Semigrupos Numéricos e Curvas, em $A^3(k)$, Parametrizadas por Monômios numa Única Variável

Elisângela de Campos

Orientador: Paulo Roberto Brumatti

Dissertação apresentada no Instituto de Matemática, Estátistica e Computação Científica, UNICAMP; como requisito parcial para a obtenção do Título de Mestre em Matemática.

Campinas
1998

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Campos, Elisângela de

C157s Semigrupos numéricos e curvas, em $A^2(k)$, parametrizadas por monômios numa única variável / Elisângela de Campos -- Campinas, [S.P. :s.n.], 1998.

Orientador : Paulo Roberto Brumatti

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Semigrupos. 2. Geometria algébrica. I. Brumatti, Paulo Roberto. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Semigrupos numéricos e curvas, em $A^3(k)$, parametrizadas por monômios numa única variável

Este exemplar corresponde a redação final da dissertação devidamente corrigida e defendida pela Srta. Elisângela de Campos e aprovada pela comissão julgadora.

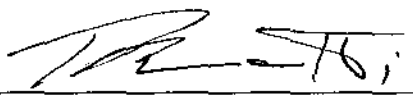
Campinas, 18 de fevereiro de 1998.

Prof.Dr. Paulo Roberto Brumatti
Orientador

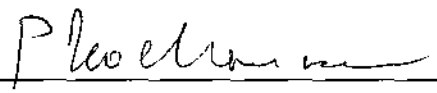
Dissertação apresentada no Instituto de Matemática, Estátistica e Computação Científica, UNICAMP; como requisito parcial para a obtenção do Título de Mestre em Matemática.

Dissertação de Mestrado defendida e aprovada em 18 de fevereiro de 1998

pela Banca Examinadora composta pelos Profs. Drs.



Prof (a). Dr (a). PAULO ROBERTO BRUMATTI



Prof (a). Dr (a). PLAMEN EMILOV KOCHLOUKOV

Prof (a). Dr (a). FERNANDO EDUARDO TORRES ORIHUELA

"Valeu a pena? Tudo vale a pena
se a alma não é pequena.
Quem quer passar além do Bojador
tem que passar além da dor..."

Fernando Pessoa

Dedico esta dissertação aos meus pais

Sebastião e Hélia,

pela vida.

Agradecimentos

Gostaria de agradecer:

- *à minha família: Hélia, Sebastião, Ana Eliza, Sandro e Irene, pelo amor e o apoio em todos os momentos.*
- *ao meu orientador Paulo Roberto Brumatti, pela motivação e paciência nas minhas falhas.*
- *à Érika Maria Chioca Lopes, pela amizade, companherismo e pelas conversas esclarecedoras desde a graduação.*
- *à Luciane e Gabriel Marostegan, pela amizade e por terem sido minha família, neste último ano.*
- *ao Daniel Pellegrino e à Ximena Mujica, pela amizade incondicional, nestes dois anos, e pelos embalos de...*
- *à Marilaine, Marcela, Luciana, Cláudia, Marcinha, Carla, Alvino, Victor, Sinval, Cláudio, Ryuichi, Júnior, Diogo, Marcelo, João, Sérgio e a todos os amigos, pelos momentos de descontração.*
- *à Kátia, Sérgio, Vaston, Ângela, Carla e Andrea, pela velha amizade e pelo apoio, mesmo à distância.*
- *à Marlene A. Chioca Lopes, pela correção da redação do texto.*
- *a todos os professores e funcionários do IMECC.*

e dizer que o apoio e a amizade, de todos vocês, foram muito importantes para que eu pudesse terminar mais esta etapa. Obrigada.

Índice

Introdução

Por uma variedade algébrica $V \subset A^n(L)$ entende-se o conjunto solução de um sistema de polinômios $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$, onde $A^n(L)$ é o espaço afim n-dimensional sobre o corpo L, e K é um subcorpo de L. Dizemos que uma variedade é uma interseção completa, se o seu ideal no anel $K[X_1, \ldots, X_n]$, dado por

$$I(V) = \{f \in K[X_1, \ldots, X_n] \mid f(x) = 0, \forall x \in V\}$$

for gerado por $n - dimV$ polinômios.

Saber que uma variedade V é interseção completa nos permite, entre outras coisas, determinar tal variedade geometricamente, mesmo que aliado a outras teorias, como a de singularidade. Tal é o caso do resultado encontrado em [5, Proposição 1.12, pag. 169], que diz que uma variedade não singular $V \subset A^n(L)$ de dimensão d é uma interseção completa se, e só se, V é a interseção de $n - d$ hipersuperfícies $H_1, \ldots, H_{n-d}$ que satisfazem: para todo $x \in V$ e para todo i, x é ponto regular de H_i e mais ainda, os hiperplanos tangentes $T_x(H_i)$ são linearmente independentes.

Este texto é baseado essencialmente no trabalho de J. Herzog [4], e nele estamos interessados em descrever condições para determinar se certo tipo de variedade, em $A^3(k)$, é ou não interseção completa. Assim, apresentaremos um critério para determinar quando curvas parametrizadas pelas equações

$$X_1 = t^{n_1} \quad X_2 = t^{n_2} \quad X_3 = t^{n_3}$$

onde k é um corpo algebricamente fechado e $(n_1, n_2, n_3) = 1$, são ou não interseção completa. Esse critério está ligado ao fato de o semigrupo gerado por n_1, n_2, n_3 ser ou não simétrico.

Para chegarmos a esse critério, introduziremos, no capítulo 1, alguns conceitos e resultados sobre Teoria de Grupos, como a definição de posto de um grupo abeliano finitamente gerado, e sobre Álgebra Comutativa, como a definição de variedades algébricas, o lema de Nakayama, o teorema da normalização de Noether, além da definição de interseção completa para ideais e variedades. No final do capítulo, daremos exemplos de curvas, em $A^3(k)$, parametrizadas do tipo descrito acima, que são e que não são interseções completas, que só serão justificados com o desenvolvimento do texto.

No capítulo 2, desenvolveremos a teoria de semigrupos, começando com a definição formal de semigrupo e algumas propriedades dessa estrutura, de acordo com [7]. Depois,

seguindo os passos de [4], daremos as definições de relação de definição de semigrupos e de anel de semigrupo. A partir de algumas propriedades referentes a essas relações, faremos uma demostração para o fato de que todo semigrupo comutativo finitamente gerado é finitamente apresentado, ou seja, é o quociente de um semigrupo livre por uma congruência finitamente gerada. Mostraremos também que o número mínimo de elementos que geram a relação definidora de um semigrupo é maior ou igual ao posto do semigrupo, menos o posto do seu grupo associado. Se a igualdade ocorre, diremos que o semigrupo é uma interseção completa. Daremos ainda, a definição e uma caracterização de semigrupo simétrico. Por fim, faremos a equivalência entre semigrupos que são interseções completas e variedades associadas a esses semigrupos. E teremos condições para justificar um dos exemplos feitos no capítulo 1.

No terceiro capítulo, estudaremos as propriedades de semigrupos dos naturais gerados por três elementos, para mostrarmos a equivalência entre semigrupos que são interseções completas e semigrupos simétricos. Aplicando esse resultado à geometria algébrica, deduziremos que uma curva, como a descrita acima, é uma interseção completa se, e somente se, o semigrupo gerado por n_1, n_2, n_3 for simétrico. Esse é o critério de que precisávamos para justificar os exemplos dados no final do primeiro capítulo.

Capítulo 1

Alguns Resultados Gerais

Este capítulo traz alguns conceitos e resultados de Teoria de Grupos e Álgebra Comutativa que serão úteis para o desenvolvimento do texto, tais como: posto de um grupo abeliano finitamente gerado, variedades algébricas, lema de Nakayama, teorema da normalização de Noether e a definição de interseção completa para ideais e variedades.

1.1 Grupos Abelianos Finitamente Gerados

No capítulo 2, vamos precisar da teoria de grupos para definirmos o grupo associado a um semigrupo S. Também será necessária a definição de posto de um grupo abeliano finitamente gerado. Para isso, vamos considerar a seguinte definição:

Definição 1.1.1 *Um grupo abeliano G é chamado grupo abeliano livre finitamente gerado, se uma das seguintes propriedades equivalentes é satisfeita:*

i) *G admite uma $\mathbb{Z}$ base finita, isto é, existem $g_1, g_2, \ldots, g_n \in G$ tais que, para cada $g \in G$, g se escreve de maneira única na forma $g = z_1g_1 + z_2g_2 + \cdots + z_ng_n$, com $z_1, \ldots, z_n \in \mathbb{Z}$.*

ii) *G admite um sistema finito de geradores linearmente independentes sobre $\mathbb{Z}$, isto é, existem $g_1, \ldots, g_n \in G$ tais que $G =< g_1, \ldots, g_n >$ e tais que se $z_1g_1 + z_2g_2 + \cdots + z_ng_n = 0$ com $z_1, \ldots, z_n \in \mathbb{Z}$, então $z_1 = \cdots = z_n = 0$.*

iii) *G é isomorfo ao produto direto de um número finito de cópias de $\mathbb{Z}$, isto é, $G \cong \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$.*

Como exemplos de grupos abelianos livres podemos citar: $\mathbb{Z}$, que tem $\{1\}$ como base; $2\mathbb{Z}$, que tem $\{2\}$ como base e $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, isto é, n cópias de $\mathbb{Z}$, que tem $\{(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,0,\ldots,1)\}$ como base.

Pode ser visto com maiores detalhes em [3] que, para um grupo abeliano livre finitamente gerado, todas as bases possuem o mesmo número de elementos.

Definição 1.1.2 *À cardinalidade comum de uma base de um grupo abeliano livre finitamente gerado, damos o nome de posto de G, que denotamos por posto G.*

Um resultado clássico da teoria de grupos sobre grupos abelianos livres finitamente gerados é dado a seguir.

Teorema 1.1.3 *: Seja G um grupo abeliano livre de posto $n > 0$ e seja H um subgrupo de G. Então:*

a) *H é um grupo livre de posto $m \leq n$.*

b) *Existe uma base $\{u_1, \ldots, u_n\}$ de G e existem inteiros positivos $c_1, \ldots, c_m \in \mathbb{N}$ tais que c_i divide c_{i+1} para todo $i = 1, \ldots, m-1$, de modo que $\{c_1u_1, \ldots, c_mu_m\}$ é uma base de H.*

Dem. : Veja [3] □

Um grupo abeliano G é finitamente gerado se ele admite um sistema finito de geradores, isto é, se $G =< g_1, \ldots, g_n >$, para alguns $g_1, \ldots, g_n \in G$. Um grupo dessa forma é imagem homomórfica de um grupo L abeliano livre finitamente gerado. Para a demonstração dessa afirmação, veja [3]. Como conseqüência disso e do teorema anterior, tem-se:

Corolário 1.1.4 *: Se $(G, +)$ é um grupo abeliano finitamente gerado e não trivial, então $G = H_1 \oplus \cdots \oplus H_r \oplus K$, onde $H_1, \ldots, H_r$ são subgrupos cíclicos, com $c_i = |H_i| > 1$, $c_i | c_{i+1}$, para $i = 1, \ldots, r+1$ e K é um subgrupo livre finitamente gerado de posto k.*

Tal resultado nos leva à seguinte definição:

Definição 1.1.5 *: Para um grupo G abeliano e finitamente gerado definimos o posto G := posto K, onde K é dado pelo resultado anterior, ou seja, é definido como o posto da parte livre de G.*

1.2 Ideal Homogêneo

Neste texto, sempre que falarmos em anel, estaremos referindo-nos a anel comutativo com identidade.

Usaremos também, nos capítulos seguintes, o conceito de ideal homogêneo e o seguinte resultado: o núcleo de um homomorfismo homogêneo é homogêneo. Mais detalhes do que será apresentado nesta seção pode ser visto em [2].

Definição 1.2.1 :

a) *Um anel graduado é um anel R junto com uma decomposição primária $R = \oplus_{i\in\mathbb{Z}} R_i$, como um $\mathbb{Z}$-módulo, tal que $R_iR_j \subset R_{i+j}$ para todo $i,\ j \in \mathbb{Z}$.*

b) *Dado um anel graduado R, um R-módulo graduado é um R-módulo M junto com uma decomposição $M = \oplus_{i\in\mathbb{Z}} M_i$, como um $\mathbb{Z}$-módulo, tal que $R_iM_j \subset M_{i+j}$, para todo $i,\ j \in \mathbb{Z}$.*

Os elementos $x \in M_i$ são chamados homogêneos de grau i; os de R_i são também chamados i-formas. De acordo com essa definição, o elemento zero é homogêneo de grau arbitrário. O grau de $x \in M_i$ é denotado por $deg\, x$. Um elemento arbitrário $x \in M$ tem uma única apresentação, $x = \sum_i x_i$, como uma soma de elementos homogêneos $x_i \in M_i$. Os elementos x_i são chamados componentes homogêneas de x.

Note que R_0 é um anel com $1 \in R_0$, que todos os somandos M_i são R_0-módulos ($R_0M_i \subset M_i$) e que $M = \oplus_{i\in\mathbb{Z}} M_i$ é uma soma direta de M como um R_0-módulo.

Definição 1.2.2 : *Seja $\phi : M \longrightarrow N$ um homomorfismo de R-módulos graduados, dizemos que ϕ é um homomorfismo homogêneo se $\phi(M_i) \subset N_i$, para todo $i \in \mathbb{Z}$.*

Sejam M um R-módulo graduado e L um submódulo de M. L é chamado um *submódulo graduado* se L é um módulo graduado e se a inclusão é um homomorfismo homogêneo. Em outras palavras, L é um submódulo graduado de M se, e somente se, L é gerado pelos elementos homogêneos de M que estão em L. Em particular, se $x \in L$, então toda compenente homogênea de x está em L.

Definição 1.2.3 : *Um ideal I de R é chamado ideal homogêneo, se dado $x \in I$ suas componentes homogêneas estão em I, isto é, se como um R-módulo, I é um submódulo graduado.*

Proposição 1.2.4 : *Se ϕ é um homomorfismo homogêneo, então $Ker(\phi)$ e $Im(\phi)$ são graduados.*

Dem. : Seja $\phi : M \longrightarrow N$ um homomorfismo homogêneo de R-módulos graduados. Do fato de ϕ ser homogêneo, vemos que

$$Ker(\phi) = \oplus_{i\in\mathbb{Z}} Ker\,\phi \cap M_i = \oplus_{i\in\mathbb{Z}} K_i$$

e portanto

$$R_i(Ker(\phi) \cap M_j) \subseteq M_{i+j}$$

pois $R_iM_j \subset M_{i+j}$.

Além disso, a inclusão de $Ker(\phi)$ em M é um homomorfismo homogêneo, pois $(Ker(\phi) \cap M_i) \subset M_i$, para todo $i \in \mathbb{Z}$. Portanto, $Ker(\phi)$ é graduado. Analogamente, tem-se que $Im(\phi)$ é graduado. □

Portanto, pela proposição acima e pela definição de ideal homogêneo, temos que o núcleo de um homomorfismo homogêneo é homogêneo.

1.3 Variedades Algébricas

Sejam $A^n(L)$ um espaço afim n-dimensional sobre um corpo L e $K \subset L$ um subcorpo.

Definição 1.3.1 : *Um subconjunto $V \subset A^n(L)$ é chamado uma K-variedade algébrica afim, se existem polinômios $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$, tal que V é o conjunto solução do sistema de equações*

$$f_i(X_1, \ldots, X_n) = 0, \quad para\ i = 1, \ldots, m \quad (1)$$

em $A^n(L)$. (1) é chamado sistema de definição de V, K o corpo de definição de V, e L o corpo de coordenadas.

Uma K-variedade V é também uma K'-variedade para qualquer subcorpo $K' \subset L$ que contém todos os coeficientes de um sistema de equações de definição de V (ou $K \subset K'$). O conceito de K-variedade é invariante sob transformações de coordenadas afins

$$X_i = \sum_{k=1}^{n} a_{ik} Y_k + b_i, \ para\ i = 1, \ldots, n$$

se os coeficientes a_{ik} e b_i estão todos em K.

Como um exemplo de K-variedade, temos a K-hipersuperfície, que é definida por apenas uma equação $f(X_1, \ldots, X_n) = 0$, onde $f \in K[X_1, \ldots, X_n]$ é um polinômio não constante. Para $n = 3$, as hipersuperfícies são chamadas simplesmente de superfícies.

Definição 1.3.2 : *Para um subconjunto $V \in A^n(L)$, o conjunto*

$$I(V) := \{F \in K[X_1, \ldots, X_n] \mid F(x) = 0, \ \forall x \in V\}$$

é chamado o ideal de V em $K[X_1, \ldots, X_n]$ e o conjunto

$$Z(I) := \{x \in A^n(L) \mid F(x) = 0, \ \forall F \in I\},$$

onde I é um ideal de $K[X_1, \ldots, X_n]$, é chamado conjunto de zeros de I (ou variedade de I).

Para as operações $I(V)$ e $Z(I)$, as regras abaixo ocorrem e podem ser facilmente mostradas.

Observação 1.3.3 :Regras:

a) $I(A^n(L)) = (0)$, se L é infinito e $I(\emptyset) = (1)$.

b) Para qualquer conjunto $V \in A^n(L)$, temos $I(V) = \sqrt{I(V)}$.

c) Para qualquer variedade $V \in A^n(L)$, temos $Z(I(V)) = V$.

d) Para duas variedades V_1 e V_2, temos que $V_1 \subset V_2$ se, e somente se, $I(V_1) \supset I(V_2)$.

e) Para duas variedades V_1 e V_2, temos:

$$I(V_1 \cup V_2) = I(V_1) \cap I(V_2) \text{ e } V_1 \cup V_2 = Z(I(V_1)I(V_2)).$$

f) Para uma família $\{V_\lambda\}_{\lambda \in \Lambda}$ de variedades V_λ,

$$\bigcap_{\lambda \in \Lambda} V_\lambda = Z(\sum_{\lambda \in \Lambda} I(V_\lambda)).$$

Dem. : : Ver [5].

Definição 1.3.4 : *Uma K-variedade V é chamada irredutível, se $V = V_1 \cup V_2$ com K-variedades V_1, V_2, então $V = V_1$ ou $V = V_2$.*

A proposição abaixo nos dá um critério de irredutibilidade para K-variedades.

Proposição 1.3.5 : *Uma K-variedade $V \subset A^n(L)$ é irredutível se, e somente se, o seu ideal $I(V)$ é primo.*

Dem. : Sejam V uma K-variedade irredutível e f_1, $f_2 \in K[X_1, \ldots, X_n]$ polinômios com $f_1 f_2 \in I(V)$. Para $H_i := Z(f_i)$, para $i = 1, 2$, nós temos que $V = (V \cap H_1) \cup (V \cap H_2)$. De fato, é claro que $(V \cap H_1) \cup (V \cap H_2) \subset V$.

Reciprocamente, seja $x \in V$, então $(f_1 f_2)(x) = 0$, isto é, $f_1(x) = 0$ ou $f_2(x) = 0$. Logo $x \in H_1$ ou $x \in H_2$ e portanto $x \in (V \cap H_1) \cup (V \cap H_2)$. Então $V = V \cap H_1$ ou $V = V \cap H_2$, pois V é irredutível. De $V \subset H_1$ ou $V \subset H_2$ segue que $f_1 \in I(V)$ ou $f_2 \in I(V)$, ou seja, $I(V)$ é primo.

Agora, seja $I(V)$ primo. Suponhamos que existam K-variedades V_1, V_2 com $V = V_1 \cup V_2$, $V \neq V_i (i = 1, 2)$. Por 1.3.3 nós temos $I(V) = I(V_1) \cap I(V_2)$ e $I(V) \neq I(V_i)$ $(i = 1, 2)$. Então existem polinômios $f_i \in I(V_i)$, $f_i \notin I(V)$ para $i = 1, 2$, mas como $f_1 f_2 \in I(V_1) \cap I(V_2) = I(V_1 \cup V_2)$, temos uma contradição. □

Definição 1.3.6 : *Um anel R é chamado Noetheriano se qualquer ideal de R for finitamente gerado.*

Como exemplos de anéis Noetherianos, temos os domínios de ideais principais, em particular os corpos (com os quais trabalharemos neste texto), bem como $\mathbb{Z}$ e $k[X]$, se k for um corpo. Qualquer imagem por homomorfismo de anel Noetheriano é Noetheriano.

Uma caracterização elementar da definição de anel Noetheriano é dada por:

Proposição 1.3.7 : *Seja R um anel. Então as seguintes condições são equivalentes:*

1. *R é Noetheriano.*
2. *Qualquer cadeia ascendente de ideais de R*

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

torna-se estacionária.

3. *Qualquer família não vazia de ideais de R contém um elemento maximal.*

Dem. : A demonstração dessa equivalência pode ser vista em [5]. □

Um resultado clássico da Álgebra Comutativa, conhecido por teorema das Bases de Hilbert, é dado pela proposição abaixo.

Proposição 1.3.8 : *Se R é um anel Noetheriano, então $R[X]$ também é.*

Dem. : Ver [5] □

Uma conseqüência da proposição acima, usada indutivamente, é que se R é Noetheriano, então $R[X_1, \ldots, X_n]$ também é. Outras conseqüências de 1.3.8 são dadas pelos corolários abaixo.

Corolário 1.3.9 : *Toda cadeia decrescente*

$$V_1 \supset V_2 \supset \cdots \supset V_n \supset \cdots$$

de K-variedades afins $V_i \subset A^n(L)$ é estacionária.

Dem. : Por 1.3.3 temos a seguinte cadeia crescente

$$I(V_1) \subset I(V_2) \subset \cdots \subset I(V_i) \subset \cdots$$

onde $I(V_i) \subset K[X_1, \ldots, X_n]$ que é estacionária pela caracterização de anel Noetheriano feita acima. Logo, usando novamente 1.3.3, concluímos que

$$V_1 \supset V_2 \supset \cdots \supset V_n \supset \cdots$$

é estacionária. □

Corolário 1.3.10 : *Para um ideal I de $R[X_1, \ldots, X_n]$, $Z(I)$ é uma K-variedade em $A^n(L)$.*

Dem. : Como $R[X_1, \ldots, X_n]$ é Noetheriano, temos $I = (f_1, \ldots, f_n)$, então $Z(I)$ é o conjunto solução do sistema de equações $f_i = 0$ para $i = 1, \ldots, m$ em $A^n(L)$. Portanto, $Z(I)$ é uma K-variedade. □

Para um ideal $I \subset R[X_1, \ldots, X_n]$ sobre um corpo K e uma extensão L de K, o conjunto de zeros $Z(I) \subset A^n(L)$ pode ser vazio. Entretanto, faremos um teorema que é fundamental para a geometria algébrica, pois garante a existência de variedades.

Teorema 1.3.11 *(Teorema dos Zeros de Hilbert): Se L é algebricamente fechado e $I \neq R[X_1, \ldots, X_n]$, então $Z(I)$ é não-vazio.*

Dem. : Ver [5]. □

Como uma conseqüência do teorema dos Zeros de Hilbert, temos o seguinte resultado: (Sua demonstração pode ser encontrada em [5].)

Proposição 1.3.12 : *Seja L/K uma extensão de corpos, onde L é algebricamente fechado. A aplicação dada por $V \longmapsto I(V)$ define uma bijeção do conjunto de todas as K-variedades $V \subset A^n(L)$ sobre o conjunto de todos os ideais $\mathfrak{a}$ de $K[X_1, \ldots, X_n]$ com $\sqrt{\mathfrak{a}} = \mathfrak{a}$. Mais ainda, para qualquer ideal $\mathfrak{a}$ de $K[X_1, \ldots, X_n]$, temos que $\sqrt{\mathfrak{a}} = I(Z(\mathfrak{a}))$.*

Definição 1.3.13 :

a) *Uma K-álgebra que (como um anel) é finitamente gerada sobre K é chamada K-álgebra afim.*

b) *Para uma K-variedade $V \subset A^n(L)$*

$$K[V] := R[X_1, \ldots, X_n]/I(V)$$

é chamado o anel de coordenadas de V.

Vamos agora dar a definição da dimensão de Krull, para com ela chegarmos à definição de dimensão de uma variedade.

Definição 1.3.14 : *Dado um anel R, o $Spec(R)$ é o conjunto dos ideais primos de R e a dimensão de Krull de R, $\dim R$ é o supremo dos comprimentos n das cadeias de ideais primos de R*

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n \quad (\mathfrak{p}_{i+1} \neq \mathfrak{p}_i) \qquad (1)$$

A altura, $ht(\mathfrak{p})$, de $\mathfrak{p} \in Spec(R)$ é o supremo dos n de todas as cadeias (1) com $\mathfrak{p} = \mathfrak{p}_n$. Para qualquer ideal $I \neq R$, a altura $ht(I)$ está definida como o ínfimo das alturas dos divisores primos de I (um divisor primo de I é um ideal primo que contém I). Definimos também dimensão (ou co-altura) do ideal I por $dim(I) := \dim R/I$.

Podemos agora definir a dimensão de uma K-variedade V.

Definição 1.3.15 : *A dimensão de Krull de uma K-variedade $V \subset A^n(L)$ é a dimensão do anel de coordenadas $K[V]$ de V, isto é, $\dim V := \dim K[V]$.*

1.4 Localização e Lema de Nakayama

Seja R um anel qualquer. Vamos generalizar a construção do corpo dos racionais $\mathbb{Q}$ a partir do anel dos inteiros $\mathbb{Z}$. Considere S um subconjunto multiplicativo de R tal que $1 \in S$. Definimos uma relação de equivalência em $R \times S$ da seguinte forma:

$$(a, s) \equiv (b, t) \Longleftrightarrow (at - bs)u = 0 \text{ para algum } u \in S.$$

Certamente essa relação é reflexiva e simétrica . Para mostrar que é transitiva, seja $(a, s) \equiv (b, t)$ e $(b, t) \equiv (c, d)$, então existem $v, w \in S$ tal que $(at - bs)v = 0$ e $(bd - ct)w = 0$. Eliminando b das duas equações obtemos $(ad - cs)tvw = 0$. Como S é fechado para a multiplicação, nós obtemos $tvw \in S$ e logo $(a, s) \equiv (c, d)$. Portanto, temos uma relação de equivalência.

Denotamos por a/s a classe de equivalência de (a, s), e por R_S o conjunto das classes de equivalência. Podemos dar a R_S uma estrutura de anel definindo a adição e a multiplicação dessas "frações" a/s da seguinte forma:

$$(a/s) + (b/t) = (at + bs)/st,$$

$$(a/s)(b/t) = ab/st.$$

Temos um homomorfismo de anéis $f : R \longrightarrow R_S$ definido por $f(x) = x/1$. Em geral f não é injetivo.

O anel R_S é chamado o anel de frações de R com relação a S e tem a seguinte propriedade universal:

Proposição 1.4.1 : *Seja $g : R \longrightarrow B$ um homomorfismo de anéis tal que $g(s)$ é uma unidade em B para todo $s \in S$. Então existe um único homomorfismo $h : R_S \longrightarrow B$ tal que $g = h \circ f$.*

Dem. : (Unicidade) Se h satisfaz as condições, então $h(a/1) = hf(a) = g(a)$ para todo $a \in R$ e logo se $s \in S$

$$h(1/s) = h((s/1)^{-1}) = h(s/1)^{-1} = g(s)^{-1}$$

e, portanto, $h(a/s) = f(a/1)h(1/s) = g(a)g(s)^{-1}$,logo h está unicamente determinado por g.

(Existência) Seja $h(a/s) = g(a)g(s)^{-1}$. Então h será certamente um homomorfismo, se provarmos que ele está bem definido. Suponhamos então que $a/s = a'/s'$, temos que existe $t \in S$ tal que $(as' - a's)t = 0$, logo

$$(g(a)g(s') - g(a')g(s))g(t) = 0;$$

agora $g(t)$ é uma unidade em B e assim $g(a)g(s)^{-1} = g(a')g(s')^{-1}$. □

Corolário 1.4.2 : *Se $g : R \longrightarrow B$ é um homomorfismo de anéis tal que:*

a) *Se $s \in S$, então $g(s)$ é uma unidade em B.*

b) *Se $g(a) = 0$, então $as = 0$ para algum $s \in S$.*

c) *Todo elemento de B é da forma $g(a)g(s)^{-1}$.*

Então existe um único isomorfismo $h : R_S \longrightarrow B$ tal que $g = h \circ f$.

Dem. : Veja [1] □

Daremos agora alguns exemplos de anéis de frações.

Exemplo 1.4.3 :

1. Seja $\mathfrak{p}$ um ideal primo de R, então $S = R - \mathfrak{p}$ é um subconjunto multiplicativo, nós escrevemos $R_{\mathfrak{p}}$ no lugar de R_S. $R_{\mathfrak{p}}$ é chamado localização de R em $\mathfrak{p}$. Os elementos a/s com $a \in \mathfrak{p}$ formam um ideal m em $R_{\mathfrak{p}}$. Se $b/t \notin m$, então $b \notin \mathfrak{p}$, logo $b \in S$ e portanto b/t é uma unidade em $R_{\mathfrak{p}}$. Disto segue que se $\mathfrak{a}$ é um ideal de $R_{\mathfrak{p}}$ e $\mathfrak{a} \nsubseteq m$, então $\mathfrak{a}$ contém uma unidade e é portanto o próprio anel. Logo m é o único ideal maximal em $R_{\mathfrak{p}}$, ou seja , $R_{\mathfrak{p}}$ é um anel local.

2. Se R é um domínio de integridade e $S = R - 0$, então R_S é o corpo de frações de R.

3. Sejam $f \in R$ e $S = \{1, f, f^2, \ldots\}$, denotamos o anel de frações neste caso por R_f.

Usando a notação $\mu(M)$ para o número de elementos de um conjunto mínimo de geradores do módulo M, podemos mostrar o Lema de Nakayama, que será usado em algumas demonstrações no desenvolvimento do texto.

Lema 1.4.4 *(Lema de Nakayama): Dado I um ideal de R que está contido na interseção de todos os ideais maximais de R. Sejam M um R-módulo arbitrário e $N \subset M$ um submódulo para o qual M/N é finitamente gerado. Se $M = N + IM$, então $M = N$.*

Dem. : Chame $\overline{M} := M/N$, ele tem um sistema mínimo de geradores $\{m_1, \ldots, m_t\}$. Suponha que $t > 0$. Como $\overline{M} = I\overline{M}$, pois $M/N = \frac{N/N+IM}{N} = I(M/N) = I\overline{M}$, existe uma equação

$$m_t = \sum_{j=1}^{t} a_j m_j \qquad (a_j \in I,\ j = 1, \ldots, t)$$

Como a_t está em todos $m \in Max(R)$, pois $I \subset \bigcap_{m \in Max(R)} m$, e portanto $1 - a_t$ é uma unidade em R, de $(1 - a_t)m_t = \sum_{j=1}^{t-1} a_j m_j$, segue que $m_t \in < m_1, \ldots, m_{t-1} >$. Isso contradiz a minimalidade do sistema de geradores de $\overline{M}$.

Logo $t = 0$ e assim $M = N$. □

Como um corolário do Lema de Nakayama, temos o resultado abaixo.

Corolário 1.4.5 : *Sejam (R, m) um anel local, $k := R/m$ seu corpo de resíduos e M um R-módulo finitamente gerado. Para elementos $m_1, \ldots, m_t \in M$ as seguintes afirmações são equivalentes:*

a) $M =< m_1, \ldots, m_t >$.

b) *O conjunto de resíduos $\overline{m_1}, \ldots, \overline{m_t} \in M/\,mM$ dos m_i formam um sistema de geradores do k-espaço vetorial M/mM.*

Dem. : Ver [5] □

Do corolário acima e de fatos sobre espaços vetoriais, nós obtemos os seguintes resultados:

Corolário 1.4.6 : *Sob as hipóteses de 1.4.5 temos:*

a) $\mu(M) = dim_k(M/mM)$.

b) $m_1, \ldots, m_t \in M$ *formam um sistema minimal de geradores de M se, e somente se, suas classes de resíduos $\overline{m_1}, \ldots, \overline{m_t} \in M/mM$ formam uma base.*

c) *Se $\{m_1, \ldots, m_t\}$ é um sistema minimal de geradores de M e se $\sum_{i=1}^{t} r_i m_i = 0$, $r_i \in R$, então $r_i \in m$ para $i = 1, \ldots, t$.*

d) *Qualquer sistema de geradores de M contém um sistema minimal.*

e) *Elementos $m_1, \ldots, m_r \in M$ podem ser estendidos a um sistema minimal de geradores de M se, e somente se, suas classes de resíduos $\overline{m_1}, \ldots, \overline{m_t}$ são linearmente independentes sobre k.*

1.5 Teorema do "Going-up"

Sejam B um anel e R um subanel de B (tal que $1 \in R$). Um elemento $x \in B$ é chamado *inteiro (ou integral)* sobre R se é raiz de um polinômio mônico com coeficientes em R, isto é, se x satisfaz uma equação da forma

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \qquad (1)$$

onde $a_i \in R$. Se todo elemento de B é inteiro sobre R, dizemos que B é uma extensão inteira de R. É claro que todos os elementos de R são inteiros sobre R.

Exemplo 1.5.1 : Considere $B = \mathbb{R}$ e $R = \mathbb{Q}$ temos que $x = \sqrt{2} \in \mathbb{R}$ é inteiro sobre $\mathbb{Q}$, pois é raiz do polinômio mônico $F = X^2 - 2 \in \mathbb{Q}[X]$.

A proposição abaixo nos dá uma caracterização clássica de elemento inteiro e sua demonstração pode ser vista em [1].

Proposição 1.5.2 : *Dados R, B anéis com R subanel de B, então as seguintes afirmações são equivalentes.*

a) *$x \in B$ é inteiro sobre R.*

b) *$R[x]$ é um R-módulo finitamente gerado.*

c) *$R[x]$ está contido em um subanel C de B, tal que C é um R-módulo finitamente gerado.*

d) *Existe um $R[x]$-módulo fiel M que é finitamente gerado como um R-módulo.*

Uma conseqüência da proposição anterior, é que se $x_i \in B$, $i = 1, \ldots n$ são inteiros sobre R, então $R[x_1, \ldots, x_n]$ é um R-módulo finitamente gerado. A demonstração desse resultado é feita por indução sobre n.

Um outro corolário de 1.5.2 é que o conjunto C dos elementos de B que são inteiros sobre R é um subanel de B contendo R. A demonstração usa o fato que se $x, y \in C$ então $R[x, y]$ é um R-módulo finitamente gerado.

O anel C, descrito acima é chamado *fecho integral* de R em B. Se $C = R$, então R é chamado *integralmente fechado* em B. O exemplo abaixo nos mostra que $\mathbb{Z}$ é integralmente fechado sobre $\mathbb{Q}$.

Exemplo 1.5.3 : Sejam $R = \mathbb{Z}$ e $B = \mathbb{Q}$. Se um número racional $x = r/s$ é inteiro sobre $\mathbb{Z}$, onde $(r, s) = 1$, então nós encontramos:

$$r^n + a_{n-1}r^{n-1}s + \cdots + a_0 s^n = 0, \ a_i \in \mathbb{Z}$$

Se existe um primo $p \in \mathbb{Z}$ tal que $p \mid s$, então $p \mid r$ também, o que é uma contradição. Logo $s = \pm 1$. Portanto $x \in \mathbb{Z}$. Logo $\mathbb{Z}$ é integralmente fechado sobre $\mathbb{Q}$.

Temos a propriedade transitiva para a dependência integral, isto é, se B é uma extensão inteira de R e C é uma extensão inteira de B, então C é uma extensão inteira de R.

A próxima proposição mostra que a dependência integral é preservada passando ao quociente e para o anel de frações.

Proposição 1.5.4 : *Seja $B \mid R$ uma extensão inteira de anéis.*

1. *Se $\mathfrak{b}$ é um ideal de B e $\mathfrak{a} = \mathfrak{b} \cap R$, então $B/\mathfrak{b}$ é inteiro sobre $R/\mathfrak{a}$.*

2. *Se S é um subconjunto multiplicativo de R, então B_S é inteiro sobre R_S.*

Dem. :

1. Se $x \in B$ temos que $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ com $a_i \in R$, pois B é inteira sobre R. Reduzindo esta equação módulo $\mathfrak{b}$, temos $\overline{x}^n + \overline{a_{n-1}}\overline{x}^{n-1} + \ldots + \overline{a_0} = 0$, com $\overline{a_i} \in R/\mathfrak{a}$, ou seja, $\overline{x} \in B/\mathfrak{b}$ é inteiro sobre $R/\mathfrak{a}$.

2. Seja $x/s \in B_S$, $x \in B$ e $s \in S$, então na equação acima temos
$$(x/s)^n + (a_{n-1}/s)(x/s)^{n-1} + \ldots + a_0/s_n = 0$$
que nos mostra que x/s é inteiro sobre R_S.

□

Proposição 1.5.5 : *Sejam $R \subseteq B$ domínios, B inteiro sobre R, então B é um corpo se, e somente se, R é um corpo.*

Dem. : Ver [1] □

Corolário 1.5.6 : *Sejam B inteiro sobre R e $\mathfrak{q}$ um ideal primo de B e $\mathfrak{p} = \mathfrak{q} \cap R$. Então $\mathfrak{q}$ é maximal se, e somente se, $\mathfrak{p}$ é maximal.*

Dem. : Por 1.5.4, temos que $B/\mathfrak{q}$ é inteiro sobre $R/\mathfrak{p}$ e, como os ideais são primos, temos que $B/\mathfrak{q}$ e $R/\mathfrak{p}$ são domínios. Logo, pela proposição anterior, temos que $B/\mathfrak{q}$ é corpo se, e somente se, $R/\mathfrak{p}$ é corpo. Logo, $\mathfrak{q}$ é maximal se, e somente se, $\mathfrak{p}$ é maximal. □

O teorema a seguir é usado na demonstração do teorema de "Going-up" e nos garante a existência de um ideal primo $\mathfrak{q}$ em B tal que, dado um ideal primo $\mathfrak{p}$ em R, ele seja a contração de $\mathfrak{q}$, isto é, $\mathfrak{q} \cap R = \mathfrak{p}$.

Teorema 1.5.7 : *Sejam B uma extensão inteira de R e $\mathfrak{p}$ um ideal primo de R. Então existe um ideal primo $\mathfrak{q}$ de B tal que $\mathfrak{q} \cap R = \mathfrak{p}$.*

Dem. : Por 1.5.4 temos $B_{\mathfrak{p}}$ é inteiro sobre $R_{\mathfrak{p}}$, onde $B_{\mathfrak{p}} = B_S$, com $S = R \setminus \mathfrak{p}$ e o diagrama

$$\begin{array}{ccc} R & \to & B \\ {\scriptstyle \alpha}\downarrow & & \downarrow{\scriptstyle \beta} \\ R_{\mathfrak{p}} & \to & B_{\mathfrak{p}} \end{array}$$

onde as setas na horizontal são injetivas, é comutativo. Seja n um ideal maximal de $B_{\mathfrak{p}}$, então $m = n \cap R_{\mathfrak{p}}$ é ideal maximal por 1.5.6. Logo, é o único ideal maximal do anel local $R_{\mathfrak{p}}$. Se $\mathfrak{q} = \beta^{-1}(n)$, então $\mathfrak{q}$ é primo e nós temos $\mathfrak{q} \cap R = \alpha^{-1}(m) = \mathfrak{p}$. □

Finalmente temos o Teorema de "Going-up".

Teorema 1.5.8 : *Sejam B uma extensão inteira de R, $\mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_n$ uma cadeia de ideais primos de R e $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m$ $(m < n)$ uma cadeia de ideais primos de B tal que $\mathfrak{q}_i \cap R = \mathfrak{p}_i$, $1 \leq i \leq m$. Então a cadeia $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m$ pode ser estendida a uma cadeia $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_n$ tal que $\mathfrak{q}_i \cap R = \mathfrak{p}_i$, para $1 \leq i \leq n$.*

Dem. : Por indução, podemos reduzir ao caso $m = 1$ e $n = 2$. Sejam $\overline{R} = R/\mathfrak{p}_1$ e $\overline{B} = B/\mathfrak{q}_1$, então $\overline{R} \subseteq \overline{B}$ e $\overline{B}$ é inteiro sobre $\overline{R}$ por 1.5.4. Logo, por 1.5.7 existe um ideal primo $\overline{\mathfrak{q}_2}$ de $\overline{B}$ tal que $\overline{\mathfrak{q}_2} \cap \overline{R} = \overline{\mathfrak{p}_2}$, a imagem de $\mathfrak{p}_2$ em $\overline{R}$. Voltando $\overline{\mathfrak{q}_2}$ para B, temos um ideal primo $\mathfrak{q}_2$ que tem as propriedades desejadas. □

Como conseqüência desse teorema temos o seguinte corolário, que nos diz qual a dimensão do anel R e de um ideal $\mathfrak{q}$ de B.

Corolário 1.5.9 : *Seja B uma extensão inteira de R, então*

a) *$dim R = dim B$.*

b) *Para qualquer $\mathfrak{q} \in Spec(B)$ nós temos $ht(\mathfrak{q}) \leq ht(\mathfrak{q} \cap R)$ e $dim \mathfrak{q} = dim(\mathfrak{q} \cap R)$.*

Dem. : Isso segue de 1.5.8 e das definições de dimensão e altura. □

1.6 Teorema da Normalização de Noether

Lembramos que elementos $Y_1, \ldots, Y_n \in A$ são *algebricamente independentes* sobre K, onde A é uma álgebra afim sobre um corpo K, se para $F \in K[X_1, \ldots, X_n]$, temos $F(Y_1, \ldots, Y_n) = 0$, então $F = 0$.

Daremos agora o Teorema da Normalização de Noether.

Teorema 1.6.1 : *Sejam A uma álgebra afim sobre um corpo K e $I \subset A$ um ideal, $I \neq A$. Existem números naturais $\delta \leq d$ e elementos $Y_1, \ldots, Y_d \in A$ tais que:*

a) *$Y_1, \ldots, Y_d$ são algebricamente independentes sobre K.*

b) *A é finitamente gerado como um $K[Y_1, \ldots, Y_d]$-módulo.*

c) *$I \cap K[Y_1, \ldots, Y_d] = (Y_{\delta+1}, \ldots, Y_d)$.*

Se K é infinito e $A = K[x_1, \ldots, x_n]$, então podemos obter também:

d) *Para $i = 1, \ldots, \delta$, Y_i é da forma $Y_i = \sum_{k=1}^{n} a_{ik} x_k$, $a_{ik} \in K$.*

Dem. : Veja [5] □

Definição 1.6.2 : *Para uma K-álgebra afim $A \neq \{0\}$, $K[Y_1, \ldots, Y_d] \subset A$ é uma normalização Noetheriana se $Y_1, \ldots, Y_d$ são algebricamente independentes sobre K e A é finitamente gerado como um $K[Y_1, \ldots, Y_d]$-módulo.*

Uma conseqüência do teorema da normalização de Noether nos dá uma condição necessária para obtermos a dimensão de uma K-álgebra afim.

Proposição 1.6.3 : *Se $K[Y_1, \ldots, Y_d] \subset A$ é uma normalização Noetheriana, então $dim A = d$.*

Dem. : Considerando o anel de polinômios $K[Y_1, \ldots, Y_d]$ sobre um corpo K, temos que:

$$(0) \subset (Y_1) \subset (Y_1, Y_2) \subset \cdots \subset (Y_1, \ldots, Y_d)$$

é uma cadeia de ideais primos de comprimento d. Portanto, pela definição de dimensão de Krull, segue que $dim\, K[Y_1, \ldots, Y_d] \geq d$, agora usando 1.5.9, temos que $dim\, A = dim\, K[Y_1, \ldots, Y_d] \geq d$.

Assim para uma cadeia de ideais primos

$$\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_m$$

em A, resta mostrar que $m \leq d$. Faremos isto por indução sobre d.

Se colocarmos $\mathfrak{p}_i := \mathfrak{q}_i \cap K[Y_1, \ldots, Y_d]$, então

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_m$$

é uma cadeia de ideais primos em $K[Y_1, \ldots, Y_d]$. Para $d = 0$, nada a fazer.

Seja $d > 0$ e suponha, como hipótese de indução, que a afirmação tenha sido provada para álgebras de polinômios com menos variáveis. Então existe algo a ser provado somente para $m > 0$.

Por 1.6.1 existe uma normalização Noetheriana $K[T_1, \ldots, T_d] \subset K[Y_1, \ldots, Y_d]$ com $\mathfrak{p}_i \cap K[T_1, \ldots, T_d] = (T_{\delta+1}, \ldots, Y_d)$, com $\delta \leq d$. Como $\mathfrak{p}_1 \neq (0)$, nós temos $\delta < d$ e, então, $K[Y_1, \ldots, Y_\delta] \subset K[Y_1, \ldots, Y_d]/\mathfrak{p}_i$ é uma normalização Noetheriana também.

Pela hipótese de indução, para o comprimento da cadeia de ideais primos

$$(0) = \mathfrak{p}_1/\mathfrak{p}_1 \subset \mathfrak{p}_2/\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m/\mathfrak{p}_1$$

nós temos $m - 1 \leq \delta < d$. Segue que $m \leq d$ e portanto $m = d$ e $dim\, A = d$. □

Como um corolário de 1.6.3 temos:

Corolário 1.6.4 : *Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ ideais primos minimais de A, se $dim\, A/\mathfrak{p}_i = r$, r fixo, para $i = 1, \ldots, s$, então para todo $\mathfrak{p} \in Spec(A)$, temos*

$$dim\, A = ht(\mathfrak{p}) + dim(A/\mathfrak{p})$$

Dem. : Essa demonstração pode ser encontrada em [5]. □

Ainda em relação à proposição 1.6.3, podemos caracterizar a dimensão de Krull de uma K-álgebra afim A, que é um domínio, de uma outra maneira. A saber, lembremos que se $L \mid K$ é uma extensão de corpos com $L = K(x_1, \ldots, x_n)$, então o grau de transcendência de L sobre K, denotado por $grtr(L)$, é o máximo dos números r, tal que existem $y_1, \ldots, y_r \in L$ algebricamente independentes sobre K, com $L \mid K(y_1, \ldots, y_r)$ sendo extensão algébrica. E, assim, a partir da proposição 1.6.3, tem-se o resultado:

Corolário 1.6.5 : *Se A é uma K-álgebra afim que é um domínio e L é o corpo de frações de A, então $dim\, A = grtr_K(L)$.*

1.7 Ideais e Variedades que são Interseções Completas

Um outro resultado importante da Álgebra Comutativa é o Teorema do Ideal Principal de Krull, que nos dá uma cota inferior para o número de geradores de um ideal de um anel Noetheriano. Formalmente temos:

Teorema 1.7.1 *(Teorema do Ideal Principal de Krull Generalizado): Seja R um anel Noetheriano, $I \neq R$ um ideal gerado por l elementos. Para qualquer divisor primo minimal $\mathfrak{p}$ de I, temos $ht(\mathfrak{p}) \leq l$.*

Dem. : Veja [5]. □

Como a altura de um ideal $I \neq (1)$ está definido como o ínfimo das alturas dos divisores primos minimais de I, segue de 1.7.1 que um ideal $I \neq (1)$ em um anel Noetheriano sempre tem altura finita, na verdade $ht(I) \leq \mu(I)$, onde $\mu(I)$ denota o número de elementos de um conjunto mínimo de geradores de I. Agora vamos estudar o caso especial em que a igualdade acontece.

Definição 1.7.2 *: Seja $I \neq R$ um ideal de um anel Noetheriano R.*

a) *I é chamado uma interseção completa, se $ht(I) = \mu(I)$.*

b) *I é chamado um "set-theoretic" interseção completa, se existirem elementos $a_1, \ldots, a_l \in I$ tais que $\sqrt{I} = \sqrt{(a_1, \ldots, a_l)}$, onde $l = ht(I)$.*

c) *Dizemos que I é localmente uma interseção completa, se I_m é uma interseção completa em R_m, para todo $m \in Max(R)$, com $I \subset m$.*

Observação 1.7.3

1. No caso **c)** $I_{\mathfrak{p}}$ também é uma interseção completa em $R_{\mathfrak{p}}$ para todo $\mathfrak{p} \in Spec(R)$ com $I \subset \mathfrak{p}$, pois se $\mathfrak{p} \subset m$, com $m \in Max(R)$, então $ht(I_m) \leq ht(I_{\mathfrak{p}}) \leq \mu(I_{\mathfrak{p}}) \leq \mu(I_m)$, e de $ht(I_m) = \mu(I_m)$ segue que $ht(I_{\mathfrak{p}}) = \mu(I_{\mathfrak{p}})$.

2. Se I é uma interseção completa, é claro que é também um "set-theoretic" e localmente uma interseção completa, pois $ht(I_{\mathfrak{p}}) \geq ht(I)$ para todo $\mathfrak{p} \in Z(I)$. veremos no final do capítulo 3, um exemplo de que a recíproca não é válida, isto é daremos uma exemplo de uma ideal que é "set-theoretic"interseção completa, mas que não é interseção completa.

3. Nos casos **a)** e **b)** da definição acima segue, do Teorema do Ideal Principal de Krull generalizado, que todos os divisores primos minimais de I têm altura l.

Uma definição equivalente a 1.7.2 para a geometria algébrica é a seguinte:

Definição 1.7.4 : *Seja V uma K-variedade d-dimensional de um espaço afim n-dimensional sobre L.*

a') *V é chamado interseção completa, se seu ideal no anel $K[X_1, \ldots, X_n]$ é gerado por $n - d$ polinômios.*

b') *V é chamado um "set-theoretic" interseção completa, se é interseção de $n - d$ K-hipersuperfícies.*

c') *Dizemos que V é localmente uma interseção completa, se o seu ideal $I(V)$ no anel $K[X_1, \ldots, X_n]$ é localmente uma interseção completa.*

Vamos mostrar que a definição 1.7.2 é equivalente à definição 1.7.4.
Dem. :

(a) $\Leftrightarrow$ a')) Se V é interseção completa então $\mu(I(V)) \leq n - d = dim\, A^n(L) - dim\, V$. Por outro lado pelo corolário 1.6.4 temos que $ht(I(V)) = n - d$ e logo $\mu(I(V)) \leq ht(I(V))$. Agora, sabemos, pelo teorema 1.7.1, que $\mu(I(V)) \geq ht(I(V))$. Portanto $\mu(I(V)) = ht(I(V))$ e, então, $I(V)$ é uma interseção completa.

Reciprocamente, se $I(V)$ é uma interseção completa, então

$$\mu(I(V)) = ht(I(V)) = dim\, A^n(L) - dim\, V = n - d$$

pela definição 1.7.2 e pelo corolário 1.6.4. Portanto, V é uma interseção completa.

(b) $\Leftrightarrow$ b')) Se V é "ideal- theoretic" uma interseção completa, então $V = \bigcap_{i=1}^{n-d} Z(f_i)$, mas pela proposição 1.3.12 $\sqrt{I(V)} = \sqrt{(f_1, \ldots, f_{n-d})}$, como queríamos.

(c) $\Leftrightarrow$ c')) Segue direto da definição.

□

Exemplo 1.7.5 : A curva $V = \{(t^4, t^{10}, t^{13}) \mid t \in k\} \subset A^3(k)$, é uma interseção completa, já a curva $V' = \{(t^3, t^4, t^5) \mid t \in k\} \subset A^3(k)$ não é uma interseção completa, onde k é um corpo algebricamente fechado. Tais fatos serão justificados por um critério que determina se uma curva do tipo $\{(t^{n_1}, t^{n_2}, t^{n_3}) \mid t \in k\} \subset A^3(k)$ é ou não uma interseção completa , onde k é um corpo algebricamente fechado e $(n_1, n_2, n_3) = 1$.

Tal critério está intimamente ligado com o fato de o semigrupo S gerado por n_1, n_2, n_3 ser ou não simétrico, o que será analizado nos próximos capítulos.

Capítulo 2

Semigrupos e Interseção Completa

Neste capítulo, daremos a definição e algumas propriedades de semigrupos. Trabalharemos com relações que definem semigrupos e mostraremos que todo semigrupo finitamente gerado é finitamente apresentado. Daremos também as definições de semigrupos numéricos e simétricos e uma caracterização de semigrupos simétricos. Por fim, daremos a noção de interseção completa para semigrupos e uma equivalência entre semigrupos que são interseções completas e curvas parametrizadas que são interseções completas.

2.1 Semigrupos

Definição 2.1.1 : *Um semigrupo é um conjunto S, não vazio, munido de uma operação binária $(*)$ associativa.*

Um semigrupo S é dito:

1. **com a propriedade do cancelamento** se para todo $a, b, c \in S$ tais que $a*b = a*c$ e $b*a = c*a$, temos $b = c$.
2. **comutativo (ou abeliano)** se para todo $a, b \in S$, temos $a*b = b*a$.
3. **com elemento neutro** se existe $a \in S$ tal que para todo $b \in S$, temos $a*b = b$ e $b*a = b$.

Exemplo 2.1.2 : O conjunto dos números naturais, que denotaremos por $\mathbb{N}$, é um semigrupo comutativo com elemento neutro com a operação de adição.

O conjunto $\dot{\mathbb{N}} = \mathbb{N} \setminus \{0\}$ é um semigrupo comutativo sem elemento neutro, com a operação de adição.

Neste texto trabalharemos com semigrupos comutativos, com a propriedade do cancelamento e com elemento neutro. Por isso, usaremos a notação aditiva $(+)$ para a operação do semigrupo; assim, quando dissermos semigrupo aditivo ou simplesmente semigrupo estaremos referindo-nos a semigupos desse tipo.

Definição 2.1.3 : *Um subsemigrupo de um semigrupo S é um subconjunto H de S que é fechado em relação à adição.*

Definição 2.1.4 : *Um semigrupo S é finitamente gerado se existe um conjunto finito, $B = \{a_1, \ldots, a_n\}$, de elementos de S, tal que S é gerado por ele, isto é,*

$$S = \{\sum_{i=1}^{n} a_i m_i,\ m_i \in I\!N\}.$$

O conjunto B é chamado conjunto (ou sistema) de geradores de S. B é dito conjunto mínimo de geradores (ou sistema minimal de geradores) se é o menor conjunto de geradores de S.

Denotamos S gerado por B por $S =< B >$.

Exemplo 2.1.5 : Considere $B = \{3, 4, 5\}$, então

$$S =< 3, 4, 5 >= \{v \in S \mid v = n_1 3 + n_2 4 + n_3 5, n_i \in I\!N, i = 1, 2, 3\}$$

é um semigrupo contido em $I\!N$.

Definição 2.1.6 : *Seja S um semigrupo finitamente gerado. Chamamos de posto de S ao número de elementos de um conjunto mínimo de geradores de S.*

A noção de semigrupo livre é fundamental para a descrição de um semigrupo genérico e é dada na nossa próxima definição.

Definição 2.1.7 : *Um semigrupo F é chamado semigrupo livre de posto n, $n \in I\!N$, se existe um sistema de geradores, $B = \{e_1, \ldots, e_n\}$, de F, tal que todo elemento $a \in F$ pode ser unicamente representado na forma: $a = b_1 e_1 + \cdots + b_n e_n$, onde $b_i \in I\!N$ para $i = 1, \ldots, n$.*

Os elementos $e_1, \ldots, e_n$ são chamados geradores livres de F.

Exemplo 2.1.8 : $F = I\!N^n = \{v = (m_1, \ldots, m_n) \mid m_i \in I\!N\}$ é um semigrupo livre, com a adição nas coordenadas, gerado por $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots, 0), \ldots,$ $e_n = (0, 0, \ldots, 1)$, que é a base canônica de $I\!N^n$.

Como não poderia deixar de ser, uma outra noção fundamental é a de homomorfismo.

Definição 2.1.9 : *Dados dois semigrupos aditivos S, S' e $\phi : S \longrightarrow S'$ uma aplicação entre eles, dizemos que ϕ é um homomorfismo entre S e S' se dados $a, b \in S$ temos*

$$\phi(a+b) = \phi(a) + \phi(b)$$

Chamamos um homomorfismo sobrejetor de epimorfismo.

Assim como construímos $\mathbb{Z}$ a partir de $\mathbb{N}$, podemos construir a partir de um semigrupo S um "menor" grupo contendo S como um subsemigrupo. De fato, consideremos em $S \times S$ a relação dada por:

$$(a,b) \sim (c,d) \Longleftrightarrow a + d = c + b.$$

Como em S temos a propriedade comutativa e do cancelamento, fica fácil mostrar que a relação $\sim$ é de equivalência. Consideremos $\tilde{S} := S \times S/\sim$ o conjunto das classes de equivalência de S, isto é, dados $(a,b) \in S \times S$, chamamos $\overline{(a,b)} = \{(c,d);\ (a,b) \sim (c,d)\}$ a classe de equivalência determinada por (a,b), temos que $\tilde{S} = \{\overline{(a,b)},\ (a,b) \in S \times S\}$.

Agora definamos em $\tilde{S}$ a adição por:

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$$

É simples mostrar que tal operação está bem definida, é associativa e comutativa. Mais ainda, observe que:

1. Dados $a \in S$, $\overline{(a,a)} = \overline{(0,0)}$ e portanto $\overline{(c,d)} = \overline{(c,d)} + \overline{(0,0)} = \overline{(a,a)} + \overline{(c,d)}$ quaisquer que sejam a, c, $d \in S$.

2. Dados a, $b \in S$, $\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b, b+a)} = \overline{(0,0)}$, isto é, $-\overline{(a,b)} = \overline{(b,a)}$.

3. $\phi : S \longrightarrow \tilde{S}$ dada por $\phi(a) = \overline{(a,0)}$ é injetiva e satisfaz $\phi(a+b) = \phi(a) + \phi(b)$.

A partir de todas estas propriedades, temos que $(\tilde{S}, +)$ é um grupo e que S pode ser identificado de modo natural com um subsemigrupo de $\tilde{S}$. Na verdade, observe que, em $\tilde{S}$, $-\overline{(b,0)} = \overline{(0,b)}$ e portanto dados $a \in S$ identificamos, em $\tilde{S}$, $\overline{(a,0)} = a$, temos então que $\overline{(a,b)} = a - b \in \tilde{S}$ e assim podemos concluir, de modo natural, que $\tilde{S}$ é o "menor" grupo que contém S como um subsemigrupo. O grupo $\tilde{S}$ é chamado grupo associado de S.

Vê-se, naturalmente, que quando S é um semigrupo gerado por $\{s_1, \ldots, s_n\}$ o grupo $\tilde{S}$ também é gerado (como grupo) por $\{s_1, \ldots, s_n\}$, isto é, se S é um semigrupo finitamente gerado, então $\tilde{S}$ é um grupo finitamente gerado e temos um novo invariante que é o posto de $\tilde{S}$, isto é, o posto da parte livre de $\tilde{S}$ (veja 1.1.5).

Definição 2.1.10 : *Dado um semigrupo aditivo e finitamente gerado S, definimos a dimensão de S como sendo o posto de $\tilde{S}$. Denotamos por $dim S = posto \tilde{S}$.*

Exemplo 2.1.11 : Seja $S =< 3, 4, 5 >$. Temos que $\tilde{S} =< S >$ e portanto $\tilde{S} = \mathbb{Z}$, que é livre de posto 1. Logo $posto\tilde{S} = 1$ e $dimS = 1$. Aliás, para qualquer semigrupo não trivial $S \subseteq \mathbb{Z}$ tem-se $dimS = 1$.

O próximo conceito nos será muito útil quando estivermos trabalhando com variedades algébricas associadas a semigrupos numéricos.

Definição 2.1.12 : *Seja A um subconjunto não vazio de S. Um ideal $\boldsymbol{a}$ de S gerado por A é definido por:*

$$\boldsymbol{a} = (A) = \{a + s, a \in A, s \in S\}.$$

Observação 2.1.13 :

1. Um ideal $\boldsymbol{a}$ é dito principal se é gerado por apenas um elemento, isto é, $\boldsymbol{a} = (a)$, onde $a \in S$.

2. Para $\boldsymbol{a} = (a)$, temos que $b \in \boldsymbol{a}$ se, e somente se $b - a \in S$ (lembre-se que podemos falar em $b - a \in \tilde{S}$). De fato,

$$b \in \boldsymbol{a} \Longleftrightarrow b = a + s, s \in S \Longleftrightarrow b - a = s \in S$$

3. Vamos denotar por $\mu(\boldsymbol{a})$ o número de elementos do conjunto mínimo de geradores de $\boldsymbol{a}$.

Considere um semigrupo S, onde para todo $s \in S$, $s \neq 0$ tem-se $-s \notin S$. Sob esta condição temos o seguinte resultado.

Proposição 2.1.14 : *Seja $\boldsymbol{a} = (a_1, \ldots, a_n)$ um ideal de S tal que $a_i - a_j \notin S, i \neq j$. Então se $\boldsymbol{a} = (b_1, \ldots, b_n)$ temos, depois de uma reordenação, se necessário, que $a_1 = b_1, \ldots, a_n = b_n$.*

Dem. : Suponhamos que $\boldsymbol{a} = (a_1, \ldots, a_n) = (b_1, \ldots, b_n)$. Temos $a_1 = b_{i_1} + s_1$, com $s_1 \in S$. Por outro lado, $b_{i_1} = a_{i_1} + s_1'$, com $s_1' \in S$.

Logo $a_1 - a_{i_1} = s_1 + s_1'$. Agora se $a_1 \neq a_{i_1}$, então $a_1 - a_{i_1} \in S, i \neq j$, que é uma contradição. Portanto $a_1 = a_{i_1}$ e $s_1 = s_1' = 0$, pela condição que assumimos em S.

Logo $a_1 = b_{i_1}$.

Analogamente temos $a_2 = b_{i_2}, \ldots, a_n = b_{i_n}$. Reordenando $b_1 = b_{i_1}, \ldots, b_n = b_{i_n}$, teremos $a_1 = b_1, \ldots, a_n = b_n$. □

Corolário 2.1.15 : *Se* $\boldsymbol{a} = (a_1, \ldots, a_n)$ *é tal que* $a_i - a_j \notin S$, $i \neq j$, *então* $\mu(\boldsymbol{a}) = n$.

Dem. : Suponhamos que $\boldsymbol{a} = (b_1, \ldots, b_{n-1})$. Pela prova da proposição anterior e depois de rearranjar, se necessário, temos $a_1 = b_1, \ldots, a_{n-1} = b_{n-1}$.

Logo $\boldsymbol{a} = (a_1, \ldots, a_{n-1}) = (b_1, \ldots, b_{n-1})$. No entanto se $a_n = a_i + s$, com $s \in S$, para algum $i = 1, \ldots, n-1$ então $a_n - a_i = s \in S$, que é uma contradição.

Portanto $\boldsymbol{a} = (a_1, \ldots, a_n)$ e $\mu(\boldsymbol{a}) = n$. □

2.2 Relações e Anel de um Semigrupo

Seja S um semigrupo finitamente gerado por $\{s_1, \ldots, s_n\}$. Existe um epimorfismo $\rho^* : F \longrightarrow S$, onde F é um semigrupo comutativo livre do posto n. Mais precisamente, dada uma base livre de $\{e_1, \ldots, e_n\}$ de F, define-se $\rho^*(\sum_{i=1}^n m_i e_i) = \sum_{i=1}^n m_i s_i$, $m_i \in \mathbb{N}$.

O epimorfismo ρ^* define uma relação binária em F:

$$\rho = \{(v, w) \in F \times F \mid \rho^*(v) = \rho^*(w)\}$$

Observamos que ρ é uma relação de equivalência e tem a seguinte propriedade de compatibilidade, que chamaremos de C: se $(v, v') \in \rho$ e $w \in F$, então $(v + w, v' + w) \in \rho$.

Definição 2.2.1 *Um subconjunto* $E \subseteq F \times F$ *é chamado uma congruência em* F *se:*

1. *E é uma relação de equivalência.*
2. *E tem a propriedade C.*

Por esta definição temos que ρ é uma congruência em F. Mais ainda, dado $v \in F$ se denotarmos a classe de equivalência determinada por v por $[v] = \{w \in F \mid (v, w) \in \rho\}$, temos que, no conjunto das classes de equivalência F/ρ, podemos definir a adição dada por

$$[v] + [w] = [v + w]$$

Tal adição está bem definida, torna F/ρ um semigrupo e a projeção canônica $\pi : F \longrightarrow F/\rho$ dada por $\pi(v) = [v]$ é um epimorfismo de semigrupos.

Lema 2.2.2 *Se* F *e* S *são semigrupos comutativos finitamente gerados,* F *é livre,* $\rho^* : F \longrightarrow S$ *é um epimorfismo e* $\rho \subseteq F \times F$ *é a congruência, dada por*

$$\rho = \{(v, w) \in F \times F \mid \rho^*(v) = \rho^*(w)\}$$

então F/ρ *é isomorfo a* S.

Dem. : Nas condições do enunciado, temos que ρ é uma congruência e que a projeção canônica $\pi : F \longrightarrow F/\rho$ dada por $\pi(v) = [v]$ é um epimorfismo de semigrupos. Agora defina $\phi : F/\rho \longrightarrow S$ por $\phi([v]) = \rho^*(v)$. Pode-se mostrar que ϕ está bem definido e é bijetor, isto é, ϕ é um isomorfismo entre semigrupos. □

A observação a seguir nos mostra como construir uma congruência a partir de uma relação qualquer em F.

Observação 2.2.3 : Do fato de que a interseção de congruências é uma congruência, podemos concluir que dada uma relação ρ existe uma "menor" congruência $\overline{\rho}$ que contém ρ. Mas, de fato, é possível construir explicitamente a congruência $\overline{\rho}$. Primeiramente, observamos que dada uma relação ρ em F, existem, a congruência trivial em F

$$\Delta = \{(v, v) \in F \times F \mid v \in F\}$$

com $F/\Delta \cong F$, e

$$\rho^{-1} = \{(v, w) \in F \times F \mid (w, v) \in \rho\}.$$

Construção de $\overline{\rho}$:

1. Coloquemos $\rho_0 = \rho \cup \rho^{-1} \cup \Delta$, então ρ_0 é reflexiva, simétrica e contém ρ.
2. Coloquemos $\rho_1 = \{(v + w, v' + w) \in F \times F \mid (v, v') \in \rho_0, w \in F\}$, então ρ_1 é reflexiva, simétrica e satisfaz a condição C e
3. (Fecho transitivo) Definamos $(v, w) \in F \times F$ um elemento de $\overline{\rho}$ se existem $v_0, v_1, \ldots, v_l \in F, v_0 = v, v_l = w$ com $(v_i, v_{i+1}) \in \rho_1$ para todo $i = 0, 1, \ldots, l - 1$.

É fácil verificar que $\overline{\rho}$ é de fato a congruência desejada.

Definição 2.2.4 *Uma congruência ρ em F é finitamente gerada se existe um subconjunto finito $\sigma \subset F \times F$ tal que $\rho = \overline{\sigma}$.*

Definição 2.2.5 *Um semigrupo S é finitamente apresentado se $S \cong F/\rho$, onde F é um semigrupo livre finitamente gerado e ρ é uma congruência finitamente gerada.*

O nosso próximo passo é, a partir de um anel comutativo com identidade R e um semigrupo aditivo S, associar um anel comutativo com identidade $R[S]$, chamado o *R-anel do semigrupo S.*

Sejam R um anel comutativo com identidade e S um semigrupo aditivo. Definimos $R[S] = \oplus_{s \in S} R x_s$ (isto é, o R-módulo livre com base $\{x_s,\ s \in S\}$) e em $R[S]$ introduzimos o produto que é estendido, respeitando a distributividade, a partir das relações $x_{s_1} x_{s_2} = x_{s_1 + s_2}$ quaisquer que sejam $s_1, s_2 \in S$. Pode-se verificar facilmente que $R[S]$ é um anel comutativo cuja unidade é x_0 (isto é, $x_0 = 1$) e, evidentemente, pela própria definição, ele é S-graduado.

Quando S é gerado por n elementos, podemos exibir um homomorfismo sobrejetor entre $R[X_1,\ldots,X_n]$ e $R[S]$ da seguinte forma:

Seja $R[X_1,\ldots,X_n]$ o anel de polinômios com n indeterminadas sobre R. Consideremos $X^v = \prod_{i=1}^n X_i^{m_i}$, $v \in \mathbb{N}^n$, $v = (m_i)$ e S como a imagem do epimorfismo $\rho^* : \mathbb{N}^n \longrightarrow S$. Este epimorfismo induz um epimorfismo de R-álgebras $\Gamma : R[X_1,\ldots,X_n] \longrightarrow R[S]$, definido por $\Gamma(X^v) = x_{\rho^*(v)}$.

Podemos considerar $R[X_1,\ldots,X_n]$ como um anel S-graduado no seguinte sentido:

Um polinômio $F \in R[X_1,\ldots,X_n]$ é dito homogêneo de grau s, $s \in S$, se $F = \sum r_v X^v$ com $\rho^*(v) = s$ para todo v tal que $r_v \neq 0$. Podemos verificar que isso define realmente uma graduação para $R[X_1,\ldots,X_n]$.

Da definição de Γ, segue que Γ é um epimorfismo homogêneo de grau zero, isto é, se $F \in R[X_1,\ldots,X_n]$ é homogêneo de grau s, então $\Gamma(F)$ é homogêneo de grau s em $R[S]$; logo, denotando por I_S o seu núcleo, temos que I_S é um ideal homogêneo, segundo a S-graduação. Para $A \in \rho$, isto é, $A = (v,w)$, $v,w \in \mathbb{N}^n$ e $\rho^*(v) = \rho^*(w)$, definimos $F_A = X^v - X^w$.

Os nossos próximos quatro resultados se referem à situação acima.

Proposição 2.2.6 : *Usando a notação acima, temos* $I_S = (\{F_A\}_{A\in\rho})$.

Dem. : Seja $J = (\{F_A\}_{A\in\rho})$. É claro que $J \subseteq I_S$, pois se $F_A = X^v - X^w$, com $A = (v,w) \in \rho$, então $\rho^*(v) = \rho^*(w)$ e assim $\Gamma(F_A) = x_{\rho^*(v)} - x_{\rho^*(w)} = 0$.

Reciprocamente, escolha $F \in I_S$, F homogêneo de grau $s, s \in S$ (basta mostrar para F homogêneo, pois I_S é homogêneo). Então $F = \sum_{i=1}^m r_{v_i} X^{v_i}$ com $\rho^*(v_i) = s$ para $i = 1,\ldots,m$ e $\sum_{i=1}^m r_{v_i} = 0$. Assim, $F = \sum_{i=1}^{m-1} r_{v_i}(X^{v_i} - X^{v_m}) = \sum_{i=1}^{m-1} r_{v_i} F_{A_i}$, onde $A_i \in \rho$ para $i = 1,\ldots,m-1$.

Como $\rho^*(v_i) = \rho^*(v_m) = s$, para todo $i = 1,\ldots,m-1$, nós obtemos que $A_i \in \rho$ para todo $i = 1,\ldots,m-1$ e então $F \in J$. Logo $I_S \subseteq J$.

Portanto, $I_S = (\{F_A\}_{A\in\rho})$. □

Com as mesmas hipóteses da proposição anterior, se tomamos $\sigma \subseteq \mathbb{N}^n \times \mathbb{N}^n$ e consideramos $\sigma_0 = \sigma \cup \sigma^{-1} \cup \Delta$ e σ_1 dados na observação 2.2.3 temos o seguinte resultado:

Lema 2.2.7 : *Seja* $\sigma = \{A_1,\ldots,A_m\}$, *onde* $A_i \in \rho$ *para* $i = 1,\ldots,m$. *Então* $(\{F_A\}_{A\in\sigma_1}) = (\{F_{A_1},\ldots,F_{A_m}\})$.

Dem. : Chame $I = (\{F_A\}_{A\in\sigma_1})$ e $J = (F_{A_1},\ldots,F_{A_m})$.

Que $J \subseteq I$ é claro, pois $F_{A_i} \in \{F_A \mid A \in \sigma_1\}$.

Reciprocamente, seja $A \in \sigma_1$. Então $A = (v+w, v'+w)$, $(v,v') \in \sigma_0$ e $w \in F$. Logo $F_A \in I$ é tal que $F_A = X^{v+w} - X^{v'+w} = X^w(X^v - X^{v'}) = X^w F_B$, com $B = (v,v') \in \sigma_0 = \sigma \cup \sigma^{-1} \cup \Delta$.

Se $B \in \sigma$, então $F_A \in J$. Se $B = (v,v') \in \sigma^{-1}$, então

$$F_A = X^w(X^v - X^{v'}) = -X^w(X^{v'} - X^v) = -X^w F_{A'}$$

com $A' = (v', v) \in \sigma$ e $F_{A'} \in J$. Logo $I \subseteq J$.

Portanto $I = J$. □

Proposição 2.2.8 : *Seja $\sigma = \{A_1, \ldots, A_m\}$, onde $A_i \in \rho$ para $i = 1, \ldots, m$. Então as seguintes condições são equivalentes:*

1. $\rho = \overline{\sigma}$.

2. $I_S = (F_{A_1}, \ldots, F_{A_m})$.

Dem. : **(1 $\Rightarrow$ 2)** Se $A \in \rho$, então $F_A = \sum F_{B_i}, B_i \in \sigma_1$. De fato, como ρ é fecho transitivo de σ_1, temos que se $A = (v, w) \in \rho$, então existem $v_0, \ldots, v_l \in F$ tais que $v = v_0$ e $w = v_l$, com $B_i = (v_i, v_{i+1}) \in \sigma_1 \subset \rho$. Assim,

$$\sum F_{B_i} = \sum_{i=1}^{l} X^{v_i} - X^{v_{i+1}} = X^{v_0} - X^{v_l} = X^v - X^w = F_A.$$

Logo $(\{F_A\}_{A \in \rho}) \subseteq (\{F_A\}_{A \in \sigma_1})$.

Por outro lado temos $(\{F_A\}_{A \in \sigma_1}) \subseteq (\{F_A\}_{A \in \rho})$, pois $\rho = \overline{\sigma}$ e assim $(\{F_A\}_{A \in \sigma_1}) = (\{F_A\}_{A \in \rho})$. Agora pela proposição 2.2.6 e pelo lema 2.2.7 segue que $I_S = (F_{A_1}, \ldots, F_{A_m})$.

(2 $\Rightarrow$ 1) Sabemos que $(F_{A_1}, \ldots, F_{A_m}) = (\{F_A\}_{A \in \overline{\sigma}})$, pois $\overline{\sigma}$ é o fecho transitivo de σ_1.

Sejam $S' = \mathbb{N}^n/\overline{\sigma}$ e $\sigma^* : \mathbb{N}^n \longrightarrow S'$ o epimorfismo canônico, então

$$0 \longrightarrow (F_{A_1}, \ldots, F_{A_m}) \longrightarrow R[X_1, \ldots, X_n] \xrightarrow{\Gamma'} R[S'] \longrightarrow 0$$

é uma sequência exata, pois por 2.2.6 $I_{S'} = (\{F_A\}_{A \in \overline{\sigma}})$. Logo temos $I_S = (F_{A_1}, \ldots, F_{A_m}) = I_{S'}$.

Portanto, se $A \in \rho$, $A = (v, w)$ então $\Gamma'(F_A) = x_{\sigma^*(v)} - x_{\sigma^*(w)} = 0$. Logo $\sigma^*(v) = \sigma^*(w)$ ou, equivalentemente, $A \in \overline{\sigma}$ e portanto $\rho = \overline{\sigma}$. □

Corolário 2.2.9 : *Um semigrupo aditivo finitamente gerado é finitamente apresentado.*

Dem. : Sejam S um semigrupo aditivo gerado por n elementos e k um corpo. O epimorfismo $\rho^* : \mathbb{N}^n \longrightarrow S$ induz o epimorfismo $k[X_1, \ldots, X_n] \xrightarrow{\Gamma} k[S]$, onde $k[S]$ é o anel de semigrupo de S sobre k.

Como k é um corpo, temos, pelo Teorema das Bases de Hilbert, que $k[X_1 \ldots, X_n]$ é um anel Noetheriano. Logo o núcleo do homomorfismo Γ, que denotaremos por I_S, é finitamente gerado.

Agora, $I_S = (\{F_A\}_{A \in \rho})$ pela proposição 2.2.6, assim $I_S = (F_{A_1}, \ldots, F_{A_m})$, com $A_i \in \rho$ para todo $i = 1, \ldots, m$.

Seja $\sigma = \{A_1, \ldots, A_m\}$. Pela proposição 2.2.8, temos que $\rho = \overline{\sigma}$, ou seja, ρ é uma congruência finitamente gerada. Logo, $S \cong F/\rho$, onde F é livre e ρ é finitamente gerada, e então, pela definição, S é finitamente apresentado. □

A nossa próxima definição é a de posto de uma congruência ρ e a partir dela vamos apresentar um resultado que relaciona o posto de ρ com a dimensão de S, onde S é o semigrupo que ela determina.

Definição 2.2.10 *Sejam F um semigrupo livre finitamente gerado e $\rho \subseteq F \times F$ uma congruência finitamente gerada. O posto de ρ é definido como sendo o número de elementos de um conjunto mínimo de geradores de ρ.*

Definição 2.2.11 *Sejam $S = F/\rho$, com F livre e $\rho \subseteq F \times F$ uma congruência. Para $A \in \rho, A = (v, v')$, nós definimos $w_A = v - v' \in \tilde{F}$. O conjunto $M_\rho(S) = \{w_A \mid A \in \rho\}$ é um subgrupo de $\tilde{F}$ e é chamado o módulo de relações de S com releção a ρ.*

É fácil ver que $\tilde{S} \cong \tilde{F}/M_\rho(S)$.

Proposição 2.2.12 *: Se F é um semigrupo livre e finitamente gerado e ρ uma congruência finitamente gerada de F e $S = F/\rho$, então $postop \geq postoS - dimS$.*

Dem. : Seja $\sigma = \{A_1, \ldots, A_r\}$, com $A_i \in \rho$ para $i = 1, \ldots, r$ e suponhamos que $\rho = \overline{\sigma}$, então $\{w_{A_i}\}, i = 1, \ldots, r$ gera $M_\rho(S)$ e portanto $postoM_\rho(S) \leq postop$.

Do fato de que $\tilde{S} \cong \tilde{F}/M_\rho(S)$ e da definição do posto de um grupo temos que $postoS = postoF - postoM_\rho(S)$. Também, $postoF \geq postoS$, pois F é livre e $\rho^* : F \longrightarrow S$ é homomorfismo sobrejetor.

Portanto, $dimS \geq postoS - postop$. □

2.3 Semigrupo Simétrico

Neste parágrafo, vamos trabalhar com uma classe especial de semigrupos.

Definição 2.3.1 *: Seja S um semigrupo de inteiros positivos. S é chamado semigrupo numérico, se para algum $m \in I\!N$ temos $m + \dot{I\!N} \subseteq S$.*

Dados $a_1, \ldots, a_n \in I\!N$, $(a_1, \ldots, a_n)$ denotará o máximo divisor comum e $[a_1, \ldots, a_n]$ denotará o mínimo múltiplo comum de $\{a_1, \ldots, a_n\}$.

Proposição 2.3.2 *: Seja S um semigrupo finitamente gerado por $\{a_1, \ldots, a_n\} \subseteq I\!N$, tal que $(a_1, \ldots, a_n) = 1$. Então S é um semigrupo numérico.*

Dem. : Seja $S =< a_1, \ldots, a_n >$, onde $(a_1, \ldots, a_n) = 1$, então $1 = a_1k_1 + \cdots + a_nk_n$, com $k_i \in \mathbb{Z}$, para $i = 1, \ldots, n$. Depois de uma reenumeração, se necessário, podemos supor que $1 \leq a_1 < \cdots < a_n$.

Para todo $z \in \mathbb{Z}$, temos $z = a_1b_1 + \cdots + a_nb_n$, com $b_i \in \mathbb{Z}$. Dividindo b_j por a_n obtemos $b_j = q_ja_n + r_j$, onde $q_j \in \mathbb{Z}$ e $0 \leq r_j < a_n$ para $j = 1, \ldots, n-1$. Logo, $z = \sum_{j=1}^{n-1} a_jr_j + a_n(b_n + \sum_{j=1}^{n-1} a_jq_j)$.

Temos que $0 \leq \sum_{j=1}^{n-1} a_jr_j < (\sum_{j=1}^{n} r_j)a_n < (n-1)a_n^2$. Portanto, se tomarmos $z \geq (n-1)a_n^2$ teremos $z > \sum_{j=1}^{n-1} a_jr_j$, logo $z - \sum_{j=1}^{n-1} a_jr_j > 0$, assim,

$$a_n(b_n + \sum_{j=1}^{n-1} a_jq_j) = z - \sum_{j=1}^{n-1} a_jr_j > 0.$$

Chamemos $b_n + \sum_{j=1}^{n-1} a_jq_j = r_n > 0$ e portanto $z = \sum_{j=1}^{n-1} a_jr_j + a_nr_n \in < a_1, \ldots, a_n >$.

Logo, acabamos de mostrar que para todo $z \geq (n-1)a_n^2$, tem-se $z \in S$, isto é, S for numérico. □

Proposição 2.3.3 : *Todo semigrupo numérico é finitamente gerado.*

Dem. : Como S é semigrupo numérico, existem $a, b \in S$ tais que $(a, b) = 1$, logo $< a, b >$ é um semigrupo numérico por 2.3.2, então seja $m_0 \in \mathbb{N}$ tal que $m_0 + \dot{\mathbb{N}} \subseteq < a, b >$.

Afirmamos que $S = (S \cap [0, m_0)) \cup [m_0, \infty)$.

Que $S \subseteq (S \cap [0, m_0)) \cup [m_0, \infty)$ é claro, pois se $s \in S$, então $s \leq m_0$ ou $s \geq m_0$. Logo $s \in (S \cap [0, m_0)) \cup [m_0, \infty)$. Reciprocamente, seja $d \in (S \cap [0, m_0)) \cup [m_0, \infty)$. Se $d \in (S \cap [0, m_0))$, então $d \in S$. Se $d \in [m_0, \infty)$, então $d \geq m_0$, logo $d \in < a, b > \subseteq S$.

Assim, S é finitamente gerado por $\{S \cap [0, m_0), a, b\}$, pela afirmação acima e por $(S \cap [0, m_0))$ ser finito e $[m_0, \infty) \subseteq < a, b >$ ser finitamente gerado. □

Proposição 2.3.4 : *Seja $n_1, \ldots, n_l \in \mathbb{N}$ com $(n_1, \ldots, n_l) = 1$. Suponhamos que $[(n_1, \ldots, n_i), n_{i+1}] \in < n_1, \ldots, n_i >$ para $i = 1, \ldots, l-1$. Então,*

$$m = \sum_{i=1}^{l-1} [(n_1, \ldots, n_i), n_{i+1}] - \sum_{i=1}^{l} n_i$$

é o maior inteiro não pertencente a $S =< n_1, \ldots, n_l >$. Mais ainda: dado $z \in \mathbb{Z}$, $z \in S$ se, e somente se, $m - z \notin S$.

Dem. : Seja $c_i = \frac{(n_1, \ldots, n_{i-1})}{(n_1, \ldots, n_i)}$, para $i = 2, \ldots, l$, então usando propriedade de máximo divisor e mínimo multiplo comum, temos $[(n_1, \ldots, n_i), n_{i+1}] = c_{i+1}n_{i+1}$, mas por hipótese $c_{i+1}n_{i+1} \in < n_1, \ldots, n_i >$, logo $[(n_1, \ldots, n_i), n_{i+1}] = c_{i+1}n_{i+1} = \sum_{j=1}^{i} r_{ij}n_j$ (*), onde $r_{ij} \in \mathbb{N}$ e c_i divide n_j para todo $i > j$.

Do fato, de $(n_1, \ldots, n_l) = 1$ sabemos que dado $z \in \mathbb{Z}$, $z = \sum_{i=1}^{l} b_i n_i$, $b_i \in \mathbb{Z}$.

Afirmação 1: Dado $z \in \mathbb{Z}$, $z = \sum_{i=1}^{l} a_i n_i$, onde para todo $i \geq 2$ tem-se $0 \leq a_i < c_i$.

dem.: Suponhamos primeiro que $z = b_1 n_1 + b_2 n_2$, então, tomando-se $b_2 = q_2 c_2 + a_2$, $0 \leq a_2 < c_2$, temos que $z = b_1 n_1 + q_2 c_2 n_2 + a_2 n_2$. Mas $c_2 n_2 = r_{11} n_1$, por (*), assim $z = (b_1 + q_2 r_{11}) n_1 + a_2 n_2$, com $0 \leq a_2 < c_2$.

Agora assumamos que dado $2 \leq k < l$ e $\overline{z} = \sum_{i=1}^{k} b_i n_i$, então $\overline{z} = \sum_{i=1}^{k} a_i n_i$, com $0 \leq a_i < c_i$ para todo $i \geq 2$.

Tomemos $z = \sum_{i=1}^{k+1} b_i n_i$, assim $z = \sum_{i=1}^{k} b_i n_i + b_{k+1} n_{k+1}$, mas $b_{k+1} = q_{k+1} c_{k+1} + a_{k+1}$ com $0 \leq a_{k+1} < c_{k+1}$, logo $z = \sum_{i=1}^{k} b_i n_i + q_{k+1} n_{k+1} c_{k+1} + a_{k+1} n_{k+1}$, agora usando (*) temos que $z = \sum_{i=1}^{k} (b_i + a_{k+1} r_{ki}) n_i + a_{k+1} n_{k+1} = \overline{z} + a_{k+1} n_{k+1}$. Mas por hipótese (de indução) $\overline{z} = \sum_{i=1}^{k} a_i n_i$, com $0 \leq a_1 < c_i$ se $i \geq 2$, isto é, $z = \sum_{i=1}^{k+1} a_i n_i$, com $0 \leq a_1 < c_i$ se $i \geq 2$. Portanto, por indução, temos o que queríamos.

Afirmação 2: Se $z = \sum_{i=1}^{l} a_i n_i$, com $0 \leq a_1 < c_i$ se $i \geq 2$, então $z \in S$ se, e só se, $a_1 \geq 0$.

dem.: É claro que se $a_1 \geq 0$ temos $z \in S$. Agora suponhamos que $z \in S$ e $a_1 < 0$. Como $z \in S$, temos que $z = \sum_{i=1}^{l} b_i n_i$, com $b_i \geq 0$, para $i = 1, \ldots, l$. Consideremos agora que $J = \{j;\ 2 \leq j \leq l \text{ e } b_j > c_j\}$, assim para todo $j \in J$ temos $b_j n_j = (b_j - c_j) n_j + c_j n_j$. Logo, trocando z por $z' = z - \sum_{j \in J} (b_j - c_j) n_j$ temos ainda que $z' \in S$ e $z' = \sum_{i=1}^{l} b_i$, com $b_1 \geq 0$ e $0 \leq b_i \leq c_i$ se $i \geq 2$. Mais ainda: ao escrevermos $z' = \sum_{i=1}^{l} a'_i n_i$ com $0 \leq a'_i < c_i$ se $i \geq 2$, temos que $a_1 = a'_1$, isto é, na verdade podemos supor que $z = \sum_{i=1}^{l} b_i n_i$, com $0 \leq b_i \leq c_i$ se $i \geq 2$. Portanto $z = \sum_{i=1}^{n} a_i n_i = \sum_{i=1}^{l} b_i n_i$ e obtemos que $\sum_{i=2}^{l} r_i n_i = r_1 n_1 \neq 0$, com $|r_i| < c_i$ para $i = 2, \ldots, l$, pois $r_i = a_i - b_i$.

Seja k o menor inteiro tal que $r_k \neq 0$. Como c_i divide n_j, para todo $i > j$, segue que $r_k \frac{n_k}{\prod_{i>k} c_i} \equiv 0 \bmod c_k$. Como $(\frac{n_k}{\prod_{i>k} c_i}, c_k) = (\frac{n_k}{(n_1, \ldots, n_k)}, \frac{(n_1, \ldots, n_{k-1})}{(n_1, \ldots, n_k)}) = 1$, nós encontramos $r_k \equiv 0 \bmod c_k$. Uma contradição, pois $|r_k| < c_k$.

Afirmação 3: Dado $z \in \mathbb{Z}$, $z \in S$ se, e só se $m - z \notin S$.

dem.: De fato, temos $m - z = (-1 - a_1) n_1 + \sum_{i=2}^{l} (c_i - a_i - 1) n_i$; segue, pela afirmação2, que $z \in S$ se, e somente se, $a_1 \geq 0$, isto é, se, e só se, $(-1 - a_1) < 0$ se, e somente se $m - z \notin S$.

Afirmação 4: m é o maior inteiro não pertencente a S.

dem.: De fato, $m = m - 0$, então $a_1 = 0$, logo $m \notin S$. Agora tomemos $z = m + k$, com $k \geq 1$, assim $m - (m + k) = -k \notin S$, portanto $z \in S$, como queríamos. □

A proposição 2.3.4 dá origem a uma definição geral.

Definição 2.3.5 : *Um semigrupo S é chamado simétrico, se existe $m \in \tilde{S}$ tal que, dado $s \in \tilde{S}$, temos $s \in S$ se, e somente se, $m - s \notin S$.*

Observação 2.3.6 :

1. Se $S \subseteq I\!N$, então m, na definição de semigrupo simétrico, é o maior inteiro não pertencente a S.

   De fato, sejam S um semigrupo simétrico, $m \in \tilde{S}$ como na definição e m' o maior inteiro não pertencente a S. É claro que $m \notin S$, pois $m = m - 0 \notin S$. Se $m \neq m'$, então $m - m' < 0$, logo $m - m' \notin S$. Mas então $m' \in S$, que é uma contradição. Portanto $m = m'$.

2. A proposição 2.3.4 não determina todos os semigrupos simétricos de inteiros. Como, por exemplo, o semigrupo S gerado por $\{5, 6, 7, 8\}$.

   Temos que $S =< 5, 6, 7, 8 >$ não satisfaz as hipóteses de 2.3.4, pois $[(5, 6), 7] = 7 \notin < 5, 6 >$. No entanto, S é simétrico, pois $S = \{5, 6, 7, 8, 10, 11, \ldots\}$ e $m = 9$ satisfaz as condições da definição 2.3.5. Que $n \in S$ com $n \geq 10$ pode se ver da seguinte forma: se $n \geq 10$, então $n = 5k + r$, $k \geq 2$ e $0 \leq r \leq 4$. Agora para $r = 0$ já temos $n \in S$, se $1 \leq r \leq 3$ temos $n = 5(k-1) + 5 + r$, com $5 + r \in \{6, 7, 8\}$ e de novo $n \in S$, para $r = 4$ temos $n = 5(k-2) + (5+1) + (5+3)$ e $n \in S$.

3. Se S é um semigrupo numérico, então $M = S - \{0\}$ é o ideal maximal de S e chamamos $M^- = \{z \in \mathbb{Z} \mid z + M \subseteq S\}$.

O próximo resultado dá outras caracterizações de um grupo simétrico.

Proposição 2.3.7 : *Seja S um semigrupo numérico, então as seguintes condições são equivalentes:*

1. *S é simétrico.*
2. *$M^- = \{m\} \cup S$, onde m é o maior inteiro não pertencente a S.*
3. *Cada ideal principal próprio de S é irredutível, isto é, se $s \in S$, $s \neq 0$, então o ideal (s) não pode ser escrito como a interseção de dois ideais em S, ambos contendo propriamente (s).*
4. *Existe um ideal principal próprio de S que é irredutível.*

Dem. : (1 $\Rightarrow$ 2) Seja $z \in M^-$ com $z \notin S$. Se $z \neq m$, então $m - z \in M$, pois S é simétrico e portanto, como $z \notin S$, tem-se $z + M \not\subseteq S$; absurdo, já que $z \in M^-$.

(2 $\Rightarrow$ 1) Suponhamos que S não é simétrico, então existe um maior inteiro $m_1 \notin S$ tal que $m - m_1 \notin S$.

Afirmamos que $M^- \supseteq \{m_1, m\} \cup S$. De fato, suponhamos que $m_1 \notin M^-$, então existe $s \in M$ tal que $m_1 + s \notin S$. Pela definição de m_1, segue que $m - m_1 - s \in S$. Portanto, $m - m_1 = (m - m_1 - s) + s$ é um elemento de S, o que é uma contradição.

Assim, se S não é simétrico, temos que $M^- \supsetneq \{m\} \cup S$ como queríamos.

(1 $\Rightarrow$ 3) Se (s) é um ideal principal e $s_1 \in S$ é tal que $s_1 \notin (s)$, então $s + m \in (s_1)$, de fato, como $s_1 \notin (s)$, segue que $s_1 - s \notin S$ e portanto $m - (s_1 - s) \in S$, pois S é simétrico. Logo $(m + s) - s_1 \in S$, ou equivalentemente $m + s \in (s_1)$.

Suponhamos agora que (s) é redutível, então existem $s_1, s_2 \in S$, $s_1, s_2 \notin (s)$ tais que $(s_1) \cap (s_2) \subseteq (s)$. Portanto, da afirmação acima, segue que $s + m \in (s_1) \cap (s_2)$, no entanto $s+m \notin (s)$, pois caso contrário $s+m-s \in S$, logo $m \in S$, o que é uma contradição.

(3 $\Rightarrow$ 4) É óbvia.

(4 $\Rightarrow$ 1) Nós mostraremos que se S não é simétrico, então cada ideal principal é redutível.

Afirmamos que se (s) é ideal principal próprio, então $(s) = (s, s + m) \cap (s, s + m_1)$, onde m é o maior inteiro não pertencente a S e m_1 é o maior inteiro não pertencente a S tal que $m - m_1 \notin S$.

De fato, é suficiente mostrar que $(s+m) \cap (s+m_1) \subseteq (s)$. Seja $s' \in (s+m) \cap (s+m_1)$, então $s' = s + m + s_1 = s + m_1 + s_2$, com $s_1, s_2 \in S$. Primeiro suponhamos $s_1 = 0$, então $m - m_1 \notin S$, uma contradição.

Portanto $s_1 > 0$ e isto implica que $m + s_1 \in S$ e assim $s' \in (s)$.

Pela definição de m e m_1, segue que $s + m_1 \in S$ e $s + m \in S$. Então $(s, s + m)$ e $(s, s + m_1)$ contêm (s) propriamente. Logo $(s) = (s, s + m) \cap (s, s + m_1)$, isto é , (s) é redutível, absurdo. Portanto S é simétrico. □

2.4 Interseção Completa

No que segue, consideraremos somente subsemigrupos finitamente gerados de $\mathbb{Z}^m = \{v = (z_1, \ldots, z_m) \mid z_i \in \mathbb{Z}\}$.

Sejam $v_1, \ldots, v_n \in \mathbb{Z}^m$ geradores de S e k um corpo algebricamente fechado. O anel de semigrupo $k[S]$ de S sobre k é isomorfo a $k[T^{v_1}, \ldots, T^{v_n}]$, onde $T^{v_i} = \prod_{j=1}^{m} T_j^{z_{ij}}$, $v_i = (z_{ij})$ para todo $i = 1, \ldots, n$ e $\{T_1, \ldots, T_m\}$ é um conjunto algebricamente independente sobre k. De fato, numa representação $S \cong \mathbb{N}^n/\rho$ e sendo J o núcleo do epimorfismo $\Gamma : k[X_1, \ldots, X_n] \longrightarrow k[T^{v_1}, \ldots, T^{v_n}]$, $\Gamma(X_i) = T^{v_i}$ para $i = 1, \ldots, n$, observaremos que $J = I_S = (F_A, A \in \rho)$, por 2.2.6, assim $k[S]$ é isomorfo a $k[T^{v_1}, \ldots, T^{v_n}]$.

Consideremos $V_S = \{(x_1, \ldots, x_n) \mid x_i \in k,\ f(x_1, \ldots, x_n) = 0, \forall\ f \in I_S\}$, nosso próximo resultado diz respeito à dimensão da variedade V_S.

Proposição 2.4.1 : *V_S é uma variedade irredutível e $dim V_S = dim S$.*

Dem. : Lembramos que V_S é irredutível se, e só se, o seu ideal $I(V_S)$ é primo, pela proposição 1.3.5. Agora, por k ser algebricamente fechado, temos $I(V_S) = \sqrt{I_S}$, mas I_S é primo e assim $I(V_S) = I_S$.

Agora, vamos mostrar que $dim V_S = dim S$. Sejam $S =< v_1, \ldots, v_n >$ e $\tilde{S}$ o seu grupo associado. Sabemos que o posto de $\tilde{S}$ é o número máximo de vetores $\mathbb{Z}$-linearmente independentes em $\{v_1, \ldots, v_n\}$. Chamando $r = posto\, \tilde{S}$, podemos supor, sem perda de generalidade, que $\{v_1, \ldots, v_r\}$ é $\mathbb{Z}$-linearmente independente.

Sabemos que $k[S] \cong k[T^{v_1}, \ldots, T^{v_n}] \cong k[X_1, \ldots, X_n]/I_S$, que é um domínio.

Chamemos $A = k[T^{v_1}, \ldots, T^{v_r}]$ e consideremos $K = c.f.(A)$ (corpo de frações de A) e $L = c.f.(k[T^{v_1}, \ldots, T^{v_r}])$, onde $k[T^{v_1}, \ldots, T^{v_r}] \subseteq A$.

Afirmação 1: A extensão $K \mid L$ é algébrica.

dem.: Considerando-se $\{v_{r+1}, v_1, \ldots, v_r\} \subset \mathbb{Z}^m$, temos que estes elementos são linearmente dependentes, isto é, $a_{r+1}v_{r+1} + a_1'v_1 + \cdots + a_r'v_r = 0$, com $a_{r+1}, a_i' \in \mathbb{Z}^m$, $i = 1, \ldots, r$ não todos nulos. Podemos supor $a_{r+1} > 0$, pois $v_1, \ldots, v_r$ são linearmente independentes, logo $a_{r+1}v_{r+1} = a_1v_1 + \cdots + a_rv_r$, com $a_i \in \mathbb{Z}^m$, $i = 1, \ldots, r+1$. Assim, $(T^{v_{r+1}})^{a_{r+1}} = T^{a_1v_1} \ldots T^{a_rv_r}$.

Logo, $T_{v_{r+1}}$ é raiz do polinômio $f(Y) = Y^{a_{r+1}} - \prod_{i=1}^{r} T^{a_iv_i} \in L$. Portanto $T^{v_{r+1}}$ é algébrico sobre L e logo fazendo de modo análogo para $v_{r+1}, \ldots, v_n$, temos que $K \mid L$ é algébrica.

Afirmação 2: $T^{v_1}, \ldots, T^{v_r}$ são algebricamente independentes.

dem.: Seja $f \in k[Y_1, \ldots, Y_r]$, então $f(Y_1, \ldots, Y_r) = \sum_I a_I (Y_1)^{i_1} \ldots (Y_r)^{i_r}$, $I = (i_1, \ldots, i_r)$.

Temos que $f(T^{v_1}, \ldots, T^{v_r}) = 0$ se, e somente se, $\sum_I a_I (T^{v_1})^{i_1} \ldots (T^{v_r})^{i_r} = 0$. Como $v_1, \ldots, v_r$ são linearmente independentes, temos que, dado $I = (i_1, \ldots, i_r)$ não existe $J = (j_1, \ldots, j_r)$ diferente de I tal que $(T^{v_1})^{i_1} \cdots (T^{v_r})^{i_r} = (T^{v_1})^{j_1} \cdots (T^{v_r})^{j_r}$ e assim segue que $a_I = 0$, para todo I. Logo $f = 0$ e a afirmação está provada.

Logo, das afirmações 1 e 2, segue que o grau de transcendência de $K \mid k$ é r e, pelo Teorema da Normalização de Noether, temos que $dim\, A = r = posto\, \tilde{S} = dim\, S$, isto é, $dim V_S = dim S$. □

A proposição a seguir nos dá uma condição necessária para que, dado um conjunto de geradores de um ideal homogêneo $\mathfrak{a}$ de um anel comutativo possamos escolher um conjunto mínimo de geradores de $\mathfrak{a}$.

Proposição 2.4.2 : *Seja $S \subset \mathbb{Z}^m$ um semigrupo finitamente gerado e suponha que S não tenha elementos invertíveis. Seja $R = \oplus_{s \in S} R_s$ um anel S-graduado, com R_0 um corpo. Então, para um ideal homogêneo $\mathfrak{a}$ de R, dado um conjunto homogêneo de*

geradores de $\mathfrak{a}$, podemos escolher um conjunto mínimo de geradores de $\mathfrak{a}$.

Dem. : Como S não tem elementos invertíveis, temos que $\mathfrak{p} = \oplus_{s\in S, s\neq 0} R_s$ é realmente um ideal de R e por $R/\mathfrak{p} = R_0$ ser um corpo, temos que $\mathfrak{p}$ é um ideal primo. Logo $R_{\mathfrak{p}}$ é um anel local.

Seja $\mathfrak{a} \subseteq \mathfrak{p}$ um ideal finitamente gerado por $\{a_1, \ldots, a_n\}$, onde a_i, para $i = 1, \ldots, n$ são elementos homogêneos, então $\mathfrak{a}R_{\mathfrak{p}}$ é finitamente gerado pelo conjunto de elementos homogêneos $B = \{a_1/1, \ldots, a_n/1\}$ em $R_{\mathfrak{p}}$.

Pelo Lema de Nakayma, podemos escolher um conjunto mínimo de geradores de $\mathfrak{a}R_{\mathfrak{p}}$ entre os elementos do conjunto de geradores B. Seja $B' = \{a_1, \ldots, a_m\}$ esse conjunto, onde $n \geq m$.

Vamos mostrar que este conjunto é um conjunto global de geradores de $\mathfrak{a}$.

Seja $x = d_{s_0} \in \mathfrak{a}$ um elemento homogêneo; temos que $x = \sum_{i=1}^{n} a_i r_i$, onde $r_i \in R$ e $a_i \in \{a_1, \ldots, a_n\}$, logo, $x/1 = \sum_{i=1}^{n} a_i r_i/1$ e assim existe $b \in R \setminus \mathfrak{p}$, $b = b_0 + \sum_{s\in S,\, s\neq 0} b_s$, $b_0 \neq 0$, tal que $xb = \sum_{i=1}^{n} a_i u_i$, $u_i \in R$.

Agora, como $u_i \in R$, temos que $u_i = u_{s'} + \sum_{s\neq s'} u_s$, onde s' é tal que $s' + s_i = s_0$, u_s é homogêneo de grau s e s_i é o grau de a_i. Assim, $\sum_{i=1}^{m} a_i u_i = \sum_{i=1}^{m} a_i u_{s_i} + \sum_{i=1}^{m} a_i \sum_{s\neq s'} u_s$ e temos que a segunda parcela do lado direito dessa igualdade tem grau diferente de s_0.

Logo, $xb_0 = \sum_{i=1}^{m} a_i u_{s'}$. Como R_0 é corpo e $b_0 \neq 0$ pertence a R_0, segue que $x = \sum_{i=1}^{m} a_i l_i$, com $l_i \in R$.

Portanto, $\{a_1, \ldots, a_m\}$ é um conjunto mínimo de geradores de $\mathfrak{a}$. □

Como conseqüência da proposição anterior, temos a iguadade entre o posto da congruência ρ e o número de elementos do conjunto mínimo de geradores de I_S.

Corolário 2.4.3 : *Se $S \subseteq \mathbb{Z}^m$ não tem elementos invertíveis, então $posto\rho = \mu(I_S)$.*

Dem. : Escolhida uma representação de $S = \mathbb{N}^n/\rho$, onde $n = posto\, S$, temos que $k[S] \cong k[X_1, \ldots, X_n]/I_S$, onde $I_S = (\{F_A\}_{A\in\rho})$ é um ideal homogêneo. Pela proposição 2.4.2, podemos escolher $\sigma = \{F_{A_1}, \ldots, F_{A_l}\} \subseteq \{F_A \mid A \in \rho\}$ tal que σ é um conjunto mínimo de geradores de I_S. Logo $\mu(I_S) = l$. Pela proposição 2.2.8, temos que $\rho = \overline{\sigma}$ e então $post o\rho \leq l = \mu(I_S)$.

Por outro lado, também pela proposição 2.2.8, dada uma congruência ρ, temos que $\mu(I_S) \leq post o\rho$. Portanto, $post o\rho = \mu(I_S)$, como queríamos. □

A nossa próxima definição é a de semigrupo que é interseção completa. Evidentemente, essa definição vem do fato de que a variedade algébrica associada a um semigrupo desse tipo é interseção completa, conforme a definição 1.7.4. Tal fato é apresentado no corolário 2.4.5.

Definição 2.4.4 : *Dizemos que um semigrupo S é uma interseção completa, se S pode ser representado como $S = F/\rho$, onde F é livre e ρ é uma congruência tal que $postO\rho = postoS - dimS$.*

Corolário 2.4.5 : *Se $S \subseteq \mathbb{Z}^m$ não tem elementos invertíveis, então as seguintes condições são equivalentes:*

1. *S é uma interseção completa.*

2. *V_S é interseção completa.*

3. *V_S é, na origem, uma interseção completa.*

Dem. : (1 $\Rightarrow$ 2) Se S é uma interseção completa, então $S = F/\rho$, onde F é livre e ρ é uma congruência tal que $postO\rho = postoS - dimS$. Pelo corolário 2.4.3, temos $\mu(I_S) = postoS - dimS$.

Agora $I_S = I(V_S)$, logo $\mu(I(V_S)) = postoS - dimS = n - dimV_S$. Portanto, V_S é gerado por $n - dimV_S$ polinômios.

Logo V_S é uma interseção completa.

(2 $\Rightarrow$ 1) Como V_S é uma interseção completa, temos que $\mu(I_S) = postoS - dimS$. Pelo corolário 2.4.3, segue que $postO\rho = postoS - dimS$.

Portanto, S é uma interseção completa.

(2 $\Rightarrow$ 3) Temos que $I_S \subset (X_1, \ldots, X_n) = m$, onde $m \in Max(k[X_1, \ldots, X_n])$. Pela demonstração da proposição 2.4.2, temos que $\mu(I_S) = \mu(I_S k[X_1, \ldots, X_n]_m)$. Por hipótese, $\mu(I_S) = postoS - dimS$, logo $\mu(I_S k[X_1, \ldots, X_n]_m) = postoS - dimS$.

Por outro lado, $ht(I_S k[X_1, \ldots, X_n]_m) = ht(I_S)$ e

$$ht(I_S) = dimk[X_1, \ldots, X_n] - dimk[X_1, \ldots, X_n]/I_S$$

$$= postoS - dimV_S = postoS - dimS$$

Portanto, $\mu(I_S k[X_1, \ldots, X_n]_m) = ht(I_S k[X_1, \ldots, X_n]_m)$ e logo V_S é, na origem, uma interseção completa, de acordo com a definição 1.7.4.

(3 $\Rightarrow$ 2) Por hipótese, temos que $\mu(I_S k[X_1, \ldots, X_n]_m) = ht(I_S k[X_1, \ldots, X_n]_m)$. Agora $ht(I_S k[X_1, \ldots, X_n]_m) = ht(I_S) = postoS - dimS$. Assim, pela demonstração da proposição 2.4.2, segue que $\mu(I_S) = postoS - dimS$. Logo, pela definição, temos que V_S é uma interseção completa. □

Observação 2.4.6 : Dado S um semigrupo representado por $S = F/\rho$, onde F é livre e finitamente gerado, consideremos $S^* := \{\rho^*(v) \mid \exists\, w \neq v \in F, (v, w) \in \rho\}$. Afirmamos que:

1. S^* é um ideal de S.
   Com efeito, se $t \in S^*$ e $s \in S$, então $t = \rho^*(v)$ tal que existe $w \in F$, $w \neq v$ com $(v, w) \in \rho$, e $s = \rho^*(v')$, $v' \in F$. Assim, $t + s = \rho^*(v) + \rho^*(v') = \rho^*(v + v')$. Afirmamos que existe $w' \in F$, $w' \neq v + v'$ tal que $(v + v', w') \in \rho$. De fato, $w' = w + v'$, pois $v + v' \neq w + v'$, já que $v \neq w$ e $(v + v', w + v') \in \rho$, pois ρ é uma congruência.

2. $S^* = \{degF_A \mid A \in \rho\}$, onde $degF_A$ denota o grau de F_A com respeito a S-graduação em $k[X_1, \ldots, X_n]$. De fato, se $\rho^*(v) \in S^*$ então existe $w \neq v$ tal que $A = (v, w) \in \rho$. Logo, para $F_A = X^v - X^w$, temos $degF_A = \rho^*(v)$. Portanto, $S^* \subseteq \{degF_A \mid A \in \rho\}$. Reciprocamente, seja $degF_A = s = \rho^*(v) \in S$, como F_A é não nulo, temos que existe $w \neq v \in F$ tal que $A = (v, w) \in \rho$. Logo, $\rho^*(v) \in S^*$ e, portanto, $\{degF_A \mid A \in \rho\} \subseteq S^*$.

A próxima proposição nos dá uma relação entre o número de elementos do conjunto mínimo de geradores de I_S e de S^*.

Proposição 2.4.7 *O número de elementos, $\mu(S^*)$, de um conjunto mínimo de geradores de S^* é menor ou igual a $\mu(I_S)$.*

Dem. : Pela observação acima, temos que $S^* = \{degF_A \mid A \in \rho\}$. Seja $\rho = \overline{\sigma}$, onde $\sigma = \{A_1, \ldots, A_n\}$ e $A_i = (v_i, w_i) \in \rho$. Temos que $postO\rho = \mu(I_S)$.

Afirmamos que $\{degF_{A_i} \mid A_i \in \sigma\}$ gera S^*.

De fato, seja $A = (v, w) \in \rho$ então $A = (\sum_{i=1}^n m_i v_i, \sum_{i=1}^n m_i' w_i)$, $m_i, m_i' \in \mathbb{N}$, para $i = 1, \ldots, n$. Assim, $degF_A = \rho^*(v) = \rho^*(\sum_{i=1}^n m_i v_i) = \sum_{i=1}^n m_i \rho^*(v_i) = \sum_{i=1}^n m_i degF_{A_i}$.

Portanto, $\mu(S^*) \leq postO\rho = \mu(I_S)$. □

Corolário 2.4.8 : *Se V_S é uma interseção completa, então $\mu(S^*) \leq postoS - dimS$.*

Dem. : Por hipótese, temos que $\mu(I_S) = postoS - dimS$.

Pela proposição anterior $\mu(S^*) \leq \mu(I_S)$, e assim temos $\mu(S^*) \leq postoS - dimS$. □

Com a teoria desenvolvida até aqui, temos condições para justificar parte do exemplo dado no final do capítulo 1. É o que faremos no próximo exemplo.

Exemplo 2.4.9 : Usando o último resultado, podemos mostrar que a variedade V de $A^3(k)$ dada pela parametrização

$$X_1 \longrightarrow t^3$$
$$X_2 \longrightarrow t^4$$
$$X_3 \longrightarrow t^5$$

não é uma interseção completa.

Com efeito, considere o semigrupo $S =< 3, 4, 5 > \subseteq \mathbb{Z}$. Se V_S fosse uma interseção completa, teríamos, de acordo com 2.4.8, que $\mu(S^*) \leq postoS - dimS = 2$, pois $postoS = 3$ e $dimS = postoZ = 1$. No entanto, S^* não é gerado por dois elementos; na verdade, $S^* = (8, 9, 10)$. Isso pode ser visto da seguinte forma: $S^* = \{8, 9, 10, 11, \ldots\}$, que $n \in S^*$ com $n \geq 10$ façamos o seguinte: se $n \geq 10$ então $n = 8k + r$, com $k \geq 1$ e $0 \leq r \leq 7$. Agora, para $r = 0$ já temos $n \in S^*$, se $1 \leq r \leq 2$ temos $n = 8(k-1) + 8 + r$ com $8 + r = 9$ ou 10 e de novo $n \in S^*$, para $3 \leq r \leq 7$, temos $r \in S$ e logo, de acordo com a definição 2.1.12, segue que $n \in S^*$. Agora, usando o corolário 2.1.15 tem-se que $\mu(S^*) = 3$. Que o posto de S é 3 se deduz imediatamente pelo fato de que $S = \{3, 4, 5, 6, 7, \ldots\}$ e que $5 \notin < 3, 4 >$.

Capítulo 3

Curvas, em $A^3(k)$, Parametrizadas por Monômios

Neste capítulo, vamos desenvolver uma teoria sobre relações minimais de semigrupos gerados por três elementos e estudar as propriedades do conjunto dessas relações, denotado por $\mathcal{M}$. Usaremos tal teoria na demonstração do teorema que nos dá uma equivalência entre semigrupos simétricos e interseções completas. Faremos uma aplicação desse teorema à geometria algébrica, dando alguns exemplos de curvas parametrizadas em $A^3(k)$ que são e que não são interseções completas. Mais ainda: daremos exemplos que provam que um resultado análogo a este teorema não é verdadeiro para semigrupos gerados por mais de três elementos.

3.1 Relações Minimais

Dado um semigrupo numérico $S =< n_1, \ldots, n_t > \subset \mathbb{N}$, consideremos $\rho^* : \mathbb{N}^t \longrightarrow S$ o epimorfismo dado por $\rho^*(e_i) = n_i$, onde $\{e_i, \ldots, e_t\}$ é a base canônica de $\mathbb{N}^t$. Evidentemente, ρ^* pode ser estendido a um epimorfismo $\overline{\rho^*} : \mathbb{Z}^t \longrightarrow \tilde{S}$ de grupos. Ao núcleo de $\overline{\rho^*}$ chamamos o conjunto de relações de S determinadas por $\{n_1, \ldots, n_t\}$, isto é, uma tal relação é um elemento $z = (z_1, \ldots, z_t) \in \mathbb{Z}^t$ tal que $z_1 n_1 + \ldots + z_t n_t$. Quando o conjunto de geradores de S está fixado, vamos dizer apenas relação de S em vez de relação de S determinada por $\{n_1, \ldots, n_t\}$.

Ainda nesta situação, no capítulo anterior, definimos $M_\rho(S) = \{w_A \mid A \in \rho\}$, onde para $A = (v, v')$, $w_A = v - v'$. Lembrando ainda que dados $A \in \mathbb{N}^t \times \mathbb{N}^t$, $A = (v, v') \in \rho$ se, e só se, $\rho^*(v) = \rho^*(v')$, temos imediatamente que $M_\rho(S) = ker(\overline{\rho^*})$, isto é, $M_\rho(S) = \{(z_1, \ldots, z_t) \in \mathbb{Z}^t \mid \sum_{i=1}^t z_i n_i = 0\}$.

Neste capítulo, estaremos interessados em semigrupos numéricos gerados por três elementos; então, desde já, fixamos $S =< n_1, n_2, n_3 >$, com $n_i > 0$, $(n_1, n_2, n_3) = 1$ e $\rho^* : \mathbb{N}^3 \longrightarrow S$ o epimorfismo dado por $\rho^*(e_i) = n_i$, onde $\{e_1, e_2, e_3\}$ é a base canônica de $\mathbb{N}^3$ e $\rho = \{(v, v') \in \mathbb{N}^3 \times \mathbb{N}^3 \mid \rho^*(v) = \rho^*(v')\}$. Daqui em diante, a menos que seja dito

o contrário, estaremos referindo-nos a essa situação.

Lema 3.1.1 : *Se $v \in M_\rho(S)$, $v = (z_1, z_2, z_3) \neq 0$, então existe um $i_v \in \{1, 2, 3\}$, tal que :*

1. *$z_{i_v} > 0$ e $z_j \leq 0$, para $j \neq i_v$, ou*

2. *$z_{i_v} < 0$ e $z_j \geq 0$. para $j \neq i_v$.*

Dem. : De $v \in M_\rho(S)$, temos que $z_1 n_1 + z_2 n_2 + z_3 n_3 = 0$. Do fato de v ser não nulo, evidentemente, os inteiros z_1, z_2, z_3 não têm todos o mesmo sinal e portanto dois deles têm o mesmo sinal e o terceiro forçosamente é não nulo e tem o sinal contrário. □

Definição 3.1.2 : *Dado $v \in M_\rho(S)$, dizemos que v é do tipo i, $1 \leq i \leq 3$ se $i_v = i$, onde i_v é dado pelo Lema 3.1.1.*

Definição 3.1.3 : *Dizemos que $v = (z_1, z_2, z_3) \in M_\rho(S)$ é uma relação minimal do tipo i, se v é do tipo i e para todo $v' = (z_1', z_2', z_3') \in M_\rho(S)$ do tipo i, temos $|z_i'| \geq |z_i|$.*
Uma relação é dita minimal, se é minimal de algum tipo.

Denotamos o conjunto das relações minimais de $M_\rho(S)$ por $\mathcal{M}$. A seguir, damos uma maneira de se obter relações minimais. Por exemplo, se queremos relações minimais do tipo 1, tomemos $c_1 \in \dot{I\!N}$ tal que $c_1 n_1$ seja o menor múltiplo de n_1 para o qual existam $r_2, r_3 \in I\!N$ com $c_1 n_1 = r_2 n_2 + r_3 n_3$, isto é,

$$c_1 = min\{c \in \dot{I\!N} \mid cn_1 = r_2 n_2 + r_3 n_3,\ r_2, r_3 \in I\!N\}.$$

É claro que c_1 existe, pois se tomarmos $c = n_2$, $r_2 = n_1$ e $r_3 = 0$ vemos que o conjunto acima é não- vazio.

Afirmamos que $v = (-c_1, r_2, r_3)$ é uma relação minimal do tipo 1. De fato, seja $v' = (a_1, a_2, a_3)$ uma relação do tipo 1, então:

a) $a_1 > 0$ e $a_2, a_3 \leq 0$, ou

b) $a_1 < 0$ e $a_2, a_3 \geq 0$.

No caso **a)** temos $a_1 n_1 = -(a_2 n_2 + a_3 n_3)$, com $-a_2, -a_3 \in I\!N$, assim, $c_1 \leq a_1$.
No caso **b)** temos $-a_1 n_1 = a_2 n_2 + a_3 n_3$, onde $-a_1 n_1 > 0$ e $c_1 \leq -a_1 = |a_1|$.
Analogamente, construímos relações minimais do tipo 2 e do tipo 3.

Proposição 3.1.4 : *Se $v' = (a_1, a_2, a_3) \in \mathcal{M}$ é uma relação minimal do tipo i, então $a_i = \pm c_i$, onde c_i é da forma descrita acima.*

Dem. : Faremos a demonstração para $v = (a_1, a_2, a_3) \in \mathcal{M}$ uma relação do tipo 1, assim temos que $|a_1| \leq |c_1|$. Por outro lado, temos que $v = (-c_1, r_2, r_3)$ é minimal do tipo 1, pelo que foi feito acima,então $|c_1| \leq |a_1|$.

Portanto $|a_1| = |c_1|$. □

A partir dessa proposição vemos que $\mathcal{M}$ é finito, pois, por exemplo, de $c_1 n_1 = r_2 n_2 + r_3 n_3$, com $r_2, r_3 \in I\!N$, temos $0 \leq r_2 \leq \frac{c_1 n_1}{n_2}$ e $0 \leq r_3 \leq \frac{c_1 n_1}{n_3}$. Um c_i dado acima é dito mínimo para as relações do tipo i.

Ilustramos com o exemplo abaixo a construção de relações minimais feita acima.

Exemplo 3.1.5 : Considerando o semigrupo $S =< 3, 4, 5 >$, vemos, de maneira simples, que $v_1 = (-3, 1, 1)$ é uma relação minimal do tipo 1; $v_2 = (1, -2, 1)$ é uma relação minimal do tipo 2 e $v_3 = (2, 1, -2)$ é uma relação minimal de tipo 3.

Voltando à situação inicial, consideremos v_1, v_2, $v_3 \in \mathcal{M}$, tais que $v_1 = (-c_1, r_{12}, r_{13})$, $v_2 = (r_{21}, -c_2, r_{23})$, $v_3 = (r_{31}, r_{32}, -c_3)$, são relações minimais do tipo 1, 2, 3 respectivamente e portanto $r_{ij} \geq 0$, $i, j \in \{1, 2, 3\}$, $i \neq j$. Distinguimos dois casos:

Caso I: $r_{ij} > 0$ para todo $i, j = 1, 2, 3$.

Caso II: Existem $i, j \in \{1, 2, 3\}$ tais que $r_{ij} = 0$.

As duas proposições a seguir são propriedades do caso I, que serão muito usadas no desenvolvimento deste capítulo.

Proposição 3.1.6 : *No caso I, temos* $v_1 + v_2 + v_3 = 0$.

Dem. : Seja $v = v_1 + v_2 + v_3 = (-c_1 + r_{21} + r_{31}, r_{12} - c_2 + r_{32}, r_{13} + r_{23} - c_3)$. Suponhamos que $v \neq 0$ e que v seja do tipo 1.

Se a primeira componente de v é menor que zero, isto é, $-c_1 + r_{21} + r_{31} < 0$, como c_1 é minimal para as relações do tipo 1, temos que $-c_1 + r_{21} + r_{31} \leq -c_1$, que é uma contradição, pois $r_{21} > 0$ e $r_{31} > 0$.

Se a primeira componente de v é maior que zero, isto é, $-c_1 + r_{12} + r_{31} > 0$, novamente, como c_1 é minimal para relações do tipo 1, temos $-c_1 + r_{12} + r_{31} \geq c_1$. Mas então $r_{21} \geq c_1$ ou $r_{31} \geq c_1$. Se supomos que $r_{21} \geq c_1$, então $v_1 + v_2 = (r_{21} - c_1, r_{12} - c_2, r_{13} + r_{23})$, onde $r_{21} - c_1 \geq 0$, $r_{13} + r_{23} > 0$ e $r_{12} - c_2 < 0$, é uma relação minimal do tipo 2. Como c_2 é minimal para as relações do tipo 2, temos $r_{12} - c_2 \leq -c_2$, ou seja, $r_{12} \leq 0$, que é uma contradição pois $r_{12} > 0$. Analogamente, se supomos $r_{31} \geq c_1$, teremos uma contradição com $r_{31} > 0$. Logo $v = 0$.

A prova é análoga se consideramos v do tipo 2 ou 3. □

A proposição seguinte descreve o conjunto de relações minimais para o caso I.

Proposição 3.1.7 : *No caso I,* $\mathcal{M} = \{\pm v_1, \pm v_2, \pm v_3\}$.

Dem. : Seja $v_1' = (-c_1, r_{12}', r_{13}')$ como no caso I, isto é, $r_{12}' > 0$ e $r_{13}' > 0$. Aplicando 3.1.6, obtemos $v_1' + v_2 + v_3 = 0$. Portanto, $v_1' = -(v_2 + v_3) = v_1$. Analogamente, mostra-se que v_2 e v_3 estão unicamente determinados. □

Na próxima proposição, consideremos $v_1 = (-c_1, r_{12}, r_{13})$, $v_2 = (r_{21}, -c_2, r_{23})$, $v_3 = (r_{31}, r_{32}, -c_3) \in \mathcal{M}$, com $r_{ij} \geq 0$ para $i, j = 1, 2, 3$, $i \neq j$.

Proposição 3.1.8 : *No caso II, temos:*

a) $\pm(0, -c_2, c_3) \in \mathcal{M}$, *ou*

b) $\pm(c_1, 0, -c_3) \in \mathcal{M}$, *ou*

c) $\pm(-c_1, c_2, 0) \in \mathcal{M}$.

Dem. : Seja $v_2 = (r_{21}, -c_2, r_{23}) \in \mathcal{M}$. Assumimos, sem perda de generalidade, que $r_{21} = 0$, assim $v_2 = (0, -c_2, r_{23})$.

Se $r_{23} = c_3$, então a afirmação é válida, isto é, $v_2 = (0, -c_2, c_3) \in \mathcal{M}$. Podemos supor então $r_{23} > c_3$, pois c_3 é minimal. Consideremos $v_2 + v_3 = (r_{31}, r_{32} - c_2, r_{23} - c_3)$. Como $r_{31} \geq 0$ e $r_{23} - c_3 > 0$, obtemos que $r_{32} - c_2 < 0$ e logo $v_2 + v_3$ é do tipo 2. Isto implica que $r_{32} - c_2 \leq -c_2$, logo $r_{32} \leq 0$, entretanto $r_{32} \geq 0$, portanto $r_{32} = 0$ e $r_{31} \geq c_1$.

Se $r_{31} = c_1$, então nossa afirmação segue novamente, isto é, $v_3 = (c_1, 0, -c_3) \in \mathcal{M}$. Assim, suponhamos que $r_{31} > c_1$, temos então que $v_1 + v_3 = (r_{31} - c_1, r_{12}, r_{13} - c_3)$ é uma relação do tipo 3, pois $r_{31} - c_1 > 0$ e $r_{12} \geq 0$, portanto $r_{13} - c_3 < 0$. Pela minimalidade de c_3, segue que $r_{13} - c_3 \leq -c_3$, logo $r_{13} = 0$.

Portanto, $v_1 = (-c_1, r_{12}, 0)$ e $r_{12} \geq c_2$. Se $r_{12} = c_2$, então $v_1 = (-c_1, c_2, 0) \in \mathcal{M}$ como queríamos. Se $r_{12} > c_2$ teremos $v_1 + v_2 + v_3 = (r_{31} - c_1, r_{12} - c_2, r_{23} - c_3)$ seria uma relação com $r_{31} - c_1 > 0$, $r_{12} - c_2 > 0$ e $r_{23} - c_3 > 0$, que é uma contradição. Portanto, $r_{31} = c_1$ e $v_3 = (c_1, 0, -c_3)$, o que prova nossa proposição. □

Seja x um número real, denotamos por $[x]$ o maior inteiro menor ou igual a x. O próximo resultado descreve explicitamente o conjunto das relações minimais no caso II.

Proposição 3.1.9 : *No caso II, o conjunto de relações minimais é:*

a) $\mathcal{M} = \{\pm(0, -c_2, c_3)\} \cup \{\pm(d(0, -c_2, c_3) + (-c_1, r_{12}, r_{13})),\ -[\frac{r_{13}}{c_3}] \leq d \leq [\frac{r_{12}}{c_2}],\ d \in \mathbb{Z}\}$,
ou

b) $\mathcal{M} = \{\pm(c_1, 0, -c_3)\} \cup \{\pm(d(c_1, 0, -c_3) + (r_{21}, -c_2, r_{23}))\},\ -[\frac{r_{21}}{c_1}] \leq d \leq [\frac{r_{23}}{c_3}],\ d \in \mathbb{Z}\}$,
ou

c) $\mathcal{M} = \{\pm(-c_1, c_2, 0)\} \cup \{\pm(d(-c_1, c_2, 0) + r_{31}, r_{32}, -c_3)),\ -[\frac{r_{32}}{c_2}] \leq d \leq [\frac{r_{31}}{c_1}],\ d \in \mathbb{Z}\}$.

Dem. : De acordo com 3.1.8, podemos assumir que $(0, -c_2, c_3) \in \mathcal{M}$. Sejam $v_1 = (-c_1, r_{12}, r_{13})$, $v_2 = (0, -c_2, c_3)$ e $\mathcal{N} = \{\pm v_2, \pm(dv_2 + v_1)\}$, onde $-[\frac{r_{13}}{c_3}] \leq d \leq [\frac{r_{12}}{c_2}]$.

É claro que $\mathcal{M} \supseteq \mathcal{N}$, pois $\pm v_2 \in \mathcal{M}$ por 3.1.8 e $dv_2 + v_1 = (-c_1, r_{12} - dc_2, r_{13} + dc_3)$ é uma relação minimal do tipo 1, por 3.1.4.

Reciprocamente, consideraremos dois casos: **caso a)** tomamos uma relação minimal do tipo 2 (ou 3) e o **caso b)** tomamos uma relação minimal do tipo 1.

caso a) Seja $v_2' = (r_{21}', -c_2, r_{23}')$ uma relação minimal do tipo 2. Se $r_{23}' = c_3$, então $v_2' - v_2 = (r_{21}', 0, 0)$, portanto $r_{21}' = 0$. Em outras palavras, $v_2' = v_2$ e logo $v_2' \in \mathcal{N}$.

Se $r_{23}' \neq c_3$, então $v_2' - v_2 = (r_{21}', 0, r_{23}' - c_3)$ é uma relação do tipo 3, pois $r_{21}' \geq 0$ então $r_{23}' - c_3 < 0$. Então, pela minimalidade de c_3, temos $r_{23}' - c_3 \leq -c_3$ e, logo, $r_{23}' = 0$. Portanto, $v_2' = (r_{21}', -c_2, 0)$.

Agora, $v_1 + v_2' = (r_{21}' - c_1, r_{12} - c_2, r_{13})$ é uma relação do tipo 2, pois $r_{21}' - c_1 \geq 0$ e $r_{13} = 0$ e, portanto, $r_{12} - c_2 \leq 0$. Se $r_{12} - c_2 = 0$, então $r_{21}' = c_1$ e $r_{13} = 0$. Logo, $v_1 = v_2'$ e então $v_2' \in \mathcal{N}$.

Se $r_{12} - c_2 < 0$, então $r_{12} - c_2 \leq -c_2$, o que implica que $r_{12} = 0$ e então $v_1 = (-c_1, 0, r_{13})$. Agora, $v_1 + v_2' - v_2 = (r_{21}' - c_1, 0, r_{13} - c_3)$ é uma relação com $r_{21}' - c_1 \geq 0$ e $r_{13} - c_3 \geq 0$. Logo, $v_1 + v_2' - v_2 = c_1$, $r_{13} = c_3$ e então $v_2' = v_2 - v_1$. Em qualquer dos dois casos, temos que $v_2' \in \mathcal{N}$. Analogamente, mostra-se que qualquer relação minimal v_3' do tipo 3 é um elemento de $\mathcal{N}$.

caso b) Se $v_1' = (-c_1, r_{12}', r_{13}')$ for qualquer relação minimal do tipo 1, então $v_1' - v_1 = (0, r_{12}' - r_{12}, r_{12}' - r_{13}) = dv_2$, onde $d \in \mathbb{Z}$ e as condições para d são óbvias. Com efeito, supondo $r_{12}' - r_{12} > 0$, teremos $r_{13}' - r_{13} \leq 0$ e portanto $v_1' - v_1$ é uma relação do tipo 2. Fazendo a divisão de $r_{12}' - r_{12}$ por c_2 e a divisão de $-(r_{13}' - r_{13})$ por c_3, obtemos $r_{12}' - r_{12} = q_2c_2 + r_2$, onde $0 \leq r_2 < c_2$ e $-(r_{13}' - r_{13}) = q_3c_3 + r_3$, onde $0 \leq r_3 < c_3$.

Suponhamos $q_2 < q_3$. Como $r_2 < c_2$ e $c_2n_2 = c_3n_3$, pois $(0, -c_2, c_3) \in \mathcal{M}$, temos

$$c_2q_2n_2 + r_2n_2 = c_3q_3n_3 + r_3n_3 < c_2q_2n_2 + c_2n_2 \Longrightarrow (q_3 - q_2 - 1)c_2n_2 < -r_3n_3$$

mas $r_3n_3 \geq 0$ e $q_3 - q_2 - 1 \geq 0$ e chegamos a um absurdo. Analogamente, supondo $q_3 < q_2$, chegaremos a um absurdo, assim $q_2 = q_3$.

Agora, devemos mostrar que $r_2 = r_3 = 0$. Como $(r_{12}' - r_{12})n_2 = (r_{13}' - r_{13})n_3$ e $q_2 = q_3$, segue que $r_2n_2 = r_3n_3$ e então $(0, -r_2, r_3)$ é uma relação do tipo 2 tal que $r_2 < c_2$, que é uma contradição, pois c_2 é minimal para as relações do tipo 2.

Logo $v_1' = v_1 + dv_2 \in \mathcal{N}$. □

Observação 3.1.10 : Para $v \in \mathbb{Z}^3$, $v = (z_1, z_2, z_3)$, nós assumimos $v^+ = (max(z_i, 0))$ e $v^- = v^+ - v$. Obviamente, temos v^+, $v^- \in \mathbb{N}^3$.

Se $v \in M_\rho(S)$, então $(v^+, v^-) \in \rho$. De fato,

$$v \in M_\rho(S) \iff \sum_{i=1}^{3} n_i z_i = 0 \iff \sum_{z_i \geq 0} n_i z_i - \sum_{-z_i > 0} n_i z_i = 0 \iff$$

$$\sum_{z_i \geq 0} n_i z_i = \sum_{-z_i > 0} n_i z_i \iff \rho^*(v^+) = \rho^*(v^-) \iff (v^+, v^-) \in \rho.$$

Lembrando que estamos supondo $S =< n_1, n_2, n_3 >$ e assim considerando R um anel comutativo com unidade e $v \in M_\rho(S)$, definimos $F_v \in R[X_1, X_2, X_3]$ por $F_v = X^{v^+} - X^{v^-}$.

Proposição 3.1.11 : *Nestas condições, temos* $I_S = (\{F_v\}_{v \in M_\rho(S)})$. *Portanto* $R[S] \cong R[X_1, X_2, X_3]/(\{F_v\}_{v \in M_\rho(S)})$.

Dem. : Sabemos por 2.2.6 que $I_S = (\{F_A\}_{A \in \rho})$.

Seja $v \in M_\rho(S)$; então, pela observação anterior, temos $(v^+, v^-) = A \in \rho$. Logo, $F_v = X^{v^+} - X^{v^-} \in (\{F_A\}_{A \in \rho})$.

Reciprocamente, se $A = (v, v') \in \rho$, então $w_A = v - v' \in M_\rho(S)$. Logo, $F_{w_A} = X^{w_A^+} - X^{w_A^-} \in (\{F_v\}_{v \in M_\rho(S)})$.

Agora, I_S é o núcleo do epimorfismo $\Gamma : R[X_1, X_2, X_3] \longrightarrow R[S]$.

Logo, temos $R[S] \cong R[X_1, X_2, X_3]/(\{F_v\}_{v \in M_\rho(S)})$. □

Na verdade, gostaríamos de provar que $I_S = (\{F_v\}_{v \in \mathcal{M}})$, mas para isso introduziremos uma ordem parcial em S da seguinte maneira: dados s_1, $s_2 \in S$, temos $s_1 \geq s_2$ se, e só se, $s_1 - s_2 \in S$. Podemos verificar que essa definição nos dá uma relação de ordem parcial sobre S

Observação 3.1.12 : Com a ordenação acima, temos a seguinte regra: se $\{s_i\}_{i=1,2,\ldots} \in S$ tal que $s_{i+1} \leq s_i$ para todo $i = 1, 2, \ldots$, então existe i_0 tal que para todo $i \geq i_0$, $s_{i+1} = s_i$. De fato, como $s_{i+1} \leq s_i$, $\forall i = 1, 2, \ldots$, então $s_i - s_{i+1} \in S$. Usando a ordenação usual dos números naturais, temos que $s_i - s_{i+1} \geq 0$, logo $s_i \geq s_{i+1}$. Assim, temos uma seqüência decrescente de números naturais. Portanto, existe i_0 tal que para $i \geq i_0$, $s_i = s_{i+1}$.

Para F, G no anel S-graduado $R[X_1, X_2, X_3]$, $deg(F) < deg(G)$ significa que $deg(F)$ é menor que $deg(G)$, no que se refere à ordenação em S.

Queremos mostrar que as relações $\{(v^+, v^-) \mid v \in \mathcal{M}\}$ geram ρ; devemos então provar, de acordo com 2.2.7, que $(\{F_v\}_{v \in \mathcal{M}}) = (\{F_v\}_{v \in M_\rho(S)})$ e essa igualdade é uma conseqüência da próxima proposição.

Proposição 3.1.13 : *Seja $v \in M_\rho(S)$. Então F_v pode ser escrito como $F_v = F' + QF_w$, onde $F' \in (\{F_v\}_{v\in\mathcal{M}})$, $w \in M_\rho(S)$, $Q \in R[X_1, X_2, X_3]$ e $deg(F_w) < deg(F_v)$.*

Dem. : Caso I: $\mathcal{M} = \{\pm v_1, \pm v_2, \pm v_3\}$, por 3.1.7.

Seja $v \in M_\rho(S)$, $v \notin \mathcal{M}$. Podemos assumir, sem perda de generalidade que, $v = (-a_1, a_2, a_3)$, $a_1 > c_1$, $a_2, a_3 \geq 0$. Obtemos

$$F_v - X_1^{a_1-c_1}F_{v_1} = X_2^{min(a_2,r_{12})}X_3^{min(a_3,r_{13})}F_w,$$

onde $w \in M_\rho(S)$.

Como $deg(F_w) = deg(F_v) - deg(X_2^{min(a_2,r_{12})}X_3^{min(a_3,r_{13})})$ e $(a_2, a_3) \neq (0,0)$, temos que $deg(X_2^{min(a_2,r_{12})}X_3^{min(a_3,r_{13})}) > 0$. Logo, $deg(F_w) < deg(F_v)$. Isso prova nossa afirmação para o caso I; tomemos $F' = X_1^{a_1-c_1}F_{v_1}$ e $Q = X_2^{min(a_2,r_{12})}X_3^{min(a_3,r_{13})}$.

Caso II: Vamos fazer nossa demonstração para o caso $\mathcal{M} = \{\pm v_2, \pm(dv_2 + v_1)\}$, onde $v_1 = (-c_1, r_{12}, r_{13})$, $v_2 = (0, -c_2, c_3)$ e $-[\frac{r_{13}}{c_3}] \leq d \leq [\frac{r_{12}}{c_2}]$.

1) Seja $v = (-a_1, a_2, a_3)$ uma relação do tipo 1. Logo, $a_1 \geq c_1$ e $a_2, a_3 \geq 0$. Podemos assumir que $a_1 > c_1$, pois se $a_1 = c_1$, então, $v \in \mathcal{M}$ e, logo, $F_v \in \{F_v, v \in \mathcal{M}\}$. Como no caso I, obtemos $F_v - X_1^{a_1-c_1}F_{v_1} = X_2^{min(a_2,r_{12})}X_3^{min(a_3,r_{13})}F_w$, com $w \in M_\rho(S)$. Se $a_2 > 0$ e $a_3 > 0$, então $deg(F_w) < deg(F_v)$ e está provado.

Suponhamos que $a_2 = 0$. Se $r_{13} > 0$, então novamente $deg(F_w) < deg(F_v)$, pois $a_3 > 0$. Se $r_{13} = 0$, então $r_{12} \geq c_2$ e $v_1' = v_1 + v_2 = (-c_1, r_{12} - c_2, c_3)$ é minimal do tipo 1, cuja terceira componente é maior que zero. Portanto $F_v - X_1^{a_1-c_1}F_{v_1'} = X_3^{min(a_3,c_3)}F_{w'}$, com $w' \in M_\rho(S)$ e $deg(F_{w'}) < deg(F_v)$, pois $min(a_3, c_3) > 0$. A prova é análoga se colocarmos $a_3 = 0$.

2) Seja $v = (a_1, -a_2, a_3)$ uma relação do tipo 2. Podemos assumir que $a_2 > c_2$, pois se $a_2 = c_2$, teremos que $F_v \in \{F_v \mid v \in \mathcal{M}\}$. Se $a_3 = 0$, então v é também uma relação do tipo 1 e isso já foi tratado no caso I.

Se $a_3 > 0$, então $F_v - X_2^{a_2-c_2}F_{v_2} = X_3^{min(a_3,c_3)}F_{w'}$, com $w' \in M_\rho(S)$ e $deg(F_{w'}) < deg(F_v)$, pois $min(a_3, c_3) > 0$. O caso em que $v \in M_\rho(S)$ é uma relação do tipo 3 é análogo a este caso. □

Como um corolário de 3.1.13, obtemos:

Teorema 3.1.14 : *As relações $\{(v^+, v^-) \mid v \in \mathcal{M}\}$ geram ρ.*

Dem. : Chamemos $I_S = (\{F_v\}_{v\in M_\rho(S)})$ e $J = (\{F_v\}_{v\in\mathcal{M}})$. Vamos mostrar que $I_S = J$ e assim, pela proposição 2.2.7, temos que ρ é gerado pelas relações $\{(v^+, v^-) \mid v \in \mathcal{M}\}$.

Como $\mathcal{M} \subseteq M_\rho(S)$, temos que $J \subseteq I_S$. Reciprocamente, seja $F_v \in I_S$ e suponhamos que $F_v \notin J$; pela proposição 3.1.13, temos que F_v pode

ser escrito como $F_v = F_1' + Q_1 F_{w_1}$, onde $F_1' \in J$, $Q_1 \in R[X_1, X_2, X_3]$, $w_1 \in M_\rho(S)$ e $deg(F_{w_1}) < deg(F_v)$. Aplicando 3.1.13 em F_{w_1}, obtemos $F_{w_1} = F_2' + Q_2 F_{w_2}$, onde $F_2' \in J$, $Q_2 \in R[X_1, X_2, X_3]$, $w_2 \in M_\rho(S)$ e $deg(F_{w_2}) < deg(F_{w_1})$. E teremos $F_v = F_1' + Q_1 F_2' + Q_1 Q_2 F_{w_2}$, onde $F_{w_2} \notin J$, pois $F_v \notin J$. Aplicando a proposição 3.1.13 sucessivamente teremos

$$F_v = F_1' + Q_2' F_2' + Q_2' F_3' + \cdots + Q_i' F_{wi}$$

onde $F_{w_i} \notin J$ e assim obtemos uma seqüência em S, $\{deg(F_{w_i})\}_{i=1,2,\ldots}$ tal que $deg(F_{w_{i+1}}) < deg(F_{w_i})$, para todo $i = 1, 2, \ldots$. Mas isso é uma contradição, pela observação 3.1.12. Portanto $F_v \in J$. Logo $I_S = (\{F_v\}_{v \in \mathcal{M}})$.

□

3.2 Semigrupos Simétricos e Interseções Completas

Nesta seção, usaremos a teoria de relações minimais, feita na seção anterior, para demonstrarmos quando um semigrupo simétrico $S =< n_1, n_2, n_3 >$ é uma interseção completa e conseqüentemente quando a curva parametrizada por S é também interseção completa.

Na situação assumida neste capítulo, temos:

Lema 3.2.1 *: Sejam* $\mathcal{M} = \{\pm(0, -c_2, c_3), \pm(d(0, -c_2, c_3) + (-c_1, r_{12}, r_{13}))\}$, *com* $d \in \mathbb{Z}$ *e* $-[\frac{r_{13}}{c_3}] \leq d \leq [\frac{r_{12}}{c_2}]$, $v_2 = (0, -c_2, c_3)$ *e*

$$v_1 = (-c_1, r_{12} + \Big[\frac{r_{13}}{c_3}\Big]c_2, r_{13} - \Big[\frac{r_{13}}{c_3}\Big]c_3) = (-c_1, \overline{r_{12}}, \overline{r_{13}}).$$

Então, para qualquer $v \in \mathcal{M}$, *temos* $v = \pm v_2$ *ou* $v = \pm(d'v_2 + v_1)$, *com* $d' = 0, 1, \ldots, [\frac{r_{13}}{c_3}] + [\frac{r_{12}}{c_2}]$.

Dem. : Seja $v \in \mathcal{M}$. Se $v = \pm v_2$, não temos nada a fazer.

Suponhamos $v = \pm(dv_2 + (-c_1, r_{12}, r_{13}))$. Temos

$$v = dv_2 + (-c_1, r_{12}, r_{13}) - (-c_1, r_{12} + \Big[\frac{r_{13}}{c_3}\Big]c_2, r_{13} - \Big[\frac{r_{13}}{c_3}\Big]c_3) + v_1$$

$$= dv_2 + (0, -\Big[\frac{r_{13}}{c_3}\Big]c_2, \Big[\frac{r_{13}}{c_3}\Big]c_3) + v_1$$

$$= (0, -dc_2, dc_3) + (0, -\Big[\frac{r_{13}}{c_3}\Big]c_2, \Big[\frac{r_{13}}{c_3}\Big]c_3) + v_1$$

$$= (0, -c_2(d + \Big[\frac{r_{13}}{c_3}\Big]), c_3(d + \Big[\frac{r_{13}}{c_3}\Big])) + v_1.$$

Chamemos $d' = d + [\frac{r_{13}}{c_3}]$, então $v = \pm(d'v_2 + v_1)$, onde $d' = 0, 1, \ldots, [\frac{r_{13}}{c_3}] + [\frac{r_{12}}{c_2}]$, pois $-[\frac{r_{13}}{c_3}] \leq d \leq [\frac{r_{12}}{c_2}]$. □

Daremos agora uma caracterização de semigrupos que são interseções completas para os casos I e II. Aqui consideraremos, como sempre, $v_1 = (-c_1, r_{12}, r_{13})$, $v_2 = (r_{21}, -c_2, r_{23})$, $v_3 = (r_{31}, r_{32}, -c_3)$, $r_{ij} \geq 0$, $i \neq j$.

Teorema 3.2.2 : *No* **caso I** : *S não é uma interseção completa.*

No **caso II**: *S é uma interseção completa.*

Dem. : Caso I: Seja $\mathcal{M} = \{\pm v_1, \pm v_2, \pm v_3\}$. Sabemos que $I_S = (F_{v_1}, F_{v_2}, F_{v_3})$, onde $F_{v_1} = X_2^{r_{12}}X_3^{r_{13}} - X_1^{c_1}$, $F_{v_2} = X_1^{r_{21}}X_3^{r_{23}} - X_2^{c_2}$, $F_{v_3} = X_1^{r_{31}}X_2^{r_{32}} - X_3^{c_3}$, onde $r_{ij} > 0$ para $i, j = 1, 2, 3$.

Suponhamos que temos uma equação

$$Q_1F_{v_1} = Q_2F_{v_2} + Q_3F_{v_3},\ Q_i \in R[X_1, X_2, X_3],\ i = 1, 2, 3.$$

Dela obtemos: $-\overline{Q_1}X_1^{c_1} = \overline{Q_2}X_1^{r_{21}}X_3^{r_{23}} + \overline{Q_3}X_3^{c_3}$, onde $\overline{Q_i} \equiv Q_i \bmod X_2$, com $\overline{Q_i} \in R[X_1, X_3]$ para $i = 1, 2, 3$.

Afirmação 1: Temos que $Q_1 \in (X_1, X_2, X_3)$.

dem.: De fato, como $r_{23} > 0$, temos $\overline{Q_1}(-X_1^{c_1}) = X_3(\overline{Q_2}X_3^{r_{12}}X_3^{r_{23}-1} - \overline{Q_3}X_3^{c_3-1})$. Devemos mostrar que X_3 divide $\overline{Q_1}$. Mas $\overline{Q_1} = X_3G + \overline{Q_1'}$, $G \in R[X_1, X_2, X_3]$ e $\overline{Q_1'} \in R[X_1]$, assim $\overline{Q_1}(X_1, 0) = \overline{Q_1'}$ e da igualdade acima $\overline{Q_1'} = 0$ e $\overline{Q_1} = X_3G$. Por outro lado, $\overline{Q_1} \equiv Q_1 \bmod X_2$, isto é, $\overline{Q_1} = Q_1 - X_2T$, com $T \in R[X_1, X_2, X_3]$. Logo, $Q_1 = X_2T + X_3G$ e, portanto, $Q_1 \in (X_1, X_2, X_3)$.

Assim, se tomarmos $\mathfrak{p}$ um ideal primo em $R[X_1, X_2, X_3]$ contendo (X_1, X_2, X_3), teremos que Q_1 não é uma unidade no anel local $R[X_1, X_2, X_3]_{\mathfrak{p}}$. Analogamente, começando com as equações do tipo $Q_2F_{v_2} = Q_1F_{v_1} + Q_3F_{v_3}$ e $Q_3F_{v_3} = Q_1F_{v_1} + Q_2F_{v_2}$, chegaremos à conclusão de que Q_2 e Q_3 não são unidades no anel local $R[X_1, X_2, X_3]_{\mathfrak{p}}$.

Afirmação 2: Dado $\mathfrak{p}$ um ideal primo de $R[X_1, X_2, X_3]$ contendo (X_1, X_2, X_3), temos que $\mu(I_SR[X_1, X_2, X_3]_{\mathfrak{p}}) = 3$.

dem.: De fato, chamemos $k(\mathfrak{p}) = R[X_1, X_2, X_3]_{\mathfrak{p}}/\mathfrak{p}R[X_1, X_2X_3]_{\mathfrak{p}}$ e suponhamos que $\overline{F_{v_1}}, \overline{F_{v_2}}, \overline{F_{v_3}} \in I_SR[X_1, X_2, X_3]/\mathfrak{p}I_SR[X_1, X_2, X_3]$, sejam $k(\mathfrak{p})$-linearmente independentes.

Assim, podemos supor que existem $Q_2, Q_3 \in R[X_1, X_2, X_3]$ tais que $F_{v_1} - Q_2F_{v_2} - Q_3F_{v_3} \in \mathfrak{p}I_SR[X_1, X_2, X_3]\mathfrak{p}$, isto é, existe $T \in R[X_1, X_2, X_3] \setminus \mathfrak{p}$, com $TF_{v_1} - TQ_2F_{v_2} - TQ_3F_{v_3} \in \mathfrak{p}I_S$, ou seja,

$$TF_{v_1} + TQ_2F_{v_2} + TQ_3F_{v_3} = Q_1'F_{v_1} + Q_2'F_{v_2} + Q_3'F_{v_3}$$

com $Q_1', Q_2', Q_3' \in \mathfrak{p}$, mas então temos, $(T - Q_1')F_{v_1} = Q"_2F_{v_2} + Q"_3F_{v_3}$ e assim teremos, pela afirmação 1, que $T - Q_1' \in (X_1, X_2X_3)$, com $Q_1' \in \mathfrak{p}$ e $T \notin \mathfrak{p}$, o que é absurdo pois $(X_1, X_2X_3) \subseteq \mathfrak{p}$. Assim, pelo lema de Nakayama, temos que $\mu(I_SR[X_1, X_2, X_3]\mathfrak{p}) = 3 \leq \mu(I_S) \leq 3$.

Agora podemos concluir que S não é interseção completa nesse caso, pois $posto\,\rho = \mu(I_S) = 3 > 2 = postoS - dimS$.

Caso II: Podemos supor que $\mathcal{M} = \{\pm(0, -c_2, c_3), \pm(d(0, -c_2, c_3) + (-c_1, r_{12}, r_{13}))\}$, com $d \in \mathbb{Z}$ e $-[\frac{r_{13}}{c_3}] \leq d \leq [\frac{r_{12}}{c_2}]$.

Sejam $v_2 = (0, -c_2, c_3)$ e $v_1 = (-c_1, r_{12} + [\frac{r_{13}}{c_3}]c_2, r_{13} - [\frac{r_{13}}{c_3}]c_3) = (-c_1, \overline{r_{12}}, \overline{r_{13}})$, então, para qualquer $v \in \mathcal{M}$, temos $v = \pm v_2$ ou $v = \pm(d'v_2 + v_1)$, com $d' = 0, 1, \ldots, [\frac{r_{13}}{c_3}] + [\frac{r_{12}}{c_2}]$, pelo lema 3.2.1.

Afirmamos que $I_S = (F_{v_1}, F_{v_2})$. Com efeito, se $v \in \mathcal{M}$, $v = dv_2 + v_1$, $d > 0$, então $v = (-c_1, \overline{r_{12}} - c_2, \overline{r_{13}} + dc_3)$ e $F_v = X_2^{\overline{r_{12}} - dc_2}X_3^{\overline{r_{13}} + dc_3} - X_1^{c_1} \in I_S$.

Sabemos que existe um polinômio $Q \in R[X_1, X_2, X_3]$, tal que $F_{dv_2} = QF_{v_2}$, então

$$\begin{aligned} X_2^{\overline{r_{12}} - dc_2}X_3^{\overline{r_{13}}}QF_{v_2} + F_{v_1} &= X_2^{\overline{r_{12}} - dc_2}X_3^{\overline{r_{13}}}F_{dc_2} + F_{v_1} \\ &= X_2^{\overline{r_{12}} - dc_2}X_3^{\overline{r_{13}}}(X_3^dc_3 - X_2^{dc_2}) + X_2^{\overline{r_{12}}}X_3^{\overline{r_{13}}} - X_1^{c_1} \\ &= X_2^{\overline{r_{12}} - dc_2}X_3^{\overline{r_{13}} + dc_3} - X_2^{\overline{r_{12}}}X_3^{\overline{r_{13}}} + X_2^{\overline{r_{12}}}X_3^{\overline{r_{13}}} - X_1^{c_1} \\ &= X_2^{\overline{r_{12}} - dc_2}X_3^{\overline{r_{13}} + dc_3} - X_1^{c_1} = F_v \end{aligned}$$

Isso prova a afirmação. Assim, $\mu(I_S) = posto\rho = 2 = postoS - dimS$. Portanto, S é uma interseção completa. □

Corolário 3.2.3 *: Em qualquer dos dois casos, $posto\rho \leq 3$.*

Dem. : Da demonstração do teorema anterior, temos, no caso I, $posto\rho = 3$ e, no caso II, $posto\rho = 2 < 3$. □

O teorema a seguir nos dá uma equivalência entre semigrupos simétricos e semigrupos que são interseções completas, além de nos fornecer uma cota inferior para o número mínimo de geradores de S^*, lembrando que $S^* = \{degF_A \mid A \in \rho\}$. Mas antes de apresentarmos tal teorema, necessitamos introduzir um novo número importante.

Seja $s(v) = \rho^*(v^+)(= \rho^*(v^-))$ para todo $v \in M_\rho(S)$ e definamos

$$\alpha := min\{s(v_1) + s(v_2) \mid v_1, v_2 \in M_\rho(S),\ v_1, v_2\ linearmente\ independentes\}$$

$$\gamma := \alpha - n_1 - n_2 - n_3.$$

Teorema 3.2.4 : *As seguintes condições são equivalentes:*

a) *S é uma interseção completa.*

b) *S^* é gerado por 2 elementos.*

c) $\gamma \notin S$.

d) *S é simétrico.*

Dem. : (**a** $\Rightarrow$ **b**) Se S é uma interseção completa, então por 2.4.5 temos que V_S é uma interseção completa, logo $\mu(S^*) \leq postoS - dimS = 2$, por 2.4.7. Portanto, S^* é gerado por 2 elementos.

(**b** $\Rightarrow$ **a**) Suponhamos que S não seja uma interseção completa; então, por 3.2.2, temos que $\mathcal{M} = \{\pm v_1, \pm v_2, \pm v_3\}$, com v_1, v_2, v_3 como no caso I.

S^* é certamente gerado por $\{s(v_1), s(v_2), s(v_3)\}$, pois S^* é gerado por $\{degF_{v_i} \mid i = 1, 2, 3\}$, de acordo com a observação 2.4.6. Suponhamos que $s(v_2) - s(v_1) \in S$, então existem $a_1, a_2, a_3 \in \mathbb{N}$ tais que $c_2n_2 - c_1n_1 = a_1n_1 + a_2n_2 + a_3n_3$, logo $(-c_1 - a_1)n_1 + (c_2 - a_2)n_2 - a_3n_3 = 0$. Como $-a_3 \leq 0$ e $-c_1 - a_1 < 0$, temos $c_2 - a_2 > 0$. Isso implica que $c_2 - a_2 \geq c_2$ e, então, $a_2 = 0$. Assim, nós obtemos a relação $v = (-c_1 - a_1, c_2, -a_3)$, que é minimal do tipo 2, portanto $v = -v_2$. Logo $r_{21} = a_1 + c_1 \geq c_1$, entretanto $r_{21} = c_1 - r_{31} < c_1$, pois $r_{31} > 0$, que é uma contradição. Portanto $s(v_2) - s(v_1) \notin S$. Analogamente, mostra-se que $s(v_i) - s(v_j) \notin S$, para $i, j = 1, 2, 3$, $i \neq j$. Logo, pelo corolário 2.1.15, temos que $\mu(S^*) = 3$, absurdo.

(**a** $\Rightarrow$ **c**)(**a** $\Rightarrow$ **d**) Podemos supor que temos as relações minimais $v_1 = (-c_1, r_{12}, r_{13})$ e $v_2 = (0, -c_2, c_3)$, pois S é interseção completa.

Afirmação 1: Temos que $[n_2, n_3] \in < n_3 >$ e $[(n_3, n_2), n_1] \in < n_3, n_2 >$.

dem.: Lembremo-nos de que $(n_1, n_2, n_3) = 1$. Como v_2 é minimal do tipo 2, temos que c_2 é o menor natural tal que $c_2n_2 = c_3n_3$ e então $[n_2, n_3] = c_2n_2 = c_3n_3 \in < n_3 >$. Como $v_1 \in \mathcal{M}$, temos que c_1n_1 é o menor mútiplo de n_1 tal que $c_1n_1 = r_{12}n_2 + r_{13}n_3$. Agora se $d = (n_2, n_3)$, então $d = n_2k + n_3k'$, com $k, k' \in \mathbb{Z}$. Logo

$$[(n_2, n_3), n_1] = d_1n_1 = bkn_2 + bk'n_3 = r_{12}n_2 + r_{13}n_3 \in < n_2, n_3 > .$$

Portanto, de acordo com a afirmação 1, a proposição 2.3.4 se aplica ao semigrupo $S =< n_1, n_2, n_3 >$.

Como $\gamma = c_2n_2 + c_1n_1 - n_1 - n_2 - n_3 = [n_2, n_3] + [(n_3, n_2), n_1] - n_1 - n_2 - n_3$, segue que $\gamma \notin S$, pela proposição 2.3.4, e que S é simétrico.

(c $\Rightarrow$ a) Suponhamos que S não é interseção completa. Sem perda de generalidade, assumimos que $s(v_1) < s(v_2) < s(v_3)$, v_i como no caso I, para $i = 1, 2, 3$. Então,

$$\begin{aligned}\gamma &= s(v_1) + s(v_2) - n_1 - n_2 - n_3 = c_1n_1 + c_2n_2 - n_1 - n_2 - n_3 \\ &= r_{12}n_2 + r_{13}n_3 + r_{21}n_1 + r_{23}n_3 - n_1 - n_2 - n_3 \\ &= (r_{21} - 1)n_1 + (r_{12} - 1)n_2 + (c_3 - 1)n_3\end{aligned}$$

A última igualdade segue de $v_1 + v_2 + v_3 = 0$. Como $r_{21} > 0$, $r_{12} > 0$ e $c_3 > 0$, temos que $\gamma \in S$, o que é uma contradição.

(d $\Rightarrow$ a) Suponhamos que S não seja interseção completa. Sejam

$$\gamma_1 = c_1n_1 + c_2n_2 - n_1 - n_2 - n_3 - r_{12}n_2 \quad \text{e}$$

$$\gamma_2 = c_1n_1 + c_2n_2 - n_1 - n_2 - n_3 - r_{21}n_1.$$

Afirmação 1: $\gamma_i \notin S$, para $i = 1, 2$.

dem.: Suponhamos que $\gamma_1 \in S$. Então existem $a_1, a_2, a_3 \in \mathbb{N}$ tais que $\gamma_1 = a_1n_1 + a_2n_2 + a_3n_3$. Agora

$$\gamma_1 = c_1n_1 + c_2n_2 - n_1 - n_2 - n_3 - r_{12}n_2 = (c_1 - 1)n_1 + (r_{32} - 1)n_2 - n_3,$$

por 3.1.6.

Podemos assumir que $0 \leq a_3 < c_3$ e segue que

$$(c_1 - 1 - a_1)n_1 + (r_{32} - 1 - a_2)n_2 - (-1 - a_3)n_3 = 0.$$

Suponhamos que $c_1 - 1 - a_1 \leq 0$, então $r_{32} - 1 - a_2 > 0$ e isto implica que $r_{32} - 1 - a_2 \geq c_2$. Como $r_{12} + r_{32} = c_2$, por 3.1.6 temos que $-1 - a_2 \geq r_{12} > 0$, logo $a_2 < 0$, uma contradição.

Suponhamos que $r_{32} - 1 - a_2 \leq 0$, então $c_1 - 1 - a_1 > 0$ e portanto $c_1 - 1 - a_1 \geq c_1$, logo $a_1 < 0$, uma contradição.

Temos portanto que $c_1 - 1 - a_1 > 0$ e $r_{32} - 1 - a_2 > 0$, logo $-1 - a_3 \leq -c_3$. Como $0 \leq a_3 < c_3$ temos que $-1 - a_3 = -c_3$, então $v_3 = (c_1 - 1 - a_1, r_{32} - 1 - a_2, -1 - c_3)$ e logo $r_{32} - 1 - a_2 = r_{32}$ e então $a_2 = -1$, o que é uma contradição. Portanto, $\gamma_1 \notin S$. Da mesma forma mostra-se que $\gamma_2 \notin S$.

Afirmação 2: $\gamma_i + s \in S$, para todo $s \in S$, $s \neq 0$, $i = 1, 2$.

dem.: Mostraremos para γ_1 e analogamente mostra-se para γ_2. Basta mostrar que $\gamma_1 + n_i \in S$, para $i = 1, 2, 3$.

$$\gamma_1 + n_1 = c_1 n_1 + c_2 n_2 - n_1 - n_2 - n_3 - r_{12} n_2 = (c_1 - 1) n_2 + (r_{13} - 1) n_3$$

$$\gamma_1 + n_2 = c_1 n_1 + c_2 n_2 - n_1 - n_2 - n_3 - r_{12} n_2 = (r_{12} - 1) n_1 + (c_3 - 1) n_3$$

$$\gamma_1 + n_3 = c_1 n_1 + c_2 n_2 - n_1 - n_2 - n_3 - r_{12} n_2 = (c_1 - 1) n_1 + (r_{32} - 1) n_2,$$

onde os coeficientes do lado direito das igualdades são positivos. Logo, $\gamma_1 + n_i \in S$ para $i = 1, 2, 3$. Isso prova a afirmação 2.

Agora, suponhamos que S é simétrico e m é o maior inteiro não pertencente a S. Temos $m - \gamma_i \in S$, pois, pela afirmação 1, $\gamma_i \notin S$ e então da afirmação 2, segue que $\gamma_i + (m - \gamma_i) = m \in S$. Portanto, temos que $m - \gamma_i = 0$. Logo $\gamma_1 = \gamma_2$ e assim $r_{21} n_1 = r_{12} n_2$, que é uma contradição pois $0 < c_2 < r_{12}$. Portanto, S é uma interseção completa. □

Como uma conseqüência do teorema anterior, temos uma fórmula para calcular o maior inteiro não pertencente a S, que é o m da definição de semigrupo simétrico.

Corolário 3.2.5 *: Se S é um semigrupo simétrico de inteiros gerado por 3 elementos $\{n_1, n_2, n_3\}$, com $(n_1, n_2, n_3) = 1$, então γ é o maior inteiro não pertencente a S.*

Dem. : Segue direto da demonstração do teorema anterior. □

O próximo resultado é uma aplicação de 3.2.4 à geometria algébrica.

Corolário 3.2.6 *A curva $V_S = \{(t^{n_1}, t^{n_2}, t^{n_3}) \mid t \in k\}$, onde k é um corpo algebricamente fechado, é uma interseção completa se, e somente se, $S =< n_1, n_2, n_3 >$ for simétrico.*

Dem. : $V_S = \{(t^{n_1}, t^{n_2}, t^{n_3}) \mid t \in k\}$ é uma interseção completa se, e somente se, $S =< n_1, n_2, n_3 >$ é uma interseção completa, por 2.4.5. E S é interseção completa se, e só se, S for simétrico, por 3.2.4. □

Daremos agora alguns exemplos de curvas parametrizadas em $A^3(k)$ que são ou não interseções completas. E com eles justificamos os exemplos dados no final do capítulo 1.

Exemplo 3.2.7 :

1. Considerando $S =< 4, 10, 13 >$, temos que

$$[4, 10] = 20 \in < 4 > \quad \text{e} \quad [(4, 10), 13] = 26 = 16 + 10 \in < 4, 10 > .$$

Assim, pela proposição 2.3.4, temos que S é simétrico e portanto, pelo teorema 3.2.4, segue que S é uma interseção completa. Pelo corolário 3.2.6, temos que

$$V_S = \{(t^4, t^{10}, t^{13}) \mid t \in k\}$$

é uma interseção completa.

Na verdade, todo semigrupo da família de semigrupos

$$\{S_m =< 4, 10, 2m + 1 >, \ com \ m \geq 3\}$$

é simétrico, pois $[(4, 10), 2m + 1] = 4m + 2 = 4(m - 2) + 10 \in < 4, 10 >$. Assim toda curva

$$V_m = \{(t^4, t^{10}, t^{2m+1}), \ t \in k\}$$

$m \geq 3$ é interseção completa.

2. Agora, consideremos $S =< 3, 4, 5 >$, S não é interseção completa, como já foi visto no exemplo 2.4.9. Outra forma de justificar isso é a seguinte: pelo exemplo 3.1.5, temos que $v_1 = (-3, 1, 1)$, $v_2 = (1, -2, 1)$, $v_3 = (2, 1, -2)$ são relações minimais de tipo $1, 2, 3$ respectivamente; então estamos no caso I e, pela proposição 3.1.7, temos que

$$\mathcal{M} = \{\pm(-3, 1, 1), \pm(1, -2, 1), \pm(2, 1, -2)\}.$$

Portanto, S não é interseção completa , por 3.2.2, logo, S não é simétrico, por 3.2.4. Assim, pelo corolário 3.2.6, temos que a curva

$$V = \{(t^3, t^4, t^5) \mid t \in k\}$$

não é uma interseção completa.

3. Considerando ainda $S =< 3, 4, 5 >$, podemos mostrar um exemplo para a observação 1.7.3 item 2, isto é, um ideal que é "set-theoretic" interseção completa, mas não é interseção completa.

De acordo com o teorema 3.1.14, temos que $I_S = (F_1, \ F_2, \ F_3)$, onde

$$F_1 = X_2X_3 - X_1^3, \ F_2 = X_1X_3 - X_2^2 \text{ e } F_3 = X_1^2X_2 - X_3^2$$

Agora, temos que $X_3^2 \equiv X_1^2X_2 \ mod(F_3)$, assim

$$F_1^2 = X_2^2X_3^2 - 2X_1^3X_2X_3 + X_1^6 \equiv X_1^2(X_2^3 - 2X_1X_2X_3 + X_1^4) \ mod(F_3) \text{ e}$$

$$F_2^2 = X_1^2X_3^2 - 2X_1X_2^2X_3 + X_2^4 \equiv X_2(X_1^4 - 2X_1X_2X_3 + X_2^3) \ mod(F_3).$$

Chamando $P = X_1^4 - 2X_1X_2X_3 + X_2^3$, temos que $F_1^2 = X_1^2P + H_1F_3$ e $F_2^2 = X_2P + H_2F_3$, onde H_1, $H_2 \in k[X_1, X_2, X_3]$, logo $F_1^2\ F_2^2 \in (P, F_3)$. Por outro lado, temos que $P \in I_S$, pois $X_1^2P \in I_S$ e I_S é primo, logo $(P, F_3) \subseteq I_S$.

Sabemos ainda que F_1, $F_2 \in \sqrt{(P, F_3)} \subseteq I_S$. Portanto $\sqrt{(P, F_3)} = I_S$. Logo I_S é "set-theoretic"uma interseção completa, mas não é interseção completa, pois pelo item anterior V não é uma interseção completa.

Na verdade, este resultado é válido para qualquer semigrupo gerado por três elementos que não é interseção completa. A generalização pode ser encontrada em [5].

Observação 3.2.8 : Observamos que o teorema 3.2.4 não é válido para semigrupos gerados por mais de três elementos. De fato.

1. O semigrupo $S =< 5, 6, 7, 8 >$ é simétrico, veja 2.3.6 , mas não é uma interseção completa, pois $S^* = (12, 13, 14, 15, 16)$. Logo $\mu(S^*) = 5$, pelo corolário 2.1.15. Por 2.4.7 temos $\mu(I_S) \geq 5$. Portanto, de acordo com 2.4.3, $postop \geq 5 > postoS - dimS = 3$.

2. Consideremos o semigrupo $S =< 6, 8, 9, 10 >$, como veremos, $\mu(S^*) = 3$ e no entanto S não é interseção completa, isto é, o análogo, neste caso, a afirmação b) do teorema 3.2.4 não é equivalente a ser interseção completa.

   Afirmação 1: Temos que $\mu(S^*) = 3$ e $\mu(I_S) \geq 3$.

   dem.: Observe que S^* é gerado por $S^* = (16, 18, 20)$; na verdade, temos que $S^* = \{16, 18, 20, 22, 24, 25, \ldots\}$. Vemos que $n \geq 24 \in S^*$, da seguinte maneira: dividindo n por 16, teremos $n = 16k + r$, com $k \geq 1$ e $0 \leq r \leq 15$, para $r \in \{6, 8, 9, 10, 12, 14, 15\}$, temos que $n \in S^*$, pois esses números estão em S, $r = 13$, temos $n = 16k - 1+20+9$ e então $n \in S^*$. Para $r = 11$, temos $n = 16(k-1)+18+9$ e novamente temos $n \in S^*$; procedendo de modo análogo para $0 \leq r \leq 7$, temos que $n \in S^*$. Agora, usando o corolário 2.1.15, temos que $\mu(S^*) = 3$ e, portanto, pela proposição 2.4.7, temos que $\mu(I_S) \geq 3$.

   Afirmação 2: Temos que $\mu(I_S) \geq 4$.

   dem.: De fato, considerando as seguintes menores relações: $(v_i, w_i) \in \rho$ para $i = 1, 2, 3, 4$ tais que

$$F_1 = X_1^3 - X_3X_4,$$

$$F_2 = X_2^2 - X_1X_4,$$
$$F_3 = X_3^2 - X_2X_4,$$
$$F_4 = X_4^2 - X_1^2X_4.$$

Devemos mostrar que $\overline{F_i} \in (I_S)_m/m(I_S)_m$ são linearmente independentes, onde $m = (X_1, X_2, X_3, X_4)$ é ideal maximal de $k[X_1, X_2, X_3, X_4]$.

Suponhamos $a_1\overline{F_1} + a_2\overline{F_2} + a_3\overline{F_3} + a_4\overline{F_4} = 0$, com $a_1, a_2, a_3, a_4 \in k$, temos que isso ocorre se, e somente se $a_1F_1 + a_2F_2 + a_3F_3 + a_4F_4 \in m(I_S)_m$, isto é,

$$a_1(X_1^3 - X_3X_4) + a_2(X_2^2 - X_1X_4) + a_3(X_3^2 - X_2X_4) + a_4(X_4^2 - X_1^2X_4) = \sum_{i=1}^{t} m_i(X^{v_i} - X^{w_i})$$

com $m_i \in m$ e $\rho^*(v_i) = \rho^*(w_i)$. A única possibilidade para que apareça $a_1X_1^3$ do lado direito da igualdade é que se tenha $X^{v_i} = X_1^2 - X_2^{t_2}X_3^{t_3}$ e que m_i tenha uma parcela X_1, mas isso não é possível, pois v_1 é a menor relação tal que X_1 aparece sozinho elevado a alguma potência, pois $6, 12 \notin < 8, 9, 10 >$, portanto $a_1 = 0$. Analogamente, mostra-se que $a_i = 0$ para $i = 2, 3, 4$. Portanto $\mu(I_S)_m \geq 4$.

Como $\mu(I_S) \geq \mu((I_S)_m) \geq 4$, segue que $postoρ = \mu(I_S) \geq 4$, por 2.4.3. Logo, S não é interseção completa, pois $postoS - dimS = 3$.

Bibliografia

[1] Atyah, M. F. e MacDonald, I. G.: *Intruduction to Commutative Algebra*, 1969.

[2] Bruns, W. e Herzorg, J.: *Cohen-Macaulay Rings*, Cambrige University Press, 1994.

[3] Garcia, A. e Lequain, Y.: *Álgebra: Um Curso de Introdução*. Rio de Janeiro, IMPA, 1988.

[4] Herzorg, J.: *Generators and Relations of Abelian Semigroups and Semigroup-Rings*. Manuscripta Math. 3 (1970), 153-193.

[5] Kunz, E.: *Introduction to Comutative Algebra and Algebric Geometry*. Bikhäuser,1985.

[6] Lang, S.: *Algebra*. Adilson-Wesley, Reading, Mass.,1974.

[7] Rédei, L.: *The Theory of Finitely Generated Commutative Semigroups*. Pergamon Press, Oxford, 1965.