

SABRINA DORNELAS MOTA

**SEMIGRUPOS DE VALORES DE ANÉIS GORENSTEIN, KUNZ E
ARF E A ÁRVORE DE SEMIGRUPOS NUMÉRICOS**

Dissertação apresentada à Universidade
Federal de Viçosa, como parte das
exigências do Programa de Pós Gra-
duação em Matemática, para obtenção
do título de *Magister Scientiae*.

**VIÇOSA
MINAS GERAIS - BRASIL
2015**

**Ficha catalográfica preparada pela Biblioteca Central da Universidade
Federal de Viçosa - Câmpus Viçosa**

T

M917s Mota, Sabrina Dornelas, 1986-
2015 Semigrupos de valores de anéis Gorenstein, Kunz e Arf e a
árvore de semigrupos numéricos / Sabrina Dornelas Mota. –
Viçosa, MG, 2015.
iv, 44f. ; 29 cm.

Orientador: Lia Feital Fusaro Abrantes.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f.43-44.

1. Matemática. 2. Semigrupos . I. Universidade Federal de
Viçosa. Departamento de Matemática. Programa de
Pós-graduação em Matemática. II. Título.

CDD 22. ed. 512.27

SABRINA DORNELAS MOTA

**SEMIGRUPOS DE VALORES DE ANÉIS GORENSTEIN, KUNZ E
ARF E A ÁRVORE DE SEMIGRUPOS NUMÉRICOS**

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

APROVADA: 29 de maio de 2015.

André Luis Contiero

Marinês Guerreiro

Renato Vidal da Silva Martins

Rogério Carvalho Picanço
(Co-orientador)

Lia Feital Fusaro Abrantes
(Orientadora)

Sumário

RESUMO	iii
ABSTRACT	iv
1 Introdução	1
2 Preliminares	3
2.1 Domínios de Valorização Discreta	3
2.2 Valorização Discreta	6
2.3 Diferenciais	7
3 Anéis e Semigrupos	9
3.1 Semigrupos numéricos	9
3.2 Anéis	12
3.3 Anéis e Semigrupos	16
3.4 Anel Local em um ponto de uma curva	19
4 Semigrupos de Anéis Gorenstein, Kunz e Arf	22
4.1 Anéis Gorenstein e Semigrupos Simétricos	22
4.2 Anéis Kunz e Semigrupos Pseudo-Simétricos	24
4.3 Anéis Arf e Semigrupos Arf	26
5 Árvore de semigrupos	29
5.1 Semigrupos simétricos	32
5.2 Semigrupos pseudo-simétricos	34
5.3 Semigrupos Arf	39
Referências Bibliográficas	43

RESUMO

MOTA, Sabrina, Dornelas, M.Sc., Universidade Federal de Viçosa, maio de 2015.
Semigrupos de Valores de Anéis Gorenstein, Kunz e Arf e a Árvore de Semigrupos Numéricos. Orientadora: Lia Feital Fusaro Abrantes, Coorientador: Rogério Carvalho Picanço.

Neste trabalho desenvolvemos dois resultados interessantes na área de semigrupos numéricos. Inicialmente abordamos semigrupos de valores de anéis unirramificados, focando em anéis Gorenstein, Kunz e Arf e seus respectivos semigrupos: simétricos, pseudo-simétricos e Arf. Tal assunto é interessante pelo fato de mostrar uma forma bem simples de identificar tais classes de anéis. Por fim trabalhamos com a árvore de semigrupos numéricos, que é um árvore infinita contendo todos os semigrupos numéricos "agrupados" de acordo com o gênero. Essa árvore mostra que o número de semigrupos dado um gênero g é finito. Mostramos também como procurar por semigrupos simétricos, pseudo-simétricos e Arf através da árvore de semigrupos.

ABSTRACT

MOTA, Sabrina, Dornelas, M.Sc., Universidade Federal de Viçosa, May, 2015.
Value Semigroups of Gorenstein, Kunz and Arf Rings and the Tree of Numerical Semigroups. Adviser: Lia Feital Fusaro Abrantes, Co-Adviser: Rogério Carvalho Picanço.

In this paper we develop two interesting results in the area of numerical semigroups. Initially we worked with value semigroup of unramified rings, focusing on Gorenstein, Kunz and Arf rings and their respective semigroups: symmetrical, pseudo-symmetrical and Arf. This subject is interesting because shows a simple way to identify such classes of rings. Finally we worked with the tree of numerical semigroups, which is an infinite tree containing all numerical semigroups "grouped" according to gender. This tree shows that the number of semigroups given a genus g is finite. We also show how to search for symmetrical, pseudo-symmetrical and Arf semigroups through the tree of numerical semigroups.

Capítulo 1

Introdução

Um *semigrupo numérico* é um subconjunto S dos números inteiros não-negativos $\mathbb{N}$ que é fechado em relação à adição, contém o zero e seu complemento em $\mathbb{N}$ é finito. Durante a segunda metade do século passado, semigrupos numéricos foram estudados, principalmente, por suas aplicações em geometria algébrica. Outras aplicações dessa teoria são encontradas em matemática discreta, teoria dos números, teoria da informação, superfícies de Riemann e álgebra comutativa.

O estudo de singularidades de curvas algébricas pode ser feito através do semigrupo de valores do anel local de cada singularidade. Neste estudo, trabalhamos com a relação entre anéis unirramificados e semigrupos numéricos e, por fim, apresentamos uma forma de se obter todos os semigrupos numéricos de acordo com o gênero.

O trabalho foi organizado da seguinte forma:

O segundo capítulo aborda alguns assuntos necessários para o entendimento do restante do trabalho.

No terceiro capítulo fazemos um estudo sobre semigrupos numéricos e sobre anéis, além da relação entre um anel unirramificado, que é aquele que possui único domínio de valorização discreta (DVD) que o contém (coincidente com seu fecho inteiro) e o semigrupo de valores desse anel, que é um semigrupo numérico.

O quarto capítulo trata dos semigrupos de valores de anéis Gorenstein, Kunz e Arf que são, respectivamente, semigrupos simétricos, pseudo-simétricos e Arf. O interessante desse estudo é que o mesmo facilita a caracterização de anéis, uma vez que classificar um anel como Gorenstein, Kunz ou Arf não é simples.

No quinto e último capítulo apresentamos a árvore de semigrupos, que é uma árvore infinita contendo todos os semigrupos numéricos, "agrupados" de acordo com o gênero. Uma aplicação interessante da árvore de semigrupos no estudo de singularidades: uma vez fixado o gênero g de uma curva, é possível estudar alguns invariantes como, por exemplo, gonalidade e peso, trabalhando com os semigrupos de gênero menor que ou igual a g e a árvore de semigrupos nos mostra que, dado o gênero, a quantidade de semigrupos é finita.

O estudo da árvore de semigrupos foi baseado no artigo *Towards a better understanding of the semigroup tree*, de M. Bras-Amoros e S. Bulygin, e enfatizamos nosso estudo em semigrupos simétricos, pseudo-simétricos e Arf.

Capítulo 2

Preliminares

Introduzimos, neste capítulo, alguns conceitos necessários para a compreensão do trabalho.

2.1 Domínios de Valorização Discreta

Um domínio de integridade D é um **anel de valorização** de seu corpo de frações F se, para todo $x \in F$, tem-se $x \in D$ ou $x^{-1} \in D$.

Sejam k um corpo algebricamente fechado de característica zero, $k[x]$ o anel de polinômios em uma variável e $k(x)$ o seu corpo de frações. Os nossos objetos de interesse neste capítulo são os anéis de valorização do corpo de funções algébricas de uma variável sobre k , que nesse caso chamaremos de **anéis de valorização discreta**, nomenclatura essa devida à teoria que vem a seguir.

Definição 2.1 *O corpo de funções $\mathbb{K} \mid_k$ de uma variável sobre k é uma extensão $\mathbb{K} \supset k$ algébrica finita de $k(x)$, para algum elemento $x \in \mathbb{K}$ que é transcendente sobre k .*

Para simplificar, nos referiremos a $\mathbb{K} \mid_k$ apenas como *corpo de funções*. Observe que se $\mathcal{O} \subseteq \mathbb{K}$ é um anel de valorização de $\mathbb{K} \mid_k$, então $k \subsetneq \mathcal{O} \subsetneq \mathbb{K}$.

As proposições a seguir listam as propriedades básicas de anéis de valorização discreta do corpo de funções $\mathbb{K} \mid_k$.

Proposição 2.2 *Seja $\mathcal{O}$ um anel de valorização do corpo de funções $\mathbb{K} \mid_k$. Então*

- (i) $\mathcal{O}$ é anel local com ideal maximal $M = \mathcal{O} \setminus \mathcal{O}^*$, onde $\mathcal{O}^* = \{z \in \mathcal{O} \mid \exists v \in \mathcal{O}; zv = 1\}$ é o grupo dos elementos invertíveis de $\mathcal{O}$.
- (ii) Para $0 \neq x \in \mathbb{K} \mid_k$, $x \in M$ se, e somente se $x^{-1} \notin \mathcal{O}$.

Demonstração: (i) Basta mostrar que M é ideal de $\mathcal{O}$. De fato, sejam $x \in M$ e $z \in \mathcal{O}$. Temos $xz \in M$ pois, caso contrário, teríamos x invertível em $\mathcal{O}$. Sejam $x, y \in M$ não nulos. Pela definição de $\mathcal{O}$ temos $\frac{x}{y} \in \mathcal{O}$ ou $\frac{y}{x} \in \mathcal{O}$. Suponha, sem perda de generalidade, que $\frac{x}{y} \in \mathcal{O}$. Então $\frac{x}{y} + 1 \in \mathcal{O}$ e daí $x + y = y \left(\frac{x}{y} + 1 \right) \in M$.

(ii) Segue diretamente da definição de M . ■

Lema 2.3 *Seja $\mathcal{O}$ um anel de valorização do corpo de funções $\mathbb{K} \mid_k$. Sejam M seu ideal maximal e $0 \neq x \in M$. Sejam $x_1, x_2, \dots, x_n \in M$ tais que $x_1 = x$ e $x_i \in x_{i+1}M$, com $i = 1, 2, \dots, n-1$. Então o grau da extensão $[\mathbb{K} : k(x)]$ é maior que ou igual a n .*

Demonstração: Observe que $[\mathbb{K} : k(x)]$ é a dimensão de $\mathbb{K}$ como $k(x)$ -espaço vetorial. Sendo assim, se o conjunto $\{x_1, x_2, \dots, x_n\}$ é linearmente independente, então $n \leq [\mathbb{K} : k(x)]$.

Suponha que tal conjunto é linearmente dependente, ou seja, que existe uma combinação linear $\sum_{i=1}^n \varphi_i(x)x_i = 0$ não trivial, com $\varphi_i(x) \in k(x)$. Podemos assumir que x não divide os φ_i 's.

Seja $a_i = \varphi_i(0)$ o termo constante de φ_i e defina $j \in \{1, 2, \dots, n\}$ tal que $a_j \neq 0$ e $a_i = 0$, para $i > j$. Temos

$$\sum_{i=1}^n \varphi_i(x)x_i = 0 \Rightarrow -\varphi_j(x)x_j = \sum_{i \neq j} \varphi_i(x)x_i$$

Note que $\varphi_i(x) \in \mathcal{O}$, para $i \in \{1, 2, \dots, n\}$, $x_i \in x_jM$ se $i < j$ e $\varphi_i(x) = xg_i(x)$, se $i > j$. Daí

$$-\varphi_j(x) = \sum_{i < j} \varphi_i(x) \frac{x_i}{x_j} + \sum_{i > j} \frac{x}{x_j} g_i(x)x_i.$$

Os somatórios do lado direito estão em M , logo $\varphi_j(x) \in M$. Por outro lado $\varphi_j(x) = a_j + xg_j(x)$, onde $g_j \in k[x]$ e $x \in M$, ou seja, $a_j = \varphi_j(x) - xg_j(x) \in M \cap k$. Por hipótese temos $a_j \neq 0$, o que nos leva a uma contradição. Portanto $\{x_1, x_2, \dots, x_n\}$ é linearmente independente. ■

Proposição 2.4 *Sejam $\mathcal{O}$ um anel de valorização do corpo de funções $\mathbb{K} \mid_k$ e M seu ideal maximal. Então:*

(i) M é principal.

(ii) Se $M = t\mathcal{O}$, então todo elemento $0 \neq z \in \mathbb{K}$ possui uma representação única da forma $z = t^n u$, para únicos $n \in \mathbb{Z}$ e $u \in \mathcal{O}^*$.

(iii) $\mathcal{O}$ é domínio de ideais principais. Mais precisamente, se $M = t\mathcal{O}$ e $\{0\} \neq I \subseteq \mathcal{O}$ é um ideal, então $I = t^n\mathcal{O}$, para algum $n \in \mathbb{N}$.

Demonstração: (i) Suponha que M não é principal e tome $0 \neq x_1 \in M$. Assim $M \neq x_1\mathcal{O}$, ou seja, existe $x_2 \in M \setminus x_1\mathcal{O}$. Temos $x_2x_1^{-1} \notin \mathcal{O}$, logo $x_2^{-1}x_1 \in M$ (pelo item (ii) da Proposição 2.2). Dessa forma, $x_1 \in x_2M$.

Continuando essa construção obtemos uma sequência infinita de elementos $x_1, x_2, \dots$ de M tais que $x_i \in x_{i+1}M$, para todo $i \geq 1$, o que é um absurdo segundo o Lema 2.3. Portanto M é principal.

(ii) Seja $z \in \mathbb{K}$. Da definição de $\mathcal{O}$, temos $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. Suponha $z \in \mathcal{O}$. Se $z \in \mathcal{O}^*$, então $z = t^0z$ e fica provado.

Suponha, agora, $z \in M$. Existe um inteiro maximal $m \geq 1$ tal que $z \in t^m\mathcal{O}$, pois considerando a sequência

$$x_1 = z, x_2 = t^{m-1}, x_3 = t^{m-2}, \dots, x_m = t,$$

o comprimento desta é limitado de acordo com o Lema 2.3. Assim, escreva $z = t^mu$, com $u \in \mathcal{O}$. Afirmamos que u é invertível em $\mathcal{O}$. De fato, se $u \in M = t\mathcal{O}$, então $u = tw$, para algum $w \in \mathcal{O}$. Daí $z = t^{m+1}w \in t^{m+1}\mathcal{O}$, o que contraria a maximalidade de m .

Para a unicidade, suponha $z = ut^{n_1} = vt^{n_2}$, com u, v invertíveis, $n_1 \geq n_2$. Então $ut^{n_1-n_2} = v$ é invertível. Como t é não invertível, então $n_1 = n_2$ e $u = v$.

(iii) $\mathcal{O}$ é um domínio, pela definição.

Seja $I \subseteq \mathcal{O}$ um ideal não nulo. O conjunto $C = \{r \in \mathbb{N} \mid t^r \in I\}$ é não vazio, pois se $0 \neq x \in I$, então $x = t^ru$, com $u \in \mathcal{O}^*$ e $r \geq 0$, daí $t^r = xu^{-1} \in I$. Tome $n = \min(C)$. Afirmamos que $I = t^n\mathcal{O}$. De fato, como $t^n \in I$, segue que $I \supset t^n\mathcal{O}$.

Seja $0 \neq y \in I$. Temos $y = t^sw$, com $w \in \mathcal{O}^*$ e $s \geq 0$. Dessa forma $t^s = yw^{-1}$ e $s \geq n$. Logo $y = t^n \cdot t^{s-n}w \in t^n\mathcal{O}$. ■

O elemento $t \in \mathcal{O}$ da proposição anterior é chamado **parâmetro local**.

2.2 Valorização Discreta

Definição 2.5 Uma **valorização discreta** de $\mathbb{K} \mid_k$ é uma função $v : \mathbb{K} \rightarrow \mathbb{Z} \cup \infty$ com as seguintes propriedades:

- (i) $v(x) = \infty \Leftrightarrow x = 0$.
- (ii) $v(xy) = v(x) + v(y)$, para todos $x, y \in \mathbb{K}$.
- (iii) $v(x + y) \geq \min \{v(x), v(y)\}$.
- (iv) Existe um elemento $z \in \mathbb{K}$ tal que $v(z) = 1$.
- (v) $v(a) = 0$, para todo $0 \neq a \in k$.

O conjunto consistindo de 0 e todos os elementos $x \in \mathbb{K}^*$ tais que $v(x) \geq 0$ é um anel, chamado **anel de valorização** de v e é um anel de valorização de $\mathbb{K}$.

Exemplo 2.6 Sejam $\mathbb{K} = \mathbb{Q}$ e p um número primo qualquer. Então qualquer elemento não nulo $x \in \mathbb{Q}$ pode ser escrito unicamente na forma $p^a y$, onde $a \in \mathbb{Z}$ e tanto o numerador como o denominador de y são primos com p . Defina $v(x)$ como a . Então o anel de valorização de v é o anel local $\mathbb{Z}_{(p)} = \left\{ \frac{c}{d}; c, d \in \mathbb{Z}, p \nmid d \right\}$.

Definição 2.7 Seja $\mathcal{O}$ um domínio de integridade. $\mathcal{O}$ é chamado um **anel de valorização discreta (DVD)** se $\mathcal{O}$ é um anel de valorização de uma valorização discreta v do corpo de frações de $\mathcal{O}$.

Observe que $\mathcal{O}$ é um anel local com ideal maximal $M = \{x \in \mathcal{O}; v(x) > 0\}$.

Lema 2.8 Sejam v uma valorização discreta de $\mathbb{K} \mid_k$ e $x, y \in \mathbb{K}$ tais que $v(x) \neq v(y)$. Então $v(x + y) = \min \{v(x), v(y)\}$.

Demonstração: Inicialmente observe que $v(ax) = v(x)$, para todo $0 \neq a \in k$. Em particular, temos $v(-y) = v(y)$. Como $v(x) \neq v(y)$, suponha, sem perda de generalidade, $v(x) < v(y)$.

Assuma $v(x + y) \neq \min \{v(x), v(y)\}$, ou seja, $v(x + y) > v(x)$. Dessa forma

$$v(x) = v((x + y) - y) \geq \min \{v(x + y), v(y)\} > v(x),$$

o que é uma contradição. Portanto $v(x + y) = \min \{v(x), v(y)\}$, se $v(x) \neq v(y)$.

■

Definição 2.9 Seja $\mathcal{O}$ um DVD de $\mathbb{K}$. Definimos

$$\begin{aligned} v : \mathbb{K} &\rightarrow \mathbb{Z} \cup \infty \\ t^n u &\mapsto n \\ 0 &\mapsto \infty, \end{aligned}$$

onde t é um parâmetro local de $\mathcal{O}$.

Esta função está bem definida, pois não depende da escolha do parâmetro local. De fato, seja t' outro parâmetro local. Então $M = t\mathcal{O} = t'\mathcal{O}$, logo $t = t'w$, para algum $w \in \mathcal{O}^*$. Portanto $t^n u = ((t')^n w^n)u = (t')^n (w^n u)$, com $w^n u \in \mathcal{O}^*$.

Teorema 2.10 *A função v acima definida é uma valorização discreta de $\mathbb{K} \mid_k$.*

Demonstração: As propriedades (i), (ii), (iv) e (v) da definição de valorização discreta são claramente satisfeitas por v . Vamos mostrar que (iii) também o é.

Sejam $x, y \in \mathbb{K}$ tais que $v(x) = n$ e $v(y) = m$. Suponha, sem perda de generalidade, $n \leq m < \infty$. Pela definição de v , temos $x = t^n u_1$ e $y = t^m u_2$, onde u_1 e u_2 são invertíveis em $\mathcal{O}$. Assim $x + y = t^n u_1 + t^m u_2 = t^n (u_1 + t^{m-n} u_2) = t^n z$, com $z \in \mathcal{O}$. Se $z = 0$, então $v(x + y) = v(0) = \infty > \min\{n, m\}$. Se $z \neq 0$, então $z = t^r u_3$, para $r \geq 0$ e $u_3 \in \mathcal{O}^*$. Daí $v(x + y) = v(t^n \cdot t^r u_3) = v(t^{n+r} u_3) = n + r \geq n = \min\{n, m\}$. Portanto v é uma valorização discreta de $\mathbb{K} \mid_k$. ■

2.3 Diferenciais

Vamos, inicialmente, definir a derivação em um corpo de funções algébricas de uma variável $\mathbb{K} \mid_k$, onde k é algebricamente fechado.

Seja $x \in \mathbb{K} \mid_k$ e defina a aplicação

$$\begin{aligned} \frac{d}{dx} : \mathbb{K} &\rightarrow \mathbb{K} \\ y &\mapsto \frac{dy}{dx} = y' \end{aligned}$$

da seguinte forma:

- i) $\frac{dy}{dx} = 0$, para todo $y \in k$;
- ii) se $y = f(x) = x^n$, então $\frac{dy}{dx} = nx^{n-1} = f'(x)$;
- iii) se $y = h(x) = \frac{f(x)}{g(x)}$, então $\frac{dh}{dx} = \frac{f'(x) \cdot g(x) - f(x) \cdot g'(x)}{g^2(x)} = h'(x)$;
- iv) se $y \in \mathbb{K} \setminus k(x)$, então y é algébrico sobre $k(x)$, o que implica que existem $f_0, \dots, f_s \in k(x)$ tais que $f_s(x)y^s + \dots + f_1(x)y + f_0(x) = 0$. Daí

$$\frac{dy}{dx} = \frac{-\sum_{i=0}^s f_i(x)y^i}{\sum_{i=0}^s i f_i(x)y^{i-1}}.$$

Lembremos que um elemento $x \in \mathbb{K}$ é dito um **elemento separável** de $x \in \mathbb{K} \mid_k$ se $\mathbb{K} \mid_{k(x)}$ é uma extensão algébrica separável. Observe que, como k tem característica zero, então cada extensão algébrica é separável.

Definição 2.11 Definimos, no conjunto $Z = \{(u, x) \in \mathbb{K} \times \mathbb{K}; \ x \text{ é separável}\}$, a relação de equivalência $\sim$ dada por

$$(u, x) \sim (v, y) \Leftrightarrow v = u \frac{dy}{dx}.$$

Denotamos uma classe de equivalência $(u, x) \in Z$ por udx e a chamamos de **diferencial de $\mathbb{K}$ em x** . Denotaremos por $\omega_{\mathbb{K}}$ o conjunto de tais classes de equivalência.

Sejam $\mathcal{O}$ um DVD de $\mathbb{K}$ e t um parâmetro local de $\mathcal{O}$. Da Proposição 2.4, temos $\mathbb{K} = \bigcup_{n \in \mathbb{Z}} t^n \mathcal{O}$. Seja $f \in \mathbb{K} \setminus k$ tal que $f \in t^n \mathcal{O} \setminus t^{n+1} \mathcal{O}$ (existência de n garantida pela proposição 2.4). Assim, $f = t^n a$, para algum $a \in \mathcal{O}^*$.

Como $\mathcal{O} = k + \mathcal{O}t$, então $f = t^n(c_1 + bt) = c_1 t^n + q$, com $q \in t^{n+1} \mathcal{O}$ e $c_1 \in k$. Daí, ou $q \in k$ ou continuamos o processo. Dessa forma, vemos que f está associada a uma série $\sum_i^n c_i t^i$, chamada **Série de Laurent de f em relação a t** .

Definição 2.12 Sejam $\lambda \in \omega_{\mathbb{K}}$ e $\mathcal{O}$ um DVD de $\mathbb{K}$. Definimos o **resíduo de λ em relação a $\mathcal{O}$** , denotado por $\text{Res}_{\mathcal{O}}(\lambda)$, da seguinte forma: tome t um parâmetro local de $\mathcal{O}$ e expresse $\lambda = fdt$. Em seguida, considere a série de Laurent de f com relação a t . Assim $\text{Res}_{\mathcal{O}}(\lambda)$ é o coeficiente do termo t^{-1} da série.

Esta definição independe da escolha do parâmetro t (veja [8]).

Capítulo 3

Anéis e Semigrupos

3.1 Semigrupos numéricos

Um **semigrupo numérico** é um subconjunto S dos números naturais $\mathbb{N}$ que é fechado em relação à adição, contém o zero e seu complemento em $\mathbb{N}$ é finito. Os elementos do complemento $\mathbb{N} \setminus S$ são chamados **lacunas** de S . O número de lacunas de um semigrupo numérico é o seu **gênero**. O menor inteiro de S a partir do qual todos os inteiros maiores pertencem ao semigrupo é chamado o **condutor** de S . A maior lacuna de S é chamada **número de Frobenius** e este é o condutor menos um. Usaremos a seguinte notação para um semigrupo numérico S com condutor c : $S = \{0, s_1, s_2, \dots, s_n = c, \rightarrow\}$.

Exemplo 3.1 $S = \{0, 5, 8, 10, 11, 13, 15, 16, 18, \rightarrow\}$ é um semigrupo numérico com condutor 18, número de Frobenius 17 e gênero 10.

Exemplo 3.2 $S_1 = \{0, 6, 7, 8, 11, \rightarrow\}$ é um semigrupo numérico com condutor 11, número de Frobenius 10 e gênero 7.

Seja S um semigrupo numérico. Um subconjunto $G \subset S$ é um conjunto gerador de S se todo elemento de S pode ser escrito como uma combinação linear com coeficientes positivos de elementos de G . Se $G = \{x_1 < x_2 < \dots < x_l\}$, usamos a notação $S = \langle x_1, x_2, \dots, x_l \rangle$. Todo semigrupo numérico possui um conjunto de geradores minimal, ou seja, um conjunto $G = \{x_1, x_2, \dots, x_n\}$ no qual nenhum elemento é combinação linear com coeficientes positivos de outros elementos do conjunto e seus elementos são chamados **geradores minimais**.

Proposição 3.3 *O conjunto minimal de geradores de um semigrupo numérico S é único.*

Demonstração: Suponha, por absurdo, que

$$G_1 = \{x_1, x_2, \dots, x_n\}$$

e

$$G_2 = \{y_1, y_2, \dots, y_m\}$$

sejam conjuntos geradores minimais distintos de S . Seja $z \in G_1 \setminus G_2$. Assim, como $z \in S$ e G_2 é conjunto gerador de S , então $z = \sum_{j=1}^r a_j y_{i_j}$, para alguns $y_{i_j} \in G_2$ e $a_j \in \mathbb{N}^*$. Agora,, cada y_{i_j} é da forma $\sum_{l=1}^s b_l x_{i_l}$, com $x_{i_l} \in G_1$ e $b_l \in \mathbb{N}^*$. Logo $z = \sum_{j=1}^r \sum_{l=1}^s a_j b_l x_{i_l}$, o que contraria o fato de z ser gerador minimal de S . Portanto $G_1 = G_2$. ■

De agora em diante, nos referiremos a um semigrupo numérico apenas como *semigrupo*, ao conjunto minimal de geradores apenas como *conjunto gerador* e aos geradores minimais apenas como *geradores*.

Exemplo 3.4 *O conjunto gerador do semigrupo*

$$S = \{0, 5, 8, 10, 11, 13, 15, 16, 18, \rightarrow\}$$

$\acute{e} < 5, 8, 11 > e$ do semigrupo $S_1 = \{0, 6, 7, 8, 11, \rightarrow\}$ $\acute{e} < 6, 7, 8, 11 >.$

Definição 3.5 *Dados E, F subconjuntos de $\mathbb{Z}$, $x \in \mathbb{Z}$ e $n \in \mathbb{N}^*$, definimos as seguintes operações:*

- i) $E + F = \{a + b; a \in E, b \in F\};$
- ii) $E + x = \{a + x; a \in E\};$
- iii) $nE = E + E + \dots + E, n \text{ parcelas};$
- iv) $E - F = \{a \in \mathbb{Z}; a + F \subseteq E\}.$

Usaremos para um subconjunto E de $\mathbb{Z}$ a mesma notação que usamos para semigrupo, ou seja, se $E = \{-3, -1\} \cup \mathbb{N} \setminus \{1, 3, 6\}$, escreveremos

$$E = \{-3, -1, 0, 2, 4, 5, 7 \rightarrow\}.$$

Definição 3.6 *Um **ideal relativo** de um semigrupo S é um conjunto não vazio $E \subseteq \mathbb{Z}$ tal que*

- i) $S + E \subseteq E;$
- ii) $x + E \subseteq S, \text{ para algum } x \in \mathbb{Z}.$

*Se $E \subset S$, dizemos apenas que E é um **ideal** de S .*

Exemplo 3.7 *Os conjuntos*

$$E = \{-5, 0, 3, 5, 6, 8, 10, 11, 13, \rightarrow\}$$

e

$$M = \{5, 8, 10, 11, 13, 15, 16, 18, \rightarrow\}$$

são, respectivamente, ideal relativo e ideal de $S = \{0, 5, 8, 10, 11, 13, 15, 16, 18, \rightarrow\}$.

Seja S um semigrupo. Então $M = \{s \in S; s > 0\}$ é sempre um ideal de S , chamado **ideal maximal de S** .

Definição 3.8 *Um ideal relativo W é dito **ideal canônico** se para qualquer ideal relativo E de S temos $W - (W - E) = E$.*

Lema 3.9 *Seja S um semigrupo com número de Frobenius γ . Existe um ideal relativo K de S tal que, para quaisquer ideais relativos $F \subseteq E$, vale $\text{card}(E \setminus F) = \text{card}((K - F) \setminus (K - E))$.*

Demonstração: Considere o conjunto

$$K = \{a; \gamma - a \notin S\} = \{\gamma - a; a \notin S\} \quad (3.1)$$

Afirmção: K é um ideal relativo de S .

De fato, seja $x \in S + K$, ou seja, $x = s + a$, com $s \in S$ e $a \in K$. Suponha $x \notin K$. Assim $\gamma - (s + a) = \gamma - s - a \in S$. Como $s \in S$, então $\gamma - a \in S$, o que é um absurdo pois $a \in K$. Logo $S + K \subseteq K$. Para verificar a segunda condição na definição de ideal relativo, tome $x = \gamma + 1$ (o condutor de S).

Mostraremos agora que dado um ideal relativo E de S , temos

$$K - E = \{\gamma - a; a \notin E\}.$$

Para isto basta mostrar que os conjuntos $A = \{a \in \mathbb{Z}; a + E \subseteq K\}$ e $B = \{\gamma - b; b \notin E\}$ são iguais.

Sejam $e \in E$ e $y = \gamma - b \in B$, ou seja, $b \notin B$. Temos $b - e \notin S$ pois, caso contrário, teríamos $b \in e + S \subset E + S \subseteq E$. Daí

$$b - e \notin S \Rightarrow \gamma - (\gamma - b) - e \notin S \Rightarrow \gamma - (y + e) \notin S \Rightarrow y + e \in K \Rightarrow y \in A.$$

Reciprocamente, seja $z \in A$ e escreva $z = \gamma - (\gamma - z)$. Suponha $z \notin B$. Então $\gamma - z \in E$ e $\gamma = z + (\gamma - z) \in K$, o que é um absurdo, pois $0 \in S$. Logo $z \in B$ e

$A = B$. Portanto

$$\begin{aligned} \text{card}((K - F) \setminus (K - E)) &= \text{card}(\{\gamma - c; c \notin F\} \setminus \{\gamma - b; b \notin E\}) \\ &= \text{card}(\{\gamma - d; d \in E \setminus F\}) \\ &= \text{card}(E \setminus F) \end{aligned}$$

■

Proposição 3.10 *Todo semigrupo S possui um ideal canônico.*

Demonstração: Seja $K = \{\gamma - a; a \notin S\}$ como definido em 3.1 e seja E um ideal relativo qualquer de S . Então

$$\begin{aligned} K - (K - E) &= \{\gamma - b; b \notin (K - E)\} \\ &= \{\gamma - (\gamma - a); a \in E\} \\ &= \{a; a \in E\} \\ &= E \end{aligned}$$

Logo K é um ideal canônico de S .

■

Exemplo 3.11 *Seja $S = \{0, 5, 8, 10, 11, 13, 15, 16, 18, \rightarrow\}$. Então $K = \{0, 3, 5, 8, 10, 11, 13, 14, 15, 16, 18, \rightarrow\}$ é um ideal canônico de S .*

3.2 Anéis

Considere k um corpo algebricamente fechado de característica zero e $\mathbb{K} |_k$ o corpo de funções algébricas em uma variável. Nesta seção, consideramos sempre A o anel local Noetheriano de dimensão 1 com ideal maximal M e $k \subset A \subset \mathbb{K}$ tal que o corpo de frações de A é $\mathbb{K}$. Neste trabalho, consideramos o caso em que A é anel uniramificado, isto é, existe um único DVD que o contém e este é o fecho inteiro $\bar{A}$ de A .

Definição 3.12 *Um A -submódulo I de $\mathbb{K}$ é dito **ideal fracionário de A** se existe $x \in A, x \neq 0$, tal que $xI \subseteq A$.*

Para ideais fracionários I e J de A definimos a seguinte operação:

$$I : J = \{x \in \mathbb{K}; xJ \subset I\}.$$

Proposição 3.13 *Se I e J são ideais fracionários de A , então $I : J$ também o é.*

Demonstração: Considere $z = xy$, com $x \in A, x \neq 0$, tal que $xI \subseteq A$ e y um elemento qualquer de J . Afirmamos que $z(I : J) \subseteq A$. De fato, se $w \in (I : J)$, então $yw \in I$. Logo $xyw \in A$. ■

Proposição 3.14 *Se I, J e L são ideais fracionários de A e f é um elemento qualquer de $\mathbb{K}$, então:*

- i) $(fI) : J = f(I : J);$
- ii) $I : (fJ) = f^{-1}(I : J);$
- iii) $(I : J) : L = I : JL.$

Demonstração: Temos:

i)

$$\begin{aligned}
 (fI) : J &= \{x \in \mathbb{K}; xJ \subset fI\} \\
 &= \{x \in \mathbb{K}; f^{-1}xJ \subset I\} \\
 &= \{fx \in \mathbb{K}; xJ \subset I\} \\
 &= f(I : J)
 \end{aligned}$$

ii)

$$\begin{aligned}
 I : (fJ) &= \{x \in \mathbb{K}; xfJ \subset I\} \\
 &= \{f^{-1}x \in \mathbb{K}; xJ \subset I\} \\
 &= f^{-1}(I : J)
 \end{aligned}$$

iii)

$$\begin{aligned}
 (I : J) : L &= \{x \in \mathbb{K}; xL \subset (I : J)\} \\
 &= \{x \in \mathbb{K}; (xL)J \subset I\} \\
 &= \{x \in \mathbb{K}; x(JL) \subset I\} \\
 &= I : JL
 \end{aligned}$$

■

Seja R um anel. Dados um R -módulo M e um ideal I de M , denotamos por $l_M(I)$, ou simplesmente $l(I)$, o comprimento da maior cadeia de submódulos de M

$$I = I_0 \supset I_1 \supset \dots \supset I_n = \{0\}.$$

Assim, se $L \subseteq J \subseteq I$ são ideais fracionários de M , então

$$l(I/L) = l(I/J) + l(J/L).$$

Definição 3.15 *Um A -ideal fracionário ω é dito **ideal canônico** de A se, para qualquer A -ideal fracionário I , tem-se $I = \omega : (\omega : I)$.*

Seja ω um ideal canônico de A . Então $x\omega$, com $x \in \mathbb{K}$ também o é, pois

$$x\omega : ((x\omega) : I) = x\omega : (x(\omega : I)) = x^{-1}(x\omega : (\omega : I)) = \omega : (\omega : I) = I,$$

para todo A -ideal fracionário I .

Proposição 3.16 *Sejam I e J ideais fracionários de A com $I \subseteq J$. Existe um A -ideal fracionário ω tal que $l_A(J/I) = l_A(\omega : I/\omega : J)$.*

Demonstração: Seja $\lambda \in \omega_{\mathbb{K}}$ uma diferencial como definido na Seção 2.3. Sabemos que $\overline{A}$ é o único DVD de $\mathbb{K}$ que contém A . Defina a aplicação

$$\begin{aligned} \varphi_{\lambda,A} : \mathbb{K} &\rightarrow k \\ f &\mapsto \text{Res}_{\overline{A}}(fA) \end{aligned}$$

Definimos ω (que depende de λ) da seguinte forma:

$$\omega = \{f \in \mathbb{K}; \varphi_{\lambda,A}(fA) = 0\}.$$

Prova-se (veja [9]) que ω é A -ideal fracionário.

Para mostrar que ω satisfaz a propriedade desejada, tomemos $I \subset J$ A -ideais fracionários, e consideremos a transformação linear

$$T : (\omega : I)/(\omega : J) \rightarrow \text{Hom}_k((J/I); k)$$

definida por $T(\overline{f}) = \varphi_{\lambda,A}(f)$ e tal que $[T(\overline{f})](\overline{g}) = \varphi_{\lambda,A}(fg)$.

A transformação T está bem definida e é injetiva. Como $\dim(\text{Hom}_k(J/I; k)) = l(J/I)$, segue

$$l((\omega : I)/(\omega : J)) \leq l(J/I), \forall I \subset J. \quad (3.2)$$

Por outro lado, temos

$$\begin{aligned}
l(J/I) &= l(J\bar{A}/(I : \bar{A})) - (l(J\bar{A}/J) + l(I/(I : \bar{A}))) \\
&\leq l(J\bar{A}/(I : \bar{A})) - (l((\omega : J)/(\omega : J\bar{A})) + l((\omega : (I : \bar{A}))/(\omega : I))) \\
&= l(J\bar{A}/(I : \bar{A})) - l((\omega : (I : \bar{A}))/(\omega : J\bar{A})) + l((\omega : I)/(\omega : J)) \\
&= l((\omega : I)/(\omega : J))
\end{aligned}$$

sendo que a primeira igualdade segue da sequência de inclusões

$$I : \bar{A} \subset I \subset J \subset J\bar{A},$$

a desigualdade segue de 3.2, e a segunda igualdade, da sequência de inclusões

$$\omega : J\bar{A} \subseteq \omega : J \subseteq \omega : I \subseteq \omega : (I : \bar{A}).$$

Para a última igualdade, observe que $J\bar{A}, I : \bar{A}$ e $\omega : \bar{A}$ são $\bar{A}$ -ideais fracionários, logo são principais. Suponha $J\bar{A} = f_1\bar{A}, I : \bar{A} = f_2\bar{A}$ e $\omega : \bar{A} = f_3\bar{A}$. Então

$$\begin{aligned}
(\omega : (I : \bar{A}))/(\omega : J\bar{A}) &= (\omega : f_2\bar{A})/(\omega : f_1\bar{A}) \\
&= ((\omega : \bar{A}) : f_2\bar{A})/((\omega : \bar{A}) : f_1\bar{A}) \\
&= (f_3\bar{A} : f_2\bar{A})/(f_3\bar{A} : f_1\bar{A}) \\
&= (f_3f_2^{-1}\bar{A})/(f_3f_1^{-1}\bar{A}) \\
&= f_1\bar{A}/f_2\bar{A} \\
&= J\bar{A}/(I : \bar{A}),
\end{aligned}$$

como queríamos. ■

Proposição 3.17 *Considere um anel A com as hipóteses descritas no início da seção. Existe um ideal canônico do anel A .*

Demonstração: Seja ω como na proposição anterior. Para todo ideal fracionário I de A , temos

$$I \subset (\omega : (\omega : I)).$$

Em particular, isso vale para o ideal $\omega : I$, daí temos $\omega : I \subset (\omega : (\omega : (\omega : I)))$.

Aplicando $(\omega : -)$ na primeira inclusão, obtemos $\omega : I \supset (\omega : (\omega : (\omega : I)))$. Logo $\omega : I = (\omega : (\omega : (\omega : I)))$.

Pela dualidade local, temos

$$l((\omega : (\omega : I))/I) = l((\omega : I)/(\omega : (\omega : (\omega : I)))) = 0.$$

Portanto $(\omega : (\omega : I)) = I$, para qualquer A -ideal fracionário I , e ω é um ideal canônico. ■

Existe um ideal canônico tal que $A \subseteq \omega \subseteq \bar{A}$. Para verificar, considere ω um ideal canônico de A e $x \in \omega$ tal que $\omega\bar{A} = x\bar{A}$ (o que é possível pois $\omega\bar{A}$ é um $\bar{A}$ -ideal fracionário). Então $x\bar{A} \subseteq \omega \subseteq x\bar{A}$ e daí $A \subseteq x^{-1}\omega \subseteq \bar{A}$. Como ω é canônico, $x^{-1}\omega$ também o é.

3.3 Anéis e Semigrupos

Assim como na seção anterior, considere k um corpo algebricamente fechado de característica zero, $\mathbb{K} \mid_k$ o corpo de funções algébricas em uma variável, A o anel local Noetheriano de dimensão 1 com ideal maximal M e $k \subset A \subset \mathbb{K}$ tal que o corpo de frações de A é $\mathbb{K}$. Lembrando que neste trabalho consideramos o caso em que A é anel unirramificado, isto é, existe único DVD que o contém, e este é o fecho inteiro $\bar{A}$ de A .

Vimos, na Seção 2.2, que a aplicação

$$\begin{aligned} v : \mathbb{K} &\rightarrow \mathbb{Z} \cup \infty \\ t^n u &\mapsto n \\ 0 &\mapsto \infty, \end{aligned}$$

onde t é um parâmetro local de $\bar{A}$ e u um invertível de $\bar{A}$, é uma valorização discreta.

Proposição 3.18 *Seja v a valorização dada por $\bar{A}$. Então $S := v(A)$ é um semigrupo numérico.*

Demonstração: Temos:

* $0 \in S$ pois $v(1) = 0$.

* Sejam $x, y \in S$. Então existem $a, b \in A$ tais que $x = v(a), y = v(b)$.

$$x + y = v(a) + v(b) = v(ab) \in S.$$

* Dado $z \in A : \overline{A}$, temos $z\overline{A} \subseteq A$. Seja t parâmetro local de $\overline{A}$. Como $A : \overline{A}$ é um $\overline{A}$ -módulo, temos $t^i z \in A : \overline{A}$ para todo $i \in \mathbb{N}$ e daí

$$v(t^i z) = v(t^i) + v(z) = i + v(z) \in S,$$

para todo i . Logo $S \setminus \mathbb{N}$ é finito.

Portanto S é um semigrupo numérico. ■

Definição 3.19 *O semigrupo $v(A)$ é denominado **semigrupo de valores do anel** A .*

Lema 3.20 *Se $v(x) = v(y)$, para $x, y \in \overline{A}$, então $v(x - uy) > v(y)$ para algum invertível $u \in A$.*

Demonstração: Sejam $x = at^\alpha, y = bt^\alpha \in \overline{A}$. Temos $v(x) = v(y) = \alpha$. Escrevendo x e y na forma de série temos $x = a_0 t^\alpha + \dots$ e $y = b_0 t^\alpha + \dots$. Fazendo $u = \frac{a_0}{b_0}$, temos o resultado. ■

Lema 3.21 *Seja I um A -ideal fracionário tal que $I \supset A$ e $I \neq A$. Considere $v(I) \setminus v(A) = \{a_1, a_2, \dots, a_\lambda\}$, $a_1 < a_2 < \dots < a_\lambda$ e seja $I'_i = \{x \in I; v(x) \geq a_i\}$. Tome I_i o A -ideal fracionário gerado por I'_i e A . Então $v(I_i) = \{a_i, \dots, a_\lambda\} \cup v(A)$ e $I_1 = I$.*

Demonstração: Tome $x \in I_i, x = x' + y$, com $x' \in I'_i$ e $y \in A$. Como $v(x') \neq v(y)$ (pela construção de I'_i), então ou $v(x) = v(y)$ ou $v(x) \geq v(x') \geq a_i$. Logo $v(I_i) = \{a_i, \dots, a_\lambda\} \cup v(A)$.

Seja $x \in I$ tal que $v(x) < a_1$. Como $v(x) \in v(A)$, existe, após sucessivas aplicações do Lema 3.20, um elemento $y \in A$ tal que $v(x - y) \geq a_1$. Logo $x - y \in I'_1$ e $x = (x - y) + y \in I_1$. ■

Proposição 3.22 *Seja I um A -ideal fracionário tal que $I \supseteq A$. Então $l(I/A) = \text{card}(v(I) \setminus v(A))$.*

Demonstração: Seja $\lambda = \text{card}(v(I) \setminus v(A))$. Faremos indução sobre $\lambda \geq 0$. Se $\lambda = 0$, então $v(I) = v(A)$ e daí $I = A$. Se $\lambda > 0$, tome $v(I) \setminus v(A) = \{a_1, a_2, \dots, a_\lambda\}$, com $a_1 < a_2 < \dots < a_\lambda$ e seja I_i o A -ideal fracionário definido no Lema 3.21. Seja J um submódulo de I tal que $I_2 \subsetneq J$. Mostremos que $v(J) = v(I)$. Seja $x \in J \setminus I_2$ e suponha $v(x - y) \neq a_1$, para todo $y \in A$. Como $v(x) \in v(A)$, temos, pelo Lema 3.21, $v(x - z) \geq a_2$, para algum $z \in A$. Como $v(x - z) \geq \min\{v(x), v(z)\}$, então $x \in I_2$, o que nos leva a uma contradição.

Portanto $v(x - y) = a_1$ para algum $y \in A$, o que mostra que $v(J) = v(I_1) = v(I)$.

Provaremos, agora, a igualdade $J = I$.

Seja $x \in I$ tal que $v(x) < a_2$. Então ou $v(x - y) = a_1$, para algum $y \in A$, ou $v(x - y) \neq a_1$, para todo $y \in A$.

No primeiro caso, existe $z \in J$ tal que $v(x - y) = v(z)$. Pelo Lema 3.20, temos $v(x - t) \geq a_2$, para algum $t \in J$, logo $x \in J$ ($I_2 \subset J$).

Se $v(x - y) \neq a_1$, para todo $y \in A$, então $v(x) \in v(A)$. Logo, pelo Lema 3.20 existe $t \in A$ tal que $v(x - t) \geq a_2$, o que implica $x \in J$. Logo $J = I$. Assim $l(I/I_2) = 1$. Por outro lado, pelo Lema 3.21 temos $v(I_2) \setminus v(A) = \{a_2, a_3, \dots, a_\lambda\}$. Pela hipótese de indução, temos $l(I_2/A) = \lambda - 1$, o que implica $l(I/A) = \lambda$. ■

Corolário 3.23 *Sejam I e J ideais fracionários de A tais que $I \supseteq J$. Então $l(I/J) = \text{card}(v(I) \setminus v(J))$.*

Demonstração: Basta aplicar a demonstração da proposição acima. ■

Proposição 3.24 *Seja ω um ideal fracionário de A tal que $a \subseteq \omega \subseteq \overline{A}$. Então ω é ideal canônico de A se, e somente se, $v(\omega)$ é ideal canônico de $v(A)$.*

Demonstração: Sejam $S = v(A)$ e γ o número de Frobenius de S .

Afirmamos que $\gamma \notin v(\omega)$. De fato, suponha, por absurdo, que $\gamma \in v(\omega)$, ou seja, que exista $x \in \omega$ tal que $\gamma = v(x)$, com $x \notin A$. Seja $y \in \omega$, com $y \neq x$. Usaremos o seguinte resultado que pode ser encontrado em [10]: "Seja I um A -ideal fracionário. Então $v(I : \overline{A}) = b + \mathbb{N}$, onde $b = \min \{a \in \mathbb{Z}; a + \mathbb{N} \in v(I)\}$. Em particular, $v(C) = \beta + \mathbb{N}$, onde β é o condutor de $v(A)$ e $C = A : \overline{A}$." Sendo assim, temos $v(xy) \in \gamma + \mathbb{N} \subset v(\omega : \overline{A})$, logo $xy \in \omega$ e daí $x \in \omega : \omega = A$, o que é um absurdo. Portanto $\gamma \notin v(\omega)$.

Seja $z \in \omega$. Suponha $v(z) \notin K$, onde $K = \{a; \gamma - a \notin S\}$. Dessa forma, $\gamma - v(z) \in S = v(A)$. Assim existe $w \in A$ tal que

$$v(w) = \gamma - v(z) \Rightarrow v(zw) = \gamma \Rightarrow \gamma \in v(\omega),$$

o que é um absurdo. Logo $v(z) \in K$ e $v(\omega) \subseteq K$.

Para finalizar a demonstração, basta mostrar a igualdade

$$\text{card}(v(\omega) \setminus v(C)) = \text{card}(K \setminus v(C)),$$

onde $C = A : \bar{A}$. De fato,

$$\begin{aligned} \text{card}(v(\omega) \setminus v(C)) &= l(\omega/C) = l(\bar{A}/A) \\ &= \text{card}(v(\bar{A}) \setminus v(A)) \\ &= \text{card}(\mathbb{N} \setminus S) \\ &= \text{card}(K \setminus (\beta + \mathbb{N})) \\ &= \text{card}(K \setminus v(C)). \end{aligned}$$

A segunda igualdade segue de $l(\bar{A}/\omega) = l(A/C)$ e a quinta de $\text{card}(\mathbb{N} \setminus S) = \text{card}((K - S) \setminus (K - N)) = \text{card}(K \setminus (S - \mathbb{N})) = \text{card}(K \setminus (\beta + \mathbb{N}))$, onde β é o condutor de S . ■

3.4 Anel Local em um ponto de uma curva

Uma **curva algébrica irredutível** $C \subset k^n$ é o lugar geométrico dos pontos cujas coordenadas cartesianas satisfazem uma equação polinomial

$$f(X_1, X_2, \dots, X_n) = 0,$$

onde f é um polinômio irredutível não constante.

Definição 3.25 *Se $C \subset k^2$ é uma curva algébrica irredutível, definimos o **anel de coordenadas** $A(C)$ como*

$$A(C) = \frac{k[X_1, X_2, \dots, X_n]}{\langle f \rangle},$$

onde $\langle f \rangle$ é o ideal gerado pelo polinômio f .

Uma vez que $A(C)$ é um domínio (pois C é irredutível se, e somente se $\langle f \rangle$ é primo), podemos falar do seu corpo quociente:

Definição 3.26 *O **corpo de frações** do anel $A(C)$ é o corpo*

$$k(C) = \left\{ \frac{h}{g}; h, g \in A(C), g \neq 0 \right\}$$

munido da relação de equivalência $\frac{h}{g} = \frac{h'}{g'}$ se, e somente se $hg' - h'g = 0$.

Definição 3.27 A cada ponto $P = (a_1, a_2, \dots, a_n) \in C$ corresponde um ideal primo $I = \langle X_1 - a_1, X_2 - a_2, \dots, X_n - a_n \rangle \subset A(C)$. O **anel local** de um ponto $P \in C$ é denotado e definido por

$$\mathcal{O}_P(C) := \left\{ \frac{h}{g} \in k(C); g \notin I \right\},$$

cujos ideal maximal é $M_P(C) = \left\{ \frac{h}{g} \in \mathcal{O}_P(C); h \in I \right\}$.

Foi provado em [5], que $\mathcal{O} \simeq \frac{k[[X_1, X_2, \dots, X_n]]}{\langle f \rangle} \simeq k[[x_1, x_2, \dots, x_n]]$, onde $x_1, x_2, \dots, x_n$ são as classes residuais de $X_1, X_2, \dots, X_n$ módulo $\langle f \rangle$. Como neste trabalho estamos considerando $\mathcal{O}$ unirramificado, então $\tilde{\mathcal{O}} \simeq k[[t]]$ (veja [6]).

Vimos, até agora, uma relação entre um anel e um semigrupo. A seguir, veremos alguns exemplos de como determinar o semigrupo de valores do anel local de uma curva C num ponto P .

Exemplo 3.28 Considere a curva $C : y^5 = x^2 \subset k^2$. A origem $P = (0, 0)$ é um ponto singular de C .

A curva admite a parametrização $x = t^5, y = t^2$. Temos

$$A(C) = \frac{k[x, y]}{\langle y^5 - x^2 \rangle} \simeq k[t^2, t^5]$$

e

$$\mathcal{O}_P(C) = \left\{ \frac{f(x)}{g(x)}; f, g \in k[t^5, t^2], g(0) \neq 0 \right\} \simeq k[[t^2, t^5]].$$

O semigrupo de valores de C é formado pelas valorizações de todos os polinômios do anel $\mathcal{O}_P(C)$, logo $S = \langle 2, 5 \rangle = \{0, 2, 4, 5, \rightarrow\}$.

Em geral, quando as classes residuais de $X_1, X_2, \dots, X_n$ módulo $\langle f \rangle$ são monômios, o semigrupo de valores de $\mathcal{O}_P(C)$ é gerado pelos expoentes destes.

Exemplo 3.29 Considere a parábola $C : y = x^2 \subset k^2$. O anel de coordenadas de C é

$$A(C) = \frac{k[x, y]}{\langle y - x^2 \rangle} = k[x, x^2] = k[x].$$

Sejam $P = (0, 0)$ e $I = \langle x, y \rangle = \langle x, x^2 \rangle = \langle x \rangle$. Então

$$\mathcal{O}_P(C) = \left\{ \frac{f(x)}{g(x)}; f, g \in k[x], g(0) \neq 0 \right\} \simeq k[[x]]$$

e

$$M_P(C) = \left\{ \frac{f(x)}{g(x)} \in \mathcal{O}_P(C); f(0) = 0 \right\}.$$

O semigrupo de valores de C é $S = \mathbb{N}$, uma vez que x gera todos os polinômios não constantes.

Vejamos um exemplo em que nem todas as classes residuais de $X_1, X_2, \dots, X_n$ módulo $\langle f \rangle$ são monômios.

Exemplo 3.30 *Considere a curva irredutível C com parametrização $x = t^4$, $y = t^6 + t^7$. Temos*

$$\mathcal{O}_P(C) = \left\{ \frac{f(x)}{g(x)}; f, g \in k[t^4, t^6 + t^7], g(0) \neq 0 \right\} \simeq k[[t^4, t^6 + t^7]].$$

A valorização de x é 4 e de y é 6. Observe que $(t^6 + t^7)^2 - (t^4)^3 = 2t^{13} + t^{14} \in \mathcal{O}_P(C)$, logo $v(2t^{13} + t^{14}) = 13 \in S$. O semigrupo de valores de C é $S = \langle 4, 6, 13 \rangle = \{0, 4, 6, 8, 10, 12, 13, 14, 16, \dots\} \neq \langle 4, 6 \rangle$.

Capítulo 4

Semigrupos de Anéis Gorenstein, Kunz e Arf

Neste capítulo introduzimos os conceitos de anéis Gorenstein, Kunz e Arf e de semigrupos simétricos, pseudo-simétricos e Arf, além da relação entre tais classes de anéis e de semigrupos.

4.1 Anéis Gorenstein e Semigrupos Simétricos

Um semigrupo S é dito **simétrico** se possui o condutor igual ao dobro do gênero, isto é, se $c = 2g$.

Uma propriedade importante de semigrupos simétricos: Se S é um semigrupo simétrico com condutor c , então um inteiro i é uma lacuna de S se, e somente se, $c - 1 - i$ é um elemento de S . De fato, como S é simétrico, a quantidade de lacunas e de elementos entre 0 e $c - 1$ é a mesma. Seja i uma lacuna de S e suponha que $c - 1 - i$ também o é. Assim existe $k \in \mathbb{N}$ tal que k e $c - 1 - k$ são elementos de S . Segue daí que $k + (c - 1 - k) = c - 1 \in S$, o que é um absurdo. Portanto $c - 1 - i \in S$. A prova da recíproca é análoga.

Um semigrupo pode ser representado através de um diagrama da seguinte forma: na primeira coluna e linha inferior coloca-se o condutor e nas colunas seguintes, dois inteiros cuja soma é o número de Frobenius, listados em ordem crescente na linha superior e decrescente na inferior. Bolinha preta significa que o número pertence ao semigrupo:

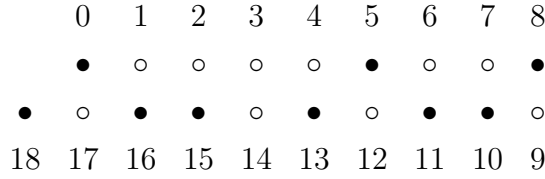


Diagrama do semigrupo $S = \langle 5, 8, 11 \rangle$.

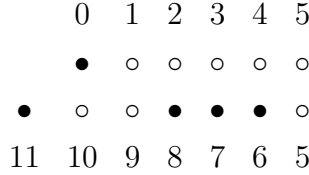


Diagrama do semigrupo $S_1 = \langle 6, 7, 8, 11 \rangle$.

Segue diretamente da propriedade anterior de semigrupo simétrico que o diagrama de um tal semigrupo possui bolinha preta em toda coluna, e obviamente esta deve ser única, uma vez que a soma dos dois elementos de uma mesma coluna é o número de Frobenius do semigrupo.

Exemplo 4.1 *O semigrupo $S = \langle 4, 6, 11 \rangle = \{0, 4, 6, 8, 10, 11, 12, 14, \rightarrow\}$ possui gênero 7 e condutor $14=2 \cdot 7$, portanto é simétrico.*

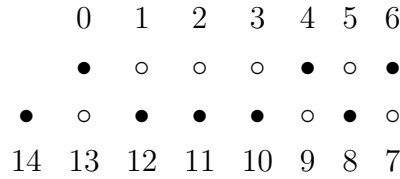


Diagrama de $S = \langle 4, 6, 11 \rangle$.

Exemplo 4.2 $S' = \langle 5, 6, 7, 8 \rangle = \{0, 5, 6, 7, 8, 10, \rightarrow\}$ é simétrico, pois possui gênero 5 e condutor 10.

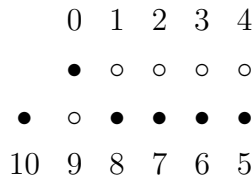


Diagrama de $S' = \langle 5, 6, 7, 8 \rangle$.

Proposição 4.3 *Sejam S um semigrupo e $K = \{c-1-a; a \notin S\}$ o ideal canônico definido na demonstração da Proposição 3.9. Então S é simétrico se, e somente se $S = K$.*

Demonstração: Observe que se o condutor c de S é par, então $S \subset K$, e se c é ímpar, então $S \setminus \{\frac{c-1}{2}\} \subset K$. Além disso, $\{c, \rightarrow\} \subset K$, pois dado $t \in \{c, \rightarrow\}$, temos $t = (c-1) - u$, com $u \in \mathbb{Z}_-^* \not\subset S$. Assim $\text{card}(K) = \text{card}(\{c, \rightarrow\} \cup (\mathbb{N} \setminus S))$. Logo S é simétrico se, e somente se $\text{card}(K) = \text{card}(S)$. Agora se S é simétrico, então tem condutor par. Assim $S \subset K$, donde segue o resultado. ■

Definição 4.4 Um anel A é dito **anel Gorenstein** se, e somente se A é um ideal canônico dele mesmo.

Observe que a caracterização de um anel como Gorenstein através da definição anterior não é uma tarefa simples. O próximo teorema mostra uma forma bem simples de determinar se um anel é Gorenstein ou não.

Teorema 4.5 Seja A como na Seção 3.2. Então A é Gorenstein se, e somente se o semigrupo $v(A)$ é simétrico.

Demonstração: Seja $v(A) = S$. Como A é Gorenstein se, e somente se $A = \omega$, onde ω é um ideal canônico de A , temos

$$A = \omega \Leftrightarrow 0 = l(\omega/A) = \text{card}(v(\omega) \setminus v(A)) = \text{card}(K \setminus S),$$

onde K é um ideal canônico de S . Logo $S = K$ e, portanto, S é simétrico. ■

4.2 Anéis Kunz e Semigrupos Pseudo-Simétricos

Um semigrupo S de gênero g e condutor c é dito um **semigrupo pseudo-simétrico** se $c = 2g - 1$.

Um propriedade importante de semigrupos pseudo-simétricos, semelhante à dos semigrupos simétricos, é a seguinte: Se S é um semigrupo pseudo-simétrico com condutor c , então qualquer inteiro i diferente de $\frac{c-1}{2}$ é uma lacuna de S se, e somente se, $c-1-i$ é um elemento de S . A demonstração desse fato é semelhante à dos semigrupos simétricos, levando-se em consideração que entre 0 e c há uma lacuna a mais que elementos de S , pois $\frac{c-1}{2} \notin S$.

Uma forma de identificar um semigrupo pseudo-simétrico através de seu diagrama é observando que, da propriedade anterior, o diagrama de um tal semigrupo possui única bolinha preta em todas as colunas, com exceção da última.

Exemplo 4.6 $S = \langle 4, 7, 9 \rangle = \{0, 4, 7, 8, 9, 11, \rightarrow\}$ é pseudo-simétrico com condutor 11 e gênero 6.

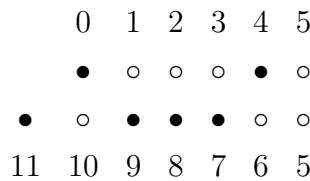


Diagrama de $S = \langle 4, 7, 9 \rangle$.

Dado um semigrupo S com número de Frobenius γ , definimos os seguintes conjuntos: $H(S) = \{a \in \mathbb{N}; \gamma - a \in S\}$ e $L(S) = \{a \in \mathbb{N}; a \notin S, \gamma - a \notin S\}$. Os elementos de $H(S)$ são chamados **furos do primeiro tipo** e os de $L(S)$, **furos do segundo tipo**.

Exemplo 4.7 *Seja $S = \{0, 4, 5, 8, 10, 12, \rightarrow\} = \langle 4, 5 \rangle$. Então $H(S) = \{1, 3, 6, 7, 11\}$ e $L(S) = \{2, 9\}$.*

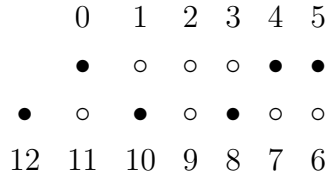


Diagrama do semigrupo $S_1 = \langle 4, 5 \rangle$.

Proposição 4.8 *Sejam S um semigrupo, c seu condutor e $L(S)$ os furos de segundo tipo de S . Então $L(S) = \{\frac{c-1}{2}\}$ se, e somente se S é pseudo-simétrico.*

Demonstração: Basta observar que $L(S) = K \setminus S$, onde $K = \{a; c - 1 - a \notin S\}$.
■

Exemplo 4.9 *Observe que os furos de segundo tipo são aqueles números em que não há bolinha preta na coluna no diagrama. Sendo assim, a proposição anterior fica claramente ilustrada através do diagrama abaixo do semigrupo pseudo-simétrico $S' = \langle 3, 5, 7 \rangle = \{0, 3, 5, \rightarrow\}$.*

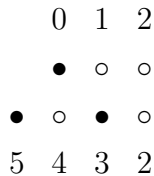


Diagrama de $S' = \langle 3, 5, 7 \rangle$.

Definição 4.10 *Um anel A é dito **anel Kunz** se, e somente se, $l(\omega/A) = 1$.*

Assim como para anéis Gorenstein, a caracterização de um anel Kunz através da definição anterior não é fácil. O próximo teorema é uma ferramenta muito interessante e simples para tal caracterização.

Teorema 4.11 *Um anel A é Kunz se, e somente se, $v(A)$ é pseudo-simétrico.*

Demonstração: Sejam $v(A) = S$, c o condutor de S e $L(S)$ os furos de segundo

tipo de S . Sabemos que A é Kunz se, e somente se $l(\omega/A) = 1$. Temos

$$\begin{aligned} l(\omega/A) = 1 &\Leftrightarrow \text{card}(v(\omega) \setminus v(A)) = 1 \\ &\Leftrightarrow \text{card}(K \setminus S) = 1 \\ &\Leftrightarrow \text{card}(L(S)) = 1 \\ &\Leftrightarrow L(S) = \left\{ \frac{c-1}{2} \right\}, \end{aligned}$$

o que equivale a termos S pseudo-simétrico. ■

4.3 Anéis Arf e Semigrupos Arf

Considere um semigrupo $S = \{\lambda_0 = 0, \lambda_1, \lambda_2, \dots, \lambda_r, \rightarrow\} \subseteq \mathbb{N}$. Dado $\lambda_k \in S$, definimos $S(k) = \{\beta - \lambda_k; \beta \in S, \beta \geq \lambda_k\}$.

Definição 4.12 Um semigrupo S é chamado **semigrupo Arf** se $S(k)$ é um semigrupo, para todo $\lambda_k \in S$.

Observe que se λ_r é o condutor de S e $\lambda_t \geq \lambda_r$, então $S(t) = \mathbb{N}$. Sendo assim, para verificar se um semigrupo é Arf, basta testar para $k < r$.

Exemplo 4.13 (a) Considere $S = \langle 3, 5, 7 \rangle = \{0, 3, 5, \rightarrow\}$. Temos

$$S(0) = \{\beta; \beta \in S, \beta \geq 0\} = S$$

$$S(1) = \{\beta - 3; \beta \in S, \beta \geq 3\} = \{0, 2, \rightarrow\} = \langle 2, 3 \rangle$$

Como $S(0), S(1)$ e $S(k)$, para $k \geq 2$, são semigrupos, então S é um semigrupo Arf.

(b) Considere, agora, $S' = \langle 3, 4 \rangle = \{0, 3, 4, 6, \rightarrow\}$. Temos

$$S'(0) = \{\beta; \beta \in S', \beta \geq 0\} = S'$$

$$S'(1) = \{\beta - 3; \beta \in S', \beta \geq 3\} = \{0, 1, 3, \rightarrow\}$$

$$S'(2) = \{\beta - 4; \beta \in S', \beta \geq 4\} = \{0, 2, \rightarrow\}$$

Como $S'(1)$ não é um semigrupo, então S' não é Arf.

Sejam $\mathcal{O}$ o anel local de um ponto P em uma curva C e $v(\mathcal{O})$ seu semigrupo de valores. Para cada $\alpha \in v(\mathcal{O})$, seja f_α um elemento de $\mathcal{O}$ tal que $v(f_\alpha) = \alpha$. Considere o conjunto

$$I_\alpha = \{g \in \mathcal{O}; v(g) \geq \alpha\}.$$

Afirmção: I_α é um ideal de $\mathcal{O}$.

De fato, sejam $g, h \in I_\alpha$. Então

$$v(g+h) \geq \min \{v(g), v(h)\} \geq \alpha.$$

Logo $g+h \in I_\alpha$. Sejam, agora, $g \in I_\alpha$ e $f \in \mathcal{O}$. Daí

$$v(fg) = v(f) + v(g) \geq \alpha,$$

ou seja, $fg \in I_\alpha$.

Sejam

$$\frac{I_\alpha}{f_\alpha} = \left\{ \frac{g}{f_\alpha}; g \in I_\alpha \right\}$$

e $\left[\frac{I_\alpha}{f_\alpha} \right]$ o menor subanel de $k[[t]]$ que contém $\frac{I_\alpha}{f_\alpha}$.

Proposição 4.14 *O anel $\left[\frac{I_\alpha}{f_\alpha} \right]$ independe da escolha do elemento f_α .*

Demonstração: Seja $f'_\alpha = \varepsilon f_\alpha$ um outro elemento de $\mathcal{O}$ tal que $v(f'_\alpha) = \alpha$, ou seja, $v(\varepsilon) = 0$. Como $\varepsilon \in \left[\frac{I_\alpha}{f_\alpha} \right]$, então $\varepsilon^{-1} \in \left[\frac{I_\alpha}{f_\alpha} \right]$. Daí

$$\frac{I_\alpha}{f'_\alpha} = \frac{I_\alpha}{\varepsilon f_\alpha} = \varepsilon^{-1} \frac{I_\alpha}{f_\alpha} \subseteq \left[\frac{I_\alpha}{f_\alpha} \right]$$

e, portanto, $\left[\frac{I_\alpha}{f'_\alpha} \right] \subseteq \left[\frac{I_\alpha}{f_\alpha} \right]$. Analogamente mostra-se $\left[\frac{I_\alpha}{f_\alpha} \right] \subseteq \left[\frac{I_\alpha}{f'_\alpha} \right]$.

Logo $\left[\frac{I_\alpha}{f'_\alpha} \right] = \left[\frac{I_\alpha}{f_\alpha} \right]$, como queríamos demonstrar. ■

Devido à independência da escolha de f_α , denotaremos o anel $\left[\frac{I_\alpha}{f_\alpha} \right]$ por $[I_\alpha]$.

O semigrupo $v([I_\alpha])$ contém o semigrupo gerado pelos inteiros $\beta - \alpha$, com $\beta \in v(\mathcal{O}), \beta \geq \alpha$, que são as valorizações dos elementos de $\frac{I_\alpha}{f_\alpha}$. Como pode ocorrer $[I_\alpha] \neq \frac{I_\alpha}{f_\alpha}$, podemos ter $v([I_\alpha]) \neq v\left(\frac{I_\alpha}{f_\alpha}\right)$, como no próximo exemplo.

Exemplo 4.15 *Considere o anel $\mathcal{O} = k[[t^3, t^7, t^{11}]]$. Podemos escrever*

$$\mathcal{O} = k[[t^3, t^7, t^{11}]] = k \oplus kt^3 \oplus kt^6 \oplus kt^7 \oplus kt^9 \oplus t^{11}k[[t]]$$

e daí $v(\mathcal{O}) = \langle 3, 7, 11 \rangle = \{0, 3, 6, 7, 9, 11, \rightarrow\}$. Temos

$$\frac{I_3}{t^3} = k \oplus kt^3 \oplus kt^4 \oplus kt^6 \oplus t^8k[[t]]$$

e o conjunto das valorizações dos elementos de $\frac{I_3}{t^3}$ é

$$v\left(\frac{I_3}{t^3}\right) = \{0, 3, 4, 6, 8, \rightarrow\}.$$

O anel $[I_3]$ gerado pelo conjunto $\frac{I_3}{t^3}$ é tal que $t^3 \cdot t^4 = t^7 \in [I_3]$ e $[I_3] = k + kt^3 + kt^4 + t^6k[[t]]$. Assim $v([I_3]) = \langle 3, 4 \rangle = \{0, 3, 4, 6, \rightarrow\}$.

Definição 4.16 Um subanel $\mathcal{O}$ do anel de séries de potências $k[[t]]$ é dito **anel Arf** se o conjunto $\frac{I_\alpha}{f_\alpha}$ é um anel, para todo $f_\alpha \in \mathcal{O} \setminus \{0\}$, isto é, se $\frac{I_\alpha}{f_\alpha} = [I_\alpha]$ para todo $\alpha \in v(\mathcal{O})$.

Se $\mathcal{O}$ é um anel Arf, então o conjunto

$$v([I_\alpha]) = \{\beta - \alpha; \beta \in v(\mathcal{O}), \beta \geq \alpha\}$$

é um semigrupo para qualquer $\alpha \in v(\mathcal{O})$, o que prova o seguinte teorema:

Teorema 4.17 O semigrupo de valores de um anel Arf é um semigrupo Arf.

Capítulo 5

Árvore de semigrupos

Neste capítulo estudamos a árvore de semigrupos, que nos mostra que a quantidade de semigrupos dado o gênero é finita, o que é crucial para o estudo de gonialidade e peso através dos semigrupos.

O estudo da árvore de semigrupos foi baseado no artigo *Towards a better understanding of the semigroup tree*, de M. Bras-Amoros e S. Bulygin, e focamos nosso estudo em semigrupos simétricos, pseudo-simétricos e Arf.

Sejam S um semigrupo, c seu condutor e g seu gênero. O conjunto

$$S' = S \cup \{c - 1\}$$

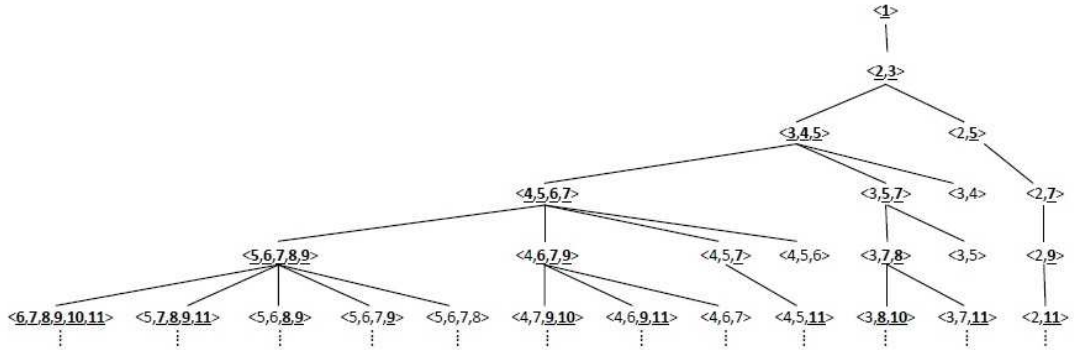
é claramente um semigrupo cujo gênero é $g - 1$. Dessa forma, todo semigrupo S de gênero g pode ser obtido a partir de um semigrupo S' de gênero $g - 1$ removendo um elemento de S' que seja maior ou igual ao seu condutor.

Proposição 5.1 *Sejam S um semigrupo e x um elemento de S . O conjunto $S^x = S \setminus \{x\}$ é um semigrupo se, e somente se, x é um gerador de S .*

Demonstração: Suponha que S^x é um semigrupo e que x não é um gerador de S . Dessa forma existem $a, b \in S$, $a \neq 0$, $b \neq 0$, tais que $x = a + b$. Como $a, b \in S^x$ mas $x \notin S^x$, segue que S^x não é fechado em relação à adição, o que contradiz o fato de S^x ser um semigrupo. Portanto x é um gerador de S .

Reciprocamente, suponha x é um gerador de S . Como $x \neq 0$, temos $0 \in S^x$. Sejam $a, b \in S^x \subset S$, a e b não nulos. S é fechado em relação à adição, $a + b \in S$. Como $S = S^x \cup \{x\}$, $a + b \in S^x$ desde que $a + b \neq x$. Como x é um gerador, temos o resultado. ■

Esta proposição mostra que os semigrupos de gênero g são obtidos a partir dos semigrupos de gênero $g - 1$ removendo um por um os geradores que são maiores que ou iguais ao condutor de cada semigrupo. Tais geradores são chamados **geradores efetivos**. O processo de retirada de geradores efetivos constrói a **árvore de semigrupos**, que é uma árvore infinita contendo todos os semigrupos numéricos. A raiz da árvore de semigrupos é o único semigrupo de gênero 0, isto é, o semigrupo numérico $\langle 1 \rangle = \mathbb{N}$. O i -ésimo nível contém todos os semigrupos de gênero i . Por convenção, quando construímos a árvore, o semigrupo S^x está à esquerda de S^y , se $x < y$. O "pai" de um semigrupo é obtido adicionando a este seu número de Frobenius.



Árvore de semigrupos numéricos.

Um semigrupo S da forma $\{0\} \cup [c, +\infty)$, onde c é o condutor de S , é chamado **semigrupo ordinário**.

Proposição 5.2 *O conjunto de geradores do semigrupo ordinário*

$S = \{0, g + 1, g + 2, \dots\}$ *é* $\{g + 1, g + 2, \dots, 2g + 1\}$ *e*

- 1) $S \setminus \{g + 1\}$ *possui* $g + 2$ *geradores efetivos*.
- 2) $S \setminus \{g + 2\}$ *possui* g *geradores efetivos*.
- 3) $S \setminus \{g + r\}$, *com* $2 < r \leq g + 1$, *possui* $g - r + 1$ *geradores efetivos*.

Demonstração: É claro que o conjunto de geradores do semigrupo ordinário $S = \{0, g + 1, g + 2, \dots\}$ é $\{g + 1, g + 2, \dots, 2g + 1\}$.

1) Observe que $S \setminus \{g + 1\}$ é um semigrupo ordinário com gênero $g + 1$, logo os seus geradores efetivos são $\{(g + 1) + 1, (g + 1) + 2, \dots, 2(g + 1) + 1\} = \{g + 2, g + 3, \dots, 2g + 3\}$, ou seja, possui $g + 2$ geradores efetivos.

2) Retirando-se $g + 2$ de S , o único elemento que não pode ser gerado pelos demais geradores é $(g + 1) + (g + 2) = 2g + 3$, logo tal elemento é o único a

virar gerador de $S \setminus \{g + 2\}$. Assim, $\{g + 3, g + 4, \dots, 2g + 1\} \cup \{2g + 3\}$ são os geradores efetivos de $S \setminus \{g + 2\}$, que são g .

3) Seja s um gerador qualquer de S diferente de $g + r$. Temos $s + (g + r) \geq 2g + 4$. Como qualquer número maior do que ou igual a $2g + 4$ pode ser gerado usando-se geradores de S diferentes de $g + r$, segue que o conjunto de geradores de $S \setminus \{g + r\}$ é $\{g + 1, g + 2, \dots, g + r - 1, g + r + 1, \dots, 2g + 1\}$. Assim, $S \setminus \{g + r\}$ possui $g - r + 1$ geradores efetivos. ■

A **enumeração** λ de um semigrupo S é a única aplicação bijetiva crescente $\mathbb{N} \rightarrow S$. Denotamos $\lambda(i)$ por λ_i . É fácil ver que $\lambda_i = i + g(i)$, onde $g(i)$ é o número de lacunas menores que λ_i .

Proposição 5.3 *Seja S um semigrupo não-ordinário com enumeração λ . Se $\lambda_{i_1} < \lambda_{i_2} < \dots < \lambda_{i_n}$ são os geradores efetivos de S , então os geradores efetivos de $S \setminus \{\lambda_{i_j}\}$ são $\lambda_{i_{j+1}}, \dots, \lambda_{i_n}$ ou $\lambda_{i_{j+1}}, \dots, \lambda_{i_n}, \lambda_{i_j} + \lambda_1$.*

Demonstração: Se x é um gerador de S diferente de λ_{i_j} , então x também é gerador de $S \setminus \{\lambda_{i_j}\}$. Como o condutor de $S \setminus \{\lambda_{i_j}\}$ é $\lambda_{i_j} + 1$, segue que $\lambda_{i_{j+1}}, \dots, \lambda_{i_n}$ são geradores efetivos de $S \setminus \{\lambda_{i_j}\}$.

Os elementos em $S \setminus \{\lambda_{i_j}\}$ que não são geradores em S e tornam-se geradores em $S \setminus \{\lambda_{i_j}\}$ devem ser da forma $\lambda_{i_j} + \lambda_r$, para algum $\lambda_r \in S$ (observe que os elementos da forma $\lambda_{i_j} + l$, onde l é uma lacuna de S , estão em S , pois λ_{i_j} é maior do que ou igual ao condutor de S , e não são gerados por λ_{i_j} , logo estão também em $S \setminus \{\lambda_{i_j}\}$). Mostremos que devemos ter $\lambda_r = \lambda_1$. Suponha $\lambda_r > \lambda_1$. Temos $\lambda_{i_j} + \lambda_r > \lambda_{i_j} + \lambda_1 > \lambda_{i_j}$, logo $\lambda_{i_j} + \lambda_r = \lambda_1 + \lambda_s$ para algum $\lambda_s \in S \setminus \{\lambda_{i_j}\}$. Segue daí que $\lambda_{i_j} + \lambda_r$ não é um gerador de $S \setminus \{\lambda_{i_j}\}$. Portanto o único elemento que não é gerador de S e pode (ou não) ser gerador de $S \setminus \{\lambda_{i_j}\}$ é $\lambda_{i_j} + \lambda_1$. ■

Seja S um semigrupo não ordinário. Dizemos que um gerador efetivo λ_{i_j} de S é **forte** se o conjunto dos geradores efetivos de $S \setminus \{\lambda_{i_j}\}$ é $\{\lambda_{i_{j+1}}, \dots, \lambda_{i_n}, \lambda_{i_j} + \lambda_1\}$. Um gerador efetivo que não é forte é chamado **fraco**.

Exemplo 5.4 *Considere o semigrupo $S_2 = \langle 4, 6, 7, 9 \rangle = \{0, 4, 6, \rightarrow\}$. Os geradores efetivos 6 e 7 são fortes pois $S_2^6 = \{0, 4, 7, \rightarrow\} = \langle 4, 7, 9, 10 \rangle$ e $S_2^7 = \{0, 4, 6, 8, \rightarrow\} = \langle 4, 6, 9, 11 \rangle$ e 9 é um gerador fraco pois, como $4 + 9 = 13 = 6 + 7$, temos $S_2^9 = \{0, 4, 6, 7, 8, 10, \rightarrow\} = \langle 4, 6, 7 \rangle$.*

Um semigrupo sem descendentes na árvore de semigrupos é chamado **folha**; com apenas um descendente, **galho**; com dois ou mais descendentes, **arbusto**.

Exemplo 5.5 O semigrupo $S = \langle 5, 8, 11 \rangle$ não possui geradores efetivos, assim não possui descendentes sendo, assim, uma folha; $S_1 = \langle 6, 7, 8, 11 \rangle$ possui 11 como único gerador efetivo, logo tem um único descendente e é um galho; $S_2 = \langle 4, 6, 7, 9 \rangle$ possui 6, 7 e 9 como geradores efetivos, logo possui três descendentes na árvore de semigrupos e é um arbusto.

A seguir, veremos como procurar por semigrupos simétricos, pseudo-simétricos e Arf na árvore de semigrupos.

5.1 Semigrupos simétricos

Como visto anteriormente, um semigrupo S é dito **simétrico** se possui o condutor igual ao dobro do gênero, isto é, se $c = 2g$.

Os semigrupos da forma $\langle 2, 2n + 1 \rangle, n \geq 1$ são simétricos de gênero n e condutor $2n$. Eles são chamados semigrupos **hiperelípticos**. Para $n > 1$, tais semigrupos possuem apenas um gerador efetivo, que é o sucessor do condutor e, portanto, são galhos.

Dado um semigrupo S com enumeração λ , a ν -**sequência** associada a S é definida por $\nu_i = \# \{j \in \mathbb{N} : \lambda_i - \lambda_j \in S\}$.

Exemplo 5.6 Para o semigrupo $S = \langle 4, 6, 11 \rangle = \{0, 4, 6, 8, 10, 11, 12, 14, \rightarrow\}$, temos

$$\begin{aligned}\nu_0 &= \# \{j \in \mathbb{N} : \lambda_0 - \lambda_j \in S\} = \# \{0\} = 1 \\ \nu_1 &= \# \{j \in \mathbb{N} : \lambda_1 - \lambda_j \in S\} = \# \{0, 1\} = 2 \\ \nu_2 &= \# \{j \in \mathbb{N} : \lambda_2 - \lambda_j \in S\} = \# \{0, 2\} = 2 \\ \nu_3 &= \# \{j \in \mathbb{N} : \lambda_3 - \lambda_j \in S\} = \# \{0, 1, 3\} = 3 \\ \nu_4 &= \# \{j \in \mathbb{N} : \lambda_4 - \lambda_j \in S\} = \# \{0, 1, 2, 4\} = 4 \\ \nu_5 &= \# \{j \in \mathbb{N} : \lambda_5 - \lambda_j \in S\} = \# \{0, 5\} = 2, \\ &\text{e assim por diante.}\end{aligned}$$

Proposição 5.7 $\nu_i = i - g(i) + \#D(i) + 1$, onde $g(i)$ é o número de lacunas menores que λ_i e $D(i) = \{l \notin S : 0 < l < \lambda_i, \lambda_i - l \notin S\}$.

Demonstração: Considere os conjuntos $J(i) = \{j \in \mathbb{N} : \lambda_i - \lambda_j \notin S\}$ e $K(i) = \{l \notin S : \lambda_i - l \in S\}$. Temos:

$$\nu_i + \#D(i) + \#J(i) + \#K(i) = g(i) + i + 1.$$

Como $\#J(i) = \#K(i)$ (pois esse é o número de formas de se escrever λ_i como

soma de um elemento e uma lacuna de S) e $\#J(i) = g(i) - \#D(i)$, temos o resultado. ■

Exemplo 5.8 *Considerando o semigrupo do exemplo 5.6, temos:*

$$\begin{aligned}
D(0) &= \{l \notin S : \lambda_0 - l \notin S\} = \emptyset \Rightarrow \\
\nu_0 &= 0 - g(0) + \#D(0) + 1 = 0 - 0 + 0 + 1 = 1 \\
D(1) &= \{l \notin S : \lambda_1 - l \notin S\} = \{1, 2, 3\} \Rightarrow \\
\nu_1 &= 1 - g(1) + \#D(1) + 1 = 1 - 3 + 3 + 1 = 2 \\
D(2) &= \{l \notin S : \lambda_2 - l \notin S\} = \{1, 3, 5\} \Rightarrow \\
\nu_2 &= 2 - g(2) + \#D(2) + 1 = 2 - 4 + 3 + 1 = 2 \\
D(3) &= \{l \notin S : \lambda_3 - l \notin S\} = \{1, 3, 5, 7\} \Rightarrow \\
\nu_3 &= 3 - g(3) + \#D(3) + 1 = 3 - 5 + 4 + 1 = 3 \\
D(4) &= \{l \notin S : \lambda_4 - l \notin S\} = \{1, 3, 5, 7, 9\} \Rightarrow \\
\nu_4 &= 4 - g(4) + \#D(4) + 1 = 4 - 6 + 5 + 1 = 4 \\
D(5) &= \{l \notin S : \lambda_5 - l \notin S\} = \{2, 9\} \Rightarrow \\
\nu_5 &= 5 - g(5) + \#D(5) + 1 = 5 - 6 + 2 + 1 = 2.
\end{aligned}$$

Proposição 5.9 *Um elemento $\lambda_i \in S$ é um gerador se, e somente se, $\nu_i = 2$.*

Demonstração: Seja $\lambda_i \in S$ um gerador. Se $k \in \{j \in \mathbb{N} : \lambda_i - \lambda_j \in S\}$, então $\lambda_i - \lambda_k = \lambda_r$, para algum $r \in \mathbb{N}$, ou seja, $\lambda_i = \lambda_r + \lambda_k$. Logo $\lambda_r = 0$ e $\lambda_k = \lambda_i$ ou $\lambda_r = \lambda_i$ e $\lambda_k = 0$, pois λ_i é gerador. Portanto $\nu_i = \#\{j \in \mathbb{N} : \lambda_i - \lambda_j \in S\} = 2$.

Reciprocamente, seja λ_i tal que $\nu_i = 2$. Assim $\{j \in \mathbb{N} : \lambda_i - \lambda_j \in S\} = \{0, i\}$ pois S é um semigrupo. Logo não existe $k \in \mathbb{N}, k \neq 0, k \neq i$ tal que $\lambda_i - \lambda_k = \lambda_r$, onde $\lambda_k, \lambda_r \in S$, ou seja, λ_i não pode ser escrito como combinação linear de dois elementos não-nulos de S . Portanto λ_i é um gerador de S . ■

O seguinte resultado segue diretamente das Proposições 5.7 e 5.9.

Proposição 5.10 *Em um semigrupo numérico S com enumeração λ , gênero g e condutor c , um elemento $\lambda_i \geq c$ é um gerador se, e somente se, $\#D(i) = g - i + 1$.*

Proposição 5.11 *Semigrupos simétricos não hiperelípticos são folhas.*

Demonstração: Vamos mostrar que um semigrupo simétrico não hiperelíptico não possui geradores efetivos, logo não possui descendentes na árvore de semigrupos.

Em um semigrupo simétrico S com enumeração λ , condutor c e gênero g , $\lambda_i \geq c$ se, e somente se, $i \geq g$. Assim, para que λ_i seja um gerador efetivo de S devemos ter $\#D(i) \leq 1$, ou seja, se $\lambda_i = c$ e $\#D(i) = 1$ ou $\lambda_i = c+1$ e $\#D(i) = 0$.

1ª situação: $\lambda_i = c$ e $\#D(i) = 1$

Não é possível pois, como $1 \notin S, c-1 \notin S$ e $1 + (c-1) = c$, deveríamos ter $1 = c-1$, caso contrário teríamos $\#D(i) \geq 2$. Mas $1 = c-1$ significa que $c = 2$, daí o semigrupo simétrico seria hiperelíptico.

2ª situação: $\lambda_i = c+1$ e $\#D(i) = 0$

Só é possível em semigrupos hiperelípticos, uma vez que em outros semigrupos temos $2 \notin S, c-1 \notin S$ e $2 + (c-1) = c+1$, o que implica $\#D(i) \geq 2$. ■

5.2 Semigrupos pseudo-simétricos

Lembremos que **semigrupos pseudo-simétricos** são aqueles semigrupos nos quais o condutor é o dobro do gênero menos um.

Proposição 5.12 *Em um semigrupo não ordinário S com enumeração λ e condutor c , um elemento $\lambda_i \neq 2\lambda_1$ é um gerador forte se, e somente se, $\lambda_i \geq c$ e $\nu_{i+\lambda_1} = 4$.*

Demonstração: Suponha λ_i um gerador forte. Se g é o gênero de S , então temos $\lambda_{i+\lambda_1} = i + \lambda_1 + g = i + g + \lambda_1 = \lambda_i + \lambda_1$, logo $\lambda_{i+\lambda_1} - \lambda_1 = \lambda_i$ e $\lambda_{i+\lambda_1} - \lambda_i = \lambda_1$. Assim, como $0, \lambda_1, \lambda_i$ e $\lambda_{i+\lambda_1}$ são diferentes, então $\nu_{i+\lambda_1} \geq 4$. Se $\nu_{i+\lambda_1} > 4$, então existe $\lambda_l \in S$ com $l \neq 0, l \neq 1, l \neq i, l \neq i + \lambda_1$ tal que $\lambda_{i+\lambda_1} - \lambda_l \in S$, o que contradiz o fato de $\lambda_{i+\lambda_1}$ ser gerador de $S \setminus \{\lambda_i\}$ e de λ_i ser um gerador forte. Portanto $\nu_{i+\lambda_1} = 4$.

Reciprocamente, suponha $\lambda_i \geq c$ e $\nu_{i+\lambda_1} = 4$. Então λ_i é um gerador de S pois se existissem $\lambda_l, \lambda_m \in S$ com $0 < l \leq m < i$ tais que $\lambda_i = \lambda_l + \lambda_m$, teríamos $\lambda_{i+\lambda_1} - \lambda_l = \lambda_m + \lambda_1 \in S$ e daí $\nu_{i+\lambda_1} > 4$. Além disso, como $\nu_{i+\lambda_1} = 4$ segue que $\lambda_{i+\lambda_1}$ só pode ser subtraído por $0, \lambda_1, \lambda_i$ e $\lambda_{i+\lambda_1}$ dentro do semigrupo. Consequentemente, $\lambda_{i+\lambda_1}$ é um gerador de $S \setminus \{\lambda_i\}$ e λ_i é um gerador forte. ■

Proposição 5.13 *1) O único semigrupo pseudo-simétrico de gênero g com apenas um intervalo de elementos entre 0 e o condutor é*

$$S_{ps_g} = \{0, g, g+1, \dots, 2g-3, 2g-1, \rightarrow\}.$$

2) O semigrupo $S_{ps_3} = \{0, 3, 5, \rightarrow\}$ possui 5 e 7 como únicos geradores efetivos. O gerador 5 é forte e o gerador 7 é fraco.

3) O semigrupo $S_{ps_4} = \{0, 4, 5, 7, \rightarrow\}$ possui apenas 7 como gerador efetivo e este é forte.

4) O semigrupo S_{ps_g} , para $g \geq 5$, é um galho, seu único gerador efetivo é c e este é fraco.

Demonstração: 1) Como S_{ps_g} é pseudo-simétrico, existem g lacunas e $g - 1$ elementos no conjunto $\{0, 1, \dots, 2g - 2\}$, sendo $g - 1$ uma lacuna. O intervalo procurado deve ter $g - 2$ elementos, uma vez que $0 \in S_{ps_g}$. Os candidatos a intervalos são $I = \{1, \dots, g - 2\}$ e $J = \{g, \dots, 2g - 3\}$. O intervalo I não pode ser o procurado pois, como $1 \in I$, teríamos $S_{ps_g} = \mathbb{N}$, que não é pseudo-simétrico. Portanto temos o resultado.

2) Temos $S_{ps_3} = \{0, 3, 5, \rightarrow\} = \langle 3, 5, 7 \rangle$, logo 5 e 7 são os únicos geradores efetivos. O semigrupo obtido quando retiramos o 5 é $S_{ps_3}^5 = \{0, 3, 6, \rightarrow\} = \langle 3, 7, 8 \rangle$, logo 5 é forte. Já o semigrupo obtido quando retiramos o 7 é $S_{ps_3}^7 = \{0, 3, 5, 8, \rightarrow\} = \langle 3, 5 \rangle$. Portanto 7 é fraco.

3) Temos $S_{ps_4} = \{0, 4, 5, 7, \rightarrow\} = \langle 4, 5, 7 \rangle$, logo 7 é o único gerador efetivo. O semigrupo obtido quando retiramos tal gerador é $S_{ps_4}^7 = \{0, 4, 5, 8, \rightarrow\} = \langle 4, 5, 11 \rangle$, logo 7 é forte.

4) Como o condutor de S_{ps_g} é $2g - 1$, segue que os números maiores que ou iguais a $4g - 2$ não podem ser geradores. Temos $4g - 3 = (2g - 3) + 2g$ e $4g - 4 = (2g - 3) + (2g - 1)$, logo $4g - 3$ e $4g - 4$ também não são geradores efetivos. Os números $2g, 2g + 1, \dots, 4g - 7, 4g - 6$ são gerados pelos números $g, g + 1, \dots, 2g - 3$, logo também não são geradores. Sendo assim, os únicos possíveis geradores efetivos de S_{ps_g} são $4g - 5$ e $c = 2g - 1$.

É claro que c é um gerador, pois não pode ser gerado pelos elementos de S menores que ele.

Se $g \geq 4$ então $4g - 5 \geq g + (2g - 1)$, e assim $4g - 5$ não é um gerador.

Por outro lado, $c = 2g - 1$ é um gerador fraco se e somente se $(2g - 1) + g$ é soma de dois elementos de S menores que $2g - 1$, ou seja, $2g - 1$ é fraco se, e somente se, $(2g - 1) + g \leq (2g - 3) + (2g - 3)$, o que é equivalente a $g \geq 5$. ■

Proposição 5.14 1) Um semigrupo com enumeração λ é pseudo-simétrico e pos-

sua $\lambda_1 = 3$ se, e somente se, é igual a

$$S = \{0, 3, 6, \dots, 3k, 3(k+1), 3(k+1)+1, 3(k+2), 3(k+2)+1, \dots, 3(2k), 3(2k)+1, 3(2k)+3, \rightarrow\},$$

para $k > 0$, ou

$$S = \{0, 3, 6, \dots, 3k, 3(k+1)-1, 3(k+1), 3(k+2)-1, 3(k+2), \dots, 3(2k-1)-1, 3(2k-1), 3(2k-1)+2, \rightarrow\},$$

para $k > 1$.

2) Com exceção de $\langle 3, 4, 5 \rangle$ e $\langle 3, 5, 7 \rangle$, cada semigrupo pseudo-simétrico com $\lambda_1 = 3$ possui único gerador efetivo que é $c+2$ e este é fraco.

3) Os descendentes de um semigrupo pseudo-simétrico com $\lambda_1 = 3$ e único gerador efetivo são semigrupos simétricos não hiperelípticos e, portanto, folhas.

Demonstração: 1) Seja S um semigrupo pseudo-simétrico com $\lambda_1 = 3$, gênero g e condutor c . Dado $j \in \mathbb{N}$, há três possibilidades para o condutor de S : $c = 3j$, $c = 3j+1$ ou $c = 3j+2$.

1º caso: $c = 3j, j \in \mathbb{N}$

Como S é pseudo-simétrico, segue $c = 2g - 1$. Daí

$$3j = 2g - 1 \Rightarrow g = \frac{3j+1}{2}, \text{ com } j \text{ ímpar.}$$

Usando a propriedade de semigrupos pseudo-simétricos ($\frac{c-1}{2} \neq i \in S$ se, e somente se, $c-1-i \notin S$) e o fato que $3 \in S$ implica $3m \in S$, para todo $m \in \mathbb{N}$, temos, para $0 \leq m < j$:

$$3m \in S \Leftrightarrow 3j-1-3m \notin S \Leftrightarrow 3(j-m)-1 = 3(j-m-1)+2 \notin S$$

Dessa forma, já identificamos j lacunas dentre as $j + \frac{j+1}{2}$ de S e j elementos dentre os $j + \frac{j-1}{2}$ de S . Dentre os j números da forma $3m+1$ entre 0 e $3j-1$, as lacunas devem ser os $\frac{j+1}{2}$ primeiros, pois $3 \in S$ e $3 + (3m+1) = 3(m+1)+1$.

$$\text{Resumindo: } \begin{cases} 3m \in S, & 0 \leq m < j \\ 3m+2 \notin S, & 0 \leq m < j \\ 3m+1 \notin S, & 0 \leq m \leq \frac{j-1}{2} \\ 3m+1 \in S, & \frac{j-1}{2} < m < j. \end{cases}$$

Colocando $j-1 = 2k$, temos

$$S = \{0, 3, 6, \dots, 3k, 3(k+1), 3(k+1)+1, 3(k+2), 3(k+2)+1, \dots, 3(2k), 3(2k)+1, 3(2k)+3, \rightarrow\}.$$

2º caso: $c = 3j+1, j \in \mathbb{N}$

O condutor de S não pode ter essa forma uma vez que $c - 1 \notin S$, porém $c - 1 = 3j$ e $3 \in S$.

3º caso: $c = 3j + 2, j \in \mathbb{N}$

Fazendo raciocínio análogo ao 1º caso, temos:

$$3j + 2 = 2g - 1 \Rightarrow g = \frac{3(j+1)}{2}, j \text{ ímpar.}$$

Para $0 \leq m \leq j$, temos:

$$3m \in S \Leftrightarrow 3j + 1 - 3m \notin S \Leftrightarrow 3(j - m) + 1 \notin S$$

Já temos $j + 1$ lacunas dentre as $j + 1 + \frac{j+1}{2}$ de S e $j + 1$ elementos dentre os $j + 1 + \frac{j-1}{2}$ de S . Logo:

$$\begin{cases} 3m \in S, & 0 \leq m \leq j \\ 3m + 1 \notin S, & 0 \leq m \leq j \\ 3m + 2 \notin S, & 0 \leq m \leq \frac{j-1}{2} \\ 3m + 2 \in S, & \frac{j-1}{2} < m < j. \end{cases}$$

Colocando $j + 1 = 2k$, temos:

$$S = \{0, 3, 6, \dots, 3k, 3(k+1) - 1, 3(k+1), 3(k+2) - 1, 3(k+2), \dots, 3(2k-1) - 1, 3(2k-1), 3(2k-1) + 2, \rightarrow\}$$

A prova da recíproca é simples: pelas construções feitas anteriormente, vê-se que tais conjuntos são semigrupos pseudo-simétricos, para todo $k \in \mathbb{N}$.

2) Um elemento maior que ou igual ao condutor deve ser $c + i = \lambda_{c-g+i}$, para algum $i \geq 0$. Como os semigrupos são pseudo-simétricos, segue

$$c = 2g - 1 \Rightarrow c - g + i = g + i - 1.$$

Pela Proposição 5.10, λ_i é gerador de S se, e somente se, $\#D(i) = g - i + 1$. Daí λ_{g+i-1} é gerador se, e somente se, $\#D(i) = 2 - i$. Como $\#D(g + i - 1) \geq 0$, segue que $i \leq 2$. Logo os únicos candidatos a geradores efetivos são $c, c + 1$ e $c + 2$.

Analisando os dois tipos de semigrupos apresentados no item 1), se S for do primeiro tipo, temos $c = [3(2k)] + 3$ e $c + 1 = [3(2k) + 1] + 3$ e se S for do segundo tipo temos $c = 3(2k - 1) + 2 = [3(2k - 1) - 1] + 3$ e $c + 1 = [3(2k - 1)] + 3$, portanto c e $c + 1$ não são geradores. Vamos mostrar que $c + 2$ é um gerador.

Semigrupos do primeiro tipo:

Temos $c + 2 = 3(2k) + 3 + 2 = 6k + 5$, logo $c + 2$ possui resto 2 módulo 3. Como todos os elementos menores que $c + 2$ possuem resto 0 ou 1 módulo 3, se $c + 2$ não fosse gerador então seria a soma de dois elementos que possuem resto 1 módulo 3, ou seja, $c + 2 = 3(k + i) + 1 + 3(k + j) + 1 = 6k + 3i + 3j + 2$, para alguns $i, j \geq 1$. Daí

$$6k + 3i + 3j + 2 = 6k + 5 \Rightarrow 3(i + j) = 3 \Rightarrow i + j = 1$$

o que é uma contradição. Portanto $c + 2$ é um gerador.

Semigrupos do segundo tipo:

Temos $c + 2 = 3(2k - 1) + 2 + 2 = 6k + 1$, logo $c + 2$ possui resto 1 módulo 3. Nesse tipo de semigrupo todos os elementos menores que $c + 2$ possuem resto 0 ou 2 módulo 3. Assim, se $c + 2$ não fosse gerador, seria a soma de dois elementos que possuem resto 2 módulo 3, ou seja, $c + 2 = 3(k + i) - 1 + 3(k + j) - 1 = 6k + 3i + 3j - 2$ para alguns $i, j \geq 1$. Daí

$$6k + 3i + 3j - 2 = 6k + 1 \Rightarrow 3(i + j) = 3 \Rightarrow i + j = 1,$$

o que é uma contradição. Logo $c + 2$ é um gerador.

Mostremos, agora, que $c + 2$ é um gerador fraco. Suponha $\lambda_k = c + 2$. Como $\lambda_k > c$, segue $\lambda_{k+\lambda_1} = c + 2 + 3 = c + 5$, logo $k + \lambda_1 = \lambda_{k+\lambda_1} - g = c + 5 - g = 2g - 1 + 5 - g = g + 4$. Pela Proposição 5.7 temos $\nu_{k+\lambda_1} = k + \lambda_1 - g + \#D(k + \lambda_1) + 1$. Supondo que $c + 2$ é forte temos, pela Proposição 5.12,

$$4 = g + 4 - g + \#D(k + \lambda_1) + 1 \Rightarrow \#D(K + \lambda_1) = -1,$$

o que é um absurdo. Portanto $c + 2$ é fraco.

3) O único descendente de S é $S \setminus \{c + 2\}$, o qual é simétrico pois seu gênero é $g + 1$ e seu condutor é $c + 3 = 2g - 1 + 3 = 2g - 2 = 2(g + 1)$. É claro que $S \setminus \{c + 2\}$ não é hiperelíptico já que $\lambda_1 = 3$. Portanto, pela Proposição 5.11, $S \setminus \{c + 2\}$ é uma folha. ■

Proposição 5.15 *Cada semigrupo pseudo-simétrico com $\lambda_1 \neq 3$ e com mais de um intervalo de elementos entre 0 e o condutor é uma folha.*

Demonstração: Para mostrarmos que um semigrupo como do enunciado é uma folha, devemos mostrar que esse semigrupo não possui geradores efetivos.

Seja $\lambda_k \geq c$, ou seja, $k \geq c - g$. Pela Proposição 5.10, λ_k é um gerador se, e somente se, $\#D(k) = g - k + 1$. Logo λ_k é gerador se, e somente se,

$$\#D(k) \leq g - (c - g) + 1 = 2g - (2g - 1) + 1 = 2.$$

Assim há três casos a considerar: $\lambda_k = c$ e $\#D(k) = 2$ ou $\lambda_k = c + 1$ e $\#D(k) = 1$ ou $\lambda_k = c + 2$ e $\#D(k) = 0$.

1º caso: $\lambda_k = c$ e $\#D(k) = 2$

Como existe mais de um intervalo de elementos entre 0 e c , existe $i \in S$, $i \neq 0, i \neq c - 2$, tal que $i + 1 \notin S$. Pela propriedade de semigrupos pseudo-simétricos, segue que $c - i - 1 \notin S$ (pois $i \in S$). Assim, temos $c = (c - i - 1) + (i + 1) = 1 + (c - 1)$, onde nenhuma das parcelas é um elemento de S . Portanto $\#D(k) \geq 4$ e c não é um gerador.

2º caso: $\lambda_k = c + 1$ e $\#D(k) = 1$

Não é possível uma vez que $c + 1 = 2 + (c - 1)$, $2 \notin S, c - 1 \notin S$ e $2 \neq c - 1$ (S é pseudo-simétrico com $\lambda_1 \neq 3$). Logo $c + 1$ também não é gerador.

3º caso: $\lambda_k = c + 2$ e $\#D(k) = 0$

É impossível, pois como $\lambda_1 \neq 3$, então 3 e $c - 1$ são lacunas. Temos $c + 2 = 3 + (c - 1)$, logo $c + 2$ não é um gerador de S . ■

5.3 Semigrupos Arf

Vejamos outra definição de semigrupo Arf:

Definição 5.16 Um semigrupo S com enumeração λ é dito **Arf** se $\lambda_i + \lambda_j - \lambda_k \in S$, para todos $i, j, k \in \mathbb{N}$ com $i \geq j \geq k$.

Observe que se λ_r é o condutor de S e $\lambda_i \geq \lambda_r$, então, para todos j, k tais que $i \geq j \geq k$, a condição de semigrupo Arf é naturalmente respeitada. Sendo assim, para verificarmos se um semigrupo é Arf, basta considerarmos os casos onde $k \leq j \leq i < r$.

Exemplo 5.17 $S = \langle 3, 5, 7 \rangle = \{0, 3, 5, \rightarrow\}$ é um semigrupo Arf. Já $S' = \langle 3, 4 \rangle = \{0, 3, 4, 6, \rightarrow\}$ não é Arf, pois $4 + 4 - 3 \notin S'$.

Proposição 5.18 As Definições 4.12 e 5.16 de semigrupo Arf são equivalentes.

Demonstração: Observe que se λ_r é o condutor de S , então $S(k)$ contém todos os inteiros maiores que ou iguais a $\lambda_r - \lambda_k = h_{k_s}$ e

$$S(k) = \{h_{k_0} = 0, h_{k_1}, h_{k_2}, \dots, h_{k_s}, \rightarrow\},$$

onde $h_{k_l} = \lambda_{k+l} - \lambda_k$.

Suponha que S é um semigrupo Arf segundo a Definição 4.12, ou seja,

$$S(k) = \{\beta - \lambda_k; \beta \in S, \beta \geq \lambda_k\}$$

é um semigrupo, para todo $\lambda_k \in S$. Tome $\lambda_t \in S$. Dados $h_{t_{l_1}}, h_{t_{l_2}} \in S(t)$, temos $h_{t_{l_1}} + h_{t_{l_2}} \in S(t)$, ou seja,

$$(\lambda_{t+l_1} - \lambda_t) + (\lambda_{t+l_2} - \lambda_t) = \lambda_{t+l_3} - \lambda_t \Rightarrow \lambda_{t+l_1} + \lambda_{t+l_2} - \lambda_t = \lambda_{t+l_3} \in S.$$

Mas λ_t é qualquer, logo temos o resultado.

Suponha, agora, que S é um semigrupo Arf segundo a Definição 5.16. Seja $\lambda_t \in S$. Vamos mostrar que $S(t)$ é um semigrupo.

* $0 \in S(t)$ pois $0 = \lambda_t - \lambda_t$.

* Sejam $h_{t_{l_1}}, h_{t_{l_2}} \in S(t)$. Temos

$$h_{t_{l_1}} + h_{t_{l_2}} = (\lambda_{t+l_1} - \lambda_t) + (\lambda_{t+l_2} - \lambda_t) = (\lambda_{t+l_1} + \lambda_{t+l_2} - \lambda_t) - \lambda_t \in S(t),$$

pois, por hipótese, temos $\lambda_{t+l_1} + \lambda_{t+l_2} - \lambda_t \in S$.

* $\lambda_r - \lambda_t = h_{t_s}$ é o condutor de $S(t)$ pela observação inicial. ■

A proposição seguinte mostra uma forma mais simples de determinar quando um semigrupo é Arf.

Proposição 5.19 Um semigrupo S é Arf se, e somente se, para quaisquer $i, k \in \mathbb{N}$ tais que $i \geq k$ tem-se $2\lambda_i - \lambda_k \in S$.

Demonstração: Suponha S Arf. Se $i = j$, da definição de semigrupo Arf temos $2\lambda_i - \lambda_k \in S$.

Reciprocamente, suponha que, para quaisquer $i, k \in \mathbb{N}$ tais que $i \geq k$, tem-se $2\lambda_i - \lambda_k \in S$. Sejam $i, j, k \in \mathbb{N}$ tais que $k \leq j \leq i < r$, onde λ_r é o condutor de S . Mostremos que $m = \lambda_i + \lambda_j - \lambda_k \in S$. Se $i = j$ ou $j = k$, então não há nada a fazer. Por outro lado, se $k < j < i$, ponha $i_0 = i, j_0 = j, k_0 = k$ e escreva $m = \lambda_{i_0} + \lambda_{j_0} - \lambda_{k_0} = (2\lambda_{j_0} - \lambda_{k_0}) + \lambda_{i_0} - \lambda_{j_0}$. Note que $2\lambda_{j_0} - \lambda_{k_0} \in S$ por hipótese e $2\lambda_{j_0} - \lambda_{k_0} > \lambda_{j_0}$. Sejam i_1, j_1, k_1 definidos por

$$\begin{aligned}\lambda_{i_1} &= \max \{2\lambda_{j_0} - \lambda_{k_0}, \lambda_{i_0}\}, \\ \lambda_{j_1} &= \min \{2\lambda_{j_0} - \lambda_{k_0}, \lambda_{i_0}\}, \\ \lambda_{k_1} &= \lambda_{j_0}.\end{aligned}$$

Logo $m = \lambda_{i_1} + \lambda_{j_1} - \lambda_{k_1}$, com $i_1 \geq j_1 > k_1$ e $i_1 \geq i_0, j_1 \geq j_0, k_1 > k_0$. Se $i_1 = j_1$, o resultado segue da hipótese. Se $i_1 \neq j_1$, podemos repetir o raciocínio obtendo três sequências crescentes de inteiros (i_t) , (j_t) e (k_t) tais que $m = \lambda_{i_t} + \lambda_{j_t} - \lambda_{k_t}$ com $i_t \geq j_t \geq k_t$. Há duas possibilidades:

* existe um índice h tal que $i_h = j_h$ ou $j_h = k_h$ e nesse caso $m \in S$;

* $i_t > j_t > k_t$, para todo t , e nesse caso a sequência (j_t) é crescente por construção. Logo existe h tal que $j_h \geq r$, daí $m > c$. Portanto $m \in S$. ■

Seja S um semigrupo com enumeração λ . Se S é um semigrupo hiperelíptico, então S é Arf, pois dados $k \leq j \leq i < r$, onde λ_r é o condutor, segue que $\lambda_i + \lambda_j - \lambda_k \in 2\mathbb{N} \subset S$. Na verdade os semigrupos hiperelípticos são os únicos semigrupos Arf que são simétricos, como mostra a proposição a seguir.

Proposição 5.20 *Se S é um semigrupo Arf e simétrico, então S é hiperelíptico.*

Demonstração: Seja c o condutor de S . Se S é Arf e $\lambda \in S$, com $\lambda < c$, então $\lambda + 1 \notin S$ pois caso contrário teríamos $2(\lambda + 1) - \lambda = \lambda + 2 \in S$. Daí seguindo o mesmo raciocínio teríamos $\lambda + 3, \lambda + 4, \dots \in S$, o que contradiz $\lambda < c$. Dessa forma dois inteiros consecutivos no intervalo $[0, c]$ não podem ser elementos de S .

Sendo S simétrico segue que dois inteiros consecutivos no intervalo $[0, c]$ também não podem ser lacunas de S , pois se $i, i + 1$ são lacunas de S então $c - i - 1, c - i - 2$ são elementos de S .

Como $0 \in S$, então $2 \in S$. Portanto S é hiperelíptico. ■

Proposição 5.21 *Em um semigrupo Arf S , um elemento $\lambda_i \neq 0, \lambda_i \neq \lambda_1$ é um gerador se, e somente se, $\lambda_i - \lambda_1 \notin S$.*

Demonstração: Seja $\lambda_i \in S, \lambda_i \neq 0, \lambda_i \neq \lambda_1$ um gerador de S . É claro que $\lambda_i - \lambda_1 \notin S$, pois, caso contrário, existiria $\lambda_j \in S$ tal que $\lambda_i = \lambda_1 + \lambda_j$ e λ_i não seria gerador de S .

Reciprocamente suponha $\lambda_i - \lambda_1 \notin S$ e que λ_i não é um gerador de S . Então existem $\lambda_j, \lambda_k \in S$, com $i > j \geq k$ tais que $\lambda_i = \lambda_j + \lambda_k$. Daí $\lambda_i - \lambda_1 = \lambda_j + \lambda_k - \lambda_1 \in S$, pois S é Arf, o que é uma contradição. Portanto λ_i é um gerador. ■

Proposição 5.22 *1) Semigrupos Arf não hiperelípticos são arbustos.*

2) Semigrupos Arf aparecem como descendentes de semigrupos com geradores fortes quando removemos um tal gerador.

Demonstração: 1) Em um semigrupo Arf S com condutor c sabemos que se $i, i+1 \in S$, então $i \geq c$. Logo $c-2$ ou $c-3$ são lacunas de S , assim como $c-1$. Como $\lambda_1 \geq 3$ (pois S é não hiperelíptico) segue da Proposição 5.21 que $c-1+\lambda_1$ e $c-2+\lambda_1$ ou $c-3+\lambda_1$ são geradores efetivos de S . Portanto S é um arbusto.

2) Seja λ_i um gerador de um semigrupo numérico Arf S e considere o semigrupo $S \cup \{\lambda_i - \lambda_1\}$. Como λ_i é gerador de S segue que $\lambda_i - \lambda_1$ é um gerador forte de $S \cup \{\lambda_i - \lambda_1\}$ e temos, portanto, o resultado. ■

Exemplo 5.23 *O semigrupo $S = \langle 3, 5, 7 \rangle = \{0, 3, 5, \rightarrow\}$ possui $S^5 = \langle 3, 7, 8 \rangle = \{0, 3, 6, \rightarrow\}$ e $S^7 = \langle 3, 5 \rangle = \{0, 3, 5, 6, 8, \rightarrow\}$ como descendentes. O semigrupo S^5 é Arf e foi obtido de S retirando o gerador 5, que é forte. O semigrupo S^7 não é Arf e foi obtido de S retirando o gerador 7 que é fraco.*

Exemplo 5.24 *O semigrupo $S = \langle 3, 7, 8 \rangle = \{0, 3, 6, \rightarrow\}$ possui descendentes $S^7 = \langle 3, 8, 10 \rangle = \{0, 3, 6, 8, \rightarrow\}$ que é Arf, e $S^8 = \langle 3, 7, 11 \rangle = \{0, 3, 6, 7, 9, 11, \rightarrow\}$ que não é Arf. Observe que os geradores 7 e 8 são ambos fortes.*

Referências Bibliográficas

- [1] M. Bras-Amoros, S. Bulygin. *Towards a better understanding of the semigroup tree*. Semigroup Forum, (2008).
- [2] D. F. N. Lara. *Semigrupos de Anéis Quase Gorenstein, Arf e Kunz*. Dissertação de Mestrado. UFMG (2010).
- [3] T. Hickmann. *Anéis de Arf e caracteres*. Dissertação de Mestrado. UEM (2010).
- [4] J. Fromentin. *Exploring the tree of numerical semigroups*. arxiv:1305.3831v1[math.CO], (2013).
- [5] L. N. de Oliveira. *Caracterização dos Germes de Curvas Planas Irredutíveis com Torção Maximal*. Dissertação de Mestrado. UFES (2011).
- [6] A. M. S. Lannes. *Semigrupos e o Teorema de Gorenstein para Singularidades de Curvas Algébricas Planas*. Dissertação de Mestrado. UFES (2013).
- [7] W. Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*. W. A. Benjamin, (2008).
- [8] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin (1993).
- [9] K. O. Stöhr. *On the poles of regular differentials of singular curves*. Boletim da SBM, 24:105-136 (1993).
- [10] M. Rosenlicht. *Equivalence Relations on Algebraic Curves*. Annals of Mathematics, Second Series, Vol.56, No. 1, pp. 169-191 (1952).
- [11] A. Grothendieck. *Theoremes de Dualite pour les Faisceaux Algebriques Coherents*. Seminaire Bourbaki, 4, 169-193 (1957).
- [12] V. Barucci, D. E. Dobbes, M. Fontana. *Maximality Properties in Numerical Semigroups, with Applications to One-Dimensional Analytically*

Irreducible Local Domains. Lecture Notes in Pure and Applied Mathematics. 153 (1994).

- [13] J. Lipman. *Stable Ideals and Arf Rings*. American Journal of Mathematics, 93, 649-685 (1971).
- [14] E. Kunz. *The Value-Semigroup of a One-Dimensional Gorenstein Ring*. Proceedings of The American Mathematical Society, 25, 748-751 (1970).