REJIANE APARECIDA CALIXTO

Condições que Caracterizam um Conjunto Tórico como Variedade Afim Tórica

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2019

REJIANE APARECIDA CALIXTO

Condições que Caracterizam um Conjunto Tórico como Variedade Afim Tórica

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica.

Orientador: Prof. Dr. Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2019

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU, MG, Brasil.

C154c
2019

Calixto, Rejiane Aparecida, 1991-
Condições que caracterizam um conjunto tórico como variedade afim tórica [recurso eletrônico] / Rejiane Aparecida Calixto. - 2019.

Orientador: Victor Gonzalo Lopez Neumann.
Dissertação (mestrado) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://dx.doi.org/10.14393/ufu.di.2019.327
Inclui bibliografia.
Inclui ilustrações.

1. Matemática. 2. Variedades tóricas. 3. Bases de Gröbner. I. Neumann, Victor Gonzalo Lopez, 1974- (Orient.) II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 51

Maria Salete de Freitas Pinheiro - CRB6/1262

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 152
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNA: Rejiane Aparecida Calixto.

NÚMERO DE MATRÍCULA: 11712MAT008.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Condições que Caracterizam um Conjunto Tórico como Variedade Afim Tórica.

ORIENTADOR: Prof. Dr. Victor Gonzalo Lopez Neumann.

Esta dissertação foi **APROVADA** em reunião pública realizada na sala 1F223, Bloco 1F, Campus Santa Mônica, em 14 de Fevereiro de 2019, às 14h, pela seguinte Banca Examinadora:

NOME	ASSINATURA
Prof. Dr. Victor Gonzalo Lopez Neumann UFU - Universidade Federal de Uberlândia	
Prof. Dr. Herivelto Martins Borges Filho USP - Universidade de São Paulo	
Prof. Dr. Cícero Fernandes de Carvalho UFU - Universidade Federal de Uberlândia	

Uberlândia-MG, 14 de Fevereiro de 2019.

Dedicatória

Dedico este trabalho à minha mãe, minha irmã Maria Eduarda e ao meu saudoso amigo Felipe Vieira (em memória).

Agradecimentos

Agradeço primeiramente a Deus por sempre guiar meus passos e colocar em meu caminho pessoas boas, que muito me ajudaram a chegar até aqui.

À minha família, por acreditarem em mim. Principalmente à minha mãe e minha avó Maria, por serem meu exemplo de força, luta, esperança e amor. Obrigada por tudo.

Aos meus amigos Nayara, Bruno, Alcindo, André, Lili e Humberto pela companhia, ensinamentos e ótimas risadas. Obrigada por tornarem meus dias em Campinas muito melhores.

À Lívia e à Bruninha, meu sincero agradecimento por me acolherem com tanto carinho em sua casa e por sempre me apoiarem.

À Suélen pelo acolhimento em Uberlândia. Obrigada, pelo carinho, amizade e companheirismo.

Aos meus amigos pelo apoio e companheirismo de sempre. Aos meus companheiros de mestrado Gabriel, Kassandra, Luis Garcia, Luis Anthony, Daniel, Telmo, Diego, Ivan, Javier, Julian e Milton pelos momentos de estudo, pelo apoio e incentivo em dias difíceis e pelos momentos de descontração.

Ao meu namorado Edwin pela companhia, cuidado, carinho, incentivo e paciência.

Agradeço ainda aos professores da Faculdade de Matemática pelos ensinamentos e conselhos ao longo destes dois anos. Em particular, ao meu orientador Victor Gonzalo, pela paciência e disposição para sanar minhas dúvidas.

Aos membros da banca pela gentileza de avaliarem este trabalho.

Por fim, agradeço à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, pelo apoio financeiro.

CALIXTO, R. A. *Condições que Caracterizam um Conjunto Tórico como Variedade Afim Tórica.* 2019. 54p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

A partir de uma matriz $\mathcal{A}$ com determinadas características, é possível definir o chamado ideal tórico $I_{\mathcal{A}}$, que por sua vez dá origem à uma variedade tórica $V(I_{\mathcal{A}})$. As colunas desta matriz $\mathcal{A}$, fornecem uma parametrização de um subconjunto da variedade tórica, que é denominado conjunto tórico. O objetivo desta dissertação é apresentar um resultado que relaciona estes dois conjuntos. Mais precisamente, é mostrado um resultado que fornece duas condições suficientes e necessárias para determinar quando um conjunto tórico determinado por uma dada matriz $\mathcal{A}$, é igual à variedade tórica determinada pela mesma matriz. São mostradas ainda, algumas aplicações deste resultado. O trabalho ainda aborda alguns conceitos como Base de Gröbner e módulos finitamente gerados. Utilizando a teoria de bases de Gröbner se pode provar alguns resultados a respeito do conjunto de geradores de um ideal tórico. Já a teoria de Módulos fornece ferramentas para que se prove o resultado principal que compõe o objetivo do trabalho.

Palavras-chave: Variedade Tórica. Ideal Tórico. Conjunto Tórico.

CALIXTO, R. A. *Conditions for Characterization of a Toric Set as an Affine Toric Variety.* 2019. 54p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

From a matrix $\mathcal{A}$ with certain characteristics, it is possible to define the toric ideal $I_{\mathcal{A}}$, which in turn gives rise to a toric variety $V(I_{\mathcal{A}})$. The columns of this matrix $\mathcal{A}$, provide a parameterization of a subset of the toric variety, which is called the toric set. The purpose of this dissertation is to present a result that relates these two sets. More precisely, a result is shown which provides two sufficient and necessary conditions to determine when a toric set determined by a given matrix $\mathcal{A}$, is equal to the toric variety determined by the same matrix. Besides, some aplications of this result are showen. The work still addresses some concepts like Gröbner Base and Finitely Generated Modules. Using the theory of Gröbner Bases one can prove some results regarding the set of generators of a toric ideal. The Modules theory, however, provides tools for proving the main result that makes up the purpose of the work.

Keywords: Toric Variety. Toric Ideal. Toric Set.

SUMÁRIO

INTRODUÇÃO

A matemática é dividida em várias áreas. Dentre estas, se encontra a geometria algébrica, que faz uso de métodos algébricos para estudar propriedades geométricas de conjuntos de soluções de sistemas de equações polinomiais. No presente trabalho estes conjuntos de soluções são denominados variedades afins. Pode-se definir variedades afins a partir de um ideal polinomial. Esta caracterização é possível através da teoria das Bases de Gröbner.

Nos últimos quarenta e oito anos, um tipo de variedade afim vem ganhando espaço nas pesquisas em geometria algébrica. Elas são chamadas variedades tóricas. De acordo com Cox, Little e Schenck [1], esta classe de variedades foram definidas formalmente em 1970, em um artigo de Demezure [2] intitulado *"Sous-groupes algébriques de rang maximum du groupe de Cremona"*. Um fato interessante que os autores mencionam é que o termo "variedade tórica" veio a surgir somente depois de 1977, quando Miles Reidv escolheu o título "*Geometry of toric varieties*" ao traduzir para o inglês o artigo de Danilov's [3], cujo título em russo era "Геометрия торических многообразий". O trabalho de Danilov's foi um dos mais importantes da época sobre o tema. E depois dele muitos outros trabalhos foram publicados, apresentando vários resultados significativos para as áreas de combinatória, políopos convexos, teoria de códigos, física, dentre outras.

É importante mencionar que é possível pensar em variedades tóricas de diversas maneiras. Duas definições distintas podem ser encontradas, por exemplo, em [1] e [4]. No presente trabalho é utilizada uma outra definição, que difere das duas encontradas nos livros citados acima. Aqui, tem-se como variedade afim tórica à variedade de um ideal tórico.

Utilizando esta caracterização de variedade tórica e alguns resultados sobre A-módulos, este trabalho visa apresentar condições necessárias e suficientes para um conjunto tórico ser caracterizado como variedade afim tórica. Este resultado é apresentado por Reyes, Villarreal e Zárate em [5] e de acordo com Katsabekis e Thoma [6], foi neste trabalho que a relação entre conjunto tórico e variedade tórica foi considerada pela primeira vez. Em particular, dizer que um conjunto tórico é uma variedade tórica, é o mesmo que dizer que esta variedade é parametrizada por monômios. Segundo Katsabekis e Thoma [7] parametrizar variedades tóricas é importante tanto por motivos teóricos como para aplicações, dando como exemplo, projeto geométrico assistido por computador.

Diante das importâncias apresentadas, é válido mencionar que existem trabalhos posteriores ao de Reyes, Villarreal e Zárate, que tratam do assunto em questão e que não foram abordados aqui. Caso o autor tenha interesse, pode consultar [6] e [7], já citados acima. Em [6], os autores provam que qualquer variedade tórica sobre um corpo algebricamente fechado, pode ser expressa como um conjunto tórico, para uma matriz apropriada. Já em [7] são apresentadas condições sob as quais um conjunto tórico é uma variedade tórica, a partir da combinação das técnicas mostradas em [5] e [6]. Além disso, os autores provam que qualquer variedade tórica

normal sobre qualquer corpo, é igual a um conjunto tórico dado por uma matriz apropriada.

Antes do resultado principal (Teorema 5.2.3) desta dissertação ser mostrado, são apresentados quatro capítulos; o Capítulo 1 trata dos conceitos preliminares a respeito de polinômios, variedade afim e ideal polinomial.

No Capítulo 2 é estudada a teoria de bases de Gröbner. É definida ordem monomial e são apresentados resultados importantes para o desenvolvimento deste trabalho, tais como o Teorema das bases de Hilbert e o Algoritmo de Buchberger's.

O capítulo 3 é composto pelo estudo de A-módulos. Um dos resultados mostrados neste capítulo é de fundamental importância para a demonstração do Teorema 5.2.3.

O capítulo 4 é dedicado ao ideal tórico, contendo a definição deste ideal e resultados a respeito de seu conjunto de geradores. Por meio da teoria das bases de Gröbner, é mostrado também como é possível calcular geradores para um ideal tórico.

Por fim, no Capítulo 5 são definidos conjunto tórico e variedade afim tórica. É demonstrado o Teorema 5.2.3, que fornece as condições para a caracterização do conjunto tórico como variedade afim tórica e além disso são apresentadas algumas aplicações deste resultado.

Rejiane Aparecida Calixto
Uberlândia-MG, 14 de Fevereiro de 2019.

CAPÍTULO 1

CONCEITOS PRELIMINARES

1.1 Polinômios

Um **monômio** nas variáveis $x_1, \ldots, x_n$ é um produto da forma

$$x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$$

cujos expoentes $\alpha_1, \ldots, \alpha_n$ são inteiros não negativos. O **grau total** deste monômio é dado pela soma $\alpha_1 + \cdots + \alpha_n$. Uma combinação linear finita de monômios com coeficientes em um corpo K é chamada de **polinômio** f nas variáveis $x_1, \ldots, x_n$.

A fim de simplificar notações, considere $\alpha = (\alpha_1, \ldots, \alpha_n)$ uma n-upla de inteiros não negativos. Podemos então escrever um monômio como

$$x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}.$$

Note que quando $\alpha = (0, \ldots, 0)$, $x^\alpha = 1$. Denotando um monômio como acima, podemos denotar seu grau total por $|\alpha| = \alpha_1 + \cdots + \alpha_n$. Com essa nova notação escrevemos o polinômio f como

$$f = \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in K,$$

com a soma dada sobre um número finito de n-uplas $\alpha = (\alpha_1, \ldots, \alpha_n)$. O conjunto de todos os polinômios nas variáveis $x_1, \ldots, x_n$ com coeficientes em K é denotado por $K[x_1, \ldots, x_n]$. Chamamos este conjunto de anel de polinômios em n variáveis.

Seja $f = \sum_\alpha a_\alpha x^\alpha$ um polinômio em $K[x_1, \ldots, x_n]$. Chamamos a_α de **coeficiente** do monômio x^α. Se $a_\alpha \neq 0$, então $a_\alpha x^\alpha$ é chamado **termo** de f e o **grau total** de $f \neq 0$ é definido por

$$deg(f) = \max \{|\alpha|; a_\alpha \neq 0\}.$$

Exemplo 1.1.1. *Considere o polinômio* $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2$ *em* $\mathbb{Q}[x, y, z]$. *Observe que* f *tem quatro termos e grau total igual a seis. Note ainda que diferentemente dos polinômios em uma variável,* f *possui dois termos de grau total máximo.*

Consideremos agora, o produto cartesiano de n fatores iguais a K:

$$\mathbb{A}_K^n = K^n = K \times \cdots \times K.$$

Chamamos $\mathbb{A}_K^n$ de **espaço afim** n-dimensional sobre um corpo K.

Como um exemplo de espaço afim, pode-se considerar o conhecido espaço euclidiano $\mathbb{R}^n$, sendo neste caso $K = \mathbb{R}$.

Podemos ver um polinômio $f = \sum_\alpha b_\alpha x^\alpha \in K[x_1, \ldots, x_n]$ como uma função $f : \mathbb{A}^n_K \to K$, definida da seguinte maneira: dado $a = (a_1, \ldots, a_n) \in \mathbb{A}^n_K$, substitui-se cada x_i por a_i na expressão que determina f. Mais precisamente, $f(a_1, \ldots, a_n) = \sum_\alpha b_\alpha a^\alpha \in K$, com $a^\alpha = a_1^{\alpha_1} \cdot \ldots \cdot a^{\alpha_n}$.

Se recorde que um polinômio nulo é aquele que tem todos os seus coeficientes iguais a zero, e dizer que uma dada função f é nula em $\mathbb{A}^n_K$ significa que $f(a) = 0$, para todo $a \in \mathbb{A}^n_K$. Com isto em mente, vejamos o próximo resultado.

Proposição 1.1.2. *Sejam K um corpo infinito e $f \in K[x_1, \ldots, x_n]$. Então $f = 0$ em $K[x_1, \ldots, x_n]$ se, e somente se, $f : \mathbb{A}^n_K \to K$ é a função nula.*

Demonstração. Se $f = 0$, então obviamente a função $f : \mathbb{A}^n_K \longrightarrow K$ é nula. Para provar o contrário, precisamos mostrar que se $f(a_1, \ldots, a_n) = 0$ para todos $(a_1, \ldots, a_n) \in \mathbb{A}^n_K$, então f é o polinômio zero. Nós usaremos indução sobre o número de variáveis n.

Seja $n = 1$. Sabemos que um polinômio não nulo, de uma variável, com grau m, possui no máximo m raízes distintas. Assim, se $f \in K[x]$ e $f(a) = 0$ para todo $a \in K$, como K é infinito, significa que f tem infinitas raízes. Portanto f é o polinômio zero.

Agora suponhamos que para todo polinômio $h \in K[x_1, \ldots, x_{n-1}]$, que se anula em todo $a \in \mathbb{A}^{n-1}_k$, temos h igual ao polinômio zero. Seja $f \in K[x_1, \ldots, x_n]$ um polinômio que se anula em todos os pontos de $\mathbb{A}^n_K$. Podemos escrever f da seguinte forma,

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1}) x_n^i, \tag{1.1}$$

sendo $g_i \in K[x_1, \ldots, x_{n-1}]$.

Se fixamos $(a_1, \ldots, a_{n-1}) \in \mathbb{A}^{n-1}_K$, temos que $f(a_1, \ldots, a_{n-1}, x_n) \in K[x_n]$. Por hipótese, f deve se anular em cada $a_n \in K$. Segue do caso $n = 1$ que $f(a_1, \ldots, a_{n-1}, x_n)$ é o polinômio zero em $K[x_n]$. Usando a expressão de f dada em (1.1), vemos que os coeficientes de f são $g_i(a_1, \ldots, a_{n-1})$, e portanto, $g_i(a_1, \ldots, a_{n-1}) = 0$ para todo i. Como $(a_1, \ldots, a_{n-1})$ foi escolhido de maneira arbitrária em $\mathbb{A}^{n-1}_k$, segue que $g_i \in K[x_1, \ldots, x_{n-1}]$ fornece a função nula em $\mathbb{A}^{n-1}_K$. Por hipótese de indução, temos que g_i é o polinômio zero em $K[x_1, \ldots, x_{n-1}]$. Isso implica que f é o polinômio zero em $K[x_1, \ldots, x_n]$ e conclui a prova da proposição. □

Antes de passarmos para o próximo resultado, vejamos um exemplo de um caso específico, de como funciona escrever $f \in K[x_1, \ldots, x_n]$, na varável x_n e com coeficientes em $K[x_1, \ldots, x_{n-1}]$.

Exemplo 1.1.3. *Considere o polinômio*

$$f(x, y, z) = x^5y^2z - x^4y^3 + y^5 + x^2z - y^3z + xy + 2x - 5z + 3.$$

Escrevendo f como um polinômio na variável x e coeficiente em $K[y, z]$, temos

$$f = (y^2z)x^5 - y^3x^4 + zx^2 + (y + 2)x + (y^5 - y^3z - 5z + 3).$$

Corolário 1.1.4. *Seja K um corpo infinito, e sejam $f, g \in K[x_1, \ldots, x_n]$. Então $f = g$ se, e somente se, $f : \mathbb{A}^n_K \to K$ e $g : \mathbb{A}^n_K \to K$ são a mesma função.*

Demonstração. Suponha que $f, g \in K[x_1, \ldots, x_n]$, fornecem a mesma função em $\mathbb{A}^n_K$. Então $f - g$ é a função nula em $\mathbb{A}^n_K$. Pela Proposição 1.1, segue que o polinômio $f - g = 0$. Isto prova que $f = g \in K[x_1, \ldots, x_n]$. A recíproca é trivial. □

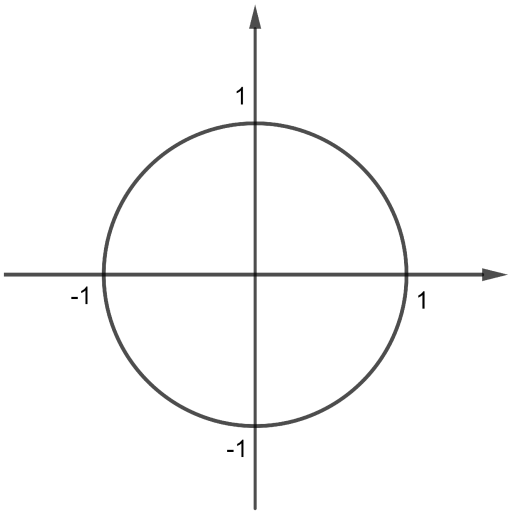
1.2 Variedades Afins e Ideais

Sejam K um corpo e $f_1, \ldots, f_s$ polinômios em $K[x_1, \ldots, x_n]$, chamamos de **variedade afim** definida por $f_1, \ldots, f_s$, ao conjunto

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n_K; f_i(a_1, \ldots, a_n) = 0 \text{ para todo } 1 \leq i \leq s\}.$$

Em outras palavras, uma variedade afim $V(f_1, \ldots, f_s) \subseteq \mathbb{A}^n_K$ é o conjunto de todas as soluções do sistema de equações $f_1(x_1, \ldots, x_n) = \ldots = f_s(x_1, \ldots, x_n) = 0$.

Exemplo 1.2.1. *Dado $f = x^2 + y^2 - 1 \in \mathbb{R}[x, y]$, temos que a variedade afim $V(x^2 + y^2 - 1)$ definida por f é o círculo de raio um centrado na origem:*



Lema 1.2.2. *Se $V, W \subseteq \mathbb{A}^n_K$ são variedades afins, então $V \cup W$ e $V \cap W$ também o são.*

Demonstração. Suponha que $V = V(f_1, \ldots, f_s)$ e $W = V(g_1, \ldots, g_t)$. Afirmamos que

$$\begin{aligned} V \cap W &= V(f_1, \ldots, f_s, g_1, \ldots, g_t), \\ V \cup W &= V(f_i g_j | \quad 1 \leq i \leq, 1 \leq j \leq t). \end{aligned}$$

A primeira igualdade é trivial, pois se $a = (a_1, \ldots, a_n) \in V \cap W$ então a anula $f_1, \ldots, f_s$ e $g_1, \ldots, g_t$, que é o mesmo que anular $f_s, \ldots, f_s, g_1, \ldots, g_t$. E claramente, se a anula $f_s, \ldots, f_s$, $g_1, \ldots, g_t$, então $a \in V \cap W$. Para provar a segunda igualdade tome $a = (a_1, \ldots, a_n) \in V$, então todos os f_i's se anulam em a, o implica que todos os $f_i g_j$'s também se anulam em a. Portanto, $V \subseteq V(f_i g_j)$ e de modo análogo vemos que $W \subseteq V(f_i g_j)$, provando assim que $V \cup W \subseteq V(f_i g_j)$. Agora vejamos que $V(f_i g_j) \subseteq V \cup W$. De fato, se $a = (a_1, \ldots, a_n) \in V(f_i g_j)$, então todos $f_i g_j$'s se anulam em a. Se $a \in V$, não temos mais nada o que provar. Suponhamos então que existe i_0 em $\{1, \ldots, s\}$ tal que $f_{i_0}(a)$ é diferente de zero. Como $(f_{i_0} g_j)$ se anula em a para todo j, segue que os g_j's devem se anular em a, o que mostra que $a \in W$, concluindo assim a demonstração. □

Além das variedades afins, outro objeto importante estudado neste trabalho, é o chamado *ideal*. Chamamos de **ideal**, um conjunto $I \subseteq K[x_1, \ldots, x_n]$ que satisfaz as seguintes condições:

1. $0 \in I$
2. Se $f, g \in I$, então $f + g \in I$

3. Se $f \in I$ e $h \in K[x_1, \ldots, x_n]$, então $hf \in I$.

Como um exemplo de ideal em $K[x_1, \ldots, x_n]$, temos o seguinte conjunto:

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \,\middle|\, h_1, \ldots, h_s \in K[x_1, \ldots, x_n] \right\},$$

com $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. Vejamos que esse conjunto assim definido é, de fato, um ideal.

Lema 1.2.3. *Se $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, então $\langle f_1, \ldots, f_s \rangle$ é um ideal de $K[x_1, \ldots, x_n]$. Chamaremos $\langle f_1, \ldots, f_s \rangle$ de **ideal gerado** por $f_1, \ldots, f_s$.*

Demonstração. Note que $0 \in \langle f_1, \ldots, f_s \rangle$, pois $0 = \sum_{i=1}^{s} 0 \cdot f_i$. Agora, tome $f, g \in I$ e $h \in K[x_1, \ldots, x_n]$. Digamos que

$$f = \sum_{i=1}^{s} p_i f_i \text{ e } \sum_{i=1}^{s} q_i f_i.$$

Assim,

$$\begin{aligned} f + g &= \sum_{i=1}^{s} (p_i q_i) f_i, \\ hf &= \sum_{i=1}^{s} (h p_i) f_i. \end{aligned}$$

Portanto, $\langle f_1, \ldots, f_s \rangle$ é um ideal. □

Quando existem $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ tais que $I = \langle f_1, \ldots, f_s \rangle$, para um dado ideal I, dizemos que I é **finitamente gerado**. Neste caso, dizemos que $f_1, \ldots, f_s$ é uma **base** de I. Note que um ideal pode ter diferentes bases.

Exemplo 1.2.4. *Não é difícil provar que $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$.*

Proposição 1.2.5. *Se $f_1, \ldots, f_s$ e $g_1, \ldots, g_t$ são bases de um mesmo ideal em $K[x_1, \ldots, x_n]$, ou seja, $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, então $V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$.*

Demonstração. Seja $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$. Então, para cada $i = 1, \ldots, s$ temos que $f_i(a_1, \ldots, a_n) = 0$. Observe que g_j está em $\langle f_1, \ldots, f_s \rangle$, para todo j. Assim, para cada $j = 1, \ldots, t$,

$$g_j = \sum_{i=1}^{s} h_i^j f_i, \quad h_i^j \in K[x_1, \ldots, x_n], \text{para todo } i.$$

Logo, $g_j(a_1, \ldots, a_n) = 0$ para todo j. Logo, $V(f_1, \ldots, f_s) \subset V(g_1, \ldots, g_t)$.

De maneira análoga, prova-se que $V(g_1, \ldots, g_t) \subset V(f_1, \ldots, f_s)$. E assim concluímos que $V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$. □

Considere uma variedade $V \in \mathbb{A}_K^n$ e defina o conjunto

$$\mathbf{I}(V) = \{ f \in K[x_1, \ldots, x_n] \,|\, f(a_1, \ldots, a_n) = 0 \text{ para todo } (a_1, \ldots, a_n) \in V \}.$$

É fácil ver que $\mathbf{I}(V)$ é um ideal. Com esta definição podemos estabelecer uma correspondência entre variedade e ideal.

Lema 1.2.6. *Se $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. Então $\langle f_1, \ldots, f_s \rangle \subseteq \boldsymbol{I}(\boldsymbol{V}(f_1, \ldots, f_s))$. A igualdade pode não ocorrer.*

Demonstração. Seja $f \in \langle f_1, \ldots, f_s \rangle$. Assim, $f = \sum_{i=1}^{s} h_i f_i$ para alguns

$$h_1, \ldots, h_s \in K[x_1, \ldots, x_n].$$

Como $f_1, \ldots, f_s$ se anulam em $V(f_1, \ldots, f_s)$, o mesmo ocorre com f. Assim, $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$. Portanto, $\langle f_1, \ldots, f_s \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$. Para mostrar que a igualdade nem sempre ocorre, considere o seguinte exemplo:

Seja $I = \langle x^2, y^2 \rangle \subset K[x_1, \ldots, x_n]$. Então a variedade $V(x^2, y^2) = \{(0,0)\}$. Assim,

$$\mathbf{I}(\mathbf{V}(x^2, y^2)) = \mathbf{I}(\{(0,0)\}),$$

ou seja, é o ideal formado por todos os polinômios que se anulam em $(0,0)$. Afirmamos que

$$\mathbf{I}(\{(0,0)\}) = \langle x, y \rangle.$$

Uma das inclusões é trivial, pois qualquer polinômio $A(x,y)x + B(x,y)y$ obviamente se anula em $(0,0)$. Assim, $\langle x, y \rangle \subset \mathbf{I}(\{(0,0)\})$. Agora, suponha que $f = \sum_{i,j} a_{ij} x^i y^j$ se anula em $(0,0)$. Então, $a_{00} = f(0,0) = 0$ e consequentemente,

$$\begin{aligned} f =& a_{00} + \sum_{\substack{i \neq 0 \\ ou \\ j \neq 0}} a_{ij} x^i y^j \\ =& 0 + \left(\sum_{\substack{i,j \\ i>0}} a_{ij} x^{i-1} y^j \right) x + \left(\sum_{j>0} a_{0j} y^{j-1} \right) y \in \langle x, y \rangle. \end{aligned}$$

Provamos assim nossa afirmação.

Sabemos que $\langle x^2, y^2 \rangle \subseteq \mathbf{I}(\{(0,0)\})$. Vejamos que $\mathbf{I}(\{(0,0)\})$ é estritamente maior que $\langle x^2, y^2 \rangle$. Para isso, note que $x \notin \langle x^2, y^2 \rangle$, pois em polinômios da forma $h_1(x,y)x^2 + h_2(x,y)y^2$ os monômios possuem sempre grau maior ou igual a dois. □

CAPÍTULO 2

BASES DE GRÖBNER

2.1 Ordem Monomial e o Algoritmo da Divisão

Veremos a seguir que é possível estabelecer uma relação de ordem sobre os monômios em $K[x_1, \ldots, x_n]$. Para isso, observe que para cada n-upla $\alpha = (\alpha_1, \ldots, \alpha_n)$ em $\mathbb{N}^n$ temos um monômio $x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ em $K[x_1, \ldots, x_n]$. Esta observação estabelece uma correspondência biunívoca entre os monômios em $K[x_1, \ldots, x_n]$ e $\mathbb{N}^n$. Além disso, dada uma ordem $\succ$ em $\mathbb{N}^n$, diremos que $x^\alpha \succ x^\beta$ se $\alpha \succ \beta$. Dessa forma, definimos uma **ordem monomial** $\succ$ em $K[x_1, \ldots, x_n]$ como sendo uma relação $\succ$ em $\mathbb{N}^n$, ou equivalentemente, uma relação $\succ$ no conjunto dos monômios x^α, $\alpha \in \mathbb{N}^n$, que satisfaz:

(i) $\succ$ é uma ordem total (ou linear) em $\mathbb{N}^n$. Isso significa que dados os monômios x^α, x^β e x^γ apenas uma das seguintes condições é verdadeira: $x^\alpha \succ x^\beta$, $x^\alpha = x^\beta$ ou $x^\alpha \prec x^\beta$. Além disso vale a transitividade, isto é, $x^\alpha \succ x^\beta$ e $x^\beta \succ x^\gamma$, sempre implica que $x^\alpha \succ x^\gamma$.

(ii) Se $\alpha \succ \beta$ e $\gamma \in \mathbb{N}^n$, então $\alpha + \gamma \succ \beta + \gamma$.

(iii) $\succ$ é uma boa ordem em $\mathbb{N}^n$, ou seja, todo subconjunto não vazio de $\mathbb{N}^n$ possui um menor elemento com relação a $\succ$.

Proposição 2.1.1. *Uma relação de ordem $\succ$ sobre $\mathbb{N}^n$ é uma boa ordem se, e somente se, toda sequência estritamente decrescente em $\mathbb{N}^n$*

$$\alpha(1) \succ \alpha(2) \succ \alpha(3) \ldots$$

estaciona em algum momento.

Demonstração. Vamos provar a proposição por contraposição: $\succ$ não é uma boa ordenação se, e somente se, existe uma sequência em $\mathbb{N}^n$ infinita e estritamente decrescente.

Suponha que $\succ$ não é uma boa ordenação, então algum subconjunto $S \subset \mathbb{N}^n$ não vazio, não tem um menor elemento. Escolha $\alpha(1) \in S$. Como $\alpha(1)$ não é o menor elemento, podemos encontrar $\alpha(2) \in S$ tal que $\alpha(1) \succ \alpha(2)$. Como $\alpha(2)$ também não é o menor elemento, existe $\alpha(3) \in S$ de tal forma que $\alpha(1) \succ \alpha(2) \succ \alpha(3)$ em S. Prosseguindo desta maneira, conseguimos uma sequência infinita estritamente decrescente

$$\alpha(1) \succ \alpha(2) \succ \alpha(3) \ldots .$$

Reciprocamente, dada uma sequência infinita estritamente decrescente, segue que

$$\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$$

é um subconjunto não vazio de $\mathbb{N}^n$ que não tem menor elemento. Assim, $\succ$ não é uma boa ordenação. □

Apresentaremos a seguir três exemplos que assumiremos a princípio, sem prova, serem ordens monomiais. Na Seção 2.2 faremos a prova de que a ordem lex é ordem monomial. Nos dois outros casos, basta prosseguir de maneira análoga.

Sejam $\alpha = (\alpha_1, \ldots, \alpha_n)$ e $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$. Recordemos que

$$|\alpha| = \sum_{i=1}^{n} \alpha_i \text{ e } |\beta| = \sum_{i=1}^{n} \beta_i.$$

Definimos:

1. **Ordem Lexicográfica**(ou **ordem lex**): Dizemos que $\alpha \succ_{lex} \beta$ se no vetor diferença $\alpha - \beta \in \mathbb{N}^n$ a primeira coordenada não nula, da esquerda para a direita, é positiva. Escrevemos $x^\alpha \succ_{lex} x^\beta$ se $\alpha \succ \beta$.

2. **Ordem Lexicográfica Graduada**(ou **ordem grlex**): Dizemos que $\alpha \succ_{grlex} \beta$ e escrevemos $x^\alpha \succ_{grlex} x^\beta$, se

$$|\alpha| > |\beta| \quad \text{ou} \quad |\alpha| = |\beta| \text{ e } \alpha \succ_{lex} \beta.$$

3. **Ordem Lexicográfica Graduada Reversa**(ou **ordem grevlex**): Diremos que

$$\alpha \succ_{grevlex} \beta$$

e escrevemos $x^\alpha \succ_{grevlex} x^\beta$, se

$$|\alpha| > |\beta| \text{ ou } |\alpha| = |\beta| \text{ e a primeira coordenada não nula em } \alpha - \beta, \text{ da direita para a esquerda, é negativa.}$$

Vejamos um exemplo pra ilustrar a ordenação dos termos de um polinômio em $K[x_1, \ldots, x_n]$.

Exemplo 2.1.2. *Seja* $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in K[x, y, z]$. *Então os termos de* f *reordenados de maneira decrescente ficam da seguinte forma:*

- *Ordem lexicográfica:* $f = -5x^3 + 7x^2y^2 + 4xy^2z + 4z^2$
- *Ordem lexicográfica graduada:* $f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$
- *Ordem lexicográfica graduada reversa:* $f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$

Seja $f = \sum_\alpha a_\alpha x^\alpha$ um polinômio não nulo em $K[x_1, \ldots, x_n]$ e seja $\succ$ a ordem monomial. O **multigrau** de f, denotado por multg(f) é o máximo do conjunto $\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}$. O **coeficiente líder** de f é CL(f) $= a_{\text{multg}(f)} \in K$. Chamamos $x^{\text{multg}(f)} = ML(f)$ de **monômio líder** de f e TL(f)=CL(f)ML(f), é dito ser o **termo líder** de f. Por exemplo, considere $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ e seja $\succ$ a ordem lex. Então:

$$\begin{aligned} \text{multg}(f) &= (3, 0, 0); \\ \text{CL}(f) &= -5; \\ \text{ML}(f) &= x^3; \\ \text{TL}(f) &= -5x^3. \end{aligned}$$

Com a definição de ordem monomial em $K[x_1,\ldots,x_n]$, é possível exibir um algoritmo da divisão em $K[x_1,\ldots,x_n]$ que possibilita dividir um polinômio $f \in K[x_1,\ldots,x_n]$ por $f_1,\ldots,f_n \in K[x_1,\ldots,x_n]$, com respeito a uma ordem monomial pré determinada. Isto significa que podemos expressar f na forma

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

sendo $q_1,\ldots,q_s$ e r pertencentes a $K[x_1,\ldots,x_n]$.

Apresentaremos a seguir o teorema que trata deste algoritmo.

Teorema 2.1.3 (Algoritmo da divisão em $K[x_1,\ldots,x_n]$). *Seja $\succ$ uma ordem monomial em $\mathbb{N}^n$ e seja $F = (f_1,\ldots,f_s)$ uma s-upla ordenada de polinômios em $K[x_1,\ldots,x_n]$. Então todo polinômio $f \in K[x_1,\ldots,x_n]$ pode ser escrito como*

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

sendo $q_1,\ldots,q_s,r \in K[x_1,\ldots,x_n]$ e ou $r = 0$ ou r é uma combinação linear, com coeficientes em K, de monômios tais que nenhum deles é divisível por algum dos $TL(f_i)$, para todo i. Chamaremos r de resto da divisão de f por F. Além disso, se $q_i f_i \neq 0$, então

$$multg(f) \succeq multg(q_i f_i).$$

Demonstração. Ver ([8], p.64). □

O Algoritmo:

Entrada: $f_1,\ldots,f_s,f$
Saída: $q_1,\ldots,q_s,r$
$q_1 := 0,\ldots,q_s := 0, r := 0$
$p := f$
Enquanto $p \neq 0$ **faça**
  $i := 1$
  divisão sucedida:=falso
  Enquanto $i \leq s$ **e** divisão sucedida = falso **Faça**
    Se $TL(fi)$divide$TL(p)$ **Então**
      $qi := qi + TL(p)/TL(f_i)$
      $p := p - (TL(p)/TL(fi))f_i$
      divisão sucedida = falso
    Senão
      $i := i + 1$
  Se divisão sucedida = false **Então**
    $r := r + TL(p)$
    $p := p - TL(p)$
Retorne $q_1,\ldots,q_s,r$ Vejamos alguns exemplos de como esse algoritmo funciona na prática:

Exemplo 2.1.4. *Vamos dividir $f = xy^2 + 1$ por $f_1 = xy + 1$ e $f_2 = y + 1$, usando a ordem lex, com $x \succ y$.*

$$\begin{array}{r|l} xy^2 + 1 & \begin{array}{l} xy + 1 \\ y + 1 \end{array} \\ \hline q_1 : & \\ q_2 : & \end{array}$$

Observe que tanto $TL(f_1) = xy$ como $TL(f_2) = y$ dividem $TL(f)$. Começaremos a divisão com o primeiro da lista, no caso, f_1. Assim, temos

$$\begin{array}{rl} xy^2+1 & \left|\begin{array}{l} xy+1 \\ \hline y+1 \end{array}\right. \\ \underline{-xy^2-y} & q_1 : y \\ -y+1 & q_2 : \end{array}$$

Repetimos o mesmo processo com $-y+1$. *Agora usando* f_2. *Daí,*

$$\begin{array}{rl} xy^2+1 & \left|\begin{array}{l} xy+1 \\ \hline y+1 \end{array}\right. \\ \underline{-xy^2-y} & q_1 : y \\ -y+1 & q_2 : -1 \\ \underline{y+1} & \\ 2 & \end{array}$$

Como 2 *não é divisível por* $TL(f_1)$ *nem por* $TL(f_2)$, *segue que o resto é* 2. *Portanto,*

$$xy^2+1 = y(xy+1)+(-1)(y+1)+2.$$

Exemplo 2.1.5. *Vamos agora dividir* $f = x^2y+xy^2+y^2$ *por* $f_1 = xy-1$ *e* $f_2 = y^2-1$, *usando também a ordem lex com* $x \succ y$. *Procedendo como no exemplo anterior, temos*

$$\begin{array}{rl} x^2y+xy^2+y^2 & \left|\begin{array}{l} xy-1 \\ \hline y^2-1 \end{array}\right. \\ \underline{-xy^2+x} & q_1 : x+y \\ xy^2+x+y^2 & q_2 : \\ \underline{-xy^2+y} & \\ x+y^2+y & \end{array}$$

Note que nem $TL(f_1)$ *nem* $TL(f_2)$ *dividem o* $TL(x+y^2+y) = x$. *Portanto* x *vai para o resto*

$$\begin{array}{rlcl} x^2y+xy^2+y^2 & \left|\begin{array}{l} xy-1 \\ \hline y^2-1 \end{array}\right. & & \underline{resto} \\ \underline{-xy^2+x} & q_1 : x+y & & \\ xy^2+x+y^2 & q_2 : & & \\ \underline{-xy^2+y} & & & \\ \underline{x+y^2+y} & & \longrightarrow & x \\ y^2+y & & & \end{array}$$

Continuando a divisão, temos

$$\begin{array}{rlcl} x^2y+xy^2+y^2 & \left|\begin{array}{l} xy-1 \\ \hline y^2-1 \end{array}\right. & & \underline{resto} \\ \underline{-xy^2+x} & q_1 : x+y & & \\ xy^2+x+y^2 & q_2 : 1 & & \\ \underline{-xy^2+y} & & & \\ \underline{x+y^2+y} & & \longrightarrow & x \\ y^2+y & & & \\ \underline{-y^2+1} & & & \\ \underline{y+1} & & \longrightarrow & x+y \\ \underline{1} & & \longrightarrow & x+y+1 \\ 0 & & & \end{array}$$

Logo, o resto é $x+y+1$ *e temos,*

$$x^2y+xy^2+y^2 = (x+y)(xy-1)+1(y^2-1)+x+y+1.$$

Uma observação importante a ser feita sobre o algoritmo da divisão em $K[x_1, \ldots, x_n]$ é que os quocientes e o resto, podem variar de acordo com a ordem que os polinômios $f_i's$ são listados. Por exemplo, para $f = xy^2 - x$ temos:

$$\begin{aligned} xy^2 - x &= y(xy-1) + 0(y^2-1) + (-x+y) \\ &= x(y^2-1) + 0(xy-1) + 0. \end{aligned}$$

2.2 Ideais Monomiais e Lema de Dickson

Seja $A \subset \mathbb{N}^n$. Chamamos o ideal $I = \langle x^\alpha | \, \alpha \in A \rangle \subseteq K[x_1, \ldots, x_n]$ de **ideal monomial**.

Exemplo 2.2.1. *$I = \langle x^4 2, x\ 3y^4, x^2y^5 \rangle \subseteq K[x,y]$ é um ideal monomial.*

Lema 2.2.2. *Seja $I = \langle x^\alpha | \, \alpha \in A \rangle$ um ideal monomial. Então um monômio x^β pertence a I se, e somente se, x^β é divisível por x^α para algum $\alpha \in A$.*

Demonstração. Se x^β é um múltiplo de x^α para algum $\alpha \in A$, então $x^\beta \in I$ por definição de ideal.

Reciprocamente, se $x^\beta \in I$, então

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}, \quad h_i \in K[x_1, \ldots, x_n] \quad \text{e} \quad \alpha(i) \in A.$$

Podemos escrever cada h_i, como $h_i = \sum_j c_{i,j} x^{\beta(i,j)}$, com $c_{i,j} \in K$. Assim,

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)} = \sum_{i=1}^{s} \left(\sum_j c_{i,j} x^{\beta_{i,j}} \right) x^{\alpha(i)} = \sum_{i,j} c_{i,j} x^{\beta_{i,j}} x^{\alpha(i)}.$$

Como o lado esquerdo da igualdade é um monômio, o lado direito também deverá ser. Logo, alguns termos da soma à direita irão se cancelar. Observe que cada termo da soma do lado direito da igualdade é divisível por algum $x^\alpha(i)$. Sendo assim, x^β tem a mesma propriedade. □

Lema 2.2.3. *Sejam $I = \langle x^\alpha | \, \alpha \in A \rangle$ um ideal monomial e $f \in K[x_1, \ldots, x_n]$. Então as seguintes afirmações são equivalentes:*

(i) $f \in I$

(ii) *Todo termo de f está em I*

(iii) *f é uma combinação $K-$linear de monômios de I.*

Demonstração. As implicações $(iii) \Rightarrow (ii) \Rightarrow (i)$ e $(ii) \Rightarrow (iii)$ são triviais. Falta então mostrarmos que $(i) \Rightarrow (iii)$. Para isto, seja $f \in I$. Da mesma forma com a qual escrevemos x^β no Lema 2.2.2, podemos escrever f, ou seja,

$$f = \sum_{i,j} c_{i,j} x^{\beta_{i,j}} x^{\alpha(i)} = \sum_{i,j} c_{i,j} \left(x^{\beta_{i,j} + \alpha(i)} \right), \quad c_{i,j} \in K.$$

Como cada $x^{\beta_{i,j}+\alpha(i)} \in I$, concluímos que f é uma combinação $K-$linear de monômios de I. □

Corolário 2.2.4. *Dois ideais monomiais I e $\tilde{I}$ são os mesmos se, e somente se, eles contém os mesmos monômios.*

Demonstração. Obviamente, dois ideais iguais possuem os mesmos monômios. Por outro lado, pelo Lema 2.2.3 segue que

$$\begin{aligned} f \in I \Leftrightarrow & f \text{ é uma combinação } K-\text{linear de monômios de } I \\ \Leftrightarrow & f \text{ é uma combinação } K-\text{linear de monômios de } \tilde{I} \\ \Leftrightarrow & f \in \tilde{I}. \end{aligned}$$

Portanto, $I = \tilde{I}$. □

Teorema 2.2.5 (Lema de Dickson). *Sejam $A \subset \mathbb{N}^n$ e $I = \langle x^\alpha | \, \alpha \in A \rangle \subset K[x_1, \ldots, x_n]$. Então I pode ser escrito na forma $\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, sendo $\alpha(1), \ldots, \alpha(s) \in A$. Em particular, I tem uma base finita.*

Demonstração. Vamos provar o resultado por indução sobre o número de variáveis n. Se $n = 1$, então

$$I = \langle x_1^\alpha | \, \alpha \in A \subseteq \mathbb{N}^n \rangle.$$

Seja β o menor elemento em $A \subseteq \mathbb{N}^n$. Então $\beta \preceq \alpha$ para todo $\alpha \in A$. Sendo assim, x_1^β divide todos os outros geradores x_1^α, implicando que $I = \langle x_1^\beta \rangle$.

Vamos assumir agora que $n > 1$ e que o teorema seja verdadeiro para $n-1$. Escrevemos as variáveis como $x_1, \ldots, x_{n-1}, y$, de forma que os monômios em $K[x_1, \ldots, x_n]$ possam ser escritos como $x^\alpha y^m$, com $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}^n$ e $m \in \mathbb{N}$.

Suponhamos que $I \subseteq K[x_1, \ldots, x_{n-1}, y]$ seja um ideal monomial. Considere o ideal

$$J = \langle x^\alpha | \, x^\alpha y^m \in I \text{ para algum } m \geq 0 \rangle.$$

Note que J é um ideal monomial em $K[x_1, \ldots, x_{n-1}]$ e por hipótese de indução segue que

$$J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle.$$

Sendo assim, por definição de J, para cada $i = 1, \ldots, s$ existe $m_i \geq 0$ tal que $x^{\alpha(i)} y^{m_i} \in I$. Seja

$$M = max \{m_1, \ldots, m_s\}$$

e considere o ideal

$$J_k = \langle x^\beta | \, x^\beta y^k \in I \rangle,$$

para $0 \leq k \leq M-1$. Novamente por hipótese de indução segue que

$$J_k = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s_k)} \rangle.$$

AFIRMAÇÃO: I é gerado pelo seguinte conjunto de monômios:

$$W = \left\{ x^{\alpha(j)} y^M | \, 1 \leq j \leq s \right\} \cup \left\{ x^{\alpha_k(i)} y^k | \, 0 \leq k \leq M-1 \text{ e } 1 \leq i \leq s_k \right\}.$$

Por construção de J e cada J_k, temos que todos os elementos de W pertencem a I. Pelo Lema 2.2.2 obtemos que todo monômio de $\langle W \rangle$ também está em I. Para vermos a outra inclusão, tome $x^\gamma y^q \in I$. Se $q \geq M$, então por definição de J temos que $x^\gamma \in J$. Logo, existe $x^{\alpha(j)} \in J$, tal que $x^{\alpha(j)} | x^\gamma$. Consequentemente, $x^{\alpha(j)} y^M | x^\gamma y^q$. Se por outro lado, $0 \leq q \leq M-1$, então $x^\gamma \in J_q$. O que implica que existe $x^{\alpha_q(i)} \in J_q$ de tal forma que $x^{\alpha_q(i)} | x^\gamma$, donde segue que $x^{\alpha_q(i)} y^q | x^\gamma x^q$. Novamente do Lema 2.2.2, temos que cada monômio de I está em $\langle W \rangle$. Portanto, pelo Corolário 2.2.4 $I = \langle W \rangle$.

Para completar a prova, devemos mostrar que o conjunto finito de geradores pode ser obtido a partir de um determinado conjunto de geradores do ideal. Voltando a escrever as variáveis

como $x_1, \ldots, x_n$, nosso ideal monomial será $I = \langle x^\alpha | \, \alpha \in A \rangle \subseteq K[x_1, \ldots, x_n]$. Precisamos mostrar que I é gerado por finitos x^α's, tais que $\alpha \in A$. Vimos no parágrafo anterior que $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle$, sendo $x^{\beta(i)}$ monômios em I. Como $x^{\beta(i)} \in I = \langle x^\alpha | \, \alpha \in A \rangle$, existe $\alpha(i) \in A$, de tal forma que $x^{\alpha(i)} | x^{\beta(i)}$. Isso implica que

$$I \subseteq \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle.$$

Claramente $\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle \subseteq I$. Portanto, $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. □

Corolário 2.2.6. *Seja $\succ$ uma relação em $\mathbb{N}^n$ satisfazendo:*

(i) $\succ$ é uma ordenação total sobre $\mathbb{N}^n$.

(ii) Se $\alpha \succ \beta$ e $\gamma \in \mathbb{N}^n$, então $\alpha + \gamma \succ \beta + \gamma$.

Então $\succ$ é uma boa ordenação se, e somente se, $\alpha \succeq 0$, para todo $\alpha \in \mathbb{N}^n$.

Demonstração. Supondo que $\succ$ é uma boa ordenação, chamemos de α_0 o menor elemento de $\mathbb{N}^n$. É suficiente mostrar que $\alpha_0 \succeq 0$. Observe que se $\alpha_0 \prec 0$, então pela hipótese (ii) temos que $\alpha_0 \succ 2\alpha_0$. O que é impossível, pois α_0 é o menor elemento de $\mathbb{N}^n$.

Para provar a recíproca, suponhamos que $\alpha \succeq 0$ para todo $\mathbb{N}^n$ e seja $A \subseteq \mathbb{N}^n$, não vazio. Precisamos mostrar que A tem um menor elemento. Se $I = \langle x^\alpha | \, \alpha \in A \rangle$ é um ideal monomial, pelo Lema de Dickson existem $\alpha(1), \ldots, \alpha(s) \in A$ tais que $I = \langle \alpha(1), \ldots, \alpha(s) \rangle$. Sem perda de generalidade, podemos assumir que $\alpha(1) \succ \ldots \succ \alpha(s)$. Afirmamos que $\alpha(1)$ é o menor elemento de A. Para provar isto, tome $\alpha \in A$. Então $\alpha \in I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ e pelo Lema 2.2.2 x^α é divisível por algum $x^{\alpha(i)}$. Isso significa que $\alpha = \alpha(i) + \gamma$ para algum $\gamma \in \mathbb{N}^n$. Então, $\gamma \succeq 0$ e pela hipótese (ii) implica que

$$\alpha = \alpha(i) + \gamma \succeq \alpha(i) + 0 \succeq \alpha(1).$$

Portanto, $\alpha(1)$ é o menor elemento de A. □

Com o resultado deste corolário fica bastante simples verificarmos que a ordem lex, definida na Seção 2.1 é de fato uma ordem monomial.

Proposição 2.2.7. *A ordem lex em $\mathbb{N}^n$ é uma ordem monomial.*

Demonstração. Devemos verificar que a ordem lex satisfaz as condições (i) e (ii) do Corolário 2.2.6 e que $\alpha \succeq_{lex} 0$ para todo $\alpha \in \mathbb{N}^n$.

(i) Que $\succ_{lex}$ é uma ordem total segue diretamente da definição e do fato que a ordem numérica usual sobre $\mathbb{N}^n$ é total.

(ii) Se $\alpha \succ_{lex} \beta$, então a primeira coordenada não nula, da esquerda para a direita, de $\alpha - \beta$, digamos $\alpha_i - \beta_i$, é positiva. Note que

$$(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta.$$

Assim, a coordenada não nula mais à esquerda de $(\alpha+\gamma)-(\beta+\gamma)$, continua sendo $\alpha_i - \beta_i$. Portanto, $\alpha + \gamma \succ_{lex} \beta + \gamma$.

Por fim, seja $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. Se todas as entradas de α são nulas, então $\alpha - 0 = 0$ e está provado o resultado. Caso contrário, temos $\alpha - 0 = \alpha$. Como todas as entradas não nulas de α estão em $\mathbb{N}$, segue o resultado. □

2.3 Base Finita de um Ideal em $K[x_1, \ldots, x_n]$

Sabemos que se $I \subseteq K[x]$ é um ideal, então existe $f \in I$ tal que $I = \langle f \rangle$, ou seja, todo ideal no anel polinomial de uma variável é finitamente gerado. Este resultado decorre do algoritmo da divisão em $K[x]$ que foi generalizado no Teorema 2.1.3 para o caso de um anel polinomial com várias variáveis. Veremos a seguir que com este resultado, podemos garantir para um ideal $I \subseteq K[x_1, \ldots, x_n]$, a existência de polinômios $f_1, \ldots, f_s$ tais que $I = \langle f_1, \ldots, f_s \rangle$.

Fixada uma ordem monomial, podemos determinar o $TL(f)$, para qualquer $f \in K[x_1, \ldots, x_n]$ não nulo. Consideremos um ideal $I \subseteq K[x_1, \ldots, x_n]$ e o conjunto dado por

$$TL(I) = \{cx^\alpha | \, \exists \, f \in I \backslash \{0\} \text{ com } TL(f) = cx^\alpha\}.$$

Seja $\langle TL(I) \rangle$ o ideal gerado pelos elementos de $TL(I)$. Note que $\langle TL(I) \rangle$ é igual ao ideal monomial $\langle ML(f) | \, f \in I \backslash \{0\} \rangle$, e portanto é também um ideal monomial. Ainda, pelo Lema de Dickson podemos obter $g_1, \ldots, g_t \in I$ tais que $\langle TL(I) \rangle = \langle TL(g_1), \ldots, TL(g_t) \rangle$. Observe que $\langle TL(g_1), \ldots, TL(g_t) \rangle = \langle ML(g_1), \ldots, ML(g_t) \rangle$.

Uma pergunta que poderíamos fazer é: Se um ideal I possui um conjunto finito de geradores, digamos $I = \langle f_1, \ldots, f_s \rangle$, então $\langle TL(f_1), \ldots, TL(f_s) \rangle = \langle TL(I) \rangle$? A resposta é não. Por definição, temos que $TL(f_i) \in TL(I) \subseteq \langle TL(I) \rangle$ e isso implica que a inclusão $\langle TL(f_1), \ldots, TL(f_s) \rangle \subseteq \langle TL(I) \rangle$ sempre ocorre. No entanto, $\langle TL(I) \rangle$ pode ser estritamente maior. Considere o seguinte exemplo.

Exemplo 2.3.1. *Seja $I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$ e a ordem monomial grlex em $K[x, y]$. Daí,*

$$x^2 = x(x^2y - 2xy + x) - y(x^3 - 2xy)$$

de modo que $x^2 \in I$. Dessa forma $TL(x^2) \in \langle TL(I) \rangle$, mas $x^2 \notin \langle x^3, x^2y \rangle$, pois x^2 não é divisível por $x^3 = TL(f_1)$ nem por $x^2y = TL(f_2)$ (Lema 2.2.2).

Dizemos que um subconjunto $G = \{g_1, \ldots, g_t\}$ de um ideal $I \subseteq K[x_1, \ldots, x_n]$ não nulo, é uma **base de Gröbner** de I, quando temos $\langle TL(g_1), \ldots, TL(g_t) \rangle = \langle TL(I) \rangle$.

Proposição 2.3.2. *Seja I um ideal polinomial em $K[x_1, \ldots, x_n]$. Dizer que $G = \{g_1, \ldots, g_t\}$ é uma base de Gröbner para I é equivalente a dizer que para todo $f \in I$, $TL(f)$ é múltiplo de algum $TL(g_i)$.*

Demonstração. Se dado $f \in I$, $TL(f)$ é múltiplo de $TL(g_i)$ para algum $g_i \in G$, pelo Lema 2.2.2 $TL(f) \in \langle TL(g_1), \ldots, TL(g_s) \rangle$. Logo, $\langle TL(I) \rangle \subseteq \langle TL(g_1), \ldots, TL(g_s) \rangle$ e como a outra inclusão é trivial, concluímos que G é base de Gröbner para I.

Agora, suponha que $G = \{g_1, \ldots, g_t\}$ seja base de Gröbner para I. Dado $f \in I$, temos que $TL(f) = CL(f)ML(f) \in \langle TL(g_1), \ldots, TL(g_s) \rangle = \langle ML(g_1), \ldots, ML(g_s) \rangle$. Novamente pelo Lema 2.2.2, temos que $ML(f)$ é divisível por algum $ML(g_i)$ e consequentemente $TL(f)$ é divisível por $TL(g_i)$. □

Teorema 2.3.3 (Teorema das bases de Hilbert). *Todo ideal $I \subseteq K[x_1, \ldots, x_n]$ tem um conjunto finito de geradores, isto é, $I = \langle f_1, \ldots, f_s \rangle$ para certos $f_1, \ldots, f_s \in I$.*

Demonstração. Se $I = \{0\}$ então tomamos $\{0\}$ como conjunto gerador. Se I contém algum polinômio não nulo, então podemos construir um conjunto de geradores $f_1, \ldots, f_s$ como segue. Primeiro fixamos um ordem monomial para usar no algoritmo da divisão e determinar os termos líderes dos polinômios em I. Consideremos agora, o ideal $\langle TL(I) \rangle$, que por ser um ideal monomial, pelo Lema de Dickson possui um conjunto finito de geradores, isto é, existem $f_1, \ldots, f_s \in I$ tais que $\langle TL(I) \rangle = \langle ML(f_1), \ldots, ML(f_s) \rangle$. Vejamos que $I = \langle f_1, \ldots, f_s \rangle$.

Como $f_i \in I$ para todo $i = 1, \ldots, s$, temos claramente que $\langle f_1, \ldots f_s \rangle \subseteq I$. Reciprocamente, seja $f \in I$ um polinômio qualquer. Dividindo f por $f_1, \ldots, f_s$ temos a seguinte expressão

$$f = q_1 f_1 + \cdots + f q_s f_s + r$$

com $r = 0$ ou nenhum termo de r é divisível por $TL(f_i)$ para todo i.

Suponha que $r \neq 0$. Então,

$$r = f - q_1 f_1 + \cdots + f q_s f_s \in I.$$

Segue daí que $TL(r) \in \langle TL(I) \rangle = \langle ML(f_1), \ldots, ML(f_s) \rangle$. Pela Proposição 2.3.2, concluímos que $TL(r)$ é múltiplo de algum $TL(f_i)$. O que contradiz a definição de resto da divisão.

Portanto, $r = 0$ e $f = q_1 f_1 + \cdots + q_s f_s$. Mostrando que $I \subseteq \langle f_1, \ldots, f_s \rangle$. □

Corolário 2.3.4. *Fixada uma ordem monomial, temos que cada ideal $I \subseteq K[x_1, \ldots, x_n]$ tem uma base de Gröbner. Além disso, cada base de Gröbner de um ideal I é uma base de I.*

Demonstração. Consequência imediata da demonstração do Teorema 2.3.3. □

Observação 2.3.5. *Uma outra consequência do Teorema 2.3.3 é a respeito de variedade afim, que agora pode ser definida por um ideal e não somente por um conjunto finito de polinômios. Denotamos por $\boldsymbol{V}(I)$ o conjunto*

$$\boldsymbol{V}(I) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n_K \,|\, f(a_1, \ldots, a_n) = 0 \text{ para todo } f \in I\}.$$

Mesmo que um ideal I diferente de zero, contenha infinitos polinômios diferentes, o conjunto $\mathbf{V}(I)$ ainda pode ser definido por um conjunto finito de equações polinomiais.

Proposição 2.3.6. *Seja $I \subseteq K[x_1, \ldots, x_n]$ um ideal. Então $V(I)$ é uma variedade afim. Em particular, se $I = \langle f_1, \ldots, f_s \rangle$, temos $\boldsymbol{V}(I) = V(f_1, \ldots, f_s)$.*

Demonstração. Pelo Teorema das Bases de Hilbert 2.3.3, $I = \langle f_1, \ldots, f_s \rangle$ para um conjunto finito de geradores. Basta provarmos que $\mathbf{V}(I) = V(f_1, \ldots, f_s)$. De fato, se $(a_1, \ldots, a_n) \in \mathbf{V}(I)$, então $f(a_1, \ldots, a_n) = 0$ para todo $f \in I$. Segue daí que $f_i(a_1, \ldots, a_n) = 0$ para todo i. Consequentemente $\mathbf{V}(I) \subseteq V(f_1, \ldots, f_s)$. Por outro lado, tome $(b_1, \ldots, b_n) \in V(f_1, \ldots, f_s)$ e seja $f \in I$. Como $I = \langle f_1, \ldots, f_s \rangle$, segue que $f = \sum_{i=1}^{s} h_i f_i$ com $h_i \in K[x_1, \ldots, x_n]$. Então,

$$f(b_1, \ldots, b_n) = \sum_{i=1}^{s} h_i(b_1, \ldots, b_n) f_i(b_1, \ldots, b_n) = \sum_{i=1}^{s} h_i(b_1, \ldots, b_n) \cdot 0 = 0.$$

Portanto, $V(f_1, \ldots, f_s) \subseteq \mathbf{V}(I)$ e assim concluímos que $\mathbf{V}(I) = V(f_1, \ldots, f_s)$, provando que $\mathbf{V}(I)$ é uma variedade afim. □

Sendo assim, podemos estabelecer uma relação entre ideais e variedades como mostra o próximo teorema.

Teorema 2.3.7. *Considere as aplicações:*

$$\textit{Variedades afins} \xrightarrow{\boldsymbol{I}} \textit{Ideais}$$

e

$$\textit{Ideais} \xrightarrow{\boldsymbol{V}} \textit{Variedades afins}$$

(i) Se $I_1 \subseteq I_2$, então $\boldsymbol{V}(I_1) \supseteq \boldsymbol{V}(I_2)$. Do mesmo modo se $V_1 \subseteq V_2$ são variedades, então $\boldsymbol{I}(V_1) \supseteq \boldsymbol{I}(V_2)$.

(ii) Para qualquer variedade V,

$$\boldsymbol{V}(\boldsymbol{I}(V)) = V.$$

Consequentemente, temos que $\boldsymbol{I}$ é injetora.

Demonstração. (i) Suponha que $I_1 \subset I_2$ e tome $a = (a_1, \ldots, a_n) \in \mathbf{V}(I_2)$. Então para todo $f \in I_2$, $f(a) = 0$. Como, $I_1 \subset I_2$, segue que $g(a) = 0$, para todo $g \in I_1$, ou seja, $a \in \mathbf{V}(I_1)$. Portanto, $V(I_2) \subseteq \mathbf{V}(I_1)$. Suponha agora que $V_1 \subseteq V_2$ e tome $f \in \mathbf{I}(V_2)$. Por definição, $f(a) = 0$, para todo $a \in V_2$. Como $V_1 \subseteq V_2$, segue que $f(a) = 0$, para todo $b \in V_1$. Logo, $f \in \mathbf{I}(V_1)$ e $\mathbf{I}(V_2) \subseteq \mathbf{I}(V_1)$.

(ii) Dado $b \in V$, temos que $f(b) = 0$, para cada $f \in \mathbf{I}(V)$. Como b é qualquer, segue que $V \subseteq \mathbf{V}(I(V))$

□

Abaixo segue outra consequência bastante importante do Teorema das Bases de Hilbert.

Vimos anteriormente que o algoritmo da divisão em $K[x_1, \ldots, x_n]$ não nos garante unicidade do resto. Veremos a seguir que ao dividirmos por uma base de Gröbner esta situação muda.

Proposição 2.3.8. *Sejam $I \subseteq K[x_1, \ldots, x_n]$ um ideal e $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner para I. Então dado $f \in K[x_1, \ldots, x_n]$, existe um único $r \in K[x_1, \ldots, x_n]$ com as duas propriedades a seguir:*

a) Ou $r = 0$ ou nenhum termo de r é divisível por qualquer dos $TL(g_i)$, para cada i.

b) Existe $g \in I$ tal que $f = g + r$.

Em particular, r é o resto da divisão de f pelos elementos de G, não importando a maneira como os elementos de G estão listados no algoritmo da divisão.

Demonstração. Pelo algoritmo da divisão podemos escrever $f = q_1 g_1 + \ldots + q_s g_s + r$, com r satisfazendo a condição a). Para satisfazer a condição b), basta tomarmos $g = q_1 g_1 + \ldots + q_s g_s \in I$. Temos assim, provada a existência de r. Para mostramos a unicidade, suponha que

$$f = g + r_1 = h + r_2$$

com g, h, r_1 e r_2 satisfazendo a) e b). isso implica que $r_1 - r_2 = h - g \in I$. Logo, $r_1 - r_2 = 0$. Caso contrário, teríamos $TL(r_1 - r_2) \in \langle TL(I)\rangle = \langle TL(g_1), \ldots, TL(g_s)\rangle$, ou seja $TL(r_1 - r_2)$ seria divisível por algum $TL(g_i)$. Mas isso não pode ocorrer, uma vez que nenhum dos termos de r_1 e r_2 são divisíveis por nenhum dos $TL(g_1), \ldots, TL(g_s)$. Portanto $r_1 = r_2$. □

Observação 2.3.9. *A Proposição 2.3.8 nos garante somente a unicidade do resto da divisão. Note que os quocientes $q_i's$ ainda podem variar de acordo com a ordem que os elementos de G são listados no algoritmo da divisão.*

Com este resultado podemos agora determinar quando um dado polinômio f pertence ou não a um ideal I.

Corolário 2.3.10. *Seja $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner para o ideal $I \subseteq K[x_1, \ldots, x_n]$ e seja $f \in K[x_1, \ldots, x_n]$. Então $f \in I$ se, e somente se, o resto da divisão de f por G é zero.*

Demonstração. Claramente se o resto é zero, temos $f \in K[x_1, \ldots, x_n]$. Reciprocamente, suponha que $f \in I$. Então,

$$f = \sum_{i=1}^{s} q_i g_i, \text{ com } q_i \in K[x_1, \ldots, x_n]$$

por definição de ideal gerado. Desta forma, $r = 0$ é tal que $f = \sum_{i=1}^{s} q_i g_i + 0$. Satisfazendo as duas propriedades da Proposição 2.3.8. Portanto o resto da de divisão de f por G é zero. □

2.4 Algoritmo de Buchberger

Vimos que todo ideal em $K[x_1, \ldots, x_n]$ possui uma base de Gröbner. O teorema seguinte, apresenta um algoritmo para a construção de uma base de Gröbner para um ideal, a partir de um conjunto finito de geradores. Sejam $f, g \in K[x_1, \ldots, x_n]$ polinômios não nulos e bx^α e cx^β, os termos líderes de f e g, respectivamente. Para cada $i \in \{1, \ldots, n\}$, consideremos $\gamma_i = max(\alpha_i, \beta_i)$ e $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{N}^n$. O **S-polinômio** de f e g é a combinação

$$S(f, g) = \frac{x^\gamma}{bx^\alpha} f - \frac{x^\gamma}{cx^\beta} g.$$

Denotaremos por $\overline{f}^F$ o resto da divisão de f por uma $s-$upla ordenada $F = (f_1, \ldots, f_s)$.

Teorema 2.4.1. *Seja $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ um ideal polinomial. Então uma base de Gröbner de I pode ser construída em um número finito de passos pelo algoritmo a seguir:*

Entrada: F=$(f_1, \ldots, f_s)$
Saída: uma base de Gröbner $G : (g_1, \ldots, g_t)$ para I, com $F \subseteq G$
$G := F$
Repita
  $G' := G$
  Para cada par $\{p, q\}$, $p \neq Q$ em G' **Faça**
    $r := \overline{S(p, q)}^{G'}$
    Se $r \neq 0$ **Então** $G := G \cup \{r\}$
Até $G = G'$
Retorne G

Demonstração. Ver ([8], p.91). □

Exemplo 2.4.2. *Considere o anel $\mathbb{Q}[x, y]$ com a ordem grlex e*

$$I = \langle f_1, f_2 \rangle = \left\langle x^3 - 2xy, x^2y - 2y^2 + x \right\rangle,$$

então $F := \{x^3 - 2xy, x^2y - 2y^2 + x\}$. Calculando o S-polinômio de f_1 e f_2 temos:

$$\begin{aligned} S(f_1, f_2) &= y(x^3 - 2xy) - x(x^2y - 2y^2 + x) = -x^2 \\ \overline{S(f_1, f_2)}^F &= -x^2 \neq 0. \end{aligned}$$

Então $f_3 := -x^2$ e $F := \{f_1, f_2, f_3\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2\}$ Agora,

$$\begin{aligned} S(f_1, f_2) &= f_3 \\ \overline{S(f_1, f_2)}^F &= 0 \\ S(f_1, f_3) &= x^3 - 2xy + x(-x^2) = -2xy \\ \overline{S(f_1, f_3)}^F &= -2xy \neq 0. \end{aligned}$$

Então $f_4 := -2xy$ e $F := \{f_1, f_2, f_3, f_4\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy\}$.
Segue que,

$$\begin{aligned} \overline{S(f_1, f_2)}^F &= \overline{S(f_1, f_3)}^F = 0 \\ S(f_1, f_4) &= 2y(x^3 - 2xy) = x^2(-2xy) = -2xy^2 = -yf_4. \end{aligned}$$

Assim,

$$\overline{S(f_1, f_4)}^F = 0.$$

Prosseguindo com o algoritmo, temos

$$\begin{aligned} S(f_2, f_3) &= x^2y - 2y^2 + x + y(-x^2) = -2y^2 + x \\ \overline{S(f_2, f_3)}^F &= -2y^2 + x \neq 0. \end{aligned}$$

Daí, $f_5 := -2y^2+x$ *e* $F := \{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$.

Conferindo os restos dos S-polinômios, obtemos:

$$\begin{aligned} S(f_1, f_5) &= y^2(x^3 - 2xy) + \frac{1}{2}x^3(-2y^2 + x) = \frac{1}{2}x^4 - 2xy^3 \\ &= \frac{1}{2}xf_1 + (y^2 - \frac{1}{2}x)f_4 \\ S(f_2, f_3) &= f_5 \\ S(f_2, f_4) &= x^2y - 2y^2 + x + \frac{1}{2}x(-2xy) = -2y^2 + x = f_5 \\ S(f_2, f_5) &= y(x^2y - 2y^2 + x) + \frac{1}{2}x^2(-2y^2 + x) = \frac{1}{2}x^3 - 2y^3 + xy \\ &= -\frac{1}{2}xf_3 + yf_5 \\ S(f_3, f_4) &= -y(-x^2) + \frac{1}{2}x(-2xy) = 0 \\ S(f_3, f_5) &= -y^2(-x^2) + \frac{1}{2}x^2(-2y^2 + x) = \frac{1}{2}x^3 \\ &= -\frac{1}{2}xf_3 \\ S(f_4, f_5) &= -\frac{1}{2}y(-2xy) + \frac{1}{2}(-2y^2 + x) = \frac{1}{2}x^2 \\ &= -\frac{1}{2}f_3. \end{aligned}$$

Logo,

$$\overline{S(f_1, f_5)}^F = \overline{S(f_2, f_3)}^F = \overline{S(f_2, f_4)}^F = \overline{S(f_2, f_5)}^F = \overline{S(f_3, f_4)}^F = \overline{S(f_3, f_5)}^F = \overline{S(f_4, f_5)}^F = 0.$$

Portanto, $F := \{f_1, f_2, f_3, f_4, f_5\}$ *é base de Gröbner para* I.

Lema 2.4.3. *Seja* G *uma base de Gröbner de* $I \subseteq K[x_1, \ldots, x_n]$. *Seja* $p \in G$ *um polinômio tal que* $TL(p) \in \langle TL(G\backslash\{p\})\rangle$. *Então,* $G\backslash\{p\}$ *é também uma base de Gröbner para* I.

Demonstração. Sabemos que $\langle TL(G)\rangle = \langle TL(I)\rangle$. Se $TL(p) \in \langle TL(\backslash\{p\})\rangle$, então temos $\langle TL(G)\rangle = \langle TL(g\backslash\{p\})\rangle$. Logo, $G\backslash\{p\}$ também é uma base de Gröbner de I. □

Sejam G e I como no Lema 2.4.3. Removendo de G qualquer polinômio p tal que $TL(p) \in \langle TL(G\backslash\{p\})\rangle$, obtemos uma nova base de Gröbner G' para I. Fazendo um ajuste nos coeficientes líderes do elementos dessa base, de forma a deixá-los todos iguais a um, obtemos uma base que denominamos **base de Gröbner minimal**.

Se G é uma base de Gröbner para o ideal I, tal que para todo $p \in G$, $CL(p) = 1$ e nenhum monômio de p pertence a $\langle TL(G\backslash\{p\})\rangle$, chamamos G de **base de Gröbner reduzida** para I. É possível, a partir de uma base de Gröbner qualquer de um ideal, construirmos uma base de Gröbner reduzida. Este é o resultado do próximo teorema.

Teorema 2.4.4. *Seja $I \neq \{0\}$ um ideal polinomial. Então, para uma dada ordenação monomial, I possui uma única base de Gröbner reduzida.*

Demonstração. Seja $G = \{g_1, \ldots, g_s\}$ uma base minimal para o ideal polinomial I. Se $g \in G$ é tal que nenhum de seus monômios pertencem a $\langle TL(G\backslash\{g\})$, dizemos que g é **reduzido** em G. Observe que se G' é outra base de Gröbner minimal para I, com $g \in G'$, então $\langle TL(G')\rangle = \langle TL(G)\rangle$ e consequentemente $\langle TL(G'\backslash\{g\})\rangle = \langle TL(G\backslash\{g\})\rangle$. Isso significa que se g é reduzido em G, então também o é em G'. Com esta observação em mente, vamos seguir com a demonstração do teorema, reduzindo todos os elementos não reduzidos de G. Suponhamos que $g_1 \in G$ não seja reduzido em G.

AFIRMAÇÃO: Fazendo $h_1 = \overline{g_1}^{G\backslash\{g_1\}}$ e considerando $G_1 = (G\backslash\{g_1\}) \cup \{h_1\}$, temos que G_1 é uma base de Gröbner minimal para I e h_1 é reduzido em G_1.

Com efeito, por definição de base de Gröbner minimal, temos que $TL(g_1)$ não é divisível por qualquer elemento de $G\backslash\{g_1\}$, e daí $TL(g_1)$ vai para o resto, implicando que $TL(h_1) = TL(g_1)$. Como $G_1 = \{h_1, g_2, \ldots, g_s\}$, segue que $G_1 \subset I$ e $TL(G_1) = TL(G)$. Portanto, G_1 é uma base de Gröbner mínima para I. Agora, h_1 é reduzido em G_1, pois é o resto da divisão de g_1 pelos elementos de $G\backslash\{g_1\}$.

Realizando o mesmo processo com g_2, obtemos $G_2 = \{h_1, h_2, g_3, \ldots, g_s\}$ que é base de Gröbner minimal para I. Pela observação feita no início da demonstração, segue que h_1 é reduzido em G_2.

Prosseguindo desta maneira com todos os elementos de G, conseguimos uma base de Gröbner reduzida para I como queríamos.

Para provar a unicidade, suponha que $G = \{g_1, \ldots, g_s\}$ e $H = \{h_1, \ldots, h_t\}$ sejam bases de Gröbner reduzidas para I. Em particular, essas bases são de Gröbner mínimas e ainda $\langle TL(G)\rangle = \langle TL(I)\rangle = \langle TL(H)\rangle$.

AFIRMAÇÃO: $TL(G) = TL(H)$.

De fato, dado $TL(g_1) \in TL(G)$, segue que $TL(g_1) \in \langle TL(H)\rangle$, e pela Proposição 2.3.2 $TL(h_j)|TL(g_1)$ para algum j. Do mesmo modo, $TL(h_j) \in \langle TL(G)\rangle$ e $TL(g_i)|TL(h_j)$ para algum i. Logo, $TL(g_i)|TL(g_1)$, o que pela minimalidade de G implica que $i = 1$ e $TL(g_1) = TL(h_j)$. Continuando dessa forma, concluímos que $TL(G) \subseteq TL(H)$. Fazendo o mesmo com os elementos de $TL(H)$, obtemos a outra inclusão. Provando a igualdade desejada. Da igualdade provada na última afirmação e do fato de G e H serem bases minimais, temos que G e H possuem o mesmo números de elementos. Com isso, dado $g \in G$. Então existe $h \in H$ tal que $TL(g) = TL(h)$. Mostraremos que $g = h$. Para isso, considere $g - h \in I$. Como g é base de Gröbner de I, segue do Corolário 2.3.10 que $\overline{g-h}^{G} = 0$. Como $TL(g) = TL(h)$, este termos se cancelam e os termos restantes não são divisíveis por nenhum elemento de $TL(G) = TL(H)$, pois G e H são reduzidas. Assim, $\overline{g-h}^{G} = g - h$ e portanto $g - h = 0$, completando a demonstração. □

CAPÍTULO 3

MÓDULOS FINITAMENTE GERADOS E ALGUMAS PROPRIEDADES

Neste capítulo apresentaremos um pouco da teoria de $A-$módulos. Em especial, na segunda seção será mostrado um resultado sobre matrizes que será de fundamental importância na conclusão dos resultados do último capítulo deste trabalho. Aqui serão apresentados somente alguns resultados sobre o assunto. Caso o leitor tenha interesse em saber mais, pode consultar a principal referência utilizada neste capítulo que foi [9].

3.1 A-módulos

Seja A um anel comutativo com unidade. Um grupo abeliano aditivo $(M,+)$ dotado de multiplicação escalar

$$\begin{aligned} A \times M &\longrightarrow M \\ (a,m) &\longmapsto a.m \end{aligned}$$

é dito um **A-módulo** se satisfaz os seguintes axiomas para todos $a_1, a_2 \in A$ e todos $m_1, m_2 \in M$:

a) $1 \cdot m_1 = m_1$

b) $(a_1 a_2) \cdot m_1 = a_1 \cdot (a_1 \cdot m_1)$

c) $(a_1 + a_2) \cdot m_1 = a_1 \cdot m_1 + a_2 \cdot m_1$

d) $a_1 \cdot (m_1 + m_2) = a_1 \cdot m_1 + a_1 \cdot m_2$.

Se $a \in A$ e $m \in M$, escrevemos também am para denotar o elemento $a \cdot m$. Considerando o A-módulo M, dizemos que um subgrupo N de M é um **A-submódulo** se a multiplicação escalar de M preserva N, ou seja, se $an \in N$, para todo $a \in A$ e para todo $n \in N$. Observe que se A é um corpo então a noção de A-módulo coincide com a de A-espaço vetorial. Veremos a seguir que muitos dos objetos definidos dentro do estudo de A-módulo são análogos aos que conhecemos de álgebra linear.

Sejam M um A-módulo e $t \in \mathbb{N}$. Sejam $m_1, \ldots, m_t$ elementos de M. O subconjunto N de M definido por

$$N = Am_1 + \cdots + Am_t = \{a_1 m_1 + \cdots + a_t m_t | \, a_i \in A\}$$

é claramente um A-módulo de M e é chamado de **submódulo gerado** por $m_1, \ldots, m_t$. O módulo M é dito **finitamente gerado** quando existe um número finito de elementos $m_1, \cdots, m_t$ de M tais que

$$M = Am_1 + \cdots + Am_t.$$

Neste caso dizemos que $\{m_1, \cdots, m_t\}$ é um **conjunto de geradores** de M.

O módulo M é dito **cíclico** se pode ser gerado por um elemento, isto é, se $M = Am$, para algum $m \in M$.

Se para todo $1 \leq j \leq t$

$$\sum_{j=1}^{t} a_j m_j = 0 \Rightarrow a_j = 0, \text{ com } a_j \in A$$

então, $\{m_1, \cdots, m_t\}$ é dito **A-linearmente independente**. No caso em que M é finitamente gerado por um conjunto de geradores A-linearmente independentes, ou equivalentemente, se o módulo M é isomorfo a A^t, dizemos que M é **livre**. Esta é equivalência, pode ser vista, considerando o homomorfismo

$$\begin{aligned} g : A^t &\longrightarrow M \\ (a_1, \ldots, a_t) &\longmapsto \sum_{i=1}^{t} (a_i m_i). \end{aligned}$$

O conjunto $\{m_1, \cdots, m_t\}$ satisfazendo estas condições é dita uma **base** para o módulo livre M. Observe que $M = Am_1 \oplus \cdots \oplus Am_t$. Esta notação significa que cada elemento $m \in M$ é escrito de forma única como uma combinação A-linear de $m_1, \ldots, m_t$.

Exemplo 3.1.1. *Seja t um inteiro positivo e considere o seguinte conjunto*

$$A^t = \{(a_1, \ldots, a_t) |\, a_i \in A\}.$$

Definindo a operação de adição coordenada a coordenada:

$$(a_1, \ldots, a_t) + (a'_1, \ldots, a'_t) := (a_1 + a'_1, \ldots, a_t + a'_t),$$

e a multiplicação escalar da seguinte maneira

$$a(a_1, \ldots, a_t) := (aa_1, \ldots, aa_t),$$

*temos que A^t é um A-módulo. Mais que isso, considerando $e_1 = (1, 0, \ldots, 0), \ldots, e_t = (0, \ldots 0, 1)$, podemos ver que $\{e_1, \ldots, e_t\}$ formam uma base para o A-módulo A^t, chamada comumente de **base canônica** de A^t.*

Exemplo 3.1.2. *Seja M um $A-$módulo e seja I um ideal do anel A. Então*

$$IM := \left\{ \sum_{j=1}^{n} \alpha_j g_j |\, n \in \mathbb{N}, \alpha_j \in I,\, g_j \in M, \text{ para todo } j \right\}$$

é um $A-$submódulo de M.

Proposição 3.1.3. *Seja A um anel com unidade e seja M um A-módulo livre finitamente gerado. Então, todas as bases de M possuem o mesmo número de elementos.*

Demonstração. Seja $\{m_1, \ldots, m_t\}$ uma base de A-módulo M. Seja I um ideal maximal de A e considere a aplicação

$$\begin{aligned} \varphi : M &\longrightarrow (A/I) \times \ldots \times (A/I) \\ (a_1m_1 + \ldots + a_tm_t) &\longmapsto (\overline{a_1}, \ldots, \overline{a_t}) \end{aligned}$$

φ é um homomorfismo sobrejetor de grupos aditivos, pois

$$\begin{aligned} \varphi((a_1m_1 + \ldots + a_tm_t) + (b_1m_1 + \ldots + b_tm_t)) =& \varphi((a_1 + b_1)m_1 + \ldots + (a_t + b_t)m_t) \\ =& (\overline{a_1 + b_1}, \ldots, \overline{a_t + b_t}) \\ =& (\overline{a_1}, \ldots, \overline{a_t}) + (\overline{b_1}, \ldots, \overline{b_t}) \\ =& \varphi(a_1m_1 + \ldots + a_tm_t) + \varphi(b_1m_1 + \ldots + b_tm_t). \end{aligned}$$

Logo φ é um homomorfismo. A sobrejetividade é óbvia.

AFIRMAÇÃO: $ker(\varphi) = IM := \left\{\sum_{j=1}^{n} \alpha_j g_j | \, n \in \mathbb{N}, \alpha_j \in I, g_j \in M, \text{ para todo } j\right\}$. De fato, dado $m \in ker(\varphi)$, então existem $a_1, \ldots, a_t \in A$ tais que

$$m = a_1m_1 + \ldots a_tm_t \quad \text{e} \quad \varphi(m) = (\overline{0}, \ldots, \overline{0}).$$

Assim,

$$\overline{a_1} = \overline{0}, \ldots, \overline{a_t} = \overline{0} \Rightarrow a_j \in I, \text{ para todo} j = 1, \ldots, t$$

Logo, $m \in IM$.

Por outro lado, seja $\sum_{j=1}^{n} \alpha_j g_j \in IM$. Então, para cada j, temos

$$g_j = a_{j1}m_1 + \ldots + a_{jt}m_t, \text{ com } a_{ji} \in A.$$

Assim,

$$\varphi\left(\sum_{j=1}^{n} \alpha_j g_j\right) = \varphi\left(\sum_{j=1}^{n}\left(\alpha_j\left(\sum_{i=1}^{t} a_{ji}m_i\right)\right)\right) = \varphi\left(\sum_{i=1}^{t}\left(m_i\left(\sum_{j=1}^{n} \alpha_j a_{ji}\right)\right)\right).$$

Como I é um ideal, segue que $\alpha_j a_{ji} \in I$, para todo i e para todo j. Logo, $\overline{\alpha_j a_{ji}} = \overline{0}$, para todo i e para todo j. Portanto,

$$\sum_{j=1}^{n} \alpha_j g_j \in ker\varphi,$$

completando assim a prova da afirmação.

Pela afirmação, sabemos que

$$M/IM \simeq \underbrace{(A/I) \times \ldots \times (A/I)}_{\text{t vezes}}. \tag{3.1}$$

Sendo A/I um corpo, M/IM tem uma estrutura de A/I-esp.vetorial dada por

$$(a + I)(m + IM) := am + IM.$$

E assim, é imediato que o isomorfismo em (3.1) é um isomorfismo de espaços vetoriais. Portanto, M/IM é um $A/I-$esp. vetorial de dimensão t.

Se M possui outra base com n elementos, argumentando da mesma forma concluímos que M/IM tem dimensão n como A/I-esp. vetorial. Pela propriedade de bases de espaços vetoriais segue que $t = n$.

□

3.2 Homomorfismo entre Módulos

Nesta seção, A sempre estará representando um anel. Nos casos em que isso não ocorrer especificaremos.

Sejam M e M' dois A-módulos. Uma aplicação $f : M \longrightarrow M'$ é um **homomorfismo de A-módulos** ou um **A-homomorfismo** se para todo $a \in A$ e para todo $m \in M$, $f(am) = af(m)$, e além disso f é um homomorfismo de grupos aditivos, isto é,

$$f(m_1 + m_2) = f(m_1) + f(m_2), \text{ para quaisquer } m_1, m_2 \in M.$$

Podemos também dizer que f é **A-linear**, ou que f é um **operador A-linear**. Se um homomorfismo de A-módulos é bijetivo, então o chamamos de **isomorfismo de A-módulos**.

Observe que a definição de homomorfismo de A-módulos é análoga à definição de transformação linear entre espaços vetoriais. E como em álgebra linear, podemos representar uma aplicação A-linear entre módulos finitamente gerados por uma matriz.

Sejam N um A-módulo finitamente gerado, M um A-módulo livre finitamente gerado e $f : N \longrightarrow M$ uma aplicação A-linear. Considere $\beta = \{v_1, \ldots, v_n\}$ o conjunto ordenado de geradores de N e $\gamma = \{w_1, \ldots, w_m\}$ uma base ordenada de M. Podemos representar f por uma matriz $m \times n$ da seguinte maneira: escrevemos para cada $j \in \{1, \ldots, n\}$

$$f(v_j) = \sum_{i=1}^{m} a_{ij} w_i, \quad \text{com } a_{ij} \in A.$$

Dizemos que a matriz $\mathcal{M} = (a_{ij})$ representa a aplicação f em relação a β e γ. Note que a matriz da aplicação f depende do conjunto de geradores de N e da base de M.

A seguir faremos algumas considerações a respeito de operações elementares sobre linhas e colunas de uma matriz. Veremos que se f, M, N, β, γ e $\mathcal{M}$ são como acima, então realizar operações elementares sobre as linhas e colunas da matriz $\mathcal{M}$ corresponde a mudanças em β e γ.

Chamamos **operações elementares** sobre as linhas (ou colunas) de $\mathcal{M}$ as seguintes operações:

1. Permutação de duas linhas (respectivamente de duas colunas);
2. Substituição de uma linha (respectivamente de uma coluna) pela soma desta linha com um múltiplo de uma outra linha (respectivamente pela soma desta coluna com um múltiplo de uma outra coluna);
3. Multiplicação de uma linha ou coluna por um elemento invertível.

Se A é uma matriz $n \times n$ que foi obtida da matriz identidade I_n aplicando-se uma, e somente uma, operação elementar, então A é dita **matriz elementar**. Toda matriz elementar é invertível e sua inversa também é uma matriz elementar.

Vejamos através de alguns exemplos que se B é uma matriz obtida da matriz $\mathcal{M}$ por meio de um operação elementar sobre suas colunas ou linhas, então $B = \mathcal{M}E$ ou $B = E\mathcal{M}$, sendo E a matriz elementar $n \times n$ ou $m \times m$, obtida aplicando-se à matriz identidade a mesma operação que deu origem a B.

Exemplo 3.2.1. *1.* ***Permutação de linhas ou colunas.***
Vamos denotar por $E_{k,k+1}$ e $E^{l,l+j}$ as matrizes elementares obtidas trocando-se a linha k com a linha $k+1$ de I_m e respectivamente a coluna l com a coluna $l+1$ de I_n. Dessa forma,

$$E_{k,k+1} = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & & & & & & \cdot \\ \cdot & & \ddots & & & & & \cdot \\ \cdot & & & 1 & & & & \cdot \\ \cdot & & & & 0 & 1 & & \cdot \\ \cdot & & & & 1 & 0 & & \cdot \\ \cdot & & & & & & \ddots & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & \dots & 0 & 1 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \leftarrow k \\ \leftarrow k+1 \\ \\ \end{matrix}$$

e

$$E^{l,l+1} = \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} l & l+1 \\ \downarrow & \downarrow \\ & \\ & \\ & \\ & \\ & \\ & \end{matrix} \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & & & & & & \cdot \\ \cdot & & \ddots & & & & & \cdot \\ \cdot & & & 1 & & & & \cdot \\ \cdot & & & & 0 & 1 & & \cdot \\ \cdot & & & & 1 & 0 & & \cdot \\ \cdot & & & & & & \ddots & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & \dots & 0 & 1 \end{bmatrix}$$

Assim, tomando $\mathcal{M} = (a_{ij})$, temos que $B = (b_{ij}) = E_{k,k+1}\mathcal{M}$ e $C = (c_{ij}) = \mathcal{M}E^{l,l+1}$ são dadas, respectivamente, por

$$b_{ij} = \begin{cases} a_{(i+1)j} & se\ i = k \\ a_{(i-1)j} & se\ i = k+1 \\ a_{ij} & caso\ contrário \end{cases} \quad e\ c_{ij} = \begin{cases} a_{i(j+1)} & se\ j = l \\ a_{i(j-1)} & se\ j = l+1 \\ a_{ij} & caso\ contrário \end{cases}.$$

2. ***Substituição de linha ou coluna.***
Substituindo a k-ésima linha da matriz I_m, pela soma da linha k com α vezes a linha $k+1$, obtemos a matriz elementar que será denotada por $E_{k,k+1}(\alpha)$. Realizando a mesma operação elementar nas colunas da matriz I_n obtemos a matriz, denotada por $E^{l,l+1}(\alpha)$.

Temos que

$$E_{k,k+1} = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & & & & & \cdot \\ \cdot & & \ddots & & & & \cdot \\ \cdot & & & 1 & \alpha & & \cdot \\ \cdot & & & 0 & 1 & & \cdot \\ \cdot & & & & & \ddots & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \end{bmatrix} \begin{matrix} \\ \\ \\ \leftarrow k \\ \leftarrow k+1 \\ \\ \\ \end{matrix}$$

e

$$E^{l,l+1} = \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \quad & \quad & \quad & l & l+1 & \quad & \quad \\ \quad & \quad & \quad & \downarrow & \downarrow & \quad & \quad \end{matrix} \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & & & & & \cdot \\ \cdot & & \ddots & & & & \cdot \\ \cdot & & & 1 & 0 & & \cdot \\ \cdot & & & \alpha & 1 & & \cdot \\ \cdot & & & & & \ddots & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \end{bmatrix}$$

Segue que $F = (f_{ij}) = E_{k,k+1}(\alpha)\mathcal{M}$ *e* $G = (g_{ij}) = \mathcal{M}E_{l,l+1}$ *são, respectivamente, como*

$$f_{ij} = \begin{cases} a_{ij} + \alpha a_{(i+1)j} & \text{se } i = k \\ a_{ij} & \text{caso contrário} \end{cases} \quad \text{e } g_{ij} = \begin{cases} a_{ij} + \alpha a_{i(j+1)} & \text{se } j = l \\ a_{ij} & \text{caso contrário} \end{cases}$$

3. ***Multiplicação de uma linha ou coluna por um elemento invertível.***
Ao multiplicarmos a linha k *da matriz* I_m *e a coluna* l *da matriz* I_n*, obtemos as matrizes elementares que serão denotadas, respectivamente, por* $E_k(\alpha)$ *e* $E^l(\alpha)$*. Desta forma,*

$$E_k(\alpha) = \begin{bmatrix} 1 & 0 & . & . & . & . & 0 \\ 0 & \ddots & & & & & . \\ . & & 1 & & & & . \\ . & & & \alpha & & & . \\ . & & & & 1 & & . \\ . & & & & & \ddots & 0 \\ 0 & . & . & . & . & 0 & 1 \end{bmatrix} \begin{matrix} \\ \\ \\ \leftarrow k \\ \\ \\ \\ \end{matrix}$$

e

$$E^l(\alpha) = \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \quad & \quad & \quad & l & \quad & \quad & \quad \\ \quad & \quad & \quad & \downarrow & \quad & \quad & \quad \end{matrix} \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \ddots & & & & & \cdot \\ \cdot & & 1 & & & & \cdot \\ \cdot & & & \alpha & & & \cdot \\ \cdot & & & & 1 & & \cdot \\ \cdot & & & & & \ddots & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \end{bmatrix}$$

e assim $H = (h_{ij}) = E_k(\alpha)\mathcal{M}$ *e* $N = (n_{ij}) = \mathcal{M}E^l(\alpha)$ *são, respectivamente, da seguinte forma*

$$h_{ij} = \begin{cases} \alpha a_{ij} & se\ i = k \\ a_{ij} & caso\ contrário \end{cases} \quad e\ n_{ij} = \begin{cases} \alpha a_{ij} & se\ j = l \\ a_{ij} & caso\ contrário \end{cases}$$

A partir dos exemplos acima, podemos observar que dada uma matriz $\mathcal{M}$, $m \times n$, com entradas em A, ao realizarmos sobre suas linhas e colunas uma sucessão finita de operações elementares, estamos transformando $\mathcal{M}$ numa matriz $B = Q\mathcal{M}P$. Quando obtemos uma matriz B dessa maneira, dizemos que B e $\mathcal{M}$ são **matrizes equivalentes** e denotamos $B \approx \mathcal{M}$. Observe que Q e P são matrizes invertíveis, pois são resultado de uma sequência finita de produtos de matrizes elementares, que são invertíveis. Portanto, se duas matrizes $\mathcal{N}$ e $\mathcal{M}$ são tais que $\mathcal{N} \approx \mathcal{M}$, então existem matrizes invertíveis Q e P de forma que $\mathcal{N} = Q\mathcal{M}P$. Com essa igualdade não é difícil provar que a relação $\approx$ é uma relação de equivalência, ou seja, as afirmações

- $\mathcal{M} \approx \mathcal{M}$
- $\mathcal{N} \approx \mathcal{M} \Rightarrow \mathcal{N} \approx \mathcal{M}$
- $\mathcal{N} \approx \mathcal{M}$ e $\mathcal{M} \approx \mathcal{P} \Rightarrow \mathcal{N} \approx \mathcal{P}$

são satisfeitas.

Sejam $f : N \longrightarrow M$ uma aplicação A-linear entre os A-módulos N e M, sendo N finitamente gerado pelo conjunto ordenado $\beta = \{v_1, \ldots, v_n\}$ e M livre, com base ordenada $\gamma = \{w_1, \ldots, w_m\}$. Seja $\mathcal{M}$ a matriz correspondente a f em relação a β e γ. Se permutamos a i_0-ésima linha de $\mathcal{M}$ com a i_1-ésima linha obtemos uma nova matriz que representa a mesma aplicação f, mas com relação a β e $\gamma_c = \{w_1, \ldots, w'_{i_0}, \ldots, w'_{i_1}, \ldots, w_m\}$, sendo $w'_{i_0} = w_{i_1}$ e $w'_{i_1} = w_{i_0}$. Da mesma forma, permutando a coluna j_0 de $\mathcal{M}$ com a coluna j_1, a matriz obtida representa f com relação a $\beta_l = \{v_1, \ldots, v'_{j_0}, \ldots, v'_{j_1}, \ldots, v_n\}$ e γ, com $v'_{j_0} = v_{j_1}$ e $v'_{j_1} = v_{j_0}$.

Se substituímos a i_0-ésima linha de $\mathcal{M}$ por

$$(\text{linha } i_0) + \lambda(\text{linha } i_1) \text{ com } \lambda \in A,$$

a matriz obtida representa f em relação a β e $\gamma_{c\lambda} = \{w_1, \ldots, w_{i_0}, \ldots, w'_{i_0}, \ldots, w_m\}$, com $w'_{i_0} = w_{i_1} - \lambda w_{i_0}$. De modo semelhante, se substituímos a coluna j_0 de $\mathcal{M}$ por

$$(\text{coluna } j_0) + \lambda(\text{coluna } j_1) \text{ com } \lambda \in A,$$

obtemos uma nova matriz representando f em relação a $\beta_{l\lambda} = \{v_1, \ldots, v'_{j_0}, \ldots, v_{i_1} \ldots, v_n\}$ com $v'_{j_0} = v_{j_0} + \lambda v_{i_1}$.

Com todas essas considerações, podemos continuar com o seguinte resultado:

Teorema 3.2.2. *Sejam* $m \geq 1$ *e* $n \geq 1$ *dois inteiros. Seja* (D, φ) *um domínio euclidiano e seja* $\mathcal{M} = (a_{ij})_{m \times n}$*, uma matriz com entradas em* D*. Então, através de uma sucessão finita de operações elementares em suas linhas e colunas, a matriz* $\mathcal{M} = (a_{ij})$ *pode ser transformada numa matriz diagonal da forma*

$$B = \begin{bmatrix} \lambda_1 & & & & \vdots & & & \\ & \lambda_2 & & & \vdots & & & \\ & & \ddots & & & & 0 & \\ & & & \lambda_r & \vdots & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & \vdots & & & \\ & 0 & & & \vdots & & 0 & \\ & & & & \vdots & & & \end{bmatrix}$$

com $0 \leq r \leq min\{m,n\}, \lambda_1, \lambda_2, \ldots, \lambda_r$ *pertencentes a* $D\backslash\{0\}$ *e* λ_j *dividindo* λ_{j+1}*, para cada* $j = 1, 2, \ldots, r-1$*. Em particular, para toda matriz* $\mathcal{M}$ *com entradas num domínio euclidiano existem matrizes* $U = (u_{ij})$ *e* $Q = (q_{ij})$ *invertíveis de ordens* m *e* n *respectivamente, tais que* $B = U\mathcal{M}Q$*.*

Demonstração. Se $\mathcal{M} = (a_{ij})$ ou $\mathcal{M}$ é nula, não temos nada o que fazer. Dessa forma, consideremos uma matriz $\mathcal{M} = (a_{ij})$, com $m > 1$ ou $n > 1$. Definimos

$$\varphi(\mathcal{M}) := min\left\{\varphi(a_{ij}) | \, a_{ij} \neq 0\right\}$$

e t o inteiro $t := t(\mathcal{M})$ dado por

$$t := min\left\{\varphi(\mathcal{N}) | \, \mathcal{N} \approx \mathcal{M}\right\}.$$

A demonstração para o caso geral é algorítmica. Sendo assim, mostraremos inicialmente como obter uma matriz $\mathcal{N} \approx \mathcal{M}$ tal que $\varphi(\mathcal{N}) = t$. Primeiro, permutamos as linhas e colunas de $\mathcal{M}$ de forma a colocar a entrada $a_{i_0j_0}$ tal que $\varphi(a_{i_0j_0}) = \varphi(\mathcal{M})$, na posição $(1,1)$. Obtendo assim, a matriz $\mathcal{M}_1 = (b_{ij})$ tal que

$$\mathcal{M}_1 \approx \mathcal{M} \text{ e } \varphi(b_{11}) = \varphi(\mathcal{M}).$$

Depois consideramos os seguintes conjuntos:

$$\begin{aligned} J_1 &= \left\{j \geq 2 | \, b_{1j} \neq 0\right\}, \\ J_2 &= \left\{j \geq 2 | \, b_{1j} = 0\right\}, \\ I_1 &= \left\{i \geq 2 | \, b_{i1} \neq 0\right\}, \\ I_2 &= \left\{i \geq 2 | \, b_{i1} = 0\right\}. \end{aligned}$$

Pra cada $j \in J_1$, fazemos a divisão euclidiana de b_{1j} por b_{11}:

$$b_{1j} = q_j b_{11} + r_j \text{ com } r_j = 0 \text{ ou } \varphi(r_j) < \varphi(b_{11}),$$

e substituímos a j-ésima coluna de $\mathcal{M}_1$ por

$$(j\text{-ésima coluna}) - q_j \cdot (\text{primeira coluna}).$$

Para cada $j \in J_2$, deixamos a $j-$ésima coluna inalterada. Note que a primeira coluna de $\mathcal{M}_1$ não foi alterada. Assim, de maneira análoga à feita com as colunas de $\mathcal{M}_1$, para cada $i \in I_1$ fazemos a divisão euclidiana de b_{i1} por b_{11}:

$$b_{i1} = q_i' b_{11} + r_i' \text{ com } r_i' = 0 \text{ ou } \varphi(r_i') < \varphi(b_{11}),$$

e substituímos a i-ésima linha da matriz obtida no passo anterior por

$$(i\text{-ésima linha}) - q'_j \cdot (\text{primeira linha}).$$

Chamaremos a matriz obtida após essas duas etapas de $\mathcal{N}_1 = (c_{ij})$. Observe que $\mathcal{N}_1 \approx \mathcal{M}$ e $\varphi(\mathcal{N}_1) \leq \varphi(\mathcal{M})$. Realizando essas duas etapas, agora com $\mathcal{N}_1$, obtemos um matriz $\mathcal{N}_2 \approx \mathcal{N}_1$ com $\varphi(\mathcal{N}_2) \leq \varphi(\mathcal{N}_1)$. Prosseguindo desta maneira, conseguimos uma sequência de matrizes $\mathcal{N}_i \approx \mathcal{M}$ tais que a sequência de números naturais $\varphi(\mathcal{N}_i)$ seja decrescente. Como sequências decrescentes de números naturais são estacionárias, depois de um número finito de passos conseguimos uma matriz $\mathcal{N} \approx \mathcal{M}$ tal que $\varphi(\mathcal{N}) = t(\mathcal{M})$.

Consideremos $\mathcal{N}$ como determinada acima. Permutando linhas e colunas em $\mathcal{N}$, podemos colocar a entrada de menor $\varphi-$valor na posição $(1,1)$, ou seja obtemos uma matriz $\mathcal{N}'_1 = (d_{ij})$ tal que

$$\mathcal{N}'_1 \approx \mathcal{N} \text{ e } \varphi(d_{11}) = \varphi(\mathcal{N}).$$

AFIRMAÇÃO 1. Existe uma matriz $\mathcal{L} = (e_{ij})$ tal que

$$\mathcal{L} \approx \mathcal{N}'_1,\ e_{11} = d_{11} \text{ e } e_{1j} = 0, \text{ para todo } j \geq 2.$$

DEMONSTRAÇÃO DA AFIRMAÇÃO 1: Sejam J'_1 e J'_2 definidos, respectivamente, de maneira análoga à feita para J_1 e J_2, mas agora com os elementos de $\mathcal{N}'_1$. Realizando em $\mathcal{N}'_1$ a primeira etapa do processo mostrado acima para obtenção de $\mathcal{N}_1$, conseguimos $\mathcal{L} := (e_{ij}) \approx \mathcal{N}'_1$ tal que as únicas possíveis entradas não nulas de sua primeira linha são $e_{11} = d_{11}$ e os r_j's com $j \in J'_1$. Observamos, no entanto, que $r_j = 0$ para cada $j \in J'_1$. De fato, se existir $j \in J'_1$ com $r_j \neq 0$, então teríamos $\mathcal{L} \approx \mathcal{M}$ e $\varphi(\mathcal{L}) \leq \varphi(r_j) < \varphi(d_{11}) = t$, o que é absurdo pela definição de t.

AFIRMAÇÃO 2. Existe uma matriz $\mathcal{C} = (f_{ij})$ tal que $\mathcal{C} \approx \mathcal{L}$, $f_{11} = e_{11}$,

$$\mathcal{C} = \begin{bmatrix} f_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \mathcal{A} & \\ 0 & & & \end{bmatrix}, \tag{3.2}$$

sendo $\mathcal{A}$ uma matriz $(m-1) \times (n-1)$ e f_{11} divide cada entrada da submatriz $\mathcal{A}$.

DEMONSTRAÇÃO DA AFIRMAÇÃO 2: Sejam I'_1 e I'_2 definidos, respectivamente, análogos a I_1 e I_2, mas com os elementos de $\mathcal{L}$. Realizando em $\mathcal{L}$ a segunda etapa do processo mostrado acima para obtenção da matriz $\mathcal{N}_1$, obtemos uma matriz $\mathcal{C} := (f_{ij}) \approx \mathcal{L}$ tal que sua primeira linha é igual a primeira linha de $\mathcal{L}$ e tal que as únicas possíveis entradas não nulas de sua primeira coluna são $f_{11} = e_{11}$ e os r'_i's com $i \in I'_1$. De novo, em virtude da definição de t, podemos garantir que $r'_i = 0$ para cada $i \in I'_1$. Assim, nossa matriz $\mathcal{C}$ satisfaz a condição 3.2.

Vamos agora verificar que f_{11} divide cada entrada da submatriz $\mathcal{A}$. Suponhamos por absurdo que existam $k \geq 2$ e $l \geq 2$ tais que f_{11} não divida f_{kl}. Fazemos a divisão euclidiana de f_{kl} por f_{11}:

$$f_{kl} = qf_{11} + r, \text{ com } r \neq 0 \text{ e } \varphi(r) < \varphi(f_{11}),$$

e substituímos a primeira linha de $\mathcal{C}$ por

$$(\text{primeira linha de } \mathcal{C}) + (k\text{-ésima linha de } \mathcal{C}).$$

Nesta nova matriz $\tilde{\mathcal{C}}$ obtida depois da substituição da primeira linha de $\mathcal{C}$ descrita acima, substituímos a sua $l-$ésima coluna por

(l-ésima coluna de $\tilde{\mathcal{C}}$) $- q\cdot$(primeira coluna de $\tilde{\mathcal{C}}$).

Desta maneira, obtemos uma matriz $\mathcal{N}' \approx \mathcal{C} \approx \mathcal{M}$ cuja entrada da primeira linha e $l-$ésima coluna é igual a r, logo uma matriz tal que $\varphi(\mathcal{N}') \leq \varphi(r) < \varphi(f_{11}) < t$, o que é impossível pela definição de t. Isto termina a prova da Afirmação 2.

Agora podemos terminar a demonstração do teorema aplicando indução sobre $min\{m,n\}$. Faça $p := min\{m,n\}$. Se $p = m = 1$, então usando a Afirmação 1 o teorema fica provado. Se $p = n = 1$ utilizamos a Afirmação 2, e temos também neste caso o resultado desejado. Suponha por indução que o teorema vale pra uma matriz $(m-1)\times(n-1)$. Então pela Afirmação 2 e pela hipótese de indução, existe uma matriz $\mathcal{A}' \approx \mathcal{A}$, sendo $\mathcal{A}$ obtida em 3.2 e $\mathcal{A}'$ da forma:

$$\mathcal{A}' = \begin{bmatrix} \lambda_2 & & & \vdots & & & \\ & \ddots & & & & 0 & \\ & & \lambda_r & \vdots & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & \vdots & & & \\ & 0 & & \vdots & & 0 & \\ & & & \vdots & & & \end{bmatrix},$$

com $\lambda_2, \ldots, \lambda_r \in D\backslash\{0\}$ e λ_j dividindo λ_{j+1}, para cada j.

Evidentemente temos

$$\mathcal{C} = \begin{bmatrix} f_{11} & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & \mathcal{A} & \\ 0 & & & \end{bmatrix} \approx \begin{bmatrix} f_{11} & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & \mathcal{A}' & \\ 0 & & & \end{bmatrix}$$

e logo,

$$\mathcal{C} \approx \begin{bmatrix} f_{11} & & & & \vdots & & & \\ & \lambda_2 & & & \vdots & & & \\ & & \ddots & & & & 0 & \\ & & & \lambda_r & \vdots & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & \vdots & & & \\ & 0 & & & \vdots & & 0 & \\ & & & & \vdots & & & \end{bmatrix}.$$

Como f_{11} divide cada entrada de $\mathcal{A}$, então f_{11} divide cada entrada de $\mathcal{A}'$, pois as entradas de $\mathcal{A}'$ são múltiplos somas de múltiplos de entradas de $\mathcal{A}$. Portanto f_{11} divide λ_2 e a demonstração está completa tomando $\lambda_1 := f_{11}$. □

Corolário 3.2.3. *Seja D um domínio euclidiano. Sejam M, N dois D-módulos livres finitamente gerados e $f : N \longrightarrow M$ um D-homomorfismo. Então, existe uma base $\beta = \{v_1, \ldots, v_n\}$ de N e uma base $\gamma = \{w_1, \ldots, w_m\}$ de M tais que a matriz que representa f em relação a estas bases é da forma*

$$\begin{bmatrix} \lambda_1 & & & & \vdots & & & \\ & \lambda_2 & & & \vdots & & & \\ & & \ddots & & & & 0 & \\ & & & \lambda_r & \vdots & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & \vdots & & & \\ & 0 & & & \vdots & & 0 & \\ & & & & \vdots & & & \end{bmatrix}$$

com $0 \leq r \leq min\{m,n\}, \lambda_1, \lambda_2, \ldots, \lambda_r$ *pertencentes a* $D\backslash\{0\}$ *e* λ_j *dividindo* λ_{j+1}*, para cada* $j = 1, 2, \ldots, r-1$.

Demonstração. Sejam β' e γ' as bases ordenadas de N e M, respectivamente. Se $\mathcal{M} = (a_{ij})$ é a matriz que representa f em relação a β' e γ', então pelo Teorema 3.2.2 podemos transformar $\mathcal{M} = (a_{ij})$ numa matriz da forma

$$\begin{bmatrix} \lambda_1 & & & & \vdots & & & \\ & \lambda_2 & & & \vdots & & & \\ & & \ddots & & & & 0 & \\ & & & \lambda_r & \vdots & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & \vdots & & & \\ & 0 & & & \vdots & & 0 & \\ & & & & \vdots & & & \end{bmatrix}$$

com $0 \leq r \leq min\{m,n\}, \lambda_1, \lambda_2, \ldots, \lambda_r$ pertencentes a $D\backslash\{0\}$ e λ_j dividindo λ_{j+1}, para cada $j = 1, 2, \ldots, r-1$. E como vimos nas considerações feitas antes do Teorema 3.2.2, essa sequência finita de operações elementares vão transformar β' e γ', respectivamente, em β e γ como desejado. □

CAPÍTULO 4

IDEAL TÓRICO

Neste capítulo estudaremos algumas características dos ideais tóricos. Veremos, com o auxílio da teoria de álgebra linear e bases de Gröbner que esses ideais, são ideais primos e também binomiais. A escrita deste capítulo foi baseada nas referências [10] e [5], exceto as duas primeiras definições, que podem ser encontradas em [11].

4.1 Geradores do Ideal Tórico e o núcleo de um $\mathbb{Z}$-homomorfismo

Seja A um anel comutativo com unidade. Um anel R é dito ser uma **A-álgebra** (ou **álgebra sobre A**), se satisfaz o seguinte:

a) $(R, +)$ é um $A-$módulo

b) $a(r_1 r_2) = (ar_1)r_2 = r_1(ar_2)$ para todo $a \in A$ e $r_1, r_2 \in R$;

Um **homomorfismo de A-álgebras**, $f : R \longrightarrow R'$ é um homomorfismo de anéis que é também um homomorfismo de $A-$módulos.

Fixe uma matriz $\mathcal{A} = (a_{ij})_{m\times n}$, com entradas inteiras não negativas a_{ij} e colunas não nulas. Considere o homomorfismo de grupos $\psi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ determinado pela matriz $\mathcal{A}$. Ou seja, dado $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$, temos $\psi(v) = v_1 a_1 + \cdots + v_n a_n \in \mathbb{Z}^m$, sendo $a_j = (a_{1j}, \ldots, a_{mj})$ a j-ésima coluna da matriz $\mathcal{A}$. Identificamos cada coluna a_j de $\mathcal{A}$ com um monômio $t^{a_j} = t_1^{a_{1j}} \cdot \ldots \cdot t_m^{a_{mj}}$.

Sejam $K[x_1, \ldots, x_n]$ e $K[t_1, \ldots, t_m]$ dois anéis polinomiais sobre K, e ϕ o homomorfismo graduado de K-álgebras,

$$K[x_1, \ldots, x_n] \longrightarrow K[t_1, \ldots, t_m], \text{ induzido por } \phi(x_j) = t^{a_j}.$$

Os anéis polinomiais são graduados por $deg(t_i) = 1$ para todo i e $deg(x_j) = deg(t^{a_j}) = a_{1j} + \cdots + a_{mj}$, para todo j. Para simplificar notação, denotaremos esta graduação pelo vetor $\tau = (\tau_1, \ldots, \tau_n)$, ou seja, cada entrada $\tau_j = deg(x_j) = a_{1j} + \cdots + a_{mj}$. Observe que com esta graduação, se $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ e consideramos o seu monômio correspondente x^α, temos que

$$deg(x^\alpha) = \langle \tau, \alpha \rangle.$$

Sendo $\langle \cdot, \cdot \rangle$ o produto interno usual em $\mathbb{R}^n$.

O núcleo de ϕ é denotado por $I_\mathcal{A}$ é chamado de **ideal tórico** associado a $\mathcal{A}$. Note que $I_\mathcal{A}$ é um ideal primo, pois $K[x_1, \ldots, x_n]/I_\mathcal{A} \simeq Im(\phi)$, que é um domínio de integridade.

Lema 4.1.1. *Os homomorfismos ϕ e ψ estão intimamente ligados, ou seja, dado*

$$\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$$

e considerando seu monômio correspondente $x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$, temos que $\phi(x^\alpha) = t^{\psi(\alpha)}$. Consequentemente, $g = x^\alpha - x^\beta$ pertence a $I_\mathcal{A} = ker(\phi)$ se, e somente se, $\alpha - \beta$ pertence ao $ker(\psi)$.

Demonstração. Temos que

$$\begin{aligned} \phi(x^\alpha) &= \phi(x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}) \\ &= \phi(x_1)^{\alpha_1} \cdot \ldots \cdot \phi(x_n)^{\alpha_n} \\ &= (t^{a_1})^{\alpha_1} \cdot \ldots \cdot (t^{a_n})^{\alpha_n} \\ &= t_1^{\sum_{j=1}^n \alpha_j a_{1j}} \cdot \ldots \cdot t_m^{\sum_{j=1}^n \alpha_j a_{mj}} \end{aligned} \tag{4.1}$$

Por outro lado,

$$\psi(\alpha) = \alpha_1 a_1 + \cdots \alpha_n a_n = (\sum_{j=1}^n \alpha_j a_{1j}, \ldots, \sum_{j=1}^n \alpha_j a_{mj}) \tag{4.2}$$

Por definição de monômios e pelas equações (4.1) e (4.2), temos $\phi(x^\alpha) = t^{\psi(\alpha)}$.
Por outro lado,

$$\begin{aligned} x^\alpha - x^\beta \in I_\mathcal{A} &\Leftrightarrow \phi(x^\alpha - x^\beta) = 0 \\ &\Leftrightarrow \phi(x^\alpha) - \phi(x^\beta) = 0 \\ &\Leftrightarrow t^{\psi(\alpha)} - t^{\psi(\beta)} = 0 \\ &\Leftrightarrow \psi(\alpha) = \psi(\beta) \\ &\Leftrightarrow \psi(\alpha - \beta) = 0 \\ &\Leftrightarrow \alpha - \beta \in ker(\psi). \end{aligned}$$

□

Os polinômios da forma $x^\alpha - x^\beta$ são chamados de **binômios**.

Lema 4.1.2. *Seja K um corpo. O ideal tórico $I_\mathcal{A}$ é gerado como um K-espaço vetorial pelo conjunto de binômios*

$$W = \{x^\alpha - x^\beta | \, \alpha, \beta \in \mathbb{N}^n \text{ com } \psi(\alpha) = \psi(\beta)\}.$$

Demonstração. Pelo Lema 4.1.1, temos claramente que $W \subset I_\mathcal{A}$. Assim, basta provarmos que cada polinômio em $I_\mathcal{A}$ é uma combinação K-linear de binômios pertencentes a W. Fixe uma ordem monomial $\prec$ em $K[x_1, \ldots, x_n]$. Seja $[W]$ o K-espaço vetorial gerado por W. Se $I_\mathcal{A} \neq [W]$, escolhemos $f \in I_\mathcal{A} \backslash [W]$, tal que $CL(f) = 1$ e $TL(f) = x^\alpha$ seja mínimo em relação à ordem monomial $\prec$. Como $f \in I_\mathcal{A}$, segue que $\phi(f) = 0$. Em particular, o termo $\phi(x^\alpha) = t^{\psi(\alpha)}$ deve se cancelar. Isso significa que existe outro monômio em f, tal que $x^\beta \prec x^\alpha$ e $\psi(\alpha) = \psi(\beta)$, ou seja, $x^\alpha - x^\beta \in I_\mathcal{A}$. Note, $f' := f - x^\alpha + x^\beta \in I_\mathcal{A}$ tem termo líder menor que $TL(f)$ e pela minimalidade do $TL(f)$, segue que f' deve pertencer a $[W]$. Mas isso implica que $f \in [W]$, gerando uma contradição. Portanto, $I_\mathcal{A} = [W]$. □

Antes de apresentarmos o próximo resultado, considere $a \in \mathbb{Z}$ e defina $a^+ = max\{a, 0\}$ e $a^- = max\{-a, 0\}$. Observe que dado um vetor $u = (u_1, \ldots, u_n) \in \mathbb{Z}^n$ podemos escrevê-lo de maneira única como $u = u^+ - u^-$, sendo $u^+ = (u_1^+, \ldots, u_n^+)$ e $u^- = (u_1^-, \ldots, u_n^-)$. Por exemplo, $(4, -5, 6) = (4, 0, 6) - (0, 5, 0)$.

Lema 4.1.3. *Sejam, $\alpha, \beta \in \mathbb{N}^n$ e $u = \alpha - \beta \in \mathbb{Z}^n$. Existe $z = (z_1, \ldots, z_n) \in \mathbb{N}^n$, tal que $\alpha = u^+ + z$ e $\beta = u^- + z$.*

Demonstração. Temos que $u = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$. Vamos mostrar que $z = (z_1, \ldots, z_n)$, com $z_i = min\{\alpha_i, \beta_i\}$ satisfaz a condição desejada. Com efeito, para cada $i = 1, \ldots, n$ temos,

$$u_i^+ + z_i = max\{\alpha_i - \beta_i, 0\} + min\{\alpha_i, \beta_i\}$$

e

$$u_i^- + z_i = max\{\beta_i - \alpha_i, 0\} + min\{\alpha_i, \beta_i\}$$

Se $\alpha_i \geq \beta_i$, então $\alpha_i - \beta_i \geq 0$. Consequentemente,

$$u_i^+ + z_i = (\alpha_i - \beta_i) + \beta_i = \alpha_i$$

e

$$u_i^- + z_i = 0 + \beta_i = \beta_i.$$

Portanto $\alpha = u^+ + z$ e $\beta = u^- + z$. □

Corolário 4.1.4. *Seja $I_{\mathcal{A}}$ um ideal tórico. Então,*

$$I_{\mathcal{A}} = \langle x^{u^+} - x^{u^-} \,|\, u \in ker(\psi) \rangle.$$

Demonstração. Pelo Lema 4.1.2, temos que $I_{\mathcal{A}} = [W]$, com $W = \{x^\alpha - x^\beta \,|\, \alpha, \beta \in \mathbb{N}^n \text{ com } \phi(\alpha) = \phi(\beta)\}$. Dessa forma, basta mostramos que $J = \langle x^{u^+} - x^{u^-} \,|\, u \in ker(\psi) \rangle = [W]$.

Seja $x^\alpha - x^\beta \in W$. Então $u = \alpha - \beta \in ker(\psi)$. Pelo Lema 4.1.3 existe $z \in \mathbb{N}^n$ tal que $\alpha = u^+ + z$ e $\beta = u^- + z$. Assim,

$$x^\alpha - x^\beta = x^z x^{u^+} - x^z x^{u^-} = x^z (x^{u^+} - x^{u^-}),$$

com $x^z \in K[x_1, \ldots, x_n]$. Logo, $x^\alpha - x^\beta \in J$ e consequentemente $[W] \subseteq J$.

Por outro lado, seja $f \in J$. Então,

$$\sum_u h_u (x^{u^+} - x^{u^-}) \text{ com } h_u \in K[x_1, \ldots, x_n] \text{ e } u \in ker(\psi).$$

Note que $x^{u^+} - x^{u^-} \in I_{\mathcal{A}}$ e como $[W] = I_{\mathcal{A}}$ é um ideal, segue que $h_u(x^{u^+} - x^{u^-}) \in [W]$ para todo $u \in ker(\psi)$. Portanto, $I_{\mathcal{A}} = \langle x^{u^+} - x^{u^-} \,|\, u \in ker(\psi) \rangle$. □

Teorema 4.1.5. *Para cada ordem monomial $\prec$ existe um conjunto de vetores $G_\prec \subset ker(\psi)$ tal que a base de Gröbner reduzida de $I_{\mathcal{A}}$ com respeito $\prec$ é igual a $\{x^{u^+} - x^{u^-}\} \,|\, u \in G_\prec\}$.*

Demonstração. Seja $\overline{W} = \{x^{u^+} - x^{u^-} \,|\, u \in ker(\psi)\}$. Pelo Corolário 4.1.4, $I_{\mathcal{A}} = \langle \overline{W} \rangle$. Note que $\overline{W} \subset I_{\mathcal{A}}$. Daí, $TL(\overline{W}) \subseteq TL(I_{\mathcal{A}})$. Logo, $\langle TL(\overline{W}) \rangle \subseteq \langle TL(I_{\mathcal{A}}) \rangle$.

Por outro lado, seja $TL(g) \in TL(I_{\mathcal{A}})$, para algum $g \in I_{\mathcal{A}}$. Então, pelo Lema 4.1.2

$$g = \sum_{i=1}^{s} a_i (x^{\alpha_i} - x^{\beta_i}) \text{ com } a_i \in K \text{ e } \psi(\alpha_i) = \psi(\beta_i).$$

O Lema 4.1.3 nos garante que para cada i, existe $z_i \in \mathbb{N}^n$ tal que $x^{\alpha_i} - x^{\beta_i} = x^{z_i}(x^{u_i^+} - x^{u_i^-})$, com $u_i = u_i^+ - u_i^- \in ker(\psi)$. Logo,

$$g = \sum_{i=1}^{s} a_i x^{z_i} (x^{u_i^+} - x^{u_i^-}).$$

Dessa forma, segue que $ML(g)$ é igual a $x^{z_i}x^{u_i^+}$ ou $x^{z_i}x^{u_i^-}$, para algum $i \in \{1,\dots,s\}$. Suponhamos sem perda de generalidade que $ML(g) = x^{z_i}x^{u_i^+}$. Isso implica que $x^{u_i^+} \succ x^{u_i^-}$, ou seja, $x^{u_i^+} = TL(x^{u_i^+} - x^{u_i^-})$. Como $x^{u_i^+} - x_i^{u^-} \in \overline{W}$, temos

$$TL(g) \in \langle TL(\overline{W})\rangle \Rightarrow TL(I_{\mathcal{A}}) \subseteq \langle TL(\overline{W})\rangle.$$

Portanto, $\langle TL(I_{\mathcal{A}}) \subseteq \langle TL(\overline{W})\rangle$ e temos a igualdade $\langle TL(I_{\mathcal{A}})\rangle = \langle TL(\overline{W})\rangle$.

Pelo Lema de Dickson (Teorema 2.2.5), existem $u_1,\dots,u_t \in ker(\psi)$, tais que $\langle TL(I_{\mathcal{A}})\rangle = \langle TL(x^{u_1^+} - x^{u_1^-}),\dots,TL(x^{u_t^+} - x^{u_t^-})\rangle$. Pela construção feita na demostração do Teorema das Bases de Hilbert (Teorema 2.3.3) temos que $G = \{x^{u_1^+} - x^{u_1^-},\dots,x^{u_t^+} - x^{u_t^-}\}$ formam uma base de Gröbner para $I_{\mathcal{A}}$. Só falta mostrarmos que as operações para reduzir esta base preservam a estrutura dos binômios.

Podemos eliminar alguns elementos de G a fim de obtermos uma base de Gröbner minimal para $I_{\mathcal{A}}$. Digamos que $G' = \{x^{w_1^+} - x^{w_1^-},\dots,x^{w_r^+} - x^{w_r^-}\}$ seja essa base minimal. Podemos supor que o termo líder de $x^{w_j^+} - x^{w_j^-} \in G'$ é $x^{w_j^+}$, para cada j.

Tome $x^{w_1^+} - x^{w_1^-} \in G'$. Como G' é mínima, sabemos que $x^{w_1^+}$ não é divisível por nenhum $x^{w_j^+}$ para $j \neq 1$. Então, $x^{w_1^+}$ vai para o resto da divisão. Agora, suponha sem perda de generalidade que $x^{w_1^-}$ seja divisível por $x^{w_2^+}$. Isto significa que existe um monômio x^z tal que $x^{w_1^-} = x^z x^{w_2^+}$. Segue que,

$$x^{w_1^+} - x^{w_1^-} = -x^z(x^{w_2^+} - x^{w_2^-}) + x^{w_1^+} - x^z x^{w_2^-}.$$

Seja $v = w_1^+ - (z + w_2^-)$. Pelo Lema 4.1.3, existe $v' \in \mathbb{N}^n$ tal que $w_1^+ = v^+ + v'$ e $z + w_2^- = v^- + v'$. Logo,

$$\begin{aligned} x^{w_1^+} - x^{w_1^-} &= -x^z(x^{w_2^+} - x^{w_2^-}) + x^{v^+ + v'} - x^{v^- + v'} \\ &= -x^z(x^{w_2^+} - x^{w_2^-}) + x^{v'}(x^{v^+} - x^{v^-}). \end{aligned}$$

Observe que $x^{v^+} - x^{v^-} \in I_{\mathcal{A}}$ e assim $v \in ker(\psi)$. Ainda,

$$\begin{aligned} x^{w_2^-} \prec x^{w_2^+} \prec x^{w_1^-} \quad &\Rightarrow \quad x^{w_2^-}x^z \prec x^{w_2^+}x^z = x^{w_1^-} \prec x^{w_1^+} \\ &\Rightarrow \quad x^{v'}x^{v^-} \prec x^{v'}x^{v^+} \\ &\Rightarrow \quad x^{v^-} \prec x^{v^+} \end{aligned} \tag{4.3}$$

Logo, $x^{v^+} \in \langle TL(I_{\mathcal{A}})\rangle$, ou seja, $x^{w_j^+} | x^{v^+}$ para algum j. Como $x^{v^+} | x^{v^+}x^{v'} = x^{w_1^+}$, segue que $x^{w_j^+} | x^{w_1^+}$. Pela minimalidade de G', concluímos que $j = 1$ e $w_j^+ = w_1^+$.Obtemos dessa forma, que $x^{w_1^+} | x^{v^+}$ e $x^{v^+} | x^{v^+}x^{v'} = x^{w_1^+}$. Isso significa que $v = 0$, isto é, $w_1^+ = v^+$ e $z + w_2^- = v^-$. Em outras palavras,

$$x^{w_1^+} = x^{v^+} \text{ e } x^{w_1^-} = x^{z+w_2^+} \succ x^{z+w_2^-} = x^{v^-} \tag{4.4}$$

Pelas equações (4.1) e (4.4) temos que $\{x^{v^+} - x^{v^-}, x^{w_2^+} - x^{w_2^-},\dots,x^{w_r^+} - x^{w_r^-}\}$ ainda é uma base de Gröbner minimal para $I_{\mathcal{A}}$. Continuando com esse processo, obtemos uma sequência $x^{v_n^+} - x^{v_n^-}$, com $x^{v_n^+} = x^{w_1^+}$ e $x^{v_{n+1}^-} \prec x^{v_n^-}$. Pela boa ordenação monomial sabemos que em algum momento esta sequência estaciona e assim, depois de um número finito de passos obtemos $x^{u^+} - x^{u^-}$, com $x^{u^+} = x^{w_1^+}$ e x^{u^-} não divisível por nenhum elemento de $TL(G')\backslash\{x^{w_1^+}\}$. Portanto, $x^{u^+} - x^{u^-}$ é reduzido em $H = \{x^{u^+} - x^{u^-}, x^{w_2^+} - x^{w_2^-},\dots,x^{w_r^+} - x^{w_r^-}\}$. Procedendo da mesma forma, conseguimos reduzir todos os elementos $x^{w_j^+} - x^{w_j^-} \in G'$, com $j = 2,\dots,r$. E portanto, obtemos uma base de Gröbner reduzida para $I_{\mathcal{A}}$ composta por binômios $x^{u^+} - x^{u^-}$, com $u = u^+ - u^- \in G_{\prec} \subset ker(\psi)$. □

Com o resultado do Teorema 5.2.3, podemos dizer que o ideal tórico $I_{\mathcal{A}}$ é um **ideal binomial**, isto é, um ideal gerado por binômios.

4.2 O cálculo de geradores para $I_{\mathcal{A}}$

Vimos anteriormente que este ideal possui uma base de Gröbner reduzida formada por binômios, mas não sabemos até o momento como calcular efetivamente esta base. Este é o objetivo dessa seção: apresentar dois resultados que nos fornecem ferramentas para calcular uma base de Gröbner para um ideal tórico.

Seja f um polinômio em $K[x_1, \ldots, x_n]$ e $I \subset K[x_1, \ldots, x_n]$ um ideal.

i) Dizemos que f é **homogêneo de grau total d**, se cada termo de f tem grau total d. Se I é gerado por polinômios homogêneos, dizemos que I é um **ideal homogêneo.**

ii) Chamamos de **ideal quociente** o conjunto $(I : f) = \{g \in K[x_1, \ldots, x_n] | \, fg \in I\}$.

iii) Chamamos o conjunto $(I : f^{\infty}) = \left\{g \in K[x_1, \ldots, x_n] | \, f^N g \in I \text{ para algum } N \in \mathbb{N}\right\}$ de **saturação** de I.

Proposição 4.2.1. *Sejam $f \in K[x_1, \ldots, x_n]$ e I um ideal de $K[x_1, \ldots, x_n]$. Então, $(I : f)$ e $(I : f^{\infty})$ são ideais.*

Demonstração. i) $0 \in (I : f)$ e $0 \in (I : f^{\infty})$, pois $0 \in I$.

ii) Sejam $g_1, g_2 \in (I : f)$ e $p_1, p_2 \in (I : f^{\infty})$. Então,

$$g_1 f \in I \text{ e } g_2 f \in I.$$

Assim,

$$(g_1 + g_2)f = g_1 f + g_2 f \in I.$$

Logo, $g_1 + g_2 \in (I : f)$. Por outro lado,

$$p_1 f^{N_1} \text{ e } p_2 f^{N_2} \in I, \text{ para alguns } N_1, N_2 \in \mathbb{N}.$$

Tomando $N = max N_1, N_2$, segue que

$$(p_1 + p_2)f^N = p_1 f^N + p_2 f^N \in I.$$

Portanto, $p_1 + p_2 \in (I : f^{\infty})$.

iii) Sejam $g \in (I : f)$, $p \in (I : f^{\infty})$ e $h \in K[x_1, \ldots, x_n]$. Então,

$$gf \in I \text{ e } pf^N \in I, \text{ para algum } N \in \mathbb{N}.$$

Como I é ideal, segue que gfh e phf^N estão em I. Portanto $gf \in (I : f)$ e $ph \in (I : f^{\infty})$. □

Proposição 4.2.2. *Fixe a ordem monomial grevlex com $x_1 \succ \ldots \succ x_n$. Seja $\mathcal{G}$ a base de Gröbner reduzida de um ideal homogêneo $I \subseteq K[x_1, \ldots, x_n]$. Então, o conjunto*

$$\mathcal{G}' = \{f \in \mathcal{G} | \, x_n \text{ não divide } f\} \cup \{f/x_n | \, f \in \mathcal{G} \text{ e } x_n \text{ divide } f\}$$

é uma base de Gröbner de $(I : x_n)$ e o conjunto

$$\mathcal{G}'' = \left\{f/x_n^N | \, f \in \mathcal{G} \text{ e } x_n^N \text{ é a maior potência de } x_n \text{ que divide } f\right\}$$

é uma base de Gröbner de $(I : x_n^{\infty})$.

Demonstração. Vamos mostrar que $\mathcal{G}'$ é base de Gröbner para $(I : x_n)$. A prova para $\mathcal{G}''$ é análoga.

Note que $\mathcal{G}' \subseteq (I : x_n)$. Isso implica que

$$\langle TL(\mathcal{G}')\rangle \subseteq \langle TL((I : x_n))\rangle .$$

Para obtermos a outra inclusão, tome $g \in (I : x_n)$. Por definição de $(I : x_n)$, temos que $x_n g \in I$. Como $\mathcal{G}$ é base de Gröbner de I, segue que para algum $f \in \mathcal{G}$, $TL(f)$ divide $TL(gx_n) = x_n TL(g)$.

A ordem monomial escolhida nos garante que x_n divide f se, e somente se, x_n divide $TL(f)$. Assim, se x_n não divide f, então f está em $\mathcal{G}'$ e $TL(f)$ divide $TL(g)$ Se x_n divide $TL(f)$, então x_n divide f e neste caso f/x_n está em $\mathcal{G}'$ e $TL(f/x_n) = TL(f)/x_n$ divide $TL(g)$. Em ambos os casos $TL(g)$ está no ideal gerado pelos termos líderes de $\mathcal{G}'$. □

Observação 4.2.3. *A ordem monomial usada na Proposição 4.2.2 faz sentido sempre que o ideal I é homogêneo com respeito a alguma graduação positiva $deg(x_i) = d_i > 0$.*

Aplicando a Proposição 4.2.2, considerando uma variável de cada vez, podemos calcular o ideal saturação

$$(I : (x_1 \cdot \ldots \cdot x_n)^\infty) = ((\ldots((I : x_1^\infty) : x_2^\infty) : \ldots) : x_n^\infty). \tag{4.5}$$

Observe que este ideal consiste dos polinômios $f \in K[x_1, \ldots, x_n]$ tais que $fx^\alpha \in I$, para algum monômio $x^\alpha \in K[x_1, \ldots, x_n]$.

Observação 4.2.4. *Considere um ideal tórico $I_\mathcal{A}$ associado a uma matriz $\mathcal{A} = (a_{ij})_{m\times n}$, com entradas inteiras não negativas a_{ij} e colunas não nulas. Na definição de ideal tórico, vimos que $I_\mathcal{A}$ tem graduação positiva $deg(x_j) = a_{1j} + \cdots + a_{mj}$. Se $\tau = (\tau_1, \ldots, \tau_n)$ é o vetor que representa esta graduação, então a ordem lexicográfica graduada reversa, neste caso, é dada da seguinte forma: $\alpha \succ_{grevlex} \beta$ e escrevemos $x^\alpha \succ_{grevlex} x^\beta$, se*

$$\langle \alpha, \tau\rangle > \langle \beta, \tau\rangle \text{ ou } \langle \alpha, \tau\rangle = \langle \beta, \tau\rangle \text{ e a primeira coordenada não nula em } \alpha - \beta,$$
$$\text{da direita para a esquerda, é negativa.}$$

Note que com esta graduação, $I_\mathcal{A}$ é um ideal homogêneo.

Assim, se $\psi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ é o homomorfismo determinado pela matriz $\mathcal{A}$ e $\mathcal{C} = \{v_1, \ldots, v_r\}$ é um subconjunto do $ker(\psi)$, definimos

$$I_\mathcal{C} := \left\langle x^{v^+} - x^{v^-} \,|\, v \in \mathcal{C} \right\rangle . \tag{4.6}$$

Claramente este ideal é dotado com a mesma graduação que $I_\mathcal{A}$. Ainda, $I_\mathcal{C}$ é homogêneo com respeito a esta graduação. Dessa forma, podemos aplicar a proposição em $I_\mathcal{C}$.

Lema 4.2.5. *Dados um número natural r e vetores $v_1, \ldots, v_r \in \mathbb{Z}^n$, considere $\sum_{i=1}^r \lambda_i v_i$, com $\lambda_i \in \mathbb{Z}$. Definimos,*

$$A = \{1 \le i \le r |\, \lambda_i \ge 0\}$$
$$B = \{1 \le i \le r |\, \lambda_i < 0\}.$$

Se $i \in B$ denotamos $\mu_i := -\lambda_i > 0$. Temos que,

$$F := x^{\left(\sum_{i\in A}\lambda_i v_i^+ + \sum_{i\in B}\mu_i v_i^-\right)} - x^{\left(\sum_{i\in A}\lambda_i v_i^- + \sum_{i\in B}\mu_i v_i^+\right)}$$

está em

$$J_{\{v_1,\dots,v_r\}} = \left\langle \left\{ x^{\lambda_i v_i^+} - x^{\lambda_i v_i^-} \,|\, i \in A \right\} \cup \left\{ x^{\mu_i v_i^-} - x^{\mu_i v_i^+} \,|\, i \in B \right\} \right\rangle.$$

Demonstração. Suponha que a afirmação é falsa, ou seja, existe um natural r tal que $F \notin J_{\{v_1,\dots,v_r\}}$. Tome r como sendo o menor possível. Podemos supor que $1 \in A$. Então, F pode ser escrito como

$$\begin{aligned} F = &\left(x^{\lambda_1 v_1^+} - x^{\lambda_1 v_1^-}\right)\left(x^{\left(\sum_{\substack{i\in A\\ i\neq 1}}\lambda_i v_i^+ + \sum_{i\in B}\mu_i v_i^-\right)}\right) \\ &+ x^{\lambda_1 v_1^-}\left(x^{\left(\sum_{\substack{i\in A\\ i\neq 1}}\lambda_i v_i^+ + \sum_{i\in B}\mu_i v_i^-\right)} - x^{\left(\sum_{\substack{i\in A\\ i\neq 1}}\lambda_i v_i^- + \sum_{i\in B}\mu_i v_i^+\right)}\right). \end{aligned}$$

Fazendo $G := x^{\left(\sum_{\substack{i\in A\\ i\neq 1}}\lambda_i v_i^+ + \sum_{i\in B}\mu_i v_i^-\right)} - x^{\left(\sum_{\substack{i\in A\\ i\neq 1}}\lambda_i v_i^- + \sum_{i\in B}\mu_i v_i^+\right)}$, temos que $G \in J_{\{v_2,\dots,v_r\}}$. Logo, $F \in J_{\{v_1,\dots,v_r\}}$. O que é um contradição. Portanto $F \in J_{\{v_1,\dots,v_r\}}$. □

Observação 4.2.6. *Dado um vetor $v \in \mathbb{Z}^n$ e $\lambda \in \mathbb{N}$, veja que*

$$x^{\lambda v^+} - x^{\lambda v^-} = (x^{v^+} - x^{v^-}) \sum_{j=1}^{\lambda} (x^{(j-1)v^+} x^{(\lambda - j)v^-}).$$

Lema 4.2.7. *Sejam α e β em $\mathbb{N}^n$. Se $x^\alpha - x^\beta \in I_{\mathcal{C}}$ (4.6), então $\alpha - \beta$ pertence ao $\mathbb{Z}$-módulo gerado por $\mathcal{C}$, que denotaremos por $[\mathcal{C}]$.*

Demonstração. Se $x^\alpha - x^\beta \in I_{\mathcal{C}}$. Então,

$$x^\alpha - x^\beta = \sum_{v\in\mathcal{C}} f(x)(x^{v^+} - x^{v^-}).$$

Como $f(x)$ pode ser escrito como uma soma cujos termos são da forma x^α ou $-x^\alpha$, existe $s \in \mathbb{N}$ tal que

$$\sum_{v\in\mathcal{C}} f(x)(x^{v^+} - x^{v^-}) = \sum_{i=1}^{s} x^{\alpha_i}(x^{w_i^+} - x^{w_i^-}), \tag{4.7}$$

com w_i ou $-w_i$ pertencentes a $\mathcal{C}$. Em outras palavras, os termos da soma do lado direito em (4.7) são da forma $x^\alpha(x^{v^+} - x^{v^-})$ ou $-x^\alpha(x^{v^+} - x^{v^-})$. No primeiro caso $w_i = v$ e no segundo $w_i = -v$. Dessa forma,

$$x^\alpha - x^\beta = \sum_{i=1}^{s} x^{\alpha_i}(x^{w_i^+} - x^{w_i^-}), \quad w_i \text{ ou } -w_i \in \mathcal{C}.$$

Provemos que $\alpha - \beta \in [\mathcal{C}]$ por indução em s.

Se $s = 1$,

$$x^{\alpha} - x^{\beta} = x^{\alpha_1}(x^{w_1^+} - x^{w_1^-}).$$

Implicando que $\alpha = \alpha_1 + w_1^+$, $\beta = \alpha_1 + w_1^-$ e consequentemente temos que $\alpha - \beta = w_1^+ - w_1^- \in [\mathcal{C}]$.

Suponhamos por indução que a afirmação seja certa para $s-1$ termos na soma. Seja

$$x^{\alpha} - x^{\beta} = \sum_{i=1}^{s} x^{\alpha_i}(x^{w_i^+} - x^{w_i^-}). \tag{4.8}$$

Em vista da igualdade acima, sabemos que deve existir $1 \leq i \leq s$ tal que $-x^{\beta} = x^{\alpha_i}(-x^{w_i^-})$. Reorganizando os índices, podemos supor $i = s$. Assim,

$$-x^{\beta} = x^{\alpha_s}(-x^{w_s^-}). \tag{4.9}$$

Donde segue que $\beta = \alpha_s + w_s^-$. Logo, podemos reescrever (4.8) como

$$x^{\alpha} - x^{\beta} = \sum_{i=1}^{s-1} x^{\alpha_i}(x^{w_i^+} - x^{w_i^-}) + x^{\alpha_s}(x^{w_s^+} - x^{w_s^-}).$$

Por (4.9), temos

$$x^{\alpha} - x^{\alpha_s + w_s^+} = \sum_{i=1}^{s-1} x^{\alpha_i}(x^{w_i^+} - x^{w_i^-}).$$

Por hipótese de indução $\alpha - (\alpha_s + w_s^+) \in [\mathcal{C}]$. Dessa forma,

$$\begin{aligned} \alpha - \beta =& \alpha - (\alpha_s + w_s^-) \\ =& \alpha - (\alpha_s + w_s^+) + (\alpha_s + w_s^+) - (\alpha_s + w_s^-) \\ =& \alpha - (\alpha_s + w_s^+) + w_s. \end{aligned}$$

Como $\alpha - (\alpha_s + w_s^+), w_s \in [\mathcal{C}]$, então $\alpha - \beta \in [\mathcal{C}]$. □

Teorema 4.2.8. *Seja $\mathcal{C} = \{v_1, \ldots, v_r\} \subset ker(\psi)$. Então, $\mathcal{C}$ gera o $ker(\psi)$ se, e somente se,*

$$(I_{\mathcal{C}} : (x_1 \cdot \ldots \cdot x_n)^{\infty}) = I_{\mathcal{A}}.$$

Demonstração. [$\Leftarrow$] Suponha que $\mathcal{C} = \{v_1, \ldots, v_r\}$ gera o $ker(\psi)$. Se $f \in I_{\mathcal{C}} : (x_1 \cdot \ldots \cdot x_n)^{\infty})$, então $fx^{\alpha} \in I_{\mathcal{C}}$ para algum monômio em $K[x_1, \ldots, x_n]$. Assim,

$$fx^{\alpha} = \sum_{i=1}^{r} g(x^{v_i^+} - x^{v_i^-}),$$

com $g \in K[x_1, \ldots, x_n]$. Segue daí que

$$\phi(f)\phi(x^{\alpha}) = \sum_{i=1}^{r} \phi(g)\phi(x^{v_i^+} - x^{v_i^-}) = 0,$$

pois $I_{\mathcal{C}} \subseteq I_{\mathcal{A}}$. Consequentemente, devemos ter $\phi(f) = 0$. Logo, $f \in I_{\mathcal{A}}$, isto é,

$$(I_{\mathcal{C}} : (x_1 \cdot \ldots \cdot x_n)^{\infty}) \subseteq I_{\mathcal{A}}.$$

Para a outra inclusão, tome $u \in ker(\psi)$. Então podemos escrever $u = \sum_{i=1}^{r} \lambda_i v_i$, com $\lambda_i \in \mathbb{Z}$. Isto implica na seguinte igualdade:

$$\frac{x^{u^+}}{x^{u^-}} - 1 = \prod_{i=1}^{r} \left(\frac{x^{v_i^+}}{x^{v_i^-}} \right)^{\lambda_i} - 1 \tag{4.10}$$

Como $\lambda_i \in \mathbb{Z}$, podemos escrever (4.10) como segue

$$\frac{x^{u^+}}{x^{u^-}} - 1 = \prod_{\lambda_i \geq 0} \left(\frac{x^{v_i^+}}{x^{v_i^-}} \right)^{\lambda_i} \prod_{\lambda_i < 0} \left(\frac{x^{v_i^-}}{x^{v_i^+}} \right)^{-\lambda_i} - 1.$$

Considerando os seguintes conjuntos:

$$\begin{aligned} A =& \{1 \leq i \leq r | \, \lambda_i \geq 0\} \\ B =& \{1 \leq i \leq r | \, \lambda_i < 0\}. \end{aligned}$$

e fazendo $\mu_i := -\lambda_i > 0$, se $i \in B$. Temos,

$$\frac{x^{u^+}}{x^{u^-}} - 1 = \prod_{i \in A} \left(\frac{x^{v_i^+}}{x^{v_i^-}} \right)^{\lambda_i} \prod_{i \in B} \left(\frac{x^{v_i^-}}{x^{v_i^+}} \right)^{\mu_i} - 1.$$

Eliminando os denominadores, obtemos

$$\prod_{i \in A} \left(x^{v_i^-} \right)^{\lambda_i} \prod_{i \in B} \left(x^{v_i^+} \right)^{\mu_i} \left(x^{u^+} - x^{u^-} \right) = x^{u^-} \left(\prod_{i \in A} \left(x^{v_i^+} \right)^{\lambda_i} \prod_{i \in B} \left(x^{v_i^-} \right)^{\mu_i} - \prod_{i \in A} \left(x^{v_i^-} \right)^{\lambda_i} \prod_{i \in B} \left(x^{v_i^+} \right)^{\mu_i} \right).$$

Fazendo

$$F := \prod_{i \in A} \left(x^{v_i^+} \right)^{\lambda_i} \prod_{i \in B} \left(x^{v_i^-} \right)^{\mu_i} - \prod_{i \in A} \left(x^{v_i^-} \right)^{\lambda_i} \prod_{i \in B} \left(x^{v_i^+} \right)^{\mu_i},$$

devemos mostrar que $F \in I_{\mathcal{C}}$. Vejamos que isto, de fato ocorre. Note que

$$F = x^{\left(\sum_{i \in A} \lambda_i v_i^+ + \sum_{i \in B} \mu_i v_i^-\right)} - x^{\left(\sum_{i \in A} \lambda_i v_i^- + \sum_{i \in B} \mu_i v_i^+\right)}.$$

Pelo Lema 4.2.5, segue que

$$F \in J_{\{v_1, \ldots, v_r\}} = \left\langle \left\{ x^{\lambda_i v_i^+} - x^{\lambda_i v_i^-} | \, i \in A \right\} \cup \left\{ x^{\mu_i v_i^-} - x^{\mu_i v_i^+} | \, i \in B \right\} \right\rangle.$$

Agora, pela Observação 4.2.6 temos que $x^{\lambda_i v_i^+} - x^{\lambda_i v_i^-}$ e $x^{\mu_i v_i^-} - x^{\mu_i v_i^+}$ estão em $I_{\mathcal{C}}$, para $i \in A \cup B$. Portanto, $F \in I_{\mathcal{C}}$ e assim fica provada a outra inclusão.

Vamos agora, provar a recíproca do Teorema. Para isso, suponhamos que

$$(I_{\mathcal{C}} : (x_1 \cdot \ldots \cdot x_n)^{\infty}) = I_{\mathcal{A}}.$$

Tome $u \in ker(\psi)$. Então $x^{u^+} - x^{u^-} \in I_{\mathcal{A}}$. Por hipótese existe $\alpha \in \mathbb{N}^n$ tal que

$$x^{\alpha}(x^{u^+} - x^{u^-}) \in I_{\mathcal{C}},$$

ou seja, $x^{\alpha + u^+} - x^{\alpha + u^-} \in I_{\mathcal{C}}$. Pelo Lema 4.2.7, concluímos que

$$(\alpha + u^+) - (\alpha + u^-) = u \in [\mathcal{C}].$$

Como u é arbitrário, temos a recíproca do Teorema provada. □

Com o resultado da Proposição 4.2.2 e do Teorema 4.2.8, podemos calcular uma base de Gröbner para um dado ideal tórico: iniciamos calculando um conjunto de geradores $\mathcal{C}$ para $ker(\psi)$. Pelo Teorema 4.2.8 temos que $(I_{\mathcal{C}} : (x_1 \cdot \ldots \cdot x_n)^{\infty}) = I_{\mathcal{A}}$. Assim, basta usarmos a Proposição 4.2.2 para calcular uma base de Gröbner para $(I_{\mathcal{C}} : (x_1 \cdot \ldots \cdot x_n)^{\infty})$.

A seguir, apresentaremos dois exemplos de como pode ser feito o cálculo da base de Gröbner para um ideal tórico. No primeiro exemplo, usaremos a graduação usual e no segundo uma graduação positiva $deg(x_i) = d_i > 0$.

Exemplo 4.2.9. *Considere a matriz*

$$\mathcal{A} = \begin{bmatrix} 1 & 3 & 1 & 5 \\ 1 & 2 & 3 & 2 \end{bmatrix}.$$

Sabemos que neste caso a graduação do ideal tórico é dada pelo vetor $\tau = (2, 5, 4, 7)$. *É fácil ver que* $ker(\psi)$ *é gerado pelo conjunto* $\mathcal{C} = \{(-7, 2, 1, 0), (4, -3, 0, 1)\}$. *Então,*

$$I_{\mathcal{C}} = \left\langle x_2^2 x_3 - x_1^7, x_1^4 x_4 - x_2^3 \right\rangle.$$

Agora vamos calcular uma base de Gröbner para o ideal saturação $(I_{\mathcal{C}} : (x_1 \cdot \ldots \cdot x_n)^{\infty})$. *Faremos isso utilizando a Proposição 4.2.2, considerando uma variável de cada vez. Para evitar confusão em cada passo dos cálculos, comecemos fazendo* $I_0 := I_{\mathcal{C}} = \langle x_2^2 x_3 - x_1^7, x_1^4 x_4 - x_2^3 \rangle$. *Vamos agora calcular uma base de Gröbner reduzida para* I_0, *com respeito à ordem grevlex com* $x_1 \prec x_4 \prec x_3 \prec x_2$.

Reordenando os os termos dos polinômios com esta ordem, temos:

1^o ***Passo:*** $\mathcal{G}_0 = \{f_{10}, f_{20}\} = \{x_2^2 x_3 - x_1^7, x_2^3 - x_1^4 x_4\}$ *e* $I_0 = \langle f_{10}, f_{20} \rangle = \langle x_2^2 x_3 - x_1^7, x_2^3 - x_1^4 x_4 \rangle$ *Aplicando o Algoritmo de Buchberger, obtemos*

$$\mathcal{G}_0 = \left\{ x_2^2 x_3 - x_1^7, x_2^3 - x_1^4 x_4, x_1^4 x_3 x_4 - x_1^7 x_2 \right\}$$

como base de Gröbner reduzida para I_0. *Dividindo* $x_1^4 x_3 x_4 - x_1^7 x_2$ *por* x_1^4 *temos que*

$$\mathcal{G'}_0 = \left\{ x_2^2 x_3 - x_1^7, x_2^3 - x_1^4 x_4, x_3 x_4 - x_1^3 x_2 \right\}$$

é uma base de Gröbner para $I_1 = (I_0 : x_1^{\infty})$.

2^o ***Passo:*** *Agora realizamos o mesmo processo com* I_1, *usando a ordem monomial grevlex com* $x_2 \prec x_4 \prec x_3 \prec x_1$. *Reordenando os termos do binômios, temos:*

$$\mathcal{G}_1 = \{f_{11}, f_{21}, f_{31}\} = \left\{ x_1^7 - x_2^2 x_3, x_1^4 x_4 - x_2^3, x_3 x_4 - x_1^3 x_2 \right\}$$

Depois da aplicação do Algoritmo de Buchberger, concluímos que $\mathcal{G}_1 = \{f_{11}, f_{21}, f_{31}\}$ *é a própria base de Gröbner reduzida de* I_1. *Como nenhum binômio desta base é dividido por nenhuma potência de* x_2, *obtemos* $\mathcal{G'}_1 = \mathcal{G}_1$, *como base de Gröbner para* $I_2 = (I_1 : x_2^{\infty})$.

3º Passo: *Reordenamos os termos dos binômios em* $\mathcal{G'}_1$ *de acordo com a ordem monomial grevlex, com* $x_3 \prec x_4 \prec x_2 \prec x_1$, *temos* $\mathcal{G}_2 = \{f_{12}, f_{22}, f_{32}\} = \{x_1^7 - x_2^2 x_3, x_2^3 - x_1^4 x_4, x_1^3 x_2 - x_3 x_4\}$. *Aplicando o Algoritmo de Buchberger em* $\mathcal{G}_2$, *não temos nenhuma alteração, ou seja,* $\mathcal{G}_2 = \{f_{12}, f_{22}, f_{32}\}$ *é base de Gröbner reduzida para* I_2. *Novamente, nenhum binômio em* $\mathcal{G}_2$ *é divisível por nenhuma potência de* x_3. *Logo* $\mathcal{G'}_2 = \mathcal{G}_2$ *é uma base de Gröbner para* $I_3 = (I_2 : x_3^{\infty})$.

4º Passo: *A ordem monomial agora será a grevlex com* $x_4 \prec x_3 \prec x_2 \prec x_1$. *Fazendo a reordenação em* $\mathcal{G}'$ *com respeito à essa ordem, obtemos*

$$\mathcal{G}_3 = \{f_{13}, f_{23}, f_{33}\} = \left\{ x_1^7 - x_2^2 x_3, x_2^3 - x_1^4 x_4, x_1^3 x_2 - x_3 x_4 \right\}.$$

Após a aplicação do Algoritmo de Buchberger em $\mathcal{G}_3$, concluímos que $\mathcal{G}_3 = \{f_{13}, f_{23}, f_{33}\}$ é base de Gröbner reduzida de I_3. Ainda, $\mathcal{G}_3 = \{f_{13}, f_{23}, f_{33}\}$ é base de Gröbner de $I_4 = (I_3 : x_4^\infty)$. Note que por (4.5), temos que $I_4 = (I_\mathcal{C} : (x_1 \cdot \ldots \cdot x_n)^\infty)$. Portanto,

$$I_\mathcal{A} = \left\langle x_1^7 - x_2^2x_3, x_2^3 - x_1^4x_4, x_1^3x_2 - x_3x_4 \right\rangle.$$

Observe que a partir desta base pode-se calcular uma base de Gröbner para $I_\mathcal{A}$ com respeito à qualquer ordem monomial desejada.

Exemplo 4.2.10. *Consideremos agora a matriz $\mathcal{A}$ como abaixo:*

$$\mathcal{A} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{bmatrix}.$$

Observe que cada coluna de $\mathcal{A}$ tem a mesma soma, a saber 3. Isto implica que o ideal tórico $I_\mathcal{A}$ é homogêneo com a graduação usual. O $ker(\psi)$ é gerado pelo conjunto $\mathcal{C} = \{(1, -2, 1, 0), (2, -3, 0, 1)\}$. Assim,

$$I_\mathcal{C} = \left\langle x_1x_3 - x_2^2, x_1^2x_4 - x_2^3 \right\rangle.$$

Agora denotaremos $I_\mathcal{C}$ por I_0 e consideraremos a ordem grevlex com $x_1 \prec x_4 \prec x_3 \prec x_2$.

1º Passo: *Reordenando os termos dos binômios geradores de I_0, de acordo com a ordem monomial em questão, obtemos*

$$\mathcal{G}_0 = \{f_{10}, f_{20}\} = \left\{x_2^2 - x_1x_3, x_2^3 - x_1^2x_4\right\}.$$

Pelo Algoritmo de Buchberger encontramos o seguinte conjunto como base de Gröbner para I_0:

$$\mathcal{G}_0 = \left\{x_2^2 - x_1x_3, x_2^3 - x_1^2x_4, x_1x_2x_3 - x_1^2x_4, -x_1^2x_3^2 + x_1^2x_2x_4\right\}.$$

Note que esta base não é reduzida. Para utilizarmos a Proposição 4.2.2 devemos ter uma base de Gröbner reduzida. Observe que para obtermos essa base, basta, neste caso, retirarmos o polinômio $x_2^3 - x_1^2x_4$ de $\mathcal{G}_0$, e assim obtemos

$$\mathcal{G}_0 = \left\{x_2^2 - x_1x_3, x_1x_2x_3 - x_1^2x_4, -x_1^2x_3^2 + x_1^2x_2x_4\right\},$$

como base de Gröbner reduzida para I_0. Dividindo $x_1x_2x_3 - x_1^2x_4$ por x_1 e $-x_1^2x_3^2 + x_1^2x_2x_4$ por x_1^2, temos que

$$\mathcal{G'}_0 = \left\{x_2^2 - x_1x_3, x_2x_3 - x_1x_4, x_3^2 - x_2x_4\right\}$$

é base de Gröbner para $I_1 = (I_0 : x_1^\infty)$.

2º Passo: *Agora vamos considerar, a ordem grevlex com $x_2 \prec x_4 \prec x_3 \prec x_1$. Reordenando os termos do polinômios em $\mathcal{G'}_0$, obtemos*

$$\mathcal{G}_1 = \{f_{11}, f_{21}, f_{31}\} = \left\{x_1x_3 - x_2^2, x_1x_4 - x_2x_3, x_3^2 - x_2x_4\right\}.$$

Calculando uma base de Gröbner reduzida para I_1, concluímos que $\mathcal{G}_1 = \{f_{11}, f_{21}, f_{31}\}$, já é a base procurada. Ainda, $\mathcal{G'}_1 = \mathcal{G}_1 = \{f_{11}, f_{21}, f_{31}\}$ é a base de Gröbner para $I_2 = (I_1 : x_2^\infty)$.

3º Passo: *Agora consideramos a ordem grevlex com $x_3 \prec x_4 \prec x_2 \prec x_1$. Reordenando dos polinômios de $\mathcal{G'}_1$, obtemos*

$$\mathcal{G}_2 : \{f_{12}, f_{22}, f_{32}\} = \left\{x_2^2 - x_1x_3, x_1x_4 - x_2x_3, x_2x_4 - x_3^2\right\}.$$

Através do Algoritmo de Bughberger, vemos que $\mathcal{G}_2 : \{f_{12}, f_{22}, f_{32}\} = \mathcal{G'}_2$ é uma base de Gröbner para I_2 e $I_3 = (I_2 : x_3^\infty)$.

4º Passo: *Aplicando o mesmo processo em I_3, com relação à ordem grevlex com $x_4 \prec x_3 \prec x_2 \prec x_1$, temos que*

$$\mathcal{G}_3 = \{f_{13}, f_{23}, f_{33}\} = \left\{x_2^2 - x_1x_3, x_2x_3 - x_1x_4, x_3^2 - x_2x_4\right\}$$

é base de Gröbner para I_3 e para $I_4 = (I_3 : x_4^\infty)$.

Portanto, pelo Teorema 4.2.8 segue que

$$I_\mathcal{A} = \left\langle x_2^2 - x_1x_3, x_2x_3 - x_1x_4, x_3^2 - x_2x_4 \right\rangle.$$

CAPÍTULO 5

VARIEDADE AFIM TÓRICA

Seja $\mathcal{A} = (a_{ij})_{m\times n}$, com entradas inteiras não negativas a_{ij} e colunas não nulas. O **conjunto tórico** Γ determinado por $\mathcal{A}$ é um subconjunto do espaço afim $\mathbb{A}^n_K$ dado parametricamente por $x_j = t_1^{a_{1j}} \cdot \ldots \cdot t_m^{a_{mj}}$, para todo $j = 1, \ldots, n$, isto é,

$$\Gamma = \left\{ \left(t_1^{a_{11}} \ldots t_m^{a_{m1}}, \ldots, t_1^{a_{1n}} \ldots t_m^{a_{mn}} \right) \in \mathbb{A}^n_K \mid t_1, \ldots, t_m \in K \right\}.$$

Lembrando que $a_j = (a_{1j}, \ldots, a_{mj})$ é o vetor cujas entradas são elementos da $j-$ésima coluna da matriz $\mathcal{A}$.

No capítulo anterior definimos o que é um ideal tórico associado à matriz $\mathcal{A}$. Chamamos de **variedade afim tórica** à variedade $\mathbf{V}(I_{\mathcal{A}})$ deste tipo de ideal. Utilizaremos vários dos resultados apresentados até aqui para provar o resultado principal deste trabalho. Nosso objetivo aqui é caracterizar quando um conjunto tórico Γ é uma variedade afim tórica nos termos da estrutura do corpo K e da condição $V(I_{\mathcal{A}}, x_i) \subset \Gamma$. As principais referências utilizadas neste capítulo foram [8] e [5].

5.1 Fecho de Zariski

Seja $S \subseteq \mathbb{A}^n_K$. O conjunto S sendo ou não uma variedade afim, temos que

$$\mathbf{I}(S) = \{f \in K[x_1, \ldots, x_n] \mid f(a) = 0 \text{ para todo a} \in S\}$$

é um ideal em $K[x_1, \ldots, x_n]$. De fato, temos que $0 \in \mathbf{I}(S)$, pois o polinômio zero se anula em todos os pontos de $\mathbb{A}^n_K$. Agora suponha que $f, g \in \mathbf{I}(S)$ e $h \in K[x_1, \ldots, x_n]$. Seja $(c_1, \ldots, c_n)$ um ponto arbitrário em S. Então,

$$\begin{aligned} f(c_1, \ldots, c_n) + g(c_1, \ldots, c_n) &= 0 + 0 = 0, \\ f(c_1, \ldots, c_n) \cdot h(c_1, \ldots, c_n) &= 0 \cdot h(c_1, \ldots, c_n) = 0. \end{aligned}$$

Logo, $\mathbf{I}(S)$ é um ideal.

Proposição 5.1.1. *Seja $S \subseteq \mathbb{A}^n_K$. A variedade afim $\boldsymbol{V}(\boldsymbol{I}(S))$ é a menor variedade que contém S, ou seja, se $W \subset \mathbb{A}^n_K$ é qualquer variedade afim contendo S, então $\boldsymbol{V}(\boldsymbol{I}(S)) \subseteq W$.*

Demonstração. Seja W uma variedade afim tal que $S \subseteq W$. Então, $\mathbf{I}(W) \subseteq \mathbf{I}(S)$ e assim, $\mathbf{V}(\mathbf{I}(S)) \subseteq \mathbf{V}(\mathbf{I}(W))$. Como W é uma variedade afim, do Teorema 2.3.7 temos que $\mathbf{V}(\mathbf{I}(W)) = W$ e assim o resultado segue. □

Em vista da proposição acima, se $S \subseteq \mathbb{A}_K^n$, chamamos de **fecho de Zarisk** de S, a menor variedade algébrica contendo S, isto é, $\mathbf{V}(\mathbf{I}(S))$. O fecho de Zarisk de S é denotado por $\overline{S}$.

Proposição 5.1.2. *Seja S e T subconjuntos de $\mathbb{A}_K^n$. Então:*

(a) $\boldsymbol{I}(\overline{S}) = \boldsymbol{I}(S)$

(b) Se $S \subseteq T$, então $\overline{S} \subseteq \overline{T}$

(c) $\overline{S \cup T} = \overline{S} \cup \overline{T}$

Demonstração. (a) $\overline{S}$ é o fecho de Zarisk de S, então $S \subseteq \overline{S}$. Segue que $\mathbf{I}(\overline{S}) \subseteq \mathbf{I}(S)$. Por outro, $f \in \mathbf{I}(S)$, então $f(a) = 0$, para todo $a \in S$. assim, $S \subseteq V(f)$. Por definição de fecho de Zarisk, segue que $\overline{S} \subseteq V(f)$. Logo, $I(\mathbf{V}(f)) \subseteq \mathbf{I}(\overline{S})$, o que implica que $f \in \mathbf{I}(\overline{S})$. Portanto, $\mathbf{I}(S) \subseteq \mathbf{I}(\overline{S})$.

(b) Suponha que $S \subseteq T$. Por definição $T \subseteq \overline{T}$. Assim, $S \subset \overline{T}$. Logo, segue da definição de $\overline{S}$ que $\overline{S} \subseteq \overline{T}$.

(c) Se $a \in S \cup T$, então

$$a \in S \text{ ou } a \in T \Rightarrow a \in \overline{S} \text{ ou } a \in \overline{T} \Rightarrow a \in \overline{S} \cup \overline{T}.$$

Logo, $S \cup T \subseteq \overline{S} \cup \overline{T}$ e consequentemente $\overline{S \cup T} \subseteq \overline{S} \cup \overline{T}$.

Por outro lado,

$$S \subseteq S \cup T \text{ e } T \subseteq S \cup T \Rightarrow \overline{S} \subseteq \overline{S \cup T} \text{ e } \overline{T} \subseteq \overline{S \cup T} \Rightarrow \overline{S} \cup \overline{T} \subseteq \overline{S \cup T}.$$

Portanto, $\overline{S} \cup \overline{T} = \overline{S \cup T}$.

□

Proposição 5.1.3 ([12], p.338)**.** *Sejam Γ e $I_{\mathcal{A}}$, respectivamente, o conjunto tórico e o ideal tórico correspondentes à matriz $\mathcal{A}$. Se K é um corpo infinito, então*

(a) $I_{\mathcal{A}} = I(\Gamma)$ *e*

(b) $V(I_{\mathcal{A}})$ *é o fecho de Zarisk de* Γ.

Demonstração. (a) Vejamos que $\Gamma \subset V(I_{\mathcal{A}})$. Para isso, tome $c = (c_1, \ldots, c_n) \in \Gamma$ e $f = \sum_\alpha k_\alpha x^\alpha \in I_{\mathcal{A}}$.

i) Denotando por $g_f = \phi(f)$ a imagem de f por ϕ. Temos que g_f é o polinômio nulo em $K[t_1, \ldots, t_m]$, ou seja, $g_f(d_1, \ldots, d_m) = 0$ para todo $d_1, \ldots, d_m \in K$. Observe ainda que $g_f = \sum_\alpha k_\alpha t^{\psi(\alpha)}$.

ii) Como $c = (c_1, \ldots, c_n) \in \Gamma$, existem $d_1, \ldots, d_m \in K$ tais que $c_j = d_1^{a_{1j}} \cdot \ldots \cdot d_m^{a_{mj}}$.

Fazendo $c^\alpha = c_1^{\alpha_1} \cdot \ldots \cdot c_n^{\alpha_n}$, temos $f(c_1, \ldots, c_n) = \sum_\alpha k_\alpha c^\alpha$. Denotando $c_j = d^{a_j}$, segue que

$$\begin{aligned} f(c_1, \ldots, c_n) &= \sum_\alpha k_\alpha d^{\alpha_1 a_1 + \cdots + \alpha_n a_n} \\ &= \sum_\alpha k_\alpha d^{\psi(\alpha)} \\ &= g_f(d_1, \ldots, d_m) = 0 \end{aligned}$$

Como $f \in I_{\mathcal{A}}$ é arbitrário concluímos que $c = (c_1, \ldots, c_n) \in V(I_{\mathcal{A}})$ e consequentemente, $\Gamma \subset V(I_{\mathcal{A}})$. Então, $\mathbf{I}(V(I_{\mathcal{A}})) \subset \mathbf{I}(\Gamma)$. Como, $I_{\mathcal{A}} \subset \mathbf{I}(V(I_{\mathcal{A}}))$, concluímos que $I_{\mathcal{A}} \subset \mathbf{I}(\Gamma)$. Para provar a outra inclusão, tome $f = \sum_\alpha k_\alpha x^\alpha \in \mathbf{I}(\Gamma)$. Sabemos que $f \in K[x_1, \ldots, x_n]$ se anula em todos os pontos $c \in \Gamma$. Seja $d = (d_1, \ldots, d_m) \in \mathbb{A}^m_K$. Se a_j é a $j-$ésima coluna da matriz $\mathcal{A}$ correspondente ao ideal tórico $I_{\mathcal{A}}$, então para todo $j = 1, \ldots, n$ temos que $\phi(x_j) = t^{a_j}$ avaliado em d, é igual a $d^{a_j} = d_1^{a_{1j}} \cdot \ldots \cdot d_m^{a_{mj}}$. Assim, $\overline{d} = (d^{a_1}, \ldots, d^{a_n}) \in \Gamma$. Fazendo $g_f = \phi(f)$, temos que

$$g_f(d) = \sum_\alpha k_\alpha d^{\psi(\alpha)}. \tag{5.1}$$

Por outro lado, sabemos que $f(d^{a_1}, \ldots, d^{a_n}) = 0$, ou seja,

$$\sum_\alpha k_\alpha \overline{d}^\alpha = \sum_\alpha k_\alpha d^{\psi(\alpha)} = 0, \tag{5.2}$$

com $(\overline{d})^\alpha = (d^{a_1})^{\alpha_1} \cdot \ldots \cdot (d^{a_n})^{\alpha_n}$. Logo, por (5.1) e (5.2) segue que $\phi(f)$ se anula em todos os pontos de $\mathbb{A}^m_k$. Como K é infinito, pela Proposição 1.1.2, segue que $\phi(f)$ é o polinômio nulo em $K[t_1, \ldots, t_m]$. Portanto $f \in I_{\mathcal{A}}$, ou seja, $\mathbf{I}(\Gamma) \subset I_{\mathcal{A}}$.

(b) Sabemos que

$$\overline{\Gamma} = \mathbf{V}(\mathbf{I}(\Gamma)).$$

Pelo item (a), temos que $I_{\mathcal{A}} = \mathbf{I}(\Gamma)$. Portanto,

$$\overline{\Gamma} = \mathbf{V}(\mathbf{I}(\Gamma)) = V(I_{\mathcal{A}}).$$

□

5.2 $\mathbb{Z}$-módulos e Variedade Afim Tórica

Sabemos pelo Teorema 3.2.2 que existem matrizes invertíveis, $U = (u_{ij})$ e $Q = (q_{ij})$ de ordens m e n respectivamente, tais que $D = U\mathcal{A}Q$, sendo D da seguinte forma:

$$D = \begin{bmatrix} \lambda_1 & & & & \vdots & & & \\ & \lambda_2 & & & \vdots & & & \\ & & \ddots & & & & 0 & \\ & & & \lambda_r & \vdots & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & \vdots & & & \\ & 0 & & & \vdots & & 0 & \\ & & & & \vdots & & & \end{bmatrix}$$

com $0 \leq r \leq min\{m, n\}, \lambda_1, \lambda_2, \ldots, \lambda_r$ pertencentes a $\mathbb{Z}\backslash\{0\}$ e λ_j dividindo λ_{j+1}, para cada $j = 1, 2, \ldots, r-1$. Como U e Q são invertíveis, denotaremos suas inversas, respectivamente, por $U^{-1} = (f_{ij})$ e $Q^{-1} = (b_{ij})$. Considere ainda e_i como sendo o vetor unitário em $\mathbb{Z}^n$ que tem a $i-$ésima coordenada igual a um e todas as outras nulas. A partir daqui todas estas notações serão fixas e utilizaremos também as mesmas notações utilizadas no Capítulo 4.

Lema 5.2.1. *Se $\psi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ é o homomorfismo determinado por $\mathcal{A}$, então $ker(\psi) = \mathbb{Z}q_{s+1} \oplus \ldots \oplus \mathbb{Z}q_n$, em que q_i corresponde a i-ésima coluna de Q.*

Demonstração. Seja $x \in \mathbb{Z}^n$ e façamos $y = Q^{-1}x$. Como $D = U\mathcal{A}Q$ segue que

$$\mathcal{A}x = 0 \Leftrightarrow U^{-1}DQ^{-1}x = 0 \Leftrightarrow U^{-1}Dy = 0 \Leftrightarrow Dy = 0. \tag{5.3}$$

Vejamos que $q_i \in ker(\psi)$ para $i \geq s+1$. De fato, $\mathcal{A}q_i = U^{-1}DQ^{-1}q_i = U^{-1}De_i$, sendo e_i o vetor em $\mathbb{Z}^n$ que tem 1 na i-ésima coordenada e 0 nas demais. Mas para $i \geq s+1$, tem-se $De_i = 0$. Logo $\mathcal{A}q_i = 0$ e $q_i \in ker(\psi)$ para $i \geq s+1$.

Por outro lado, se $x \in ker(\psi)$, então $\mathcal{A}x = 0$ e por (5.3), $Dy = 0$. Assim, escrevendo $y = (y_1, \ldots, y_n)$, temos para $i = 1, \ldots, s$ que $\lambda_i y_i = 0$ e consequentemente $y_i = 0$. Portanto, $x = Qy = \sum_{i=s+1}^{n} y_i q_i$. Além disso, o fato de Q ser invertível, implica que suas colunas são linearmente independentes, o que completa a demonstração.

□

Proposição 5.2.2. *Seja $\psi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ a aplicação linear determinada por $\mathcal{A}$ e $v_j = \sum_{i=1}^{s} b_{ij}q_i$, sendo q_i a i-ésima coluna de Q. Se $\{e_1, \ldots, e_n\}$ é a base canônica de $\mathbb{Z}^n$, então $\{v_j - e_j\}_{j=1}^{n}$ é um conjunto gerador de $ker(\psi)$.*

Demonstração. Observe inicialmente que $e_j = \sum_{i=1}^{n} b_{ij}q_i$ para todo $1 \leq j \leq n$, pois QQ^{-1} é igual a matriz identidade. Dessa forma, podemos escrever

$$v_j = \sum_{i=1}^{s} b_{ij}q_i = e_j - \sum_{i=s+1}^{n} b_{ij}q_i \Rightarrow v_j - e_j = -\sum_{i=s+1}^{n} b_{ij}q_i \quad (j = 1, \ldots, n) \tag{5.4}$$

e pelo Lema 5.2.1, concluímos que $v_j - e_j \in ker\psi$ para todo $j = 1, \ldots, n$. Observe que podemos escrever a matriz identidade da seguinte forma, $I_{id} = (\delta_{ik})$, com $\delta_{ik} = 1$ se $i = k$ e $\delta_{ik} = 0$ caso contrário (o símbolo δ_{ik} é chamado **delta de Kronecker**). Da igualdade (5.4) segue que,

$$\begin{aligned} \sum_{j=1}^{n} q_{jk}(e_j - v_j) &= \sum_{j=1}^{n} q_{jk}\left(\sum_{i=s+1}^{n} b_{ij}q_i\right) \\ &= \sum_{i=s+1}^{n} q_i\left(\sum_{j=1}^{n} b_{ij}q_{jk}\right) \end{aligned}$$

Agora, $\sum_{j=1}^{n} q_{jk}b_{ij} = \delta_{ik}$, pois é o produto da i-ésima linha de Q^{-1} pela k-ésima coluna de Q. Logo,

$$\sum_{j=1}^{n} q_{jk}(e_j - v_j) = \sum_{i=s+1}^{n} q_i\delta_{ik} = q_k$$

para $k \geq s+1$. Consequentemente, q_k está no subgrupo de $\mathbb{Z}^n$ gerado por $\{e_j - v_j\}_{j=1}^{n}$ para todo $k \geq s+1$, provando o que queríamos.

□

Teorema 5.2.3. *Sejam K um corpo, Γ o conjunto tórico determinado por $\mathcal{A}$ e $I_{\mathcal{A}}$ o seu ideal tórico. Então $\Gamma = V(I_{\mathcal{A}})$ se, e somente se, as duas seguintes condições são satisfeitas:*

(a) Se $(b_1, \ldots, b_n) \in V(I_{\mathcal{A}})$ e $b_j \neq 0$ para todo j, então $b_1^{q_{1i}} \ldots b_n^{q_{ni}}$ tem raiz λ_i-ésima em K para $i = 1, \ldots, s$.

(b) $V(I_{\mathcal{A}}, x_i) \subset \Gamma$ para $i = 1, \ldots, n$.

Demonstração. [$\Leftarrow$]: Suponhamos que sejam válidas as condições (a) e (b). Pela demonstração da Proposição 5.1.3, temos que $\Gamma \subset V(I_{\mathcal{A}})$.

Para provar a outra inclusão, tome um ponto $c = (c_1, \ldots, c_n) \in V(I_{\mathcal{A}})$. Pela condição (b), se algum $c_j = 0$, temos imediatamente $V(I_{\mathcal{A}}) \subset \Gamma$. Assim, podemos supor que $c_j \neq 0$ para todo j. Pela condição (a) temos que existem $t'_1, \ldots, t'_s \in K$, tais que

$$(t'_i)^{\lambda_i} = c_1^{q_{1i}} \cdot \ldots \cdot c_n^{q_{ni}} = c^{q_i} \quad (i = 1, \ldots, s) \tag{5.5}$$

Por conveniência de notação estendemos a definição de t'_i, fazendo $t'_i = 1$ para $i = s+1, \ldots, m$ e $t' = (t'_1, \ldots, t'_m)$. Faça,

$$t_j = (t'_1)^{u_{1j}} \cdot \ldots \cdot (t'_m)^{u_{mj}} \in K, \quad (j = 1, \ldots, m), \tag{5.6}$$

com $U = (u_{ij})$.

AFIRMAÇÃO: $t^{a_k} = t_1^{a_{1k}} \cdot \ldots \cdot t_m^{a_{mk}} = c_k$ para $k = 1, \ldots, n$. Para provar essa afirmação, precisaremos de várias igualdades que serão apresentas a seguir.

Fazendo $U^{-1} = (f_{ij})$ e comparando as colunas na igualdade $U^{-1}D = \mathcal{A}Q$, tem-se

$$\lambda_i f_i = \sum_{j=1}^{n} q_{ji} a_j \quad (i = 1, \ldots, s), \tag{5.7}$$

com $f_i = (f_{1i}, \ldots, f_{mi})$ e $a_j = (a_{1j}, \ldots, a_{mj})$ denotando a $i-$ésima e a $j-$ésima colunas de U^{-1} e $\mathcal{A}$, respectivamente. Em seguida, comparando as colunas da igualdade $\mathcal{A} = (U^{-1}DQ^{-1})$, obtemos:

$$a_k = \sum_{j=1}^{s} \lambda_j b_{jk} f_j \quad (k = 1, \ldots, n), \tag{5.8}$$

com $Q^{-1} = (b_{ij})$. Da equação (5.6) e do fato de $UU^{-1} = I_{id}$ segue que

$$\begin{aligned} t^{f_k} =& t_1^{f_{1k}} \cdot \ldots \cdot t_m^{f_{mk}} \\ =& ((t'_1)^{u_{11}} \cdot \ldots \cdot (t'_m)^{u_{m1}})^{f_{1k}} \cdot \ldots \cdot ((t'_1)^{u_{1m}} \cdot \ldots \cdot (t'_m)^{u_{mm}})^{f_{mk}} \\ =& (t'_1)^{\sum_{j=1}^{m} u_{1j} f_{jk}} \cdot \ldots \cdot (t'_m)^{\sum_{j=1}^{m} u_{mj} f_{jk}} \\ =& (t'_1)^{\delta_{1k}} \cdot \ldots \cdot (t'_m)^{\delta_{mk}} = t'_k \quad (k = 1, \ldots, m) \end{aligned} \tag{5.9}$$

sendo δ_{ik} o delta de Kronecker, para $i = 1, \ldots, m$. Na Proposição 5.2.2, foi definido

$$v_j = \sum_{i=1}^{s} b_{ij} q_i = \left(\sum_{l=1}^{s} q_{1l} b_{lj}, \ldots, \sum_{l=1}^{s} q_{nl} b_{lj} \right), \quad (j = 1, \ldots, n). \tag{5.10}$$

Vimos que $v_j - e_j \in ker(\psi)$. Escrevendo $v_j = v_j^+ - v_j^-$, segue que $v_j^+ - v_j^- - e_j \in ker(\psi)$. Isto implica que $x^{v_j^+} - x^{e_j + v_j^-} \in I_{\mathcal{A}}$. Como $c \in V(I_{\mathcal{A}})$, segue que $c^{v_j^+} = c^{e_j + v_j^-}$, ou seja,

$$c^{v_j} = c^{e_j} = c_j, \quad (j = 1, \ldots, n). \tag{5.11}$$

Com todas essas igualdades temos que,

$$\begin{aligned} t^{a_k} &\overset{(5.8)}{=} t^{\sum_{j=1}^{s} \lambda_i b_{jk} f_j} \\ &= (t^{f_1})^{\lambda_1 b_{1k}} \cdot \ldots \cdot (t^{f_s})^{\lambda_s b_{sk}} \\ &\overset{(5.9)}{=} (t'_1)^{\lambda_1 b_{1k}} \cdot \ldots \cdot (t'_s)^{\lambda_s b_{sk}} \\ &\overset{(5.5)}{=} (c^{q_1})^{b_{1k}} \cdot \ldots \cdot (c^{q_s})^{b_k} \\ &= a^{\sum_{j=1}^{s} b_{jk} q_j} \overset{(5.10)}{=} c^{v_k} \overset{(5.11)}{=} c_k, \end{aligned}$$

para $k = 1, \ldots, n$. Portanto, $c \in \Gamma$, como queríamos.

[$\Rightarrow$]: Suponhamos que $\Gamma = V(I_{\mathcal{A}})$. Como $V(I_{\mathcal{A}}, x_i) \subset V(I_{\mathcal{A}})$, para todo $i = \ldots, n$, obtemos facilmente a condição (b). Para provar a condição (a), tome $c = (c_1, \ldots, c_n) \in V(I_{\mathcal{A}})$, com $c_i \neq 0$ para todo i. Por definição de Γ, existem $d_1, \ldots, d_m \in K$ tais que $c_j = d_1^{a_{1j}} \cdot \ldots \cdot d_m^{a_{mj}}$, com $j = 1, \ldots, n$. Pela equação (5.7), obtemos

$$\begin{aligned} c_1^{q_{1i}} \cdot \ldots \cdot a_n^{q_{ni}} &= (d^{a_1})^{q_{1i}} \cdot \ldots \cdot (d^{a_n})^{q_{ni}} \\ &= d^{\sum_{j=1}^{n} q_{ji} a_j} \\ &\overset{(5.7)}{=} d^{\lambda_i f_i} \end{aligned}$$

para $i = 1, \ldots, s$. Logo,

$$c_1^{q_{1i}} \cdot \ldots \cdot c_n^{q_n i} = (d^{f_i})^{\lambda_i}.$$

□

Corolário 5.2.4. *Se K é algebricamente fechado, então $V(I_{\mathcal{A}}) \subset \Gamma \cup V(x_1 \cdot \ldots \cdot x_n)$.*

Demonstração. Seja $c = (c_1, \ldots, c_n) \in V(I_{\mathcal{A}})$. Suponhamos que $c \notin V(x_1 \cdot \ldots \cdot x_n)$. Então, $c_i \neq 0$ para todo i. Como K é algebricamente fechado, segue que para cada $i = 1, \ldots, n$, existem raízes em K para o polinômio da forma $x^{\lambda_i} - c^{q_i}$, com $c^{q_i} = c_1^{q_{1i}} \cdot \ldots \cdot c_n^{q_{ni}} \in K$. A partir daqui podemos proceder como na primeira parte da demonstração do Teorema5.2.3, para concluirmos que $c \in \Gamma$. □

Corolário 5.2.5. *Se K é algebricamente fechado, então $V(I_{\mathcal{A}}) = \Gamma$ se, e somente se, $V(I_{\mathcal{A}}, x_i) \subset \Gamma$ para todo i.*

Demonstração. Se K é algebricamente fechado então a condição (a) do Teorema 5.2.3 é satisfeita e daí segue que $V(I_{\mathcal{A}}) = \Gamma$ se, e somente se, $V(I_{\mathcal{A}}, x_i) \subset \Gamma$ para todo i. □

Observação 5.2.6. *Se nos corolários acima, assumirmos verdadeira a condição (a) do Teorema 5.2.3, em vez de K algebricamente fechado, os corolários continuam válidos.*

Veremos a seguir uma aplicação mais concreta destes resultados.

Proposição 5.2.7. *Seja d um inteiro positivo e*

$$A = \{(a_1, \ldots, a_m) \in \mathbb{N}^m | \, a_1 + \cdots + a_m = d\}.$$

Se K é um corpo algebricamente fechado e $\mathcal{A}$ é a matriz cujas colunas são vetores em A, então o conjunto tórico Γ determinado por $\mathcal{A}$ é uma variedade afim tórica.

Demonstração. Denotando por $A_i = (a_{1i}, \ldots, a_{mi})$, cada vetor em A, definimos o conjunto

$$\mathcal{B} = \left\{t^{A_i} | \, A_i \in A\right\} = \{f_1, \ldots, f_m, f_{m+1}, \ldots, f_s\},$$

sendo

$$s = \begin{pmatrix} d+m-1 \\ m-1 \end{pmatrix}.$$

Seja $\mathcal{A}$ a matriz cujas colunas são os $A_i's \in A$. Pode-se ordenar essas colunas modo que $f_i = t_i^d$ para $i = 1, \ldots, m$ e $\#supp(f_i) \geq 2$ para $i > m$, sendo $supp(t^a) = \{t_i | \, a_i > 0\}$. Dessa maneira, $\phi : K[x_1, \ldots, x_s] \longrightarrow K[t_1, \ldots, t_m]$ é dada da seguinte forma:

$$\phi(x_i) = \begin{cases} t_i^d, & \text{se } i = 1, \ldots, m \\ t_1^{a_{1i}} \cdot \ldots \cdot t_m^{a_{mi}}, & \text{se } i > m \end{cases}$$

O conjunto tórico Γ de $\mathcal{A}$ pode ser escrito como

$$\Gamma = \{(f_1(t_1, \ldots, t_m), \ldots, f_s(t_1, \ldots, t_m)) |\, t_1, \ldots, t_m \in K\}\,. \tag{5.12}$$

Fixe um inteiro $1 \leq i \leq s$. Pelo Corolário 5.2.5 é suficiente provar que

$$V(I_{\mathcal{A}}, x_i) \subset \Gamma, \tag{5.13}$$

sendo $I_{\mathcal{A}}$ o ideal tórico associado a matriz $\mathcal{A}$. Vamos usar indução em m. Se $m = 1$, então $A = \{d\}$, $\mathcal{A} = [d]$, $f = t^d \in K[t]$, com $\phi(x) = t^d$. Assim, dado $a \in V(I_{\mathcal{A}}, x)$ segue que $a = 0$, que obviamente pertence a Γ. Note que se $i > m$, então $x_i^d - x_1^{a_{1i}} \cdot \ldots \cdot x_m^{a_{mi}} \in I_{\mathcal{A}}$. De fato,

$$\begin{aligned} \phi(x_i^d - x_1^{a_{1i}} \cdot \ldots \cdot x_m^{a_{mi}}) =& \phi(x_i)^d - \phi(x_1)^{a_{1i}} \cdot \ldots \cdot \phi(x_m)^{a_{mi}} \\ =& (f_i)^d - (t_1^d)^{a_{1i}} \cdot \ldots \cdot (t_m^d)^{a_{mi}} \\ =& (f_i)^d - (t_1^{a_{1i}} \cdot \ldots \cdot t_m^{a_{mi}})^d = 0. \end{aligned} \tag{5.14}$$

Consequentemente, tomando $c = (c_1, \ldots, c_s) \in V(I_{\mathcal{A}}, x_i)$, então $c_i = 0$ e ainda,

$$c_i^d - (c_1^{a_{1i}} \cdot \ldots \cdot c_m^{a_{mi}}) = 0 \Rightarrow c_1^{a_{1i}} \cdot \ldots \cdot c_m^{a_{mi}} = 0,$$

ou seja, $c_j = 0$ para algum $1 \leq j \leq m$. Podemos então assumir que $1 \leq i \leq m$. Por simplicidade de notação, vamos considerar $i = 1$, ou seja, $c \in V(I_{\mathcal{A}}, x_1)$ e assim $c = (0, c_2, \ldots, c_n)$. Observe que para cada $f_j = t_1^{a_{1j}} \cdot \ldots \cdot t_m^{a_{mj}}$, com $a_{1j} > 0$, tem-se $c_j = 0$. De fato, já vimos que $x_j^d - x_1^{a_{1j}} \cdot \ldots \cdot x_m^{a_{mj}} \in I_{\mathcal{A}}$, como $c \in V(I_{\mathcal{A}}, x_1)$, segue que

$$c_j^d - 0^{a_{1j}} c_2^{a_{2j}} \cdot \ldots \cdot c_m^{a_{mj}} = 0 \Rightarrow c_j = 0.$$

Suponhamos por indução que para toda matriz com $m-1$ linhas, tal que a soma das entradas das colunas seja igual a d, (5.13) seja verdadeira. Removendo de $\mathcal{A}$, a primeira linha e todas as colunas A_j tais que $a_{1j} > 0$, obtemos uma submatriz de $\mathcal{A}$, que chamaremos de $\mathcal{A}'$. Dessa forma, $\mathcal{A}'$ tem $m-1$ linhas e a soma das entradas de suas colunas continua sendo igual a d. Por hipótese de indução, segue que $\Gamma' = V(I'_{\mathcal{A}})$, sendo Γ' e $I'_{\mathcal{A}}$, respectivamente, o conjunto tórico e o ideal tórico de $\mathcal{A}'$. O homomorfismo ϕ' correspondente a $\mathcal{A}'$ é a restrição do homomorfismo ϕ a $K[x_i |\, a_{1i} = 0]$. Assim, podemos ver que

$$I'_{\mathcal{A}} \subset I_{\mathcal{A}}. \tag{5.15}$$

Logo,

$$V(I_{\mathcal{A}}) \subset V(I'_{\mathcal{A}}). \tag{5.16}$$

O conjunto tórico Γ', pode ser visto como um "subconjunto" de Γ. Podemos escrevê-lo como

$$\Gamma' = \{(f_i(0, t_2, \ldots, t_m) |\, a_{1i} = 0) | t_2, \ldots, t_m \in K\}\,. \tag{5.17}$$

Da forma como Γ' foi descrito em (5.17), podemos enxergar cada ponto b de Γ' como um ponto de Γ, completando b colocando zero nas j-ésimas entradas, tal que $a_{1i} > 0$. Consideremos

então o vetor $c' = (c_i | \, a_{1i} = 0)$. Segue de (5.16) que $c' \in V(I'_{\mathcal{A}})$. Agora, pelo Corolário 5.2.4, temos que

$$V(I'_{\mathcal{A}}) \subset \Gamma' \cup V(x_{i_1} \cdot \ldots \cdot x_{i_{s'}}),$$

com i_j tal que $a_{1i_j} = 0$. Assim,

I. $c' \in \Gamma'$

ou

II. $c' \in V(x_{i_1} \cdot \ldots \cdot x_{i_{s'}})$, o que implica

$$c' \in V(I'_{\mathcal{A}}) \cap V(x_{i_j}) = V(I'_{\mathcal{A}}, x_{i_j}), \qquad \text{para algum } 1 \leq j \leq s.'$$

Por hipótese de indução $c' \in \Gamma'$. Nos dois casos temos $c' \in \Gamma'$. Enxergando c' como um ponto em Γ, temos exatamente o ponto c. Portanto $c \in \Gamma$.

□

Vejamos um exemplo para ilustrar a demonstração da Proposição 5.2.7.

Exemplo 5.2.8. *Considere a matriz*

$$\mathcal{A} = \begin{bmatrix} 2 & 0 & 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 1 & 0 & 1 \end{bmatrix}.$$

sobre o corpo $K = \mathbb{C}$. *Então,* $f_1 = t_1^2, f_2 = t_2^2, f_3 = t_3^2, f_4 = t_2t_3, f_5 = t_1t_2, f_6 = t_1t_3$ *e*

$$\Gamma = \left\{ (t_1^2, t_2^2, t_3^2, t_2t_3, t_1t_2, t_1t_3) | \, t_1, t_2, t_3 \in K \right\}.$$

Tomando $c = (c_1, \ldots, c_6) \in V(I_{\mathcal{A}}, x_1)$, *temos que* $c = (0, c_2, c_3, c_4, 0, 0)$. *Assim,*

$$\mathcal{A}' = \begin{bmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \end{bmatrix} \text{ e } \Gamma' = \left\{ (t_2^2, t_3, t_2t_3) | \, t_2, t_3 \in K \right\}.$$

Supomos que $V(I'_{\mathcal{A}}) = \Gamma'$. *Veja que se* $b = (t_2^2, t_3, t_2t_3) \in \Gamma'$, *então* $\overline{b} = (0, t_2^2, t_3, t_2t_3, 0, 0) \in \Gamma$, $(t_1 = 0)$. *Temos que* $c' = (c_2, c_3, c_4) \in V(I'_{\mathcal{A}})$ *e completando-o, obtemos* $(0, c_2, c_3, c_4, 0, 0) = c$. *Logo,* $c \in \Gamma$.

A seguir, apresentamos outra consequência do Teorema 5.2.3, que pode ser usada para provar que as curvas monomiais sobre corpos arbitrários são variedades afins tóricas.

Corolário 5.2.9. *Se as colunas de* $\mathcal{A}$ *geram* $\mathbb{Z}^m$ *como* $\mathbb{Z}-$*módulo, então* $\Gamma = V(I_{\mathcal{A}})$ *se, e somente se,* $V(I_{\mathcal{A}}, x_i) \subset \Gamma$ *para todo* i.

Demonstração. Sabemos que $\mathcal{A}$ determina um homomorfismo entre $\mathbb{Z}^n$ e $\mathbb{Z}^m$. Como as colunas de $\mathcal{A}$ geram $\mathbb{Z}^m$, temos que esse homomorfismo é sobrejetor. Pelo Corolário 3.2.3 podemos obter

uma base β de $\mathbb{Z}^n$ e uma base β' de $\mathbb{Z}^m$ tais que a matriz que representa este homomorfismo é da forma

$$\mathcal{M} = \begin{bmatrix} \lambda_1 & & & & \vdots & & & \\ & \lambda_2 & & & \vdots & & & \\ & & \ddots & & & & 0 & \\ & & & \lambda_r & \vdots & & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & \vdots & & & \\ & 0 & & & \vdots & & 0 & \\ & & & & \vdots & & & \end{bmatrix}$$

com $0 \leq r \leq min\{m, n\}, \lambda_1, \lambda_2, \ldots, \lambda_r$ pertencentes a $\mathbb{Z}\backslash\{0\}$ e λ_j dividindo λ_{j+1}, para cada $j = 1, 2, \ldots, r-1$. Observe que as colunas da matriz $\mathcal{M}$ formam um conjunto $\mathbb{Z}-$linearmente independente e continuam gerando $\mathbb{Z}^m$. Logo, as colunas de $\mathcal{M}$ formam uma base para $\mathbb{Z}^m$. Pela Proposição 3.1.3 segue que $m = r$. Assim,

$$\mathcal{M} = \begin{bmatrix} \lambda_1 & & & \vdots & \\ & \lambda_2 & & \vdots & \\ & & \ddots & & 0 \\ & & & \lambda_m & \vdots \end{bmatrix}$$

Com $\lambda_i \in \mathbb{Z}\backslash\{0\}$ e $\lambda_i | \lambda_{i+1}$, para $i = 1, \ldots, m-1$. Vejamos que $\lambda_i = 1$, para todo i. Como $\mathcal{M}$ determina o mesmo homomorfismo que $\mathcal{A}$, segue que dado $e_i \in \mathbb{Z}^m$, existe $x = (x_1, \ldots, x_m) \in \mathbb{Z}^n$ tal que $\mathcal{M}x = e_i$. Isso implica que $\lambda_1 x_1 = \ldots = \lambda_{i-1}x_{i-1} = \lambda_{i+1}x_{i+1} = \ldots = \lambda_m x_m = 0$ e $\lambda_i x_i = 1$. Assim, x_i é o inverso multiplicativo de λ_i e como as únicas unidades em $\mathbb{Z}$ são 1 ou -1 e $\lambda_i > 0$, concluímos que $\lambda_i = 1$ para todo i. Temos assim a condição (a) do Teorema 5.2.3 satisfeita. Portanto $\Gamma = V(I_{\mathcal{A}})$ se, e somente se, a condição (b) acontece. □

Um conjunto tórico Γ no espaço afim $\mathbb{A}^n_K$ é chamado **curva monomial**, se a matriz $\mathcal{A}$ correspondente a Γ, tem apenas uma linha, ou seja, $\mathcal{A} = [a_1 \ldots a_n]$ e $a_1, \ldots, a_n$ são inteiros positivos relativamente primos [13].

Proposição 5.2.10. *Seja K um corpo arbitrário e Γ uma curva monomial. Então $\Gamma = V(I_{\mathcal{A}})$.*

Demonstração. Como $a_1, \ldots, a_n$ são primos entre si, segue que $\mathbb{Z} = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n$ e pelo Corolário 5.2.9 é suficiente mostrar que $V(I_{\mathcal{A}}, x_i) \subset \Gamma$, para todo i. Assim, seja $c \in V(I_{\mathcal{A}}, x_i)$. Note que todo binômio da forma $x_i^{a_j} - x_j^{a_i} \in I_{\mathcal{A}}$ e consequentemente se anulam em c. Isso implica que $c = 0$ e portanto pertence a Γ. Logo, $V(I_{\mathcal{A}}, x_i) \subset \Gamma$. □

Proposição 5.2.11. *Se K é um corpo algebricamente fechado, e $\mathcal{A} = [a_1 \ldots a_n]$, com*

$$mdc(a_1, \ldots, a_n) = d.$$

Então, $\Gamma = V(I_{\mathcal{A}})$.

Demonstração. Como o corpo K é algebricamente fechado, pelo Corolário 5.2.5 basta provarmos que $V(I_{\mathcal{A}}, x_i) \subset \Gamma$, para todo i. Observe que os binômios da forma $x_i^{a_j} - x_j^{a_i}$ estão em $I_{\mathcal{A}}$. Isto independe do fato de $a_1, \ldots, a_n$ não serem primos. Podemos então concluir a demonstração da mesma forma que foi feito na Proposição 5.2.10.

□

Proposição 5.2.12. *Se K é um corpo infinito e $\Gamma = V(I)$ para algum ideal $I \subset K[x_1, \ldots, x_n]$, então $\Gamma = V(I_{\mathcal{A}})$.*

Demonstração. Pela Proposição 5.1.3, temos que $\mathbf{I}(\Gamma) = I_{\mathcal{A}}$ e $V(\mathbf{I}(\Gamma)) = V(I_{\mathcal{A}})$. Como Γ é uma variedade, segue que $\Gamma = V(I_{\mathcal{A}})$. □

Em vista da Proposição 5.2.12 poderíamos nos perguntar se Γ pode ser uma variedade, mas não uma variedade afim tórica. Para mostrar que isso é possível, temos o seguinte exemplo:

Exemplo 5.2.13. *Seja $K = \mathbb{Z}_3$ e $\mathcal{A} = (2, 4)$. Então,*

$$\Gamma = \{(0,0),(1,1)\} = V(x_1 - x_2, x_2^2 - x_2) \quad , \quad P = \langle x_2 - x_1^2 \rangle.$$

É fácil verificar que neste caso $D = (2, 0)$, $Q = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$, ou seja, $\lambda_1 = 2$. Note que $(2, 1) \in V(P)$, logo $V(P) \neq \Gamma$. Pensando no exemplo em termos do Teorema 5.2.3, observe que não existe $a \in \mathbb{Z}_3$ tal que $a^2 = 2^1.1^0 = 2$, isto é, a condição (a) do Teorema 5.2.3 não é satisfeita.

Variedade afins tóricas são completamente parametrizadas por monômios quando K é algebricamente fechado ou quando a variedade é normal (ver [6] e [7]).

REFERÊNCIAS BIBLIOGRÁFICAS

[1] COX, D.; LITTLE, J.; SCHENCK, H. *Toric varieties*. Graduate studies in mathematics. American Mathematical Society, 2011.

[2] DEMAZURE, M. Sous-groupes algébriques de rang maximum du groupe de cremona. *Annales scientifiques de l'École Normale Supérieure*, v. 3, série 4, n. 4, p. 507–588, 1970. https://doi.org/10.24033/asens.1201.

[3] DANILOV, V. I. The geometry of toric varieties. *Russian Mathematical Surveys*, London, v. 33, n. 2, p. 97, 1978. https://doi.org/10.1070/RM1978v033n02ABEH002305.

[4] FULTON, W. *Introduction to toric varieties*. Number 131. Princeton University Press, 1993.

[5] REYES, E.; VILLARREAL, R. H.; ZáRATE, L. A note on affine toric varieties. *Linear Algebra and its Applications*, v. 318, n. 1, p. 173 – 179, oct. 2000. https://doi.org/10.1016/S0024-3795(00)00166-X.

[6] KATSABEKIS, A.; THOMA, A. Toric sets and orbits on toric varieties. *Journal of Pure and Applied Algebra*, v. 181, n. 1, p. 75 – 83, 2003. https://doi.org/10.1016/S0022-4049(02)00305-5.

[7] KATSABEKIS, A.; THOMA, A. Parametrizations of toric varieties over any field. *Journal of Algebra*, v. 308, n. 2, p. 751 – 763, 2007. https://doi.org/10.1016/j.jalgebra.2006.08.016.

[8] COX, D.; LITTLE, J.; O'SHEA, D. *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra*. 4. ed. Springer International Publishing, 2015. https://doi.org/10.1007/978-3-319-16721-3.

[9] GARCIA, A.; LEQUAIN, Y. *Elementos de álgebra*. 5. ed. Rio de Janeiro: IMPA, 2008.

[10] STURMFELS, B. *Gröbner bases and convex polytopes*. American Mathematical Soc., 1996.

[11] HUNGERFORD, T. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2003. https://doi.org/10.1007/978-1-4612-6101-8.

[12] VILLARREAL, R. *Monomial algebras*. Chapman & Hall/CRC Monographs and Research Notes in Mathematics. CRC Press, 2015.

[13] ELIAHOU, S. Idéaux de définition des courbes monomiales. In: Greco, S.; Strano, R. *Complete Intersections:* Lectures Given at the 1st 1983 Session of the Centro Internationale Matematico Estivo (C.I.M.E.) Held at Acireale (Catania), Italy, June 13-21, 1983. Heidelberg: Springer, 1984. p. 229–240.