relação de equivalência $(a,d) \sim (a',d') \Leftrightarrow a \cdot d' = a' \cdot d$. No conjunto das classes de equivalência, as quais denotamos por $[a/d]$, definimos operações pelas regras seguintes: $[a/d]+[a'/d'] := \big[(a \cdot d' + a' \cdot d)/d \cdot d'\big]$ e $[a/d] \cdot [a'/d'] := [a \cdot a'/d \cdot d']$. Então obtemos um corpo $K := F/\sim$ e um homomorfismo injetor entre anéis $D \to K$, $h : a \mapsto [a/1]$. Vamos pensar que este é uma inclusão $D \leqslant K$. O corpo construído $KD := K$ se chama o corpo de *frações* de D. Ele satisfaz a seguinte propriedade:

- para qualquer corpo C que contém D, $D \leqslant C$, existe um único homomorfismo $h : K \to C$ tal que $hd = d$ para todo $d \in D$.

Assim, num certo sentido, K é único.

4.6.6. Voltando ao Exemplo 3.2.6, podemos provar que $I_r := \big\{f : [0,1] \to \mathbb{R} \mid fr = 0\big\} \lhd_m \mathrm{Func}\big([0,1],\mathbb{R}\big)$ para todo $r \in [0,1]$. Realmente, a função $|_r : \mathrm{Func}\big([0,1],\mathbb{R}\big) \to \mathbb{R}$, $|_r : f \mapsto fr$, é um homomorfismo entre anéis e I_r é o núcleo de $|_r$.

4.7. Definição. Seja K um corpo e seja V um K-módulo. Então V é dito *K-espaço linear.* Se V é finitamente gerado, $V = Kg_1 + \cdots + Kg_n$, então, escolhendo entre os $g_1, \ldots, g_n$ um subconjunto minimal de geradores, podemos ver que $g_1, \ldots, g_n$ são *K-linearmente independentes,* isto é, $k_1 \cdot g_1 + \cdots + k_n \cdot g_n = 0$ para $k_1, \ldots, k_n \in K$ implica $k_1 = \cdots = k_n = 0$. Com efeito, se, por exemplo, $k_n \neq 0$, então $g_n = -k_n^{-1} \cdot (k_1 \cdot g_1 + \cdots + k_{n-1} \cdot g_{n-1})$ e, portanto, $g_n \in Kg_1 + \cdots + Kg_{n-1}$. Isto implica $V = Kg_1 + \cdots + Kg_{n-1}$. Uma contradição.

Mais ainda, todo elemento de V tem uma única forma $v = k_1 \cdot g_1 + \cdots + k_n \cdot g_n$ com $k_1, \ldots, k_n \in K$. Em outras palavras, $g_1, \ldots, g_n$ formam uma *base linear* de V.

4.8. Definição. Seja D um domínio D munido de uma função $\varphi : D \setminus 0 \to \mathbb{N}$ que satisfaz as propriedades seguintes:

- Para todos $a, b \in D$ com $b \neq 0$, existem $q, r \in D$ tais que $a = qb + r$, onde $r = 0$ ou $r \neq 0$ e $\varphi r < \varphi b$.
- Para todos $0 \neq a, b \in D$, temos $\varphi a \leqslant \varphi(ab)$.

Neste caso, dizemos que (D, φ) é um domínio *euclidiano.* Em palavras: um domínio euclidiano é um domínio que tem "divisão com resto".

4.9. Exemplos. 7. Os números inteiros $\big(\mathbb{Z}, |\cdot|\big)$ munidos da função valor absoluto é um domínio euclidiano.

4.9.8. Seja K um corpo. Então o anel dos polinômios $K[x]$ munido da função "grau" é um domínio euclidiano.

4.9.9. Os números inteiros de Gauss $\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\} \leqslant \mathbb{C}$ munidos da função $N : x \mapsto |x|^2$ é um domínio euclidiano. (Para todo $c \in \mathbb{C}$, existe um $q \in \mathbb{Z}[i]$ tal que $|c - q|^2 \leqslant (\frac{1}{2})^2 + (\frac{1}{2})^2 < 1$. Resta aplicar isto para $c = a/b$, onde $a, b \in \mathbb{Z}[i]$ com $b \neq 0$, e utilizar o fato que N é multiplicativa.)

4.10. Definição. Um domínio D se chama *principal* se todo ideal de D é *principal,* isto é, gerado por um elemento.

4.11. Lema. *Todo domínio euclidiano é principal.*

Demonstração. Seja $0 \neq I \lhd D$ um ideal não-nulo no domínio euclidiano (D, φ) e seja $0 \neq g \in I$ com o valor φg mínimo. Claro que $I \supset Dg$. Seja $a \in I$. Então existem $q, r \in D$ tais que $a = qg + r$, onde $r = 0$ ou $r \neq 0$ e $\varphi r < \varphi g$. É fácil ver que $r \in I$. Pela escolha de g, temos $r = 0$ ■

4.12. Definição. Seja A um anel e seja $s \in A$. Então s é dito *inversível* em A se existe $s' \in A$ tal que $ss' = 1$. É fácil ver que tal s' é único. Ele se chama *inverso* a s e é denotado por s^{-1} caso exista.

Seja D um domínio. Dizemos que os elementos $0 \neq a, b \in D$ são *associados* se existe um elemento inversível $s \in D$ tal que $b = sa$. É facil verificar que a relação "ser associado" é uma relação de equivalência.

4.13. Definição. Seja D um domínio e sejam $0 \neq a, b \in D$. Dizemos que a *divide* b ou que a é um *divisor* de b, denotando $a|b$, se existe $q \in D$ tal que $b = qa$. É imediato que, para $0 \neq a, b \in D$, o fato que $a|b$ é equivalente a $Da \supset Db$. Um elemento $0 \neq p \in D$ se chama *irredutível* se ele não é inversível e possui somente divisores triviais. Isto significa que todos os divisores de p são ou associados a p ou inversíveis. Em outras palavras, p é irredutível se $p = ab$ implica que exatamanete um dos a e b é inversível.

4.14. Definição. Um domínio D é de *fatoração única* ou *fatorial* se

EF. Para todo elemento não-inversível $0 \neq a \in D$, existem $m \geqslant 1$ e elementos irredutíveis $p_1, \ldots, p_m \in D$ tais que $a = p_1 \ldots p_m$ ("fatoração existe").
UF. Se $p_1 \ldots p_m = q_1 \ldots q_n$ com $p_1, \ldots, p_m, q_1, \ldots, q_n \in D$ irredutíveis e $m, n \geqslant 1$, então $m = n$ e, a menos da ordenação, p_i é associado a q_i ("fatoração é única").

Na prática, é mais confortável utilizar a seguinte condição equivalente à da unicidade:

UF′. $p|ab \Rightarrow p|a$ ou $p|b$ para todo elemento irredutível $p \in D$.

Em outras palavras:

UF″. $Dp \lhd_p D$ para todo elemento irredutível $p \in D$.

4.15. Proposição. *Todo domínio principal é fatorial.*

Demonstração. Seja D um domínio principal e suponhamos que um elemento não-inversível $0 \neq d_0 \in D$ não admita fatoração. Então d_0 não é irredutível e, portanto, pode ser decomposto, $d_0 = q_1 d_1$, onde nenhum dos q_1 e d_1 é inversível. Se ambos q_1 e d_1 admitem uma fatoração no produto de elementos irredutíveis, juntando essas fatorações, poderíamos obter uma fatoração de d_0. Portanto, podemos supor que d_1 não admite fatoração. Agindo deste modo, obtemos $d_{i-1} = q_i d_i$ para todo $i > 0$, onde $q_i, d_i \in D$ são não-inversíveis. Isto implica que $Dd_{i-1} \subset Dd_i$. É fácil ver que a união $I = \bigcup_{i=0}^{\infty} Dd_i$ da cadeia de ideais é um ideal. Logo, existe um $d \in D$ tal que $I = Dd$. Sendo $d \in Dd$, temos $d \in Dd_i$ para algum i, implicando $Dd = Dd_i$ e, portanto, $Dd_i = Dd_{i+1}$. Resta observar que a igualdade $Da = Db$ para $0 \neq a, b \in D$ é equivalente ao fato que a é associado a b (assim, podemos concluir que q_{i+1} é inversível).

Seja $p \in D$ um elemento irredutível. Vamos provar que Dp é um ideal maximal de D. Seja $J \lhd D$ tal que $Dp \subsetneqq J$. Então, para algum $g \in D$, temos $J = Dg$ e g divide p, mas g não é associado a p. Pela Definição 4.13 g é inversível. Logo, $J = D$. Sendo Dp maximal, ele é primo pelo Definição-Lema 4.5 pois todo corpo é um domínio. Assim verificamos a condição UF″ ■

O leitor curioso pode reler a Seção 2 considerando módulos finitamente gerados sobre um domínio principal no lugar de grupos abelianos finitamente gerados.

Seja D um domínio e sejam $0 \neq a_1, a_2, \ldots, a_n \in D$. Dizemos que $0 \neq d \in D$ é um divisor *comum* de $a_1, a_2, \ldots, a_n$ se d divide todo a_i. Um divisor comum d de $a_1, a_2, \ldots, a_n$ se chama *maior* divisor comum de $a_1, a_2, \ldots, a_n$ se qualquer divisor comum de $a_1, a_2, \ldots, a_n$ divide d. Por esta definição, todos os maiores divisores comuns de $a_1, a_2, \ldots, a_n$ são associados se existirem. Escrevendo $d = \text{mdc}(a_1, \ldots, a_n)$ para o maior divisor comum d de $a_1, \ldots, a_n$, deve-se levar em conta que a igualdade vale somente no sentido de "a menos de ser associado". É fácil ver que, em todo domínio fatorial, existem divisores comuns de qualquer coleção finita de elementos não-nulos. Por uma demonstração semelhante à do Lema 2.8, em todo domínio principal D, para quaisquer $0 \neq a_1, a_2, \ldots, a_n \in D$, existem $t_1, t_2, \ldots, t_n \in D$ tais que $\text{mdc}(a_1, a_2, \ldots, a_n) = t_1a_1 + t_2a_2 + \cdots + t_na_n$.

4.16. Definição. Seja D um domínio fatorial e seja $0 \neq f = c_nx^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \in D[x]$ um polinômio não-nulo. O maior divisor comum dos coeficientes de f é dito o *conteúdo* de f e se denota por $cf := \text{mdc}(c_0, c_1, \ldots, c_{n-1}, c_n)$. Claramente, $f = cf \cdot f_0$, onde $cf_0 = 1$.

4.17. Lema (Gauss)**.** *Seja D um domínio fatorial e sejam $0 \neq f, g \in D[x]$ polinômios não-nulos. Então $c(fg) = cf \cdot cg$.*

Demonstração. Temos $f = cf \cdot f_0$ e $g = cg \cdot g_0$ com $cf_0 = cg_0 = 1$. Basta provar que $c(f_0g_0) = 1$. Suponhamos que $p|c(f_0g_0)$ para algum elemento irredutível $p \in D$. Temos $f_0 = c_mx^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0$ e $g_0 = d_nx^n + d_{n-1}x^{n-1} + \cdots + d_1x + d_0$, onde $m, n \geqslant 0$ e $c_m, d_n \neq 0$. De $cf_0 = cg_0 = 1$ segue que existem coeficientes c_i e d_j não-divisíveis por p, em particular, não-nulos. Tomemos i e j mínimos possíveis e consideremos o coeficiente de grau $i + j$ do polinômio f_0g_0. Este é $b_{i+j} := c_0d_{i+j} + c_1d_{i+j-1} + \cdots + c_{i-1}d_{j+1} + c_id_j + c_{i+1}d_{j-1} + \cdots + c_{i+j}d_0$. Pela escolha de i, os coeficientes $c_0, c_1, \ldots, c_{i-1}$ são divisíveis por p. Pela escolha de j, os coeficientes $d_{j-1}, \ldots, d_0$ são divisíveis por p. Portanto, $p|b_{i+j}$ implica $p|c_id_j$. Uma contradição com UF′ ■

4.18. Teorema. *Seja D um domínio fatorial. Então $D[x]$ é um domínio fatorial.*

Demonstração. Denotamos por K o corpo de frações de D. Considerando D como um subanel em K, podemos interpretar os polinômios de $D[x]$ como os polinômios de $K[x]$, isto é, temos $D \subset K$ e $D \subset D[x] \subset K[x]$.

Primeiramente, vamos mostrar que os elementos irredutíveis em $D[x]$ são exatamente: elementos irredutíveis em D (aqueles que têm grau 0) ou polinômios $p \in D[x]$ de grau > 0 com $cp = 1$ que são irredutíveis em $K[x]$. Levando em conta que o grau do produto de dois polinômios não-nulos é a soma dos graus dos polinômios envolvidos, podemos ver que os elementos inversíveis em $D[x]$ são exatamente os inversíveis em $D \subset D[x]$. Pela mesma razão, os elementos irredutíveis de grau 0 em $D[x]$ são exatamente os irredutíveis em $D \subset D[x]$.

Seja $p \in D[x]$ um polinômio de grau > 0. Então $p = cp \cdot p_0$, onde $p_0 \in D[x]$ e $cp_0 = 1$. Logo, para p ser irredutível em $D[x]$, é necessário que $cp = 1$.

Se p é redutível em $K[x]$, então p é redutível em $D[x]$. Realmente, para uma decomposição não-trivial $p = p_1p_2$ em $K[x]$, ambos p_1 e p_2 tem grau > 0, pois os elementos inversíveis em $K[x]$ são exatamente os polinômios não-nulos de grau 0. Multiplicando por denominador comum dos coeficientes de um polinômio de $K[x]$, conseguimos um polinômio de $D[x]$. Deste modo, obtemos polinômios $f_1 := d_1p_1$ e $f_2 := d_2p_2$ pertencendo a $D[x]$, onde $d_1, d_2 \in D$. Agora obtemos $d_1d_2p = c_1c_2g_1g_2$, onde $f_i = c_ig_i$, $g_i \in D[x]$, $c_i := cf_i$ e $cg_i = 1$ para todo $i = 1, 2$. Pelo Lema 4.17, d_1d_2 e c_1c_2 são associados em D, pois $cp = 1$. Em outras palavras, podemos supor que $p = g_1g_2$ é uma decomposição não-trivial em $D[x]$.

Reciprocamente, suponhamos que p seja redutível em $D[x]$. Então $p = p_1p_2$, com $p_1, p_2 \in D[x]$ não-inversíveis em $D[x]$. De $cp = 1$ segue que ambos p_1 e p_2 têm grau > 0. Assim obtemos uma decomposição não-trivial de p em $K[x]$.

Provaremos EF para $D[x]$. Seja $f \in D[x]$. Considerando f em $K[x]$, podemos decompor f em produto de polinômios irredutíveis em $K[x]$, $f = p_1p_2 \ldots p_n$. Como acima, podemos achar os elementos

$0 \neq d_i \in D$ tais que $q_i := d_i p_i \in D[x]$. Fazendo $c_i := cq_i$, obtemos $q_i = c_i g_i$ com $g_i \in D[x]$ e $cg_i = 1$. Assim, $d_1 d_2 \dots d_n f = c_1 c_2 \dots c_n g_1 g_2 \dots g_n$. Pelo Lema 4.17, $d_1 d_2 \dots d_n \cdot cf = c_1 c_2 \dots c_n$. Cancelando $d_1 d_2 \dots d_n$, obtemos $f = cf \cdot g_1 g_2 \dots g_n$. Pelas considerações acima, g_i é irredutível em $D[x]$, pois $cg_i = 1$ e o polinômio g_i é associado em $K[x]$ ao polinômio p_i, irredutível em $K[x]$. Resta decompor cf em produto de elementos irredutíveis em D e lembrar que estes são irredutíveis em $D[x]$.

Provaremos UF′ para $D[x]$. Seja p irredutível em $D[x]$ e suponhamos que p divide fg em $D[x]$, onde $0 \neq f, g \in D[x]$. Assim, $pq = fg$ para algum $q \in D[x]$. Caso p tenha grau 0, sabemos que $p \in D$ é irredutível em D. Pelo Lema 4.17, p divide $cf \cdot cg$. Pela UF′ válida em D, $p|cf$ ou $p|cg$ em D. Daí concluímos que $p|f$ ou $p|g$ em $D[x]$. Caso p seja de grau > 0, sabemos que p é irredutível em $K[x]$ e que $cp = 1$. Pelos Exemplo 4.9.8, Lema 4.11 e Proposição 4.15, $K[x]$ é um domínio fatorial. Logo, $p|f$ ou $p|g$ em $K[x]$. Digamos, $pg = f$ para algum $g \in K[x]$. Como acima, para um $0 \neq d \in D$ apropriado, temos $b := dg \in D[x]$, $b = cb \cdot b_0$ e $f = cf \cdot f_0$, onde $b_0, f_0 \in D[x]$ e $cb_0 = cf_0 = 1$. Logo, $cb \cdot pb_0 = cf \cdot df_0$. Pelo Lema 4.17, $cb = cf \cdot d$. Assim, $pb_0 = f_0$, isto é, p divide f_0 em $D[x]$. Portanto, p divide f em $D[x]$ ∎

4.19. Critério (Eisenstein)**.** *Seja D um domínio fatorial, seja $p \in D$ irredutível e seja $f = c_n x^n + c_{n-1}x^{n-1} \cdots + c_0 \in D[x]$ com $n > 0$. Suponhamos que p não divida c_n, que p divida $c_{n-1}, \dots, c_0$ e que p^2 não divida c_0. Então f é irredutível em $K[x]$, onde K é o corpo de frações de D.*

Demonstração. Suponhamos que $f = f_1 f_2$, onde $f_1, f_2 \in D[x]$ são de graus $k > 0$ e $n - k > 0$, respectivamente. O homomorfismo canônico $^- : D \to \overline{D}$, onde $\overline{D} := D/Dp$, induz um homomorfismo $^- : D[x] \to \overline{D}[x]$. Pela UF″ válida para D e pela Definição-Lema 4.5, $\overline{D}$ é um domínio. Temos $\overline{f} = \overline{c}_n x^n \neq \overline{0}$. Sendo $\overline{D}$ um domínio, obtemos $\overline{f}_1 = \overline{a}_k x^k$ e $\overline{f}_2 = \overline{b}_{n-k} x^{n-k}$, onde $\overline{c}_n = \overline{a}_k \cdot \overline{b}_{n-k}$. De $k > 0$ e $n - k > 0$ segue que os termos constantes de f_1 e de f_2 são divisíveis por p implicando que c_0 é divisível por p^2. Uma contradição. Portanto, na decomposição de f em produto de polinômios irredutíveis em $D[x]$ somente um polinômio irredutível pode ter grau > 0. Pela descrição de polinômios irredutíveis em $D[x]$ presente na demonstração do Teorema 4.18, concluímos o desejado ∎

4.20. Decomposição em frações parciais. *Seja K um corpo, sejam $0 \neq f, g \in K[x]$ polinômios não-nulos e seja $g = \prod_{i=1}^{n} p_i^{r_i}$ uma decomposição de g em produto de polinômios irredutíveis, onde $r_i > 0$ e os p_i's não são associados por pares. Então $\frac{f}{g} = a + \sum_{i=1}^{n} \sum_{j=1}^{r_i} \frac{b_{ij}}{p_i^j}$, onde $a, b_{ij} \in K[x]$ e, para todos i e j, o grau de b_{ij} é estritamente menor do que o de p_i caso b_{ij} não seja nulo.*

Demonstração. Consideramos os polinômios $g_i := \frac{g}{p_i^{r_i}} \in K[x]$, $i = 1, 2, \dots, n$. Claramente, $\operatorname{mdc}(g_1, g_2, \dots, g_n) = 1$. Sendo $K[x]$ um domínio principal, podemos encontrar $t_1, t_2, \dots, t_n \in K[x]$ tais que $\sum_{i=1}^{n} t_i g_i = 1$. Logo, $\frac{f}{g} = \frac{f \sum_{i=1}^{n} t_i g_i}{g} = \sum_{i=1}^{n} \frac{a_i}{p_i^{r_i}}$ para alguns $a_i \in K[x]$. Resta repetidamente aplicar o algoritmo euclidiano, dividindo com resto a_i por p_i ∎

Um polinômio não-nulo se chama *mônico* se o seu coeficiente de grau maior é igual a 1. Seja A um anel e sejam $a, b \in A[x]$ com b mônico. É fácil ver que existem $q, r \in A[x]$ tais que o grau de r é menor do que o de b (ou $r = 0$) e $a = qb + r$. Em outras palavras, a divisão com resto funciona em polinômios sobre qualquer anel se dividimos por um polinômio mônico.

4.21 Observação. *Seja A um anel, seja $f \in A[x]$ e seja $a \in A$. Se $f(a) = 0$, então $f = (x - a)q$ para algum $q \in A[x]$.*

Demonstração. Dividindo com resto f por $x - a$, obtemos $f = (x-a)q + r$, onde $r \in A$. Substituíndo $x := a$, vemos que $r = 0$ ∎

Na situação descrita na Observação 4.21, dizemos que $a \in A$ é uma *raiz* de $f \in A[x]$. Dizemos que uma raiz $a \in A$ de $f \in A[x]$ tem *multiplicidade* m se $f = (x - a)^m h$, onde $h \in A[x]$ e $h(a) \neq 0$.

4.22. Lema. *Seja D um domínio e seja $f \in D[x]$ um polinômio que possui n raízes distintas $r_1, \ldots, r_n \in D$. Então $f = (x - r_1) \cdot \ldots \cdot (x - r_n)g$ para algum $g \in D[x]$.*

Demonstração. Por indução sobre n, podemos supor que $f = (x - r_1) \cdot \ldots \cdot (x - r_{n-1})h$ para algum $h \in D[x]$. De $f(r_n) = 0$, de $r_n \neq r_i$ para todo $i \neq n$ e de D ser um domínio, segue que $h(r_n) = 0$. Pela Observação 4.21, $h = (x - r_n)g$ ■

4.23. Fórmula de interpolação de Lagrange. *Seja K um corpo, sejam $a_1, \ldots, a_{n+1} \in K$ distintos por pares e sejam $v_1, \ldots, v_{n+1} \in K$ arbitrários. Então existe um polinômio único $f \in K[x]$ de grau $\leqslant n$ (ou nulo) tal que $f(a_i) = v_i$ para todo $1 \leqslant i \leqslant n + 1$.*

Demonstração. Façamos $f_i := (x - a_1) \ldots (x - a_{i-1})(x - a_{i+1}) \ldots (x - a_n)$. Então $f_i(a_i) \neq 0$. O desejado polinômio é dado por $f := \sum_{i=1}^{n} \frac{v_i f_i}{f_i(a_i)}$. A unicidade segue do Lema 4.22 ■

Seja A um anel e seja $f := a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in A[x]$. Definimos a *derivada* f' de f pela regra: $f' := a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$. É fácil ver que a função $f \mapsto f'$ é um endomorfismo do A-módulo $A[x]$. Por indução definimos as derivadas *sucessivas* $f'' := (f')'$, ..., $f^{(n+1)} := \big(f^{(n)}\big)'$.

4.24. Regra de Leibniz. *Seja A um anel e sejam $f, g \in A[x]$. Então $(fg)' = f'g + fg'$.*

Demonstração. Sendo derivada um endomorfismo do A-módulo $A[x]$, basta verificar a identidade para $f := x^m$ e $g := x^n$ ■

Seja A um anel. A regra $h : n \mapsto n \cdot 1$ define um homomorfismo de anéis $h : \mathbb{Z} \to A$. Claramente, a imagem $S := h\mathbb{Z}$ de h é o subanel mínimo de A. Pelo Teorema 3.12.1, $S \simeq \mathbb{Z}/\mathbb{Z}n$ para algum $n \geqslant 0$. Caso $n > 0$, chamamos n a *característica* de A e denotamos $\chi A := n$. Neste caso, a característica é simplesmente o período aditivo do anel.

Caso seja válida a condição

$$ma = 0 \Rightarrow m = 0 \text{ ou } a = 0$$

para todos $m \in \mathbb{Z}$ e $a \in A$, dizemos que A tem *característica zero,* escrevendo $\chi A = 0$. Neste caso, $S \simeq \mathbb{Z}$.

Para todo domínio D, $\chi D = 0$ ou χD é um número primo. Com efeito, se $md = 0$ e $0 \neq d \in D$, então $(m \cdot 1)d = 0$ e $m \cdot 1 = 0$. Portanto, $\chi D = 0$ ou $m \cdot 1 = 0$ para algum $m > 0$. No último caso, $p := \chi D > 0$ tem que ser um número primo, pois $S \simeq \mathbb{Z}/\mathbb{Z}p$ é um domínio e sabemos que $\mathbb{Z}p \lhd_p \mathbb{Z}$ se e só se p é primo (vide os Definição-Lema 4.5, UF$''$ e Exemplo 4.6.4).

Seja A um anel de característica prima $p := \chi A$. Sendo $\mathbb{Z} \cdot 1 \simeq \mathbb{F}_p$ um corpo, A é um $\mathbb{F}_p$-espaço linear. Segue do binômio de Newton que $\Phi : A \to A$, $\Phi : a \mapsto a^p$, é um endomorfismo chamado endomorfismo de *Frobenius.*

Seja K um corpo de característica $\chi K = 0$. Então K contém um subcorpo isomorfo a $\mathbb{Q}$ pois $\mathbb{Z}$ é um subanel de K e $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$. Logo, K é um $\mathbb{Q}$-espaço linear.

4.25. Critério. *Seja A um anel de característica 0, $\chi A = 0$, seja $r \in A$ e seja $f \in A[x]$. Então r é uma raiz de f de multiplicidade m se e só se $0 = f(r) = f'(r) = \cdots = f^{(m-1)}(r) \neq f^{(m)}(r)$.*

Demonstração. Pela Observação 4.21, sempre podemos escrever $f = (x-r)^m h$ com $m \geqslant 0$, $h \in A[x]$ e $h(r) \neq 0$. Pela regra de Leibniz 4.24, temos $f^{(k)}(r) = 0$ para $0 \leqslant k < m$ e $f^{(m)}(r) = m!\, h(r) \neq 0$ ■

4.26. Teorema. *Seja K um corpo finito e seja $p = \chi K$. Então $|K| = p^n$ para algum $n > 0$. A identidade $x^{p^n} = x$ vale para todos os elementos $x \in K$. O grupo multiplicativo $K^* := K \setminus 0$ de K é cíclico.*

Demonstração. K é um $\mathbb{F}_p$-espaço linear. Portanto, possui uma base linear sobre $\mathbb{F}_p$, digamos, de n elementos. Logo, $|K| = p^n$. O grupo K^* tem $p^n - 1$ elementos. Denotamos por q o período de K^*. Claramente, q divide $p^n - 1$. Todo $x \in K^*$ satisfaz a identidade $x^q = 1$. Consequentemente, todo

elemento de K é uma raiz do polinômio $x^{q+1}-x$. Pelo Lema 4.22, $q+1 \geqslant p^n$ pois o corpo K possui p^n elementos distintos. Daí, $q = p^n - 1$. Resta, utilizando o Teorema 2.13, resolver o seguinte

4.27. Exercício. Seja A um grupo abeliano finito. Se a ordem de A é igual ao período de A, então A é cíclico ■

Seja C um anel fixo. Um anel A munido de um homomorfismo $C \to A$ de anéis se chama *C-álgebra.* Um outro jeito de definir C-álgebra: uma C-álgebra A é um anel A que é simultaneamente um C-módulo tal que as igualdades $c \cdot (a_1 \cdot a_2) = (c \cdot a_1) \cdot a_2 = a_1 \cdot (c \cdot a_2)$ são válidas para todos $a_1, a_2 \in A$ e $c \in C$. Uma *subálgebra* é um subanel que é simultaneamente um submódulo. Claramente, a intersecção de qualquer família de subálgebras é uma subálgebra. Daí obtemos o conceito de C-subálgebra gerada por um subconjunto $G \subset A$, denotada por $C[G]$. Um *homomorfismo* de C-álgebras é simplesmente um homomorfismo de anéis e, simultaneamente, de C-módulos. Um outro jeito de definir um homomorfismo entre C-álgebras A_1 e A_2 : temos homomorfismos $h_i : C \to A_i$, $i = 1, 2$; um homomorfismo de anéis $h : A_1 \to A_2$ é dito *homomorfismo* de C-álgebras se $h \circ h_1 = h_2$.

4.28. Definição. Seja $A = C[G]$ uma C-álgebra gerada por G. Dizemos que A é uma C-álgebra *livre* com *geradores livres* G se, para qualquer função $f : G \to A'$, onde A' é uma C-ágebra, existe um único homomorfismo de C-álgebras $h : A \to A'$ que estende f, isto é, $h|_G = f$.

Vamos observar que existem C-álgebras livres finitamente geradas. São C-álgebras de polinômios de várias variáveis sobre C. Realmente, seja $A := C[x_1, \ldots, x_n]$, seja A' uma C-álgebra e seja $f : x_i \mapsto a_i \in A'$. Para construir um homomorfismo de C-álgebras $h : A \to A'$ que estende f, precisamos levar o monômio $x_1^{i_1} \ldots x_n^{i_n}$, $i_1, \ldots, i_n \geqslant 0$ (se $i_1 = \cdots = i_n = 0$, este monômio é 1 por definição), para $a_1^{i_1} \ldots a_n^{i_n}$. Daí obtemos a definição de h (a única possível) :

$$h : \sum_{i_1,\ldots,i_n \geqslant 0} c_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n} \mapsto \sum_{i_1,\ldots,i_n \geqslant 0} c_{i_1,\ldots,i_n} a_1^{i_1} \ldots a_n^{i_n}.$$

É fácil verificar que essa regra realmente define um C-homomorfismo $h : A \to A'$. Este homomorfismo pode ser descrito como $hf := f(a_1, \ldots, a_n)$, ou seja, como $hf := f|_{x_1=a_1,\ldots,x_n=a_n}$. O caso particular e importante de $A' = C$ já foi utilizado nos Exemplo 4.2.3, Observação 4.21 e Lema 4.22. Neste caso, escolhendo "valores" $x_1 = c_1, \ldots, x_n = c_n$, obtemos o "valor" $f(c_1, \ldots, c_n)$ do polinômio $f \in C[x_1, \ldots, x_n]$. Assim, definimos uma função

$$C[x_1, \ldots, x_n] \to \mathrm{Func}(\underbrace{C \times \cdots \times C}_{n \text{ vezes}}, C) \qquad f \mapsto \big((c_1, \ldots, c_n) \mapsto f(c_1, \ldots, c_n)\big)$$

que é um homomorfismo de C-álgebras (vide o Exemplo 3.2.6). Este homomorfismo de substituição "considera" as expressões formais chamadas polinômios como "funções de n variáveis". Será que são as mesmas coisas? Sim, em algumas circunstâncias:

4.29. Lema. *Seja D um domínio infinito. Então o homomorfismo $D[x_1, \ldots, x_n] \to \mathrm{Func}(D^n, D)$ é injetivo.*

Demonstração. Indução sobre n. Para $n = 0$, ambas álgebras são iguais a D e o homomorfismo é idêntico. Seja $f \in D[x_1, \ldots, x_n]$ um polinômio que é nulo como função, isto é, $f(d_1, \ldots, d_n) = 0$ para todos $d_1, \ldots, d_n \in D$. Precisamos provar que $f = 0$ (como expressão formal). Sendo $D[x_1, \ldots, x_n] = D[x_1, \ldots, x_{n-1}][x_n]$, podemos escrever $f = f_m x_n^m + \cdots + f_0$, onde $f_0, \ldots, f_m \in D[x_1, \ldots, x_{n-1}]$. Supondo que $f \neq 0$, podemos supor que $f_m \neq 0$. Pela hipótese de indução, existem $d_1, \ldots, d_{n-1} \in D$, tais que $f_m(d_1, \ldots, d_{n-1}) \neq 0$. Sendo f nulo como função, $f_m(d_1, \ldots, d_{n-1})d^m + \cdots + f_0(d_1, \ldots, d_{n-1}) = 0$ para todo $d \in D$. Isto significa que todo $d \in D$ é uma raiz do polinômio não-nulo $g := f_m(d_1, \ldots, d_{n-1})x^m + \cdots + f_0(d_1, \ldots, d_{n-1}) \in D[x]$. Pelos Lema 4.22 e infinitude de D, chegamos a uma contradição ■

4.30. Exercício. Podemos omitir a condição de que D é um domínio no Lema 4.29 ou que D é infinito?

Seja C um anel. O grupo de permutações Σ_n age sobre a C-álgebra de polinômios $P := C[t_1, \dots, t_n]$, $\Sigma_n \curvearrowright P$, pela regra $\sigma f := f(t_{\sigma^{-1}1}, \dots, t_{\sigma^{-1}n})$. Os polinômios de

$$S := C[t_1, \dots, t_n]^{\Sigma_n} := \{ f \in C[t_1, \dots, t_n] \mid \sigma f = f \text{ para todo } \sigma \in \Sigma_n \}$$

são ditos *simétricos*. É fácil verificar que S é uma C-subálgebra de P. Façamos $p_{i,n} := t_1^i + \dots + t_n^i$ para $i \geqslant 1$ e

$$C[x, t_1, \dots, t_n] \ni F_n := (x - t_1) \cdot \ldots \cdot (x - t_n) :=$$

$$(\mathbf{4.31}) \qquad = x^n - s_{1,n}(t_1, \dots, t_n)x^{n-1} + s_{2,n}(t_1, \dots, t_n)x^{n-2} - \dots + (-1)^n s_{n,n}(t_1, \dots, t_n).$$

É fácil ver que $p_{i,n}, s_{i,n} \in C[t_1, \dots, t_n]^{\Sigma_n}$.

4.32. Teorema. *A C-álgebra $C[t_1, \dots, t_n]^{\Sigma_n}$ é gerada por $s_{1,n}, \dots, s_{n,n}$. Caso $\mathbb{Q} \subset C$, a C-ágebra $C[t_1, \dots, t_n]^{\Sigma_n}$ admite os geradores $p_{1,n}, \dots, p_{n,n}$.*

Demonstração. Definimos em $C[x_1, \dots, x_n]$ um grau "novo" gr de um polinômio fazendo $\operatorname{gr} x_i = i$. (Assim o grau "novo" de um monômio é a soma dos graus "novos" das variáveis nele envolvidos, contando com multiplicidades.) Por indução sobre n provemos que, para todo polinômio $f \in C[t_1, \dots, t_n]^{\Sigma_n}$, existe um polinômio $g \in C[x_1, \dots, x_n]$ tal que $\operatorname{gr} g \leqslant \deg f$ e $f = g(s_{1,n}, \dots, s_{n,n})$. O caso $n = 1$ é óbvio.

Substituindo em (4.31) $t_n = 0$, obtemos $s_{1,n}|_{t_n=0} = s_{1,n-1}$, $\dots$, $s_{n-1,n}|_{t_n=0} = s_{n-1,n-1}$. Pela hipotése de indução, $f|_{t_n=0} = g_1\big(s_{1,n}|_{t_n=0}, \dots, s_{n-1,n}|_{t_n=0}\big)$, onde $g_1 \in C[x_1, \dots, x_{n-1}]$ e $\operatorname{gr} g_1 \leqslant \deg f|_{t_n=0} \leqslant \deg f$. Observamos que $\deg g_1(s_{1,n}, \dots, s_{n-1,n}) \leqslant \operatorname{gr} g_1 \leqslant \deg f$, pois $\deg s_{i,n} \leqslant i$.

Agora façamos a indução sobre $d := \deg f$. O caso $\deg f = 0$ é trivial. Claramente, o polinômio $f_1 := f - g_1(s_{1,n}, \dots, s_{n,n-1})$ é simétrico e $\deg f_1 \leqslant \deg f$. De $f_1|_{t_n=0} = 0$ segue que f_1 é divisível por t_n. Sendo f_1 simétrico, ele é divisível por $t_1 \cdot \ldots \cdot t_n = \pm s_{n,n}$. Portanto $f_1 = s_{n,n} f_2$, onde f_2 é simétrico e $\deg f_2 \leqslant \deg f - n$. Pela hipotése de indução sobre d, existe $g_2 \in C[x_1, \dots, x_n]$ tal que $\operatorname{gr} g_2 \leqslant \deg f - n$ e $f_2 = g_2(s_{1,n}, \dots, s_{n,n})$. Consequentemente, $f = g_1(s_{1,n}, \dots, s_{n-1,n}) + s_{n,n} g_2(s_{1,n}, \dots, s_{n,n})$.

Suponhamos que $\mathbb{Q} \subset C$. Obviamente, $\frac{\partial F_n/\partial x}{F_n} = \sum_{i=1}^n \frac{1}{x - t_i}$ e $\frac{1}{x - t_i} = \sum_{j \geqslant 0} \frac{t_i^j}{x^{j+1}}$. Portanto,

$$(\mathbf{4.33}) \qquad \frac{\partial F_n/\partial x}{F_n} \cdot x = n + \frac{p_{1,n}}{x} + \dots + \frac{p_{i,n}}{x^i} + \dots$$

Multiplicando (4.33) por $\dfrac{F_n}{x^n}$, obtemos

$$n - (n-1)\frac{s_{1,n}}{x} + (n-2)\frac{s_{2,n}}{x^2} - \dots + (-1)^{n-1}\frac{s_{n-1,n}}{x^{n-1}} =$$

$$= \Big(1 - \frac{s_{1,n}}{x} + \frac{s_{2,n}}{x^2} - \dots + (-1)^n \frac{s_{n,n}}{x^n}\Big)\Big(n + \frac{p_{1,n}}{x} + \dots + \frac{p_{i,n}}{x^i} + \dots\Big).$$

Comparando os coeficientes de $\frac{1}{x^k}$, chegamos às fórmulas de *Newton*: Para $1 \leqslant k \leqslant (n-1)$ temos

$$p_{k,n} - p_{k-1,n}s_{1,n} + p_{k-2,n}s_{2,n} - \dots + (-1)^{k-1}p_{1,n}s_{k-1,n} + (-1)^k n s_{k,n} = (-1)^k(n-k)s_{k,n},$$

isto é,

$$(\mathbf{4.34}) \qquad p_{k,n} - p_{k-1,n}s_{1,n} + p_{k-2,n}s_{2,n} - \dots + (-1)^{k-1}p_{1,n}s_{k-1,n} + (-1)^k k s_{k,n} = 0.$$

Para $k = n$, temos

$$p_{k,n} - p_{k-1,n}s_{1,n} + p_{k-2,n}s_{2,n} - \cdots + (-1)^{n-1}p_{1,n}s_{n-1,n} + (-1)^n n s_{n,n} = 0.$$

Assim, a fórmula (4.34) é válida também para $k = n$. Para $k > n$, temos

$$p_{k,n} - p_{k-1,n}s_{1,n} + p_{k-2,n}s_{2,n} - \cdots + (-1)^n p_{k-n,n}s_{n,n} = 0.$$

Suponhamos que $\mathbb{Q} \subset A$. Por indução sobre k, a fórmula (4.34) válida para $1 \leqslant k \leqslant n$ permite obter uma expessão polinomial de $s_{k,n}$ em $p_{i,n}$'s, $1 \leqslant i \leqslant n$ ■

Um exemplo importante de um polinômio simétrico é o *discriminante*: Seja $f = x^n + c_1x^{n-1} + \cdots + c_n$ um polinômio mônico sobre um corpo K. Em uma extensão algébrica $F \supset K$, temos uma decomposição $f = (x - r_1)\dots(x - r_n)$, onde $r_1, \dots, r_n \in F$. Façamos $\operatorname{discr} f(r_1, \dots, r_n) := \prod_{i<j}(r_i - r_j)^2$. Sendo simétrico em r_i's, $\operatorname{discr} f$ é um polinômio em c_k's. Por outro lado, $\operatorname{discr} f$ "sabe" se f tem todas as raízes distintas: isto é equivalente à desigualdade $\operatorname{discr} f \neq 0$.

A. Teoria de Galois (definições e exercícios)

Sejam $k \subset K$ corpos (= uma extensão de corpos). Podemos tratar K como um k-espaço linear. Uma extensão $k \subset K$ é dita *finita* se $\dim_k K < \infty$. Um $a \in K$ é dito *algébrico sobre* k se existe um polinômio mônico $p \in k[x]$ tal que $p(a) = 0$. Tal polinômio (mônico) $p(x)$ de grau mínimo se chama *polinômio minimal de* α *sobre* k. Claramente, o polinômio minimal é irredutível em $k[x]$. A extensão $k \subset K$ é dita *algébrica* se todo $a \in K$ é algébrico.

Seja $k \subset K$ uma extensão de corpos e seja $G \subset K$. Denotamos por $k[G]$ e por $k(G)$, respectivamente, a k-subálgebra de K gerada por G e o k-subcorpo (isto é, um subcorpo que contém k) de K gerado por G.

Exercícios. Mostre as seguintes afirmações.

1. As extensões de corpos $k \subset F$ e $F \subset K$ são finitas se e só se a extensão $k \subset K$ é finita. Neste caso, $\dim_k K = \dim_k F \cdot \dim_F K$. (Dica: se a_i's formam uma base k-linear de F e b_j's formam uma base F-linear de K, então os elementos a_ib_j's formam uma base k-linear de K.)

2. Qualquer extensão finita $k \subset K$ é algébrica. (Dica: para $a \in K$, considere uma dependência k-linear entre os elementos $1, a, a^2, \dots$)

3. Seja $a \in K$ um elemento algébrico sobre $k \subset K$. Então $k[a] = k(a)$. (Dica: note que qualquer domínio de dimensão finita sobre k é um corpo e aplique este fato para $k[a]$.)

4. Um elemento $a \in K$ é algébrico sobre $k \subset K$ se e só se a extensão $k \subset k(\alpha)$ é finita.

5. Seja $k \subset K$ uma extensão gerada por um conjunto finito de elementos algébricos sobre k. Então a extensão $k \subset K$ é finita.

6. As extensões de corpos $k \subset F$ e $F \subset K$ são algébricas se e só se a extensão $k \subset K$ é algébrica. (Dica: Seja $a \in K$ um elemento algébrico sobre F e seja F' o k-subcorpo de F gerado pelos coeficientes do polinômio minimal de a sobre F. Então a extensão $F' \subset F'(a)$ é finita e a extensão $k \subset F'$ é finita se a extensão $k \subset F$ é algébrica.)

7. Seja $p \in k[x]$ um polinômio irredutível. Então $k[x]/\operatorname{Ideal} p$ é um corpo, onde $\operatorname{Ideal} p$ denota o ideal de $k[x]$ gerado por p. (Dica: o mesmo fato vale para qualquer domínio principal.)

8. Seja $a \in K$ um elemento algébrico sobre $k \subset K$ e seja p o polinômio minimal de a sobre k. Então, para qualquer $f \in k[x]$, $f(a) = 0$ implica que f é divisível por p. Além disso, $k(a) \simeq k[x]/\operatorname{Ideal} p$ e $\dim_k k(a) = \deg p$.

9. Sejam $k \subset k(a)$ e $k' \subset k'(a')$ extensões algébricas e seja $\sigma : k \to k'$ um isomorfismo de corpos. Denotamos pela mesma letra o homomorfismo induzido entre os anéis de polinômios $\sigma : k[x] \to k'[x]$. Seja $p \in k[x]$ o polinômio minimal de a sobre k. Suponhamos que σp é o polinômio minimal de a' sobre k'. Então existe um único isomorfismo $\overline{\sigma} : k(a) \to k'(a')$ que estende σ tal que $\overline{\sigma}a = a'$.

Seja k um corpo e seja $M \subset k[x]$ um conjunto de polinômios. Uma extensão $k \subset K$ de corpos é dita *corpo de decomposição de* M se todo polinômio $f \in M$ se decompõe sobre K na forma $f = a(x - r_1) \cdot \ldots \cdot (x - r_n)$, onde $a \in k$, e K é gerado sobre k por todas as raízes de polinômios de M.

Seja $k \subset K$ uma extensão de corpos. Denotamos por $\texttt{subfields}_k\, K$ o conjunto de todos os subcorpos de K que contêm k.

Seja G um grupo. Denotamos por $\texttt{subgroups}\, G$ o conjunto de todos os subgrupos de G.

Exercícios. Mostre as seguintes afirmações.

10. Seja $f \in k[x]$, $\deg f = n$. Então existe K, um corpo de decomposição de f e $\dim_k K \leqslant n!$. (Dica: Use a indução sobre n. Seja p um divisor irredutível de f. Então, sobre o corpo $K' = k[x]/\operatorname{Ideal} p$, o polinômio f possui uma raiz r, K' é gerado sobre k por r e $\dim_k K' \leqslant n$. Portanto, $f = (x - r)f'$, onde $f' \in K'[x]$ e $\deg f' < n$. Resta utilizar a hipótese de indução para K' e f'.)

11. Seja $\sigma : k \to k'$ um isomorfismo de corpos e seja $f \in k[x]$. Seja $k \subset K$ um corpo de decomposição de f e seja $k' \subset K'$ um corpo de decomposição de σf. Então existe um isomorfismo de corpos $\overline{\sigma} : K \to K'$ que estende σ. (Dica: Use a indução sobre $\deg f$. Seja p um divisor irredutível de f. Seja $r \in K$ uma raiz de p e seja $r' \in K'$ uma raiz de σp. Denotamos $K_0 := k(r)$ e $K_0' := k'(r')$. Pelo Exercício 9, obtemos um isomorfismo $\sigma_0 : K_0 \to K_0'$ que estende σ tal que $\sigma_0 r = r'$. Sobre K_0, o polinômio f tem a forma $f = (x - r)f_0$. Obviamente, $\sigma f = (x - r')\sigma_0 f_0$. Resta utilizar a hipótese de indução para $\sigma_0 : K_0 \to K_0'$ e $f_0 \in K_0[x]$.)

12. Seja $\sigma : k \to k'$ um isomorfismo de corpos e seja $M \subset k[x]$ um conjunto de polinômios. Seja $k \subset K$ um corpo de decomposição de M e seja $k' \subset K'$ um corpo de decomposição de σM. Então existe um isomorfismo de corpos $\overline{\sigma} : K \to K'$ que estende σ. (Dica: aplique o lema de Zorn para as triplas (M_i, K_i, σ_i) apropriadamente ordenadas, onde $M_i \subset M$, $k \subset K_i \subset K$ é um corpo de decomposição de M_i, $\sigma_i : K_i \to K_i'$ é um isomorfismo de corpos que estende σ e $k' \subset K_i' \subset K$ é um corpo de decomposição de σM_i.)

13. Seja k um corpo e seja $G \subset k^*$ um subgrupo finito. Então G é cíclico. (Dica: seja p o período de G, considere o número de raízes do polinômio $x^p - 1$.)

14. Seja $p > 0$ um número primo e seja $n > 0$. Então existe um único (a menos de isomorfismo) corpo K tal que $|K| = p^n$. (Tal corpo se denota por $\mathbb{F}_{p^n}$.)

15. Seja $p > 0$ um número primo e seja $n > 0$. Para todo m que divide n, existe um único subcorpo $K \subset \mathbb{F}_{p^n}$ tal que $|K| = p^m$. (Dica: Seja $a \in \mathbb{F}_{p^n}$ um gerador do grupo cíclico $\mathbb{F}_{p^n}^*$. Então $|a| = p^n - 1$. Para qualquer divisor m de n, o número $p^m - 1$ divide o número $p^n - 1$, isto é, $p^n - 1 = d(p^m - 1)$. Portanto, para $b := a^d$, temos $|b| = p^m - 1$. Isto implica que o polinômio $x^{p^m - 1} - 1$ possui $p^m - 1$ raízes distintas: $b^0, b, b^2, \ldots$ Logo, o polinômio $x^{p^m} - x$ possui p^m raízes distintas que formam o subcorpo desejado.)

16. Seja $k \subset k(a) =: K$ uma extensão algébrica de corpos. Então, para $\mathrm{G}_K\, k := \{g \in \operatorname{Aut} K \mid g|_k = 1_k\}$, temos $|G_K k| \leqslant \dim_k K$. (Dica: Seja $p \in k[x]$ o polinômio minimal de a sobre k. Qualquer $g \in G_K k$ leva a para uma raiz de p que pertence a K e tal g é determinado pela imagem indicada (vide o Exercício 9).)

17. Teorema fundamental da teoria de Galois para corpos finitos. Seja $q := p^n$, onde $p > 0$ é um número primo e $n > 0$. Então o grupo $\operatorname{Aut} \mathbb{F}_q = \mathrm{G}_{\mathbb{F}_q}\, \mathbb{F}_p$ é cíclico de ordem n gerado pelo automorfismo de Frobenius. Existe uma bijeção (a *correspondência de Galois*) entre $\texttt{subfields}_{\mathbb{F}_p}\, \mathbb{F}_q$

e $\mathtt{subgroups}\,\mathrm{G}_{\mathbb{F}_q}\,\mathbb{F}_p$ dada por $\mathrm{F}_{\mathbb{F}_q}\,S := \{a \in \mathbb{F}_q \mid Sa = a\}$ e $\mathrm{G}_{\mathbb{F}_q}\,F := \{g \in \mathrm{Aut}\,\mathbb{F}_q \mid g|_F = 1_F\}$ para $F \in \mathtt{subfields}_{\mathbb{F}_p}\,\mathbb{F}_q$ e $S \in \mathtt{subgroups}\,\mathrm{G}_{\mathbb{F}_q}\,\mathbb{F}_p$.

Um corpo K é dito *algebricamente fechado* se todo polinômio de grau > 0 sobre K possui uma raiz. É fácil ver que um corpo K é algebricamente fechado se e só se qualquer extensão algébrica de K coincide com K.

18. Proposição. *Seja k um corpo. Então existe uma extensão algébrica $k \subset K$ com K algebricamente fechado, chamada* fecho algébrico *de k e denotada por $K = \overline{k}$.*

Seja $\sigma : k \to K$ um homomorfismo de corpos com K algebricamente fechado e seja $k \subset F$ qualquer extensão algébrica. Então existe um homomorfismo $\overline{\sigma} : F \to K$ que estende σ. Em particular, o fecho algébrico de k é único a menos de um isomorfismo sobre k.

Demonstração. Enumeramos todos os polinômios de $k[x]$ de grau > 0 por números transfinitos ordinais: f_i, $i < \tau$. Façamos $K_0 := k$. Seja $\varepsilon \leqslant \tau$ um ordinal. Por indução transfinita, para todo $i \leqslant \varepsilon$, construímos uma extensão algébrica $k \subset K_i$ de modo que f_i se decompõe sobre K_i em fatores de grau 1 e que $K_i \subset K_j$ para $i \leqslant j \leqslant \varepsilon$. Se, para todo $i < \varepsilon$, os K_i's já são construídos e ε é um ordinal limite, façamos $K_\varepsilon := \bigcup_{i<\varepsilon} K_i$. Se existe um ordinal α tal que $\varepsilon = \alpha + 1$, então definimos K_ε como o corpo de decomposicão do polinômio f_α sobre K_α, $K_\alpha \subset K_\varepsilon$. Claramente, $k \subset K = K_\tau$ é uma extensão algébrica. Seja $K \subset E$ uma extensão algébrica e seja $a \in E$. Sendo a extensão $k \subset E$ algébrica, temos o polinômio minimal f_i de a sobre k. Pela construção, $a \in K$.

Para o resto, basta aplicar o lema de Zorn para as duplas (F', σ') apropriadamente ordenadas, onde $k \subset F' \subset F$ e $\sigma' : F' \to K$ é um homomorfismo que estende σ ∎

Uma extensão algébrica de corpos $k \subset K$ é dita *normal* se todo polinômio p irredutível em $k[x]$ que possui uma raiz em K se decompõe sobre K nos fatores de grau 1.

19. Proposição. *Seja $k \subset K$ uma extensão algébrica. Então as seguintes condições são equivalentes.*
1. *A extensão $k \subset K$ é normal.*
2. *K é um corpo de decomposição de algum conjunto de polinômios $M \subset k[x]$.*
3. *Para todo corpo $F \supset K$ e para qualquer homomorfismo $\sigma : K \to F$ idêntico sobre k, temos $\sigma K = K$.*

Demonstração. 1 ⇒ 2. Basta tomar como M o conjunto de todos os polinômios minimais sobre k de todos os elementos de K.

2 ⇒ 3. Seja $f \in M \subset k[x]$. Então $\sigma f = f$ e $f = a(x - r_1) \cdot \ldots \cdot (x - r_n)$, onde $a \in k$ e $r_1, \ldots, r_n \in K$. Daí, $\sigma r_1, \ldots, \sigma r_n$ é uma permutação de $r_1, \ldots, r_n$. Sendo K gerado sobre k por todos tais r_i's, obtemos $\sigma K = K$.

3 ⇒ 1. Tomemos $F := \overline{K} = \overline{k}$. Seja $a \in K$ e seja $p \in k[x]$ o polinômio minimal de a sobre k. Então $p = (x - a)(x - r_1) \cdot \ldots \cdot (x - r_n)$, onde $r_i \in F$. Para todo i, existe um homomorfismo $\sigma_i : k(a) \to k(r_i)$ sobre k tal que $\sigma_i a = r_i$. Pela Proposição 18, podemos estender σ_i para um homomorfismo $\overline{\sigma}_i : K \to F$. Agora, $r_i = \overline{\sigma}_i a \in \overline{\sigma}_i K = K$ ∎

Seja $k \subset K$ uma extensão algébrica. Então (em $\overline{k} = \overline{K}$) existe uma extensão normal mínima que contém K chamada *fecho normal* de K. Essa é o corpo de decomposição dos polinômios minimais sobre k para todos os elementos de K. Se a extensão $k \subset K$ é finita, então o fecho normal é uma extensão finita, pois, pela Proposição 19, o fecho normal é o corpo de decomposição dos polinômios minimais para os geradores de K sobre k.

Seja $k \subset K$ uma extensão de corpos. Um elemento $a \in K$ algébrico sobre k é dito *separável* sobre k se todas as raízes (no fecho algébrico $\overline{k}$ de k) do seu polinômio minimal sobre k são distintas. Seja $f \in k[x]$ o polinômio minimal para $a \in K$. Suponhamos que f tenha uma raiz $r \in \overline{k}$ de multiplicidade > 1. Então a derivada f' também tem a raiz r. Se $f' \neq 0$, então, sendo f é irredutível e sendo $\deg f > \deg f'$, o maior divisor comum de f e f' é 1. Daí, obtemos $fg + f'h = 1$ para alguns polinômios $g, h \in k[x]$.

Substituindo $x = r$, obtemos $0 = 1$. Uma contradição. Portanto, $f' = 0$. Isto pode ocorrer apenas quando $f = q(x^p)$ para algum polinômio $q \in k[x]$, onde $p \neq 0$ é a característica de k. Em particular, caso $p = 0$, os polinômios irredutíveis não têm raízes múltiplas.

Dizemos que uma extensão algébrica de corpos $k \subset K$ é *separável* se todo elemento $a \in K$ é separável sobre k. Para um corpo K de característica $p \neq 0$, façamos $K^p := \{a^p \mid a \in K\}$.

20. Proposição. *Seja k um corpo de característica $p \neq 0$. Então são válidas as seguintes afirmações.*
1. *Sejam $k \subset F \subset K$ extensões de corpos. Se $a \in K$ é separável sobre k, então a é separável sobre F.*
2. *Sejam $k \subset F \subset K$ extensões de corpos. Se a extensão $k \subset K$ é separável, então a extensão $F \subset K$ é separável.*
3. *Seja $k \subset K$ uma extensão finita de corpos. Então a extensão $k \subset K$ é separável se e só se $kK^p = K$.*
4. *Seja $k \subset K$ uma extensão de corpos e seja $a \in K$ um elemento algébrico sobre k. Então a é separável sobre k se e só se a extensão $k \subset k(a)$ é separável.*
5. *Sejam $k \subset F$ e $F \subset K$ extensões separáveis de corpos. Então a extensão $k \subset K$ é separável.*

Demonstração. 1. O polinômio minimal de a sobre F divide em $F[x]$ o polinômio minimal de a sobre k.

2 segue de **1**.

3. Suponhamos que a extensão $k \subset K$ é separável. Por **2**, a extensão $kK^p \subset K$ é separável. Qualquer $a \in K$ é uma raiz do polinômio $g := x^p - a^p$ sobre kK^p. Portanto, o polinômio minimal f de a sobre kK^p divide g. Por outro lado, $g = (x - a)^p$ que implica $\deg f = 1$, pois f não tem raízes múltiplas. Em outras palavras, $a \in kK^p$.

Suponhamos que $kK^p = K$ e seja $a \in K$ não-separável sobre k, isto é, o polinômio minimal f de a sobre k tem a forma $f = q(x^p)$ para algum $q \in k[x]$. Seja $m + 1 := \deg f$. Então $1, a, \ldots, a^m$ são linearmente independentes sobre k. Seja $e_0, e_1, \ldots, e_n$ uma base k-linear de K que contém $1, a, \ldots, a^m$, $n \geqslant m$. Então $K = ke_0 + ke_1 + \cdots + ke_n$. De $K = kK^p$ concluímos que $K = kK^p = ke_0^p + ke_1^p + \cdots + ke_n^p$. Em outras palavras, $e_0^p, e_1^p, \ldots, e_n^p$ é uma base K-linear de F. Em particular, $1^p, a^p, a^{2p} \ldots, a^{mp}$ são k-linearmente independentes. De $q(a^p) = 0$, concluímos que $1^p, a^p, (a^p)^2, \ldots, (a^p)^l$ são k-linearmente dependentes, onde $l := \deg q < \deg f = m + 1$. Uma contradição.

4. Podemos supor que $K = k(a)$ com a separável sobre k. Por **3**, é suficiente mostrar que $kK^p = K$. Por **1**, a é separável sobre kK^p. Por outro lado, a é uma raiz do polinômio $g := x^p - a^p \in kK^p[x]$ e $g = (x - a)^p$. Assim, o polinômio minimal de a sobre kK^p é $x - a$. Logo, $a \in kK^p$.

5. Seja $a \in K$. Denotamos por F' o subcorpo de F gerado sobre k pelos coeficientes do polinômio minimal f de a sobre F. É claro que f é o polinômio minimal de a sobre F'. Portanto, a é separável sobre F'. Seja $K' := F'(a)$. Por **4**, a extensão $F' \subset K'$ é separável. A extensão $k \subset F'$ é separável também. Temos $\dim_k F' < \infty$ e $\dim_{F'} K' < \infty$. Por **3**, obtemos $K' = F'K'^p = kF'^pK'^p = k(F'K')^p = kK'^p$ ∎

21. Teorema (sobre um elemento primitivo)**.** *Seja $k \subset k(a, b_1, \ldots, b_n) =: K$ uma extensão algébrica tal que todos os b_i's são separáveis sobre k. Então $K = k(d)$ para algum $d \in K$.*

Demonstração. Podemos supor que $|k| = \infty$. Por indução sobre n, podemos supor que $n = 1$. Sejam $f, g \in k[x]$ respectivamente os polinômios minimais para $a, b := b_1$ sobre k. Seja $c \in k$ e sejam $b, r_1, \ldots, r_m \in \overline{k}$ todas as raízes de g (distintas por pares, pois b é separável sobre k). Consideremos o polinômio $h_c := f\big(c(x - b) + a\big)$ que tem raiz b. Note que r_i é uma raiz de h_c se e só se $c(r_i - b) + a$ é uma raiz de f. Já que k é infinito, podemos escolher $c \in k$ de modo que os polinômios g e h_c tenham apenas uma raiz comum b. Façamos $d =: a - cb$ e $F := k(d) \subset K$. Obviamente, $g, h_c \in F[x]$. O maior divisor comum de g e h_c em $F[x]$ tem a forma $ug + vh_c$ para alguns $u, v \in F[x]$. Este pode ser somente $x - b$, impicando que $b \in F$ e, portanto, $a \in F$ ∎

Uma extensão algébrica de corpos é dita *extensão de Galois* se ela é normal e separável. Lidaremos somente com as extensões finitas de Galois.

22. Teorema (fundamental da teoria de Galois)**.** *Seja $k \subset K$ uma extensão finita de Galois. Então, para todo $F \in \mathtt{subfields}_k K$, a extensão $F \subset K$ é de Galois. As fórmulas $\mathrm{F}_K S := \{a \in K \mid Sa = a\}$ e $\mathrm{G}_K F := \{g \in \operatorname{Aut} K \mid g|_F = 1_F\}$ para $F \in \mathtt{subfields}_k K$ e $S \in \mathtt{subgroups}\,\mathrm{G}_K k$ definem uma bijeção* (a correspondência de Galois) *entre $\mathtt{subfields}_k K$ e $\mathtt{subgroups}\,\mathrm{G}_K k$ tal que $|\mathrm{G}_K F| = \dim_F K$. Um subgrupo $S \leqslant \mathrm{G}_K k$ é normal se e só se a extensão $k \subset \mathrm{F}_K S$ é normal. Neste caso, $\mathrm{G}_{\mathrm{F}_K S} k \simeq \mathrm{G}_K k/S$.*

Demonstração. Seja $F \in \mathtt{subfields}_k K$. Pela Proposição 19.2, K é um corpo de decomposição de $M \subset k[x]$, implicando que K é um corpo de decomposição de $M \subset F[x]$. Pelas Proposições 19.2 e 20.2, a extensão $F \subset K$ é de Galois. Pelo Teorema 21, $K = k(d)$. Seja $r \in \overline{k}$ uma raiz do polinômio minimal p de d sobre k. Pelo Exercício 9, existe um isomorfismo $\sigma : k(d) \to k(r) \subset \overline{k}$ idêntico sobre k tal que $\sigma d = r$. Pela Proposição 19.3, $\sigma \in \mathrm{G}_K k$. As raízes de p são distintas por pares. Portanto, $|\mathrm{G}_K k| \geqslant \deg p = \dim_k K$. Pelo Exercício 16, $|\mathrm{G}_K k| \leqslant \dim_k K$. Logo, $|\mathrm{G}_K F| = \dim_F K$ para todo $F \in \mathtt{subfields}_k K$.

Note que $F \subset F'$ implica $\mathrm{G}_K F \supset \mathrm{G}_K F'$, que $S \subset S'$ implica $\mathrm{F}_K S \supset \mathrm{F}_K S'$, que $F \subset \mathrm{F}_K \mathrm{G}_K F$ e que $S \subset \mathrm{G}_K \mathrm{F}_K S$ para quaisquer $F, F' \in \mathtt{subfields}_k K$ e $S, S' \in \mathtt{subgroups}\,\mathrm{G}_K k$. Daí, $\mathrm{G}_K F \supset \mathrm{G}_K F'$, onde $F \subset F' := \mathrm{F}_K \mathrm{G}_K F$, e $\mathrm{G}_K F \subset \mathrm{G}_K \mathrm{F}_K(\mathrm{G}_K F)$, isto é, $\mathrm{G}_K F = \mathrm{G}_K F'$. Por outro lado, de $|\mathrm{G}_K F| = \dim_F K$, $|\mathrm{G}_K F'| = \dim_{F'} K$ e $F \subset F'$, concluímos que $F = F'$, ou seja, que $\mathrm{F}_K \mathrm{G}_K F = F$ para todo $F \in \mathtt{subfields}_k K$.

Seja $S \in \mathtt{subgroups}\,\mathrm{G}_K k$. Pelo Teorema 21, $K = \mathrm{F}_K S(d)$ para algum $d \in K$. Seja $\{d_1, \ldots, d_m\}$ a S-órbita de d. Obviamente, $m \leqslant |S|$. Façamos $f := (x - d_1) \cdot \ldots \cdot (x - d_m)$. É fácil ver que $f \in \mathrm{F}_K S[x]$. Logo, $\dim_{\mathrm{F}_K S} K = \dim_{\mathrm{F}_K S} \mathrm{F}_K S(d) \leqslant m \leqslant |S|$. Por outro lado, $S \subset \mathrm{G}_K \mathrm{F}_K S$ implica $|S| \leqslant |\mathrm{G}_K \mathrm{F}_K S| = \dim_{\mathrm{F}_K S} K$. Portanto, $S = \mathrm{G}_K \mathrm{F}_K S$.

É fácil verificar que $\mathrm{G}_K(\sigma F) = \sigma(\mathrm{G}_K F)\sigma^{-1}$ para todos $\sigma \in \mathrm{G}_K k$ e $F \in \mathtt{subfields}_k K$. Se a extensão $k \subset F$ é normal, então $\sigma F = F$ pela Proposição 19.3, implicando $\mathrm{G}_K F \lhd \mathrm{G}_K k$.

Se $S \lhd \mathrm{G}_K k$, então $\sigma\,\mathrm{F}_K S = \mathrm{F}_K S$ para todo $\sigma \in \mathrm{G}_K k$, pois $\mathrm{G}_K(\sigma\,\mathrm{F}_K S) = \sigma(\mathrm{G}_K \mathrm{F}_K S)\sigma^{-1} = \sigma S \sigma^{-1} = S$. Pela Proposição 19.3, levando em conta que a extensão $k \subset K$ é normal, concluímos que a extensão $k \subset \mathrm{F}_K S$ é normal. Finalmente, a função dada pela regra $h : \sigma \mapsto \sigma|_F$, onde a extensão $k \subset F$ é normal, define um homomorfismo $h : \mathrm{G}_K k \to \mathrm{G}_K F$. É claro que $S := \mathrm{G}_K F$ é o núcleo de h. A imagem $G := h\,\mathrm{G}_K k$, isomorfa a $\mathrm{G}_K k/S$, satisfaz $\mathrm{F}\,G := \{f \in F \mid Gf = f\} = k$, pois $\mathrm{F}_K \mathrm{G}_K k = k$. Resta aplicar o seguinte

22. Lema. *Seja F um corpo, seja $\operatorname{Aut} F \geqslant G$ um grupo finito de automorfismos de F e seja $k := \{f \in F \mid Gf = f\}$. Então $k \subset F$ é uma extensão de Galois e $\dim_k F = |G|$.*

Demonstração. Denotamos $n := |G|$. Seja $a \in F$ e seja $\{a_1, \ldots, a_m\}$, $m \leqslant n$, a G-órbita de a. O polinômio $f := (x - a_1) \cdot \ldots \cdot (x - a_m) \in k[x]$ não tem raízes múltiplas e $f(a) = 0$. Logo, a é separável sobre k e todas as raízes do polinômio minimal de a sobre k pertencem a F. Pelas Proposições 19 e 20, a extensão $k \subset F$ é de Galois. Claramente, $G \leqslant \mathrm{G}_F k$. Além disso, $\dim_k k(a) \leqslant n$ para todo $a \in K$. Resta aplicar a igualdade $|\mathrm{G}_F k| = \dim_k F$ e o seguinte

Exercício. Mostre a seguinte afirmação.

23. Seja $k \subset F$ uma extensão separável de corpos tal que $\dim_k k(a) \leqslant n$ para todo $a \in F$. Então $F = k(a)$ para algum $a \in F$. (Dica: considere $a \in F$ com a dimensão $\dim_k k(a)$ máxima e aplique o Teorema 21.)

24. Lema. *Sejam $k \subset F$ uma extensão finita de Galois e $E \subset K$ uma extensão algébrica de corpos. Suponhamos que o corpo K é gerado por F, E e que $F \cap E = k$. Então $E \subset K$ é uma extensão finita de Galois e a regra $h : \sigma \mapsto \sigma|_F$ identifica os grupos $\mathrm{G}_K E$ e $\mathrm{G}_F k$.*

Demonstração. Se um subconjunto $A \subset F$ gera o corpo F sobre k, então A gera o corpo K sobre E. O polinômio minimal de $a \in A$ sobre k é divisível em $E[x]$ pelo polinômio minimal de a sobre E. Logo,

a extensão $E \subset K$ é normal e separável. Pela Proposição 19, h é um homomorfismo. Já que K é gerado por A sobre E, este h é injetivo. Para a imagem $S := h\,\mathrm{G}_K\,E \leqslant \mathrm{G}_F\,k$, temos $k \subset \mathrm{F}_F\,S \subset F \cap E = k$ ■

Seja G um grupo e seja K um corpo. Um *caracter* de G em K é simplesmente um homomorfismo de grupos $\chi : G \to K^*$. Podemos interpretar caracteres como funções de G para K.

25. Lema. *Seja G um grupo, seja K um corpo e sejam $\chi_1, \ldots, \chi_n$ caracteres distintos por pares. Então $\chi_1, \ldots, \chi_n$ são K-linearmente independentes.*

Demonstração. Suponhamos que $c_1\chi_1 + \cdots + c_n\chi_n = 0$ para $c_1, \ldots, c_n \in K$ nem todos nulos e tomemos n o mínimo possível. Então todos os c_i's são não-nulos, $n \geqslant 2$ e a indicada dependência linear é essencialmente única. Sendo os χ_i's caracteres, temos $c_1(\chi_1 g_0)\chi_1 + \cdots + c_n(\chi_n g_0)\chi_n = 0$ para qualquer $g_0 \in G$. Portanto, $\chi_k g_0/\chi_1 g_0 = 1$ para todos $k > 1$ e $g_0 \in G$. Uma contradição ■

Seja $k \subset K$ uma extensão finita de Galois. Definimos a *norma* $N_k^K : K \to k$ pela fórmula $N_k^K a := \prod_{\sigma \in \mathrm{G}_K\,k} \sigma a$ (é fácil ver que o produto está em k). Obviamente, temos $N_k^K(a_1 \cdot a_2) = N_k^K a_1 \cdot N_k^K a_2$ para todos $a_1, a_2 \in K$.

26. Lema (teorema 90 de Hilbert)**.** *Seja $k \subset K$ uma extensão finita de Galois tal que o grupo $\mathrm{G}_K\,k$ é cíclico gerado por σ. Seja $b \in K$. Então $N_k^K b = 1$ se e só se existe um $a \in K^*$ tal que $b = a/\sigma a$.*

Demonstração. Denotamos $n := |\sigma| = n$. Seja $N_k^K b = 1$. Considerando $1, \sigma, \ldots, \sigma^{n-1}$ como caracteres de K^* em K, obtemos $a := \big(1 + b\sigma + b(\sigma b)\sigma^2 + \cdots + b(\sigma b)\ldots(\sigma^{n-2}b)\sigma^{n-1}\big)c \neq 0$ para algum $c \in K^*$ pelo Lema 25. Uma verificação imediata mostra que $b(\sigma a) = a$, pois $b(\sigma b)\ldots(\sigma^{n-1}b) = 1$ ■

27. Lema. *Seja k um corpo de característica 0 que contém todas as raízes n-ésimas da unidade. Se $k \subset K$ é uma extensão de Galois cujo grupo $\mathrm{G}_K\,k$ é cíclico e $\dim_k K = n$, então $K = k(a)$, onde $0 \neq a^n \in k$. Reciprocamente, se $0 \neq a^n \in k$, então a extensão $k \subset k(a)$ é de Galois, o grupo $\mathrm{G}_{k(a)}\,k$ é cíclico e $\dim_k k(a)$ divide n.*

Demonstração. Denotamos por σ um gerador do grupo $\mathrm{G}_K\,k$. Pela hipótese, existe uma raiz n-ésima da unidade $b^{-1} \in k$, $|b| = n$. Logo, $N_k^K b^{-1} = (b^{-1})^n = 1$. Pelo Lema 26, existe $a \in K^*$ tal que $\sigma a = ab$. Daí, $\sigma^i a = ab^i$. Portanto, a extensão $k \subset k(a)$ possui pelo menos n automorfismos. Isto implica $K = k(a)$. De $\sigma a^n = (ab)^n = a^n$ segue $a^n \in k$.

Reciprocamente, toda raiz do polonômio $x^n - a^n \in k[x]$ tem a forma ab^i. Portanto, $k \subset k(a)$ é uma extensão de Galois. Seja $\sigma \in \mathrm{G}_{k(a)}\,k$. Então $\sigma a = ab^{m_\sigma}$. Agora, é fácil ver que a função $h : \sigma \mapsto \beta^{m_\sigma}$ é um homomorfismo injetivo para o grupo de raízes n-ésimas da unidade ■

Um grupo finito G é dito *solúvel* se existem subgrupos $G = N_0 \triangleright N_1 \triangleright N_2 \triangleright \cdots \triangleright N_m = 1$ tais que os grupos N_i/N_{i+1} são cíclicos. Uma extensão finita de corpos $k \subset F$ é dita *solúvel* se existe uma extensão finita $F \subset K$ tal que $k \subset K$ é uma extensão de Galois e cujo grupo $\mathrm{G}_K\,k$ é solúvel. Uma extensão finita de corpos $k \subset F$ é dita *radical* se existe uma extensão finita $F \subset K$ tal que $K = k(a_1, \ldots, a_m)$ e $a_i^{n_i} \in k(a_1, \ldots, a_{i-1})$ para todo $i = 1, 2 \ldots, m$.

28. Teorema. *Seja k um corpo de característica 0. Então uma extensão finita de corpos $k \subset K$ é solúvel se e só se é radical.*

Demonstração. Seja $k \subset K$ uma extensão solúvel. Podemos supor que ela é de Galois. Pelo Teorema 22, temos uma cadeia $k = K_0 \subset K_1 \subset \cdots \subset K_m = K$ tal que as extensões $K_i \subset K_{i+1}$ são cíclicas (isto é, de Galois com os grupos $\mathrm{G}_{K_{i+1}}\,K_i$ cíclicos). Denotamos $n_i := \dim_{K_i} K_{i+1}$ e $n := \mathrm{mmc}(n_0, n_1, \ldots, n_{m-1})$. Seja a uma raiz n-ésima primitiva da unidade, $|a| = n$, e seja $F := k(a)$. O corpo F contém todas as raízes n-ésimas da unidade.

Denotamos por F_i o corpo gerado por K_i e F. Pelo Teorema 22, a extensão $F_i \cap K_{i+1} \subset K_{i+1}$ é de Galois e o grupo $\mathrm{G}_{K_{i+1}}(F_i \cap K_{i+1}) \leqslant \mathrm{G}_{K_{i+1}}\,K_i$ é um grupo cíclico cuja ordem divide n. Pelo Lema 24,

$F_i \subset F_{i+1}$ é uma extensão de Galois cujo grupo $\mathrm{G}_{F_{i+1}} F_i$ é isomorfo a $\mathrm{G}_{K_{i+1}} K_i$. Portanto, a extensão $F_i \subset F_{i+1}$ é cíclica e $\dim_{K_i} K_{i+1}$ divide n para todo i. Pelo Lema 27, $F_{i+1} = F_i(a_i)$, onde $a_i^{m_i} \in F_i$. Além disso, $F = F_0 = k(a)$ e $a^n \in k$.

Seja $k \subset K$ uma extensão radical. Podemos supor que $K = k(a_1, \ldots, a_m)$ e $a_i^{n_i} \in k(a_1, \ldots, a_{i-1})$ para todo $i = 1, 2 \ldots, m$. Façamos $n := \mathrm{mmc}(n_0, n_1, \ldots, n_{m-1})$ e $K_i = k(a, a_1, \ldots, a_i)$, onde a é uma raiz n-ésima primitiva da unidade, $|a| = n$. (Assim, K_0 contém todas as raízes n-ésimas da unidade.) Então $K_i = K_{i-1}(a_i)$ e $a_i^n \in K_{i-1}$ para todo $i = 1, 2, \ldots, m$. Pelo Lema 27, a extensão $K_{i-1} \subset K_i$ é cíclica. Por outro lado, a extensão $k \subset K_0 = k(a)$ é de Galois e o grupo $\mathrm{G}_{K_0} k$ é abeliano, pois qualquer homomorfismo $\sigma : K_0 \to \overline{k}$, idêntico sobre k, é dado pela imagem de a e esta imagem é necessariamente da forma a^j com $\mathrm{mdc}(j, n) = 1 \ldots$ ∎

Exercícios. Mostre as seguintes afirmações assumindo que todos os corpos têm característica 0.

29. Seja G um grupo solúvel. Então qualquer subgrupo de G e qualquer quociente de G são solúveis.

30. O grupo A_5 não possui subgrupos normais próprios.

31. Seja $k \subset K$ uma extensão finita de Galois. A extensão $k \subset K$ é solúvel se e só se o grupo $\mathrm{G}_K k$ é solúvel.

32. Seja $K := k(t_1, \ldots, t_n)$ o corpo de frações da k-álgebra dos polinômios $k[t_1, \ldots, t_n]$ em n variáveis $t_1, \ldots, t_n$ sobre k, onde k é um corpo. Façamos $F := k(s_1, \ldots, s_n)$, onde $s_i := s_{i,n}(t_1, \ldots, t_n)$ são polinômios simétricos tais que $f := (x - t_1) \cdot \ldots \cdot (x - t_n) = x^n - s_{1,n}x^{n-1} + \cdots + (-1)^n s_{n,n}$. Então $F \subset K$ é uma extensão de Galois e $\mathrm{G}_K F \simeq \Sigma_n$. (Dica: Note que K é um corpo de decomposição do polinômio $f \in F[x]$. Pelos Exercícios 10 e 11, $\dim_F K \leqslant n!$. Por outro lado, o grupo Σ_n age sobre K e $\mathrm{F}_K \Sigma_n = \{a \in K \mid \Sigma_n a = a\} \supset F$. Pelo Lema 22, $\mathrm{F}_K \Sigma_n \subset K$ é uma extensão de Galois e $\dim_{\mathrm{F}_K \Sigma_n} K = |\Sigma_n| = n!$.)

33. Existem $a_1, a_2, a_3, a_4, a_5 \in \mathbb{C}$ tais que as raízes do polinômio $x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ não podem ser expressas em a_1, a_2, a_3, a_4, a_5 utilizando as operações $+$, $-$, $\cdot$, $/$ e $\sqrt[n]{}$.