

Grupos e Áneis Livres e a forma canonica de Jordan

Leandro Martins Ciolleti

Capítulo 1

Teoria de Grupos

1.1 Grupos

Iniciaremos estudo de um estrutura algébrica de grande uso na atualidade, Os Grupos, que são utilizados em Física, Computação e outras áreas do conhecimento.

Considere um conjunto G qualquer, vamos agora a primeira definição destas notas.

Definição 1.1.1 *Lei de Composição Interna: dado um conjunto G , uma lei de composição interna em G , é uma função*

$$\begin{aligned} \odot : G \times G &\longrightarrow G \\ (g_1, g_2) &\mapsto g_1 g_2 \end{aligned}$$

no caso em que G possui tal função denotamos (G, \cdot) , apenas para dizer que G é um conjunto com uma lei de composição interna.

Exemplo: O conjunto dos números naturais com a soma $(\mathbb{N}, +)$ é um conjunto com uma lei de composição interna, já (\mathbb{N}, \exp) não é um conjunto com uma lei de composição interna, pois $\exp(1) \notin \mathbb{N}$. Vejamos a definição formal de Grupo.

Definição 1.1.2 *Grupo: é um conjunto com uma lei de composição interna, tal que para $\forall g_1, g_2, g_3 \in G$ temos;*

1. associatividade de \odot , i.e: $(g_1 \odot g_2) \odot g_3 = g_1 \odot (g_2 \odot g_3)$;

2. existe elemento neutro da operação \odot , i.e, $e \in G$ tal que $g \odot e = e \odot g = g$ para todo $g \in G$;
3. para todo elemento $g \in G$, existe $g' \in G$ tal que $g \odot g' = g' \odot g = e$, e este elemento é denotado por g^{-1} .

Exemplos: $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ e o conjunto dos complexos de módulo 1, com a multiplicação complexa, são exemplos de grupos.

1.2 Grupos de Permutações

Discutiremos a respeito de um caso muito especial de grupo, os Grupos de Permutações.

Dado um conjunto X , denotaremos por $|X|$ o número de elementos de X . Se X é um conjunto finito e $\sigma : X \rightarrow X$ uma bijeção ou permutação dos elementos de X , denotaremos por $x\sigma$ a imagem de x por σ . Definimos ainda o *Grupo Simétrico dos Elementos de X* por $\text{Sym}(X) = \{\sigma; \sigma : X \rightarrow X \text{ é uma bijeção}\}$, se $|X| = n \Rightarrow |\text{Sym}(X)| = n!$, e denotamos $\mathbb{S}_n = \text{Sym}(\{1, \dots, n\})$.

Teorema 1.2.1 *Seja $\text{supp}(\sigma) = \{x \in X : x \neq x\sigma\}$ o suporte de σ . Se $\sigma_1, \sigma_2 \in \text{Sym}(X)$ e $\text{supp}(\sigma_1) \cap \text{supp}(\sigma_2) = \emptyset$, então $\sigma_1\sigma_2 = \sigma_2\sigma_1$.*

Demonstração: se $x \in \text{supp}(\sigma_1) \Rightarrow (x\sigma_1)\sigma_2 = x\sigma_1$ e $(x\sigma_2)\sigma_1 = x\sigma_1$, e o resultado segue, analogamente para os casos em que $x \in \text{supp}(\sigma_2)$ e $x \in X \setminus (\text{supp}(\sigma_1) \cup \text{supp}(\sigma_2))$. ■

Uma permutação σ em $\text{Sym}(X)$ é um objeto normalmente denotado por

$$\begin{pmatrix} x_1 & \dots & x_n \\ x_1\sigma & \dots & x_n\sigma \end{pmatrix}.$$

Definimos como a ordem de σ e denotamos por $O(\sigma)$, como sendo o menor número natural n tal que $\sigma^n = \text{id}$, se n é a ordem de σ então a lista

$$(x_i \ x_i\sigma \ x_i\sigma^2 \ \dots \ x_i\sigma^{n-1})$$

é chamada de um n -ciclo, um 2-ciclo é dito uma transposição.

Proposição 1.2.1 *Qualquer ciclo de tamanho k é o produto de $k - 1$ transposições.*

Demonstração: tome $(x_1 \dots x_k)$ e escreva como $(x_1 x_2)(x_1 x_3) \dots (x_1 x_k)$.

■

Teorema 1.2.2 *Toda permutação é o produto de ciclos independentes.*

1.3 Grupos Abelianos Livres

Seja \mathcal{A} um grupo aditivo abeliano, o qual freqüentemente denotaremos por $(\mathcal{A}, +)$.

Definição 1.3.1 *Grupo Abeliano Livre: seja \mathcal{F} um grupo abeliano. Diremos que \mathcal{F} é um grupo abeliano livre se existe $X \subset \mathcal{F}$ tal que para todo grupo abeliano \mathcal{A} e toda aplicação $\phi : X \rightarrow \mathcal{A}$, existe uma única extensão de ϕ a um homomorfismo de \mathcal{F} em \mathcal{A}*

Inserir o Digrama

Dado um conjunto X vamos construir um grupo abeliano livre \mathcal{F} , que chamaremos de grupo abeliano livre \mathcal{F} com base em X . Considere o conjunto $\mathcal{F} = \{f; f : X \rightarrow \mathbb{Z}\}$, vamos munir este conjunto de uma operação $+$ que o tornará um grupo abeliano. Se $f, g \in \mathcal{F}$. Definimos $f + g$ em cada ponto $x \in X$ por $(f + g)(x) = f(x) + g(x)$. É claro que $f + g \in \mathcal{F}$ e que $(\mathcal{F}, +)$ é um grupo abeliano. Agora para cada $x \in X$ definimos a função

$$\delta_x(y) = \begin{cases} 1, & \text{se } y = x \\ 0, & \text{caso contrário.} \end{cases}$$

Agora tome $\overline{X} = \{\delta_x; x \in X\}$. Observe que $\overline{X} \subset \mathcal{F}$. Considere uma aplicação $\phi : \overline{X} \rightarrow \mathcal{A}$ qualquer. Mostraremos agora que ϕ pode ser estendida a um homomorfismo ψ definido em todo \mathcal{F} tomando valores em \mathcal{A} . Com efeito, considere a aplicação $\psi : \mathcal{F} \rightarrow \mathcal{A}$ definida por $\psi(f) = \sum_{x \in X} f(x)\phi(\delta_x)$. Note

que

$$\begin{aligned} \psi(f + g) &= \sum_{x \in X} (f(x) + g(x))\phi(\delta_x) \\ &= \sum_{x \in X} f(x)\phi(\delta_x) + \sum_{x \in X} g(x)\phi(\delta_x) \\ &= \psi(f) + \psi(g) \end{aligned}$$

logo ψ é um homomorfismo. Para todo $\delta_z \in \overline{X}$ temos

$$\psi(\delta_z) = \sum_{x \in X} \delta_z(x)\phi(\delta_x) = \phi(\delta_z)$$

O que mostra que $\psi|_{\bar{X}} = \phi$ e que \mathcal{F} é um grupo abeliano livre.

Acabamos de aprender como construir um grupo abeliano livre a partir de um conjunto X qualquer. Quando $|X| = k < \infty$, denotaremos por F_k o grupo livre obtido pela construção acima. É interessante notar que $F_k \cong \mathbb{Z}^k$. Este fato deve ser demonstrado pelo leitor como exercício. Quando $|X| = \infty$ normalmente não temos um modelo concreto deste grupo. Porém se construímos \mathcal{F} a partir do seguinte conjunto

$$\mathcal{F} = \{f : X \rightarrow \mathbb{Z} : |\{x \in X : f(x) \neq 0\}| < \infty\}$$

segue que podemos enxergar cada elemento de F como uma sequência infinita. Outro fato sobre grupos abelianos livres é que $F_{k_1+k_2} \cong F_{k_1} \oplus F_{k_2}$.

Proposição 1.3.1 *Qualquer subgrupo $\mathcal{A} \subset F_k$ é finitamente gerado.*

Demonstração: demonstraremos por indução em k ;

- se $k = 1$, $F_1 \cong \mathbb{Z}$, todo subgrupo de \mathbb{Z} é cíclico;
- suponhamos verdadeira a proposição para $k - 1$, seja $\mathcal{A} \subset F_k$ e tome $N = \{(0, \dots, 0, n) : n \in F_k\}$, observe ainda que $N \triangleleft F_k$, daí $\frac{F_k}{N} \cong F_{k-1}$, e as classes laterais de N são,

$$f + N = (f_1, \dots, f_{k-1}, f_k) + N = (f_1, \dots, f_{k-1}, 0) + N,$$

agora defina a aplicação $\left\{ \begin{array}{l} \pi : F_k \rightarrow F_{k-1} \\ (f_1, \dots, f_{k-1}, f_k) \mapsto (f_1, \dots, f_{k-1}, 0) \end{array} \right.$, temos que $\pi(\mathcal{A}) \subset F_{k-1}$, que pela hipótese de indução é finitamente gerado, digamos, por $\{b_1, \dots, b_s\}$ e temos $a_i \in \mathcal{A}$ tais que $\pi(a_i) = b_i$, $i = 1, \dots, s$, assim considere $a \in \mathcal{A}$ e observe que

$$\pi(a) = m_1 b_1 + \dots + m_s b_s$$

e que para o elemento $b \in \mathcal{A}$ dado por

$$b = m_1 a_1 + \dots + m_s a_s \in \mathcal{A},$$

temos que $\pi(a) = \pi(b)$. Logo segue da definição de π que $a - b \in N$. É claro da definição de N que temos $N \cong \mathbb{Z}$, e portanto N deve ser gerado por um elemento. Seja c este gerador. Assim podemos afirmar que existe $m \in \mathbb{N}$ tal que $a - b = mc$, e daí tiramos a seguinte igualdade

$a = m_1a_1 + \dots + m_s a_s + mc$. E concluímos por fim que \mathcal{A} é finitamente gerado. ■

É interessante observar que todo conjunto não-vazio de subgrupos de F_k , pelo *Lema de Zorn*, possui um elemento maximal. No entanto, podemos demonstrar tal fato sem evocar o *Lema de Zorn*; pois se $\mathcal{A} = \{\text{subgrupos de } F_k\}$, temos que se $A_1 \in \mathcal{A}$ não é maximal (onde a relação de ordem parcial em \mathcal{A} é A_1 "é subgrupo de..."), então existe $A_2 \supset A_1$, estritamente, se A_2 não é maximal, e assim por diante conseguimos uma cadeia de continência estrita

$$A_1 \subset A_2 \subset A_3 \subset \dots$$

Consideremos agora o conjunto $U = \bigcup_{i=1} A_i$. Como $U \subset F_k$ ele é finitamente gerado. Sejam $\{a_1, \dots, a_s\}$, seu geradores. Claramente cada a_i pertence a algum A_j . Pela definição da cadeia deve existir um $n \in \mathbb{N}$ tal que $\{a_1, \dots, a_s\} \subset A_n$. Mas isto implica que $A_n = A$ e logo $A_n \supseteq A_{n+1} \supset A_n$, uma contradição. ■

Definição 1.3.2 *Grupo Livre de Torção:* dizemos que um grupo \mathcal{A} é livre de torção se $na=0$ implicar $a=0$; equivalentemente, a ordem de todo elemento do grupo é infinita.

Teorema 1.3.1 *Se \mathcal{A} é finitamente gerado e livre de torção, então $A \cong F_k$ para algum k .*

1.4 Soma Direta

Definição 1.4.1 *Soma direta de grupos:* sejam $\mathcal{A}_1, \dots, \mathcal{A}_n$ grupos abelianos, definimos;

$$\mathcal{A} = \mathcal{A}_1 \times \dots \times \mathcal{A}_n = \mathcal{A}_1 \oplus \dots \oplus \mathcal{A}_n = \{(a_1, \dots, a_n) : a_i \in \mathcal{A}_i\},$$

como a soma direta dos grupos $\mathcal{A}_1, \dots, \mathcal{A}_n$.

Podemos tornar o conjunto \mathcal{A} definido acima, um grupo munindo A com as operações de grupo tomadas componente a componente.

Seja \mathcal{A} um grupo abeliano e $B_1, B_2 < \mathcal{A}$, tais que $\{B_1, B_2\}$ é a decomposição direta de \mathcal{A} , i.e, $\mathcal{A} = B_1 + B_2$ e $B_1 \cap B_2 = 0$ defina,

$$\begin{cases} \pi_1 : \mathcal{A} \rightarrow \frac{\mathcal{A}}{B_2} \\ \pi_2 : \mathcal{A} \rightarrow \frac{\mathcal{A}}{B_1} \end{cases}$$

agora defina o homomorfismo;

$$\begin{aligned} \Pi : \quad \mathcal{A} &\longrightarrow B_1 \oplus B_2 \\ a &\mapsto (\pi_1(a), \pi_2(a)), \end{aligned}$$

observe que $\ker \Pi = \ker \pi_1 \cap \ker \pi_2 = \{0\}$, nos diz que Π é injetivo, vejamos que Π é sobrejetivo; qual seria a imagem inversa de $(a_1 + B_2, a_2 + B_1)$? Para ver isto basta escrever $a = a_1 + a_2$ e verificar que $(a_1 + B_2, a_2 + B_1) = \Pi(a_1 + a_2)$, comprovando realmente que Π é sobrejetivo. Logo podemos dizer que Π é um isomorfismo. Utilizando o 2º Teorema dos isomorfismos constatamos que são válidas também as seguintes relações:

$$\overline{B_1} = \frac{\mathcal{A}}{B_1} = B_1 + \frac{B_2}{B_1} \cong \frac{B_2}{B_1 \cap B_2},$$

$$\overline{B_2} = \frac{\mathcal{A}}{B_2} = B_2 + \frac{B_1}{B_2} \cong \frac{B_1}{B_1 \cap B_2},$$

Definição 1.4.2 *Subgrupos Linearmente Independentes:* dado um grupo \mathcal{A} e $\mathcal{A}_1, \dots, \mathcal{A}_n < \mathcal{A}$, dizemos que $\mathcal{A}_1, \dots, \mathcal{A}_n$ são linearmente independentes se

$$a_1 + \dots + a_n = 0, \quad a_i \in \mathcal{A}_i.$$

Então $a_i = 0$ para todo $i=1, \dots, n$; e neste caso $\mathcal{A} = \mathcal{A}_1 + \dots + \mathcal{A}_n$ e $\{\mathcal{A}_1, \dots, \mathcal{A}_n\}$ é decomposição direta de \mathcal{A}

Proposição 1.4.1 *Se $\{\mathcal{A}_1, \dots, \mathcal{A}_n\}$ é decomposição direta de um grupo abeliano \mathcal{A} , então $\mathcal{A} \cong \mathcal{A}_1 \oplus \dots \oplus \mathcal{A}_n$*

Demonstração:

Provaremos este resultado fazendo uma indução em n . Sabemos que a proposição é verdadeira para $n = 1$, suponhamos que a proposição seja verdadeira para $n - 1$. Ponha $\mathcal{A}'_2 = \mathcal{A}_2 + \dots + \mathcal{A}_n$ veja que $\mathcal{A}_1 \cap \mathcal{A}'_2 = 0$, pois se $a \in \mathcal{A}_1 \cap \mathcal{A}'_2 \Rightarrow a = a_2 + \dots + a_n \Rightarrow -a + a_2 + \dots + a_n = 0$. Como $a \in \mathcal{A}_1$ e $\{\mathcal{A}_1, \dots, \mathcal{A}_n\}$ é decomposição direta segue que $a = 0$, portanto $\{\mathcal{A}_1, \mathcal{A}'_2\}$ é decomposição direta de $\mathcal{A} \Rightarrow \mathcal{A} \cong \mathcal{A}_1 \oplus \mathcal{A}'_2$, e pela hipótese de indução $\mathcal{A}'_2 \cong \mathcal{A}_2 \oplus \dots \oplus \mathcal{A}_n$ e o resultado segue. ■

Proposição 1.4.2 *Sejam $\mathcal{A}_1, \dots, \mathcal{A}_n$, grupos abelianos com $B_i < \mathcal{A}_i$, com $\mathcal{A} \cong \bigoplus_{i=1}^n \mathcal{A}_i$ e $B \cong \bigoplus_{i=1}^n B_i$, $B < \mathcal{A}$, então*

$$\frac{\mathcal{A}}{B} \cong \bigoplus_{i=1}^n \frac{\mathcal{A}_i}{B_i}.$$

Demonstração:

Seja $\{\mathcal{A}_1, \dots, \mathcal{A}_n\}$ decomposição direta de \mathcal{A} , $B_i < \mathcal{A}_i$, $B = \sum B_i = \{b_1 + \dots + b_n : b_i \in B_i\}$, então

$$\frac{\mathcal{A}}{B} \supset \frac{\mathcal{A}_i + B}{B} = \overline{\mathcal{A}_i}$$

pelo 2º Teorema dos Homomorfismos, segue

$$\overline{\mathcal{A}_i} = \frac{\mathcal{A}_i + B}{B} \cong \frac{\mathcal{A}_i}{\mathcal{A}_i \cap B},$$

agora devemos mostrar que $\mathcal{A}_i \cap B = B_i$, está claro que $B_i \subset \mathcal{A}_i \cap B$. Reciprocamente, tome $a \in \mathcal{A}_i \cap B \Rightarrow a = b_1 + \dots + b_n \Rightarrow -a + b_1 + \dots + b_n = 0 \Rightarrow b_1 + \dots + (b_i - a) + \dots + b_n = 0 \Rightarrow b_i - a = 0 \Rightarrow a \in B_i$.

Observe que $\sum \overline{\mathcal{A}_i} = \frac{\mathcal{A}}{B} = \{a + B : a \in \mathcal{A}\}$, pois temos $a + B = (a_1 + B) + \dots + (a_n + B)$ com $a_i \in \overline{\mathcal{A}_i}$ e portanto $a_i + B \in \overline{\mathcal{A}_i}$. Que a decomposição é direta segue da fato $(a_1 + B) + \dots + (a_n + B) = B \Rightarrow (a_1 + \dots + a_n) + B = B \Rightarrow a \in B \Rightarrow a_1 + \dots + a_n = b_1 + \dots + b_n \Rightarrow \sum (b_i - a_i) = 0 \Rightarrow a_i \in B$. ■

Capítulo 2

Teoria de Anéis

2.1 Anéis

Um Anel é um conjunto \mathcal{A} com duas operações de composição binária, a saber, uma dita adição e outra a multiplicação dos elementos de \mathcal{A} , denotamos $(\mathcal{A}, +, \cdot)$. Este conjunto, juntamente com estas duas operações, possui as seguintes propriedades:

1. $(\mathcal{A}, +)$ é um grupo abeliano;
2. as duas operações são associativas; isto é, dados $a, b, c \in \mathcal{A} \Rightarrow (a + b) + c = a + (b + c)$ e $(ab)c = a(bc)$;
3. temos a distributividade da multiplicação à esquerda e à direita; i.e $a, b, c \in \mathcal{A} \Rightarrow (a + b)c = ac + bc$; $a(b + c) = ab + ac$;
4. existe elemento neutro da multiplicação; i.e, $\exists e \in \mathcal{A}$ tal que $ae = ea = a \forall a \in \mathcal{A}$

Não restringimos a nossa definição de Anel a anéis comutativos, isto é $ab = ba$ para todo $a, b \in \mathcal{A}$, porém a grande maioria dos resultados que vamos extrair desta estrutura terão como hipótese a comutatividade do anel em questão. Neste texto sempre que a estrutura comutativa for essencial anunciaremos que ela será usada, a menos que o contexto deixe claro.

Definição 2.1.1 *Domínio: Dizemos que um anel A é um Domínio se A é um anel, com a seguinte propriedade. Se $a, b \in \mathcal{A}$ são tais que*

$ab = 0_{\mathcal{A}}$ então, ou $a = 0_{\mathcal{A}}$ ou $b = 0_{\mathcal{A}}$. Onde $0_{\mathcal{A}}$ é o elemento neutro da adição de \mathcal{A} ,

No estudo de grupos, vimos o conceito de subgrupo, analogamente na teoria de anéis temos o conceito de subanel.

Definição 2.1.2 *Subanel:* seja \mathcal{A} um anel, um conjunto $\mathcal{B} \subset \mathcal{A}$ tal que $(\mathcal{B}, +, \cdot)$ é um anel, é dito um subanel de \mathcal{A} , onde $+$ e \cdot são as operações definidas em \mathcal{A}

Definição 2.1.3 *Homomorfismo de Anéis:* sejam \mathcal{A}, \mathcal{B} anéis, considere uma aplicação $f : \mathcal{A} \rightarrow \mathcal{B}$ tal que, para todo $a_1, a_2 \in \mathcal{A}$ tenhamos

$$f(a_1 + a_2) = f(a_1) + f(a_2) \text{ e } f(a_1 a_2) = f(a_1) f(a_2),$$

Uma aplicação com tais propriedades é dita um homomorfismo de anéis.

O núcleo de um homomorfismo é definido como o conjunto $\ker f = \{a \in \mathcal{A} : f(a) = 0\}$, é interessante observar que $\ker f$ é um subanel de \mathcal{A} , mais que isso, $\ker f$ é um ideal de \mathcal{A} , objeto que definimos a seguir.

Definição 2.1.4 *Ideal de um Anel:* ideal de um anel \mathcal{A} , é um subanel \mathcal{I} tal que, se $a \in \mathcal{A}$ e $b \in \mathcal{I}$, então temos que $ab \in \mathcal{I}$ e $ba \in \mathcal{I}$.

Abaixo temos alguns exemplos concretos dos conceitos definidos logo acima. **Exemplo:** $\ker f$ é um ideal.

Exemplo: Seja G um grupo aditivo, considere o conjunto, $End(G) = \{f : G \rightarrow G; f \text{ é homomorfismo}\}$, as operações $f_1 + f_2 : g \mapsto f_1(g) + f_2(g)$ e $f_1 f_2 := f_2(f_1(g))$, tornam $End(G)$ um anel.

Se G um grupo livre possuindo n geradores x_1, \dots, x_n e $f \in End(G)$. então existem $a_{ij} \in \mathbb{Z}$ tais que

$$x_i f = a_{i1} x_1 + \dots + a_{in} x_n, \quad i = 1, \dots, n.$$

Assim podemos escrever $x f = Ax$, para alguma matriz $A_{n \times n}$ com entradas em \mathbb{Z} .

Seja \mathcal{A} um anel comutativo e \mathcal{I} um ideal de \mathcal{A} . Temos que $\mathcal{I} \triangleleft \mathcal{A}$ pois, pela definição de \mathcal{I} , temos que $x\mathcal{I} = \mathcal{I}x$. Podemos conseguir

homomorfismo de $\overline{\mathcal{A}} = \frac{\mathcal{A}}{\mathcal{I}} = \{a + \mathcal{I} : a \in \mathcal{A}\}$ com o anel \mathcal{A} , para tal tome $\phi : \mathcal{A} \rightarrow \frac{\mathcal{A}}{\mathcal{I}}$ como sendo a projeção canônica. Operando com este homomorfismo, vemos que o quociente $\frac{\mathcal{A}}{\mathcal{I}}$ está bem definido e as operações

$$\begin{cases} (a_1 + \mathcal{I}) + (a_2 + \mathcal{I}) = a_1 + a_2 + \mathcal{I} \\ (a_1 + \mathcal{I}) \cdot (a_2 + \mathcal{I}) = a_1 a_2 + \mathcal{I}, \end{cases}$$

tornam $\frac{\mathcal{A}}{\mathcal{I}}$ um anel chamado de *Anel Quociente* de \mathcal{A} por \mathcal{I} .

O 1º Teorema dos Isomorfismos

Teorema 2.1.1 *Se $f : \mathcal{A} \rightarrow \mathcal{B}$ é um homomorfismo de anéis, então*

$$f(\mathcal{A}) \cong \frac{\mathcal{A}}{\ker f}.$$

Este teorema nada mais é que uma versão melhorada do *1º Teorema de Isomorfismos* para grupos. Como resultado temos que um homomorfismo se decompõe como abaixo:

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{f} & \mathcal{B} \\ \text{proj. canônica} \downarrow & & \uparrow \text{inclusão} \\ \frac{\mathcal{A}}{\mathcal{I}} & \xrightarrow{\cong} & \text{Im}(f) \end{array}$$

Em um grupo tínhamos o grupo normal, não obstante, na Teoria de Anéis, temos os ideais desempenhando o mesmo papel.

Se \mathcal{A} é um anel comutativo e $a \in \mathcal{A}$ então o conjunto $a\mathcal{A} = \{ax : x \in \mathcal{A}\} \triangleleft \mathcal{A}$ é um ideal de \mathcal{A} . Os ideais da forma $a\mathcal{A}$ são chamados de *Ideais Principais*.

Exemplo: Em \mathbb{Z} , todos os ideais são principais.

Seja $\mathcal{I} \triangleleft \mathbb{Z}$, se \mathcal{I} não é principal, então tome $n = \min\{\mathcal{I} \cap \mathbb{Z}_{>0}\}$, se $i \in \mathcal{I} \setminus n\mathbb{Z} \Rightarrow i = nb + r, 0 \leq r < n$ mas $r = i - nb \in \mathcal{I}$, contrariando a escolha de n . Conseqüentemente todo subgrupo aditivo de \mathbb{Z} é um ideal.

Denotemos por $U(\mathcal{A}) = \{a \in \mathcal{A} : \exists b \in \mathcal{A}; ab = ba = 1\}$ o conjunto dos elementos invertíveis em \mathcal{A} . Pode-se mostrar que $U(\mathcal{A})$ é um grupo multiplicativo. Caso $U(\mathcal{A}) = \mathcal{A} \setminus \{0\}$, dizemos que \mathcal{A} é um *Corpo*.

Exemplo: de corpos, $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ (com p primo).

Em um anel comutativo \mathcal{A} , o ideais $\{0\}$ e \mathcal{A} são chamados de ideais triviais de \mathcal{A} .

Proposição 2.1.1 *Se \mathcal{A} é um anel que só possui ideais triviais, então \mathcal{A} é um corpo.*

De fato se $a \in \mathcal{A} \setminus \{0\} \Rightarrow a\mathcal{A} = \mathcal{A} \Rightarrow a^{-1} \in \mathcal{A} \Rightarrow \mathcal{A} \setminus \{0\} \subseteq U(\mathcal{A})$

■

Em um grupo tínhamos o conceito de grupo livre, já em um anel, temos o conceito de Anel de Polinômios.

Definição 2.1.5 *Seja $\mathcal{A} \supset X$ um anel comutativo. Diremos que \mathcal{A} é anel livre com base X , se toda aplicação $\phi : X \rightarrow \mathcal{B}$, onde \mathcal{B} é um anel comutativo, estende-se unicamente a um homomorfismo $\Phi : \mathcal{A} \rightarrow \mathcal{B}$. Os elementos de \mathcal{A} são ditos polinômios com coeficientes inteiros e variáveis em X .*

2.2 Módulos e Álgebras

Módulos

Vamos introduzir agora uma nova estrutura algébrica que chamaremos de *Módulo*. O leitor que já conhece a definição de espaços vetoriais sobre um corpo \mathbb{K} , verá que esta nova estrutura é uma generalização de espaços vetoriais.

Definição 2.2.1 *Seja \mathcal{A} um anel unitário e M um grupo abeliano aditivo, um Módulo sobre um anel \mathcal{A} é uma aplicação,*

$$\begin{array}{ccc} \varphi : \mathcal{A} & \longrightarrow & \text{End}(M) \\ a & \longmapsto & ma \end{array}$$

em um módulo definimos as operações $M \times \mathcal{A} \rightarrow M$:

1. $(m_1 + m_2)a = m_1a + m_2a$;
2. $m(a_1 + a_2) = ma_1 + ma_2$;
3. $m.1 = m$;
4. $(ma_1)a_2 = m(a_1a_2)$.

Como exemplos de \mathcal{A} -módulos temos os espaços vetoriais sobre um corpo K ; seja V um espaço vetorial sobre um corpo K , temos que V é um K -módulo, onde o módulo é dado por

$$\begin{aligned} \varphi: V &\longrightarrow \text{End}(K) \\ v &\longmapsto kv \end{aligned}.$$

Todo grupo abeliano é um \mathbb{Z} -módulo. Todo anel é módulo sobre si mesmo

Definição 2.2.2 *Submódulo: considere um \mathcal{A} -módulo e $N < M$ um subgrupo abeliano aditivo, dizemos que N é um submódulo se, para todo $n \in N$ e todo $a \in \mathcal{A}$, temos $na \in N$*

Como fora observado antes um anel é um módulo sobre si mesmo, e neste caso os submódulos de um anel, são ditos ideais de um anel; simbolicamente

$$\{\text{submódulos de } \mathcal{A}\} = \{\text{ideais de } \mathcal{A}\}.$$

Sejam M, N módulos sobre um mesmo anel \mathcal{A} , considere a aplicação $f: M \rightarrow N$, dizemos que f é um *homomorfismo de módulos* se $f(m_1 + m_2) = f(m_1) + f(m_2)$ e $f(ma) = f(m)a$. Para um exemplo considere U, V espaços vetoriais sobre um corpo K , toda e qualquer transformação linear $T: U \rightarrow V$ é um homomorfismo de módulos. Endomorfismos são homomorfismo de módulos de um anel \mathcal{A} .

Definição 2.2.3 *Módulo Quociente: seja M um \mathcal{A} -módulo e $N < M$, um submódulo, se $\frac{M}{N}$ tem a estrutura de \mathcal{A} -módulo, tal que a projeção canônica $\pi: M \rightarrow \frac{M}{N}$ é um homomorfismo de módulos, então $\frac{M}{N}$ é dito o módulo quociente de M por N .*

Definição 2.2.4 *Soma Direta de Módulos: se M, N são \mathcal{A} -módulos, definimos*

$$\begin{aligned} M \oplus N &= \{(m, n) : m \in M, n \in N\} \\ (m, n)a &= (ma, na) \end{aligned},$$

como a soma direta de módulos

Agora vejamos o que podemos falar a respeito da geração de módulos.

Definição 2.2.5 *Conjunto Gerador:* seja M um \mathcal{A} -módulo e $S \subset M$ um subconjunto. Dizemos que M é gerado por S , ou que S é gerador de M , como módulo se todo $m \in M$ se escreve como $m = m_1s_1 + \dots + m_t s_t$, $s_i \in S$. Além disso dizemos que M é finitamente gerado quando S é finito.

Exemplo: Considere o espaço vetorial \mathbb{R}^n , sabemos que \mathbb{R}^n é um \mathbb{R} -módulo e seu conjunto gerador é

$$\mathcal{B} = \{e_1, \dots, e_n\} \subset \mathbb{R}^n,$$

onde $e_i = (0, \dots, \underbrace{1}_{\text{posição } i}, \dots, 0)$.

No caso em que um \mathcal{A} -módulo M é gerado por um conjunto finito S , e este é o menor conjunto que gera M , dizemos que S é uma base para M e definimos a *dimensão* de M como a cardinalidade de S .

Exemplo: seja \mathbb{K} um corpo, o anel de polinômios $\mathbb{K}[x]$ é um \mathbb{K} -módulo que não é finitamente gerado, pois a sua base é $\{x^n\}_{n \in \mathbb{Z}_{\geq 0}}$. O espaço vetorial \mathbb{R}^n é finitamente gerado. Frequentemente nos referimos aos elementos de uma base como um conjunto *linearmente independente*, ou seja nenhum elemento de uma base $S = \{s_1, \dots, s_k\}$ é escrito como combinação linear dos demais, equivalentemente um conjunto é linearmente independente somente quando tivermos que a combinação linear trivial de seus elementos só é possível se o módulo que forma esta combinação for o módulo nulo, em símbolos:

$$m_1s_1 + \dots + m_k s_k = 0 \Leftrightarrow m_i = 0 \forall i = 1, \dots, k$$

. Com base no que acabamos de ver podemos definir um subconjunto L.I.(linearmente independente) de um \mathcal{A} -módulo como sendo um subconjunto $\mathcal{L} \subset \mathcal{A}$ tal que a única combinação linear nula de elementos de \mathcal{L} for a trivial, daí podemos redefinir base como sendo o maior subconjunto L.I de M que gera o módulo M (prove!).

Definição 2.2.6 *Módulo Livre:* um \mathcal{A} -módulo M é livre com base S se toda aplicação $\varphi : S \rightarrow M'$, em que M' é um \mathcal{A} -módulo, estende-se unicamente a um homomorfismo de \mathcal{A} -módulos.

Exemplo: sejam U e V espaços vetoriais sobre um corpo \mathbb{K} , sabemos de Álgebra Linear que para definir uma transformação linear $T : U \rightarrow V$, basta defini-la em uma base de U , portanto espaços vetoriais são exemplos de módulos livres. Mais geralmente se M é um módulo livre, o conjunto $M^n = \{(m_1, \dots, m_t) : m_i \in M\}$ é um \mathcal{A} -módulo e o conjunto

$$\mathcal{B} = \{e_1, \dots, e_n\} \subset \mathbb{R}^n,$$

onde $e_i = (0, \dots, \underbrace{1}_i, \dots, 0)$ é uma base livre para M^n , podemos ver que M^n também é um módulo livre pois seja

$$\begin{aligned} \varphi : \mathcal{B} &\longrightarrow M \\ e_i &\mapsto \varphi(e_i). \end{aligned}$$

Podemos estender φ a um homomorfismo $\Phi : M^n \rightarrow M$, tal que para todo $v = m_1e_1 + \dots + m_n e_n \in M$ tenhamos $\Phi(v) = m_1\varphi(e_1) + \dots + m_n\varphi(e_n)$.

Definição 2.2.7 *Módulo Cíclico:* dizemos que um \mathcal{A} -módulo M é cíclico quando o seu conjunto gerador tem um único elemento, em símbolos;

$$\forall m_1 \in M, \exists a \in \mathcal{A}; m_1 = ma.$$

Exemplo: $m\mathcal{A} = \{ma : a \in \mathcal{A}\}$ é submódulo e se m gera $M \Rightarrow m\mathcal{A} = M$. Então temos que o homomorfismo de \mathcal{A} -módulos, com M um módulo cíclico;

$$\begin{aligned} \varphi : \mathcal{A} &\longrightarrow M \\ a &\mapsto ma, \end{aligned}$$

nos dá via 1º Teorema dos Homomorfismos que $M \cong \frac{\mathcal{A}}{\mathcal{I}}$, onde $\mathcal{I} \triangleleft \mathcal{A}$. E obtemos o seguinte resultado.

Todo módulo cíclico é isomorfo a um módulo quociente da forma $\frac{\mathcal{A}}{\mathcal{I}}$ onde $\mathcal{I} \triangleleft \mathcal{A}$.

Definição 2.2.8 *Anéis de Ideais Principais:* um anel \mathcal{A} é um anel de ideais principais se todo ideal de \mathcal{A} é da forma $a\mathcal{A}$ para algum $a \in \mathcal{A}$

Exemplos: \mathbb{Z} é um anel de ideais principais. Em virtude de todo corpo não possuir ideais não-triviais, resulta que todo corpo é um anel de ideais principais.

Definição 2.2.9 *Anéis Euclidianos:* um anel é euclidiano se existe uma função $\theta : \mathcal{A} \rightarrow \mathbb{N}$ tal que para todo $a, b \in \mathcal{A}$, existe $c, r \in \mathcal{A}$ com

$$a = bc + r,$$

$$\theta(r) < \theta(b) \text{ ou } r = 0.$$

Exemplos: em \mathbb{Z} , $\theta(n) = |n|$; em $\mathbb{K}[x]$, $\theta(p) = \text{grau}(p)$.

Teorema 2.2.1 *Todo anel euclidiano é anel de ideais principais.*

Demonstração: seja $\mathcal{I} \triangleleft \mathcal{A}$ e $i \in \mathcal{I}$ tal que a função $\theta(i)$ é a menor possível. Temos que $i\mathcal{A} \subset \mathcal{I} \subset \mathcal{A}$, tome $j \in \mathcal{I} \setminus i\mathcal{A}$. Desde que \mathcal{A} é um anel euclidiano;

$$j = ic + r, \text{ onde } \theta(r) < \theta(c) \text{ ou } r = 0;$$

mas $\theta(i)$ é o menor possível, se $r \neq 0 \Rightarrow r = j - ic \in \mathcal{I}$ contrariando a definição de $\theta(i)$, portanto devemos ter $r = 0$, daí $j = ic \in i\mathcal{A}$, agora contrariando a escolha de j . Logo, todo anel euclidiano é anel de ideais principais. ■

Definição 2.2.10 *Se A é um anel, dizemos $p \in A$ é primo se $p = ab$ implica que $a \in U(A)$ ou $b \in U(A)$.*

Definição 2.2.11 *Seja p um elemento primo de um anel \mathcal{A} . Se sempre que $ab \in p\mathcal{A}$ implicar que $a \in p\mathcal{A}$ ou $b \in p\mathcal{A}$, então diremos que o anel A é um anel fatorial.*

Definição 2.2.12 *um ideal \mathcal{I} é primo se e somente se, $ab \in \mathcal{I}$ então $a \in \mathcal{I}$ ou $b \in \mathcal{I}$.*

Proposição 2.2.1 *Se um ideal, de uma anel comutativo com unidade \mathcal{A} , é primo, então $\frac{\mathcal{A}}{\mathcal{I}}$ é domínio, e reciprocamente.*

De fato se \mathcal{I} é primo, então para $ab \in \mathcal{I}$ temos que $a \in \mathcal{I}$ ou $b \in \mathcal{I}$, agora considere o anel $\frac{\mathcal{A}}{\mathcal{I}} = \{a + \mathcal{I} : a \in \mathcal{A}\}$ se $(a_1 + \mathcal{I})(a_2 + \mathcal{I}) =$

$a_1a_2 + \mathcal{I} = \mathcal{I} \Rightarrow a_1 \in \mathcal{I}$ ou $a_2 \in \mathcal{I} \Rightarrow \frac{\mathcal{A}}{\mathcal{I}}$ é domínio. A recíproca é imediata. ■

Exemplo: em \mathbb{Z} , $n\mathbb{Z}$ é ideal primo $\Leftrightarrow n$ é primo.

Suponha que n não seja primo então existem $1 < a, b < n \in \mathbb{Z}$ tais que $n = ab$, daí $ab \in n\mathbb{Z}$, mas por hipótese $a \in n\mathbb{Z}$ ou $b \in n\mathbb{Z}$, suponha que $a = kn \Rightarrow n = knb \Rightarrow n(1 - kb) = 0$, como \mathbb{Z} é domínio $n = 0$ ou $1 - kb = 0 \Rightarrow n = 0$ ou $b = 1$, uma contradição, logo n é primo. Reciprocamente, se n é primo, caso $ab \in n\mathbb{Z}$, teremos que n divide a ou n divide $b \Rightarrow a \in n\mathbb{Z}$ ou $b \in n\mathbb{Z}$.

Definição 2.2.13 *Ideal Maximal:* o ideal maximal de um anel \mathcal{A} é um ideal próprio \mathcal{I} com a seguinte propriedade, quando existir ideal \mathcal{J} de \mathcal{A} , tal que $\mathcal{I} \subseteq \mathcal{J} \subseteq \mathcal{A}$ então $\mathcal{I} = \mathcal{J}$ ou $\mathcal{J} = \mathcal{A}$.

Teorema 2.2.2 *Seja \mathcal{A} um anel comutativo unitário e \mathcal{I} um ideal de \mathcal{A} . Então $\frac{\mathcal{A}}{\mathcal{I}}$ é corpo se e somente se, \mathcal{I} é maximal.*

Demonstração: suponha que exista ideal $\mathcal{I} \subseteq \mathcal{J} \subseteq \mathcal{A}$ com $\mathcal{I} \neq \mathcal{J} \Rightarrow \exists x \in \mathcal{J} \setminus \mathcal{I} \Rightarrow x + \mathcal{I} \neq \mathcal{I}$, desde que $\frac{\mathcal{A}}{\mathcal{I}}$ é corpo, existe $y + \mathcal{I} \in \frac{\mathcal{A}}{\mathcal{I}}$ tal que $xy + \mathcal{I} = 1 + \mathcal{I} \Rightarrow xy - 1 \in \mathcal{I}$, como $x \in \mathcal{J} \Rightarrow xy \in \mathcal{J} \Rightarrow 1 \in \mathcal{J} \Rightarrow \mathcal{J} = \mathcal{A}$. Reciprocamente se \mathcal{I} é maximal, suponha que exista $x + \mathcal{I} \neq \mathcal{I} \Rightarrow x \notin \mathcal{I}$, assim obtemos $\mathcal{I} \subset \mathcal{I} + \langle x \rangle \subset \mathcal{A}$, como \mathcal{I} é maximal $\Rightarrow \langle x \rangle = \mathcal{A}$, e portanto existe $y \in \mathcal{I}$ e $a \in \mathcal{A}$ tal que $y + ax = 1 \Rightarrow 1 - ax \in \mathcal{I} \Rightarrow (a + \mathcal{I})(x + \mathcal{I}) = 1 + \mathcal{I} \Rightarrow X + \mathcal{I}$ é invertível e $\frac{\mathcal{A}}{\mathcal{I}}$ é corpo. ■

Definição 2.2.14 *Anel Fatorial:* um anel \mathcal{A} é fatorial se todo ideal da forma $a\mathcal{A}$, ($a \in \mathcal{A}$ primo) é um ideal primo.

Daí todo Domínio de Ideais Principais (*DIP*) é fatorial. Pois se \mathcal{A} é DIP e $p\mathcal{A}$ é primo, devemos mostrar que $p\mathcal{A}$ é um ideal primo: seja $ab \in p\mathcal{A} \Rightarrow p$ divide $ab \Rightarrow p$ divide a ou p divide $b \Rightarrow a \in p\mathcal{A}$ ou $b \in p\mathcal{A}$.

Álgebras

Agora faremos a introdução de mais uma estrutura algébrica, a qual é conhecida como *Álgebra*.

Definição 2.2.15 *K-Álgebra:* Seja K um anel comutativo e \mathcal{A} um anel qualquer. Dizemos que \mathcal{A} é uma *K-Álgebra* se:

1. $(\mathcal{A}, +)$ é um *K-módulo*;
2. $k(a_1a_2) = (ka_1)a_2$, $k \in K$, $a_i \in \mathcal{A}$.

Exemplo: $(M_{n \times n}(\mathbb{R}), +, \cdot, r \in \mathbb{R})$;

para $A, B \in M_{n \times n}(\mathbb{R})$, temos as matrizes $A + B$, $A \cdot B$ e rA .

Para uma *K-álgebra* também podemos discutir sobre geradores.

Definição 2.2.16 *Conjunto Gerador de Uma K-álgebra:* dizemos que $S \subset \mathcal{A}$ é um gerador de \mathcal{A} , como *Álgebra*, quando todo elemento $a \in \mathcal{A}$ se escreve como

$$a = k_1 s_1^{n_{11}} \dots s_t^{n_{1t}} + \dots + k_r s_1^{n_{r1}} \dots s_t^{n_{rt}}, \quad k_i \in K, \quad s_j \in S \text{ e } n_{ij} \in \mathbb{Z}_{\geq 0}.$$

Analogamente ao caso dos módulos, dizemos que uma *K-álgebra* é finitamente gerada se S é finito.

Exemplo: o anel $\mathbb{K}[x]$ é uma *K-álgebra* finitamente gerada por $\{1, x\}$. Neste exemplo, é interessante observar que $\mathbb{K}[x]$ não é finitamente gerado como módulo, porém é finitamente gerado como *Álgebra*.

Definição 2.2.17 *Álgebra Livre:* dizemos que uma *K-álgebra* é livre com base X se toda aplicação $\varphi : X \rightarrow \mathcal{B}$, em que \mathcal{B} é uma *K-álgebra*, estende-se unicamente a um homomorfismo de *K-álgebras*.

Proposição 2.2.2 *Todo polinômio de grau n , sobre um domínio, tem no máximo n raízes.*

Demonstração: Faremos esta demonstração por indução em n . Se $n = 1$ então temos $f(t) = at + b$. Suponhamos que t_1 e t_2 são raízes de f . Então $at_1 + b = 0 = at_2 + b$ logo $at_1 = at_2$ e portanto $a(t_1 - t_2) = 0$ como f esta sobre um domínio e $a \neq 0$ segue $t_1 = t_2$. Supondo que o resultado seja verdadeiro para $n - 1$. Suponha então que grau de f seja n e que α seja uma raiz de f . Considere o ideal

$$I = \{f \in F[t] : f(\alpha) = 0\} \triangleleft F[t]$$

É fato que este ideal é gerado por $(t - \alpha)$ e assim podemos escrever $f = (t - \alpha)g$ para algum $g \in F[t]$ tal que $\text{grau}(g) = (n - 1)$. Se β é também uma raiz de f e $\beta \neq \alpha$ segue que β é necessariamente uma raiz de g . Mas pela hipótese de indução β pertence a um conjunto de cardinalidade menor ou igual a $(n - 1)$ e portanto f tem no maximo n raízes. ■

Corolário 2.2.1 *Se F é um corpo finito, $|F| = n$ então $U(F)$ é cíclico.*

Demonstração: Já que $U(F)$ é um grupo comutativo sabemos que $U(F) \cong C_1 \times \dots \times C_k$ onde cada C_i é cíclico. Se $U(F)$ não é cíclico então existe $m < n - 1$ tal que $\alpha^m = 1$ para todo $\alpha \in U(F)$. Mas isto quer dizer que o polinômio $f(t) = t^m - 1$ tem pelo menos $|U(F)| = n - 1$ raízes, mas isto contradiz o teorema acima. ■

Definição 2.2.18 *Seja A um anel e M um A -Módulo. Então dizemos que M é Notheriano se todo conjunto $A \neq \emptyset$ de submódulos tem elemento maximal.*

Dito de outra forma M não possui cadeia infinita crescente de submódulos.

Proposição 2.2.3 *Todo Módulo Notheriano é finitamente gerado.*

Demonstração: Seja M um módulo Notheriano e considere o conjunto

$$A = \{\text{submódulos finitamente gerados}\}$$

Seja $N \in \max(A)$, onde $\max(A)$ denota o conjunto dos elementos maximais de A . Se $N \neq M$ tome $m \in M \setminus N$ qualquer. Então temos $N + mA \subset A$ e $N \subset N + mA$ o que contraria a maximalidade de N .

Usando a notação $\mathcal{N} = \{\text{Módulos Notherianos}\}$ temos que:

1. $M \in \mathcal{N}, N < M \Rightarrow N \in \mathcal{N}$
2. $M \in \mathcal{N}, N < M \Rightarrow \frac{\mathcal{M}}{N} \in \mathcal{N}$
3. $N \in \mathcal{N}, \frac{\mathcal{M}}{N} \in \mathcal{N} \Rightarrow M \in \mathcal{N}$
4. Para cada $M \in \mathcal{N}$ e para cada sequência $L_1 \subset L_2 \subset \dots \subset M$ a sequência $L_1 + N \subset L_2 + N \subset \dots \subset M$ é tal que $L_i + N = L_{i+1} + N$ para $i > i_0$ e a sequência $L_1 \cap N \subseteq L_2 \cap N \subseteq \dots$ é tal que $L_i \cap N = L_{i+1} \cap N$ para $i > i_1$.

A demonstração destes fatos será deixada como exercício.

Suponha que A, B e N sejam submódulos de M e que $A \subset B$ e

$$\begin{aligned} A \cap N &= B \cap N \\ A + N &= B + N \end{aligned}$$

então $A = B$.

Por hipótese $A \subset B$. Agora vamos considerar $b \in B$ segue da segunda relação que podemos escrever $b = a + n$ e daí concluir que $n = b - a \in B$, pois $a, b \in B$. Observe que $n \in N \cap B = N \cap A$ logo $N \in A$ mas então $b \in A$.

Teorema 2.2.3 *Se M_1 e M_2 são Módulos Notherianos então $M_1 \oplus M_2$ é também um módulo Notheriano.*

Demonstração: Temos que arrumar uma prova deste fato.

Teorema 2.2.4 *Um anel A é Notheriano se, e somente se, todo ideal $I \triangleleft A$ é finitamente gerado.*

Demonstração: Vamos inicialmente provar a recíproca. Considere uma sequência $I_1 \subset I_2 \subset \dots \subset A$. E seja $I = \bigcup_{n \geq 1} I_n$ usando a hipótese de I ser finitamente gerado podemos escrever

$$I = i_1 A + \dots + i_k A \quad \text{onde } i_j \in I_j;$$

mas isto significa que todo elemento de I pertence a I_k . E como $I_k \subset I$ temos $I_k = I$, o que prova que A é Noetheriano. Agora vamos supor que A é Noetheriano. Vamos construir um conjunto de geradores indutivamente. Seja $i_1 \in A \setminus \{0\}$ se $\langle i_1 \rangle \subsetneq A$, tomamos $i_2 \in A \setminus \langle i_1 \rangle$, construímos então o ideal $\langle i_1, i_2 \rangle$ se $\langle i_1, i_2 \rangle \subsetneq A$, tomamos um elemento $i_3 \in A \setminus \langle i_1, i_2 \rangle$ e continuamos esta construção. Como A é Noetheriano a sequência $\langle i_1 \rangle \subset \langle i_1, i_2 \rangle \subset \dots$ é obrigatoriamente finita. Portanto existe $k \in \mathbb{N}$ tal que $\langle i_1, \dots, i_k \rangle = A$ e o teorema esta totalmente provado. ■

Proposição 2.2.4 *Seja $A \in \mathcal{N}$, e M um A -Módulo. $M \in \mathcal{N}$ se, e somente se, M é finitamente gerado.*

Demonstração: Se M é finitamente gerado, podemos escrever $M = m_1A + \dots + m_kA$ e logo a aplicação que denotaremos por φ definida abaixo:

$$\begin{array}{ccc} A^k & \xrightarrow{\text{sobre}} & M \\ e_i & \longmapsto & m_i \end{array}$$

é sobrejetiva. Pelo primeiro teorema dos homomorfismos temos $M \cong \frac{A^k}{\text{Ker}(\varphi)}$ como A^k e $\text{Ker}(\varphi)$ são finitamente gerados concluímos que $M \in \mathcal{N}$.

Se $M \in \mathcal{N}$ segue do teorema anterior que M é finitamente gerado. ■

Teorema 2.2.5 *(Teorema da base de Hilbert) Se A é um anel Noetheriano então $A[t]$ também é Noetheriano.*

Demonstração: Seja $I \triangleleft A[t]$. Consideramos $f \in A[t]$ e denotamos por $c(f)$ o coeficiente principal de f . Definimos o conjunto

$$J_n = \{c(f) : f \in I \text{ e } \text{grau}(f) \leq n\}$$

E fato que $J_n \triangleleft A$. Vamos supor que $c(f), c(f_1)$ e $c(f_2)$ sejam elementos quaisquer de J_n e $a \in A$. então é fácil ver que $c(f_1) + c(f_2) = c(f_1 + f_2) \in J_n$. E que $ac(f) = c(af) \in J_n$.

Vamos definir agora o seguinte conjunto

$$R_n = \{f \in A[t] : \text{grau}(f) \leq n\}$$

Observemos que R_n é um A -submódulo de $A[t]$ finitamente gerado, pois é gerado por $\{1, t, t^2, \dots, t^n\}$. Como vimos acima, R_n deve ser Noetheriano. Então é claro que $I \cap R_n$ também é Noetheriano e gerado por f_1, \dots, f_k . Vamos verificar agora que I é gerado por $I \cap R_n$. Faremos isto construindo indutivamente polinômios cuja soma é exatamente f . Com efeito, Sejam $f \in I$ e $c(f)$ seu coeficiente principal. É fato que existe um polinômio, $g \in I \cap R_n$ tal que $c(g) = c(f)$. Portanto $\text{grau}(g) = l \leq n$. consideramos então o polinômio gt^{m-l} . Observe que este polinômio pertence a $I \cap R_n$ e que $f - gt^{m-l}$ é tal que $\text{grau}(f - gt^{m-l}) < m$. Procedendo indutivamente contruímos o polinômio f com elementos de $I \cap R_n$. ■

A indução a que nos referimos no final da prova nos permite a cada etapa baixar em algumas unidades o grau do polinômio f usando alguns polinômios do ideal $I \cap R_n$. E observamos que a prova realmente se concretiza pois a soma destes polinômios utilizados é realmente f !

Corpo de Frações

Nesta seção faremos a construção clássica de um corpo a partir de um domínio. E usaremos esta construção para provarmos um resultado importante a respeito de anéis de polinômios.

Seja A um domínio. Considere o produto cartesiano

$$A \times A = \{(x, y) : x, y \in A\}$$

Definiremos em $A \times A \setminus F = \{(x, y) : y \neq 0\}$ a seguinte relação de equivalência.

$$\langle x_1, y_1 \rangle \sim \langle x_2, y_2 \rangle \Leftrightarrow \exists a_1, a_2 \in A \setminus \{0\} \text{ tais que } \begin{array}{l} x_1 a_2 = x_2 a_1 \\ y_1 a_2 = y_2 a_1 \end{array}$$

Verificaremos uma, das três propriedades de uma relação de equivalência. Suponha que $\langle x_1, y_1 \rangle \sim \langle x_2, y_2 \rangle$ e que $\langle x_2, y_2 \rangle \sim \langle x_3, y_3 \rangle$. Então temos

$$\begin{aligned} a_2 \langle x_1, y_1 \rangle &= a_1 \langle x_2, y_2 \rangle \\ b_3 \langle x_2, y_2 \rangle &= b_1 \langle x_3, y_3 \rangle \\ a_1 b_3 \langle x_1, y_1 \rangle &= a_1 b_2 \langle x_3, y_3 \rangle \end{aligned}$$

Por comodidade denotaremos as classes de equivalência pela notação de frações. Isto é, daqui em diante $\frac{x}{y}$ denotará a classe de equivalência

de um par ordenado $\langle x, y \rangle$. Usando a relação de equivalência acima podemos verificar que, com a soma definida abaixo, $\{\text{frações}, +\}$ é um grupo abeliano.

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} = \frac{y_2x_1}{y_2y_1} + \frac{y_1x_2}{y_2y_1} = \frac{y_2x_1 + y_1x_2}{y_2y_1}$$

e definindo o produto de classes por

$$\frac{x_1}{y_1} \cdot \frac{x_2}{y_2} = \frac{x_1x_2}{y_1y_2}$$

o conjunto $A \times A \setminus F$ é um corpo. Este corpo será denotado por $\mathbb{Q}(A)$ e chamado de corpo de frações do anel A . Será importante em muitos casos ver A como um subanel de $\mathbb{Q}(A)$. isto é feito via o homomorfismo de inclusão de anéis $a \mapsto \frac{a}{1} = \langle a, 1 \rangle / \sim$.

Nossos próximos resultados seguirão no sentido de estabelecer uma equivalência entre as três afirmações abaixo, para anéis fatoriais A

1. $a_1a_2 = 0 \Rightarrow a_1 = 0$ ou $a_2 = 0$.
2. Todo elemento primo gera ideal primo.
3. Se $a \in A \setminus U(A)$ então a pode ser escrito como produto de elementos primos.

Lema 2.2.1 (*Lema de Gauss*) *Seja A um anel fatorial, se $f \in A[t]$ é primo em $\mathbb{Q}(A)[t]$ então f é primo em $A[t]$.*

Demonstração: Se f é primo em $\mathbb{Q}(A)[t]$ então existem $g, h \in \mathbb{Q}(A)[t]$ tais que $f = gh$. Como nossos polinômios estão sobre $\mathbb{Q}(A)$ então podemos escrever $g = \frac{g_1}{a}$ e $h = \frac{h_1}{b}$ para $a, b \in A$ e $g_1, h_1 \in A[t]$. Logo nosso polinômio f pode ser reescrito como $f = \frac{g_1}{a} \cdot \frac{h_1}{b}$ e daí temos $fab = g_1h_1$. Seja p divisor primo de ab . Seja $\bar{A} = A/pA$, observe que \bar{A} é domínio, pois pA é primo. Assim podemos definir um homomorfismo de redução mod- p de $A[t] \mapsto \bar{A}[t]$ que manda $\underline{p} \mapsto \bar{p}$. Já que $p|f$ temos que $0 = \overline{abf} = \overline{g_1} \cdot \overline{h_1}$ em $\bar{A}[t]$. Logo $\overline{g_1} = 0$ ou $\overline{h_1} = 0$. Vamos supor que seja $\overline{g_1} = 0$ então sabemos que todos os coeficientes de g_1 são divisíveis por p e portanto $g_1 = pg_2$ com $g_2 \in A[t]$. Logo temos $f = \frac{pg_2 \cdot h_1}{ab}$

e utilizando este processo recursivamente esgotamos todos os divisores primos de ab e nosso teorema está provado. ■

Teorema 2.2.6 (*Cr terio de Eisenstein*) *Se A   um anel fatorial, $f \in A[t]$ e existe um elemento primo $p \in A$ tal que $a_n \notin pA, a_{n-1}, \dots, a_0 \in pA$ e $a_0 \notin p^2A$. Ent o f   irredut vel.*

Demonstra o: Veja que podemos escrever

$$a_n t^n + a_{n-1} t^{n-1} \dots a_0 = f = gh$$

onde $g = b_k t^k + \dots + b_0$ e $h = c_l t^l + \dots + c_0$ com $k + l = n$ e $k, l > 0$. Neste caso   claro que $a_0 = b_0 c_0$ supondo que $b_0 \notin pA$ temos $a_0 \in pA$. Segue da hip tese que $c_l b_k = a_n \notin pA$. Seja $r \in \mathbb{N}$ o menor poss vel tal que $c_r \notin pA$. Como sabemos

$$a_r = c_r b_0 + c_{r-1} b_1 + \dots + c_0 b_r$$

Lembrando que estamos supondo que $b_0 \notin pA$ e que pela defini o de c_r este tamb m n o pertence a este ideal, temos que $b_0 c_r \notin pA$. Veja que $c_{r-1} b_1, \dots, c_0 b_r \in pA$, pela escolha de r . Da  segue que a_r n o pode pertencer a pA o que   uma contradi o. ■

Teorema 2.2.7 *Se A   um anel fatorial, ent o $A[t]$ tamb m   um anel fatorial*

Demonstra o: Seja $f \in A[t]$. Vamos escrever f como produto de fatores irredut veis pertencentes ao anel $\mathbb{Q}(A)[t]$. Isto  

$$f = f_1 \cdots f_n \quad \text{onde } f_i \in \mathbb{Q}(A)[t] \text{   irredut vel}$$

Sabemos pelo lema de Gauss que existem $g_1, \dots, g_n \in A[t]$ polin mios irredut veis em $A[t]$, tais que $f = a \cdot g_1 \dots g_n$ onde $a \in A$ e $a = p_1 \dots p_k$ com p_i primo em A . ■

Teorema 2.2.8 *Todo M dulo finitamente gerado sobre dom nio de ideais principais   soma direta de M dulos C clicos*

Demonstração: Vamos supor que M seja finitamente gerado sobre um domínio de ideais principais A . Já mostramos anteriormente que usando o primeiro teorema dos homomorfismos, temos $M \cong \frac{A^n}{N}$ onde $N \subset A^n$. Existe um homomorfismo $\varphi : A^m \rightarrow A^n$ tal que $M \cong \frac{A^n}{\text{Ker}(\varphi)}$.

Sejam

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \text{ base de } A^m \text{ e } Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \text{ base de } A^n$$

É fato que podemos representar o homomorfismo φ por uma matriz $T_{m \times n}$ sobre A e daí $X\varphi = TY$. Usamos agora o fato que a matriz T é associada a uma matriz diagonal. Diremos que $a = (a_1, \dots, a_n) \in A^n$ é unimodular se $a_1A + \dots + a_nA = A$. Que nos permite concluir que existe $(b_1, \dots, b_n) \in A^n$ tai que $\sum_{i=1}^n a_i b_i = 1$. Observe que se uma matriz P é invertível então suas linhas são unimodulares.

Lema 2.2.2 *Para toda linha unimodular sobre um DIP existe uma matriz P invertível tal que P contem esta linha.*

Demonstração:remos a demonstração por indução no número de linhas e colunas da matriz. Consideremos o caso $n = 2$, assim $a_1\mathcal{A} + a_2\mathcal{A} = \mathcal{A}$ e tome a matriz $\begin{pmatrix} a_1 & a_2 \\ -b_2 & b_1 \end{pmatrix}$ de modo que $a_1b_1 + a_2b_2 = 1 \Rightarrow \det \begin{pmatrix} a_1 & a_2 \\ -b_2 & b_1 \end{pmatrix} = 1$. Suponhamos que o lema está provado para linhas de tamanho $< n$. Considere a n -úpla (a_1, \dots, a_n) e considere o ideal $\mathcal{I} = a_1\mathcal{A} + \dots + a_{n-1}\mathcal{A} = a\mathcal{A}$ (pois por hipótese estamos em um DIP), assim podemos reescrever $a_i = aa_i'$ e existem b_i 's tais que (a_1', \dots, a_{n-1}') é unimodular, pois $a_1b_1, \dots, a_{n-1}b_{n-1} = a \Rightarrow a_1'b_1, \dots, a_{n-1}'b_{n-1} = 1$. Pela hipótese de indução, (a_1', \dots, a_{n-1}') é uma linha de uma matriz invertível, a primeira linha, digamos, de P . Seja $Q = P^{-1}$, então o produto matricial

$$(a_1 \dots a_n) \begin{pmatrix} & & & & 0 \\ & Q & & & 0 \\ & & & & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = (a, 0, \dots, 0, a_n),$$

o resultado é uma linha unimodular $\Rightarrow a\mathcal{A} + a_n\mathcal{A} = \mathcal{A} \Rightarrow (a_1, \dots, a_n)$ é uma linha de uma matriz invertível R e é uma linha de

$$\begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix} R,$$

como queríamos. ■

Dada uma matriz T . Dentre as matrizes associadas a T , encontremos uma matriz T_1 com elemento t , tal que $t\mathcal{A}$ é maximal. Podemos supor que

$$T_1 = \begin{pmatrix} t & \dots \\ \vdots & \dots \end{pmatrix},$$

caso tenhamos

$$T_1 = \begin{pmatrix} t & s & \dots \\ \vdots & & \dots \\ 0 & & \dots \end{pmatrix},$$

e $s \notin t\mathcal{A} \Rightarrow t\mathcal{A} + s\mathcal{A} = r\mathcal{A} \supset t\mathcal{A}$, contradizendo a escolha de t , logo todo elemento de $T_1 \in t\mathcal{A}$, se a matriz que temos em mãos não é como T_1 , digamos que temos uma matriz S , e esta matriz seja tal que $\sum s_{ij}\mathcal{A} = \mathcal{A}$, se $s_{11} \notin S$

como toda matriz é associada a uma matriz diagonal, para a matriz T anteriormente citada podemos conseguir uma matriz diagonal tal que

$$\begin{pmatrix} t_1 & \dots & 0 \\ 0 & \ddots & \vdots \\ 0 & \dots & t_n \end{pmatrix},$$

onde $\sum t_i\mathcal{A} = \mathcal{A}$. Donde concluímos ;

Teorema 2.2.9 (*Forma Canônica de Jordan*) Seja $A \in \mathbb{M}_{n \times n}(\mathbb{C})$, então a matriz A é conjugada a uma matriz J da forma

$$J = \begin{pmatrix} J_1 & \dots & 0 \\ 0 & \ddots & \vdots \\ \dots & \dots & J_k \end{pmatrix}, \text{ onde}$$

$$J_i = \begin{pmatrix} \lambda & 1 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ 0 & \ddots & \vdots & 0 \\ 0 & \dots & \vdots & 1 \\ 0 & \dots & \lambda & 0 \end{pmatrix}, \text{ os } J_i \text{'s, são únicos a menos de permutação.}$$

**Obs: Este texto foi baseado em algumas notas de aula do curso de Álgebra Avançada, ministradas pelo professor Víctor Guerassimov do Departamento de Matemática da UFMG.*