Álgebra

Enno Nagel

Sumário

Introdução

Este manuscrito apresenta um caleidoscópio de teoremas principais da álgebra com as suas demonstrações auto-contidas.

1. Anéis e Módulos

Um anel A é um grupo *aditivo*, um grupo abeliano para uma operação +, e um monóide multiplicativo para uma operação · tal que a *lei distributiva* é satisfeita, isto é,

$$(a+b)c = ac + bc \quad \text{para todo } a,b \text{ e } c \text{ em A.}$$

Supomos em seguida que o monóide multiplicativo é *abeliano* e que contém um elemento neutro 1.

Um *homomorfismo* $f\colon \mathrm{A} \to \mathrm{B}$ entre dois anéis é uma aplicação que satisfaz $f(a+b) = f(a) + f(b)$ e $f(ab) = f(a)f(b)$. Ele é

- um *endomorfismo* se B = A,
- um *monomorfismo* se é injetor,
- um *epimorfismo* se é sobrejetor, e
- um *epimorfismo* se é um monomorfismo e epimorfismo, e
- um *automorfismo* se é um endomorfismo e isomorfismo.

Um *subanel* B em um anel A é um anel em A, isto é, um subgrupo aditivo de A tal que $b\mathrm{B} \subseteq \mathrm{B}$ para todo b em B. Por exemplo, a imagem de $\mathbb{Z}$ em A é um subanel.

Um *ideal* I em A é um subgrupo aditivo de A tal que $a\mathrm{I} \subseteq \mathrm{I}$ para todo a em A. Por exemplo, 0, A e $(x) = \mathrm{A}x$ para todo x em A, o ideal *gerado* por x, são ideais.

Se I e J são ideais, então o ideal gerado por eles é

$$\mathrm{I} + \mathrm{J} = \{i + j : i \in \mathrm{I}, j \in \mathrm{J}\}$$

e o seu produto é

$$\mathrm{IJ} = \{i_1 j_1 + \cdots + i_n j_n : i_1, \ldots, i_n \in \mathrm{I}, j_1, \ldots, j_n \in \mathrm{J}\}.$$

Temos $\mathrm{IJ} \subseteq \mathrm{I} \cap \mathrm{J}$.

O homomorfismo quociente $\pi\colon \mathrm{A} \to \mathrm{A/I}$ é definido como o (único) homomorfismo tal que qualquer homomorfismo $\mathrm{A} \to \mathrm{B}$ que anula I fatore como $\mathrm{A} \to \mathrm{A/I} \to \mathrm{B}$. Explicitamente, $\mathrm{A/I} = \{a + \mathrm{I} : a \in \mathrm{A}\}$ e $\pi(a) = a + \mathrm{I}$.

O núcleo $\ker f = \{a \in \mathrm{A} : f(a) = 0\}$ de um homomorfismo f é um ideal. Vice-versa, todo ideal I é o núcleo da aplicação $\mathrm{A} \to \mathrm{A/I}$.

Ideais Máximos

Lema 1.1. *Dado um ideal* I *em um anel* A*, existe um ideal máximo que contém* I.

Demonstração: Pelo Lema de Zorn, basta ver que toda cadeia $\{I_i\}$ de ideais ordenada pela inclusão $\subseteq$ tem a cota superior (= ideal que contém todo ideal da cadeia) $I = \bigcup I_i$. □

Um ideal é *máximo* se o único ideal distinto que o contém é A. Por exemplo, um elemento a em A é contido em um ideal máximo se, e tão-somente se, a não é uma unidade.

O *ideal de Jácobson* é definido por

$$J = \bigcap \{ \text{ ideais máximos } \}.$$

Um elemento a em A é uma *unidade* se existe b, denotado por a^{-1}, tal que $ab = 1$. Denote A^* o grupo multiplicativo das *unidades de* A. Se $A^* = A - \{0\}$ é máximo, A é chamado de *corpo.*

Se $S \subseteq A$ é multiplicativamente fechado e sem divisores de zero, então a *localização* de A por S é

$$S^{-1}A = \{(s,a) : s \in S, A \in A\}/\sim$$

onde $(s',a') \sim (s'',a'')$ se existe t em S tal que $s'' = ts'$ e $a'' = ta'$ é um anel cujas classes de equivalência são denotadas por s/t. Se P é um ideal *primo*, isto é, $xy \in P$ implica ou x, ou y em P, então o seu completamento $A - P$ é multiplicativamente fechado. Denote A_P a localização de A por $A - P$.

Lema 1.2. *Tem-se*

$$J = \{x \in A | \textit{ para todo } y \in A \textit{ vale } 1 - xy \in A^*\}.$$

Demonstração: Mostramos $J \supseteq$ o lado direito por contraposição: Seja x em A. Seja M um ideal máximo tal que $x \notin M$. Logo, existe y em A e m em M tal que $yx + m = 1$, isto é, $1 - yx$ em M; em particular, $1 - yx \notin A^*$.

Mostremos $J \subseteq$ o lado direito por contraposição: Seja x em A. Se existe y em A tal que $1 - xy \notin A^*$, então seja M um ideal máximo que contém $1 - xy$. Se M contivesse x, então conteria $xy + 1 - xy = 1$, então M conteria 1, uma contradição. Logo, $M \not\ni x$. □

Domínios euclidianos, principais e de fatoração única

Seja A um anel.

Definição 1.3. Seja A um anel. Para dois elementos a e b,

- um *maior divisor comum* $d = \mathrm{mdc}(a,b)$ é um divisor de a e b, tal que, se e é outro divisor de a e b, então d divide e.
- um *menor múltiplo comum* $m = \mathrm{mmc}(a,b)$ é um múltiplo de a e b, tal que, se n é outro múltiplo de a e b, então n é múltiplo de m.

Um elemento a em A é um *divisor de zero* se existe b em A não-nulo tal que $ab = 0$. A é um *domínio íntegro* se não tem divisores de zero.

Dois elementos a e b em A são *associados* se existe ϵ em A^* tal que $b = \epsilon a$.

Observação 1.4. Seja A um anel. Se A é um domínio íntegro, então o maior divisor comum e o menor múltiplo comum de dois a e b em A é univocamente determinado exceto associação, isto é,

- dois maiores divisores d' e d'' comuns são associados, e
- dois menores múltiplos m' e m'' comuns são associados.

Demonstração: Se d' e d'' são dois maiores divisores, então, por definição, $d'|d''$ e $d''|d'$, isto é, existem u e v em A tal que $d' = uvd'$ e $d'' = uvd''$. Como A não tem divisores de zero, ou d' e d'' são nulos, ou $uv = 1$; em ambos os casos, d' e d'' são associados.

Da mesma maneira para dois menores múltiplos comuns. □

Exemplo 1.5.

- Se $\mathrm{A} = \mathbb{Z}$, então $\mathbb{A}^* = \{\pm 1\}$. Logo o maior divisor comum e o menor múltiplo comum é determinado afora o seu sinal. Por convenção usa-se o número positivo.
- Se $\mathrm{A} = \mathbf{K}[\mathrm{X}]$ para um corpo $\mathbf{K}$, então $\mathbb{A}^* = \{\mathbf{K}\}$. Logo o maior divisor comum e o menor múltiplo comum é univocamente determinado afora um múltiplo escalar. Por convenção usa-se o cujo coeficiente *dominante*, o coeficiente da maior potência de X, é igual a 1.

Um elemento a em A é *irredutível* se, para todo b em A, se b divide a, então a e b são associados.

Definição. A é um domínio de *fatoração única* se

- é um domínio íntegro, e
- todo a em A é produto de elementos irredutíveis, univocamente determinado exceto a ordem e associação dos fatores.

Um elemento a em A é *primo* se, para todo b e c em A, se a divide bc, então a divide ou b ou c.

Exemplo 1.6. São domínios de fatoração única:

(i) O anel $\mathbb{Z}$ com $v = |\cdot|$.

(ii) O anel polinomial A[X] para um domínio de fatoração única A.

(iii) O anel polinomial $\mathbb{Z}[X]$ é um domínio de fatoração única, mas não é um domínio principal porque o ideal $\langle 2, X\rangle$ não é gerado por um único elemento! (Veja abaixo para a definição de um domínio principal.)

Proposição 1.7. *Se* A *é um domínio de fatoração única, então todo elemento irredutível é primo.*

Demonstração: Seja p irredutível e a, b em A tais que $p|ab$, isto é, existe c em A tal que $pc = ab$. Escreve

$$pc_1 \cdots c_\gamma = a_1 \cdots a_\alpha \cdot b_1 \cdots b_\beta.$$

Pela unicidade da fatoração, em particular p é associado a um dos fatores irredutíveis do lado direto; em particular p divide ou a ou b. □

Define a relação de equivalência $a \sim b$ por a é associado a b. Um anel é um domínio de fatoração única se, e tão-somente se, para todo elemento a em A existem expoentes univocamente determinados $e(f)$, um para cada classe de equivalência de elemento irredutível f e quase todos nulos, tais que

$$a \sim \prod f^{e(f)}.$$

Proposição 1.8. *Se* A *é um domínio de fatoração única, então, para todo par de elementos a e b, existe um maior divisor comum e um menor múltiplo comum deles.*

Demonstração: Se

$$a \sim \prod f^{e_a(f)} \quad \text{e} \quad b \sim \prod f^{e_b(f)}$$

então

$$\mathrm{mdc}(a,b) \sim \prod f^{\min\{e_f(a),e_f(b)\}} \quad \text{e} \quad \mathrm{mmc}(a,b) \sim \prod f^{\max\{e_f(a),e_f(b)\}}.$$

□

Um anel é um *domínio principal* se

- é um domínio íntegro, e
- todo ideal é gerado por um único elemento.

Exemplo 1.9. São domínios principais:

(i) O anel $\mathbb{Z}$ com $v = |\cdot|$.

(ii) O anel polinomial $k[\mathrm{X}]$ para um corpo k.

(iii) O anel $\mathbb{Z}[w]$ para $w = \frac{1+\sqrt[2]{-d}}{2}$ para $d = 19{,}43{,}67$ ou 163 é um domínio principal, mas não é euclidiano! (Veja abaixo para a definição de um domínio euclidiano.)

Lema 1.10. *Se* A *é um domínio principal, então* A *é um domínio de fatoração única.*

Demonstração: Existência da fatoração: Se a em A, então ou a é irredutível, ou $a = a_1 a_2$ tais que $\langle a\rangle \subset \langle a_1\rangle$ e $\langle a\rangle \subset \langle a_2\rangle$. Semelhantemente, ou a_1 é irredutível, ou $a_1 = a_{1,1}a_{1,2}$ e, ou a_2 é irredutível, ou $a_2 = a_{2,1}a_{2,2}$. Como A é um domínio principal, em particular, todo ideal é finitamente gerado, esta iterada divisão termina após um número finito de passos. (Se existisse uma cadeia infinita de inclusões próprias $\mathrm{I}_1 \subset \mathrm{I}_2 \subset \ldots$, então o ideal $\mathrm{I} = \mathrm{I}_1 \cup \mathrm{I}_2 \cup \ldots$ não seria finitamente gerado.)

Unicidade da fatoração: Precisamos de demonstrar primeiro que todo elemento irredutível é primo: Seja a em A. Mostremos que se $\mathrm{I} = \langle a\rangle$ não é máximo, então a é redutível: Como I não é máximo, existe $\mathrm{A} \supset \mathrm{J} = \langle b\rangle \supset \mathrm{I}$, isto é, $a = bc$ onde nem b, nem c são unidades; isto é, a é redutível. Em particular, se I é irredutível, então é primo (como I é máximo se, e tão-somente se, o quociente A/I é um corpo e I é primo se, e tão-somente se, o quociente A/I é um domínio íntegro).

Seja $a = a_1 \cdots a_m$ e $b = b_1 \cdots b_n$ uma decomposição em elementos irredutíveis. Como todo fator do lado esquerdo é primo e todo fator do lado direito é irredutível, ele é associado a um dos fatores do lado direito, e vice-versa, como todo fator do lado direito é primo e todo fator do lado esquerdo é irredutível, ele é associado a um dos fatores do lado esquerdo. Logo, $m = n$ e $b_1 \sim a_1, \ldots, b_n \sim a_n$. □

Um anel A é um *domínio euclidiano* se existe uma *função de grau* $v\colon \mathrm{A} \to \mathbb{N} \cup \{-\infty\}$ tal que $v(0) = -\infty$ e para todo a e b não-nulo com $v(b) \leq v(a)$ existem q e r tais que

$$a = bq + r \quad \text{com } v(r) < v(b).$$

Exemplo 1.11.

(i) O anel $\mathbb{Z}$ com $v = |\cdot|$.

(ii) O anel $\mathbb{Z}[i]$ com $v = |\cdot|$.

(iii) O anel polinomial $k[\mathrm{X}]$ para um corpo k.

Lema 1.12. *Se* A *é um domínio euclidiano, então* A *é um domínio principal.*

Demonstração: Seja I um ideal em A e i_0 em I um elemento não-nulo em I de grau mínimo. Para todo $a = i$ em I e $b = i_0$ existem q e r tais que

$$a = qb + r \quad \text{com } v(r) < v(b).$$

Em particular, r em I. Como $v(r) < v(b)$ e $v(b) = v(i_0)$ é mínimo, $r = 0$. Isto é, $\mathrm{I} = \langle i_0 \rangle$. □

Proposição 1.13 (Lema de Bézout). *Seja* A *um anel. Se* A *é um domínio principal, então*

$$\langle a \rangle + \langle b \rangle = \langle \mathrm{mdc}(a,b) \rangle \quad e \quad \langle a \rangle \cap \langle b \rangle = \langle \mathrm{mmc}(a,b) \rangle$$

Demonstração: Quanto à primeira igualdade para o maior divisor comum, como A é principal, existe m tal que

$$\langle m \rangle = \langle a \rangle + \langle b \rangle \subseteq \langle \mathrm{mdc}(a,b) \rangle.$$

Como $m = \lambda a + \mu b$ para alguns λ e μ em A, obtemos que todo divisor de a e b divide m. Logo $\langle \mathrm{mdc}(a,b) \rangle \supseteq \langle m \rangle$. Isto é, $\langle \mathrm{mdc}(a,b) \rangle = \rangle \langle m \rangle = \langle a \rangle + \langle b \rangle$.

Quanto à segunda igualdade para o menor múltiplo comum, como A é principal, existe m tal que

$$\langle m\rangle = \langle a\rangle \cap \langle b\rangle \subseteq \langle \mathrm{mmc}(a,b)\rangle.$$

Como $m = \lambda a$ e $m = \mu b$ para alguns λ e μ em A, obtemos que todo múltiplo de a e b é múltiplo de m. Logo $\langle \mathrm{mmc}(a,b)\rangle \subseteq \langle m\rangle$. Isto é, $\langle \mathrm{mmc}(a,b)\rangle = \rangle\langle m\rangle = \langle a\rangle \cap \langle b\rangle$. □

Localização de Ideais Primos

Se $S \subseteq A$ é multiplicativamente fechado e sem divisores de zero, então a *localização* de A por S é

$$S^{-1}A = \{(s,a) : s \in S, A \in A\}/\sim$$

onde $(s',a') \sim (s'',a'')$ se existe t em S tal que $s'' = ts'$ e $a'' = ta'$ é um anel cujas classes de equivalência são denotadas por s/t. Se P é um ideal *primo*, isto é, $xy \in P$ implica ou x, ou y em P, então o seu completamento $A - P$ é multiplicativamente fechado. Denote A_P a localização de A por $A - P$.

Lema 1.14. *A localização*

$$\{\textit{ideais de } A\} \twoheadrightarrow \{\textit{ideais de } S^{-1}A\}$$

é sobrejetora. Mais exatamente, $J \mapsto J \cap A$ *é uma retração, isto é,* $S^{-1}(A \cap J) = J$.

Demonstração: Seja J em $S^{-1}A$. Mostremos que $J = S^{-1}I$ com $I = J \cap A$.
Como J é um ideal, $J \supseteq S^{-1}I$.
Para $J \subseteq S^{-1}I$, seja x/s em J. Logo x em I, isto é, x/s em S^{-1}. □

Para um anel A denote,

$$\mathrm{Spec}\, A := \{ \text{ todos os ideais primos em A}\}.$$

Se $A \twoheadrightarrow B$ com núcleo I, então a aplicação induzida $\mathrm{Spec}\, B \to \mathrm{Spec}\, A$ é injetora e os q em Spec B correspondem aos p em Spec A que contêm o núcleo I. Se $A \hookrightarrow B$ a situação é mais complicada.

Proposição 1.15. *Seja* A *um anel comutativo e* S *um subconjunto sem divisor de* 0. *A localização*

$$\{p \in \mathrm{Spec}\, A : p \cap S = \emptyset\} \leftrightarrow \mathrm{Spec}\, S^{-1}A$$

é bijetora.

Mais exatamente, as aplicações $q \mapsto q \cap A$ *e* $p \mapsto S^{-1}p$ *são mutuamente inversas.*

Demonstração: Mostremos primeiro que são bem definidas: se q é um ideal primo em $B := S^{-1}A$, então $q \cap A$ é primo em A. Vice versa, se p é um ideal primo em A, então

$$S^{-1}A/S^{-1}p = S^{-1}A/p$$

não tem divisores de zero, isto é, $S^{-1}p$ é ou primo, ou 0. É zero se, e tão-somente se, $p \cap S \neq \emptyset$.

Demonstremos agora que $q \mapsto q \cap A$ e $p \mapsto S^{-1}p$ são inversos, isto é, que

$$p = S^{-1}p \cap A(*) \quad \text{e} \quad q = S^{-1}(q \cap A(**)$$

Quanto à $(*)$: Como p é um ideal, $p \subseteq S^{-1}p \cap A$. Para mostrar $p \supseteq S^{-1}p \cap A$, seja x em p e s em S tais que $s^{-1}x$ em A. Mostremos que $s^{-1}x$ em p. Como $s(s^{-1}x) = x$ em p e s não é em p, por p ser primo, necessariamente $s^{-1}x$ em p.

Quanto à $(**)$: Isto é demonstrado em Lema 1.14 para qualquer ideal, não necessariamente primo. □

Definição 1.16. A *dimensão de Krull* de um anel A é o maior comprimento de cadeias de ideais primos, onde

- uma *cadeia de ideais primos* são ideais primos p_0, p_1, …, p_n distintos e crescentes, isto é,
$$p_0 \subset p_1 \subset \ldots \subset p_n, \text{ e}$$
- o *comprimento* de uma tal cadeia é n.

Exemplo 1.17. A dimensão de Krull de $A[x_1, \ldots, x_n]$ é $\dim A + n$.

Proposição 1.18. *Sejam* A *e* B *anéis tais que* $B \supseteq A$. *Se* A *e* B *são domínios íntegros e se* B *é integral sobre* A, *então* B *é um corpo se, e tão-somente se,* A *é um corpo.*

Demonstração: Seja A um corpo. Seja y em B. Como B é integral sobre A, existe $y^n + a_{n-1}y^{n-1} + \cdots + a_0$ para a_{n-1}, …, a_0 em A com n mínimo entre todas tais equações. Como A é um domínio íntegro, $a_0 \neq 0$. Como A é um corpo, $y^{-1} = a_0^{-1}(y^{n-1} + a_{n-1}y^{n-1} + \cdots + a_1)$; isto é, B é um corpo.

Seja B um corpo. Seja x em A e seja $y = x^{-1}$ em B. Como B é integral sobre A, existe $y^n + a_{n-1}y^{n-1} + \cdots + a_0$ para a_{n-1}, …, a_0 em A com n mínimo entre todas tais equações. Logo multiplicação por x^n resulta em $y = x^{-1} = -(a_{n-1} + a_{n-2}x + \cdots + a_0x^{n-1})$ em A; isto é, A é um corpo. □

Nota que a pré-imagem de um ideal primo é um ideal primo. Contudo, a pré-imagem de um ideal máximo não necessariamente é um ideal máximo: por exemplo, a pré-imagem de 0 em $\mathbb{Q}$ sob a inclusão $\mathbb{Z} \hookrightarrow \mathbb{Q}$ não é máximo em $\mathbb{Z}$. Porém, se a imagem é integral, a pré-imagem de todo ideal máximo é um ideal máximo:

Corolário 1.19. *Sejam* A *e* B *anéis tais que* $B \supseteq A$. *Seja* J *um ideal em* B. *Se* B *é integral sobre* A *e* J *é primo, então* J *é máximo se, e tão-somente se,* $J \cap A$ *é máximo.*

Demonstração: Aplica Proposição 6.7 aos domínios íntegros B/J e $A/J \cap A$. □

Sejam A e B anéis com $A \to B$. Se $A \twoheadrightarrow B$, então

$$\operatorname{Spec} A \to \operatorname{Spec} B$$

é injetora. Se B é integral sobre A, então uma injetividade mais restrita vale:

Corolário 1.20. *Sejam* A *e* B *anéis com* $A \subseteq B$. *Se* B *é integral sobre* A *e* q' *e* q'' *ideais primos em* B *tal que* $q' \subseteq q''$ *e* $q' \cap A = q'' \cap A$, *então* $q' = q''$.

Demonstração: Se B é integral sobre A e $S \subseteq A$ multiplicativamente fechado, então $S^{-1}B$ é integral sobre $S^{-1}A$. Em particular, B_p é integral sobre A_p

Seja $q' \cap A = p = q'' \cap A$ primo. Seja $m(= (A - p)^{-1}p)$ o ideal máximo no anel local A_p.

Sejam $n' = (A - p)^{-1}q'$ e $n'' = (A - p)^{-1}q''$ as extensões de q' e q'' em B_p. As suas interseções m' e m'' em A_p são o ideal máximo m. Como B_p é integral sobre A_p, por Corolário 1.19 os ideais n' e n' são máximos em B_p. Logo, como B_p é local, $n' = n = n''$ é o único ideal máximo em B_p, logo $q' = n' \cap B = n \cap B = n'' \cap B = q''$. □

Se B é integral sobre A, então a aplicação induzida $\operatorname{Spec} B \to \operatorname{Spec} A$ é sobrejetora:

Teorema 1.21 (Going-Up). *Sejam* A *e* B *anéis tais que* $B \supseteq A$. *Se* B *é integral sobre* A, *então para todo ideal* p *primo existe um ideal* q *em* B *tal que* $p = q \cap A$.

Demonstração: Seja B_p a localização de B pelo conjunto multiplicativamente fechado $A - \mathfrak{p}$.

Seja n um ideal máximo de B_p. Por Corolário 1.19, $m = n \cap A_p$ é máximo. Como p é primo, A_p é local, logo $m \cap A = p$.

Seja $q = n \cap B$. Por n ser máximo, temos $q \cap (A - p) = \emptyset$; logo q é primo por Proposição 1.15. Temos

$$q \cap A = (n \cap B) \cap A = (n \cap A_p) \cap A = p \cap A = A.$$

Teorema 1.22 (Going-Up). *Sejam* A *e* B *anéis tais que* $B \supseteq A$. *Seja*

$$p_0 \subset p_1 \subset \ldots \subset p_n,$$

uma cadeia de ideais primos crescente em A *e*

$$q_0 \subset q_1 \subset \ldots \subset q_m$$

com $m < n$ *uma cadeia de ideais primos crescente em* B *com* $q_0 \cap A = p_0$, ..., $q_m \cap A = p_m$. *Se* B *é integral sobre* A, *então a cadeia em* B *pode ser estendida a uma cadeia*

$$q_0 \subset q_1 \subset \ldots \subset q_m \subset q_{m+1} \subset \ldots \subset q_n$$

com $q_{m+1} \cap A = p_{m+1}$, ..., $q_n \cap A = p_n$.

Demonstração: Aplica Teorema 1.21 a A/p_m e B/q_m, e itera. □

Corolário 1.23. *Sejam* A *e* B *anéis tais que* $B \supseteq A$. *Se* B *é integral sobre* A, *então a dimensão de Krull de* B *é igual à dimensão de Krull de* A.

Módulos

Seja A um anel. Um *módulo* sobre A é um grupo abeliano com uma operação linear de A sobre M, isto é, com um homomorfismo de anéis $A \to \mathrm{End}(M)$ (= o anel dos endomorfismos do grupo abeliano M), ou, equivalentemente, tal que

- $a(x+y) = ax + ay$, e
- $(a+b)x = ax + bx$

Exemplo 1.24.

- Para $A = \mathbb{Z}$, os módulos são os grupos abelianos.
- Para k um corpo, os módulos sobre k são espaços vetoriais.
- Os módulos sobre A contidos em A são os *ideais*.

Uma aplicação $f : M \to N$ entre dois módulos sobre A é um homomorfismo se ela é *linear*, isto é,

- *aditiva*, isto é, $f(m' + m'') = f(m') + f(m'')$ para m', m'' em M, e

- *multiplicativa* para escalares, isto é, $f(am) = af(m)$ para a em A e m em M.

Para um ideal I em A e um submódulo S, seja

$$\mathrm{IS} := \{i_1 s_1 + \cdots + i_n s_n : i_1, \ldots, i_n \in \mathrm{I}, s_1, \ldots, s_n \in \mathrm{S}\}$$

o módulo gerado por I e S.

Dado um submódulo S em um módulo M, o homomorfismo quociente $\pi\colon \mathrm{M} \to \mathrm{M/S}$ é definido como o (único) homomorfismo tal que qualquer homomorfismo $\mathrm{M} \to \mathrm{N}$ que anula S fatore como $\mathrm{M} \to \mathrm{M/S} \to \mathrm{N}$. Explicitamente, $\mathrm{M/S} = \{m + \mathrm{S} : m \in \mathrm{M}\}$ e $\pi(m) = m + \mathrm{S}$.

O *núcleo* de um homomorfismo $f\colon \mathrm{M} \to \mathrm{N}$ é dado por

$$\ker f := \{m \in \mathrm{M} : f(m) = 0\}.$$

A sua *imagem* por

$$\operatorname{im} f = f(\mathrm{M}) = \{n \in \mathrm{N} : \text{ existe } m \in \mathrm{M} \text{ com } f(m) = n\}.$$

O *co-núcleo* é definido por $\operatorname{coker} f = \mathrm{M}/\operatorname{im} f$.

Se $\mathrm{X} = \{x_i\}$ é um subconjunto de M, então

$$\langle \mathrm{X} \rangle := \{\sum_i a_i x_i : a_i \in \mathrm{A}, x_i \in \mathrm{X}\}$$

é o submódulo gerado por X em M. Um módulo M é finitamente gerado, se, e tão-somente se, existe um epimorfismo

$$\mathrm{A}^n \twoheadrightarrow \mathrm{M}$$

onde $\mathrm{A}^n = \mathrm{A} \oplus \cdots \oplus \mathrm{A} := \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in \mathrm{A}\}$ é a soma direta de n cópias de A.

Um módulo é *simples* se os seus únicos submódulos são ele mesmo e 0.

Lema 1.25. *O módulo* M *é simples se, e tão-somente se,* $\mathrm{M} = \mathrm{A/M}$ *para um ideal máximo* M *de* A.

Demonstração: Como é simples, é gerado por um único elemento, isto é, existe um epimorfismo $\pi\colon \mathrm{A} \twoheadrightarrow \mathrm{M}$. Os submódulos N correspondem por $\mathrm{N} \mapsto \pi^{-1}\mathrm{N}$ aos ideais em A. □

Teorema 1.26 (Lema de Nakayama). *Seja* M *um módulo e* J *o radical de Jácobson. Se* M *é finitamente gerado, então* $M/JM = 0$ *se, e tão-somente se,* $M = 0$.

Demonstração: Seja $JM = M$. Demonstremos por indução sobre n = o mínimo número de geradores de M que $M = 0$. Se $n = 1$, isto é, existe m em M tal que $M = Am$, então existe j em J tal que $jm = m$. Isto é, $(1 - j)m = 0$. Pela caracterização de J, $(1 - j) \in A^*$, logo $m = 0$. Seja $n > 1$ e $M = Am_1 + \cdots + Am_n$. Pela hipótese, $M = Jm_1 + \cdots + Jm_n$, em particular, existem $j_1, \ldots, j_n$ em J tais que, por exemplo,

$$m_1 = j_1 m_1 + j_2 m_2 + \cdots + j_n m_n.$$

Isto é,

$$(1 - j_1)m_1 = j_2 m_2 + \cdots + j_n m_n.$$

Por Lema 1.2 $(1 - j) \in A^*$, logo

$$m_1 = \tilde{j}_2 m_2 + \cdots + \tilde{j}_n m_n \quad \text{para } \tilde{j}_2, \ldots, \tilde{j}_n \in J.$$

Isto é, m_1 em $J\tilde{M}$ onde $\tilde{M} = Am_2 + \cdots + Am_n$ é um submódulo gerado por $n - 1$ elementos. Como $JM = M$, em particular, $J\tilde{M} = \tilde{M}$. Pela hipótese de indução, $\tilde{M} = 0$, logo $m_1 = 0$, logo $M = 0$. □

Corolário 1.27. *Seja* $\phi : M \to N$ *um homomorfismo entre módulos sobre* A. *Seja* I *um ideal em* A. *Se* I *é contido no radical de Jácobson, então* ϕ *é sobrejetor se, e tão-somente se,* $\bar{\phi} : \bar{M} \to \bar{N}$ *é sobrejetor onde* $\bar{\cdot}$ *denote o quociente por* I.

Demonstração: Aplica o Lema de Nakayama aos có-núcleo $\operatorname{coker}\phi$ e $\operatorname{coker}\bar{\phi}$ de ϕ e $\bar{\phi}$. □

Corolário 1.28. *Seja* M *um módulo sobre* A. *Seja* I *um ideal em* A. *Se* I *é contido no radical de Jácobson, então* $x_1, \ldots, x_n$ *geram* M *se, e tão-somente se,* $\bar{x}_1, \ldots, \bar{x}_n$ *geram* $\bar{M} = M/IM$.

Demonstração: Aplica Corolário 1.27 aos epimorfismos $A^r \to M$ e $\bar{A}^r \to \bar{M}$ para $\bar{A} = A/I$. □

2. Decomposição Primária

Seja A um anel (comutativo com 1 = o elemento multiplicativo neutro). Um elemento não-nulo a de A é um *divisor de zero* se existe b não-nulo tal que $ab = 0$. Por exemplo, se p e q em $\mathbb{Z} - \{0, \pm 1\}$, então $\mathbb{Z}/pq\mathbb{Z}$ tem os divisores de zero p e q.

Definição. Um ideal q é *primário* se para x, y em A tais que xy em q, mas x não em q, então existe um expoente n tal que y^n em q.

Equivalentemente, q é primário se, e tão-somente se, todo divisor de zero em A/q é nilpotente.

Recorde-se o *radical* de um ideal I definido por

$$r(I) := \{a \text{ em } A : \text{ existe } n \text{ tal que } a^n \in I\}.$$

Observação 2.1. Se $I = q$ é primário, então $p = r(q)$ é primo. Chamamos p o (ideal) primo *associado* a q e denotamos por p para um ideal primário p.

Definição. Uma *decomposição primária* de um ideal I em A é uma igualdade

$$I = q_1 \cap \ldots \cap q_n$$

para $q_1, \ldots, q_n$ ideais primários.

Um ideal é *decomponível*, se existe uma decomposição primária dele.

A decomposição primária $I = q_1 \cap \ldots \cap q_n$ é *mínima* se

- os radicais $r(q_1), \ldots, r(q_n)$ são distintos, e
- para nenhum $i = 1, \ldots, n$ temos $q_i \not\subseteq \bigcap_{j \neq i} q_j$.

Para um ideal I e x em A, seja

$$I : x = \{a \text{ em } A : ax \text{ em } I\}$$

Por I ser um ideal, se x em I, então $I : x = A$.

Teorema 2.2 (Primeira Unicidade). *Seja* $I = q_1 \cap \ldots \cap q_n$ *uma decomposição primária e sejam* $p_1 = r(q_1), \ldots, p_n = r(q_n)$ *os primos associados aos ideais na decomposição primária de* I. *Se é mínima, então*

$$\{p_1, \ldots, p_n\} = \{r(I : x) \text{ para todos os } x \text{ em } A\}.$$

Em particular, $p_1, \ldots, p_n$ *não dependem dos ideais primários* $q_1, \ldots, q_n$.

Demonstração: Temos

$$r(\mathrm{I}) = r(q_1 \cap \ldots \cap q_n) = r(q_1) \cap \ldots \cap r(q_n).$$

Se q é um ideal primário e $x \notin q$, então para todo a em A com ax em q existe n tal que a^n em q. Isto é, se $x \notin q$, então

$$\begin{aligned} r(q : x) =& \{a \in \mathrm{A} : \text{ existe } n \text{ tal que } a^n x \text{ em } q\} \\ =& \{a \in \mathrm{A} : \text{ existe } n \text{ tal que } a^n \text{ em } q\} = r(q). \end{aligned}$$

Caso contrário, se $x \in q$, então $q : x = \mathrm{A}$ (para qualquer ideal, não necessariamente primário); em particular, $r(q : x) = \mathrm{A}$.

Logo,

$$r(\mathrm{I} : x) = \bigcap_{q \notin x} r(q : x).$$

Em particular, para q_{i_0} em $\{q_1, \ldots, q_n\}$, seja x em $\bigcap_{i \neq i_0} q_i$. Logo,

$$r(\mathrm{I} : x) = r(q : x).$$

Recordemo-nos: Se $\mathrm{S} \subseteq \mathrm{A}$ é multiplicativamente fechado e sem divisores de zero, então a *localização* de A por S é

$$\mathrm{S}^{-1}\mathrm{A} = \{(s,a) : s \in \mathrm{S}, \mathrm{A} \in \mathrm{A}\}/\sim$$

onde $(s',a') \sim (s'',a'')$ se existe t em S tal que $s'' = ts'$ e $a'' = ta'$ é um anel cujas classes de equivalência são denotadas por s/t. Se P é um ideal *primo*, isto é, $xy \in \mathrm{P}$ implica ou x, ou y em P, então o seu completamento $\mathrm{A} - \mathrm{P}$ é multiplicativamente fechado. Denote A_P a localização de A por $\mathrm{A} - \mathrm{P}$.

Um conjunto Σ de ideais é *isolado* se para p em Σ e $q \subseteq p$ segue que q em Σ.

Teorema 2.3 (Segunda Unicidade). *Seja* $\mathrm{I} = q_1 \cap \ldots \cap q_n$ *uma decomposição primária e* $p_1 = r(q_1)$, *...*, $p_n = r(q_n)$. *Seja* Σ *um conjunto de ideais isolado. Põe* $\mathrm{Q} = \{q_1, \ldots, q_n\}$ *e* $\mathrm{P} = \{p_1, \ldots, p_n\}$ *Se* $\Sigma \subseteq \mathrm{P}$, *então*

$$\bigcap_{q \in \mathrm{Q} \text{ tal que } r(q) \in \Sigma} q$$

é independente de Q. *Em particular,*

$$\bigcap_{q \in \mathrm{Q} \text{ tal que } r(q) \text{ é mínimo}} q$$

é independente de Q.

Demonstração: Estipulemos:

(i) Seja $S \subseteq A$ multiplicativamente fechado e q primário com radical p.

  (a) Se $S \cap p \neq \emptyset$, então $S^{-1}q \cap A = A$.

  (b) Se $S \cap p = \emptyset$, então $S^{-1}q \cap A = q$.

(ii) Se $I = q_1 \cap \ldots \cap q_n$ tal que $q_1, \ldots, q_m \cap S = \emptyset$ e $q_{m+1}, \ldots, q_n \cap S \neq \emptyset$, então

$$S^{-1}I = S^{-1}q_1 \cap \ldots \cap S^{-1}q_m$$

e

$$S^{-1}I \cap A = q_1 \cap \ldots \cap q_m$$

Demonstremos:

(i)

  (a) Se $S \cap p \neq \emptyset$, então existe a em S e n tal que a^n em q; como S é multiplicativamente fechado, a^n em S. Logo 1 em $S^{-1}q$, isto é, $S^{-1}q = S^{-1}A$. Em particular $S^{-1}q \cap A = A$.

  (b) Se $S \cap p = \emptyset$, então, para a em A e s em S, as em q implica, por q ser primário, a em q; logo $S^{-1}q \cap A = q$.

(ii) Se $I = q_1 \cap \ldots \cap q_n$ tal que $q_1, \ldots, q_m \cap S = \emptyset$ e $q_{m+1}, \ldots, q_n \cap S \neq S$, então, pelo que acabamos de demonstrar,

$$\begin{aligned} S^{-1}I &= S^{-1}(q_1 \cap \ldots \cap q_n) \\ &= (S^{-1}q_1 \cap \ldots \cap S^{-1}q_m) \cap (S^{-1}q_{m+1} \cap \ldots \cap S^{-1}q_n) \\ &= S^{-1}q_1 \cap \ldots \cap S^{-1}q_m. \end{aligned}$$

Logo,

$$S^{-1}I \cap A = q_1 \cap \ldots \cap q_m.$$

Se pomos

$$S = A - \bigcup_{q \in Q \text{ tal que } r(q) \in \Sigma} r(q),$$

então

$$S^{-1}I \cap A = \bigcap_{q \in Q \text{ tal que } r(q) \in \Sigma} q.$$

Anéis Noetherianos

Seja Σ um conjunto *parcialmente ordenado*; isto é, tem uma relação $\leq$ que é

- *reflexiva*, isto é, $x \leq x$,
- *transitiva*, isto é, se $x \leq y$ e $y \leq z$, então $x \leq z$, e
- se $x \leq y$ e $y \geq x$ então $x = y$.

Denote $y \geq x$ que $x \leq y$.

Exemplo 2.4. Por exemplo, para um conjunto S, o conjunto ¶(S) dos subconjuntos de S com $\leq$ definida pela inclusão $\subseteq$ é um conjunto parcialmente ordenado.

Proposição 2.5. *Toda sequência crescente $x_1 \leq x_2 \leq \ldots$ em Σ é* estacionária*, isto é, existe n tal que $x_n = x_{n+1} = \cdots$, se, e tão-somente se, todo subconjunto não-vazio σ de Σ contém um elemento* máximo*, isto é, um elemento x para que não existe $y \geq x$ em σ diferente de x.*

Demonstração: Se existe um subconjunto σ sem elemento máximo, isto é, para todo x em σ existe y em σ com $y \geq x$, então, dada uma sequência finita $x_1 \leq \ldots x_n$, existe $y = x_{n+1} \geq x_n$ diferente de x; a sequência (x_n) assim construida não é estacionária.

Se todo subconjunto σ tem um elemento máximo, então em particular $\{x_n\}$ tem um elemento máximo x_N; necessariamente $x_N = x_{N+1} = \cdots$. □

Se Σ é o conjunto dos submódulos de um módulo, e $\leq$ é $\subseteq$ respectivamente $\supseteq$, então a condição em Proposição 5.2 é a *condição da cadeia crescente* e o módulo é *noetheriano* respectivamente *decrescente* e o módulo é *artiniano.*

Um anel A é *noetheriano* se é noetheriano como módulo sobre A (cujos submódulos são os ideais).

Um ideal I é *irredutível* se

$$\text{I} = \text{J} \cap \text{K} \text{ implica } \text{J} = \text{I} \text{ ou } \text{K} = \text{I}.$$

Lema 2.6. *Seja* A *um anel. Se é noetheriano, então todo ideal é a interseção finita de ideais irredutíveis.*

Demonstração: Caso contrário, então o conjunto dos ideais para que o lema não vale não é vazio, logo tem um máximo elemento I por A ser noetheriano. Em particular I é redutível, isto é, $\text{I} = \text{J} \cap \text{K}$ onde $\text{J} \supset \text{I}$ e $\text{K} \supset \text{I}$. Logo, J e K são interseções finitas de ideais irredutíveis; contradição! □

Lema 2.7. *Seja* A *um anel. Se é noetheriano, então todo ideal irredutível é primário.*

Demonstração: Pela passagem ao quociente do ideal irredutível em questão, basta mostrar que se 0 é irredutível, então é primário. Seja $xy = 0$ com $x \neq 0$, e considere a cadeia dos ideais anuladores

$$\operatorname{Ann} x \subseteq \operatorname{Ann} x^2 \subseteq \dots$$

Como A é noetheriano, existe n tal que $\operatorname{Ann} x^n = \operatorname{Ann} x^{n+1}$. Logo $(x^n) \cap (y) = 0$; pois se a em (y), então $ax = 0$, e se a em (x^n), isto é, $a = bx^n$, então $0 = ax = (bx^n)x = bx^{n+1}$. Como $\operatorname{Ann} x^{n+1} = \operatorname{Ann} x^n$, temos $bx^n = 0$, isto é, $a = 0$. Logo, como 0 é irredutível e $y \neq 0$, concluímos $x^n = 0$. □

Corolário 2.8. *Seja* A *um anel. Se* A *é noetheriano, então todo ideal tem uma decomposição primária.*

Anéis de Dimensão 1

Dois ideais I e J são *coprimos* (ou *relativamente primos*) se todo ideal que contêm I e J necessariamente contém 1, isto é, se $\mathrm{I} + \mathrm{J} = \mathrm{A}$.

Lema 2.9. *Seja* A *um anel e* $\mathrm{I}_1, \dots, \mathrm{I}_n$ *ideais em* A. *Se* $\mathrm{I}_1, \dots, \mathrm{I}_n$ *são coprimos, então*

$$\mathrm{I}_1 \cap \dots \cap \mathrm{I}_n = \mathrm{I}_1 \cdots \mathrm{I}_n.$$

Demonstração: Por indução sobre n, basta demonstrar que se $\mathrm{I} + \mathrm{J} = \mathrm{A}$, então

$$\mathrm{I} \cap \mathrm{J} \subseteq \mathrm{IJ}.$$

Seja a em $\mathrm{I} \cap \mathrm{J}$ e $1 = i + j$. Como ai e aj são em IJ, logo $a = ai + aj$ é em IJ. □

Seja A um anel. O ideal I em A tem uma *fatoração primária* se existem ideais primários $q_1, \dots, q_n$ tais que

$$\mathrm{I} = q_1 \cdots q_n.$$

Um anel sem divisores de zero tem *dimensão* 1 se, e tão-somente se, todo ideal primo diferente de 0 é máximo.

Proposição 2.10. *Seja* A *um anel. Se* A *é noetheriano, sem divisores de zero e de dimensão* 1, *então todo ideal* I *tem uma fatoração primária, isto é,*

$$\mathrm{I} = q_1 \cdots q_n \quad \textit{para } q_1, \dots, q_n \textit{ primários.}$$

Demonstração: Como A é noetheriano, I tem uma decomposição primária

$$\mathrm{I} = q_1 \cap \ldots \cap q_n \quad \text{para } q_1, \ldots, q_n \text{ primários}$$

e $p_1 = r(q_1), \ldots, p_n = r(q_n)$ os primos associados aos primários todos diferentes. Como A tem *dimensão* 1 e é sem divisores de zero se, e tão-somente se, todo ideal primo não-nulo é máximo, logo $p_1, \ldots, p_n$ são máximos. Por serem diferentes, são coprimos, isto é, $p' + p'' = \mathrm{A}$ para diferentes p' e p'' em $\{p_1, \ldots, p_n\}$. Como

$$r(q' + q'') = r(r(p') + r(p'')) = r(p' + p'') = r(1) = 1$$

e

$$r(\mathrm{I}) = 1 \quad \text{se, e tão-somente se, } \mathrm{I} = 1,$$

os $q_1, \ldots, q_n$ são coprimos. Por Lema 9.19,

$$q_1 \cap \ldots \cap q_n = q_1 \cdots q_n.$$

Se

$$\mathrm{I} = q_1 \cdots q_n.$$

é outra fatoração, então, pelo mesmo argumento,

$$\mathrm{I} = q_1 \cap \ldots \cap q_n.$$

Logo, todo ideal primo não-nulo é máximo, por Teorema 2.3, a fatoração é única. □

Anéis de Dedekind

Um anel A é um *domínio de Dedekind* se é

- sem divisores de zero,
- noetheriano, isto é, todo ideal é finitamente gerado,
- de dimensão 1, isto é, todo ideal primo é máximo, e
- integralmente fechado, isto é, se x em $\mathrm{Q} = \mathrm{Q}(\mathrm{A})$ e $\mathrm{P}(\mathrm{X})$ em $\mathrm{A}[\mathrm{X}]$ satisfazem $\mathrm{P}(x) = 0$, então x em A.

Teorema 2.11. *Seja* A *um anel Se é noetheriano, sem divisores de zero, de dimensão* 1 *e integralmente fechado, então todo ideal primário é uma potência de um ideal primo.*

Corolário 2.12. *Seja* A *um anel. Se* A *é Dedekind, então todo ideal é o produto único de ideais primos.*

Demonstração: Por Proposição 2.10 e Teorema 2.11. □

Lema 2.13. *Um elemento x em* B *é integral sobre* A *se, e tão-somente se,* $A[x]$ *é finitamente gerado sobre* A.

Lema 2.14. *Se* $A \subseteq B \subseteq C$ *são anéis tais que* B *é integral sobre* A *e* C *sobre* B, *então* B *é integral sobre* A.

Demonstração: x em C é integral sobre B se, e tão-somente se, existem b_{n-1}, $\ldots$, b_0 em B tais que $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$. O anel $B' = A[b_1, \ldots, b_n]$ é finitamente gerado sobre A e $B'[x]$ é finitamente gerado sobre B'. Logo $B'[x]$ é finitamente gerado sobre A. Por Lema 6.1, x é integral sobre A. □

Proposição 2.15. *Seja* A *integralmente fechado,* K *o seu corpo de frações,* L *uma extensão finita separável sobre* K *e* B *o fecho integral de* A *em* L. *Então existe uma base* $v_1, \ldots, v_n$ *de* L *sobre* K *tal que* $B \subseteq Av_1 + \cdots + Av_n$

Teorema 2.16. *O anel dos inteiros* A *de um corpo de números finito* K *é Dedekind.*

Demonstração: Domínio íntegro: Não tem divisores de zero.

Noetheriano: Como K é separável, existe uma base $v_1, \ldots, v_n$ de K sobre $\mathbb{Q}$ tal que $A \subseteq \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$. Logo, A é finitamente gerado, logo noetheriano.

Integralmente fechado: Seja x em K integral sobre A. Pela transitividade da integralidade, x é integral sobre $\mathbb{Z}$. Isto é, x em A

Todo ideal primo não-nulo é máximo: Como A é integral sobre $\mathbb{Z}$, por Corolário 1.20, $\mathfrak{p} \cap \mathbb{Z} = 0$ se, e tão-somente se, $\mathfrak{p} = 0$; logo, se $\mathfrak{p}$ é não-nulo, então $\mathfrak{p} \cap \mathbb{Z}$ é máximo em $\mathbb{Z}$. Por Corolário 1.19, o ideal $\mathfrak{p}$ é máximo. □

3. Módulos finitamente gerados

Um *domínio principal* é um domínio íntegro, isto é, sem divisores de zero, cujos ideais são todos *principais*, isto é, gerado por um único elemento.

Homologia Elementar

Definição 3.1. Um módulo P sobre um anel A é *projetivo*, se para todo homomorfismo $P \to M$ e todo epimorfismo $N \twoheadrightarrow M$ entre módulos sobre A, existe $P \to N$ que fatora $P \to M$.

Um módulo I sobre um anel A é *injetor*, se para todo homomorfismo $M \to I$ e todo monomorfismo $M \hookrightarrow N$ entre módulos sobre A, existe $N \to I$ que fatora $M \to I$.

Lema 3.2 (Baer's Criterion). *Um módulo* I *sobre um anel* A *é injetor se, e tão-somente se, para todo ideal* $\mathfrak{a}$ *em* A*, todo homomorfismo* $\mathfrak{a} \to I$ *pode ser estendido a um homomorfismo* $A \to I$.

Demonstração: Sejam dados um módulo N, um submódulo $M \hookrightarrow N$ e um homomorfismo $\alpha\colon M \to I$. Precisamos de demonstrar que existe uma extensão $N \to I$ de α. Seja P o conjunto de todas as extensões $\alpha\colon M' \to I$ para $M \subseteq M' \subseteq N$ ordenado por extensão entre homomorfismos. Pelo Lema de Zorn, existe uma extensão máxima $\alpha'\colon M' \to I$ em P. Precisamos de mostrar que $M' = N$:

Caso contrário, existe n em $N - M'$. O conjunto $\mathfrak{a} = \{a \in A : an \in M'\}$ é um ideal de A. Pela hipótese, o homomorfismo

$$\mathfrak{a} \to M' \to I$$

dado por $a \mapsto an \mapsto \alpha'(n)$ estende-se a um homomorfismo $f\colon A \to I$. Seja $M'' = M' + An$, e define $a''\colon M'' \to I$ por

$$\alpha''(a' + an) = \alpha'(a') + f(a) \qquad \text{para } a' \in M', a \in A.$$

É bem-definido porque $\alpha'(an) = f(a)$ para $an \in M' \cap An$, e estende α'; contradição a α' ser máximo! □

Lema 3.3. *Uma sequência exata da forma*

$$0 \to N \xrightarrow{i} M \xrightarrow{p} P \to 0$$

cinde*, se, equivalentemente,*

(i) *existe uma retração* $r\colon \mathrm{M} \to \mathrm{N}$*, isto é, tal que* $r \circ i = \mathrm{id}$.

(ii) *existe uma secão* $s\colon \mathrm{P} \to \mathrm{M}$*, isto é, tal que* $p \circ s = \mathrm{id}$.

(iii) $\mathrm{M} \simeq \mathrm{N} \oplus \mathrm{P}$.

Demonstração: (iii) $\implies$ (i): Define r como projeção de $\mathrm{M} = \mathrm{N} \times \mathrm{P}$ a N.

(iii) $\implies$ (ii): Define s como injeção de N em $\mathrm{M} = \mathrm{N} \oplus \mathrm{P}$.

(i) $\implies$ (iii): Define $\alpha\colon \mathrm{M} \to \mathrm{N} \oplus \mathrm{P}$ por $m \mapsto r(m), p(m)$.

É injetor: Seja $r(m) = 0 = p(m)$, isto é, m em $\ker p \cap \ker r = \operatorname{im} i \cap \ker r$. Logo, existe n tal que $m = i(n)$, e $r(i(n)) = n = 0$. Logo, $m = 0$.

É sobrejetor: Como p é sobrejetor e $r \circ i = \mathrm{id}$, em particular, r é sobrejetor, também α é sobrejetor.

(ii) $\implies$ (iii): Define $\beta\colon \mathrm{N} \oplus \mathrm{P} \to \mathrm{M}$ por $n, p \mapsto i(n) + s(p)$.

É injetor: Como $\operatorname{im} i = \ker p$, temos por construção da seção s que $\operatorname{im} s \cap \operatorname{im} i = 0$. Logo, como i e s, porque $p \circ s = \mathrm{id}$ são injetores, também β é injetor.

É sobrejetor: Seja m em M, e $m'' = s(p(m))$. Seja $m' = m - m''$. Temos

$$p(m') = p(m - m'') = p(m) - p(m) = 0,$$

isto é, m' em $\ker p = \operatorname{im} i$. □

Proposição 3.4. *Dada uma sequência exata da forma*

$$0 \to \mathrm{I} \xrightarrow{i} \mathrm{M} \xrightarrow{p} \mathrm{P} \to 0.$$

Se o módulo I *é injetor ou* P *é projetor, então ela cinde.*

Demonstração: Por I ser injetor, existe para $i\colon \mathrm{I} \hookrightarrow \mathrm{M}$ um homomorfismo $r\colon \mathrm{M} \to \mathrm{I}$ que fatora a identidade id sobre I, isto é, tal que $\mathrm{id} = r \circ i$

Por P ser projetivo, existe para $p\colon \mathrm{M} \twoheadrightarrow \mathrm{P}$ um homomorfismo $s\colon \mathrm{M} \to \mathrm{I}$ que fatora a identidade id sobre P, isto é, tal que $\mathrm{id} = p \circ s$. □

Um módulo M é *livre* se existe um conjunto I tal que $\mathrm{M} \simeq \mathrm{A}^{(\mathrm{I})} := \bigoplus_{i \in \mathrm{I}} \mathrm{A}$.

Lema 3.5. *Se* P *é livre, então é projetivo.*

Demonstração: Seja $\mathrm{P} \to \mathrm{M}$ e $n\colon \mathrm{N} \twoheadrightarrow \mathrm{M}$. Define $\mathrm{P} \to \mathrm{N}$ sobre uma base de P pela escolha de quaisquer pré-imagens dos valores de n sobre ela. □

Teorema Fundamental

Um módulo M é *finitamente gerado* se existe $A \oplus \cdots \oplus A \twoheadrightarrow M$. Um elemento m em M é de *torção* se existe a em A não-nulo tal que $am = 0$.

Teorema 3.6 (Teorema Fundamental sobre Módulos finitamente gerados). *Seja* M *um módulo sobre* A. *Se* A *é um domínio principal e* M *é finitamente gerado, então*

$$M = A^r \oplus A/\langle e_1 \rangle \oplus \cdots \oplus A/\langle e_n \rangle$$

onde $A^r = A \oplus \cdots \oplus A$ *com r fatores e* $e_1 | \ldots | e_n$ *em* A.

Demonstração: Seja M um módulo sobre A.

Afirmação: Se M é finitamente gerado e sem torção, então M é livre.

Prova: Seja $K = Q(A)$ o corpo das frações de A. Usemos indução sobre a dimensão de $V := M \otimes K$. Como M não tem torção, $M \hookrightarrow V$.

Se $\dim V = 1$, então $M \subseteq K$. Sejam $x_1/y, \ldots, x_n/y$ os geradores de M em K. Como A é um domínio principal, o ideal $(x_1, \ldots, x_n)$ gerado por $x_1, \ldots, x_n$ tem um único gerador x. Logo $M = A \cdot x/y \subseteq K$.

Se $\dim V > 1$, então seja L uma reta em V e considera a sequência exata

$$0 \to L \to V \to V/L \to 0$$

que induz a sequência exata

$$0 \to L \cap M \to M \to M/L \cap A \to 0.$$

Temos $L \cap M \neq \emptyset$; caso contrário, M estaria incluso em um complemento de L em V, isto é, M geraria um espaço vetorial de dimensão $< \dim V$, em contradição ao que M gera tudo de V. Como A é um domínio principal, em particular noetheriano, $L \cap M$ e $M/L \cap A$ são finitamente gerados. Logo, pela hipótese de indução, $L \cap M$ e $M/L \cap A$ são livres.

Como $M/L \cap A$ é livre, em particular é projetivo; isto é, esta sequência cinde. Logo M é livre.

Afirmação: $M = S \oplus T$ onde S respectivamente T são os submódulos sem torção respectivamente de torção.

Prova: Temos a sequência exata

$$0 \to T \to M \to S \to 0.$$

Como S é livre, a sequência cinde.

Afirmação: Se M é finitamente gerado e de torção, então

$$\mathrm{M} = \mathrm{A}/\langle e_1\rangle \oplus \cdots \oplus \mathrm{A}/\langle e_n\rangle$$

onde $e_1 | \ldots | e_n$ em A.

Prova: Como M é finitamente gerado e A é um domínio principal, existe o máximo ideal (e) que anula M. Isto é, $\bar{\mathrm{M}} = \mathrm{M}/e\mathrm{M}$ é um módulo sobre $\bar{\mathrm{A}} = \mathrm{A}/e\mathrm{A}$, e existe um elemento $\bar{m}$ em $\bar{\mathrm{M}}$ não-nulo cujo anulador é (e), isto é, $\bar{\mathrm{A}} \hookrightarrow \bar{\mathrm{M}}$. Temos a sequência exata

$$0 \to \bar{\mathrm{A}} \to \bar{\mathrm{M}} \to \bar{\mathrm{M}}/\bar{\mathrm{A}} \to 0.$$

Pela hipótese de indução sobre o número mínimo de geradores,

$$\bar{\mathrm{M}}/\bar{\mathrm{A}} \xrightarrow{\sim} \mathrm{A}/\langle e_1\rangle \oplus \cdots \oplus \mathrm{A}/\langle e_n\rangle$$

onde $e | e_1 | \ldots | e_n$. Para concluir, precisa de demonstrar que a sequência cinde, isto é, que $\bar{\mathrm{A}}$ é injetor sobre $\bar{\mathrm{A}}$. Pelo Critério de Baer, precisamos de demonstrar que todo homomorfismo $\phi\colon \bar{\mathrm{I}} \hookrightarrow \bar{\mathrm{A}}$ de módulos sobre $\bar{\mathrm{A}}$ para um ideal $\bar{\mathrm{I}}$ em $\bar{\mathrm{A}}$ estende-se a um homomorfismo $\Phi\colon \bar{\mathrm{A}} \to \bar{\mathrm{A}}$. Seja $\bar{\mathrm{I}} = \bar{f}\bar{\mathrm{A}}$ com $f | e$ em A. Isto é, $\bar{\mathrm{I}} = \bar{\mathrm{A}}[e/f]$. Como

$$\frac{e}{f}\phi(f) = 0 \iff e | e\frac{\phi(f)}{f} \iff \phi(f)/f \in \mathrm{A},$$

o homomorfismo $\phi\colon \bar{\mathrm{A}}[e/f] \to \bar{\mathrm{A}}$ fatora em $\bar{\mathrm{A}}[e/f] \to \bar{\mathrm{A}}[e/f] \to \bar{\mathrm{A}}$. Por isso, podemos estender ϕ a $\Phi\colon \bar{\mathrm{A}} \to \bar{\mathrm{A}}$ por $1 \mapsto \phi(f)/f$. □

Dois ideais I e J são *coprimos* (ou *relativamente primos*) se todo ideal que contêm I e J necessariamente contém 1, isto é, se $\mathrm{I} + \mathrm{J} = \mathrm{A}$.

Teorema 3.7 (Teorema Chinês dos Restos). *Seja* A *um anel. Sejam* I *e* J *ideais em* A. *Se* I *e* J *são relativamente primos, então*

$$\mathrm{A}/\mathrm{I} \cap \mathrm{J} \xrightarrow{\sim} \mathrm{A}/\mathrm{I} \times \mathrm{A}/\mathrm{J}.$$

Demonstração: A aplicação é injetora, porque $\mathrm{A} \to \mathrm{A}/\mathrm{I} \times \mathrm{A}/\mathrm{J}$ tem núcleo $\mathrm{I} \cap \mathrm{J}$.

Os ideais I e J são relativamente primos se, e tão-somente se, $\mathrm{I} + \mathrm{J} = \mathrm{A}$, isto é, existem i em I e j em J tal que $i + j = 1$. Como a imagem é um ideal sobre A, é suficiente mostrar que os seus geradores (1,0) e (0,1) são valores. Calculamos

$$j \equiv i + j = 1 \bmod \mathrm{I} \quad \text{e} \quad j \equiv 0 \bmod \mathrm{J}$$

e

$$i \equiv 0 \bmod \mathrm{I} \quad \text{e} \quad i \equiv i + j = 1 \bmod \mathrm{J}.$$

Seja A um anel. Um elemento a em A é irredutível se $xy = a$ implica ou x, ou y, invertível. A é um domínio de *fatoração única* se

- é um domínio íntegro, e
- todo a em A é produto de elementos irredutíveis, univocamente determinado exceto a ordem e associação dos fatores.

Lema 3.8. *Se* A *é um domínio principal, então* A *é um domínio de fatoração única.*

Demonstração: Existência da fatoração: Se a em A, então ou a é irredutível, ou $a = a_1 a_2$ tais que $\langle a \rangle \subset \langle a_1 \rangle$ e $\langle a \rangle \subset \langle a_2 \rangle$. Semelhantemente, ou a_1 é irredutível, ou $a_1 = a_{1,1} a_{1,2}$ e, ou a_2 é irredutível, ou $a_2 = a_{2,1} a_{2,2}$. Como A é um domínio principal, em particular, todo ideal é finitamente gerado, esta iterada divisão termina após um número finito de passos. (Se existisse uma cadeia infinita de inclusões próprias $\mathrm{I}_1 \subset \mathrm{I}_2 \subset \ldots$, então o ideal $\mathrm{I} = \mathrm{I}_1 \cup \mathrm{I}_2 \cup \ldots$ não seria finitamente gerado.)

Unicidade da fatoração: Precisamos de demonstrar primeiro que todo elemento irredutível é primo: Seja a em A. Mostremos que se $\mathrm{I} = \langle a \rangle$ não é máximo, então a é redutível: Como I não é máximo, existe $\mathrm{A} \supset \mathrm{J} = \langle b \rangle \supset \mathrm{I}$, isto é, $a = bc$ onde nem b, nem c são unidades; isto é, a é redutível. Em particular, se I é irredutível, então é primo (como I é máximo se, e tão-somente se, o quociente A/I é um corpo e I é primo se, e tão-somente se, o quociente A/I é um domínio íntegro).

Seja $a = a_1 \cdots a_m$ e $b = b_1 \cdots b_n$ uma decomposição em elementos irredutíveis. Como todo fator do lado esquerdo é primo e todo fator do lado direito é irredutível, ele é associado a um dos fatores do lado direito, e vice-versa, como todo fator do lado direito é primo e todo fator do lado esquerdo é irredutível, ele é associado a um dos fatores do lado esquerdo. Logo, $m = n$ e $b_1 \sim a_1$, …, $b_n \sim a_n$. □

Lema 3.9. *Se* A *é um domínio de fatoração única, então todo elemento irredutível é primo.*

Demonstração: Seja p irredutível e a, b em A tais que $p|ab$, isto é, existe c em A tal que $pc = ab$. Escreve

$$pc_1 \cdots c_\gamma = a_1 \cdots a_\alpha \cdot b_1 \cdots b_\beta .$$

Pela unicidade da fatoração, em particular p é associado a um dos fatores irredutíveis do lado direto; em particular p divide ou a ou b. □

Corolário 3.10. *Se* A *é um domínio de fatoração única, então, para qualquer ideal* I*, existem primos* $p_1, \ldots, p_n$ *(diferentes) e expoentes* $e_1, \ldots, e_n$ *tais que*

$$A/I \xrightarrow{\sim} A/\langle p_1^{e_1} \rangle \times \cdots \times A/\langle p_n^{e_n} \rangle.$$

Demonstração: Pelo Teorema Chinês dos Restos. □

4. Forma de Jordan

Seja V um espaço vetorial de dimensão finita sobre um corpo k. Um corpo k é *algebricamente fechado* se todo polinómio p em $k[\mathrm{X}]$ tem uma raiz em k. O nosso alvo é a demonstração do seguinte teorema:

Teorema 4.1 (Forma Normal de Jordan). *Seja* T *um endomorfismo de* V. *Se k é algebricamente fechado, então* V *é a soma direta de subespaços,* $\mathrm{V} = \mathrm{V}_1 \oplus \cdots \oplus \mathrm{V}_n$, *tais que a restrição t de* T *a cada subespaço é*

$$t = \lambda \cdot \mathrm{id} + \mathrm{N}$$

onde N *é o endomorfismo nilpotente dado por trasladar uma base $v_1, \ldots, v_n$, isto é,*

$$v_1 \mapsto v_2, \ldots, v_{n-1} \mapsto v_n \text{ e } v_n \mapsto 0.$$

Domínios euclidianos, principais e de fatoração única

Seja A um anel.

Definição 4.2. Seja A um anel. Para dois elementos a e b,

- um *maior divisor comum* $d = \mathrm{mdc}(a,b)$ é um divisor de a e b, tal que, se e é outro divisor de a e b, então d divide e.
- um *menor múltiplo comum* $m = \mathrm{mmc}(a,b)$ é um múltiplo de a e b, tal que, se n é outro múltiplo de a e b, então n é múltiplo de m.

Um elemento a em A é um *divisor de zero* se existe b em A não-nulo tal que $ab = 0$. A é um *domínio íntegro* se não tem divisores de zero.

Dois elementos a e b em A são *associados* se existe ϵ em A^* tal que $b = \epsilon a$.

Observação 4.3. Seja A um anel. Se A é um domínio íntegro, então o maior divisor comum e o menor múltiplo comum de dois a e b em A é univocamente determinado exceto associação, isto é,

- dois maiores divisores d' e d'' comuns são associados, e
- dois menores múltiplos m' e m'' comuns são associados.

Demonstração: Se d' e d'' são dois maiores divisores, então, por definição, $d' | d''$ e $d'' | d'$, isto é, existem u e v em A tal que $d' = uvd'$ e $d'' = uvd''$. Como A não tem divisores de zero, ou d' e d'' são nulos, ou $uv = 1$; em ambos os casos, d' e d'' são associados.

Da mesma maneira para dois menores múltiplos comuns. □

Exemplo 4.4.

- Se A = $\mathbb{Z}$, então $\mathbb{A}^* = \{\pm 1\}$. Logo o maior divisor comum e o menor múltiplo comum é determinado afora o seu sinal. Por convenção usa-se o número positivo.
- Se A = $\mathbf{K}[X]$ para um corpo $\mathbf{K}$, então $\mathbb{A}^* = \{\mathbf{K}\}$. Logo o maior divisor comum e o menor múltiplo comum é univocamente determinado afora um múltiplo escalar. Por convenção usa-se o cujo coeficiente *dominante*, o coeficiente da maior potência de X, é igual a 1.

Um anel é um *domínio principal* se

- é um domínio íntegro, e
- todo ideal é gerado por um único elemento.

Exemplo 4.5. São domínios principais:

(i) O anel $\mathbb{Z}$ com $v = |\cdot|$.

(ii) O anel polinomial $k[X]$ para um corpo k.

(iii) O anel $\mathbb{Z}[w]$ para $w = \frac{1+\sqrt[2]{-d}}{2}$ para $d = 19{,}43{,}67$ ou 163 é um domínio principal, mas não é euclidiano! (Veja abaixo para a definição de um domínio euclidiano.)

Um anel A é um *domínio euclidiano* se existe uma *função de grau* $v\colon A \to \mathbb{N} \cup \{-\infty\}$ tal que $v(0) = -\infty$ e para todo a e b não-nulo com $v(b) \leq v(a)$ existem q e r tais que

$$a = bq + r \qquad \text{com } v(r) < v(b).$$

Exemplo 4.6.

(i) O anel $\mathbb{Z}$ com $v = |\cdot|$ pela divisão com resto.

(ii) O anel $\mathbb{Z}[i]$ com $v = |\cdot|$.

(iii) O anel polinomial $k[X]$ para um corpo k pela divisão polinomial.

Lema 4.7. *Se* A *é um domínio euclidiano, então* A *é um domínio principal.*

Demonstração: Seja I um ideal em A e i_0 em I um elemento não-nulo em I de grau mínimo. Para todo $a = i$ em I e $b = i_0$ existem q e r tais que

$$a = qb + r \quad \text{com } v(r) < v(b).$$

Em particular, r em I. Como $v(r) < v(b)$ e $v(b) = v(i_0)$ é mínimo, $r = 0$. Isto é, $\mathrm{I} = \langle i_0 \rangle$. □

Proposição 4.8 (Lema de Bézout). *Seja* A *um anel. Se* A *é um domínio principal, então*

$$\langle a \rangle + \langle b \rangle = \langle \mathrm{mdc}(a,b) \rangle \quad e \quad \langle a \rangle \cap \langle b \rangle = \langle \mathrm{mmc}(a,b) \rangle$$

Demonstração: Quanto à primeira igualdade para o maior divisor comum, como A é principal, existe m tal que

$$\langle m \rangle = \langle a \rangle + \langle b \rangle \subseteq \langle \mathrm{mdc}(a,b) \rangle.$$

Como $m = \lambda a + \mu b$ para alguns λ e μ em A, obtemos que todo divisor de a e b divide m. Logo $\langle \mathrm{mdc}(a,b) \rangle \supseteq \langle m \rangle$. Isto é, $\langle \mathrm{mdc}(a,b) \rangle = \rangle \langle m \rangle = \langle a \rangle + \langle b \rangle$.

Quanto à segunda igualdade para o menor múltiplo comum, como A é principal, existe m tal que

$$\langle m \rangle = \langle a \rangle \cap \langle b \rangle \subseteq \langle \mathrm{mmc}(a,b) \rangle.$$

Como $m = \lambda a$ e $m = \mu b$ para alguns λ e μ em A, obtemos que todo múltiplo de a e b é múltiplo de m. Logo $\langle \mathrm{mmc}(a,b) \rangle \subseteq \langle m \rangle$. Isto é, $\langle \mathrm{mmc}(a,b) \rangle = \rangle \langle m \rangle = \langle a \rangle \cap \langle b \rangle$. □

Computar o Maior Divisor Comum pelo Algoritmo de Euclides. Sejam a e b números inteiros positivos tal que $a \geq b$ e com

$$a = b \cdot q + r \quad \text{com } 0 \leq r < b. \qquad (\dagger)$$

Equação $(\dagger) \implies d \mid a,b$ se, e somente se, $d \mid b,r$, $\implies$

$$\{\text{divisores comuns de } a \text{ e } b\} = \{\text{divisores comuns de } b \text{ e } r\},$$

em particular

$$\mathrm{mdc}(a,b) = \mathrm{mdc}(b,r).$$

Reaplicando a divisão com resto aos números menores b e r,

$$b = r \cdot q' + r' \quad \text{com } |r'| < |r|$$

e por isto

$$\mathrm{mdc}(b,r) = \mathrm{mdc}(r,r').$$

Iterando, chegamos a $s := r'^{\cdots'}$ e $r'^{\cdots''}$ com $r'^{\cdots''} = 0$, isto é

$$\mathrm{mdc}(a,b) = \ldots = \mathrm{mdc}(s,0) = \mathbf{s}.$$

Exemplo. Por exemplo, calculamos o maior divisor comum de $a = 748$ e $b = 528$ pela iterada divisão com resto:

$$\begin{aligned} 748 &= 528\cdot 1+220 \\ 528 &= 220\cdot 2+88 \\ 220 &= 88\ \cdot 2+\mathbf{44} \\ 88 &= 44\ \cdot 2+0, \end{aligned}$$

logo $\mathrm{mdc}(528,220) = 44$. Isto é,

$$\text{o maior divisor comum } = \text{ o penúltimo resto .}$$

Teorema (Algoritmo de Euclides). Sejam a e b números inteiros positivos com $a \geq b$. O seguinte algoritmo calcula $\mathrm{mdc}(a,d)$ em um número finito de passos:

*(*inicialização*) Põe* $r_0 = a$ *e* $r_1 = b$*, e* $i = 1$.
*(*divisão com resto*) Divide* r_{i-1} *por* r_i *com resto para obter*

$$r_{i-1} = r_i q_i + r_{i+1} \qquad \textit{com } |r_{i+1}| \leq |r_i|.$$

*(*iteração*) Distingue entre:*

- *ou* $r_{i+1} = 0$*, então* $r_i = \mathrm{mdc}(a,b)$ *e o algoritmo termina,*
- *ou* $r_{i+1} \neq 0$*, então ponha* $i := i + 1$ *e continue no passo (*divisão com resto*).*

Computar o Maior Divisor Comum como Combinação Linear pelo Algoritmo de Euclides Estendido. Para elementos $v_1, \ldots, v_d$ em A, uma **combinação linear** de $v_1, \ldots, v_d$ é uma soma s de múltiplos inteiros deles,

$$s = \lambda_1 v_1 + \cdots + \lambda_d v_d \qquad \text{com inteiros } \lambda_1, \ldots, \lambda_d.$$

O *Algoritmo de Euclides Estendido* mostra iterativamente que

$$\textbf{maior divisor comum} \text{ de } a \text{ e } b \ = \ \textbf{combinação linear} \text{ de } a \text{ e } b \ .$$

Teorema 4.9 (O algoritmo de Euclides Estendido). *Para quaisquer a e b em* A*, o seu maior divisor comum* $\mathrm{mdc}(a,b)$ *é uma combinação linear de a e b; isto é, existem u e v em* A *tais que*

$$\mathrm{mdc}(a,b) = au + bv.$$

Demonstração: Inicialmente, com $r_0 := a$, $r_1 := b$,

$$r_0 = r_1 q_i + r_2 \quad \text{com } |r_2| < |r_1|.$$

Isto é, $r_2 = r_0 - r_1 q_1$, $\Longrightarrow$

$$r_0, r_1, \text{ e } r_2 = \text{ combinações lineares de } a \text{ e } b \ .$$

Por indução,

$$r_{i-1} = r_i q_i + r_{i+1} \quad \text{com } |r_{i+1}| \leq |r_i|.$$

Como r_{i-1} e r_i são combinações lineares de a e b,

$$r_{i+1} = r_{i-1} - r_i q_i = \text{ uma combinação linear de } a \text{ e } b \ .$$

Em particular, quando finalmente $r_{\mathrm{I}+1} = 0$,

$$r_{\mathrm{I}} = \mathrm{mdc}(r_{\mathrm{I}}, r_{\mathrm{I}+1}) = \mathrm{mdc}(a,b) = \text{ combinação linear de } a \text{ e } b \ .$$

Exemplo. Já calculamos o maior divisor comum de $a = 748$ e $b = 528$,

$$\begin{aligned} 748 &= 528{\cdot}1{+}220 \\ 528 &= 220{\cdot}2{+}88 \\ 220 &= 88\ {\cdot}2{+}\mathbf{44} \\ 88 &= 44\ {\cdot}2{+}0, \end{aligned}$$

Logo,

$$\begin{aligned} 220 &= 748{-}528{\cdot}1 = a - b \\ 88 &= 528{-}220{\cdot}2 = b - (a-b)2 = 3b - 2a \\ \mathbf{44} &= 220{-}88\ {\cdot}2 = (a-b) - (3b-2a)2 = 5a - 7b, \end{aligned}$$

e, com efeito,

$$44 = 5 \cdot 748 - 7 \cdot 528.$$

Para um anel A, dois ideais I e J são *coprimos* (ou *relativamente primos*) se todo ideal que contêm I e J necessariamente contém 1, isto é, se $\mathrm{I} + \mathrm{J} = \mathrm{A}$. Dois elementos a e b em A são *coprimos* se os seus ideais principais são coprimos.

Lema 4.10. *Seja* T *um endomorfismo de* V *e* $\mathrm{P}(x)$ *em* $k[x]$ *tal que* $\mathrm{P}(\mathrm{T}) = 0$. *Se* $\mathrm{P} = \mathrm{QR}$, *então* T *se restringe a endomorfismos de* $\mathrm{U} = \ker \mathrm{Q}(\mathrm{T})$ *e* $\mathrm{W} = \ker \mathrm{R}(\mathrm{T})$. *Se* Q *e* R *são relativamente primos, então* $\mathrm{V} = \mathrm{U} \oplus \mathrm{W}$.

Demonstração: Para u em U, temos $\mathrm{Q}(\mathrm{T})(\mathrm{T}(u)) = [\mathrm{TQ}(\mathrm{T})](u) = 0$ e para w em W, temos $\mathrm{R}(\mathrm{T})(\mathrm{T}(u)) = [\mathrm{TR}(\mathrm{T})](u) = 0$, isto é, T se restringe a endomorfismos de U respectivamente de W.

Seja v em V. Como Q e R são relativamente primos, existem A e B tais que

$$\mathrm{AQ} + \mathrm{BR} = 1$$

Põe $u = [\mathrm{BR}(\mathrm{T})](v)$ e $w = [\mathrm{AQ}(\mathrm{T})](v)$. Logo

$$v = u + w$$

Como $\mathrm{P}(\mathrm{T}) = 0$ e $\mathrm{P} = \mathrm{QR}$, temos u em U e w em W.

Seja v em $\mathrm{U} \cap \mathrm{W}$, isto é, $\mathrm{Q}(\mathrm{T})(v) = 0$ e $\mathrm{R}(\mathrm{T})(v) = 0$. Logo $v = \mathrm{A}(\mathrm{T})(\mathrm{Q}(\mathrm{T})v) + \mathrm{B}(\mathrm{T})(\mathrm{R}(\mathrm{T})v) = 0$. □

Lema 4.11. *Seja* k *um corpo. Se* k *é algebricamente fechado, então todo polinómio* $p(x)$ *em* $k[x]$ *é produto*

$$p(x) = \prod \{\mathrm{X} - \lambda : \lambda \text{ raiz de } p(x)\}$$

Demonstração: O anel $k[x]$, como k é um corpo, é euclidiano; o resultado segue pela iterada divisão com resto. □

Corolário 4.12. *Seja* T *um endomorfismo de* V. *Se* k *é algebricamente fechado, então* V *é a soma direta de subespaços,* $\mathrm{V} = \mathrm{V}_1 \oplus \cdots \oplus \mathrm{V}_n$, *tais que a restrição* t *de* T *a cada subespaço é*

$$t = \lambda \cdot \mathrm{id} + \mathrm{N}$$

onde λ *em* k *e* N *é um endomorfismo nilpotente.*

Demonstração: Como $\dim \mathrm{End}(V) < \infty$, as potências 1, T, T^2, ... são linearmente dependentes para um expoente suficientemente alto, isto é, existe P em $k[x]$ tal que

$$P(T) = 0.$$

Como k é algebricamente fechado, existem pelo lema $\lambda_1, \ldots, \lambda_n$ *distintos* em k e expoentes $e_1, \ldots, e_n$ tais que

$$P(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_n)^{e_n}.$$

Como λ_1 é distinto de $\lambda_2, \ldots, \lambda_n$, os polinómios $Q(X) = (X-\lambda_1)^{e_1}$ e $R(X) = (X-\lambda_2)^{e_2} \cdots (X-\lambda_n)^{e_n}$, os únicos divisores comuns são unidades, isto é, $\mathrm{mdc}(Q,R) = 1$; logo, pelo Lema de Bézout, Proposição 4.8, os polinómios Q e R são coprimos. Logo, por iterada aplicação de Lema 4.10,

$$V = V_1 \oplus \cdots \oplus V_n$$

onde $V_1 = \ker(T-\lambda)^{e_1}, \ldots, V_n = \ker(T-\lambda)^{e_n}$ e T se restringe a endomorfismos de $V_1, \ldots, V_n$. Isto é, em cada tal subespaço $W = V_1, \ldots, V_n$,

$$T = \lambda \mathrm{id} + N$$

com $N = T - \lambda \cdot \mathrm{id}$ e $N^e = 0$. □

Ora, para demonstrar Teorema 4.1, falta só demonstrar:

Teorema 4.13. *Seja* N *um endomorfismo de* V. *Se* N *é nilpotente, então* $V = V_1 \oplus \cdots \oplus V_n$ *e em cada* $W = V_1, \ldots, V_n$ *existe uma base* $w_1, \ldots, w_n$ *tal que* N *a traslade, isto é,*

$$w_1 \mapsto w_2, \ldots, w_{n-1} \mapsto w_n \text{ e } w_n \mapsto 0.$$

Demonstração: Por indução pela dimensão de V. Como N é nilpotente, a imagem $\mathrm{im}\, N \subset V$ é um subconjunto próprio do contra-domínio; também, N se restringe a um endomorfismo de $\mathrm{im}\, N$. Logo, pela hipótese da indução, $\mathrm{im}\, N = V_1 \oplus \cdots \oplus V_n$ tal que N opere por traslado em cada $V = V_1, \ldots, V_n$, isto é,

$$v_1, Nv_1, \ldots, N^{e_1-1}v_1, \ldots, v_n, Nv_n, \ldots, N^{e_n-1}v_n$$

é uma base de $\mathrm{im}\, N$.

Sejam $u_1, \ldots, u_n$ tais que $v_1 = Nu_1, \ldots, v_n = Nu_n$ sob N.

Temos $\ker N \cap \mathrm{im}\, N = \langle N^{e_1-1}v_1, \ldots, N^{e_n-1}v_n \rangle$. Estende estes por $w_1, \ldots, w_k$ a uma base de $\ker N$.

O número de vetores de

$$u_1, v_1, \mathrm{N}v_1, \ldots, \mathrm{N}^{e_1-1}v_1, \ldots, u_n, v_n, \mathrm{N}v_n, \ldots, \mathrm{N}^{e_n-1}v_n, w_1, \ldots, w_k$$

é $\dim \operatorname{im} \mathrm{N} + (n+k) = \dim \operatorname{im} \mathrm{N} + \dim \ker \mathrm{N} = \dim \mathrm{V}$.

Estes vetores são linearmente independentes: Os $w_1, \ldots, w_k$ são linearmente independentes, em $\ker \mathrm{N}$ e por escolha $\langle w_1, \ldots, w_k \rangle \cap \operatorname{im} \mathrm{N} = 0$. Logo, basta verificar que

$$u_1, \mathrm{N}u_1, \ldots, \mathrm{N}^{e_1}u_1, \ldots, u_n, \mathrm{N}u_n, \ldots, \mathrm{N}^{e_n}u_n,$$

são linearmente independentes: Caso contrário, aplica N para obter uma dependência linear entre os vetores $v_1, \ldots, \mathrm{N}^{e_1-1}v_1, \ldots, v_n, \ldots, \mathrm{N}^{e_n-1}v_n$ em contradição ao que eles constituem uma base de $\operatorname{im} \mathrm{N}$! O endomorfismo N traslada as bases

$$\{u_1, \mathrm{N}u_1, \ldots, \mathrm{N}^{e_1}u_1\}, \ldots, \{u_n, \mathrm{N}u_n, \ldots, \mathrm{N}^{e_1}u_n\}, \{w_1\}, \ldots, \{w_k\}.$$

Teorema Fundamental de Álgebra

Fato. *O corpo $\mathbb{C}$ é algebricamente fechado.*

Demonstração: Segue pela observação que todo polinómio real de grau ímpar tem uma raiz pelo Teorema do Valor Intermediário. □

Corolário 4.14. *Seja V um espaço vetorial sobre k. Seja T um endomorfismo de V. Se $k = \mathbb{R}$, então não todo polinómio $\mathrm{P}(\mathrm{X})$ em $\mathbb{R}[\mathrm{X}]$ tem uma raiz, mas λ é uma raiz complexa de $\mathrm{P}(\mathrm{X})$ se, e tão-somente se, $\bar{\lambda}$ é uma raiz complexa de $\mathrm{P}(\mathrm{X})$; logo*

$$\mathrm{P}(\mathrm{X}) = (\mathrm{X} - \lambda_1)(\mathrm{X} - \bar{\lambda}_1) \cdots (\mathrm{X} - \lambda_n)(\mathrm{X} - \bar{\lambda}_n) \cdot (\mathrm{X} - \lambda_{n+1}) \cdots (\mathrm{X} - \lambda n + m)$$

onde $\lambda_1, \ldots, \lambda_n$ em $\mathbb{C} - \mathbb{R}$ e $\lambda_{n+1}, \ldots, \lambda_{n+m}$ em $\mathbb{R}$. Se t é um endomorfismo de $\mathbb{R} \oplus \mathbb{R}$ e t não tem nenhum valor próprio, isto é, o seu polinómio característico de grau 2 não tem nenhuma raiz em $\mathbb{R}$, então

$$t = \mathrm{C}$$

onde $\mathrm{C} = \lambda \cdot \mathrm{R}$ é o produto de um escalamento λ e uma rotação $\mathrm{R} = \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ para a e b em k com $a^2 + b^2 = 1$. e uma forma canónica para endomorfismos sobre $\mathbb{R}$, análoga à da sobre $\mathbb{C}$, pode ser obtida.

Aplicações

Define a série de potências $\exp(Z) = \sum_n \frac{1}{n!} Z^n$. Se o corpo k é normado, então $\mathrm{End}(V)$ para todo espaço vetorial de dimensão finita V é normado. Para A em $\mathrm{End}(V)$, temos $\|A^n\| \leq \|A\|^n$, e como $C^n < \frac{1}{n!}$ para n suficientemente grande, a série dada por $\exp(A)$ converge para todo A em $\mathrm{End}(V)$ absolutamente, obtendo a função

$$\exp\colon \mathrm{End}(V) \to \mathrm{End}(V).$$

Lema 4.15. *Seja $\sum_n a_n$ uma série. Se ela converge absolutamente ao limite a, então para toda permutação σ de $\mathbb{N}$, a série $\sigma(a) := \sum_n a_{\sigma(n)}$ converge absolutamente e o seu limite é a.*

Corolário 4.16. *Seja* A *uma matriz quadrática. Existe uma matriz invertível* B *tal que*

$$B^{-1} \exp(A) B = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_n \end{pmatrix}$$

onde cada bloco $A = A_1, \ldots, A_n$ é da forma

$$A = \begin{pmatrix} \exp\lambda & & \\ & \ddots & \\ & & \exp\lambda \end{pmatrix} \begin{pmatrix} 1 & 1/2 & \ldots & \ldots & 1/n! \\ & 1 & 1/2 & \ldots & 1/(n-1)! \\ & & \vdots & & \\ & & & & 1 \end{pmatrix}.$$

Demonstração: Pelo Teorema de Jordan, existe uma matriz invertível B tal que $B^{-1}AB = \lambda E + N$ tem forma de Jordan, isto é, N é nilpotente. Como a convergência de $\exp(A)$ é absoluta, obtemos

$$B^{-1} \exp(A) B = \exp B^{-1}AB = \exp(\lambda \cdot E + N) = \exp(\lambda) \cdot E \exp(N).$$

Logo, com E a matriz de unidade cujas únicas entradas não-nulas são as diagonais com o valor 1, e N é nilpotente, obtemos a forma enunciada. □

5. Anéis Noetherianos e o Teorema de Base de Hilbert

Seja Σ um conjunto *parcialmente ordenado*; isto é, tem uma relação $\leq$ que é

- *reflexiva*, isto é, $x \leq x$,
- *transitiva*, isto é, se $x \leq y$ e $y \leq z$, então $x \leq z$, e
- se $x \leq y$ e $y \geq x$ então $x = y$.

Denote $y \geq x$ que $x \leq y$.

Exemplo 5.1. Por exemplo, para um conjunto S, o conjunto $\mathcal{P}(S)$ dos subconjuntos de S com $\leq$ definida pela inclusão $\subseteq$ é um conjunto parcialmente ordenado.

Proposição 5.2. *Toda sequência crescente $x_1 \leq x_2 \leq \ldots$ em Σ é* estacionária*, isto é, existe n tal que $x_n = x_{n+1} = \cdots$, se, e tão-somente se, todo subconjunto não-vazio σ de Σ contém um elemento* máximo*, isto é, um elemento x para que não existe $y \geq x$ em σ diferente de x.*

Demonstração: Se existe um subconjunto σ sem elemento máximo, isto é, para todo x em σ existe y em σ com $y \geq x$, então, dada uma sequência finita $x_1 \leq \ldots x_n$, existe $y = x_{n+1} \geq x_n$ diferente de x; a sequência (x_n) assim construida não é estacionária.

Se todo subconjunto σ tem um elemento máximo, então em particular $\{x_n\}$ tem um elemento máximo x_N; necessariamente $x_N = x_{N+1} = \cdots$. □

Módulos Noetherianos

Se Σ é o conjunto dos submódulos de um módulo, e $\leq$ é $\subseteq$ respectivamente $\supseteq$, então a condição em Proposição 5.2 é a *condição da cadeia crescente* e o módulo é *noetheriano* respectivamente *decrescente* e o módulo é *artiniano.*

Um anel A é *noetheriano* se é noetheriano como módulo sobre A (cujos submódulos são os ideais).

Exemplo 5.3.

- Um grupo abeliano finito é noetheriano e artiniano.
- O anel $\mathbb{Z}$ é noetheriano, mas não é artiniano.

- O anel dos polinómios em um número finito de incógnitas $k[x_1, \ldots, x_d]$ com coeficientes em um corpo k é noetheriano, mas não é artiniano.
- O anel dos polinómios $k[x_1, x_2, \ldots]$ para uma infinitude de incógnitas é nem noetheriano nem artiniano.

Proposição 5.4. *Um módulo é noetheriano se, e tão-somente se, todo submódulo é gerado por um número finito de elementos.*

Demonstração: Se todo submódulo é gerado por um número finito de elementos, então, dada uma sequência crescente $M_1 \subseteq M_2 \subseteq \ldots$ de submódulos, existe M_N para N suficientemente grande que contém todos os geradores de $M = \bigcup M_n$; logo $M_N = M_{N+1} = \cdots$.

Seja N um submódulo de M; seja Σ o conjunto dos submódulos finitamente gerados de N. Não é vazio porque contém 0. Logo, contém um elemento máximo N_0. Se $N_0 \subset N$, isto é, existe x em $N - N_0$, considera o submódulo N_1 gerado pelos geradores de N_0 e por x. Logo, N_0 não era máximo; contradição. □

Exemplo 5.5.

- Todo domínio de ideais principais é noetheriano.
- Em particular, os anéis euclidianos.
- Em particular, $k[x]$ para um corpo k e $\mathbb{Z}$.

Proposição 5.6. *A categoria dos módulos noetherianos é abeliana: Isto é, para toda sequência exata de módulos*

$$0 \to M' \to M \to M'' \to 0,$$

o módulo M *é noetheriano se, e tão-somente se,* M' *e* M'' *são noetherianos.*

Igual com artiniano no lugar de noetheriano.

Demonstração: $\Longrightarrow$: Seja M noetheriano. Como todo submódulo de M é finitamente gerado, em particular, todo submódulo de $M' \subseteq M$. Seja N'' um submódulo de M''. Logo, a sua pré-imagem $N = \pi^{-1}(N'')$ sob $\pi\colon M \twoheadrightarrow M''$, como submódulo de M, é finitamente gerada por $x_1, \ldots, x_n$. Logo $\pi(x_1), \ldots, \pi(x_n)$ geram N''.

$\Longleftarrow$: Seja M' e M'' noetherianos. Seja N um submódulo de M. Logo $\pi\colon N \twoheadrightarrow N''$ para um módulo finitamente gerado N'' e $N' = N \cap M'$ é finitamente gerado. Logo N é gerado pelos geradores (cuja quantidade é finita) de N'' e de N'. □

Exemplo 5.7.

- O anel $\mathbb{Z}/n\mathbb{Z}$ é noetheriano e artiniano.

Corolário 5.8. *Seja* M *um módulo e* ϕ *um homomorfismo entre anéis. Se* M *é noetheriano, então* $\phi(M)$ *é noetheriano.*

Demonstração: Temos $0 \to \ker\phi \to M \to \operatorname{im}\phi \to N$. □

Corolário 5.9. *Uma soma finita direta de módulos noetherianos é noetheriana. Igual com artiniano no lugar de noetheriano.*

Demonstração: Por indução, usando

$$0 \to M_n \to M_1 \oplus \cdots \oplus M_{n-1} \oplus M_n \to M_1 \oplus \cdots \oplus M_{n-1} \to 0.$$

e Proposição 5.6. □

Corolário 5.10. *Seja* A *um anel. Se* A *é noetheriano, isto é, é notheriano como módulo sobre* A*, então todo módulo finitamente gerado sobre* A *é noetheriano.*

Demonstração: Um módulo M é finitamente gerado se, e tão-somente se,

$$A \oplus \cdots \oplus A \twoheadrightarrow M$$

Por Corolário 5.9, o lado esquerdo é noetheriano. Por Corolário 5.8, o lado direito também é noetheriano. □

Anéis Noetherianos

Recapitulemos que as seguintes condições para um anel A são equivalentes:

- Todo conjunto de ideais não-vazio contém um ideal máximo.
- Toda cadeia de ideais crescente é estacionária.
- Todo ideal é finitamente gerado.

Para um polinómio $a_nX^n + \cdots + a_0$, designe o *coeficiente dominante* o coeficiente a_n da maior potência da incógnita.

Teorema 5.11 (Teorema da Base de Hilbert)**.** *Seja* A *um anel. Se* A *é noetheriano, então* $A[x]$ *é noetheriano.*

Demonstração: Seja I um ideal em $A[x]$. Os coeficientes (das potências) dominantes formam um ideal i em A. Como A é noetheriano, i é finitamente gerado por $a_1, \ldots, a_n$. Sejam $f_1, \ldots, f_n$ polinómios com coeficientes dominantes $a_1, \ldots, a_n$ e graus $r_1, \ldots, r_n$. Seja $r = \max\{r_1, \ldots, r_n\}$ o maior grau entre eles, e I′ o ideal em $A[x]$ gerado por eles.

Seja $f = ax^m + \cdots$ em I. Temos a em i. Se $m \geq r$, então escreve $a = u_1a_1 + \cdots + u_na_n$ com $u_1, \ldots, u_n$ em A; o grau de $f - [u_1f_1x^{m-r_1} + \cdots + u_nf_nx^{m-r_n}]$ é $< m$, e continua a ser em I. Procedendo desta maneira, obtemos f' em I′ tal que $f = f' + g$ com o grau de $g < r$.

Isto é, para R o A-módulo gerado por $x^0, x^1, \ldots, x^{r-1}$, acabamos de demonstrar que $I = (I \cap R) + I'$.

Por Corolário 5.10, R é noetheriano. Logo, por Proposição 5.4, $I \cap R$ é finitamente gerado como módulo sobre A. Se $f_1', \ldots, f_n'$ geram $I \cap R$, então $f_1', \ldots, f_n'$ e $f_1, \ldots, f_n$ geram I. Isto é, I é finitamente gerado, logo $A[x]$ é noetheriano. □

Observação 5.12. Se A é noetheriano, então $A[[x]]$ é noetheriano.

Demonstração: Usa os coeficientes das menores potências (em vez das maiores) e procede como na demonstração acima. □

Aplicações

Corolário 5.13. *Se* A *é noetheriano, então* $A[x_1, \ldots, x_n]$ *é noetheriano*

Demonstração: Por iterada aplicação do Teorema de Base de Hilbert, usando

$$A[x_1, \ldots, x_n, x_{n+1}] = A[x_1, \ldots, x_n][x_{n+1}].$$

Corolário 5.14. *Seja* B *uma álgebra finitamente gerada sobre um anel* A. *Se* A *é noetheriano, então* B *é noetheriano.*

Demonstração: Por Corolário 5.13 e Corolário 5.8. □

Corolário 5.15. *Seja* A *um anel e* X *um locus em* $A \times \cdots \times A$, *isto é, os* x *tais que* $f(x) = 0$ *para todo* f *em um ideal* I *em* $A[T_1, \ldots, T_n]$. *Se* A *é noetheriano, em particular, se* A *é um corpo, então* X *é o locus de um número finito de* $f_1, \ldots, f_n$ *em* $A[T_1, \ldots, T_n]$.

Se $A = k$ é um corpo e $C = k[X]$, então todo anel B em C é finitamente gerado como álgebra sobre A por [Gal57]. Contudo, se A não é um corpo (ou C tem mais de uma incógnita), então existem contra-exemplos: Por exemplo, se $A = \mathbb{Z}$, então o anel $B = 2 \cdot \mathbb{Z}[X]$ dos polinómios cujos coeficientes são pares não é finitamente gerado como álgebra sobre A.

Um critério suficiente para que um anel B em C seja finitamente gerado como álgebra sobre A, é que C é finitamente gerado como *módulo* sobre B:

Proposição 5.16. *Sejam* $A \subseteq B \subseteq C$ *anéis. Se* A *é noetheriano,* C *finitamente gerado como álgebra sobre* A *e* C *é finitamente gerado como módulo sobre* B*, então* B *é finitamente gerado como álgebra sobre* A.

Demonstração: Sejam $x_1, \ldots, x_m$ geradores de C como álgebra sobre A e $y_1, \ldots, y_n$ geradores de C como módulo sobre B. Logo, existem expressões

$$x_i = b_{i,1}y_1 + \cdots + b_{i,n}y_n \quad \text{e} \quad y_i y_j = b_{i,j,1}y_1 + \cdots + b_{i,j,n}y_n. \tag{$*$}$$

Seja $A \subseteq B_0 \subseteq B$ a álgebra gerada sobre A pelos $b_{i,j}$ e $b_{i,j,k}$. Pelo Teorema da Base de Hilbert, Corolário 5.14, B_0 é noetheriano.

Todo elemento em C é um polinómio em $x_1, \ldots, x_m$ com coeficientes em A. Logo, por iterada aplicação de $(*)$, uma soma em $y_1, \ldots, y_n$ com coeficientes em B_0. Isto é, C é finitamente gerado como módulo sobre B_0 (e não apenas sobre B).

Como B_0 é noetheriano, C é noetheriano sobre B_0. Em particular, o submódulo B em C é finitamente gerado como módulo sobre B_0.

Como B_0 é finitamente gerada como álgebra sobre A, logo B é finitamente gerada como álgebra sobre A. □

Teorema 5.17 (Lema de Zariski). *Seja* C *uma extensão de um corpo* k*. Se* C *finitamente gerado como álgebra sobre* k*, então* C *é (uma extensão de corpos) algébrica sobre* k.

Demonstração: Por contraposição, suponhamos que $C = k[x_1, \ldots, x_n]$ não é algébrico sobre k. Se C não é algébrico sobre k, então sejam $x_1, \ldots, x_r$ algebricamente independentes sobre k e $x_{r+1}, \ldots, x_n$ algébricos (= algebricamente dependentes) sobre $B := k(x_1, \ldots, x_r)$. Isto é, C é finitamente gerado como módulo sobre B. Por Proposição 5.16, o anel B é finitamente gerada como álgebra sobre k, isto é, $B = k[y_1, \ldots, y_s]$ para $y_1 = \frac{f_1}{g_1}, \ldots, y_s = \frac{f_s}{g_s}$ com polinómios $f_1, \ldots, f_s$ e $g_1, \ldots, g_s$ não-nulos sobre k nas incógnitas $x_1, \ldots, x_r$. O polinómio $h = g_1 \cdots g_s + 1$ em $k[x]$ é indivisível por $g_1, \ldots, g_s$; logo h^{-1} não é um polinómio em $y_1, \ldots, y_s$; isto é, B não é um corpo. □

Teorema 5.18 (Versão fraca do Nullstellensatz). *Seja k um corpo algebricamente fechado. Sejam $f_1, \ldots, f_n$ em $\mathrm{A} := k[x_1, \ldots, x_d]$. Se $\mathrm{I} = \langle f_1, \ldots, f_n \rangle \subset \mathrm{A}$, então existe um zero comum de $f_1, \ldots, f_n$.*

Demonstração: O ideal I é contido em um ideal máximo m. A extensão A/m é um corpo que é uma extensão finita (como álgebra) K de k. Pelo Lema de Zariski, K é uma extensão algébrica. Como k é algebricamente fechado, $\mathrm{K} = k$.

Seja $\phi \colon \mathrm{A} \to \mathrm{A}/m = k$ a aplicação de quociente. Logo

$$z := \phi(x) = (\phi(x_1), \ldots, \phi(x_d))$$

tem entradas em k e satisfaz para todo $f = f_1, \ldots, f_n$ que

$$f(z) = f(\phi(x)) = \phi(f(x)) = 0$$

pois $f_1, \ldots, f_n$ em $\mathrm{I} \subseteq m$. □

6. Nullstellensatz

Uma *álgebra* sobre um anel k é um anel A com um homomorfismo $k \to \mathrm{A}$. A álgebra é *finitamente gerada* sobre k (como álgebra) se existe um número finito de elementos $a_1, \ldots, a_n$ em A e um epimorfismo

$$\begin{aligned} k[x_1, \ldots, x_n] &\twoheadrightarrow \mathrm{A} \\ x_1, \ldots, x_n &\mapsto a_1, \ldots, a_n. \end{aligned}$$

Dado um polinómio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ de grau n, o seu *coeficiente dominante* é a_n, o coeficiente da potência com o expoente máximo n. Um polinómio é *mónico* se o seu coeficiente dominante é 1. Sejam A e B anéis tais que $\mathrm{A} \subseteq \mathrm{B}$. Um elemento b em B é *integral* sobre A se existe um polinómio mónico $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ em $\mathrm{A}[x]$ tal que $f(b) = 0$. (Equivalentemente, um polinómio cujo coeficiente dominante é invertível em A; em particular, se $\mathrm{A} = k$ é um corpo, então b é integral sobre k se, e tão-somente se, é algébrico sobre k.) Um anel B é *integral* sobre A se todo os elementos em B são integrais.

Elementos $x_1, \ldots, x_n$ em um anel A são *algebricamente dependentes* se existe P em $\mathrm{A}[\mathrm{T}]$ diferente de 0 tal que $\mathrm{P}(x_1, \cdot, x_n) = 0$. Uma álgebra B finitamente gerada sobre um anel A é *puramente transcendental* se os geradores são algebricamente independentes sobre A.

Lema 6.1. *Se* $\mathrm{A} \subseteq \mathrm{B}$ *são anéis, então são equivalentes:*

(i) *O elemento* b *em* B *é integral sobre* A*,*

(ii) *A álgebra* $\mathrm{A}[b]$ *é finitamente gerado como módulo sobre* A*,*

(iii) *A álgebra* $\mathrm{A}[b]$ *é contida em um anel* C *em* B *que é finitamente gerado como módulo sobre* A*,*

Demonstração: (i) $\implies$ (ii): Se b é integral, isto é, existe um polinómio mónico $f(x)$ tal que $f(x) = 0$, então $\mathrm{A}[\mathrm{X}]/\langle b \rangle \twoheadrightarrow \mathrm{A}[b]$; em particular, $\mathrm{A}[b]$ é finitamente gerada.

(ii) $\implies$ (iii): Põe $\mathrm{C} = \mathrm{A}[b]$.

(iii) $\implies$ (i): Seja $\mathrm{C} \supseteq \mathrm{A}[b]$ finitamente gerada como módulo sobre A. Logo, existe uma relação $b^n = a_{n-1}b^{n-1} + \cdots + a_0$. Isto é, $f(b) = 0$ para $f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0$. □

Lema 6.2. *Seja* B *uma álgebra sobre* A *e* M *um módulo sobre* B. *Se* M *é finitamente gerado sobre* B *e* B *é finitamente gerada como módulo sobre* A*, então* M *é finitamente gerado sobre* A.

Demonstração: Se $m_1, \ldots, m_k$ geram M sobre B e $b_1, \ldots, b_l$ geram B sobre A, então os kl produtos $m_i b_j$ para $i = 1, \ldots, k$ e $j = 1, \ldots, l$ geram M sobre A. □

Corolário 6.3. *Seja* B *uma álgebra sobre* A. *Se* B *é finitamente gerada como álgebra sobre* A*, então são equivalentes:*

(i) B *é integral sobre* A,

(ii) *todos os geradores de* B *são integrais sobre* A,

(iii) B *é finitamente gerada como módulo sobre* A,

(iv) B *é contida em um módulo* C *finitamente gerado sobre* A.

Demonstração: (i) $\Longrightarrow$ (ii): Se todo elemento em B é integral sobre A, então em particular os seus geradores.

(ii) $\Longrightarrow$ (iii): Por indução sobre o número de geradores. O caso $n = 1$ foi tratado em Lema 6.1 Se $n > 1$, então x_n é em particular integral sobre $A[x_1, \ldots, x_{n-1}]$, logo, $A[x_1, \ldots, x_{n-1}, x_n]$ é finitamente gerado sobre $A[x_1, \ldots, x_{n-1}]$. Logo $A[x_1, \ldots, x_{n-1}, x_n]$ é por Lema 6.2 finitamente gerado como módulo sobre A.

(iii) $\Longrightarrow$ (iv): Põe C = B.

(iv) $\Longrightarrow$ (i): Seja b em B. Como $b \in$ C e C é finitamente gerado sobre A como módulo, por Lema 6.1, b é integral sobre A □

Lema 6.4 (Transitividade da integralidade). *Sejam* A $\subseteq$ B $\subseteq$ C *anéis. Se* B *é integral sobre* A *e* C *é integral sobre* B*, então* B *é integral sobre* A.

Demonstração: Um elemento c em C é integral sobre B se, e tão-somente se, existem $b_{n-1}, \ldots, b_0$ em B tais que

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0.$$

Como todos os seus geradores são integrais, o anel $B' = A[b_1, \ldots, b_n]$ é finitamente gerado como módulo sobre A. Por Lema 6.1, $B'[c]$ é finitamente gerado como módulo sobre B′. Logo $B'[c]$ é finitamente gerado sobre A por Lema 6.2. Equivalentemente, por Lema 6.1.(iii), c é integral sobre A. □

Lema 6.5. *Seja k um corpo e seja para $\mu = (\mu_1, \ldots, \mu_e)$ em $\mathbb{N}\times\cdots\times\mathbb{N}$ o automorfismo ϕ_μ sobre $k[x_1, \ldots, x_e, \mathrm{X}]$ definido por*

$$x_1, \ldots, x_e, \mathrm{X} \mapsto x_1 + \mathrm{X}^{\mu_1}, \ldots, x_1 + \mathrm{X}^{\mu_e}, \mathrm{X}.$$

Se P em $k[x_1, \ldots, x_e, \mathrm{X}]$, então existe μ tal que $\phi_\mu(\mathrm{P})$ em $\mathrm{A}[\mathrm{X}]$ para $\mathrm{A} = k[x_1, \ldots, x_e]$ tem coeficiente dominante em k.

Demonstração: Demonstremos a existência de μ por indução em e:

Se $e = 0$, então P em $k[\mathrm{X}]$ e $\mu = (0, \ldots, 0)$ basta.

Se $e > 0$, suponhamos que a hipótese vale para e. Escreve P como polinómio em $k[x_1, \ldots, x_e, \mathrm{X}][x_{e+1}]$, isto é,

$$\mathrm{P} = a_0 + a_1 x_{e+1} + \cdots + a_l x_{e+1}^l$$

com a_0, a_1, …, a_l em $k[x_1, \ldots, x_e, \mathrm{X}]$. Pela hipótese de indução, existe $\nu = \mu_{1,\ldots,e} = (\mu_1, \ldots, \mu_e)$ tal que $\phi_\nu(a_l)$ tem coeficiente dominante em k.

Para $\mu = \mu_{1,\ldots,e,e+1} = (\mu_1, \ldots, \mu_e, \mu_{e+1})$, obtemos

$$\phi_\mu(\mathrm{P}) = \phi_\nu(a_0) + \phi_\nu(a_1)(\mathrm{X}^{\mu_{e+1}} + x_{e+1}) + \cdots + \phi_\nu(a_l)(\mathrm{X}^{\mu_{e+1}} + x_{e+1})^l$$

Como $\phi_\nu(a_l)$ tem coeficiente em k, podemos escolher μ_{e+1} suficientemente grande para

$$\epsilon_l + \mu_{e+1} l > \epsilon_{l-1} + \mu_{e+1}(l-1), \ldots, \epsilon_1 + \mu_{e+1}, \epsilon_0$$

ou, equivalentemente,

$$\mu_{e+1} l > \epsilon_{l-1} - \epsilon_l, \frac{\epsilon_{l-2} - \epsilon_l}{2}, \ldots, \frac{\epsilon_0 - \epsilon_l}{l}$$

onde $\epsilon_0, \epsilon_1, \ldots, \epsilon_l$ são os graus de X de $\phi_\nu(a_0)$, $\phi_\nu(a_1)$, …, $\phi_\nu(a_l)$ como polinómios em X. Isto é, suficientemente grande para o polinómio $\phi_\mu(\mathrm{P})$ em X ter coeficiente dominante em k. □

Teorema 6.6 (Normalização de Noether). *Seja k um corpo e A uma álgebra sobre k. Se A é finitamente gerada (como álgebra), então existe $\mathrm{B} \subseteq \mathrm{A}$ puramente transcendental tal que A é integral sobre B; isto é, existem $y_1, \ldots, y_r$ em A algebricamente independentes tais que A é integral sobre $k[y_1, \ldots, y_r]$.*

Demonstração: Seja A gerado por $y_1, \ldots, y_n, y_{n+1}$. Se $y_1, \ldots, y_{n+1}$ são algebricamente independentes sobre k, então a proposição vale. Logo, suponhamos que y_{n+1} depende de $y_1, \ldots, y_n$, isto é, existe um polinómio P em $k[y_1, \ldots, y_n, X]$ que anula y_{n+1}. Seja $\mu = (\mu_1, \ldots, \mu_n)$ dado por Lema 6.5, isto é, tal que o automorfismo ϕ_μ definido por

$$\begin{aligned} k[x_1, \ldots, x_n, X] &\to k[x_1, \ldots, x_n, X] \\ x_1, \ldots, x_n, X &\mapsto x_1 + X^{\mu_1}, \ldots, x_1 + X^{\mu_n}, X. \end{aligned}$$

torna $\phi_\mu(P)$ em um polinómio em X cujo coeficiente dominante é em k.

Põe $z_1 = \phi_\mu^{-1}(y_1)$, …, $z_{n+1} = \phi_\mu^{-1}(y_{n+1})$. Como ϕ_μ é um automorfismo, $z_1, \ldots, z_n, z_{n+1}$ geram $k[y_1, \ldots, y_n, y_{n+1}]$, e

$$\phi_\mu(P)(z_1, \ldots, z_n, z_{n+1}) = \phi_\mu(\phi_\mu^{-1}(P(y_1, \ldots, y_n, y_{n+1}))) = P(y_1, \ldots, y_n, y_{n+1}) = 0.$$

Logo z_{n+1} é integral sobre $B_n := k[z_1, \ldots, z_n]$, testemunhado por $\phi_\mu P$.

Ou $k[z_1, \ldots, z_n]$ é puramente transcendental, ou existe um elemento algébrico. z em $\{z_1, \ldots, z_n\}$, digamos $z = z_n$, anulado por um polinómio P em $k[z_1, \ldots, z_{n-1}]$. Logo, pelo mesmo argumento, um polinómio mónico, isto é, z_n é integral sobre $B_{n-1} := k[z_1, \ldots, z_{n-1}]$. Continuando desta maneira, obtemos uma cadeia de extensões reciprocamente integrais $B := B_{n_0} \subseteq B_{n_0+1} \subseteq B_n \subseteq A$ com B puramente transcendental. Pela transitividade da integralidade, Lema 6.4, A é integral sobre B. □

Nullstellensatz

Proposição 6.7. *Sejam* A *e* B *anéis tais que* $B \supseteq A$. *Se* A *e* B *são domínios íntegros e se* B *é integral sobre* A, *então* B *é um corpo se, e tão-somente se,* A *é um corpo.*

Demonstração: Seja A um corpo. Seja y em B. Como B é integral sobre A, existe $y^n + a_{n-1}y^{n-1} + \cdots + a_0$ para $a_{n-1}, \ldots, a_0$ em A com n mínimo entre todas tais equações. Como A é um domínio íntegro, $a_0 \neq 0$. Como A é um corpo,

$$1 = y a_0^{-1}(y^{n-1} + a_{n-1}y^{n-1} + \cdots + a_1)$$

isto é, B é um corpo.

Seja B um corpo. Seja x em A e seja $y = x^{-1}$ em B. Como B é integral sobre A, existe $y^n + a_{n-1}y^{n-1} + \cdots + a_0$ para $a_{n-1}, \ldots, a_0$ em A com n mínimo entre todas tais equações. Logo multiplicação por x^n resulta em $y = x^{-1} = -(a_{n-1} + a_{n-2}x + \cdots + a_0x^{n-1})$ em A; isto é, A é um corpo. □

Dado um anel A, denote por A^* as suas *unidades* ou elementos *invertíveis*, isto é,

$$A^* = \{a \in A : \text{ existe } b \in A \text{ com } ab = 1\}.$$

Lema 6.8. *Se* A *é um domínio, isto é, um anel sem divisores de zero, então, para todo* n*,*

$$A[x_1, \ldots, x_n]^* = A^*.$$

Demonstração: Como A tem nenhum divisor de zero, $\deg fg = \deg f + \deg g$ onde deg denote o grau (total) de um polinómio. Logo $\deg fg \leq 0$ se, e tão-somente se, f e g em A. Em particular, se f é invertível, então f em A. □

Teorema 6.9 (Lema de Zariski). *Seja* K *uma extensão de um corpo* k*. Se* K *finitamente gerado como álgebra sobre* k*, então* K *é (uma extensão de corpos) algébrica sobre* k*.*

Demonstração: Pela normalização de Noether, K é uma integral extensão finita de uma álgebra finitamente gerada puramente transcendental $B = k[x_1, \ldots, x_n]$, isto é, $x_1, \ldots, x_n$ são algebricamente independentes sobre k. Como K é uma extensão integral de B e K é um corpo, por Proposição 6.7 B é um corpo. Por Lema 6.8, o anel $B = k[x_1, \ldots, x_n]$ é um corpo se, e tão-somente se, $n = 0$, isto é, $B = k$. Isto é, K é integral, em particular algébrica, sobre k. □

Teorema 6.10 (Versão fraca do Nullstellensatz). *Seja* k *um corpo algebricamente fechado. Sejam* $f_1, \ldots, f_n$ *em* $A := k[x_1, \ldots, x_d]$*. Se* $I = \langle f_1, \ldots, f_n \rangle \subset A$*, então existe um zero comum de* $f_1, \ldots, f_n$*.*

Demonstração: O ideal I é contido em um ideal máximo m. A extensão A/m é um corpo que é uma extensão finita (como álgebra) K de k. Pelo Lema de Zariski, K é uma extensão algébrica. Como k é algebricamente fechado, $K = k$.

Seja $\phi : A \to A/m = k$ a aplicação de quociente. Logo

$$z := \phi(x) = (\phi(x_1), \ldots, \phi(x_d))$$

tem entradas em k e satisfaz para todo $f = f_1, \ldots, f_n$ que

$$f(z) = f(\phi(x)) = \phi(f(x)) = 0$$

pois $f_1, \ldots, f_n$ em $I \subseteq m$. □

7. Teoremas de Sylow

Antes de darmos a definição abstrata de um grupo, introduzamos permutações de um conjunto finito como exemplo de um grupo. A noção do grupo surgiu pelo estudo das permutações das raízes de um polinómio para demonstrar a irresolubilidade da quíntica.

Mostraremos

1. que todo subgrupo decompõe um grupo em classes de equivalências da mesma cardinalidade (o Teorema de Lagrange),
2. a cardinalidade de uma órbita divide a do grupo (o Teorema da Órbita).

Logo, já sabemos demonstrar o *Teorema de Cauchy*: Seja G um grupo. Se um número primo p divide #G, então existe um subgrupo P de G com #P = p.

Os *Teoremas de Sylow* generalizam este teorema para subgrupos de quaisquer potência de p.

Permutações

Permutações são funções injetoras $f\colon \mathrm{X} \to \mathrm{X}$ com X finito. Como o domínio e contra-domínio têm a mesma cardinalidade, uma permutação é *bijetora*. Observamos que

- existe uma função $e = \mathrm{id}$ definida por $x \mapsto x$,
- a composição $g \circ f$ de duas funções injetoras $f\colon \mathrm{X} \to \mathrm{X}$ e $g\colon \mathrm{X} \to \mathrm{X}$ é injetora,
- uma função f é bijetora se, e tão-somente se, f pode ser *invertida*, isto é, existe g tal que $f \circ g = \mathrm{id} = g \circ f$.

Logo, as permutações de um conjunto finito formam um *grupo* que *suporemos todos finitos*:

Definição 7.1. Um grupo é um conjunto G com uma operação $\cdot$ sobre $\mathrm{G} \times \mathrm{G}$ que satisfaz

- a lei *associativa*, isto é, $g(hi) = (gh)i$ para todo g, h e i em G,
- a lei do *elemento neutro*, existe e em G tal que $eg = ge = g$ para todo g em G
- a lei da *existência do inverso*, para todo g em G existe h em G, denotado por g^{-1}, tal que $gh = hg = e$.

História

Toda equação polinomial de grau 2,3,4 tem soluções que se exprimem

- pelos seus coeficientes $a_0, a_1, \ldots$ e números racionais,
- sujeitos às operações $+, \cdot$ e $\sqrt[n]{\cdot}$ (para $n = 2,3,4$)

A fórmula

- para $n = 2$, o *completamento do quadrado*, é conhecida há mais de 2000 anos, e
- para $n = 3$ (de *Cardan*) e $n = 4$ (de *Ferrari*) data do século XVI.

Questão. *Há uma fórmula dando as raízes para $n = 5$?*

A História da noção do Grupo começa pela sua introdução por *Evariste Galois* em 1831 para demonstrar a *irresolubilidade* da *Quíntica*, isto é, a inexistência de uma fórmula geral para as soluções de um polinómio $P(X) = X^5 + a_4X^4 + \cdots + a_0$ de quinto grau. Ele observou que

- a resolubilidade da quíntica corresponde a uma propriedade do grupo (chamado de *Galois*) dado por certas permutações do conjunto $R = \{\zeta_1, \ldots, \zeta_5\}$ das (até) cinco raízes de $P(X)$, e
- que existem grupos de Galois que não satisfazem esta propriedade.

Noções Básicas

Denote o *grupo simétrico* por

$$S_n = \{ \text{ todas as permutações sobre } \{1, \ldots, n\}\}.$$

Grupos. Um grupo generaliza a ideia de composição de permutações; o Teorema de Cayley abaixo mostrará que esta intuição tem fundamento matemático:

Definição 7.2. Um subgrupo é um subconjunto de um grupo fechado sob $\cdot$.

Como exemplos existe o subgrupo em G gerado por um subconjunto X definido por

$$\langle X\rangle := \{g_1 \dots g_n \in G : g_1, \dots, g_n \in X^{\pm 1}\}$$

onde $X^{\pm 1} = \{x^{\pm 1} : x \in X\}$. Em particular, por um único elemento g em G, temos

$$\langle X\rangle := \{g^n \in G : n \in \mathbb{Z}\}$$

Note que se G é finito, então basta escolher g_1, …, g_n em X e n em $\mathbb{N}$ porque existe n em $\mathbb{N}$ tal que $g^n = e$.

Definição 7.3. A *ordem* de um grupo é a sua cardinalidade. Se g em G, a *ordem* de g é a ordem de $\langle g\rangle$.

Operações. Pela sua definição, S_n opera sobre $\{1, \dots, n\}$.

Definição 7.4. Denote $G \curvearrowright X$ que G opere sobre X, isto é,

- $ex = x$ para todo x em X, e
- $g \cdot (h \cdot x) = (gh) \cdot x$ para todo g e h em G e x em X.

Por exemplo,

- G opera sobre X = G por traslação $x \mapsto gx$
- G opera sobre X = G por conjugação $x \mapsto gxg^{-1}$
- G opera sobre X = { os subconjuntos de G} por conjugação $S \mapsto gSg^{-1} := \{gsg^{-1} : s \in S\}$.

Teorema 7.5 (Teorema de Cayley). *Todo grupo "é subgrupo" de um grupo simétrico.*

Demonstração: Denote X = G e observa que a aplicação

$$\tau_g : X \ni x \mapsto g \cdot x \in X$$

é invertível por g^{-1}; logo é uma permutação de X. Se #G = n, então $G \hookrightarrow S_n$ por $g \mapsto \tau_g$. □

Resultados Básicos

Define sobre G a relação $\sim$ por

$$g' \sim g \quad \text{se existe } h \in \mathrm{H} \text{ tal que } g' = gh.$$

É uma relação de equivalência; em particular, é transitiva pela lei associativa: Se $g' = gh$ e $g'' = g'h'$, então $g'' = g'(hh')$. Logo G é a união disjunta de #G/#H classes de equivalência de $\sim$.

Definição 7.6. Para um subgrupo H em denote

$$\mathrm{G/H} := \mathrm{G}/\sim$$

o conjunto das classes de equivalência sob a relação $\sim$ definida por $g' \sim g$ se existe h em H com $g' = hg$.

Os seguintes dois teoremas básicos formam o pontapé para estudar as cardinalidades de subgrupos:

Teorema 7.7 (Teorema de Lagrange). *Para um grupo* G *com subgrupo* H*,*

$$\#\mathrm{G} = \#(\mathrm{G/H})\#\mathrm{H}.$$

Demonstração: Cada classe gH tem a cardinalidade #H porque a aplicação $g\cdot\colon \mathrm{H} \to g\mathrm{H}$ definida por

$$h \mapsto g \cdot h$$

é uma aplicação invertível por $g^{-1}\cdot$. □

Corolário 7.8 (Teorema da Estabilização da Órbita). *Se* G *opera sobre* X*, então*

$$\mathrm{G/G}_x \xrightarrow{\sim} \mathrm{G}x$$
$$g\mathrm{G}_x \mapsto gx$$

onde Gx *é a órbita de* x *e* G$_x$ *é o subgrupo em* G *dos elementos que fixam* x*.*

Demonstração: A aplicação G/G$_x \to$ Gx é bijetora pois:

- é bem-definida porque $g\mathrm{G}_x = h\mathrm{G}_x$ se, e tão-somente se, $g^{-1}h$ em G$_x$, logo $gx = g(g^{-1}h)x = hx$.
- é injetora porque $gx = hx$ se, e tão-somente se, $g^{-1}h$ em G$_x$, e
- é sobrejetora pela definição da imagem. □

Teorema de Cauchy e Sylow

O Teorema de Cauchy mostra a existência de um subgrupo para o caso mais elementar de um grupo cuja ordem é um número primo:

Teorema 7.9 (Teorema de Cauchy). *Seja* G *um grupo e* p *um número primo. Se* $p|\#\mathrm{G}$*, então existe subgrupo em* G *de ordem* p*.*

Demonstração: Seja

$$\mathrm{S} = \{(g_1, \ldots, g_p) \text{ em G tais que } g_1 \cdots g_p = e\}.$$

Isto é, $(g_1, \ldots, g_p)$ em S se, e tão-somente se, $g_p = (g_1 \cdots g_{p-1})^{-1}$; logo $\#\mathrm{S} = \#\mathrm{G}^{p-1}$.

Seja t o traslado sobre S definido por $g_1 \mapsto g_2$, …, $g_{p-1} \mapsto g_p$ e $g_p \mapsto g_1$. É invertível (pelo traslado no sentido oposto). Seja T o grupo gerado por t. Temos $\#\mathrm{T} = p$. O número p sendo primo, pelo Teorema da Estabilização da Órbita, ou $\#\mathrm{T}s = 1$, ou $\#\mathrm{T}s = p$.

Decompõe

$$\mathrm{S} = \bigcup \{\mathrm{T}s : s \in \mathrm{S} \text{ com } \#\mathrm{T}s = p\} \cup \bigcup \{\mathrm{T}s : s \in \mathrm{S} \text{ com } \#\mathrm{T}s = 1\}$$

Como $p|\#\mathrm{S}$ e $p|\#\bigcup_{\#\mathrm{T}s=p} \mathrm{T}s$, temos $p|\#\bigcup_{\#\mathrm{T}s=1} \mathrm{T}s$. Temos s em S e $\#\mathrm{T}s = 1$ se, e tão-somente se, $s = (g, \ldots, g)$ com $g^p = e$. Como $\mathrm{P} := \{g \in \mathrm{G} : g^p = e\} \neq \emptyset$ porque e em P, e $p|\#\mathrm{P}$, existe $g \neq e$ em G em P, isto é, tal que $g^p = e$. O grupo $g, g^2, \ldots, g^{p-1}, g^p = e$ é um grupo de ordem p. □

Para um grupo G e um subgrupo H de G, um elemento g em G *normaliza* H se $g\mathrm{H}g^{-1} \subseteq \mathrm{H}$. O *normalizador* de H é $\mathrm{N(H)} = \{g \in \mathrm{G} : g\mathrm{H}g^{-1} = \mathrm{H}\}$. Um subgrupo H é *normal* se N(H) = G; isto é, todo g em G normaliza H. Se H é normal, então a operação natural $\cdot$ sobre o conjunto G/H torna-o em um grupo.

As seguintes três afirmações são chamadas o primeiro, segundo e terceiro Teorema de Sylow:

Teorema 7.10 (Teoremas de Sylow). *Seja* G *um grupo e* p *um número primo.*

(i) *Se* p^k *é a maior potência de* p *que divide* $\#\mathrm{G}$*, então existe um subgrupo* H *em* G *com* $\#\mathrm{H} = p^k$*.*

(ii) *Todos tais subgrupos são conjugados.*

(iii) *O número* n *de tais subgrupos satisfaz* $n \equiv 1 \bmod p$*.*

Demonstração: Seja P um p-subgrupo de G máximo, isto é, o maior subgrupo de G em que a ordem de cada elemento é uma potência de p. Pelo Teorema de Cauchy, a cardinalidade de um p-subgrupo é uma potência de p: Se existisse outro primo $q|\#G$, então existiria um subgrupo H com $\#H = q$.

Temos $\#P = p^k$ se, e tão-somente se, $\#G/\#P \not\equiv 0 \bmod p$. Para demonstrar (i), demonstremos $\#G/\#P \not\equiv 0 \bmod p$:

Seja N o normalizador de P. Temos

$$\#G/\#P = \#G/\#N \cdot \#N/\#P$$

Se $p|\#N/\#P$, então, pelo Teorema de Cauchy, o grupo N/P conteria um subgrupo de ordem p. Logo, a sua pré-imagem seria um p-grupo maior do que P, em contradição à escolha de P.

Demonstremos $p \nmid \#G/\#N$ para concluir que $\#G/\#P \not\equiv 0 \bmod$: Como p é primo, o produto de dois fatores não-nulos módulo p é não-nulo módulo p. Pelo Teorema da Estabilização da Órbita, $\#G/\#N = \#X$ onde

$$X = G \cdot P = \{gPg^{-1} : g \in G\}$$

é a órbita de P sob conjugação de G. Demonstremos mais precisamente

$$\#X \equiv 1 \bmod p;$$

isto demonstrará também (iii) por (ii). O grupo P opera sobre X por conjugação. (Enquanto X tem uma única órbita para G, isto é, a operação de G é transitiva, mas a de P não necessariamente.) Como P é um p-grupo, basta demonstrar pelo Teorema da Estabilização da Órbita que {P} é a única órbita unitária entre as órbitas de P sobre X. Seja $\{gPg^{-1}\}$ outra órbita unitária; isto é, P normaliza gPg^{-1}. Equivalentemente, $g^{-1}Pg$ normaliza P. Logo $Q = Pg^{-1}Pg$ tem imagem não-trivial em $Q \twoheadrightarrow Q/N$. Como P, e igualmente $g^{-1}Pg$, é um p-grupo, Q/N contém pelo Teorema de Cauchy um subgrupo de ordem p. Logo, a sua pré-imagem é um p-grupo de ordem maior do que a de P, em contradição à escolha de P.

Demonstremos (ii); como observado, isto implicará (iii). Seja Q outro p-subgrupo máximo. Em particular, Q opera sobre X e pelo mesmo argumento como usado em (i), existe uma única órbita unitária $\{gPg^{-1}\}$ entre as órbitas de Q sobre X; isto é, Q normaliza gPg^{-1}. Equivalentemente, $g^{-1}Qg$ normaliza P. Se $P \neq g^{-1}Qg$, então $N \supseteq gQg^{-1} \twoheadrightarrow gQg^{-1}P/P$ tem imagem não-trivial. Como Q, e igualmente $PgQg^{-1}$, é um p-grupo, gQg^{-1}/P contém pelo Teorema de Cauchy um subgrupo de ordem p. Logo, a sua pré-imagem é um p-grupo de ordem maior do que a de P, em contradição à escolha de P. □

Lema 7.11. *Seja* G *um grupo. Se* G *é um p-grupo, então* #Z(G) *é não-trivial.*

Demonstração: Pelo Teorema de Estabilização da Órbita aplicado à operação de conjugação de G sobre X = G,

$$\#G = \#Z(G) + \sum\{\text{órbitas não-unitárias }\}.$$

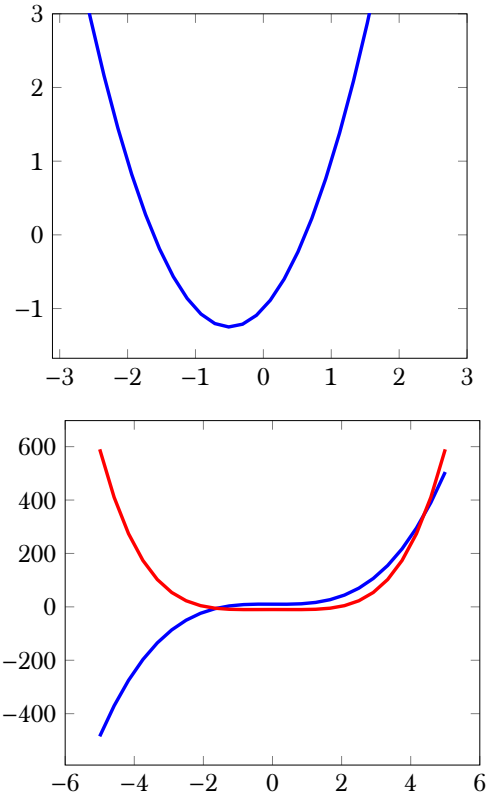
Como G é um p-grupo, necessariamente todas as órbitas não-unitárias têm cardinalidade divisível por p. Logo, $p|\#Z(G)$. Como $\#Z(G) > 0$ porque contém e, necessariamente $\#Z(G) = p^k$ para $k \geq 1$. □

Corolário 7.12. *Seja* G *um grupo e p um número primo. Se* $p^k|\#G$, *então* G *contém um subgrupo de ordem* p^k.

Demonstração: Pelo Teorema de Sylow, existe um p-grupo P de ordem máximo p^K em G. Logo, basta demonstrar: Dado um grupo G de ordem p^K, existe para todo $k = 1,\ldots,K$ um subgrupo H de ordem p^k.

Usemos indução sobre a cardinalidade p^k de G. Se $k = 1$, então, ou e, ou G, são os únicos p-grupos. Seja $k > 1$ e valha a hipótese de indução. Por Lema 7.11, o centro #Z(G) é um p-grupo não-trivial. Pela hipótese de indução para $\bar{G} = G/Z(G)$, existe para todo p^k que divide $\#\bar{G}$ um subgrupo $\bar{H}$ de cardinalidade p^k. Da mesma forma para Z(G) (em vez de $\bar{G}$). Logo, existe para todo p^k que divide #G um subgrupo H de cardinalidade p^k. □

Exemplo 7.13. Todo grupo de ordem 20 é decomponível: Pelo Terceiro Teorema de Sylow, existe pelo menos um subgrupo de ordem 5. O seu número $n \equiv 1 \bmod 5$ e, como órbita da operação de conjugação pelo Teorema da Estabilização da Órbita, $n|20$; logo $n = 1$. Pelo Segundo Teorema de Sylow, todos os subgrupos de ordem 5 são conjugados; logo o único subgrupo de ordem 5 é normal.



8. Teoria de Galois p-ádica

Definição. Um *polinômio* é uma expressão obtida pelas operações + e · sobre uma incógnita X e $\mathbb{Q}$.

Ele pode ser escrito da forma

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$$

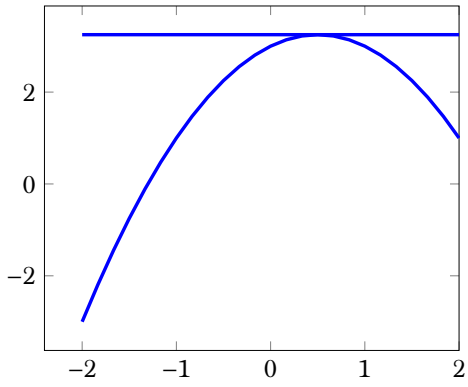
com a_n, a_{n-1}, …, a_0 em $\mathbb{Q}$; fornece uma função $f : \mathbb{R} \to \mathbb{R}$. Por exemplo, a função polinomial $f(x) = x^2 + x - 1$ tem a seguinte curva:

Frequentemente interessa o ponto

- em que duas tais curvas se intersectam, ou
- em que uma tal curva atinge seu máximo:

Achar as coordenadas destes pontos reduz-se à resolução de uma equação polinomial

$$f(X) = X^n + a_{n-1} X^{n-1} + \cdots + a_0 = 0.$$



Isto é, queremos calcular as *raízes* de f, os números $r_1, \ldots, r_n$ tais que $f(r_1)$, $\ldots$, $f(r_n) = 0$.

Questão. *Há uma fórmula para calcular as raízes de f?*

Soluções em grau menor

Quanto maior o grau n do polinômio, tanto mais engenhosidade requerida para calcular a raiz:

- (Completamento do Quadrado) Se $n = 2$, isto é $x^2 + px + q = 0$, então

$$x^2 + px + q = (x + p/2)^2 - p^2/4 + q$$

  e obtemos

$$x = -p/2 \pm \sqrt{p^2/4 - q}. \qquad (*)$$

- (Método de Cardan) Se $n = 3$, isto é $x^3 + ax^2 + bx + c = 0$, então

  (i) Substitua x por $\tilde{x} = x + h$ com $h = -a/3$, para obtermos

$$\tilde{x}^3 + p\tilde{x} + q = x^3 + ax^2 + bx + c.$$

  (ii) Substitua $\tilde{x}$ por $x' + x''$ tal que $x'x'' = -p/3$, para obter

$$x'^3 + x''^3 + (x' + x'')(3x'x'' + p) + q = x'^3 + x''^3 + q.$$

  (iii) Ponha $X' = x'^3$ e $X'' = x''^3$, para obtermos

$$X' + X'' = -q \qquad \text{e} \qquad X'X'' = -p^3/27.$$

Como

$$(X+\alpha)(X+\beta) = X^2 + (\alpha+\beta)X + \alpha\beta,$$

segue que os valores X' e X'' são as soluções de

$$X^2 - qX - p^3/27 = 0.$$

A fórmula $(*)$ para $n = 2$ nos dá para $\tilde{x} = \sqrt[3]{X'} + \sqrt[3]{X''}$,

$$\tilde{x} = \sqrt[3]{-q/2 + \sqrt{q^2/4 + p^3/27}} + \sqrt[3]{-q/2 - \sqrt{q^2/4 + p^3/27}}.$$

- Se $n = 4$, isto é $x^4 + \cdots = 0$, então o *Método de Ferrari* mostra como reduzir a uma equação polinomial de grau 3.

Então toda equação polinomial de grau 2, 3 ou 4 tem soluções que se exprimem

- pelos seus coeficientes $a_0, a_1, \ldots$ e números racionais,
- sujeitos às operações $+,\cdot$ e $\sqrt[n]{\cdot}$ (para $n = 2,3,4$)

Questão. *Há uma fórmula dando as raízes para $n = 5$?*

Permutações de Raízes

Para raízes $r_1, \ldots, r_n$, o seu *Corpo de Números* é

$$\begin{aligned}&\mathbb{Q}(r_1, \ldots, r_n)\\ :=&\{ \text{ todos os números obtidos por } + \text{ e } \cdot \text{ sobre } \mathbb{Q} \text{ e } r_1, \ldots, r_n\}\end{aligned}$$

Por exemplo, para $f(X) = X^4 - 2$ com raízes $\{\pm\sqrt[4]{2}, \pm\sqrt{-1}\sqrt[4]{2}\}$, estes números têm a forma

$$\begin{aligned}\mathbb{Q}(\sqrt{-1}\sqrt[4]{2}) = &\mathbb{Q} \quad \oplus\mathbb{Q}\sqrt[4]{2} \quad \oplus\mathbb{Q}\sqrt[4]{2}^2 \quad \oplus\mathbb{Q}\sqrt[4]{2}^3\\ &\oplus\mathbb{Q}\sqrt{-1} \quad \oplus\mathbb{Q}\sqrt{-1}\sqrt[4]{2} \quad \oplus\mathbb{Q}\sqrt{-1}\sqrt[4]{2}^2 \quad \oplus\mathbb{Q}\sqrt{-1}\sqrt[4]{2}^3,\end{aligned}$$

um espaço vetorial de dimensão 8 sobre $\mathbb{Q}$.

Definição (Corpo Radical). Um corpo de números $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ é *radical* se, para cada $i = 1, \ldots, m$, existe s_i tal que

$$\alpha_i^{s_i} \text{ em } \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1}).$$

Por exemplo

$$r = \sqrt[2]{\sqrt[3]{2} + 5 - \sqrt[2]{12}}.$$

é no corpo de números radical

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[2]{12}, \sqrt[2]{\sqrt[3]{2} + 5 - \sqrt[2]{12}}).$$

Observação (Radical = Formulável). As raízes de um polinômio são num corpo de números radical se, e tão-somente se, são dadas por uma fórmula.

Notamos que,

- o corpo radical pode ser maior que o gerado pelas raízes;
- em particular os geradores podem diferir das raízes.

Questão. *Como as raízes revelam a radicalidade?*

Recordemo-nos de que um *automorfismo* é uma aplicação

- injetora cujo domínio iguala a sua imagem (= *auto*), e
- que respeita as operações + e · (= *homomorfismo*).

Definição (Grupo de Galois). Sejam $r_1, \ldots, r_n$ as raízes de um polinômio irredutível em $\mathbb{Q}[X]$. O seu *Grupo de Galois* é

$$\mathrm{Gal}(\mathbb{Q}(r_1, \ldots, r_n)/\mathbb{Q}) := \{ \text{ todas as } \textit{permutações} \text{ das raízes } r_1, \ldots, r_n \text{ que } \textit{se estendem a automorfismos sobre } \mathbb{Q}(r_1, \ldots, r_n) \ \}$$

Por exemplo para $f(X) = X^4 - 2$ e as suas raízes

$$\{\pm\sqrt[4]{2}, \pm\sqrt{-1}\sqrt[4]{2}\},$$

toda permutação σ que respeita + e · satisfaz

- $\sigma(-\cdot) = -\sigma(\cdot)$,
- $\sigma(\sqrt{-1}) = \pm\sqrt{-1}$,

Logo há 8 permutações no Grupo de Galois dadas

- por $\dagger$ em $\{\pm 1, \pm\sqrt{-1}\}$ dado por $\sqrt[4]{2} \mapsto \dagger\sqrt[4]{2}$, e

$$\left|\begin{array}{c} \sqrt[4]{2} \\ \downarrow \\ \dagger\sqrt[4]{2} \end{array}\right| \left|\begin{array}{c} -\sqrt[4]{2} \\ \downarrow \\ -\dagger\sqrt[4]{2} \end{array}\right| \left|\begin{array}{c} \sqrt{-1}\ \sqrt[4]{2} \\ \downarrow \\ *\sqrt{-1}\dagger\sqrt[4]{2} \end{array}\right| \left|\begin{array}{c} -\sqrt{-1}\ \sqrt[4]{2} \\ \downarrow \\ -*\sqrt{-1}\dagger\sqrt[4]{2} \end{array}\right|$$

- por $*$ em $\{\pm 1\}$ dado por $\sqrt{-1}\sqrt[4]{2} \mapsto *\sqrt{-1}\sqrt[4]{2}$,

da forma que as permutações são dadas pela tabela

Examinamos o corpo radical $\mathbb{Q}(\sqrt[n]{\alpha})$ que é incluso no corpo

$$\mathbb{Q}(\sqrt[n]{\alpha}, \zeta_n) \quad \text{onde } \zeta_n \text{ é uma raiz de 1 de ordem } n$$

gerado pelas raízes do polinômio $f(X) = X^n - \alpha$.

O Grupo de Galois G' de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é descrito por

$$\begin{aligned} G' &\hookrightarrow (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma &\mapsto k \quad \text{determinado por } \sigma(\zeta) = \zeta^k, \text{ e} \end{aligned}$$

o Grupo de Galois G'' de $\mathbb{Q}(\sqrt[n]{\alpha}, \zeta_n)$ sobre $\mathbb{Q}(\zeta_n)$, isto é, que fixa todo elemento em $\mathbb{Q}(\zeta_n)$, é descrito por

$$\begin{aligned} G'' &\hookrightarrow \mathbb{Z}/n\mathbb{Z} \\ \sigma &\mapsto k \quad \text{determinado por } \sigma(\alpha) = \zeta^k\alpha. \end{aligned}$$

Os monomorfismos $G' \hookrightarrow \mathbb{Z}/n\mathbb{Z}^*$ e $G'' \hookrightarrow \mathbb{Z}/n\mathbb{Z}$ unem-se a

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{\alpha}, \zeta_n)/\mathbb{Q}) \hookrightarrow \begin{pmatrix} \mathbb{Z}/n\mathbb{Z}^* & \mathbb{Z}/n\mathbb{Z} \\ & 1 \end{pmatrix}$$

Recordemo-nos da notação $\mathbb{F}_p$ para o corpo finito de p elementos; explicitamente dado por $\mathbb{Z}/p\mathbb{Z}$.

Teorema (Galois). *Seja p um número primo e f em $\mathbb{Q}[X]$ de grau p. Existe uma fórmula para os zeros de f se, e tão-somente se, o Grupo de Galois dos zeros de f é contido em $\begin{pmatrix} \mathbb{F}_p^* & \mathbb{F}_p \\ & 1 \end{pmatrix}$*

Para $p = 5$ e $f(X) = X^5 - X + 1$, todas as permutações das raízes $r_1, \ldots, r_5$ respeitam $+$ e $\cdot$. Isto é, o Grupo de Galois é

$$\{ \text{ todas as permutações de } \mathbb{F}_5 \},$$

o qual não é um subgrupo de $\begin{pmatrix} \mathbb{F}_5^* & \mathbb{F}_5 \\ & 1 \end{pmatrix}$. Logo, não há fórmula.

Um elemento α na extensão E de um corpo F é *algébrico* se existe $P(X) \in F[X]$ tal que $P(\alpha) = 0$. Entre todos os tais P com $P(\alpha) = 0$ existe um único polinômio $M(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ de grau mínimo (ou, equivalentemente, irredutível) e cujo coeficiente dominante é igual a 1, o *polinômio mínimo* de α. A extensão E de um corpo F é *algébrica* se todo elemento é algébrico; equivalentemente, se é gerada por elementos algébricos. Em particular, E é uma extensão algébrica finitamente gerada de F, se, e tão-somente se, o espaço vetorial E tem dimensão finita sobre F; chamemos uma tal extensão de extensão *finita* e denote $[E : F] = \dim_F E$. Se E é gerado por um elemento α e M(X) o seu polinómio mínimo, então $F[\alpha] = F[X]/M(X)F[X]$; em particular, $\dim_F E =$ grau de M(X).

Um polinómio P(X) sobre um corpo **K** é *separável* se se todos os zeros (em uma extensão normal de **K**) de P são diferentes.

Proposição 8.1. *Um polinômio* P(X) *é separável se, e tão-somente se,* P(X) *e* P′(X) *são relativamente primos.*

Demonstração: Se P(X) é separável, então para qualquer zero α, pelo produto $P(X) = (X - \alpha) \cdots Q(X)$, observamos que α não é um zero de P′(X).

Se P(X) não é separável, então $P = (X - \alpha)^2 Q(X)$, e α é um zero de P′(X) também pela regra de produto da derivação. □

Observação 8.2. O maior divisor comum de P e P′ pode ser computado pelo algoritmo de Euclides.

Proposição 8.3. *Os polinômios irredutíveis sobre um corpo k são todos separáveis se, e tão-somente se, a característica de k é* 0. *Mais precisamente, se* **K** *tem característica* 0*, então todo polinômio é separável, e se* **K** *tem característica* $p > 0$*, então o polinômio é separável se, e tão-somente se, em um polinómio em* X^p.

Demonstração: Seja P um polinómio irredutível. Por Proposição 8.1, P é separável se, e tão-somente se, P e P′ são relativamente primos. Caso contrário, P|P′ porque P é irredutível. Logo, como o grau de P′ é menor do que o de P, temos $P' = 0$. Se $P' = 0$, então P e P′ não são relativamente primos, então P não é separável. Isto é, P é separável se, e tão-somente se, $P' \neq 0$. Temos $P' = 0$ se, e tão-somente se, a característica é $p > 0$ e P é um polinômio em X^p. □

Uma elemento α da extensão E algébrica de um corpo F é *separável* se o polinômio mínimo M(X) de α é separável.

Observação 8.4. Se a característica de F é 0, então toda extensão é separável.

A extensão E de um corpo F é *separável* se todo elemento é separável; equivalentemente, se é gerada por elementos separáveis.

Teorema 8.5 (Teorema do Elemento Primitivo). *Uma extensão finita é separável se, e tão-somente se, é gerada por um único elemento separável.*

Proposição 8.6. *A extensão* E *finita de um corpo* F *é separável, se, e tão-somente se, para toda extensão normal* N *que contém* E *existem* $[\mathrm{E} : \mathrm{F}]$ *homomorfismos* $\mathrm{E} \hookrightarrow \mathrm{N}$ *que fixam* F.

Demonstração: Por indução, basta olhar o caso que α seja um elemento separável que gera E. Todo automorfismo que fixa F tem de enviar α a um zero do polinômio mínimo M de α, e o valor de α determina o automorfismo. Logo, existem $\leq \mathrm{E} : \mathrm{F}$ homomorfismos $\mathrm{E} \hookrightarrow \mathrm{N}$. Se E é separável, então existem $\mathrm{E} : \mathrm{F}$ zeros diferentes, e todo zero como valor de α determina um homomorfismo $\mathrm{E} \hookrightarrow \mathrm{N}$. □

Uma extensão E algébrica de um corpo F é *normal* se $\mathrm{P}(\mathrm{X}) \in \mathrm{F}[\mathrm{X}]$ e α em E tais que $\mathrm{P}(\alpha) = 0$, então todos os zeros de $\mathrm{P}(\mathrm{X})$ são em E. Uma extensão de *Galois* é uma extensão normal e separável.

A formulação e demonstração do Teorema Fundamental da Teoria de Galois segue as dadas por Emil Artin nas suas Notre Dame lectures. Notemos que E é Galois:

Teorema 8.7 (Teorema Fundamental da Teoria de Galois). *Seja* F *um corpo. Se* E *é uma extensão de Galois de* F*, isto é,* $\mathrm{E} = \mathrm{F}(a_1, \ldots, a_n)$ *é gerado por elementos distintos tais que* $(\mathrm{X} - a_1) \cdots (\mathrm{X} - a_n)$ *em* $\mathrm{F}[\mathrm{X}]$*, então*

- *o grupo* $\mathrm{G} = \mathrm{Aut}(\mathrm{E}/\mathrm{F})$ *é finito,*
- *são aplicações mutuamente inversas*

$$\begin{aligned} \{\textit{sub-extensões } \mathrm{E}/\mathrm{S}/\mathrm{F}\} &\tilde{\longrightarrow} \{\textit{subgrupos de } \mathrm{G}\} \\ \mathrm{S} &\mapsto \mathrm{Aut}(\mathrm{E}/\mathrm{S}) \\ \mathrm{E}^{\mathrm{H}} &\mapsfrom \mathrm{H} \end{aligned}$$

- *vale* $\mathrm{E} : \mathrm{S} = \#\,\mathrm{Aut}(\mathrm{E}/\mathrm{S})$ *e* $\#\mathrm{H} = \mathrm{E} : \mathrm{E}^{\mathrm{H}}$.

Demonstração: Demonstremos que as aplicações são mutuamente inversas, isto é

$$S = E^{\mathrm{Aut}(E/S)} \quad \text{e} \quad H = \mathrm{Aut}(E/E^H).$$

Como as inclusões valem sempre, bastaria mostrar que as cardinalidades são iguais, isto é,

$$E : S = E : E^{\mathrm{Aut}(E/S)} \quad \text{e} \quad \#H = \mathrm{Aut}(E/E^H).$$

Em vez de demonstrar estas igualdades, demonstremos

$$E : S = \#\,\mathrm{Aut}(E/S) \quad \text{e} \quad \#H = E : E^H \qquad (*)$$

que as implica por

$$E : S = \#\,\mathrm{Aut}(E/S) = E : E^{\mathrm{Aut}(E/S)} \quad \text{e} \quad \#H = E : E^H = \#\,\mathrm{Aut}(E : E^H);$$

e, além disso mostra à terceira (em particular, à primeira) parte da proposição! Logo, basta de demonstrar $(*)$.

Demonstremos $E : S = \#\,\mathrm{Aut}(E/S)$! Por indução, basta de demonstrar que se $\mathbf{K} = S(a_1, \ldots, a_{i-1})$ e $\mathbf{L} = \mathbf{K}(a_i)$ para $i \leq n$, então existem exatamente $\mathbf{L} : \mathbf{K}$ extensões do mergulho $\phi\colon \mathbf{K} \to E$ a $\mathbf{L}$. Ou, equivalentemente, que (a imagem sob ϕ d') o polinômio mínimo P de $a = a_i$ sobre $\mathbf{K}$ tem exatamente $\mathbf{L} : \mathbf{K}$ raízes. Como $\mathbf{L} = \mathbf{K}[X]/P\mathbf{K}[X]$, logo $\mathbf{L} : \mathbf{K}$ = grau de P, isto vale se, e tão-somente se, P tem nenhuma raiz dupla. Isto vale porque P, o polinômio mínimo de a_i, divide o polinômio $(X - a_1) \cdots (X - a_n)$ sem raiz dupla.

Demonstremos $\#H = E : E^H$! Como $H \subseteq \mathrm{Aut}(E/E^H)$ e $\#\,\mathrm{Aut}(E/E^H) = [E : E^H]$ pela primeira parte, basta mostrar $E : E^H = \dim_{E^H} E \leq \#H$. Isto é, quaisquer $b_1, \ldots, b_n$ em E para $n > \#H$ são linearmente dependentes sobre E^H; isto é,

$$b^\perp \cap (E^H)^n \neq 0$$

para $b = (b_1, \ldots, b_n)$ e $\cdot^\perp$ os vetores ortogonais em E^n a $\cdot$ com respeito ao produto escalar.

Se e em $(E^H)^n$ é ortogonal a b, então $he = e$ é ortogonal a hb; logo

$$b^\perp \cap (E^H)^n = (Hb)^\perp \cap (E^H)^n.$$

Seja x um dos vetores diferentes de zero $Hb^\perp$ com o número máximo de entradas iguais a zero. Seja $x_k \neq 0$ uma entrada diferente de zero; após escalamento, suponhamos $x_k = 1$.

Se x não fosse em $(E^H)^n$, isto é, existisse um h em H tal que $y := x - hx \neq 0$, então y em $Hb^\perp$ e $y_k = 0$; em contradição à escolha de x. □

Utilidade do Números p-ádicos

Como $\mathbb{Q}_p$ é completo, as propriedades algébricas são de um ponto de vista da Teoria dos Números mais fáceis do que as de $\mathbb{Q}$: Recordemo-nos de que o Grupo de Galois de uma extensão $\mathbf{E}$ de um corpo $\mathbb{F}$ consiste de todos os automorfismos do corpo $\mathbf{E}$ que fixam $\mathbb{F}$. Pela definição de $\mathbb{Q}_p$ como completamento de $\mathbb{Q}$, a inclusão $\mathbb{Q} \subseteq \mathbb{Q}_p$ é densa. Logo, toda aplicação contínua sobre $\mathbb{Q}_p$ é determinada pelos seus valores sobre $\mathbb{Q}$, isto é,

$$\mathrm{Aut}(\bar{\mathbb{Q}}_p) = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}).$$

Porém, ao contrário de $\mathbb{R}$, o completamento de $\mathbb{Q}$ para $|\cdot|$, cujo grupo de Galois absoluto

$$\mathrm{Gal}(\bar{\mathbb{R}}/\mathbb{R}) = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \bar{\cdot}\}$$

é finito, o grupo de Galois absoluto $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ de $\mathbb{Q}_p$, embora mais fácil do que o de $\mathbb{Q}$, continua a ser infinito.

9. Extensões Ciclotómicas

Seja **K** um corpo. Denote

$$\mu_n := \{x \text{ em } \mathbf{K} \text{ tais que } x^n = 1\}.$$

Pela iterada divisão com resto um polinômio P de grau n tem $\leq n$ raízes: pela divisão com resto $P = Q(X - \alpha) + R$ com grau $R < 1$, isto é, constante; como $P(\alpha) = 0$, necessariamente $R = 0$. Como $x^n = 1$ se e tão-somente se $P(x) = 0$ para $P(X) = X^n - 1$, vale

$$\#\{x \text{ em } \mathbf{K}^* \text{ tal que } x^n = 1\} \leq n$$

Se a característica de **K** é $p \nmid n$ ou 0, então

$$\#\mu_n = n$$

pois a derivada nX^{n-1} é relativamente primo a $X^n - 1$.

Proposição 9.1. *Todo grupo* G *tal que, para toda ordem n,*

$$\#\{g \text{ em G tais que } g^n = 1\} \leq n \quad (\dagger)$$

é cíclico, *isto é, gerado por um elemento.*

Demonstração: Seja x um elemento em G de *ordem* (= o menor número $n > 0$ tal que $x^n = 1$) máxima. Se $n < \#G$, então há por (†) um y em G cuja ordem não divide n. Então a ordem de $z = xy$ é $> n$, em *contradição à escolha* de n. □

Corolário 9.2. *O grupo* μ_n *é cíclico.*

Demonstração: por Proposição 9.1, porque se x tem ordem n, se, e tão-somente se é zero de $P(X) = X^n - 1$; e $P(X)$ tem $\leq n$ = grau P zeros. □

Teoria de Galois

Um elemento α na extensão E de um corpo F é *algébrico* se existe $P(X) \in F[X]$ tal que $P(\alpha) = 0$. Entre todos os tais P com $P(\alpha) = 0$ existe um único polinômio $M(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ de grau mínimo (ou, equivalentemente, irredutível) e normalizado (isto é, cujo coeficiente dominante é igual a 1), o *polinômio mínimo* de α.

Observação. Observemos que, se M é um polinómio mínimo, então todo zero α de M tem M como polinómio mínimo, porque M anula α, é irredutível e normalizado. Logo, pela unicidade, M o polinómio mínimo de α.

Injetividade

Seja ζ_0 um gerador de μ_n e P o seu polinômio mínimo.

Lema 9.3. *Todos os zeros de* P *são geradores de* μ_n.

Demonstração: Se ζ não é gerador de μ_n, então ζ é zero de um polinômio $X^d - 1$ para $d \mid n$. Logo, o seu polinómio mínimo M divide $X^d - 1$. Se $P(\zeta)$ fosse 0, então, pela observação, $P = M|X^d - 1$. Em particular, todos os zeros de P estariam em μ_d; contradição a ζ_0 ser zero de P! Logo $P(\zeta) \neq 0$. □

Seja $\mathbb{Z}/n\mathbb{Z}$ o "menor" anel tal que $n \mapsto 0$, isto é, se A tal que $n \mapsto 0$, então existe $\mathbb{Z}/n\mathbb{Z} \to A$. Explicitamente, $\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} : n \in \mathbb{Z}\}$. Seja

$$\mathbb{Z}/n\mathbb{Z}^* = \{\text{todas as unidades em } \mathbb{Z}/n\mathbb{Z}\}.$$

e seja a *função de Euler* $\phi\colon \mathbb{N} \to \mathbb{N}$ dada por

$$n \mapsto \#\mathbb{Z}/n\mathbb{Z}^*.$$

Proposição 9.4 (Injetivade do homomorfismo). *Temos o mergulho*

$$\begin{aligned} \mathrm{Gal}(\mathbf{K}(\mu_n)/\mathbf{K}) &\hookrightarrow \mathbb{Z}/n\mathbb{Z}^* \\ \sigma &\mapsto k \text{ onde } \sigma(\zeta) = \zeta^k \end{aligned}$$

para um gerador ζ *de* μ_n.

Demonstração: Se P é o polinômio mínimo de ζ, então todo automorfismo σ em $\mathrm{Gal}(\mathbf{K}(\mu_n)/\mathbf{K})$ permuta os zeros de P, isto é, por Lema 9.3, permuta os geradores de μ_n. Como $\mu_n = \mathbb{Z}/n\mathbb{Z}$, e

$$\{\text{geradores de } \mathbb{Z}/n\mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}^*,$$

temos

$$\mathbb{Z}/n\mathbb{Z}^* \xrightarrow{\sim} \{\text{ geradores de } \mu_n\}$$

dado por $k \mapsto \zeta^k$ para um gerador ζ de μ_n. Logo, o homomorfismo é bem-definido.

É injetor porque ζ gera μ_n e por isso todo homomorfismo σ de $\mathbf{K}(\mu_n)$ que fixa $\mathbf{K}$ é determinado pela imagem $\sigma(\zeta)$. □

Sobrejetividade

Recordemo-nos de que $\mathbb{Z}$ é um domínio euclidiano, em particular, existe o maior divisor comum. Como $\mathbb{Z}^* = \{\pm 1\}$, definimo-lo pelo maior divisor comum positivo.

Definição 9.5. Um polinómio não-nulo $f(x)$ em $\mathbb{Z}[x]$ é *primitivo* se o maior divisor comum dos seus coeficientes é (associado a) 1.

Lema 9.6. *Sejam f e g em $\mathbb{Z}[x]$. Se f e g são primitivos, então fg é primitivo.*

Demonstração: Por contraposição: Seja fg não primitivo, isto é, existe p em $\mathbb{Z}$ que divide todos os coeficientes de fg, isto é, tal que

$$\overline{fg} = \bar{f}\bar{g} = 0 \in \mathbb{Z}/p\mathbb{Z}[x]$$

onde $\overline{fg}$, $\bar{f}$ e $\bar{g}$ denotem as reduções de fg, f e g módulo p, isto é, os polinómios cujos coeficientes são as reduções módulo p dos coeficientes de fg, f e g. Logo, como $\mathbb{Z}/p\mathbb{Z}$ é um domínio íntegro, ou $\bar{f}$, ou $\bar{g}$ é zero. Em particular, não ambos, f e g são primitivos. □

Proposição 9.7. *Seja f em $\mathbb{Z}[x]$. Se f é não-constante e primitivo, e se $f(x) = g(x)h(x)$ para $g(x)$ e $h(x)$ em $\mathbb{Q}[x]$, então $g(x)$ e $h(x)$ em $\mathbb{Z}[x]$.*

Demonstração: Seja $f = gh$ com f, g em $\mathbb{Q}[x]$. Logo, existem d e e em $\mathbb{Z}$ tais que

$$d \cdot f(x) = e g_0(x) h_0(x)$$

com g_0 e h_0 em $\mathbb{Z}[x]$ primitivos. Por Lema 9.6 $g_0(x)h_0(x)$ é primitivo. Como $f(x)$ é primitivo e não-constante, necessariamente $d = e$. Isto é, $f(x)$ é redutível em $\mathbb{Z}[x]$. □

Corolário (Lema de Gauss). *Seja f em $\mathbb{Z}[x]$. Se f não é constante e primitivo, então f é (ir)redutível em $\mathbb{Z}[x]$ se, e tão-somente se, f é (ir)redutível em $\mathbb{Q}[x]$.*

Demonstração: Se f é redutível em $\mathbb{Z}[x]$, então a fortiori em $\mathbb{Q}[x]$.

A implicação inversa é Proposição 9.7. □

Seja ζ uma raiz primitiva em μ_n e $m(x)$ o seu polinómio mínimo em $\mathbb{Q}[x]$. Por Lema 9.3,

$$\{ \text{ zeros de } m(x)\} \subseteq \{ \text{ raízes primitivas em } \mu_n\}.$$

Por Proposição 9.4, temos

$$\deg m(x) = \mathbb{Q}(\zeta) : \mathbb{Q} = \#\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \leq \#\mathbb{Z}/\mathbb{Z}^* = \phi(n).$$

Temos #{ raízes de $m(x)$ } $\leq \deg m(x)$. Mostraremos

$$\#\{ \text{ raízes de } m(x) \} \geq \phi(n)$$

para concluir $\mathbb{Q}(\zeta) : \mathbb{Q} = \phi(n)$.

Lema 9.8. *Tem-se*

$$\prod_{\zeta \in \mu_n - \{1\}} 1 - \zeta = n.$$

Demonstração: Tem-se

$$\prod_{\zeta \in \mu_n - \{1\}} X - \zeta = X^n - 1/X - 1 = X^{n-1} + \cdots + X + 1.$$

Ao substituirmos X por 1, obtemos o resultado. □

Lema 9.9. *Seja p um número primo e ζ em μ_n. Se $p \nmid n$, então $\zeta^i \equiv 1 \bmod p$ implica $\zeta^i = 1$.*

Demonstração: Por contraposição, mostremos equivalentemente que se $\zeta^i - 1 \neq 0$, então $p \nmid \zeta^i - 1$. Como $p \nmid n$, por Lema 9.8,

$$\prod_{\zeta \in \mu_n - \{1\}} (1 - \zeta) = n \not\equiv 0 \bmod p.$$

Logo $1 - \zeta \not\equiv 0 \bmod p$ para todo $\zeta \neq 1$ em μ_n; em particular, para todo ζ^i. □

Como $m(x)$ é mínimo, $m(x) | X^n - 1$. Isto é, existe $h(x)$ em $\mathbb{Q}[x]$ tal que $X^n - 1 = m(x)h(x)$.

Proposição 9.10. *Seja ζ uma raiz de $m(x)$ e $X^n - 1 = m(x)g(x)$ e p um número primo. Se ζ^p é uma raiz de $h(x)$, então $p | n$.*

Demonstração: Como $X^n - 1$ é primitivo e não-constante, pelo Lema de Gauss, mais exatamente Proposição 9.7, $m(x)$ e $g(x)$ em $\mathbb{Z}[x]$. Se $h(\zeta^p) = 0$, então

$$0 = h(\zeta^p) \equiv h^{(p)}(\zeta^p) \equiv h(\zeta)^p \bmod p$$

onde $h^{(p)}(x)$ é o polinómio cujos coeficientes são as p-ésimas potências dos de $h(x)$. Logo, $X^n - 1 = \bar{m}(x)\bar{g}(x)$ em $\mathbb{Z}/p\mathbb{Z}[x]$ tem a raiz dupla ζ; equivalentemente, $n(\zeta^{n-1} - 1) \equiv 0 \bmod p$.

Como ζ é uma raiz de $m(x)$, em particular primitiva por Lema 9.3, em particular, $\zeta^{n-1} \neq 1$. Se $p \nmid n$, então, por Lema 9.9, $\zeta^{n-1} \not\equiv 1 \bmod p$. Como $\mathbb{Z}/p\mathbb{Z}$ é domínio íntegro, segue $n \equiv 0 \bmod p$; isto é, $p|n$; contradição a $p \nmid n$! Logo $p|n$. □

Corolário 9.11. *Temos*

$$\#\{ \textit{ raízes de } m(x) \} = \phi(n).$$

Demonstração: Seja ζ uma raiz de $m(x)$. Por Proposição 9.10, para todo primo p que não divide n, também ζ^p é uma raiz de $m(x)$. Como tais p geram o grupo multiplicativo $\mathbb{Z}/n\mathbb{Z}^*$ e

$$\mathbb{Z}/n\mathbb{Z}^* \xrightarrow{\sim} \{\text{raízes primitivas em } \mu_n\},$$

logo

$$\{ \text{ raízes de } m(x) \} = \{\text{raízes primitivas em } \mu_n\}.$$

Corolário 9.12. *Temos*

$$\mathbb{Q}(\zeta) : \mathbb{Q} \geq \phi(n).$$

Demonstração: Temos

$$\mathbb{Q}(\zeta) : \mathbb{Q} = \deg m(x) \geq \#\{ \text{ raízes de } m(x) \} = \phi(n);$$

a última igualdade por Corolário 9.11. □

Corolário 9.13 (Sobrejetividade do homomorfismo sobre $\mathbb{Q}$). *O homomorfismo entre grupos*

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) &\hookrightarrow \mathbb{Z}/n\mathbb{Z}^* \\ \sigma &\mapsto k \textit{ onde } \sigma(\zeta) = \zeta^k \end{aligned}$$

para um gerador ζ de μ_n é sobrejetor.

Demonstração: Por Proposição 9.4 o homomorfismo é injetor. Por Corolário 9.12 e pelo Teorema Fundamental da Teoria de Galois, o lado esquerdo tem cardinalidade $\phi(n)$ = a cardinalidade do lado direito. Logo, o homomorfismo é bijetor. □

Cálculo da Função de Euler

Para calcular $\phi(n)$, decomponhamos n nos seus fatores primos.

Definição 9.14. Seja A um anel. Para dois elementos a e b,

- um *maior divisor comum* $d = \mathrm{mdc}(a,b)$ é um divisor de a e b, tal que, se e é outro divisor de a e b, então d divide e.
- um *menor múltiplo comum* $m = \mathrm{mmc}(a,b)$ é um múltiplo de a e b, tal que, se n é outro múltiplo de a e b, então n é múltiplo de m.

Um elemento a em A é um *divisor de zero* se existe b em A não-nulo tal que $ab = 0$. A é um *domínio íntegro* se não tem divisores de zero.

Dois elementos a e b em A são *associados* se existe ϵ em A^* tal que $b = \epsilon a$.

Observação 9.15. Seja A um anel. Se A é um domínio íntegro, então o maior divisor comum e o menor múltiplo comum de dois elementos a e b em A é univocamente determinado exceto associação, isto é,

- dois maiores divisores d' e d'' comuns são associados, e
- dois menores múltiplos m' e m'' comuns são associados.

Demonstração: Se d' e d'' são dois maiores divisores, então, por definição, $d'|d''$ e $d''|d'$, isto é, existem u e v em A tal que $d' = uvd'$ e $d'' = uvd''$. Como A não tem divisores de zero, ou d' e d'' são nulos, ou $uv = 1$; em ambos os casos, d' e d'' são associados.

Da mesma maneira para dois menores múltiplos comuns. □

Um anel A é um *domínio euclidiano* se existe uma *função de grau* $v\colon A \to \mathbb{N} \cup \{-\infty\}$ tal que $v(0) = -\infty$ e para todo a e b não-nulo com $v(b) \leq v(a)$ existem q e r tais que

$$a = bq + r \quad \text{com } v(r) < v(b).$$

Exemplo 9.16. Anéis euclidianos são

(i) o anel $\mathbb{Z}$ com $v = |\cdot|$,

(ii) o anel $\mathbb{Z}[i]$ com $v(a + bi) = a^2 + b^2$, e

(iii) o anel polinomial A[X] para um domínio íntegro A com $v(f)$ definido pelo grau de f.

Lema 9.17. *Se* A *é um domínio euclidiano, então* A *é um domínio principal.*

Demonstração: Seja I um ideal em A e i_0 em I um elemento não-nulo em I de grau mínimo. Para todo $a = i$ em I e $b = i_0$ existem q e r tais que

$$a = qb + r \quad \text{com } v(r) < v(b).$$

Em particular, r em I. Como $v(r) < v(b)$ e $v(b) = v(i_0)$ é mínimo, $r = 0$. Isto é, $\mathrm{I} = \langle i_0 \rangle$. □

O maior divisor comum e o menor múltiplo comum de dois elementos a e b em um anel A não sempre existe. Porém, se A é um domínio de fatoração única, então existe, sim. Um domínio principal é em particular um de fatoração única; a seguinte Proposição 9.18 mostra diretamente que o maior divisor comum e o menor múltiplo comum em um domínio principal sempre existe:

Proposição 9.18. *Seja* A *um anel. Se* A *é um domínio principal, então*

$$\langle a \rangle + \langle b \rangle = \langle \mathrm{mdc}(a,b) \rangle \quad e \quad \langle a \rangle \cap \langle b \rangle = \langle \mathrm{mmc}(a,b) \rangle$$

Demonstração: Como A é um domínio principal, existe d em A tal que $\langle a \rangle + \langle b \rangle = \langle d \rangle$. Em particular, $d|a, b$. Logo,

$$\langle \mathrm{mdc}(a,b) \rangle \subseteq \langle d \rangle = \langle a \rangle + \langle b \rangle$$

Como mdc(a,b) pertence a $\{d \in \mathrm{A} : d|a, b\}$,

$$\langle a \rangle + \langle b \rangle \subseteq \langle \mathrm{mdc}(a,b) \rangle.$$

Concluímos

$$\langle \mathrm{mdc}(a,b) \rangle \subseteq \langle a \rangle + \langle b \rangle \subseteq \langle \mathrm{mdc}(a,b) \rangle,$$

logo $\langle a \rangle + \langle b \rangle = \mathrm{mdc}(a, b)$.

Semelhantemente: Como A é um domínio principal, existe m em A tal que $\langle a \rangle \cap \langle b \rangle = \langle m \rangle$. Em particular, $a, b|m$. Logo,

$$\langle \mathrm{mmc}(a,b) \rangle \supseteq \langle m \rangle = \langle a \rangle \cap \langle b \rangle$$

Como mmc(a,b) pertence a $\{m \in \mathrm{A} : a, b|m\}$,

$$\langle a \rangle \cap \langle b \rangle \supseteq \langle \mathrm{mmc}(a,b) \rangle.$$

Concluímos

$$\langle \mathrm{mmc}(a,b) \rangle \subseteq \langle a \rangle \cap \langle b \rangle \subseteq \langle \mathrm{mmc}(a,b) \rangle,$$

logo $\langle a \rangle \cap \langle b \rangle = \mathrm{mmc}(a, b)$. □

Nota. O maior divisor comum de dois números em um domínio euclidiano pode ser calculado explicitamente pelo *Algoritmo de Euclides Estendido*; vide Teorema 4.9.

Dois ideais I e J são *co-primos* (ou *relativamente primos*) se todo ideal que contêm I e J necessariamente contém 1, isto é, se $\mathrm{I}+\mathrm{J}=\mathrm{A}$.

Lema 9.19. *Seja* A *um anel e sejam* I *e* J *ideais em* A. *Se* I *e* J *são relativamente coprimos, então*

$$\mathrm{I}\cap\mathrm{J}=\mathrm{IJ}.$$

Demonstração: Basta demonstrar que se $\mathrm{I}+\mathrm{J}=\mathrm{A}$, então

$$\mathrm{I}\cap\mathrm{J}\subseteq\mathrm{IJ}.$$

Seja a em $\mathrm{I}\cap\mathrm{J}$ e $1=i+j$. Como ai e aj são em IJ, logo $a=ai+aj$ é em IJ. □

Teorema 9.20 (Teorema Chinês dos Restos). *Seja* A *um anel e sejam* I *e* J *ideais em* A. *Se* I *e* J *são relativamente primos, então*

$$\mathrm{A}/\mathrm{IJ}\xrightarrow{\sim}\mathrm{A}/\mathrm{I}\times\mathrm{A}/\mathrm{J}.$$

Demonstração: A aplicação é injetora, porque $\mathrm{A}\to\mathrm{A}/\mathrm{I}\times\mathrm{A}/\mathrm{J}$ tem núcleo $\mathrm{I}\cap\mathrm{J}=\mathrm{IJ}$ por Lema 9.19.

A aplicação é sobrejetora, porque I e J são relativamente primos se, e tão-somente se, $\mathrm{I}+\mathrm{J}=\mathrm{A}$, isto é, existem i em I e j em J tal que $i+j=1$. Como a imagem é um ideal sobre A, é suficiente mostrar que os seus geradores (1,0) e (0,1) são valores. Calculamos

$$j\equiv i+j=1 \bmod \mathrm{I} \quad \text{e} \quad j\equiv 0 \bmod \mathrm{J}$$

e

$$i\equiv 0 \bmod \mathrm{I} \quad \text{e} \quad i\equiv i+j=1 \bmod \mathrm{J}.$$

Corolário 9.21 (Teorema Chinês dos Restos para os Inteiros). *Se m e n são coprimos, isto é* $\mathrm{mdc}(m,n)=1$, *então*

$$\mathbb{Z}/mn\mathbb{Z}=\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}.$$

Demonstração: Como $\mathbb{Z}$ é um domínio euclidiano, em particular, um domínio principal, as condições de Proposição 9.18 são satisfeitas e

$$\langle m\rangle\langle n\rangle=\langle \mathrm{mmc}(m,n)\rangle=\langle mn\rangle \quad \text{e} \quad \langle m\rangle+\langle n\rangle=\langle \mathrm{mdc}(m,n)\rangle=\langle 1\rangle.$$

Por Teorema 9.20

$$\mathbb{Z}/\langle mn\rangle\mathbb{Z}=\mathbb{Z}/\langle m\rangle\langle n\rangle\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}/\langle m\rangle\mathbb{Z}\times\mathbb{Z}/\langle n\rangle\mathbb{Z}.$$

Corolário 9.22. *Se $n = p_1^{e_1} \cdots p_n^{e_n}$ é a decomposição de n em fatores primos, então*

$$\mathbb{Z}/n\mathbb{Z}^* \xrightarrow{\sim} \mathbb{Z}/p_1^{e_1}\mathbb{Z}^* \times \cdots \times \mathbb{Z}/p_n^{e_n}\mathbb{Z}^*.$$

Demonstração: Por indução, usando que os produtos cujos fatores são dados por dois conjuntos de números primos têm um divisor comum se, e tão-somente se, a interseção dos dois conjuntos não é vazia, obtemos por Corolário 9.21

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{e_n}\mathbb{Z}.$$

Como π é um isomorfismo de anéis, em particular é um homomorfismo multiplicativo; logo

$$\mathbb{Z}/n\mathbb{Z}^* \xrightarrow{\sim} \mathbb{Z}/p_1^{e_1}\mathbb{Z}^* \times \cdots \times \mathbb{Z}/p_n^{e_n}\mathbb{Z}^*.$$

Lema 9.23. *Um elemento x em $\mathbb{Z}/p^n\mathbb{Z}$ é uma unidade se, e tão-somente se, p não divide x. Isto é,*

$$\mathbb{Z}/p^n\mathbb{Z}^* = \{x + y \in \mathbb{Z}/p^n\mathbb{Z} : x = 1, \ldots, p-1 \text{ e } y = 1, \ldots, p^{n-1}\}.$$

Demonstração: Um elemento x é uma unidade em um anel A se, e tão-somente se, o endomorfismo dado pela multiplicação $m\colon a \mapsto x \cdot a$ é sobrejetor. Se A é finito, então m é sobrejetor se, e tão-somente se, m é injetor. O endomorfismo dado pela multiplicação $m\colon a \mapsto x \cdot a$ é injetor se, e tão-somente se, x não divide 0.

Como $A = \mathbb{Z}/p^n\mathbb{Z}$ é finito, e x divide 0 se, e tão-somente se, p divide x, concluímos que x é uma unidade se, e tão-somente se, p não divide x. □

Corolário 9.24. *Se $n = p_1^{e_1} \cdots p_n^{e_n}$ é a decomposição de n em fatores primos, então*

$$\phi(n) = (p_1 - 1)p_1^{e_1-1} \cdots (p_n - 1)p_n^{e_n-1}.$$

Teoria do Corpo de Classes p-ádico

A *Teoria do Corpo de Classes* classifica as representações de dimensão 1 de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Todas elas fatoram através do seu quociente abeliano máximo. Vamos descrevê-lo:

Teorema (Kronecker-Weber). *A extensão* abeliana máxima *de $\mathbb{Q}_p$ (= a maior extensão em $\overline{\mathbb{Q}}_p$ cujo Grupo de Galois é abeliano) é $\mathbb{Q}_p(\mu)$ com*

$$\mu = \bigcup_{n\in\mathbb{N}} \mu_n \qquad e \qquad \mu_n = \{ \text{ todos os } \zeta \text{ em } \overline{\mathbb{Q}}_p \text{ tal que } \zeta^n = 1\}$$

as raízes da unidade. Equivalentemente, com $\cdot^{\mathrm{ab}}$ o maior quociente abeliano,

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)^{\mathrm{ab}} = \mathrm{Gal}(\mathbb{Q}_p(\mu)/\mathbb{Q}_p)$$

Com

$$\mu_{p^\infty} = \bigcup_{n\in\mathbb{N}} \mu_{p^n} \quad \text{e} \quad \mu_{\not p} = \bigcup_{n\in\mathbb{N}} \mu_{p^n-1},$$

vale

$$\mathbb{Q}_p(\mu) = \mathbb{Q}_p(\mu_{p^\infty}) \otimes \mathbb{Q}_p(\mu_{\not p}).$$

Tem-se

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p) &\xrightarrow{\sim} \mathbb{Z}/p^n\mathbb{Z}^* \\ \sigma &\mapsto k \quad \text{com } \sigma(\zeta) = \zeta^k \text{ para } \zeta \text{ gerador de } \mu_{p^n} \end{aligned}$$

e

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n-1})/\mathbb{Q}_p) &\xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \\ \sigma &\mapsto k \quad \text{com } \sigma = \phi^k \text{ para } \phi = \cdot^p \text{ Frobenius} \end{aligned}$$

Logo

$$\mathrm{Gal}(\mathbb{Q}_p(\mu)/\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p^* \times \widehat{\mathbb{Z}} = \widehat{\mathbb{Q}}_p^*$$

Definimos o *Grupo de Weil* $\mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ pela imagem inversa

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)^{\mathrm{ab}} & \xrightarrow{\sim} & \mathbb{Z}_p^* \times \widehat{\mathbb{Z}} = \widehat{\mathbb{Q}}_p^* \\ \bigcup & & \bigcup \\ \mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)^{\mathrm{ab}} & \xrightarrow{\sim} & \mathbb{Z}_p^* \times \mathbb{Z} = \mathbb{Q}_p^* \end{array}$$

A imagem inversa de $\mathbb{Q}_p = \mathbb{Z}_p^* \times \widehat{\mathbb{Z}}$ sob o isomorfismo $\mathrm{Gal}(\mathbb{Q}_p(\mu)/\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p^* \times \widehat{\mathbb{Z}} = \widehat{\mathbb{Q}}_p^*$ é o *Grupo de Weil* $\mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Seja $\mathbf{K}$ um *corpo de números p-ádicos*, isto é, uma extensão finita de $\mathbb{Q}_p$ e seja V um $\mathbf{K}$-espaço vetorial de dimensão finita. Investiguemos as ações sobre V quando $\dim \mathrm{V} = 1$:

Teorema (Corpo de Classes). *Para* $\mathbf{K}$ *corpo de números p-ádicos,*

$$\mathrm{Gal}(\overline{\mathbf{K}}/\mathbf{K})^{\mathrm{ab}} \xrightarrow{\sim} \widehat{\mathbf{K}}^*.$$

Corolário (Langlands para $\dim \mathrm{V} = 1$). *Dado um corpo topológico e* V *um espaço vetorial de dimensão* 1*, há um espaço vetorial* B *tal que "naturalmente"*

$$\left\{ \begin{array}{c} \textit{representações contínuas} \\ \mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \mathrm{V} \end{array} \right\} \quad \overleftrightarrow{\sim} \quad \left\{ \begin{array}{c} \textit{representações contínuas} \\ \mathrm{GL}_1(\mathbb{Q}_p) \curvearrowright \mathrm{B} \end{array} \right\}$$

A. O Lema de Zorn

Uma *ordenação parcial* é uma relação $\leq$ sobre um conjunto X que é

- *reflexiva*, isto é, $x \leq x$,
- *anti-simétrica*, isto é, se $x \leq y$ e $y \leq x$, então $x = y$, e
- *transitiva*, isto é, se $x \leq y$ e $y \leq z$, então $x \leq z$.

Se $x \leq y$, digamos que x é *menor* que y. Denote $x < y$ que $x \leq y$ e $x \neq y$. Denote $y \geq x$ que $x \leq y$, digamos que y é *maior* que x, e denote $y > x$ que $x < y$.

Uma *ordenação total* ou *cadeia* é uma ordenação parcial que satisfaz, além disso, que ou $x \leq y$, ou $y \leq x$.

Um elemento x_0 em X é

- *mínimo* se não existe $x < x_0$ em X, e
- *máximo* se não existe $x > x_0$ em X.

Um elemento x_0 em X é

- o *menor* elemento se $x_0 \leq x$ para todo x em X, e
- o *maior* elemento se $x_0 \geq x$ para todo x em X.

Se X é totalmente ordenado, então todo elemento mínimo é o menor elemento e todo elemento máximo é o maior elemento.

Uma *boa ordenação* é uma ordenação total tal que todo subconjunto não-vazio tem um menor elemento.

Seja Y um subconjunto de X. Um elemento x em X é

- uma cota *inferior* se $x \leq y$ para todo y em Y, e
- uma cota *superior* se $x \geq y$ para todo y em Y.

Se X é bem-ordenado e existe uma cota superior de Y que não pertence a Y, então existe um *supremo* s de Y, uma menor cota superior entre todas as cotas superiores de Y que não pertence a Y, e $Y = \{x \in X : x < s\}$.

Um subconjunto Y é um *segmento inicial* (ou *fechado*) em um conjunto parcialmente ordenado X, se, para todo y em Y, se $x \leq y$, então x em Y. Denote $X \leq Y$ que X é um segmento inicial em Y (e $Y \geq X$ que $X \leq Y$), e $X < Y$ que $X \leq Y$ e $X \neq Y$ (e $Y > X$ que $X < Y$).

Demonstração

A união de uma cadeia de conjuntos bem-ordenados é bem-ordenada:

Lema A.1. *Seja* X *parcialmente ordenado e* $\mathcal{F}$ *uma coleção de subconjuntos de* X *bem-ordenados. Se para todo* C *e* D *em* $\mathcal{F}$*, ou* $C \leq D$*, ou* $C \geq D$*, então* $E = \bigcup \mathcal{F}$ *é bem-ordenado e* $E \geq C$ *para todo* C *em* $\mathcal{F}$.

O Lema de Zorn frequentemente é formulado com uma condição mais restritiva, isto é: Todo subconjunto totalmente ordenado, ao invés de apenas todo subconjunto bem-ordenado (= subconjunto totalmente ordenado cujos subconjuntos não-vazios todos têm um elemento menor), tem uma cota superior. Porém, na prática, esta restrição revela-se irrelevante. Demonstremos a formulação mais geral:

Teorema A.2 (Lema de Zorn). *Dado um conjunto* X *não-vazio e parcialmente ordenado. Se todo subconjunto bem-ordenado tem uma cota superior, então* X *tem um elemento máximo.*

Demonstração (segundo H. Kneser): Suponhamos o contrário, isto é, para cada elemento x em X exista $y > x$. Logo, pela hipótese, para cada subconjunto bem-ordenado $C \subseteq X$ existe um supremo de C que não pertence a C, denotado por $g(C)$. Define um *g-conjunto* como um subconjunto bem-ordenado $C \subseteq X$ tal que todo $c \in C$ é supremo de $\{c' \in C : c' < c\}$, isto é, $c = g(\{c' \in C : c' < c\})$.

Afirmação: Se C e D são g-conjuntos, então, ou $C \leq D$, ou $C \geq D$.

Prova: Seja $W = \bigcup\{B \subseteq X : B \leq C \text{ e } B \leq D\}$. Como todos os subconjuntos B são segmentos iniciais, também W é um segmento inicial; logo $W \leq C$ e $W \leq D$, e W é o maior subconjunto com esta propriedade. Se $W = C$ ou $W = D$, então a demonstração é finalizada. Suponhamos o contrário, isto é, $W < C$ e $W < D$, e sejam c em C e d em D os supremos de W em C respectivamente D, isto é,

$$\{c' \in C : c' < c\} = W = \{d' \in D : d' < d\}.$$

Como C e D são g-conjuntos, $c = g(W) = d$. Põe $W' := W \cup \{g(W)\}$; é um g-conjunto $> W$ que satisfaz $W' \leq C$ e $W' \leq D$: contradição a W ser máximo com esta propriedade!

Põe $W := \bigcup\{$ todos os g-conjuntos$\}$. A união de uma cadeia de g-conjuntos é um g-conjunto: Pela Afirmação as condições de Lema A.1 são satisfeitas, logo W é bem-ordenado. Além disto, como união de g-conjuntos, W é um g-conjunto; é o maior g-conjunto em X. Porém, $W' = W \cup \{g(W)\}$ é um g-conjunto $> W$: contradição a W ser máximo com esta propriedade! □

O Lema de Zorn equivale ao Axioma da Escolha. O nome faz referência ao matemático Max Zorn, mas sua primeira formulação se deve ao matemático polonês Kazimierz Kuratowski.

Uma Aplicação

Como aplicação do *Lema de Zorn*, provemos que *todo espaço vetorial* V *possui uma base*, um subconjunto de vetores linearmente independentes que gera V. O Lema de Zorn fornecerá um subconjunto B de vetores linearmente independentes máximo; provemos que tal B é uma base, isto é, gera V:

Lema A.3. *Seja* V *um espaço vetorial e* B *um subconjunto de vetores linearmente independentes em* V. *Se* B *é máximo, então* B *gera* V.

Demonstração: Seja $x \in \mathrm{V} - \mathrm{B}$ não-nulo. Como B é máximo, o superconjunto próprio de B definido por $\mathrm{B} \cup \{x\}$ contém vetores linearmente dependentes; isto é, existe uma combinação linear $\alpha_1 v_1 + \cdots + \alpha_n v_n + \beta x = 0$ com alguns coeficientes não-nulos. Logo $\beta \neq 0$, caso contrário já B teria tido vetores linearmente independentes. Portanto, $x = \frac{-\alpha_1}{\beta} v_1 + \cdots + \frac{-\alpha_n}{\beta} v_n$. Isto é, B gera V. □

Teorema A.4 (Todo espaço vetorial tem uma base). *Seja* V *um espaço vetorial. Se* L *é um conjunto de vetores linearmente independentes em* V*, então existe um conjunto de vetores linearmente independentes máximo em* V *que contém* L.

Demonstração: Para aplicar o Lema de Zorn, construamos um conjunto e definir uma relação de ordem parcial: Como desejamos aumentar um conjunto de vetores linearmente independentes, definamos

$$\mathrm{X} = \{x \in \mathrm{P(V)} : x \supseteq \mathrm{L} \text{ e } x \text{ consiste de vetores linearmente independentes } \}$$

e equipamos X com a ordem parcial natural dada por $x \leq y$ se $x \subseteq y$. O conjunto X não é vazio, porque $\mathrm{L} \in \mathrm{X}$.

Provemos que todo subconjunto totalmente ordenado de X tem uma cota superior: Seja $\mathrm{T} \subseteq \mathrm{X}$ não-vazio e totalmente ordenado.

Põe $\mathrm{Q} = \bigcup\{x \in \mathrm{T}\}$. Pela sua definição, Q é uma *cota superior*, isto é, $x \subseteq \mathrm{Q}$ para todo $x \in \mathrm{T}$. Para concluir, falta verificar que Q em X, isto é, $\mathrm{L} \subseteq \mathrm{Q}$ e que todos os vetores em Q são linearmente independentes:

Como L é um subconjunto de todo elemento de X, então L é um subconjunto de todo elemento de T. Logo, $\mathrm{L} \subseteq \mathrm{Q}$

Verifiquemos que Q é linearmente independente: Seja $\alpha_1 v_1 + \alpha_2 v_2 + \ldots \alpha_n v_n = 0$ uma combinação linear de elementos distintos de Q. Como Q é uma união de conjuntos, existe para todo $i = 1, \ldots, n$ um x_i em T tal que $v_i \in x_i$. Como T é totalmente ordenado, dentre os x_i existe um deles x_{i_0} que é superconjunto de todos os outros. Logo $v_i \in x_{i_0}$ para todo $i = 1, \ldots, n$; portanto $\alpha_1 v_1 + \alpha_2 v_2 + \ldots \alpha_n v_n = 0$ é uma combinação linear de vetores de x_{i_0}. Como x_{i_0} é um conjunto de vetores linearmente independentes, obtemos $\alpha_1, \ldots, \alpha_n = 0$. Isto é, todos os vetores em Q são linearmente independentes.

Ora se aplica o *Lema de Zorn* ao conjunto X para obter um elemento máximo B. □

História

Kazimierz Kuratowski provou em 1922 [1] uma versão menos genérica do Lema de Zorn (usando conjuntos parcialmente ordenados pela inclusão e fechados relativamente à união arbitrária de cadeias bem-ordenadas). O Lema na sua forma atual (usando qualquer relação de ordem, e usando qualquer cadeia totalmente ordenada) foi proposto independentemente por Max Zorn em 1935. [2] Zorn propôs esta formulação como um novo axioma da teoria dos conjuntos, como um substituto do teorema da bem-ordenação, exibiu algumas das suas aplicações na álgebra. Ele também prometeu mostrar a equivalência entre o seu lema e o *axioma da escolha* em outro artigo, mas nunca o escreveu.

[1] Casimir Kuratowski, *Une méthode d'élimination des nombres transfinis des raisonnements mathématiques*, Fundamenta Mathematicae 3 (1922), pp. 76–108. icm

[2] Max Zorn, *A remark on method in transfinite algebra*, Bulletin of the American Mathematical Society 41 (1935), no. 10, pp. 667–670.

Referências

[AM16] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, economy ed., Addison-Wesley Series in Mathematics, Westview Press, Boulder, CO, 2016, For the 1969 original see [MR0242802]. MR 3525784.

[Gal57] D. Gale, *Subalgebras of an algebra with a single generator are finitely generated*, Proc. Amer. Math. Soc. **8** (1957), 929–930. MR 0091273. DOI 10.2307/2033694.