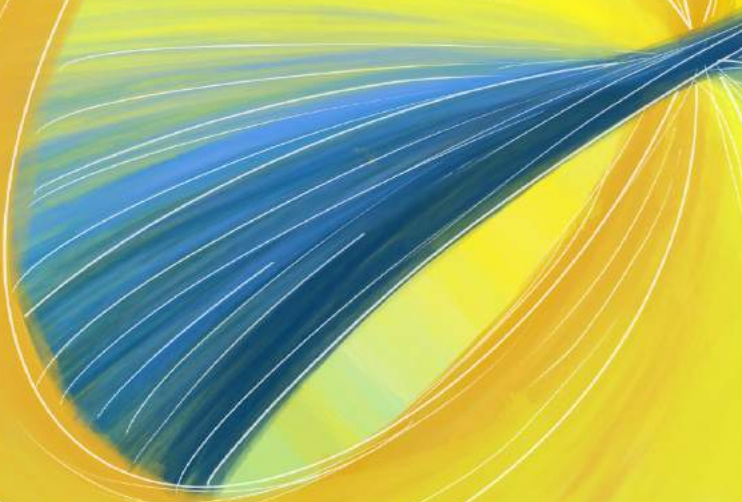
Códigos Geométricos

Uma introdução via corpos de funções algébricas



Gilberto Brito de Almeida Filho
Saeed Tafazolian

impa

33º Colóquio Brasileiro de Matemática

Códigos Geométricos

Uma introdução via corpos de funções algébricas

Códigos geométricos, uma introdução via corpos de funções algébricas
Primeira impressão, julho de 2021

ISBN 978-65-89124-49-8
MSC (2020) Primary: 14H05, Secondary: 12F05, 11T71, 94B05

Coordenação Geral Carolina Araujo

Produção Books in Bytes **Capa** Izabella Freitas & Jack Salvador

Realização da Editora do IMPA
IMPA
Estrada Dona Castorina, 110
Jardim Botânico
22460-320 Rio de Janeiro RJ

www.impa.br
editora@impa.br

Sumário

1 Corpos de Funções Algébricas

1.1 Propriedades de Curvas

Neste capítulo abordaremos a teoria geral de Corpos de Funções Algébricas: Lugares, Divisores, anéis de valorização e Espaço de Riemann–Roch.

A menos de menção do contrário, neste capítulo sempre consideraremos K um corpo arbitrário.

Para um polinômio $f(x,y) \in K[x,y]$ a curva plana afim associada à f é o conjunto

$$\mathcal{X}_f := \left\{(a:b) \in \overline{K}^2 |\ f(a,b) = 0\right\}.$$

De forma análoga, dado polinômio homogêneo $F(X,Y,Z) \in K[X,Y,Z]$ a curva plana projetiva associada à F é o conjunto

$$\mathcal{X}_F := \left\{(a:b:c) \in \mathbb{P}^2(\overline{K}) |\ F(a,b,c) = 0\right\}.$$

Observamos que a partir de uma polinômio afim podemos obter um polinômio homogêneo e vise versa. Com efeito, seja $f(x,y) \in K[x,y]$ com $deg(f) = r$ então *homogenizando* f obtemos $F(X,Y,Z) = Z^r f(\frac{X}{Z}, \frac{Y}{Z})$. Reciprocamente, dado um polinômio homogêneo $F(X,Y,Z) \in K[X,Y,Z]$ obtemos um polinômio

em $K[x, y]$ *desomogenizando* com relação à uma das três variáveis $F(X, Y, 1)$, $F(X, 1, Z)$, $F(1, Y, Z)$. Estas operações de desomogenizar e homogenizar polinômios também cria uma relação entre os pontos das curvas, isto é, dado um ponto $(a, b) \in \overline{K}^2$ da curva afim $\mathcal{X}_f$ então temos que $(a : b : 1) \in \mathbb{P}^2(\overline{K})$ é um ponto da curva projetiva homogenizada $Z^r f(\frac{X}{Z}, \frac{Y}{Z})$. Por outro lado, se $(a : b : c) \in \mathbb{P}^2(\overline{K})$ com $Z \neq 0$ (resp. $X \neq 0$, ou $Y \neq 0$) é um ponto pertencente ao polinômio homogêneo $F(X, Y, Z)$ então $(a : b : 1)$ é um ponto da curva afim $F(x, y, 1)$ (resp. $F(1, y, z)$, $F(x, 1, z)$). O ponto $(a : b : 1)$ (com $Z \neq 0$) é chamado de *ponto afim* da curva $F(X, Y, Z)$, quando $Z = 0$ dizemos que o ponto está no *infinito*.

Sejam $\mathcal{X}_F$ um curva e $p \in \mathcal{X}_F$ ponto. Dizemos que p é um *ponto singular* se

$$\begin{aligned} F_X(p) &= 0; \\ F_Y(p) &= 0; \\ F_Z(p) &= 0, \end{aligned}$$

onde F_X, F_Y, F_Z denotam as derivadas parciais em relação a cada variável. Caso contrário dizemos que p é um *ponto não singular*. Neste caso, a reta tangente em um ponto não singular é dada por

$$F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0.$$

Curvas que não contém pontos singulares são chamadas de *curvas não singulares*.

A vantagem de utilizar curvas não singulares é que podemos obter o gênero destas curvas utilizando apenas o grau do polinômio. Mais precisamente, se $\mathcal{X}_F$ é uma curva não singular, então o gênero de $\mathcal{X}_F$ é

$$g = \frac{(deg(F) - 1)(deg(F) - 2)}{2}. \tag{1.1}$$

Ressaltamos que para curvas planas em geral a formula para o calculo do gênero é um pouco diferente da formula acima.

Exemplo 1.1.1. *Seja K um corpo com* $\mathrm{Char}(K) \neq 2$. *Considere a curva dada pela equação*

$$F : Y^2T - (X - c_1T)(X - c_2T)(X - c_3T)$$

com $c_1, c_2, c_3 \in K$ distintos entre si. As derivadas parciais são:

$$\begin{aligned} F_X =& (X - c_2T)(X - c_3T) + (X - c_1T)(X - c_3T) + (x - c_1T)(X - c_2T); \\ F_Y =& 2YT; \\ F_T =& -c_1(X - c_2T)(X - c_3T) - c_2(X - c_1T)(X - c_3T) - c_3(X - c_1T)(X - c_2T), \end{aligned}$$

igualando as três derivadas a zero, obtemos que a única solução possível é $(0:0:0)$ *e desta forma* F *é não singular. Utilizando a formula do gênero, temos que* $g(F) = 1$.

Uma $\mathcal{X}_F$ curva definida sobre um corpo K é dita ser *geometricamente irredutível* sobre K se o polinômio F é irredutível sobre $\overline{K}$. Vamos sempre estar assumindo que uma curva é geometricamente irredutível.

Sobre as considerações acima podemos ver alguns exemplos:

Exemplo 1.1.2 (Curva Hermitiana)**.** *Seja q potência de um primo. Considere a equação* $X^{q+1} = Y^q Z + Y Z^q$. *Esta equação é chamada de* Curva Hermitiana $\mathcal{H}_q$ *definida sobre* $\mathbb{F}_{q^2}$. *Algumas propriedades de* $\mathcal{H}_q$

- *é geometricamente irredutível.*
- *As derivadas parciais de* $\mathcal{H}_q$ *são:* $F_X = X^q,\ F_Y = -Z^q,\ F_Z = Y^q$.

Vemos que $\mathcal{H}_q$ *é não singular. Vamos analisar um caso particular. Considerando* $q = 2$, *podemos facilmente calcular* $\mathbb{F}_{q^2} = \frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$, *ie,* $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ *com* $\alpha^2 = 1 + \alpha$.

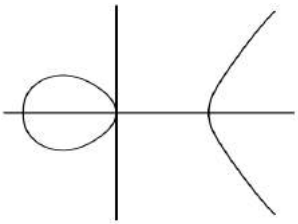
$\mathcal{H}_2$ *possui pontos no infinito? Resposta: O único ponto no infinito é o ponto* $P_\infty := (0:1:0)$, *pois* $\mathcal{H}_2 : (\frac{X}{Z})^{q+1} - (\frac{Y}{Z})^q - \frac{Y}{Z}$. *E esse é o único ponto em* $\mathcal{H}_2$ *quando* $Z = 0$.

De forma análoga podemos mostrar que $(0:1:0)$ *é o único ponto no infinito de* $\mathcal{H}_q$ *com* $Z = 0$.

Exemplo 1.1.3. *Seja* $K = \mathbb{Q}$. *Considere a equação* $G(X, Y, T) = Y^2T - X^3 + XT^2$. *então as derivadas parciais são:*

$$\begin{aligned} F_X &= 3X^2 - T^2; \\ F_Y &= 2YT; \\ F_T &= Y^2 - 2XT. \end{aligned}$$

Pela igualdade $F_Y = 0$ *temos que* $T = 0$ *ou* $Y = 0$. *Se* $T = 0$ *então por* $F_X = F_T = 0$ *temos* $X = Y = 0$. *Se* $Y = 0$ *então por* $F_X = F_T = 0$ *concluímos* $X = T = 0$. *Portanto, G é não singular e possui gênero um. Seja* $P = (T : X : Y)$ *um ponto na curva, quando* $T = 0$ *temos que* $Y = 0$ *e portanto* $P = P_\infty = (0:1:0)$ *é o único ponto no infinito. Abaixo podemos ver a figura do gráfico curva.*

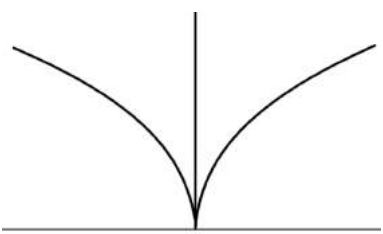


Exemplo 1.1.4. *Seja* $K = \mathbb{R}$. *Considere o polinômio* $g(X,Y,Z) := Y^2Z^3 - X^5 - X^3Z^2$

$$\begin{aligned} g_X &= -(5X^4 + 3X^2Z^2) \\ g_y &= 2YZ^3 \\ g_Z &= 3Z^2Y^2 - 2X^3Z, \end{aligned} \quad ;$$

Como as derivadas não se anulam simultaneamente, temos que g é não singular.

Abaixo podemos ver a figura do gráfico curva.



Como podemos constatar no próximo exemplo, existem curvas que são singulares.

Exemplo 1.1.5. *Seja* $K = \mathbb{F}_q$ *um corpo com* $q = l^3$ *elementos. Considere a curva dada pela equação* $F : Y^{l^2} - YT^{l^2-1} = X^{l^2-l+1}T^{l-1}$. *Então temos que as derivadas parciais são:*

$$\begin{aligned} F_X &= (l^2 - l + 1)X^{l^2-l}T^{l-1}; \\ F_Y &= (l^2)Y^{l^2-1} - T^{l^2-1}; \\ F_T &= (l^2 - 1)YT^{l^2-2} - (l-1)X^{l^2-l+1}T^{l-2} \end{aligned} \quad ,$$

é uma curva singular, com um único ponto singular para $T = 0$. *De fato, de* $F_Y = 0$ *temos que* $Y = 0$ *logo* $(0:1:0)$ *é o único ponto singular.*

Como um dos nossos principais objetivos é o estudo sobre corpos finitos, convém mostrarmos que sobre um corpo finito sempre existem polinômio irredutíveis. Donde segue a motivação do próximo exemplo.

Exemplo 1.1.6. *Seja $\mathbb{F}_q$ um corpo com q elementos. Para cada natural n existe um polinômio irredutível em $\mathbb{F}_q$ de grau n.*

Vamos denotar por $N_q(n)$ o número de polinômios mônico irredutíveis de grau n em $\mathbb{F}_q$.

Afirmação 1:

Seja $f \in \mathbb{F}_q[x]$ mônico, irredutível de grau d. $f|x^{q^n} - x \iff d|n$. De fato, se $d|n$ então $\mathbb{F}_q \subset \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$. Seja α uma raiz qualquer de f em alguma extensão de $\mathbb{F}_q$, logo $d = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ e portanto $\mathbb{F}_{q^d} = \mathbb{F}_q(\alpha)$. Assim, $\alpha \in \mathbb{F}_{q^n}$ e $\alpha^{q^n} - \alpha = 0$ então $f|x^{q^n} - x$. Reciprocamente, se $f|x^{q^n} - x$ considere α uma raiz qualquer de f em alguma extensão de $\mathbb{F}_q$, logo $\alpha^{q^n} - \alpha = 0$ e assim $\alpha \in \mathbb{F}_{q^n}$ e portanto $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$, isto é, $d|n$.

Afirmação 2:

Para cada natural n, $x^{q^n} - x$ é igual ao produto de todos os polinômios irredutíveis sobre $\mathbb{F}_q$ com grau dividindo n.

Com efeito, pela afirmação 1 temos que cada polinômio mônico irredutível com grau dividindo n aparece pelo menos uma vez na fatoração de $x^{q^n} - x$. Como $x^{q^n} - x$ é separável, então cada irredutível aparece exatamente uma única vez na fatoração de $x^{q^n} - x$.

Afirmação 3:

$q^n = \sum_{d|n} d N_q(d)$. *para cada natural n.*

De fato, segue da afirmação 2 comparando o grau de cada lado da igualdade.

*(**Fato:** **Fórmula de inversão de Möbius**)*

Seja $f(n)$ uma função sobre os naturais e $F(n) = \sum_{d|n} f(d)$. Então, para cada natural n temos que

$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}).$$

Então obtemos que

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

E portanto $N_q(n) > 0$ para cada natural n. Para mais detalhes sobre a Fórmula de inversão de Möbius veja (Martinez et al. 2018).

Ao longo deste livro iremos estudar mais aspectos destas e de outras curvas, nos apropriando da linguagem de curvas e corpos de funções.

1.2 Introdução à Corpos de Funções Algébricos

Começamos esta seção relembrando a definição de base de transcendência. Considere F/K uma extensão qualquer de corpos. Dizemos que um conjunto T de F é *algebricamente dependente* se existe um número natural n, um polinômio não nulo $p(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ e ainda elementos distintos $t_1, \ldots, t_n \in T$ satisfazendo $f(t_1, \ldots, t_n) = 0$. No caso contrário dizemos que T é *algebricamente independente* sobre K.

Usando a inclusão de conjuntos algebricamente independentes podemos aplicar o Lema de Zorn para obter um conjunto maximal algebricamente independente. Este conjunto maximal chamaremos de *base de transcendência* de F/K.

Exemplo 1.2.1. *Considere $p(x, y) \in \mathbb{Q}[x, y]$ dado por $p(x, y) = x^3 + y - 1$. Definindo o corpo quociente $F = \frac{\mathbb{Q}[x,y]}{p(x,y)}$ temos que as variáveis $z = \frac{x}{p(x,y)}$ e $w = \frac{y}{p(x,y)}$ são uma base de transcendência de F sobre $\mathbb{Q}$.*

Da definição de base de transcendência, vemos que uma mesma extensão não temos unicidade com relação a base. Porém, como veremos no próximo resultado, a cardinalidade é invariante.

Teorema 1.2.1. *Qualquer duas bases de transcendência possuem mesma cardinalidade.*

A partir da seguinte definição concentraremos nosso estudo em extensões com base de transcendência de tamanho 1.

Definição 1.2.1. *Um* corpo de funções algébricas *F/K de uma variável sobre K é uma extensão de corpos $K \subset F$ tal que F é uma extensão algébrica finita de $K(x)$ para algum elemento $x \in F$ que é transcendente sobre K.*

Para facilitar referências futuras, iremos abreviar Corpos de Funções Algébricos para Corpos de Funções.

No caso em que F/K é uma extensão com base de transcendência de tamanho $s \geqslant 2$ dizemos que F é um corpo de funções algébrico de n variáveis.

Exercício 1.2.1. *Considere o conjunto* $\mathcal{K} := \{u \in F \mid u \text{ é algebrico sobre } K\}$. *Mostre que com as operações de usuais de* F, $\mathcal{K}$ *é um subcorpo de* F.

O corpo $\mathcal{K}$ é chamado *corpo de constantes* de F/K.

Seja F/K uma extensão de corpos. Um subconjunto finito $\{x_1, \ldots, x_r\} \subset F$ é algebricamente independente sobre K se não existe $p(t_1, \ldots, t_r)$ em $K[t_1, \ldots, t_r]$ satisfazendo $p(x_1, \ldots, x_r) = 0$. Um subconjunto $S \subset F$ é algebricamente independente sobre K se todos os subconjuntos finitos de S são algebricamente independentes sobre K.

Uma base de transcendência da extensão F/K é um subconjunto $\mathcal{A}$ de F que satisfaz:

- $\mathcal{A}$ é algebricamente independente.
- $\mathcal{A} \subset \mathcal{A}'$ e $\mathcal{A}'$ é um subconjunto algebricamente independente de F, então $\mathcal{A} = \mathcal{A}'$.

Portanto, chamamos de *grau de transcendência*, e denotamos por $trdeg(F/K)$, a cardinalidade da base transcendência de F/K.

Sobre o grau de transcendência de F/K temos dois resultados importantes: *F/K é uma extensão algébrica se, e somente se,* $trdeg(F/K) = 0$.

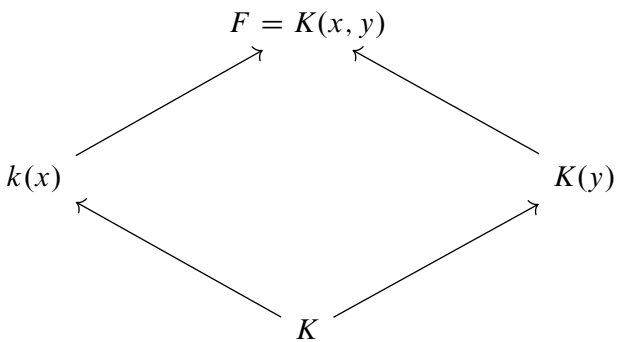
Se F é algébrico sobre $K(A)$, para algum subconjunto A de F, então A contém uma base de transcendência de F/K.

Exemplo 1.2.2. *O* corpo de funções racionais F/K *é chamado racional, denotamos por* $F = K(x)$, *para algum* $x \in F$ *que é transcendente sobre* K. *Mais adiante iremos explorar esse exemplo de forma mais profunda.*

Exemplo 1.2.3. *Seja* $K = \mathbb{Q}$ *e considere* $p(X, Y) = X^3 - Y^2 + Y + 1 \in K[X, Y]$. *Considere o quociente* $F = \frac{K[X,Y]}{p(X,Y)}$. *Fazendo* $x := X \ mod \ p(X, Y)$ *e* $y := Y \ mod \ p(X, Y)$ *temos que* $F = K(x, y)$ *com* $x^3 = y^2 - y - 1$ *é um corpo de funções algébricas de uma variável.*

Da Teoria de Extensões de Corpos podemos obter uma representação para F/K através de uma equação polinomial. Uma vez que x é transcendente sobre K temos que $F/K(x)$ é uma extensão finita. Se tomarmos qualquer outro elemento transcendente y sobre K então x e y terão uma relação de dependência sobre K uma vez que o grau de transcendência é um. Em outras palavras, existe um polinômio $p(z, w) \in K[z, w]$ tal que $p(x, y) = 0$. Desta forma, concluímos que x é algébrico sobre $K(y)$ (via $p(z, y) \in K(y)[z]$) e y algébrico sobre $K(x)$

(via $p(x, w) \in K(x)[w]$). Vendo o corpo de funções F/K como $F = K(x, y)$ podemos escolher estudar a extensão mais conveniente pois podemos ver como duas extensões, isto é, podemos ver F como extensão de $k(x)$ ou de $K(y)$. Conforme diagrama abaixo.



Observamos que a definição acima pode ser resgatada se partimos de uma curva plana projetiva (ou afim). Seja $\mathcal{X}_F$ um curva plana algébrica, projetiva, irredutível sobre um corpo K associada ao polinômio homogêneo $F \in K[X, Y, Z]$.

Desta forma consideramos o seguinte conjunto

$$\frac{K(X,Y,Z)}{(F)} := \left\{ \overline{G}(X,Y,Z) |\ G(X,Y,Z) \in K(X,Y,Z)\ G \text{ homogêneo} \right\},$$

onde $\overline{G}(X, Y, Z)$ denota a classe do polinômio G. Tal conjunto é um domínio de integridade, pois F é irredutível. Dizemos que dois polinômios são equivalentes se sua diferença é múltipla de F. Isto nos permite construir o corpo de frações $\mathcal{Q}_F$. Para avaliar uma tal fração em um ponto projetivo, queremos o resultado não dependa do representante do representante escolhido. Portanto, exigimos que o numerador e o denominador tenham um representantes ambos com o mesmo grau. O corpo de funções de $\mathcal{X}_F$, denotado por $K(\mathcal{X}_F)$, é o conjunto de elementos de $\mathcal{Q}_F$ admitindo uma tal representação (O caso afim é obtido de forma similar). Esses elementos recebem o nome de *funções racionais* de $\mathcal{X}_F$. Um elemento $z \in K(\mathcal{X}_F)$ é chamado de *função regular* em um ponto p se $z = \frac{G(X,Y,Z)}{Q(X,Y,Z)}$ com $Q(p) \neq 0$. Observe portanto que toda função racional tem um número finito de pontos onde ela não é regular.

Dentro do Corpo das Funções Racionais $K(x)$ encontramos um conjuntos com algumas propriedades interessantes. Considere um polinômio mônico irredutível

$f(x) \in K[x]$. Definimos o seguinte conjunto

$$\mathcal{O}_f := \left\{ \frac{u(x)}{v(x)} | \; u(x), v(x) \in K[x], \; f(x) \nmid u(x) \right\}.$$

Verificamos que este conjunto satisfaz as seguintes propriedades:

- É um anel;
- $K \subset \mathcal{O}_f \subset F, \mathcal{O} \neq F, \; K$;
- Para todo $z \in F$ temos que $z \in \mathcal{O}_f$ ou $z^{-1} \in \mathcal{O}_f$.

Exercício 1.2.2. *Mostre que o conjunto $\mathcal{O}_f$ definido acima é de fato as propriedades são satisfeitas. Mostre ainda que se $g(x)$ é outro polinômio mônico irredutível então $\mathcal{O}_f \neq \mathcal{O}_g$*

Estes fatos motivam a seguinte definição.

Definição 1.2.2. *Um* anel de valorização *de um corpo de funções F/K é um anel $\mathcal{O} \subset F$ tal que:*

- *$K \subset \mathcal{O} \subset F, \mathcal{O} \neq F, \; K$ e*
- *para todo $z \in F$ temos que $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.*

Como veremos a seguir este anel possui propriedades muito interessantes. Uma delas em especial será abordada quando tentarmos calcular um tipo especial de conjunto de números naturais.

Para um anel de valorização $\mathcal{O}$, considere o conjunto de todos os elementos invertíveis de $\mathcal{O}$, isto é, $\mathcal{O}^* = \{y \in \mathcal{O} | \; \exists w \in \mathcal{O}$ tal que $yw = 1\}$. Para o próximo resultado, lembramos que um *anel local* é um anel com único ideal maximal.

Proposição 1.2.1. *Dado um anel de valorização qualquer $\mathcal{O}$ de F/K, as seguintes propriedades são validas:*

a) $P := \mathcal{O} \setminus \mathcal{O}^*$ é único ideal maximal de $\mathcal{O}$, isto é, $\mathcal{O}$ é um anel local.

b) Dado $0 \neq u \in F$, temos que $u \in P$ se, e somente se, $u^{-1} \notin \mathcal{O}$.

Demonstração. a) P é um ideal maximal de $\mathcal{O}$.

- P é um ideal: Sejam $x, y \in P$ e $z \in \mathcal{O}$ temos claramente que xz não é invertível, logo $xz \in P$. Pela definição $\mathcal{O}$ temos que $x/y \in \mathcal{O}$ ou $y/x \in \mathcal{O}$. Sem perda de generalidade podemos assumir que $y/x \in \mathcal{O}$. Então $x + y = x(1 + y/x) \in \mathcal{O}$.
- P é maximal: Seja I um ideal tal que $P \subsetneq I \subset \mathcal{O}$, então dado $x \in J$ temos que x é invertível e portanto $J = \mathcal{O}$.

Segue da definição de P que ele é o único.

b) Dado $u \in F$. Se $u \in P$ então $u^{-1} \notin \mathcal{O}$, pois caso contrário, teríamos que $1 = uu^{-1} \in P$ o que é um absurdo. A reciproca é imediata.

□

Se considerarmos $\mathcal{K}$ o corpo de constantes de F/K podemos observar que $\mathcal{K} \subset \mathcal{O}$ e que $\mathcal{K} \cap P = \{0\}$ (Deixamos a verificação deste fato para o leitor).

Definição 1.2.3. *O ideal P definido no item* 1. *do Teorema* 8 *é chamado de* place *do corpo de funções F/K. Vamos denotar o conjunto de todos os places de F/K por $\mathbb{P}(F)$.*

No contexto de curvas à definição análoga é a seguinte: Seja Y uma curva e $p \in Y$ um ponto. $\mathcal{O}_q(Y) := \mathcal{O}_p$ é o conjunto de funções definidas em p. O ideal maximal deste anel é $m_p(Y) := \{f \in \mathcal{O}_q(Y) |\ f(p) = 0\}$ e portanto temos o equivalente em curvas à um place.

Proposição 1.2.2. *Seja $\mathcal{O}$ um anel de valorização de F/K, cujo ideal maximal é P e $0 \neq x \in P$. Dados elementos $x_1, \ldots, x_m \in P$ tais que $x = x_1$ e $x_j \in x_{j+1}P$ para $i = 1, \ldots, m-1$. Então*

$$m \leqslant [F, K(x)] < \infty.$$

Demonstração. Como $F/K(x)$ é uma extensão finita, basta mostrarmos que $\{x_1, \ldots, x_m\}$ é um conjunto linearmente independente sobre $K(x)$. Para provar este fato, vamos supor que existe um relação de dependência, i.e., existem $f_1(x)$, ..., $f_m(x) \in K(x)$ tais que $\sum_{i=1}^{m} f_i(x)x_i = 0$. Desta relação podemos supor que cada $f_i \in k[x]$ pois se tratam de elementos da forma $\frac{u_i}{v_i}$. Escrevendo

$$\sum_{i \neq j}^{m} f_i(x)x_i = -f_j(x)x_j, \tag{1.2}$$

onde j é o maior índice tal que $f_i(0) \neq 0$. Então para $i > j$ temos que $f_i(x) = xg_i(x)$ (com $g_i(x) \in K[x]$) e por hipótese para $i < j$ temos $x_i \in x_j P$. Portanto podemos reescrever a igualdade 1.2 como

$$-f_j(x)x_j = \sum_{i<j}^{m} f_i(x)x_i + \sum_{i>j}^{m} xg_i(x)x_i.$$

Então dividindo tudo por x_j obtemos que $f_j(x) \in P$, uma vez que $\frac{x_i}{x_j} \in P$. Por outro lado, dado a propriedade de ff_j temos que $f_j(x) = a_j + xu(x)$ onde $u(x) \in K[x]$ e $0 \neq a_j \in K$. Como $a_j = f_j(x) - xu(x) \in P$ temos uma contradição. □

Munidos deste lema podemos computar algumas propriedades satisfeitas por places.

Teorema 1.2.2. *Seja $\mathcal{O}$ um anel de valorização de F/K e P seu ideal maximal. Então*

a) $P = t\mathcal{O}$ (P é um ideal principal). Se P é gerado por t então para cada $0 \neq w \in F$ existem $m \in \mathbb{Z}$ e $u \in \mathcal{O}^*$ tais que $w = t^m u$.

b) Seja I um ideal de $\mathcal{O}$ com $\{0\} \neq I \subset \mathcal{O}$. Se $P = t\mathcal{O}$, então $I = t^n\mathcal{O}$, para algum $n \in \mathbb{N}$.

Demonstração. a) Supomos por contradição que P não é principal. Então existe $x \in P$ tal que $x\mathcal{O} \subsetneq P$, i.e, existe $x_1 \in P$ com $x_1 \notin x\mathcal{O}$. Pela proposição anterior temos que $x_1^{-1}x \in P$, ou seja, $x \in x_1 P$. Seguindo desta forma obtemos um conjunto infinito de elementos $x, x_1, \ldots$ tais que $x_j \in x_{j+1}P$ o que contradiz o lema anterior. Portanto, P é principal. Para provar a segunda parte, dividimos da seguinte forma:

Existência : Seja $w \in F$ e t tal que $P = t\mathcal{O}$. Se $w \in \mathcal{O}^\times$ então $w = t^0 w$. Caso contrário, pela definição de $\mathcal{O}$ temos que $w \in \mathcal{O}$ ou seu inverso. Sem perda de generalidade, podemos supor que $w \in \mathcal{O}$ e portanto $w \in P$. O lema anterior garante que existe m o maior natural tal que $w = t^m u$ com $u \in \mathcal{O}$.

Afirmação: $u \in \mathcal{O}^\times$. De fato, se não estivesse, teríamos que $u \in P$ e portanto $u = t^r v$ com $r \geqslant 1$ e $v \in \mathcal{O}$. Assim, $w = t^{m+r}v$ o que contradiz a maximalidade de m.

Unicidade: se $z = t^m u = t^n v$ com $u, v \in \mathcal{O}^\times$ e m, n são números inteiros. Então $t^{n-m} = uv^{-1}$, isto obriga que $n - m = 0$.

b) Seja I um ideal não nulo de $\mathcal{O}$. Segue o item anterior que o conjunto $\{n \in \mathbb{N} | t^n \in I\}$ é vazio. Considere $m := min\{n \in \mathbb{N} | t^n \in I\}$.

Afirmação: $I = t^m\mathcal{O}$. Com efeito, segue da definição de m basta apenas mostrar que $I \subseteq I^m\mathcal{O}$. Dado $z \in I$ temos que $z = t^r u$ com $r \geqslant 1$ e $u \in \mathcal{O}^\times$, logo $z = t^m(t^{r-m}u) \in I^m\mathcal{O}$ (note que $r \geqslant m$).

□

Observamos do segundo item do teorema anterior que $\mathcal{O}$ é um domínio de ideais principais. Um anel satisfazendo as propriedades do teorema anterior é chamado de *anel de valorização discreta*. Veremos nas próximas seções que estas propriedades se conectam com uma outra definição.

To elemento de t de um place P que é o gerador de P é chamado de *parâmetro local* de P (Em outras literaturas pode receber outras nomenclaturas: parâmetro uniformizador, elemento primo).

Podemos observar que o place de anel de valorização $\mathcal{O}$ do corpo de funções F/K o descreve unicamente. Em outras palavras, $\mathcal{O} = \{w \in F | z^{-1} \notin P\}$. Com este dado, podemos reescrever a definição como $\mathcal{O}_P := \mathcal{P}$ e chamá-lo de *anel de valorização do place P*.

Utilizando o Teorema 9 vamos construir uma importante aplicação. Considere um place P de F/K com parâmetro local t. Então pelo Item 1. do Teorema 1.2.2 para cada $0 \neq w \in F$ temos que existe $m \in \mathbb{Z}$ tal que $w = t^m u$ para algum $u \in \mathcal{O}^\times$. Desta forma podemos definir a aplicação $v_P : F \to \mathbb{Z} \cup \{\infty\}$ como

$$v_P(w) = \begin{cases} m, \ se \ w \neq 0 \\ \infty, \ se \ w = 0. \end{cases}$$

É possível verificar que está aplicação é bem definida, isto é, depende somente do place $P = t\mathcal{O}$. Agora vamos verificar algumas propriedades que esta aplicação possui:

Sejam $x = t^n u$ e $y = t^m v$ com $u, v \in \mathcal{O}^\times$.

1. Como $xy = t^{n+m}uv$ temos que $v_P(xy) = n + m$.

2. É claro que $v_P(t) = 1$.

3. Dado $a \in K$, temos $a \in \mathcal{O}^\times$. Escrevendo $a = t^0 a$ obtemos $v_P(a) = 0$.

4. $x+y = t^n u+t^m v.\, t^m(t^{n-m}u+v) = t^m w$, com $w = t^{n-m}u+v$. Se $w = 0$ obtemos que $v_P(x+y) = \infty$. No caso em que $w \neq 0$ temos $w = t^k u'$ com $k \geqslant 0$ e $u' \in \mathcal{O}^\times$. Portanto, $v_P(x+y) = m+k \geqslant v_P(x), v_P(y)$.

Generalizando a aplicação v_P, temos a seguinte definição.

Definição 1.2.4. *Seja F/K um copo de funções. Dizemos que uma aplicação $v : F \to \mathbb{Z} \cup \{\infty\}$ é uma* valorização discreta *sobre F/K se:*

1. *$v(wz) = v(w) + v(z)$, para todos $w, z \in F$;*
2. *$v(z+w) \geqslant min\{v(z), v(w)\}$, para todos $w, z \in F$;*
3. *$v(z) = \infty$ se, e somente se, $z = 0$;*
4. *Existe $z \in F$ tal que $v(z) = 1$;*
5. *Para cada $0 \neq u \in K$ temos que $v(u) = 0$.*

Observamos que a aplicação v_P é uma valorização discreta.

Proposição 1.2.3 (Desigualdade Triangular)**.** *Seja v uma valorização discreta de F/K. Dados $0 \neq x, y \in F$ com $v(x) \neq v(y)$ então $v(x+y) = min\{v(x),\ v(y)\}$.*

Demonstração. Como $v(x) \neq v(y)$ podemos supor que $v(x) < v(y)$. Se tivermos $v(x+y) \neq v(x)$, então pelas propriedades de valorização temos que $v(x+y) > v(x) = min\{v(x), v(y)\}$. Assim

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

o que é um absurdo (note que $v(y) = v(-y)$). □

Corolário 1.2.1 (Desigualdade Triangular Generalizada)**.** *Seja v uma valorização discreta de F/K. Dados $0 \neq x_1, x_2, \ldots, x_n \in F$ com $v(x_i) \neq v(x_j)$ para cada $i \neq j$, então $v\left(\sum_{i=1}^{n} x_i\right) = min\{v(x_1),\ v(x_2), \ldots, v(x_n)\}$.*

Lema 1.2.1. *Sejam F/K, v uma valorização discreta sobre F e $a_1,\ a_2, \ldots, a_n \in F$. Se $\sum_{i=1}^{n} a_i = 0$, então existe $i \neq j$ tal que $v(a_i) = v(a_j)$.*

Demonstração. Se $\sum_{i=1}^{n} a_i = 0$, então aplicando v temos

$$v\left(\sum_{i=1}^{n} a_i\right) = v(0) = \infty.$$

Se $min_{1\leqslant i\leqslant n}\{v(a_i)\} = \infty$, então $a_i = 0$, para cada i, isto é, $v(a_i) = \infty$.
Se $min_{1\leqslant i\leqslant n}\{v(a_i)\} < \infty$, então $v\left(\sum_{i=1}^{n} a_i\right) \neq min_{1\leqslant i\leqslant n}\{v(a_i)\}$, então $v(a_i) = v(a_j)$ para $i \neq j$. □

Exemplo 1.2.4. *Seja K um corpo qualquer e considere $F = K(x, y)$ com $y = x^3+1$. Seja Q um place tal que $v_Q(x) < 0$. Vamos calcular o sinal da valorização de y em relação à Q. Utilizando a equação $y = x^3 + 1$ temos*

$$v_Q(y) = v_Q(x^3 + 1) = min\left\{3v_Q(x), 0\right\} = 3v_Q(x) < 0.$$

Analogamente, se P é um place com $v_P(x) < 0$ então $v_P(y) < 0$.

Utilizando a valorização discreta em um place P de F/K podemos representar o anel de valorização de uma nova forma.

Teorema 1.2.3. *Sejam F/K um corpo de funções e $P \in \mathbb{P}_F$ um place. Sobre a valorização v_P podemos afirmar que:*

a) Dado uma place $P \in \mathbb{P}_F$, temos que

$$\begin{aligned} \mathcal{O}_P &= \{z \in F |\ v_P(z) \geqslant 0\} \\ \mathcal{O}_P^{\times} &= \{z \in F |\ v_P(z) = 0\} \\ P &= \{z \in F |\ v_P(z) > 0\} \end{aligned}$$

b) Dada uma valorização discreta v sobre F/K os conjuntos

$$A_v := \{z \in F |\ v_P(z) \geqslant 0\} \quad e \quad I_v := \{z \in F |\ v_P(z) > 0\}$$

são respectivamente anel de valorização e um place.

c) $t \in F$ é um parâmetro local de $P \Leftrightarrow v_P(t) = 1$.

Demonstração. a) Segue diretamente de observações anteriores.

b) Dados $z, w \in A_v$ segue das propriedades 1. e 2. da definição 1.2.4 que A_v é um subanel de F, pois $v(wz) = v(z) + v(w) \geqslant 0$ e $v(w+z) \geqslant \{v(w), v(z)\} \geqslant 0$. Para $x, y \in I_v$ e $z \in A_v$ temos novamente das propriedades 1. e 2. da definição 1.2.4 que $v(xz) = v(x) + v(z) > 0$ e $v(x+y) \geqslant \{v(x), v(y)\} > 0$. O item c) é imediato da definição de v_p. □

Definição 1.2.5. *Seja $z \in F$ e P um place de F/K.*

1. *Dizemos que P é* zero *de z se $v_P(z) > 0$;*
2. *Dizemos que P é* polo *de z se $v_P(z) < 0$.*

Exemplo 1.2.5. *Seja $F = K(x)$. Considere o elemento $z := \frac{x^2-2x-1}{x^2+x-6} \in F$. temos que 1 é zero de z e $2, -3$ são polos de z. Seja P_1 o place associado à 1 e P_2, P_3 os places associados à $2, -3$ respectivamente. Logo, $v_{P_1}(z) > 0$, $v_{P_2}(z) < 0$ e $v_{P_3}(z) < 0$. Note que P_1 tem multiplicidade dois, isto é, seu divisor é* $\mathrm{div}(z) = 2P_1 - P_2 - P_3$.

A noção de multiplicidade de pontos é muito importante quando estamos tratando de curvas algébricas.

Uma noção importante sobre um place é o seu grau. Para estarmos habilitados a fazer essa definição observamos o seguinte: dado uma anel de valorização $\mathcal{O}_P$ de F/K com ideal maximal, podemos obter o quociente $\frac{\mathcal{O}_P}{P}$ cujos elementos são classes residuais modulo P (é fácil verificar que este quociente é na verdade um corpo). Um fato interessante deste quociente é que podemos identificar tanto K quanto $\mathcal{K}$ como subcorpos de $\frac{\mathcal{O}_P}{P}$. De fato, como $K \subset \mathcal{O}_P$ e $K \subset \mathcal{K}$ temos que $K \cap P = \{0\}$. Portanto, a aplicação canônica $\mathcal{O}_P \to \frac{\mathcal{O}_P}{P}$ induz uma imersão de K em $\frac{\mathcal{O}_P}{P}$. $\mathcal{K}$ segue de forma análoga.

Definição 1.2.6. *Seja P um place de F/K.*

1. *$F_P := \frac{\mathcal{O}_P}{P}$ é chamado de* corpo das classes residuais *de P.*
2. *O* grau *do place P é definido como o grau da extensão de F_P/K, isto é, $deg(P) = [F_P : K]$*

Os places de grau um descrevem um papel importante na teoria e portanto também são chamados de *places racionais* de F/K.

Teorema 1.2.4. *Sejam P um place de F/K e $0 \neq z \in P$ com $[F : k(z)] = m$. Então $Deg(P) \leqslant m$.*

Demonstração. Vamos mostrar que qualquer conjunto com m elementos de F_P é linearmente independente sobre K. Para isso, consideramos $f_1^P, \ldots, f_m^P \in F_P$ linearmente independentes sobre K (onde f_i^P denotam classes residuais de elementos $f_i \in \mathcal{O}_P$). Vamos mostrar que o conjunto $f_1, \ldots, f_n \in \mathcal{O}_P$ é linearmente independente sobre $K(z)$. De fato, se existe uma combinação não trivial sobre $K(z)$, então

$$\sum_{i=1}^{m} f_i a_i(z) = 0 \tag{1.3}$$

com $a_i(z) \in K(z)$. Sem perda de generalidade podemos assumir que $a_i(z) \in K[z]$ e que existem polinômios da forma $a_i(z) = b_i + z g_i(z)$ com $b_i \neq 0$. Agora, passando a relação de congruência modulo P teremos que f_i^P não são linearmente independentes, o que contradiz a hipótese.

□

Consideremos um place P de grau um de F/K. Então temos que $F_P = K$. Se adicionarmos a hipótese de K ser algebricamente fechado, então toda extensão finita de K terá grau um e consequentemente todos os places serão racionais. Por exemplo, se $K = \mathbb{C}$, existem infinitos places de grau um e, portanto existem places. Mas podemos questionar se dado um corpo de funções genérico, ele sempre terá algum place? A resposta a esta questão segue do próximo resultado.

Teorema 1.2.5. *Seja F/K um corpo de funções e A um anel tal que $K \subset A \subset F$. Suponha ainda que A contenha um ideal próprio $I \neq \{0\}$. Então existe um place P de F tal que $I \subset P$ e $\mathcal{O}_P \subset A$.*

Demonstração. Definimos o seguinte conjunto

$$\mathcal{A} := \{U \subset F \mid U \text{ é um anel com } A \subset U \text{ e } UI \neq U\}$$

Vemos que $A \in \mathbb{A}$ e, portanto $\mathcal{A} \neq \emptyset$. Ainda para cada $\mathcal{U} \subset \mathcal{A}$ totalmente ordenado temos que o conjunto $V := \bigcup_{U \in \mathcal{U}} U$ é um subanel satisfazendo $A \subset V$. Notamos que $V \in \mathcal{A}$, para vamos mostrar que $V \neq IV$. Caso tivéssemos $V = IV$ então $\sum_{i=1}^{r} a_i v_i$ com $a_i \in I$ e $v_i \in V$ então $v_1, \ldots, v_r \in T$ para algum $T \in \mathcal{U}$

(este fato decorre da propriedade de $\mathcal{U}$ ser totalmente ordenado). Então $1 \in TI$, o que contradiz a definição de $\mathcal{A}$. Como todo conjunto totalmente ordenado de $\mathcal{A}$ possui um limitante superior teremos aplicando o Lema de Zorn a existência de elemento maximal $\mathcal{O}$ em $\mathcal{A}$.

Vamos provar que $\mathcal{O}$ é um anel de valorização, isto é, para cada $w \in F$ temos $w \in \mathcal{O}$ ou $w^{-1} \in \mathcal{O}$. Com efeito, suponha que exista um elemento em F que não satisfaça esta propriedade, ou seja, existe $z \in F$ tal que $z, z^{-1} \notin \mathcal{O}$. Pelo fato de $\mathcal{O}$ ser maximal temos que $\mathcal{O}[z] = I\mathcal{O}[z]$ e $\mathcal{O}[z^{-1}] = I\mathcal{O}[z^{-1}]$. Desta maneira podemos escrever $1 = \sum_{i=0}^{s} a_i z^i$ e $1 = \sum_{j=0}^{r} b_j z^{-j}$ com $m, n \geqslant 1$ os menores com essa propriedade, $a_i, b_j \in I\mathcal{O}$. Sem perda de generalidade podemos supor que $s \leqslant r$, então multiplicando a primeira equação por $(1 - b_0)$, a segunda por $a_s z^s$ e somando as mesmas obtemos a seguinte igualdade

$$1 = \sum_{i=0}^{s-1} c_i z^i$$

com $c_i \in I\mathcal{O}$ e isto contradiz a minimalidade de s. Portanto, $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$. □

Observação 1.2.1. *Os elementos do conjunto acima são da forma* $\sum a_i u_i$*, isto é,* $IU := \left\{ \sum a_i u_i | a_i \in I,\ u_i \in U \right\}$

Corolário 1.2.2. *Seja F/K um corpo de funções. Todo elemento transcendental de F possui pelo menos um zero e um polo.*

Demonstração. Segue do Teorema 1.2.5 □

Já sabemos que o conjunto de places de um corpo de funções nunca é vazio. Em seguida queremos responder a seguinte pergunta: dado um corpo de funções F/K seu conjunto de places é finito? Para responder essa pergunta vamos ao seguinte resultado.

Teorema 1.2.6. *Sejam $P_1, \ldots, P_n$ places em F/K distintos dois à dois, $x_1, \ldots, x_n \in F$ e $s_1, \ldots, s_n \in \mathbb{N}$. Então existe $w \in F$ satisfazendo*

$$v_{P_i}(w - x_i) = s_i$$

para cada $i = 1, \ldots, n$.

Demonstração. Consultar (Stichtenoth 1993). □

O teorema anterior é conhecido como *Teorema da aproximação fraca*. Munidos deste resultado somos capazes de provar o seguinte corolário.

Exemplo 1.2.6. *Seja F/K um corpo de função. Sejam $P_1, \ldots, P_n$ n places distintos de F. Considere $a_1, a_2, \ldots, a_n \in F$ são elementos arbitrários e sejam $m_1, m_2, \ldots, m_n$ ser números naturais arbitrários. Então o sistema de congruências $x \equiv a_i \, mod P_i$ tem uma solução em F.*

Corolário 1.2.3. *Todo corpo de funções possui infinitos places.*

Demonstração. Suponha que exista somente um número finito de places, digamos $P_1, \ldots, P_n$. Então pelo teorema anterior podemos encontrar um elemento $x \in F$ transcendente sobre K tal que $v_{P_i}(x) > 0$. Este fato indica que x não possui polos o que contradiz o resultado 1.2.2. □

Teorema 1.2.7. *Seja F/K um corpo de funções.*

(a) Seja $z \in F$, $P_1, \ldots, P_m \in F/K$ zeros de z. Então

$$\sum_{i=1}^{m} v_{P_i}(z) P_i \leqslant [F : K(z)].$$

(b) Cada $0 \neq z \in F$ possui um número finito de polos e zeros.

Demonstração. a) Para simplificar a notação vamos denotar por $v_{P_i} = v_i$ e $Deg(P_i) = d_i$. Como cada P_i é principal existe t_i tal que

$$v_k(t_i) = \begin{cases} 1, \ se \ k = i \\ 0, \ se \ k \neq i. \end{cases}$$

Escolhamos $s_{i_1}, \ldots, s_{i_{f_i}} \in \mathcal{O}_{P_i}$ tais que as classes residuais $s_{i_1}^{P_i}, \ldots, s_{i_{f_i}}^{P_i}$ formam uma base para F_{P_i} sobre K. Por uma aplicação mais simples do Teorema 1.2.6, podemos encontrar $z_{ij} \in F$ tais que para cada i, j

$$vi(s_{ij} - z_{ij}) > 0 \, e \, v_k(z_{ij}) > v_k(z)$$

para $k \neq i$.

Vamos mostrar que os elementos $t_i^a z_{ij}$ são linearmente independentes sobre $K(x)$. Como o número de elementos dessa forma é igual à

$$\sum_{i=1}^{r} f_i v_i(z) = \sum_{i=1}^{r} v_{Pi}(x) Deg(P_i),$$

temos que a prova dessa proposição seguirá dessa afirmação. Suponhamos que exista um combinação linear não trivial sobre $K(x)$

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{v_i(x)} u_{ija}(x) t_i^a z_{ij} = 0. \tag{1.4}$$

Sem perda de generalidade, podemos assumir $u_{ija} \in K[x]$ e que nem todos u_{ija} são divisíveis por x.

Então existem índices $k \in \{1, \ldots, r\}$ e $c \in \{0, \ldots, e_k - 1\}$ tais que $x | u_{kja}(x)$, para todo $a < c$ e para todo $j \in \{1, \ldots, f_k\}$, e $x - u_{kjc}(x)$, para algum $j \in \{1, \ldots, f_k\}$.

Multiplicando 1.4 por $t_k - c$, obtemos

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{v_i(x)} u_{ija}(x) t_i^a t_k^{-c} z_{ij} = 0.$$

Para $i \neq k$, todas as parcelas da soma anterior estão em P_k, já que

$$v_k(\phi_{ija}(x) t_i^a t_k^{-c} z_{ij}) =$$
$$v_k(\phi_{ija}(x)) + v_k(t_i^a) + v_k(t_k^{-c}) + v_k(z_{ij}) > -c + v_k(x) > 0.$$

Para $i = k$ e $a < c$, temos que

$v_k(\phi_{ija}(x) t_k^{a-c} z_{kj}) = v_k(\phi_{kja}(x)) + v_k(t_k^{a-c}) + v_k(z_{kj}) > -c + v_k(x) > 0$. Para $i = k$ e $a > c$, temos que $v_k(\phi_{kja}(x) t_k^{a-c} z_{kj}) > v_k(x) + a - c > a - c > 0$. Combinando os casos anteriores, temos que

$$\sum_{j=1}^{f_k} \phi_{kjc}(x) z_{kj} \in P_k.$$

Notemos que $\phi_{kjc}(x)(P_k) \in K$, uma vez que tudo que for múltiplo de x pertence à P_k, de modo que no quociente F_{P_k} só resta o termo constante, e que nem todos $\phi_{kjc}(x)(P_k) = 0$, pois x não divide todos os $\phi_{kjc}(x)$, donde temos uma combinação linear não trivial

sobre K. Mas isso é uma contradição, pois $\left\{z_{k_1}(P_k), \ldots, z_{k_{f_k}}(P_k)\right\}$ é uma base de F_{P_k}/K (pois $v_i(s_{ij} - z_{ij}) > 0$ implica que $s_{ij} - z_{ij} \in P_i$ e assim $s_{ij}(P_i) = z_{ij}(P_i)$, com $\{s_{i1}(Pi), \ldots, s_{if_i}(P_i)\}$ sendo uma base de F_{P_i}/K).

b) Se $x \in K$ a afirmação é imediata. Suponha $z \in F$ com $z \notin K$, isto é, z não é constante. Então pelo item a) temos que z possui um número finito de zeros. Para mostrar que z possui finitos polos vemos que z^{-1} possui um número finito de zeros e isto fato segue novamente do item a).

□

Corolário 1.2.4. *Seja F/K um corpo de funções. Então $[\mathcal{K} : K] < \infty$.*

Demonstração. Como $\mathbb{P}_F \neq \emptyset$ (item b) do Teorema 1.2.7), podemos tomar $P \in \mathbb{P}_F$. Lembrando que podemos identificar $\mathcal{K}$ em F_P via o mapa canônico, por consequência deste fato obtemos $[\mathcal{K} : K] \leqslant [F_P : K]$ que é finito pelo Teorema 1.2.5. □

Vamos agora aprofundar nossos estudos sobre corpo de funções racionais. Seja $F = K(x)$ com x transcendente sobre K. Seja $f(x) \in K[x]$ um polinômio mônico e irredutível sobre K. Considere os seguintes conjuntos:

$$\mathcal{O}_f := \left\{\frac{u(x)}{v(x)} |\ u(x), v(x) \in K[x]\ e\ f(x) \nmid v(x)\right\} \tag{1.5}$$

e

$$P_f := \left\{\frac{u(x)}{v(x)} |\ u(x), v(x) \in K[x],\ f(x)|u(x)\ e\ f(x) \nmid v(x)\right\} \tag{1.6}$$

Exercício 1.2.3. *Mostre que os conjuntos $\mathcal{O}_f$ e P_f são anel de valorização e place de $K(x)$ respectivamente.*

Em particular, quando $f(x) = x - a$ com $a \in K$ escrevemos simplesmente $\mathcal{O}_a := \mathcal{O}_f$ e $P_a := P_f$. Com está notação fica claro que cada elemento de K corresponde a um place em $K(x)$. Outro anel de valorização em $K(x)$ é

$$\mathcal{O}_\infty = \left\{ \frac{u(x)}{v(x)} | \; u(x), v(x) \in K[x] \; e \; deg(u) \leqslant deg(v) \right\}$$

Cujo ideal maximal é

$$P_\infty = \left\{ \frac{u(x)}{v(x)} | \; u(x), v(x) \in K[x], \; deg(u) < deg(v) \right\} \tag{1.7}$$

Chamamos a atenção do leitor para o fato de que essa escrita depende do elemento gerador de $K(x)$. O place P_∞ é chamado de *place infinito* de $K(x)$.

Exercício 1.2.4. *Mostre que K é o corpo de de constantes de $K(x)$.*

Proposição 1.2.4. *Sobre o corpo de funções racionais $K(x)$ podemos afirmar que:*

a) Seja $P = P_f$ o place definido em 1.6. Temos que $f(x)$ é parâmetro local de P.

b) O corpo residual $K(x)_P$ é isomorfo à $\frac{K[x]}{<f(x)>}$, isto é, a aplicação $\phi : \frac{K[x]}{<f(x)>} \to K(x)_P$

$$\phi(u(x) \; mod \; f(x)) = u(x) + P$$

Consequentemente, $deg(P) = deg(f)$.

c) Seja $P = P_\infty$ definido em 1.7. Então um parâmetro local para P_∞ é $\frac{1}{x}$ e, consequentemente $Deg(P_\infty) = 1$.

Demonstração. a) Seja $P = P_{p(x)} = \left\{ \frac{f(x)}{g(x)} | f, g \in K[x], \; p | f \; e \; p \nmid g \right\}$, onde $p = p(x) \in K[x]$ é um polinômio irredutível. Logo o ideal $< p(x) > \subset P = < t(x) >$ como $p(x)$ é irredutível e mônico conclui-se $p(x) = t(x)$.

b) Agora defina $\phi : K[x] \to \frac{O_P}{P}$ dado por $\phi(f) = f(x)(P)$. Como p é irredutível temos que $\text{Ker}(\phi) = < P >$ e ϕ é sobrejetiva uma vez que dado $z \in O_P$, $z = \frac{u(x)}{v(x)}$ com $u(x), v(x) \in K[x]$ coprimos e $p(x) \nmid v(x)$. Logo existem $a, b \in K[x]$ tais que $a(x)p(x) + b(x)v(x) = 1$, então $z = \frac{a(x)u(x)}{v(x)} + b(x)v(x)$. Daí $z + P = (b(x)u(x)) + P \in \text{Im}\,\phi$. Portanto, $\frac{K[x]}{<p>} \simeq \frac{O_P}{P}$. e $deg(P) = deg(p(x))$. A ultima afirmação segue de

$$deg(p(x)) = [\frac{K[x]}{< p(x) >} : K] = [K(x)_P : K] = Deg(P).$$

c) A inclusão $\frac{1}{x}\mathcal{O}_\infty \subset P_\infty$ é clara. Dado $u \in P_\infty$ temos que $u = \frac{p(x)}{q(x)}$ com $deg(p(x) < deg(q(x)$ então $u = \frac{1}{x}\frac{xp(x)}{q(x)} \in \mathcal{O}_\infty$. Portanto, $\mathcal{O}_\infty = P_\infty$, ou seja, $\frac{1}{x}$ é parâmetro local de P_∞. Agora, observando que $\frac{K(x)}{P_\infty} \simeq \frac{K[\frac{1}{x}]}{<\frac{1}{x}>}$ temos que $Deg(P_\infty) = 1$.

□

Observamos pelo segundo item do teorema anterior que cada place de grau está em correspondência com polinômios lineares, e portanto com cada elemento de K. Desta forma, se K é um corpo finito então $K(x)$ terá um número finito de places de grau um.

Observação 1.2.2. *Seja K um corpo. A proposição anterior nos permite concluir que:*

a) $\mathbb{P}_{K(X)}$ *está em bijeção com* $\{$ *polinômio irredutível de* $K[X]\} \cup \{1/X\}$.

Este fato decorre imediatamente da proposição.

b) $\#\left\{P \in \mathbb{P}_{K(X)} |\ deg(P) = 1\right\} = 1 + \#K$.

De fato, Segue do item a) desta observação que dado $P \in \mathbb{P}_{K(x)}$ *existe* $p(x) \in K[x]$ *mônico e irredutível tal que* $P = P_{p(x)}$. *Se* $1 = deg(P)$, *então pelo item b) do teorema anterior temos que* $1 = deg(P) = deg(p(x))$. *Assim,* $p(x) = x - a$ *para algum* $a \in K$. *Desta forma concluímos que* $\#\left\{P \in \mathbb{P}_{K(X)} |\ deg(P) = 1\right\} = 1 + \#K$. *Observamos ainda que se K é um corpo finito, então existirá um número finito de places de grau um em* $K(x)$.

c) Por exemplo, suponha $K = \mathbb{R}$. *Sabemos que os únicos polinômios irredutíveis são os de grau um e os de grau dois* $ax^2 + bx + c$ *tais que* $b^2 - 4ac < 0$.*Logo, os places em* $\mathbb{R}(x)$ *são dados por polinômios irredutíveis descritos acima. Pelo item c) que* $\#\left\{P \in \mathbb{P}_{K(X)} |\ deg(P) = 1\right\} = 1 + \#K = \infty$.

Segue do item b) do teorema anterior que em $\mathbb{R}(x)$ *só existem places de grau um ou dois.*

Teorema 1.2.8. *Os únicos places de* $K(x)$ *são da forma* P_f *ou* P_∞.

Demonstração. Dado $P \in \mathbb{P}_{K(X)}$ qualquer. Se $P = P_\infty$ não há o que fazer. Então suponha que $P \neq P_\infty$. Temos dois casos para o elemento x. Note que se $x \notin O_P$, então $P = P_\infty$, absurdo. Então $x \in O_P$. Assim $K[x] \subset O_P$ e

definindo $I := K[x] \cap P$, temos que I é um ideal primo de $K[x]$. O mapa de classe de resíduos induz uma inclusão de $\frac{K[x]}{I}$ em $\frac{O_P}{P}$ então pela Teorema 1.2.4 temos que $I \neq 0$ e portanto existe um (unicamente determinado) polinômio mônico irredutível $p(x) \in K[x]$ tal que $I = p(x)K[x]$. Note que todo polinômio $g(x)$ tal que $p(x) \nmid g(x)$ não pode estar em I, ie, $g(x) \notin P$ e $\frac{1}{g(x)} \in O_P$. Assim, $O_{p(x)} \subset O_P$ e pelo Teorema 1.2.3 temos que $O_P = O_{p(x)}$, ou seja, $P = P_{p(x)}$. □

1.3 Divisores

A partir desta seção assumiremos que $\mathcal{K} = K$.

Seja F/K denotará um corpo de funções de uma variável com $\mathcal{K} = K$.

Definição 1.3.1. *O* grupo de divisores *de F/K é definido como o grupo abeliano livre gerado pelos places F/K e é denotado por $Div(F)$. Os elementos deste grupo são chamados de* divisores *de F.*

Mais especificamente, os divisores são somas formais

$$D = \sum_{i=1}^{n} n_{P_i} P_i$$

onde $n_{P_i} \in \mathbb{Z}$ e $P_i \in \mathbb{P}_F$.

Os números n_{P_i} são chamados de *coeficientes do divisor D*. Para aqueles $n_i's$ que não são nulos definimos o suporte do divisor D como

$$\text{Supp}(D) = \{P \in \mathbb{P}_F \mid n_P \neq 0\}$$

Um divisor da forma $D = P$ com $P \in \mathbb{P}_F$ é dito *divisor primo*.

Ressaltamos algumas propriedades do grupo $Div(F)$. Dados dois divisores $D = \sum_{P \in \mathbb{P}_F} n_P P$ e $D' = \sum_{P \in \mathbb{P}_F} m_P P$ temos que

1. A soma de D e D' é da forma:

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + m_P) P$$

2. O divisor D é nulo se cada $n_P = 0$

Ainda podemos estabelecer uma ordenação parcial no grupo $Div(F)$. Dados dois divisores $D = \sum_{P \in \mathbb{P}_F} n_P P$ e $D' = \sum_{P \in \mathbb{P}_F} m_P P$ dizemos que

$$D \leqslant D' \Leftrightarrow n_P \leqslant m_P \text{ para todo } P \in \mathbb{P}_F.$$
$$\text{Se ainda tivermos que } D \neq D' \text{ escrevemos que } D < D'.$$

Quando cada $n_P \geqslant 0$ dizemos que D é um *divisor efetivo*. Dado um divisor $D = \sum_{P \in \mathbb{P}_F} n_P P$ podemos definir a aplicação $v_P(D) = n_P$ para cada $P \in \mathbb{P}_F$. Em termos desta aplicação podemos reescrever

$$\text{Supp}(D) = \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\} \text{ e } D = \sum_{P \in \text{Supp}(D)} v_P(D)P$$

Exercício 1.3.1. *Considere a curva dada pela equação $Z^3 + X^3 + Y^3 = 0$ definida sobre $\mathbb{F}_2$. Considere a função $z = \frac{x}{y+z}$ e a reta L com equação $X = 0$. Calcule os places em comum entre z e L.*

Definição 1.3.2. *O* grau *de um divisor $D = \sum_{P \in \mathbb{P}_F} n_P P$ é definido como*

$$Deg(D) = \sum_{P \in \mathbb{P}_F} v_P(D) Deg(P)$$

Vemos que a aplicação $Deg : Div(F) \to \mathbb{Z}$ dada por $Deg(D)$ é um homomorfismo.

Exemplo 1.3.1. *Seja F/K um corpo de funções. Dados $Q, P \in \mathbb{P}_F$ dois places com grau um e dois respectivamente. Podemos definir os seguintes divisores: $D_1 = 5P$, $D_2 = 23Q$ e $D_3 = 7P + Q$. Para exemplificar as definições acima temos:*

a) $D_1 + D_2 = 5P + 23Q$;

b) $D_1 + D_3 = 12P + Q$;

c) D_1 *não é comparável com* D_2, $D_3 \geqslant D_1$;

d) $v_P(D_3) = 7$, $v_Q(D_3) = 1$, *e* $v_{P'}(D_3) = 0$ *para todo place* $P' \neq P, Q$.

e) $Deg(D_1) = 5$, $Deg(D_2) = 46$ *e* $Deg(D_3) = 9$.

Como sabemos, cada $0 \neq z \in F$ possui um número finito de polos e zeros. Então vamos denotar por $Z := \{P \in \mathbb{P}_F | v_P(z) > 0\}$ e $N := \{P \in \mathbb{P}_F | v_P(z) < 0\}$ o conjuntos de zeros e polos de z respectivamente, logo tanto Z quanto N são conjuntos finitos. Isto dá sentido a próxima definição.

Definição 1.3.3. *Seja* $0 \neq z \in F$. *Definimos então*

1. $\mathrm{div}(z)_0 := \sum_{P \in Z} v_P(z)P$, *o* divisor de zeros *de* z. *O número* $v_P(z)$ *é chamado* ordem do zero P;
2. $\mathrm{div}(z)_\infty := \sum_{P \in N} -v_P(z)P$, *o* divisor de polos *de* z. *O número* $v_P(z)$ *é chamado* ordem do polo P;
3. $\mathrm{div}(z) := \mathrm{div}(z)_0 - \mathrm{div}(z)_\infty$, *o* divisor principal *de* z.

Observamos que os divisores de zeros e polos são ambos divisores efetivos e que o divisor principal pode ser escrito da forma

$$\mathrm{div}(z) = \sum_{P \in \mathbb{P}_F} v_P(z)P. \tag{1.8}$$

Definição 1.3.4. *O conjunto dos divisores*

$$Princ(F) := \{\mathrm{div}(z) |\ 0 \neq z \in G\}$$

é um subgrupo de $Div(F)$ *e é chamado de* grupo dos divisores principais *de* F.

Dizemos que dois divisores $D,\ D' \in Div(F)$ são *equivalentes* e escrevemos $D \sim D'$ se existe $0 \neq z \in F$ tal que $D = D' + \mathrm{div}(z)$.

Exercício 1.3.2. *Mostre que* $Princ(F)$ *é um subgrupo de* $Div(F)$.

Definição 1.3.5. *Dado* $D \in Div(F)$, *definimos o* espaço de Riemann–Roch *associado à* D *como*

$$\mathcal{L}(D) := \{z \in F |\ \mathrm{div}(z) \geqslant -D\} \cup \{0\}$$

Escrevendo o divisor $D = \sum_{i=1}^{n} a_i P_i - \sum_{j=1}^{m} b_j Q_j$ com $a_i, b_j > 0$, podemos destacar algumas propriedades imediatas: para cada $z \in \mathcal{L}(D)$

- z possui zeros de ordem maior ou igual à b_j em Q_j;
- z possui polos somente em cada P_i, com ordem menor ou igual à a_i.

Exercício 1.3.3. *Seja $D \in Div(F)$. Mostre que:*

(a) $z \in \mathcal{L}(D) \Leftrightarrow v_P(z) \geqslant -v_P(D)$ *para cada* $P \in \mathbb{P}_F$.

(b) $\mathcal{L}(D) \neq \{0\} \Leftrightarrow$ *existe* $A \in Div(D)$ *tal que* $A \geqslant 0$ *e* $A \sim D$.

Seja $D \in Div(F)$. Um fato interessante sobre $\mathcal{L}(D)$ ele é um espaço vetorial sobre K. Com efeito, tomando $w, z \in \mathcal{L}(D)$ e $\lambda \in K$ temos pela propriedades de valorização que para cada $P \in \mathbb{P}_F$

$$v_P(w+z) \geqslant min\{v_P(w), v_P(z)\} \geqslant -v_P(D)$$
$$v_P(\lambda w) = v_P(w) \geqslant -v_P(D).$$

Com isso, devemos verificar que este espaço vetorial tem ou não dimensão finita sobre K. Mas antes de verificarmos este fato, veremos a relação entre esses espaços quando estes estão associados à divisores equivalentes. Sejam dois divisores equivalentes D e D', isto é, $D = D' + (z)$, então $\mathcal{L}(D) \simeq \mathcal{L}(D')$. Para verificar este fato, basta observar que as aplicações

$$\begin{aligned} \psi : \mathcal{L}(D) &\longrightarrow \mathcal{L}(D) \\ x &\longmapsto xz \end{aligned}$$

e

$$\begin{aligned} \phi : \mathcal{L}(D) &\longrightarrow \mathcal{L}(D) \\ x &\longmapsto xz^{-1} \end{aligned}$$

são mapas K-lineares um o inverso do outro.

Proposição 1.3.1. *Sejam $D, D' \in Div(F)$.*

a) $\mathcal{L}(0) = K$.

b) $\mathcal{L}(D) = \{0\}$ *quando* $D < 0$.

c) Se $D \leqslant D'$, *então* $\mathcal{L}(D) \subset \mathcal{L}(D')$ *e* $dim_K(\frac{\mathcal{L}(D')}{\mathcal{L}(D)}) \leqslant Deg(D' - D)$.

d) $\mathcal{L}(D)$ *tem dimensão finita. Se ainda tivermos* $Deg(D) \geqslant 0$ *então*

$$dim_K(\mathcal{L}(D)) \leqslant Deg(D) + 1.$$

e) Se $D \sim D'$ *então* $dim_K(\mathcal{L}(D)) = dim_K(\mathcal{L}(D'))$

Demonstração. a) A inclusão $K \subset \mathcal{L}(0)$ é imediata. Agora, dado $0 \neq z \in \mathcal{L}(0)$ temos pelo Exercício 1.3.3 que $v_P(z) \geqslant 0$ para cada $P \in \text{Supp}(P)$, isto implica que z não tem polos, isto é, $z \in K$. Portanto, $K = \mathcal{L}(0)$.

b) Seja D um divisor com $D < 0$. suponha que existe $0 \neq z \in \mathcal{L}(D)$ novamente pelo Exercício 1.3.3 temos $v_P(z) \geqslant -D > 0$ isto implica que z não tem polos, mas possui pelo menos um zero. Absurdo!

c) Sejam D e D' dois divisores tais que $D \leqslant D'$. Primeiro vamos mostrar que $\mathcal{L}(D) \subset \mathcal{L}(D')$. Com efeito, seja $z \in \mathcal{L}(D)$ então $(z) \geqslant -D$, como $D \leqslant D'$ temos que $\text{div}(z) \geqslant -D \geqslant -D'$. Portanto, $z \in \mathcal{L}(D')$. Para verificar a segunda afirmação observamos que $D' = D + P_1 + \cdots + P_r$ onde $P_i \in \mathbb{P}_F$ e $r \geqslant 0$. Segue da primeira parte que

$$\mathcal{L}(D) \subset \mathcal{L}(D + P_1) \subset \cdots \subset \mathcal{L}(D + P_1 + \cdots + P_r).$$

Portanto, basta mostrar que $dim_K\left(\frac{\mathcal{L}(D+P_1)}{\mathcal{L}(D)}\right) \leqslant 1$. Suponha que $D' = D+P$, onde P é um place. Como v_P é sobrejetora, então podemos escolher $u \in F$ tal que $v_P(u) = v_P(D') = v_P(D) + 1$.

Dado $z \in \mathcal{L}(D')$ temos que $v_P(z) \geqslant v_P(D') = -v_P(u)$, isto é, $v_P(xu) \geqslant 0$. Definindo a aplicação $f : \mathcal{L}(D') \to \frac{\mathcal{O}_P}{P}$ dada por $f(z) = xu + P$. É fácil ver que esta aplicação tem kernel igual à $\mathcal{L}(D)$ e portanto induz uma aplicação injetiva entre K-espaços vetoriais, ou seja,

$$dim_K\left(\frac{\mathcal{L}(D')}{\mathcal{L}(D)}\right) \leqslant dim_K(F_P) = Deg(P) = Deg(D') - Deg(D).$$

d) Seja D um divisor. Se $Deg(D) \leqslant 0$ já vimos que possui dimensão finita. Suponha que $Deg(D) = m > 0$ então pelo item anterior temos que $dim_K(\mathcal{L}(D)) = dim_K\left(\frac{\mathcal{L}(D)}{\mathcal{L}(0)}\right) + 1 \leqslant m + 1$.

e) Suponha que $D = D' + (z)$ para algum $z \in F$. Defina a aplicação $\phi : \mathcal{L}(D') \to \mathcal{L}(D)$ dada por $\phi(x) = xz$ é um homomorfismo de K-espaços vetoriais com inversa é dada por $\psi(y) = yz^{-1}$. Portanto, $dim_K(\mathcal{L}(D)) = dim_K(\mathcal{L}(D'))$.

□

Pelo item d) vemos que $\mathcal{L}(D)$ possui dimensão finita sobre K. Este fato é tão importante que gera trabalhos acadêmicos onde se busca exibir uma base para o espaço de Riemann–Roch $\mathcal{L}(D)$. Por outro lado, a utilização da base de um espaço de Riemann–Roch pode ajudar a caracterizar certos tipos de curvas. Este fato torna importante sermos capazes de calcular a dimensão de um dado divisor.

Definição 1.3.6. *Para cada $D \in Div(F)$ definimos a* dimensão do divisor D *como $\ell(D) := dim_K(\mathcal{L}(D))$.*

Nos próximos resultados iremos nos preparar para sermos capazes de efetuar o calculo da dimensão de um divisor D.

Teorema 1.3.1. *Seja $0 \neq z \in F$. Então*

$$Deg(z)_0 = Deg(z)_\infty = [F : K(z)]. \tag{1.9}$$

Demonstração. Escrevamos $m = [F : K(z)]$ e $D = \text{div}(z)_\infty = \sum_{i=1}^{s} -v_{P_i}(z)P_i$, onde $P_1, \ldots, P_s$ são todos os polos de z. Então

$$Deg(D) = \sum_{i=1}^{s} v_{P_i}(x^{-1})Deg(P_i) \leqslant [F : K(z)].$$

Basta mostrarmos que a desigualdade contrária também é satisfeita. Escolhamos uma base $f_1, \ldots, f_m$ de $F/K(z)$ e um divisor D' tal que $D' \geqslant 0$ e $(f_i) \geqslant -D'$, para $i = 1, \ldots, m$. Então temos que

$$\ell(kD + D') \geqslant m(k + 1), \ para\ todo\ k \geqslant 0. \tag{1.10}$$

Escrevendo $d' = deg(D')$, obtemos que

$$n(k + 1) \leqslant \ell(kD + D') \leqslant Deg((kD + D')+) + 1 = Deg(kD + D') + 1 = kDeg(D) + Deg(D') + 1 = kDeg(D) + d' + 1.$$

Logo $m(k+1) \leqslant k deg(D) + d' + 1 \Rightarrow k(deg(D) - n) \geqslant n - d' - 1$, para cada $k \in \mathbb{N}$.

Note que o lado direito da última desigualdade não depende de k, portanto $\deg(D) \geqslant n$. Desse modo, provamos que $Deg((z)_\infty) = [F : K(z)]$. Como $(z)_0 = (z^{-1})_\infty$, podemos concluir que $Deg((z)_0) = Deg((z^{-1})_\infty) = [F : K(z^{-1})] = [F : K(z)]$.

Vamos provar 1.10. Para isso, basta mostrarmos que os elementos $x^i f_j$, com $0 \leqslant i \leqslant k$ e $1 \leqslant j \leqslant n$, pertencem ao espaço $L(kD + D')$ e são linearmente independentes sobre K, pois isso nos dá que $l(kD + D') = \dim(L(kD + D')) > n(k+1)$.

De fato, $(z^i) = i(z) = i(z)_0 - i(z)_\infty \geqslant -i(z)_\infty \geqslant -k(z)_\infty = -kD$, pois $i \leqslant k$, e $(f_j) \geqslant -D'$, para todo $j = 1, \ldots, n$. Daí, $(z^i f_j) = (z^i) + (f_j) \geqslant -kD - D'$, ou seja, $z^i f_j \in L(kD + D')$.

Ainda, se $\sum_{j=1}^{m} \sum_{i=1}^{k} a_{ij} z^i f_j = 0$, com $a_{ij} \in K$, temos que $\sum_{j=1}^{m} \left(\sum_{i=1}^{k} a_{ij} z^i \right) f_j = 0$, donde $\sum_{i=1}^{k} a_{ij} z^i = 0$, para todo $j = 1, \ldots, m$. Como z é um elemento transcendente sobre K, temos que $a_{ij} = 0$, para todos $i = 1, \ldots, k$, $j = 1, \ldots, m$. Isso mostra que os elementos $z^i f_j$ são linearmente independentes sobre K.

□

Como $Deg(z)_0 = Deg(z)_\infty$ temos que todo divisor principal tem grau nulo.

Corolário 1.3.1. *Sejam $D, D' \in Div(F)$ e $z \in F$.*

a) Se $D \sim 0 \Leftrightarrow D = (z)$ para algum $z \in F$.

a) Se $D = D' + (z)$, então $Deg(D) = Deg(D')$.

b) Se $Deg(D) = 0$, então D é principal $\Leftrightarrow \ell(D) = 1$.

Demonstração. Segue diretamente da proposição anterior. □

Exercício 1.3.4. *Se $\mathcal{X}$ é uma cúbica (afim) dada por $y^2 + x(x-1)(x-a)$, onde $a \in K \setminus \{0, 1\}$ e $F = K(x, y)$. Considere $z = x^{-1}$. Mostre que $\mathcal{L}(s \operatorname{div}(z)_0) \subset K[x, y]$ e que se $s \geqslant 1$ então $\ell(s \operatorname{div}(z)_0) = 2s$.*

Proposição 1.3.2. *Existe uma constante $\lambda \in \mathbb{Z}$ tal que para cada divisor $D \in Div(F)$ vale a seguinte desigualdade:*

$$Deg(D) - l(D) \leqslant \lambda.$$

Demonstração. Veja em (Childress 2009; Stichtenoth 1993). □

Definição 1.3.7. *Definimos o* gênero *de F/K como*

$$g(F) := max\{Deg(D) + 1 - l(D) |\ D \in Div(F)\} \tag{1.11}$$

Corolário 1.3.2. $g(F) \in \mathbb{N}$.

Demonstração. Exercício. □

Exemplo 1.3.2. *Uma curva é dita* racional *se possui gênero zero. Em particular,* $g(\mathbb{P}^1) = 0$.

Sobre curvas racionais temos a seguinte caracterização.

Proposição 1.3.3. *Seja $\mathcal{X}$ uma curva plana irredutível e não singular. São equivalentes as seguintes afirmações.*

a) $\mathcal{X}$ é isomorfo à $\mathbb{P}^1$;

b) existe $p \in \mathcal{X}$ tal que $l(P) > 1$.

Demonstração. Corolário da seção 8.2 de (Fulton 1989). □

2 Teorema de Riemann–Roch

Neste Capítulo veremos o Teorema de Riemann–Roch e algumas aplicações. o Teorema de Riemann–Roch possui varias aplicações na Geometria Algébrica, um dos objetivos deste capítulo é utilizar este teorema para relacionar curvas e semi-grupos numéricos. Ainda, veremos a definição de extensões de corpos de funções que generaliza o conceito apresentado no Capítulo 1 e exibimos dois especias e bem conhecidos de extensões: extensão de Kummer e extensão Artin– Schreier.

2.1 O Teorema de Riemann–Roch

Definição 2.1.1. *Seja F/K um corpo de funções de gênero g. Para $D \in Div(F)$ definimos o* índice de especialidades *de D como*

$$i(D) := l(D) - Deg(D) + g - 1 \tag{2.1}$$

Seja F/K um corpo de funções de gênero g. Então Dado $D \in Div(F)$ temos da definição de gênero de um corpos de funções que a seguinte desigualdade é satisfeita

$$l(D) \geq Deg(D) + 1 - g. \tag{2.2}$$

Como vimos no Capítulo anterior, curvas e corpos de funções algébricos estão relacionados. Assim, podemos dizer que o gênero de uma curva é o mesmo que o gênero do corpo de função associado à ela. Porém, quando falamos de curvas planas existem outras maneiras de calcular o gênero de uma curva ou de exibir uma cota para o mesmo. Denotando por $r_p = v_p(\mathcal{X})$ a valorização da curva $\mathcal{X}$ num ponto $p \in \mathcal{X}$. Se m é o grau desta curva e g o gênero, então

$$g \leqslant \frac{(m-1)(m-2)}{2} - \sum_{p \in \mathcal{X}} \frac{r_p(r_p-1)}{2}.$$

Sabemos ainda que no caso particular de uma curva não singular, o gênero da curva é dado por

$$g = \frac{(m-1)(m-2)}{2}.$$

Em algumas literaturas o valor $v_p(\mathcal{X})$ é chamado de multiplicidade da curva no ponto p.

Exercício 2.1.1. *Ache uma cota para o gênero das seguintes curvas. Se for possível, calcule explicitamente o gênero.*

a) $x^2 + y^2 + z^2$;

b) $x^2y^2 - z^2(x^2 + y^2)$;

c) $x^{q+1} - y^q - y$;

d) $z^9 + x^3y^6 + y^3x^6$.

Teorema 2.1.1 (Teorema de Riemann)**.** *Seja F/K um corpo de funções de gênero g. Então existe $a \in \mathbb{Z}$ que depende somente de F/K tal que $Deg(D) \geqslant a$ implica que*

$$l(D) = Deg(D) + 1 - g.$$

Demonstração. Escolhamos um divisor D' com $g = deg(D') - \ell(D_0) + 1$ e definamos $a = deg(D') + g$.

Se $deg(D) \geqslant a$, então

$$l(D - D') \geqslant deg(D - D') + 1 - g = deg(D) - deg(D') + 1 - g \geqslant a - deg(D') + 1 - g = 1.$$

Assim, existe um elemento $0 \neq z \in L(D - D')$. Consideremos o divisor $D'' = A + \mathrm{div}(z) \geqslant D'$.

Então, pelo temos que $Deg(D) - \ell(D) = deg(D'') - \ell(D'') \geqslant deg(D') - \ell(D') = g - 1$.

Portanto $l(A) \leqslant deg(A) - g + 1$, o que nos dá finalmente a igualdade desejada. □

Como consequência deste teorema obtemos que o índice de especialidade de qualquer divisor sempre será um número natural.

Exemplo 2.1.1. *Seja K um corpo qualquer. Vamos mostrar que $K(x)/K$ possui gênero zero. Com efeito, seja P um polo de x, então tomando n suficientemente grande, podemos aplicar o Teorema de Riemann para $\mathcal{L}(nP)$. Como $1, x, \ldots, x^n$ são linearmente independentes sobre K temos*

$$1 + n \leqslant \ell(nP) = n + 1 - g.$$

Logo, $g \leqslant 0$, isto é, $g = 0$ (pelo Corolário 1.3.2).

Sobre gênero de corpos de funções (ou curvas) podemos fazer a seguinte pergunta: dado g um numero natural, existe um corpo de funções algébricos com este gênero?

Vimos que para $g = 0$ ou 1 esta resposta é afirmativa. Para demais valores, basta considerarmos a curva dada por $f(x)y^2 + g(x)$ onde f, g são polinômios de grau g e $g + 2$, respectivamente.

Voltaremos a esta pergunta para o caso particular quando tratarmos de curvas definidas sobre corpos finitos que são "maximais".

Definição 2.1.2. *Um* adele *de F/K é uma aplicação*

$$\begin{aligned} \alpha : \mathbb{P}_F &\longrightarrow F \\ P &\longmapsto \alpha_P \end{aligned}$$

$\alpha_P \in \mathcal{O}_P$ para quase todo P. O conjunto $\mathcal{A}_F : \{\alpha \mid \alpha$ é um adele $\}$ de todos adeles de F/K é chamado de espaço de adeles *de F/K. É fácil ver que $\mathcal{A}_F$ possui estrutura de K-espaço vetorial.*

Mais ainda, como uma função $z \in F$ possui um número finito de polos, a multiplicação $z\alpha_P$ pode ser definida da mesma forma e ainda será um adele, de onde segue que $\mathcal{A}_F$ também possui estrutura de $F-$espaço vetorial. O mesmo

argumento também nos permite ver que a aplicação constante $P \mapsto z$ um adele, dito um *adele principal*, e, assim, temos uma inclusão de F em $\mathcal{A}_F$. Portanto, a valorização v_P se estende naturalmente à $\mathcal{A}_F$ definindo $v_P(\alpha) := v_P(\alpha_P)$.

Dado um divisor $D \in Div(F)$ nos definimos o conjunto

$$\mathcal{A}_F(D) := \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geqslant -v_P(D),\ \forall P \in \mathbb{P}_F\}.$$

Claramente $\mathcal{A}_F(D)$ é um K-subespaço de $\mathcal{A}_F$.

Exercício 2.1.2. *Sejam $D_1, D_2 \in Div(F)$ com $D_1 \leqslant D_2$. Mostre que $\mathcal{A}_F(D_1) \subset \mathcal{A}_F(D_2)$ e*

$$\frac{\mathcal{A}_F(D_2)}{\mathcal{A}_F(D_1)} = Deg(D_2) - Deg(D_1). \tag{2.3}$$

Teorema 2.1.2. *Para todo $D \in Div(F)$ temos que*

$$i(D) = dim_K\left(\frac{\mathcal{A}_F}{\mathcal{A}_F(D) + F}\right).$$

Demonstração. ver em (Stichtenoth 1993). □

A demonstração do seguinte corolário é imediata.

Corolário 2.1.1. *Seja g o gênero de F/K. Então*

$$dim_K\left(\frac{\mathcal{A}_F}{\mathcal{A}_F(0) + F}\right) = g.$$

Definição 2.1.3. *Uma aplicação K-linear $\omega : \mathcal{A}_F \to K$ que se anula em $\mathcal{A}_F(D)+F$ para algum $D \in Div(F)$ é chamada de* diferencial de Weil. *O conjunto*

$$\Omega_F := \{\omega \mid \omega \text{ é um diferencial de Weil}\}$$

é chamado de módulo de diferenciais de Weil *de F/K.*

Assim como fizemos para o conjunto de todos adeles de F/K podemos para cada $D \in Div(F)$ definir o conjunto

$$\Omega_F(D) := \{\omega \in \Omega_F \mid \omega \text{ se anula em } \mathcal{A}_F(D) + F\}.$$

Destacamos que Ω_F possui estrutura de K-espaço vetorial. Com efeito, sejam $\omega_1, \omega_2 \in \Omega_F$ e $\lambda \in K$ com ω_1 se anulando em $\mathcal{A}_F(D_1)$ e ω_2 se anulando em $\mathcal{A}_F(D_2)$. Então pelo Exercício 2.1.2 temo que $\lambda\omega_1 - \omega_2$ se anula em $\mathcal{A}_F(D_3)$ para qualquer divisor D_3 tal que $D_3 \leqslant D_1$ e $D_3 \leqslant D_2$.

Seja $D \in Div(F)$, considere o conjunto $\left(\frac{\mathcal{A}_F}{\mathcal{A}_F(D)+F}\right)^*$ dos funcionais K-lineares de $\frac{\mathcal{A}_F}{\mathcal{A}_F(D)+F}$. Definimos a aplicação

$$\begin{aligned} \gamma : \Omega_F &\longrightarrow \frac{\mathcal{A}_F}{\mathcal{A}_F(D)+F} \\ \omega &\mapsto \overline{\omega} \end{aligned}$$

onde $\overline{\omega}$ é uma aplicação definida por $\overline{\omega}(u + \mathcal{A}_F(D) + F) := \omega(u)$. Temos que γ é K-isomorfismo linear e portanto

$$dim_K \Omega_F = i(D). \tag{2.4}$$

Por 2.4 temos que $\Omega_F \neq \{0\}$. Outra consequência de 2.4 (e Teorema 2.1.2) é que temos a seguinte versão preliminar do Teorema de Riemann–Roch.

$$l(D) = Deg(D) + 1 - g + i(D), \tag{2.5}$$

para cada $D \in Div(F)$.

Definição 2.1.4. *Sejam $z \in F$ e $\omega \in \Omega_F$. Definimos o mapa*

$$\begin{aligned} z\omega : \mathcal{A}_F &\longrightarrow K \\ a &\mapsto \omega(za) \end{aligned}$$

Observamos que $z\omega \in \Omega_F$. De fato, como ω se anula em $\mathcal{A}_F(D) + F$ para algum divisor D, então $z\omega$ se anula em $\mathcal{A}_F((D + (z)) + F)$. Portanto, Ω_F, possui estrutura de $F-$espaço.

Exercício 2.1.3. *Mostre que com a aplicação acima, Ω_F é um $F-$espaço vetorial.*

Para cada diferencial de Weil não nulo ω definimos o seguinte conjunto

$$\mathcal{M}(\omega) := \{D \in Div(F) | \ \omega \ se \ anula \ em \ \mathcal{A}_F(D) + F\}.$$

Como consequência do Teorema de Riemann observamos que existe uma constante a que depende somente do corpo F satisfazendo a condição de que um divisor

D com $Deg(D) \geqslant a$ então o índice de especialidade é nulo, isto é, $i(D) = 0$. Este fato somado ao de que $\dim(\frac{\mathcal{A}_F}{\mathcal{A}_F(D)+F}) = i(D)$ garante que todo elemento $\mathcal{M}(\omega)$ possui grau menor que a. Desta forma temos a existe de um elemento V em $\mathcal{M}(\omega)$ com grau o maior possível.

Proposição 2.1.1. *Seja F/K um corpo de funções.*

a) $dim_F(\Omega_F) = 1$.

b) Seja $0 \neq \omega \in \Omega_F$. Então existe um divisor unicamente determinado $W \in \mathcal{M}(\omega)$ tal que $D \leqslant W$ para todo $D \in \mathcal{M}(\omega)$.

Demonstração. □

Definição 2.1.5. *Seja $0 \neq \omega \in \Omega_F$. O divisor (ω) é chamado* divisor canônico *de F/K. (ω) é um divisor unicamente determinado satisfazendo:*

1. *ω se anula em $\mathcal{A}_F((\omega)) + F$,*
2. *Se ω se anula em $\mathcal{A}_F(D) + F$ então $D \leqslant (\omega)$.*
3. *Para $P \in \mathbb{P}_F$ definimos $v_P(\omega) := v_P((\omega))$.*
4. *Um place P é dito* zero *de ω se $v_P(\omega) > 0$. O diferencial de Weil é dito* regular *em P se $v_P(\omega) \geqslant 0$ e* holomorfa *se $v_P(\omega) \geqslant 0$ para todo place P.*
5. *Um place P é dito polo de ω se $v_P(\omega) < 0$.*

Notamos que para cada $0 \neq z \in F$ e $0 \neq \omega \in \omega_F$ temos que

$$(z\omega) = \text{div}(z) + (\omega). \tag{2.6}$$

Com efeito, existe uma divisor D tal que ω se anula em $\mathcal{A}_F(D) + F$. Portanto, $z\omega$ se anula em $\mathcal{A}_F(D + (z)) + F$. Então $\text{div}(z) + (\omega) \leqslant (z\omega)$ e consequentemente $(z\omega) + \text{div}(z^{-1}) \leqslant (z\omega z^{-1}) = (\omega)$. Juntando essas informações segue a igualdade.

Proposição 2.1.2. *Seja D um divisor em um corpo de funções F/K de gênero g.*

a) $\Omega_F(D) = \{\omega \in \Omega_F \,|\, \omega = 0 \text{ ou } (\omega) \geqslant D\}$, $\Omega_F(0) = \{\omega \in \Omega_F \,|\, \omega \text{ é regular}\}$ *e* $\dim(\Omega_F(0)) = g$.

b) Sejam W e W' dois divisores canônicos. Então existe $0 \neq z \in F$ tal que $W' = W + \mathrm{div}(z)$.

Demonstração. a) Basta aplicar a definição anterior e a igualdade 2.4.

b) Segue da observação acima e do item *a*) da Proposição 2.1.1.

□

Teorema 2.1.3. *Sejam $D \in Div(F)$ um divisor qualquer e $W = (w)$ um divisor canônico de F/K. Então $\mathcal{L}(W-D)$ e $\Omega_F(D)$ são isomorfismos como K-espaços.*

Demonstração. Considere a aplicação

$$\begin{aligned} \Psi : \mathcal{L}(W - D) &\longrightarrow \Omega_F(D) \\ z &\longmapsto z\omega \end{aligned}$$

Segue da igualdade 2.6 que Ψ está bem definida e sua linearidade e injetividade surge diretamente da sua definição, portanto basta verificarmos a sobrejetividade. Com efeito, dado $\omega' \in \Omega_F(D)$. Como $\Omega_F(D)$ tem dimensão um, existe $z \in F$ tal que $\omega' = z\omega$. Desta forma $\mathrm{div}(z) + W = \omega' \leqslant D$ e isto implica que $z \in \mathcal{L}(W - D)$, isto é, $\Psi(z) = \omega'$.

□

Segue o Teorema 2.1.3 e do fato $i(D) = dim_K \Omega_F(D)$ que

$$i(D) = l(W - D) \tag{2.7}$$

para qualquer $D \in Div(F)$.

Os resultados precedentes convergem no importante resultado a seguir

Corolário 2.1.2 (Teorema de Riemann–Roch). *Seja W um divisor canônico do corpo de funções F/K de gênero g. Para qualquer divisor $D \in Div(F)$ temos*

$$l(D) = Deg(D) + 1 - g + l(W - D). \tag{2.8}$$

Corolário 2.1.3. *Todo divisor canônico de um corpo de funções F/K de gênero g satisfaz*

$$Deg(W) = 2g - 2 \ \ e \ \ \ell(W) = g$$

Demonstração. Primeiro vamos calcular a dimensão de um divisor canônico. Seja $D = 0$ um divisor nulo, então pelo Teorema de Riemann–Roch temos que $1 = l(0) = 1 - g + l(W)$, isto é, $l(W) = g$. Agora tomando $D = W$ obtemos que $g = l(W) = 1 - g + l(0) + Deg(W)$, ou seja, $Deg(W) = 2g - 2$. □

No próximo exemplo voltamos ao Exemplo 1.1.1 onde estudamos uma curva C com equação $y^2 = (x - c_1)(x - c_2)(x - c_3)$ e verificamos que a mesma possui gênero um.

Exemplo 2.1.2. *Vamos mostrar utilizando o Teorema de Riemann–Roch que uma curva com $g = 1$ tem mesma equação que C. De fato, seja $P \in C$ um ponto qualquer. Então pelo item a) do Teorema de Riemann temos que $l(P) \geqslant 1$. Da Proposição 1.3.3 temos que $l(P) = 1$.*

***Afirmação:** Dado um número natural $s \geqslant 1$ temos que $l(sP) = s$. De fato, como $g = 1$ temos que todo divisor canônico possui grau nulo, assim $Deg(W - sP) = -s < 0$. Portanto, $l(sP) = s + 1 - 1 = s$, isto é, $l(P) = 1$, $l(2P) = 2$, ..., $l(iP) = i$ para cada $i \geqslant 1$.*

Como $sP \geqslant (s + 1)P$ obtemos a seguinte cadeia de inclusões

$$\mathcal{L}(P) \subsetneq \mathcal{L}(2P) \subsetneq \cdots \subsetneq \mathcal{L}(6P). \tag{2.9}$$

Seja $1, x$ uma base para $\mathcal{L}(2P)$. Pela equação 2.9 seja $y \notin \mathcal{L}(2P)$ tal que $1, x, y$ seja base de $\mathcal{L}(3P)$. Observamos que $(x)_\infty = 2P$ (Caso contrário C seria racional) e $\mathrm{div}(y)_\infty = 3P$, então $K_C = K(y, x)$ e $[K_C : K(x)] = 2$. Segue portanto que $1, x, y, xy, x^2, y^2 \in \mathcal{L}(6P)$. Então existe uma relação

$$b_1 y^2 + y(a_1 + a_2 x) = f(x), \tag{2.10}$$

com $a_1, a_2, b_1, b_2 \in K$ e $f(x) \in K[x]$ um polinômio com grau no máximo três. Após algumas manipulações adequadas, podemos reescrever a equação 2.10 como $y^2 = (x - c_1)(x - c_2)(x - c_3)$, com $c_1, c_2, c_3 \in K$.

Corpos de funções algébricos que contém um divisor de grau um e possuem gênero um são chamados de *corpos de funções elípticos*. Um curva cujo corpo de funções satisfaz as condições anteriores é chamada de *curva elíptica*.

Proposição 2.1.3. *Sejam F/K um corpo de funções de gênero g e D um divisor tal que $Deg(D) \geqslant 2g - 1$. Então $l(D) = Deg(D) + 1 - g$.*

Demonstração. Basta notar que $Deg(W - D) \leqslant (2g - 2) - (2g - 1) < 0$, onde W é um divisor canônico de F. □

No próximo resultado, caracterizamos todos os divisores canônicos.

Proposição 2.1.4. *Seja F/K um corpo de funções de gênero g. Um divisor D é canônico se, e somente se, $Deg(D) = 2g-2$ e $l(D) \geqslant g$.*

Demonstração. A ida desta afirmação já foi verificada. Agora seja D um divisor tal que $Deg(D) = 2g-2$ e $l(D) \geqslant g$. Como]

$$l(W-D) + 1 - g = Deg(D) + l(W-D) + 1 - g \geqslant g,$$

onde concluímos que $l(W-D) \geqslant 1$. Portanto, $Deg(W-D) = 0$ e como vimos anteriormente estes dois divisores são equivalentes. □

Definição 2.1.6. *Seja $P \in \mathbb{P}_F$. Um inteiro $a \geqslant 0$ é chamado de* não lacuna (ou non-gap number) *de P se existe um elemento $x \in F$ tal que $(x)_\infty = aP$. Caso contrário a é chamado de* lacuna (ou gap number) *de P.*

Proposição 2.1.5. *Sejam F/K um corpo de funções de gênero g e $P \in \mathbb{P}_F$. Então cada $a \geqslant 2g$ é um não lacuna de F. Em outras palavras existe $x \in F$ com divisor de polos $(x)_\infty = aP$.*

Demonstração. Dado um inteiro $a \geqslant 2g$, consideramos o divisor $D = aP$, então $Deg((a-1)P) = (a-1)Deg(P) \geqslant 2g-1$. Segue da Proposição 2.1.3 que $l((a-1)P) = (a-1)Deg(P) + 1 - g$ e $l(aP) = aDeg(P) + 1 - g$, ou seja, $l((a-1)P) < l(aP)$. Assim, $\mathcal{L}((a-1)P) \subsetneq \mathcal{L}(aP)$. Em outras palavras, cada elementos x de $\mathcal{L}(aP)$ que não está em $\mathcal{L}((a-1)P)$ satisfaz $(x)_\infty = aP$.

□

Esta proposição mostra que dado F/K um corpo de funções de gênero g (ou uma curva plana de gênero g) todo natural $n \geqslant 2g$ é um não lacuna de F, isto é, os números $2g, 2g+1, 2g+2, \ldots$, são sempre não lacunas. Percebemos que para um corpo de funções (ou uma curva) de gênero g existirão um número finito de números que são lacunas e estes se encontram abaixo de $2g-1$. Este fato aguça nossa intuição para a possibilidade do surgimento de um novo objeto (isto ficará mais claro nos próximos resultados).

Teorema 2.1.4 (*Teorema das lacunas de Weierstrass*)**.** *Suponha que F/K possui gênero $g > 0$ e P um place de grau um. Então existe exatamente g lacunas $i_1 < \cdots < i_g$ de P. Temos ainda que,*

$$i_1 = 1 \quad e \quad i_g \leqslant 2g-1.$$

Demonstração. temos a seguinte caracterização das lacunas:

$$a \text{ é lacuna de P se, e só se, } \mathcal{L}((a-1)P) = \mathcal{L}(aP).$$

Olhando para a sequência de espaços vetoriais

$$K = \mathcal{L}(0) \subset \mathcal{L}(P) \subset \mathcal{L}(2P) \subset \cdots \mathcal{L}((2g-1)P)$$

E lembrando que $dim\mathcal{L}(0) = 1$, $dim\mathcal{L}((2g-1)P) = g$ e $dim\mathcal{L}(iP) \leqslant dim\mathcal{L}((i-1)P) + 1$, para todo i. Juntando essas informações podemos concluir o teorema. □

Exercício 2.1.4. *Considere $\mathcal{X}$ uma curva, $D \in Div(\mathcal{X})$ e $p \in \mathcal{X}$ um ponto. Mostre que $\ell(W - D - p) \neq \ell(W - D)$ se, e somente se, $\ell(D + p) = \ell(D)$, onde W é um divisor canônico.*

Exercício 2.1.5. *Considere $\mathcal{X}$ uma curva e $D, D' \in Div(\mathcal{X})$ divisores tais que $D + D' = W$, onde W é um divisor canônico. Mostre que $\ell(D) - \ell(D') = \frac{Deg(D) - Deg(D')}{2}$*

2.2 Semigrupos Numéricos

Antes de apresentarmos a definição de semigrupo de Weierstrass precisamos da seguinte definição.

Definição 2.2.1. *Seja $S \subset \mathbb{N}_0$. Dizemos que S é um* Semigrupo Numérico *se:*

1. $0 \in S$.
2. $x + y \in S$, *para* $x, y \in S$.
3. $G(S) := \mathbb{N}_0 - S$ *é finito.*

Os elementos de $G(S)$ são chamados de *lacunas* (ou gaps) de S. A cardinalidade de $G(S)$ é chamada de *gênero* de S. Sobre semigrupos numéricos existem outros elementos importantes que valem a pena serem destacadas. Entre eles são:

1. A *Multiplicidade* de um semigrupo numérico é o menor elemento não nulo de S. Denotamos $m(S) := min\{x \in S \mid x \neq 0\}$.
2. O *número de Frobenius* de S é o maior natural que não está em S. Denotamos $F(S) := maxG(S)$.

Exemplo 2.2.1. *$S = \mathbb{N}_0$ é um semigrupo numérico com gênero zero. Além disso, é o único semigrupo o qual possui gênero nulo.*

Se S possui gênero g podemos mostrar que

$$0 \leqslant m(S) \leqslant g + 1.$$

Exemplo 2.2.2. *Se S tem gênero g e multiplicidade igual à 2, então*

$$S = \{0, 2, 4, 6, \ldots, 2g - 2, 2g, 2g + 1, \ldots\}.$$

Este semigrupo é chamado de semigrupo Hiperelíptico.

Notamos que se S tem gênero g, então $[2g, \infty) \subset S$. Com efeito, em $[1, 2g]$ existem, pelo menos, g não lacunas $b_1, \ldots, b_g$. Se existe $x \geqslant 2g$ sendo uma gap, então $x \neq x - b_i \in G(S)$ para cada $i = 1, \ldots, g$. Portanto, existiriam pelo menos $g + 1$ gaps o que é um absurdo.

Dado um semigrupo numérico S, um elemento de S é chamado de *condutor* de S e, denotado por $c(S)$, se para cada $x \in \mathbb{N}$ com $x \geqslant c$ então $x \in S$. Em outras palavras $c(S) = F(S) + 1$.

Sobre o condutor de um semigrupo, temos o seguinte resultado.

Lema 2.2.1. *Seja S um semigrupo numérico de gênero g. Então $g + 1 \leqslant c(S) \leqslant 2g$.*

Exemplo 2.2.3. *Considere o conjunto $S = \{0, 5, 10, 11, 12, 14, \ldots\}$. Vemos que $G(S) = \{1, 2, 3, 4, 6, 7, 8, 9, 13\}$ é finito e que é fechado em ralação a soma. Logo, $g(S) = 9$ e $m(S) = 5$. Notamos que*

Definição 2.2.2. *Dados $n_1, n_2, \ldots, n_r \in \mathbb{N}$ relativamente primos entre si. O conjunto*

$$< n_1, n_2, \ldots, n_r >:= \{a_1 n_1 + \cdots + a_r n_r | \; com \; a_1, \ldots, a_r \in \mathbb{N}_0\}$$

é um semigrupo numérico. Tal semigrupo é chamado de semigrupo gerado *por $n_1, n_2, \ldots, n_r$*

Todo semigrupo numérico possui um conjunto de geradores, para mais detalhes ver (Rosales e Garcia-Sánchez 2009).

Exemplo 2.2.4. *Seja $S =< 2, 3 >$. Como 2 é coprimo com 3 temos que S é um semigrupo numérico onde $S = \{0, 2, 3, 4, 5, 6, 7, \ldots\}$ e $G(S) = \{1\}$*

Para semigrupos numéricos como do exemplo anterior, isto é, gerados por dois elementos, existe uma formula dependendo apenas dos geradores: Se $S =< a, b >$ então

$$g(S) = \frac{(a-1)(b-1)}{2} \tag{2.11}$$

Para ver a demonstração deste fato o leitor pode consultar (Rosales e Garcia-Sánchez 2009).

As demonstrações dos próximos resultados são deixadas como exercício ao leitor.

Teorema 2.2.1. *Sejam S semigrupo numérico e $m \in S$. Estão $S \setminus \{m\}$ é um semigrupo numérico se, e somente se, m é um gerador minimal de S.*

Teorema 2.2.2. *Sejam S' e S dois semigrupos numéricos. Então*

a) $S + S' = \{m + n |\ m \in S \text{ e } n \in S'\}$ semigrupo numérico.

b) Se α é um conjunto de geradores de S e β é um conjunto de geradores de S', então $\alpha \cup \beta$ é um conjunto de geradores de $S + S'$.

Seja $\mathcal{X}_F$ uma curva plana, projetiva, irredutível e considere um ponto $P \in \mathcal{X}_F$.
Considere $\mathcal{L}(mP)$ o conjunto de funções racionais com polos somente em P.
Construímos o conjunto $U = \bigcup_{m \geqslant 0} \mathcal{L}(mP)$.
Notamos a seguinte caracterização

$$l(mP) = l((m-1)P) + 1 \text{ se e só se } f \in U \text{ com } v_P(f) = -m.$$

Definimos o seguinte conjunto

$$H_F(P) := \left\{-v_P(f) |\ f \in U^*\right\}. \tag{2.12}$$

Teorema 2.2.3. *O conjunto $H_F(P)$ é um semigrupo numérico de gênero g.*

Demonstração. Se $m, n \in \Lambda_F(P)$ então existem $f, g \in A$ tais que $v_P(f) = -m$ e $v_P(g) = -n$. Se $m \geqslant 2g - 1$, temos pelo Teorema de Riemann–Roch que $\ell(mP) = m + 1 - g$ onde g é o gênero da curva. Por outro lado, temos por resultados anteriores que $m \in \Lambda_F(P)$ para todo $m \geqslant 2g$. Isto mostra que $l(mP) = l((m-1)P)$ somente para g valores de m. Logo, $\#G(\Lambda_F(P)) = g$. □

Definição 2.2.3. *Um semigrupo numérico S é dito ser um* semigrupo de Weierstrass *se existe uma curva $\mathcal{X}_F$ e um ponto $P \in \mathcal{X}_F$ tais que $S = H_F(P)$.*

Neste primeiro exemplo estudaremos à curva Hermitiana. O semigrupo desta curva tem sua importância devido a caracterizar a família de semigrupos gerados por dois elementos como sendo todos Weierstrass. Neste exemplo utilizamos propriedades de curvas para obter o semigrupo, nas sessão seguintes aprenderemos outros métodos para calcular este e outros semigrupo de forma mais simples.

Exemplo 2.2.5. *Seja q potência de um primo, $\mathcal{H}_q : X^{q+1} - Y^q Z - Y Z^q$ sobre $\mathbb{F}_{q^2}$. Sabemos que $P_\infty = (0 : 1 : 0)$ é o único ponto no infinito (com $Z = 0$) da curva $\mathcal{H}_q$.*
Como a reta tangente a curva Hermitiana em P_∞ é $-Z$, temos que $t = \frac{X}{Y}$ é parâmetro local em P_∞.
Observamos que $\frac{X}{Z}, \frac{Y}{Z}$ são funções regulares fora de P_∞. Calculando a valorização, temos:

- $t^{q+1} = (\frac{Z}{Y})^q + \frac{Z}{Y} \Rightarrow v_{P_\infty}((\frac{Z}{Y})^q + \frac{Z}{Y}) = q + 1 \Rightarrow v_{P_\infty}(\frac{Y}{Z}) = -(q+1)$.
- $(\frac{Z}{Y})^{q+1} = (\frac{Y}{Z})^q + \frac{Y}{Z} \Rightarrow (q+1) v_{P_\infty}(\frac{X}{Z}) = -q(q+1) \Rightarrow v_{P_\infty}(\frac{X}{Z}) = -q$.

Logo, $q, q+1 \in H_{\mathcal{H}_q}(P_\infty)$. Portanto, o semigrupo gerado por $q, q+1$ ($< q, q+1 >$) está contido em $H_{\mathcal{H}_q}(P_\infty)$. Utilizando a fórmula para gênero de um semigrupo gerado por dois elementos, temos que

$$g(< q, q+1 >) = \frac{q(q-1)}{2}$$

. Conclusão:

$$H_{\mathcal{H}_q}(P_\infty) =< q, q+1 > .$$

A luz do exemplo anterior, podemos questionar se todo semigrupo numérico é um semigrupo de Weierstrass. Esta problemática foi introduzida em 1890 por Hurwitz. Após quase 80 anos de estudos foi observada uma condição necessária para que um semigrupo numérico fosse de Weierstrass. Tal condição é chamada de condição de Buchtweitz e é apresentada a seguir. Seja H um semigrupo numérico com conjuntos de lacunas $G := \{\ell_1, \ldots, \ell_g\}$. Definimos o conjunto das n somas de G por

$$nG := \{\ell_{i_1} + \cdots + \ell_{i_n} | \ell_{i_j} \in G\}.$$

A condição dada por Buchtweitz é: H é Weierstrass então

$$\#nG \leqslant (2n-1)(g-1)$$

para todo $n \in \mathbb{N}$ com $n \geqslant 2$.

Essa condição é ideal para verificarmos que semigrupo numérico H não é Weierstrass. Por exemplo, um dos primeiros exemplos que mostram que nem todo semigrupo numérico é Weierstrass é H tal que $G = \{1, 2, \ldots, 11, 12, 19, 21, 24, 25\}$.

Vejamos mais alguns exemplos de semigrupos de Weierstrass.

Exemplo 2.2.6. *Curva GK: Considere $q = n^3$, para $n \geqslant 2$. A curva $\mathcal{GK}$ é definida pela equações*

$$\begin{aligned} z^{n^2-n+1} &= y\sum_{i=0}^{n}(-1)^{i+1}x^{i(n-1)} \\ x^n + x &= y^{n+1}, \end{aligned}$$

definida sobre $\mathbb{F}_{q^2}$. O gênero de $\mathcal{GK}$ é dado por $g = \frac{(n^3+1)(n^2-2)}{2} + 1$ e possui um único ponto no infinito $P_\infty = (1:0:0:0)$. Outra propriedade interessante desta curva é que ela é uma curva maximal.

Vamos denotar por $P_j := (a_j, 0, 0) \in \mathcal{GK}(\mathbb{F}_{q^2})$ tais que $a_j^n + a_j = 0$, para $j = 1, \ldots, n$. $Q_j := (a_j, b_j, 0) \in \mathcal{GK}(\mathbb{F}_{q^2})$ tais que $a_j^n + a_j = b_j^{n+1}$ e $b_j \neq 0$, para $j = 1, \ldots, n^3 - n$. Usando as equações da curva $\mathcal{GK}$ podemos exibir funções satisfazendo

$$\begin{aligned} (z) &= \sum_{j=1}^{n^3-n} Q_j + \sum_{j=1}^{n} P_j - n^3 P_\infty \\ (y) &= \sum_{j=1}^{n}(n^2-n+1)P_j - (n^3-n^2+n)P_\infty \\ (x-a_j) &= (n^3+1)(P_j - P_\infty). \end{aligned}$$

Usando essas funções podemos provar que

$$H(P_\infty) = H(Q_i) = H(P_j) = < n^3 - n^2 + n, n^3 + 1, n^3 >,$$

para cada $i = 1, \ldots, n^3 - n$ e $j = 1, \ldots, n$.

Exemplo 2.2.7. *(Matthews e Peachey 2010) Seja* $\mathbb{F}_{27} = \mathbb{F}_3(w)$*, onde* $w^3 - w + 1 = 0$*. A curva norma-traço sobre* $\mathbb{F}_{27}$ *é dada pela equação* $y^9 + y^3 + y = x^{13}$*. Esta curva possui exatamente 9 places da forma* $P_i = P_{0a_i}$*, onde* $a_0 = 0, a_1 = 1, a_2 = 2, a_3 = w, a_4 = w^3, a_5 = w^9, a_6 = w^14, a_7 = w^16, a_8 = w^22$*. Após alguns cálculos obtemos*

$$G(P_\infty) = \{1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 15, 16, 17, 19, 20, 21, 23, 24, 25, 28, 29, 30, 32, 33, 34, 37, 38, 41, 42, 43, 46, 47, 50, 51, 55, 56, 59, 60, 64, 68, 69, 73, 77, 82, 86, 95\},$$

onde P_∞ *é o ponto no infinito da curva norma-traço.*

2.3 Extensões Algébricas de Corpos de Funções

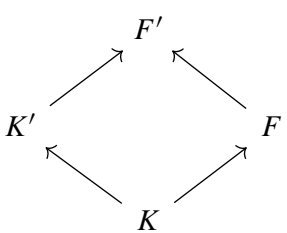
Seja F/K um corpo de funções de uma variável sobre o corpo de constantes K e vamos considerar F'/K' um corpo de funções de uma variável sobre o corpo de constantes K' tal que $F \subset F'$ é uma extensão algébrica e $K \subset K'$.

Nesta seção vamos considerar que K é um corpo perfeito e vamos considerar que F e F' estão ambos sobre um mesmo corpo algebricamente fechado.

Definição 2.3.1. *Um corpo de funções* F'/K' *é chamado de* extensão algébrica *de* F/K *se* $F \subset F'$ *como extensão algébrica e* $K \subset K'$*.*

1. F'/K' *é chamada de* extensão de corpos constante *se* $F' = FK'$*, isto é,* F' *é o corpo compósito de* F *e* K'*.*
2. F'/K' *é chamada de* extensão finita *se* $[F' : F] < \infty$*.*

Podemos observar a definição no diagrama abaixo.



Sobre a definição acima observamos através do diagrama e de propriedades do grau de transcendência que K'/K é uma extensão algébrica. Verificamos ainda

que $F \cap K' = K$. Com efeito, se $x \in F \cap K'$, temos que $x \in F$ e x é algébrico sobre K, pois $x \in K$. Como K é algebricamente fechado em F, temos que $x \in K$, o que mostra que $F \cap K' \subset K$.

Exemplo 2.3.1. *Um exemplo de extensões: Tomemos $K = K' = \mathbb{F}_q$, $F = K(x)$ como o corpo de de funções racionais e $F' = K(x, y)$ com $y^q = x^{q+1} + x$.*

Sobre a definição anterior e a Definição 1.2.1, podemos construir novos objetos. Suponha que $K = \mathbb{F}_q$ um corpo com q elementos. Considere corpos de funções F_i/K com $i \geqslant 0$ satisfazendo

1. $F_i \subsetneqq F_{i+1}$, para todo $i \geqslant 0$.
2. F_{i+1}/F_i é finita e separável.
3. $lim_{i\to\infty} g(F_i) = \infty$.

A sequência acima é chamada de Torre de funções. Note que $F_{i+1} = F_i(x_i)$.

A seguir apresentamos alguns exemplos de Torre de Funções sobre $\mathbb{F}_q$:

$$\mathcal{TF}: \qquad x_{i+1}^m = a(x_i + b)^m + c \tag{2.13}$$

$$\mathcal{F}_1: \qquad x_{i+1}^2 = \frac{x_i(1 - x_i)}{x_i + 1} \tag{2.14}$$

$$\mathcal{F}_2: \qquad x_{i+1}^2 = \frac{x_i^2 + 1}{2x_i} \tag{2.15}$$

Em (2.13) $a, b, c \in \mathbb{F}_q^\times$, com $ab^m + c = 0$ e $mdc(m, q) = 1$. Em (2.15) $2 \nmid q$. A Torre 2.13 é chamada Torre de Fermat. Mais informações sobre estas Torres, o leitor encontrará em (Garcia, Stichtenoth e Rück 2003).

Seja $z \in F$. Para diferenciar os divisores (z), $(z)_0$ e $(z)_\infty$ em cada extensão vamos denotar $(z)^F$, $(z)_0^F$ e $(z)_\infty^F$ em $Div(F)$ e $(z)^{F'}$, $(z)_0^{F'}$ e $(z)_\infty^{F'}$ em $Div(F')$.

Lema 2.3.1. *Seja F'/K' uma extensão algébrica de F/K. Se F'/K' é uma extensão finita de F/K se, e só se, K'/K é finita.*

Demonstração. Suponhamos que F'/K' é uma extensão finita de F/K. Então F' pode ser considerado um corpo de funções sobre K cujo corpo de constantes é K' . De fato, por hipótese F'/F é uma extensão finita e como F/K é um corpo de funções, temos que existe $w \in F$, w transcendente sobre K, tal que $[F : K(w)] < \infty$. Isso nos dá que $F'/K(w)$ é uma extensão finita. Ainda, como K' é

algebricamente fechado em F', temos que o corpo de constantes de F'/K é K'. Portanto, concluirmos que $[K' : K] < \infty$.

A volta deixamos como exercício para o leitor. □

Definição 2.3.2. *Seja F'/K' uma extensão de algébrica de F/K. Um place $Q \in \mathbb{P}_{F'}$ é dito uma* extensão *(ou está sobre) de $P \in \mathbb{P}_F$ quando $P \subset Q$. Quando Q está sobre P denotamos $Q|P$.*

Está definição levanta três pontos. Primeiro ponto é se para cada place em $\mathbb{P}_F$ existe uma extensão. O segundo ponto é se a quantidade de places sobre um dado place em $P \in \mathbb{P}_F$. E finalmente o terceiro ponto é se dado um place Q em F' existe algum place P em F tal que $Q|P$. Vamos responder estes pontos ao longo dessa sessão.

Exemplo 2.3.2. *Seja K um corpo qualquer. Considere $F = K(x, y)$ com $y^3 = x$. Seja $P \in m\mathbb{P}_F$ o zero de y, então valorizando temos que $v_P(x) = 3v_P(x) > 0$ logo P também é zero de x. Se P_0 é zero de x em $K(x)$ temos que $v_P(x) = 3v_{P_0}(x)$.*

Como observaremos, o fenômeno que ocorre no exemplo anterior sempre é satisfeito.

Teorema 2.3.1. *Seja F'/K' uma extensão de algébrica de F/K. Considere $P \in \mathbb{P}_F$, $Q \in \mathbb{P}_{F'}$, $\mathcal{O}_F$ e $\mathcal{O}_{F'}$. São equivalentes as seguintes afirmações:*

a) $Q|P$;

b) $\mathcal{O}_P \subset \mathcal{O}_Q$

c) Existe $e \in \mathbb{Z}$ tal que $e \geqslant 1$ e $v_Q(z) = ev_P(z)$, $\forall z \in F$.

Demonstração. Exercício. □

Observamos que se $Q|P$ então pelo item c) do teorema anterior temos que $P = Q \cap F$ e $\mathcal{O}_P = \mathcal{O}_Q \cap F$. Desta forma, existe uma imersão de F_P em F_Q dada pela seguinte aplicação

$$\begin{aligned} \phi : \frac{\mathcal{O}_P}{P} &\longrightarrow \frac{\mathcal{O}_Q}{Q} \\ x + P &\longmapsto x + Q \end{aligned}$$

Então definimos o *grau relativo* $f(Q|P) := [F_Q : F_P]$ (que pode ser finito ou infinito.)

O inteiro do Teorema 2.3.1 e é chamado *índice de ramificação* de Q sobre P e é denotado por $e(Q|P) := e$. Quando $e(Q|P) > 1$ dizemos que $Q|P$ se *ramifica* e se $e(Q|P) = 1$ dizemos que $Q|P$ se *não se ramifica*.

Seja F'/K' uma extensão de algébrica de F/K. Se F_1/K_1 é uma extensão de algébrica de F'/K' e $Q_1 \in \mathbb{P}_{F_1}$ uma extensão de Q então

$$e(Q_1|P) = e(Q_1|Q)e(Q|P) \tag{2.16}$$

$$f(Q_1|P) = f(Q_1|Q)f(Q|P). \tag{2.17}$$

Com efeito, como $v_{P'}(x) = e(P'|P).v_P(x)$, para cada $x \in F$, e $v_{P_1}(z) = e(P_1|P')v_{P'}(z)$, para todo $z \in F'$, temos que $v_{P_1}(x) = e(P_1|P')e(P'|P)v_P(x)$, para todo $x \in F$, donde $e(P_1|P) = e(P_1|P')e(P'|P)$. A segunda igualdade segue de forma análoga.

Proposição 2.3.1. *Seja F'/K' uma extensão de algébrica de F/K. Considere $P \in \mathbb{P}_F$, $Q \in \mathbb{P}_{F'}$ com Q uma extensão de P. Então $f(Q|P) < \infty \Leftrightarrow [F' : F] < \infty$.*

Demonstração. Consideremos as inclusões $K \subset F_P \subset F'_{P'}$ e $K \subset K' \subset F'_{P'}$, donde $[F_P : K] < \infty$ e $[F'_{P'} : K'] < \infty$. Então, segue que $[F'_{P'} : F_P] < \infty \Leftrightarrow [K' : K] < \infty$. Dessa forma, $[F'_{P'} : F_P] < \infty \Leftrightarrow [F' : F] < \infty$. □

Os próximos lemas respondem dois dos três pontos mencionados acima e são deixados como exercício.

Lema 2.3.2. *Dado um place Q em $\mathbb{P}_{F'}$ existe exatamente um place $P \in \mathbb{P}_F$ tal que $Q|P$.*

Lema 2.3.3. *Seja F'/K' uma extensão de algébrica de F/K. Todo place P em $\mathbb{P}_F$ possui um número finito e não nulo de extensões em F'/K'.*

Lema 2.3.4. *Seja F'/K' uma extensão de algébrica de F/K e $z \in F'$ elemento transcendente sobre K. Então $[K'(z) : K(z)] = [K' : K]$.*

Teorema 2.3.2 (Equação Fundamental)**.** *Sejam F'/K' uma extensão de algébrica de F/K, $P \in \mathbb{P}_F$ e $Q_1, \ldots, Q_m$ places em F' tais que $Q_i|P$ para cada $i = 1, \ldots, m$. Então*

$$\sum_{i=1}^{m} e_i(Q_i|P) f_i(Q_i|P) = [F' : F]. \tag{2.18}$$

Demonstração. Tomando $x \in F$ tal que P seja o único zero de x em F/K. Seja $s = v_P(x) > 0$. Então pelo Lema 2.3.3 os places $Q_1, \ldots, Q_m \in \mathbb{P}_F$ são exatamente os zeros de x em F'/K' uma que $v_{Q_i} = e(Q_i|P)s > 0$. Calculando o grau de $F'/K(x)$ de duas formas diferentes obteremos o resultado desejado. Com efeito,

$$\begin{aligned}
[F' : K(x)] =& [F' : K'(x)][K'(x) : K(x)] \\
=& \left(\sum_{i=1}^{m} v_{Q_i}(x) Deg(Q_i) \right) [K' : K] \\
=& \left(\sum_{i=1}^{m} e_i v_P(x) [F'_{Q_i} : K'] . [K' : K] \right) \\
=& v_P(x) \left(\sum_{i=1}^{m} e_i [F'_{Q_i} : F_P][F_P : K] \right) \\
=& sDeg(P) \left(\sum_{i=1}^{m} e_i f_i \right).
\end{aligned}$$

Por outro lado $[F'K(x)] = [F' : F][F : K(x)] = [F' : F]sDeg(P)$, pois $\mathrm{div}(x)_0^F = sP$. □

Seja $G : X \to Y$ um morfismo não constante de curvas projetivas não singulares definidas sobre um corpo K. Então $K(Y)$ é visto como subcorpo de $K(X)$ e $n := [K(X) : K(Y)] < \infty$. O índice de ramificação é definido da seguinte forma: dado $p \in X$ e $q := f(p)$. Seja $t \in \mathcal{O}_q(Y)$ um parâmetro local do anel de valorização de q em $K(Y)$. Considere v_p a valorização discreta associada à p. O índice de ramificação é $e(p) := v_p(t)$.

Definição 2.3.3. *Sejam F'/K' uma extensão de algébrica de F/K com $[F' : F] < \infty$ e $P \in \mathbb{P}_F$.*

1. *P é* totalmente ramificado *em F'/F se existe um place $Q \in \mathbb{P}_{F'}$ com $Q|P$ e $e(Q|P) = [F' : F]$.*

2. *P se* decompõe completamente *em F'/F se existem exatamente m places distintos $Q \in \mathbb{P}_{F'}$ com Q sobre P.*

2.4 Extensões Especiais

Nesta seção vamos estudar dois tipos específicos de extensões de corpos de funções algébricos. São eles: extensões tipo Kummer e extensões tipo Artin–Schreier. Estes dois tipo de extensões são interessantes pois podemos explicitar o gênero utilizando novas formulas, além é claro de apresentarem muitas outras propriedades.

Definição 2.4.1. *Sejam F'/F uma extensão finita de corpos e $a \in F$. Considerando a transformação $F-$linear $T_a : F' \to F'$ definida por $T_a(x) = ax$, escrevemos o polinômio característico de T_a como $det(Ix - T_a) := f_a(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Então definimos a aplicação* Traço *e* Norma *como:*

1. $N_{F'/F}(a) = detT_a = (-1)^n f_a(0) = (-1)^n b_0$.
2. $Tr_{F'/F}(a) = -b_{n-1}$,

Se $\{a_1, \ldots, a_n\}$ é uma base de F'/F e

$$a * a_i = \sum_{j=1}^{n} a_{ij} a_j,$$

com $a_{ij} \in F$ Então podemos escrever

$$N_{F'/F}(a) = det(a_{ij}),$$
$$Tr_{F'/F}(a) = \sum_{j=1}^{n} a_{ii}.$$

Lema 2.4.1. *Seja F'/F uma extensão cíclica de grau n, com $G = Gal(F'/F) =< \alpha >$ ($\alpha \in F'$). Então*

a) $Tr_{F'/F}(a) = 0$ *se, e somente se, existe $b \in F'$ satisfazendo $a = b - \alpha(b)$.*

b) $N_{F'/F}(a) = 1$ *se, e somente se, existe $c \in F'$ satisfazendo $a = \frac{c}{\alpha(c)}$.*

Definição 2.4.2 (Extensão tipo Kummer)**.** *Seja F/K uma extensão algébrica de funções, onde K contém uma raiz $n-$ésima primitiva da unidade ($n > 1$ e coprimo com a característica de K). Suponha que exista um elemento $u \in F$ satisfazendo*

$$u \neq z^r \ para\ todo\ z \in F\ e\ r|n,\ r > 1. \tag{2.19}$$

Definimos a extensão de Kummer F'/F *como*

$$F' = F(w)\ com\ w^n = u. \tag{2.20}$$

Teorema 2.4.1. *Sejam* $\text{Char}(K) = p$ *e* $n \in \mathbb{N}$ *tais que* p *não divide* n. *Suponha que* K *contenha uma raiz primitiva da unidade* z_n. *Então a extensão* F'/F *é cíclica de grau* n *se, e somente se,* $z \in F'$ *tal que* $F' = F(z)$ *com polinômio* $\phi(t) = t^n - u$ *é o polinômio minimal de* z *sobre* F. *Neste caso,* F'/F *é uma extensão de Kummer.*

Demonstração. Suponha que F'/F é cíclica de grau n. Então $G = Gal(F'/F) = <\alpha>$ com $o(\alpha) = n$. Observamos que $N_{F'/F}(z_n) = z_n^n = 1$ e portanto pelo lema anterior temos que existe $z \in F'$ tal que $\alpha(z) = z_n z$. Uma vez que $\alpha^i(z) = z_n^i z$ temos que $\alpha^i(z) = z \Leftrightarrow n|i$. Desta forma $zz_n, \ldots, zz_n^{n-1}$ são conjugados distintos de z, assim o polinômio irredutível minimal de F é da forma $\phi(t) := \prod_{n-1}^{i=0}(t - z_n^i z)$.

Por outro lado, α satisfaz a seguinte propriedade $\alpha(z^n) = (\alpha(z))^n = (zz_n)^n = z^n$, isto é, $z^n = a \in F$. Portanto, como $z, zz_n, \ldots, zz_n^{n-1}$ são raízes de $t^n - a$ concluímos que $\phi(t) = t^n - a$.

Reciprocamente, se $\phi(t) = t^n - a$ é o polinômio minimal de z sobre F então $z, zz_n, \ldots, zz_n^{n-1}$ são raízes distintas de ϕ onde z é um elemento qualquer no fecho algébrico $\overline{F}$ de F. A verificação de F'/F é cíclica é imediata. □

O próximo resultado não será demonstrado aqui, o leitor interessado pode consultá-lo em (Stichtenoth 1993), (Villa Salvador 2006).

Corolário 2.4.1. *Seja* F'/F *uma extensão de Kummer, com* $F' = F(w)$ *com* $w^n = u$ *e* u *raiz* $n-$*ésima primitiva da unidade em* K. *Se* $\mathcal{K}$ *denota o corpo constante de* F', g' *o gênero de* F' *e* g *o gênero de* F *então*

$$g' = 1 + \frac{n}{[\mathcal{K} : K]}\left(g - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}_F}(1 - \frac{mdc(n, v_P(u))}{n})Deg(P)\right).$$

Um caso especial do teorema anterior é quando $K' = K$. Por exemplo, se assumirmos que existe um place $P \in \mathbb{P}_F$ tal que $mdc(n, v_P(u)) = 1$ então u satisfaz a condição 2.19 pois se $u = z^r$ para algum $r > 0$ temos que $v_P(u) = r v_P(w)$ e portanto $mdc(n, v_P(u)) \geqslant r > 1$, absurdo. Agora, seja $Q \in \mathbb{P}_{F'}$ uma extensão de P, pelo item c) do teorema anterior temos que $e(Q|P) = n = [F' : F]$. Suponhamos que $[K' : K] > 1$, considerando o corpo compósito $F_0 := FK'$ e o place $Q_0 := F_0 \cap Q$. Temos que $e(Q|Q_0) = [F' : F_0]$ e pelo teorema anterior temos $1 = e(Q|Q_0) = [F' : F_0] > 1$ contradição. Logo, $[K' : K] = 1$ e portanto $K' = K$.

Um importante fato das observações acima é a simplificação do calculo do gênero

$$g' = 1 + n\,(g-1) + \frac{1}{2}\left(\sum_{P\in\mathbb{P}_F}(n - r_P)Deg(P)\right). \tag{2.21}$$

Exemplo 2.4.1. *Seja $K = \mathbb{C}$. Considere $F = K(x,y)$ com $y^2 = (x+1)(x+2)(x+3)(x+13)(x+11)$. Então o gênero de F é 2. De fato, temos que $F = F_0(y)$ onde $F_0 := K(x)$. Vamos denotar $p_1 = (x+1)$ $p_2 = (x+2)$, $p_3 = (x+3)$, $p_4 = (x+13)$, $p_5 = (x+11)$, os zeros de p_i por $P_i \in \mathbb{P}_F$ e o polo de x por P_∞. Então temos que $v_{P_i}((x+1)(x+2)(x+3)(x+13)(x+11)) = 1$ e $v_{P_\infty}((x+1)(x+2)(x+3)(x+13)(x+11)) = -5$ Segue do comentário acima que K é o corpo constante de F e $[F : F_0] = 2$. Vemos que os números a_P para $P \in \mathbb{P}_F$ são:*

$$\begin{aligned} a_P &= 1 && se\ P = P_i,\ i = 1,\ldots,5 \\ a_P &= 2 && se\ P \neq P_i,\ i = 1,\ldots,5 \\ a_{P_\infty} &= 1 && pois\ 5 \equiv 1 mod\, 2. \end{aligned}$$

Portanto, utilizando a igualdade 2.21 temos que $g = 2$.

Exemplo 2.4.2. *Seja $K = \mathbb{C}$. Considere $F = K(x,y)$ com $y^2 = (x+21)(x+32)(x+53)(x+71)(x+99)(x+86)$. Então o gênero de F é 2. De fato, temos que $F = F_0(y)$ onde $F_0 := K(x)$. Vamos denotar $p_1 = (x+21)$ $p_2 = (x+32)$, $p_3 = (x+53)$, $p_4 = (x+71)$, $p_5 = (x+99)$, $p_6 = (x+86)$ os zeros de p_i por $P_i \in \mathbb{P}_F$ e o polo de x por P_∞. Então temos que $v_{P_i}((x+21)(x+32)(x+53)(x+71)(x+99)(x+86)) = 1$ e $v_{P_\infty}((x+21)(x+32)(x+53)(x+71)(x+99)(x+86)) = -6$ Segue do comentário acima que K é o corpo constante de F e $[F : F_0] = 2$. Vemos que os números a_P para $P \in \mathbb{P}_F$ são:*

$$\begin{aligned} a_P &= 1 && se\ P = P_i,\ i = 1,\ldots,6 \\ a_P &= 2 && se\ P \neq P_i,\ i = 1,\ldots,6 \\ a_{P_\infty} &= 2 && pois\ 6 \equiv 0 mod\, 2. \end{aligned}$$

Portanto, utilizando a igualdade 2.21 temos que $g = 3$.

Generalizando esses exemplos temos a seguinte proposição.

Proposição 2.4.1. *Considere K um corpo com* $\mathrm{Char}(K) \neq 2$. *Seja $F = K(x, y)$ onde*

$$y^2 = f(x) = p_1(x)p_2(x) \cdot \cdots \cdot p_r(x),$$

onde $p_1(x), p_2(x), \ldots, p_r(x) \in K[x]$ são polinômios mônicos, irredutíveis e distintos dois à dois. Se $deg(f) = d$ então

$$g(F) = \begin{cases} \frac{d-2}{2}, \ se\ 2|d \\ \frac{d-1}{2}, \ se\ 2 \nmid d. \end{cases}$$

Definição 2.4.3. *Seja F/K um corpo de funções algébricas de característica $p > 0$. Se existe um elemento $u \in F$ satisfazendo*

$$u \neq z^p - z, \ \forall z \in F, \tag{2.22}$$

então F'/F com $F' := F(y)$ onde $y^p - y = u$ é chamada de extensão Artin–Schreier *(ou para simplificar* tipo A.S. *).*

Com base na definição de extensões tipo AS, vamos estudar o sinal da valorização da função $u - (z^p - z)$.

Lema 2.4.2. *Seja F/K um corpo de funções algébricas de característica $p > 0$. Para um place $P \in \mathbb{P}_F$ e um elemento $u \in F$, temos que existe um elemento $z \in F$ tal que $v_P(u - (z^p - z)) \geqslant 0$, ou para algum $z \in F$ vale*

$$v_P(u - (z^p - z)) = -m < 0, \ com\ m \not\equiv mod\ p.$$

Neste ultimo caso, temos que

$$-m = max\{v_P(u - (z^p - z)) |\ z \in F\}.$$

Para um corpo de funções algébricas F/K de característica $p > 0$ e um place $P \in \mathbb{P}_F$, definimos

$$m_P := \begin{cases} -m, \ se\ existe\ um\ elemento\ z \in F\ tal\ que \\ v_P(u - (z^p - z) = -m < 0\ e\ m \not\equiv mod\ p, \\ -1, \ se\ v_P(u - (z^p - z) \geqslant 0\ para\ algum\ z \in F. \end{cases}$$

Observe que o lema anterior garante que m_P está bem definido. A seguir temos um resultado sobre extensões Tipo A.S., como os passos da demonstração são análogos ao do Teorema 2.4.1 deixamos como exercício.

O próximo resultado não será demonstrado aqui, o leitor interessado pode consultá-lo em (Stichtenoth 1993), (Childress 2009).

Teorema 2.4.2. *Sejam* $\mathrm{Char}(K) = p > 0$ *e* F/K *um corpo de funções. Então* F'/F *é uma extensão cíclica de grau* p *se, e somente se, existe um elemento* z *em* F' *tal que* $F' = F(z)$ *com polinômio minimal* $\psi(t) = t^p - t - a \in F[t]$.

Corolário 2.4.2. *Sejam* F'/F *uma extensão Artin–Schreier de característica* $p > 0$ *e* $u \in F$ *o elemento satisfazendo a Definição 2.4.3. Denote* g' *o gênero de* F' *e* g *o gênero de* F. *Se existe pelo menos um place* $P' \in \mathbb{P}_F$ *com* $m_{P'} > 0$ *então*

$$g' = gp - \frac{p-1}{2}\left(2 - \sum_{P \in \mathbb{P}_F} (m_P + 1) Deg(P)\right).$$

Proposição 2.4.2. *Sejam* F/K *uma extensão de corpos com* $\mathrm{Char}(K) = p > 0$ *e* $a(t) \in K[t]$ *um polinômio aditivo e separável com grau* p^n *e todas as raízes em* K. *Dado* $u \in F$ *o elemento suponha que para cada* $P \in \mathbb{P}_F$ *existe um elemento* $z \in F$ *satisfazendo*

$$v_P(u - a(z)) \geqslant 0$$
$$ou\, v_P(u - a(z)) = -m, com\ m > 0\ e\ p \nmid m.$$

então se F'/F *com* $F' := F(y)$ *onde* $a(y) = u$ *possui um place* $P \in \mathbb{P}_F$ *com* $m_P > 0$ *as afirmação abaixo são verdadeiras:*

a) A extensão F'/F *é uma extensão Galois de grau* p^n.

b) K *é algebricamente fechado em* F'.

c) $P \in \mathbb{P}_F$ *não ramifica em* $F'/F \Leftrightarrow m_P = -1$.

d) $P \in \mathbb{P}_F$ *é totalmente ramificado* $\Leftrightarrow m_P > 0$. *Neste caso, se* $Q \in \mathbb{P}_{F'}$ *é a única extensão de* P *em* F'/F *temos que*

$$d(Q|P) = (p^n - 1)(m_p + 1).$$

d) Denote g' o gênero de F' e g o gênero de F. Se existe pelo menos um place $P' \in \mathbb{P}_F$ com $m_{P'} > 0$ então

$$g' = gp^n - \frac{p^n - 1}{2}\left(2 - \sum_{P \in \mathbb{P}_F} (m_P + 1) Deg(P)\right).$$

Exemplo 2.4.3. *Considere a extensão de Kummer $F/\mathbb{F}_q(x)$ dada por*

$$y^m = \prod_{i=1}^{r} (x - a_i)^s,$$

com $mdc\{m, sr\} = 1$ e $a_i \in \mathbb{F}_q$ então podemos exibir divisores importantes:

1. $\operatorname{div}(x - a_i) = m(P_i - P_\infty)$.
2. $\operatorname{div}(y) = \sum_{i=1}^{r} sP_i - rsP_\infty$.
3. $\operatorname{div}(\prod_{i=1}^{r}(x - a_i)) = \sum_{i=1}^{r} mP_i - rmP_\infty$.
4. $\operatorname{div}(z) = \sum_{i=1}^{r} P_i - rP_\infty$, *onde* $z = y^a(\prod_{i=1}^{r}(x - a_i))^b$ *com* $as + bm = 1$.

Sobre este tipo de extensão temos que o semigrupo de Weierstrass no ponto no infinito P_∞(se este é racional) é $H(P_\infty) =< m, r >$. Ainda, se considerarmos que P_1 também é racional temos que

$$H(P_1) = \mathbb{N} \setminus \left\{ mk + j \,|\, 1 \leqslant j \leqslant m - 1 - \lfloor \frac{m}{r} \rfloor,\ 0 \leqslant k \leqslant r - 2 - \lfloor \frac{rj}{m} \rfloor \right\}.$$

Para mais detalhes, ver (Shudi e Hu 2016).

3 Códigos Algébricos

Neste capítulo veremos a definição de códigos algébricos bem como seus principais elementos. Uma família de códigos interessante que iremos abordar é dada por códigos que possuem uma estrutura de subespaço vetorial. Veremos algumas propriedades destes códigos e ainda uma ideia inicial de codificar e decodificar uma informação recebida.

Este capitulo além de abordar conceitos gerais de códigos algébricos, serve como base aos estudos do próximo capitulo, onde estudaremos outra família de códigos, a saber, códigos geométricos.

3.1 Códigos

Ao longo da história da humanidade, os seres humanos se comunicaram através da transmissão de códigos (ou mensagens), sejam eles por meio de sinais, sons ou caracteres. Na atualidade, vivemos num universo onde a transmissão é feita por meio digital e, onde requer que esta transmissão seja cada vez mais rápida e assertiva. Nós deparamos que essa transmissão de códigos cotidianamente, por exemplo, ao trocar mensagens pelo celular, ou a simples leitura de um código de barras.

Portanto, obter um processo de codificação e decodificação que seja preciso

e "rápido" se torna necessário para que todas estas coisas fluam de maneira eficiente.

Inicialmente consideramos um conjunto finito de objetos A, este conjunto chamaremos de *alfabeto* e sua cardinalidade de $q = \#(A) > 1$. Dado um natural n definimos $A^n := A \times \cdots \times A$, os elementos de A^n são chamados de *palavras*.

Exemplo 3.1.1. *Considere o alfabeto* $A := \{A, B, F, R, E, I, G, T\}$. *Então*

$$C_0 := \{AAAA, BABA, ARAR, TATA\}$$
$$C_1 := \{AAAA, GGGG, RRRR, IIII, RRRR\}$$

são códigos e C_1 *é chamado de* código de repetição.

Exemplo 3.1.2. *Considere o Alfabeto* $A = \mathbb{Z}_2 = \{0, 1\}$. *Se* $n = 2$ *então* $\{(0,0), (1,1), (1,0), (0,1)\}$ *são todas as palavras de* A^2

Dada duas palavras $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots b_n)$ em A^n definimos sua distância $d(a, b)$ como

$$d(a, b) = \#\{i \mid b_i \neq a_i\}.$$

$d(a, b)$ é chamado de *distância de Hamming* (ou *métrica de Hamming*).

Exemplo 3.1.3. *Considere o alfabeto* $A = \mathbb{F}_2 = \{0, 1\}$. *Em* A^4 *tomemos os elementos* $u_1 = (1, 1, 1, 1)$, $u_2 = (1, 0, 1, 0)$, $u_3 = (0, 0, 0, 1)$ *e* $u_4 = (0, 0, 0, 0)$. *Então*

$$d(u_1, u_2) = 2$$
$$d(u_3, u_2) = 3$$
$$d(u_3, u_0) = 1$$
$$d(u_1, u_4) = 4$$

Observação 3.1.1. *O leitor familiarizado com as noções de métricas pode conferir que de fato* $d(-,-)$ *é uma métrica, isto é,* $d(-,-)$ *satisfaz para cada* $a, b, c \in A^n$*:*

- $d(a, b) \geqslant 0$ *e* $d(a, b) = 0 \Leftrightarrow a = b$.
- $d(a, b) = d(b, a)$.

- $d(a,b) \geqslant d(a,c) + d(c,b)$.

Este fatos permitem portanto definir uma topologia em A^n, isto é,podemos definir as noções de bolas e esferas.

Definição 3.1.1. *Qualquer conjunto C com $\emptyset \neq C \subset A^n$ é chamado de* $q-$ário código *de comprimento n. Os elementos de C são chamados de* palavras código *(ou* vetores código*).*

Como A é um conjunto finito, temos que C também será. Denotando $c := \#(C) \in \mathbb{N}$ definimos a cardinalidade logarítmica por $k := log_q(c) \in \mathbb{R}$.

Utilizando a distância de Hamming podemos definir uma nova distância. Considere um $q-$código de comprimento n então

$$d = d(C) := min\{d(a,b) |\, a,b \in C \text{ e } a \neq b\}$$

é chamada de *distância mínima* do código C, ou simplesmente distância mínima. Um código com esses parâmetros é chamado de $[n,k,d]-$*código*.

Exemplo 3.1.4. *Considere o código*

$$C = \{x = (0,0,1), y = (0,1,0), z = (0,1,1), o = (0,0,0)\},$$

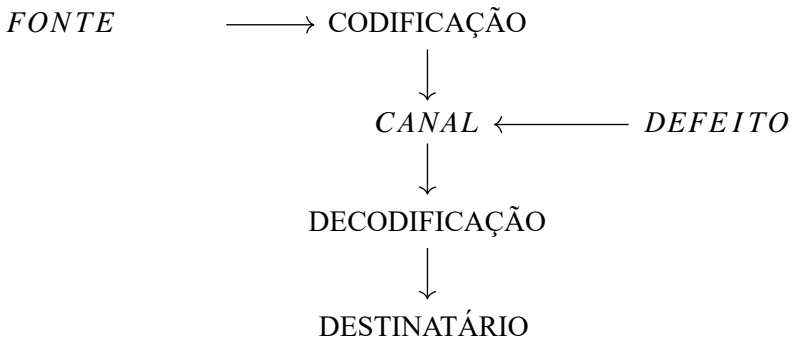
sobre $\mathbb{F}_2$. Então vamos calcular todas as distância entre os elementos de C.

$$\begin{aligned} d(x,y) &= 2 \\ d(x,z) &= 1 \\ d(x,o) &= 1 \\ d(z,y) &= 1 \\ d(o,y) &= 1 \\ d(o,z) &= 2 \end{aligned}$$

Portanto $d(C) = 1$. Em outras palavras C é um $[3,2,1]-$código.

Com os parâmetros q,k e d podemos definir novos parâmetros: $R := \frac{k}{n}$ e $\delta := \frac{d}{n}$

Abaixo apresentamos um diagrama simples que exemplifica o sistema de codificação (este sistema foi descrito por Shannon)



O sistema de codificação de uma mensagem entre um emissor e um destinatário pode apresentar erros entre o processo de codificação e decodificação. A ideia central de códigos corretores de erros é deixar a mensagem final o mais próximo possível da mensagem inicial.

Para exemplificar, podemos tomar como exemplo a língua portuguesa. Se olharmos o palavra *amtemática* recebida por algum tipo de mensagem, logo perceberemos que esta palavra não existe em nosso vocabulário. Concluímos rapidamente que houve algum erro de digitação, basicamente é este processo que os corretores de textos fazem, eles comparam cada palavra que está sendo digitada com as palavras pré-gravadas em seu sistema e exibem aquelas que estão mais "próximas" da palavra desejada. Portanto, voltando à *amtemática* percebemos que a palavra mais próxima é *matemática*. Porém nem sempre é possível exibir uma única palavra: considere a palavra *qola* as palavras $bola$, $cola$ e $mola$ estão igualmente próximas.

A luz do comentário acima podemos nos perguntar o que seria um código "ótimo"? Um código é ótimo quando n é "grande" e R, δ são os maiores possíveis. Este termo vem da Teoria da Informação.

Agora vamos tratar da relação de detecção e correção de um dado código C. Considere que recebemos uma mensagem (ou um elemento) z. Podemos detectar se esta esta mensagem possui algum tipo de erro, ou não, se um método para verificar se $z \in C$. Se o erro não existir o processo de correção não se aplicará, mas caso seja detectado um erro o processo de correção irá substituir a elemento z por um elemento $w \in C$ que esteja o mais próximo possível de z. Então fica claro, pelo comentário acima, que é necessário que exista nenhum tipo de ambiguidade para determinar w. O processo em que a mensagem (ou palavra) recebida, eventualmente com erros, e retorna uma mensagem (ou palavra) corrigida é chamado de *decodificação*.

Seja t um número inteiro positivo. Um código C $detecta-t-erro$ se, sempre que uma palavra código v contém pelo menos um e no máximo t erros, a palavra v portanto não é uma palavra código. Um código C é $detecta-u-erro$ se detecta t erros, porém não detecta erros acima de $t+1$.

A prova dos dois próximos resultados são deixados como exercícios para o leitor.

Teorema 3.1.1. *Seja C um código com distância mínima $d = d(C)$ e seja*

$$k := \lfloor \frac{d-1}{2} \rfloor.$$

Então podemos detectar até $d-1$ erros e corrigir até k erros.

Corolário 3.1.1. *Seja código C com distância mínima $d = d(C)$. Então C pode corrigir até k erros se e somente se $d \geqslant 2k+1$.*

O valor $k = \lfloor \frac{d-1}{2} \rfloor$ é chamado de *capacidade de correção* de C

3.2 Códigos Lineares

Nesta seção iremos sempre considerar o alfabeto sendo um corpo finito $\mathbb{F} = \mathbb{F}_q$ onde $q = p^n$ e p um número primo. Nesta seção vamos definir a noção de códigos lineares e algumas de suas propriedades.

Definição 3.2.1. *Seja $\mathbb{F}_q$ o alfabeto com $q = p^n$. Um código C de comprimento n é dito* código $\mathbb{F}_q-$linear *(ou simplesmente código linear) se $C \subset \mathbb{F}_q^n$ é um $\mathbb{F}_q-$subespaço linear.*

Ao longo desta seção um código C sempre denotará um código linear.

Dados dois códigos C e C' de mesmo comprimento sobre $\mathbb{F}_q$. Então é imediato mostrar que os conjuntos $C \cup C'$ e $C \cap C'$ também são códigos sobre $\mathbb{F}_q$.

Dado um código $\mathbb{F}-$linear C seus elementos podem ser vistos como vetores e $\mathbf{v}$ e portanto contém a origem $\mathbf{0}$. Este fato torna uma vantagem a utilização de códigos lineares uma vez que podemos calcular a distância mínima de uma segunda forma. Para isso, introduzimos um novo objeto.

Definição 3.2.2. *Sejam C um código $\mathbb{F}-$linear e $z \in C$. O* peso *de z é definido como*

$$wt(z) := d(z, \mathbf{0}).$$

O número

$$wt(C) := min\{wt(z) |\ z \in C,\ z \neq \mathbf{0}\}.$$

é chamado de peso *do código* C.

A seguir destacamos uma propriedade interessante do peso de palavras sobre um corpo de dois elementos.

Exemplo 3.2.1. *Sejam* $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n$. *Se o peso de* $\boldsymbol{u}$ *e* $\boldsymbol{v}$ *tem mesma paridade, então* $\boldsymbol{u} + \boldsymbol{v}$ *deve ter o mesmo peso.*

Para códigos lineares concluímos que a distância mínima é dada por $d(C) = wt(C)$. De fato, para $\mathbf{x}, \mathbf{y} \in C$ temos que $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$. Sejam $\mathbf{u}, \mathbf{v}, \mathbf{w} \in C$ tais que $d(\mathbf{u}, \mathbf{v}) = d(C)$ e $wt(C) = wt(\mathbf{w})$. Então por um lado temos que $d(C) = d(\mathbf{u}, \mathbf{v}) = wt(\mathbf{u} - \mathbf{v}) \geqslant wt(C)$. Por outro lado, $wt(C) = wt(\mathbf{w}) = d(\mathbf{w}, \mathbf{0}) \geqslant d(C)$. Portanto, $d(C) = wt(C)$.

A distância de Haminng pode ser obtida através da definição de peso de um vetor.

Lema 3.2.1. *Para cada* $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q$ *temos que* $d(\boldsymbol{x}, \boldsymbol{y}) = wt(\boldsymbol{x} - \boldsymbol{y})$.

Demonstração. Sabemos que $d(\mathbf{x}, \mathbf{y}) = 0 \Leftrightarrow \mathbf{x} = \mathbf{y}$, que é equivalente à $w(\mathbf{x} - \mathbf{y}) = 0$. Vamos supor que $\mathbf{x} \neq \mathbf{y}$. $wt(\mathbf{x} - \mathbf{y}) = d(\mathbf{x} - \mathbf{y}, 0) = d(\mathbf{x}, \mathbf{y})$ □

Destacamos que $\mathbb{F}_q$ tem característica 2, então $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} + \mathbf{y})$.

Dados dois códigos C e C' sobre $\mathbb{F}_q$ de mesmo comprimento, podemos definir o conjunto

$$C + C' := \{\mathbf{u} + \mathbf{v} |\ \mathbf{u} \in C,\ \mathbf{v} \in C'\}.$$

O próximo resultado segue diretamente de propriedades de álgebra linear e deixamos a demonstração como exercício ao leitor.

Lema 3.2.2. *Sejam* C *e* C' *códigos sobre* $\mathbb{F}_q$. *Então* $C + C'$ *é um código linear sobre* $\mathbb{F}_q$

Observamos que em $\mathbb{F}_q^n$ podemos definir um *produto interno* da seguinte forma

$$< \mathbf{z}, \mathbf{w} >:= \sum_{i=1}^{n} z_i w_i,$$

para cada $\mathbf{z}, \mathbf{w} \in \mathbb{F}_q^n$

Definição 3.2.3. *Seja $C \subset \mathbb{F}_q^n$ um código linear. Então*

$$C^{\perp} := \{w \in \mathbb{F}_q^n | \ < w, z >= 0, \ \forall z \in C\}$$

é um código linear e é chamado de código dual *de C. Dizemos que C é* auto dual *se $C = C^{\perp}$.*

Destacamos que se C e C' são dois códigos sobre $\mathbb{F}_q$ de mesmo comprimento, onde $C \subset C'$ então o dual inverte as inclusões, isto é, $(C')^{\perp} \subset C^{\perp}$. Com efeito, seja $\mathbf{u} \in (C')^{\perp}$, então $< \mathbf{u}, \mathbf{x} >= 0$ para cada $\mathbf{x} \in C'$, em particular para $\mathbf{x} \in C$. Portanto, $< \mathbf{u}, \mathbf{x} >= 0$ para todo $\mathbf{x} \in C$, com isso concluirmos a demonstração.

Lema 3.2.3. *Sejam C e C' códigos sobre $\mathbb{F}_q$. Então o dual de $C + C'$ é $C^{\perp} \cap (C')^{\perp}$.*

Demonstração. Exercício. □

Considere C um código com distância mínima d, dimensão k e comprimento n, como anteriormente dizemos que C é um $[n, k, d]-$código. Tomando uma base qualquer de C podemos construir uma aplicação injetiva e linear $\Delta : \mathbb{F}_q^k \to \mathbb{F}_q^n$ enviando os elementos da base de $\mathbb{F}_q^k$ em elementos da base de C . A matriz G associada a este mergulho é chamada de *matriz geradora* e satisfaz a seguinte sequencia exata

$$0 \longrightarrow \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-k} \longrightarrow 0$$

em outras palavras $\Theta : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ é uma aplicação sobrejetora onde $\mathrm{Im}(\Delta) = \mathrm{Ker}(\Theta)$. A matriz H associada à aplicação Θ é chamada de *matriz de verificação*. Como Δ é injetiva temos a seguinte relação $C = \mathrm{Im}(\Delta) = \mathrm{Ker}(\Theta)$ e $\Theta(\mathbf{z}) = 0$ para cada $\mathbf{z} \in C$.

Para encontrar a matriz G procedemos da seguinte forma: tomamos a base canônica $\{\mathbf{e}_i\}_{i=1}^n$ de $\mathbb{F}_q^n$ e uma base $\{\mathbf{v}_i\}_{i=1}^k$ de C então a solução do sistema $\mathbf{v}_i = \sum_{j=1}^{n} a_{ij}\mathbf{e}_j$ define a matriz G, isto é, $G = [a_{ij}]$.

Observação 3.2.1. *Observamos que a matriz geradora associada a um código C com base $\{v_i\}_{i=1}^k$ é formada por pela base de C, onde cada linha é representada por v_i. Desta forma, a matriz geradora não é única, pois depende da base escolhida.*

Exemplo 3.2.2. *Considere o código*

$$C = \{(0,0,0,0), (1,0,0,0), (0,1,0,0), (1,1,0,0)\}$$

sobre $\mathbb{F}_2$. *Então* $(1,0,0,0), (0,1,0,0)$ *é uma base para* C *e portanto a matriz geradora de* C *com essa base é dada por:*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

A seguir apresentamos dois resultados que relacionam o código dual com a matriz geradora e matriz de verificação de um código.

Lema 3.2.4. *Seja* $C \subset \mathbb{F}_q^n$ *um código de dimensão* k *e matriz geradora* G. *Então*

a) $C^\perp$ *é um código.*

b) $C^\perp = \{z \in \mathbb{F}_q^n \mid Gz^t = \mathbf{0}\}$.

c) $C^\perp$ *tem dimensão* $n - k$.

Demonstração. a) Segue imediatamente das propriedades de produto vetorial.

b) Sejam $\mathbf{u}_1, \ldots, \mathbf{u}_k$ as linhas da matriz G. Então para cada $\mathbf{x}$ temos que $G\ \mathbf{x}^t = (< \mathbf{v}_1, \mathbf{x} >, \ldots, < v_k, \mathbf{x} >)$. Portanto, $\mathbf{x} \in C^\perp \Leftrightarrow (< v_1, \mathbf{x} >, \ldots, < \mathbf{v}_k, \mathbf{x} >) = 0$.

c) Considere a aplicação tal que $\phi(\mathbf{x}) = G\mathbf{x}^t$. Note que $C^\perp = ker(\phi)$ tem dimensão k. Usando o Teorema do Núcleo e Imagem o resultado segue.

□

Do lema anterior se $C \subset \mathbb{F}_q^n$ então

$$\dim(C) + \dim(C^\perp) = n \tag{3.1}$$

Exemplo 3.2.3. *Considere o código* $C := \{(0,0,0), (1,0,0), (0,1,0), (1,1,0)\}$ *sobre* $\mathbb{F}_2$ *então* $C^\perp = \{(0,0,0), (0,0,1)\}$.

A demonstração do próximo resultado é deixado como exercício.

Lema 3.2.5. *As seguintes afirmações são verdadeiras:*

a) toda palavra-código em um código sobre $\mathbb{F}_2$ auto-dual tem peso par.

b) Sejam $\boldsymbol{u}, \boldsymbol{v}$ palavras-código em um código binário auto-dual. Suponha que os pesos de $\boldsymbol{v}$ e $\boldsymbol{u}$ sejam divisíveis por 4. Então o peso de $\boldsymbol{u} + \boldsymbol{v}$ também é um múltiplo de 4.

Segue de (3.1) que todo código auto-dual de comprimento n tem dimensão $\frac{n}{2}$.

Corolário 3.2.1. *Sejam $C \subset \mathbb{F}_q^n$ um código de dimensão k e M matriz geradora de $C^\perp$. Então*

a) $C = (C^\perp)^\perp$.

b) $C^\perp = \{\boldsymbol{z} \in \mathbb{F}_q^n \mid M\boldsymbol{z}^t = \boldsymbol{0}\}$.

Demonstração. a) Claramente $C \subset (C^\perp)^\perp$ e pelo resultado anterior ambos tem mesma dimensão, portanto são iguais.

b) Segue de maneira análoga aprova do item b) do resultado anterior.

□

A seguir veremos como a matriz de verificação H de um código C carrega informações sobre o peso $wt(C)$. Enunciamos dois próximos resultados, sem demonstração.

Lema 3.2.6. *Seja H a matriz de verificação do código C. Se existe $\boldsymbol{z} \in C$ tal que $wt(\boldsymbol{v}) = r$ então existem r colunas de H que são linearmente dependentes.*

Corolário 3.2.2. *O peso de um código C é igual à s se, e somente se, quaisquer $s-1$ colunas da matriz H de verificação de C são $l.i.$ e existem s colunas $l.d.$.*

No próximo resultado vamos utilizar a matriz geradora de um código C dado para obter sua matriz de verificação. Vamos denotar a matriz identidade $m \times m$ por I_m.

Teorema 3.2.1. *Seja C um $[n,k]-$código com matriz geradora $G = (I_k|X)$ no formato padrão. Então a matriz de verificação é dada por $H = (-G^t|I_{n-k})$*

Demonstração. Sabemos que $HG^t = 0$ é satisfeita. Considerando as $n-k$ ultimas linhas de H, podemos mostrar facilmente que são linearmente independentes. Do Corolário 3.2.1 concluímos o resultado. □

Pela definição de distância mínima e pelo corolário anterior podemos escrever $d(C)$ como

$$d(C) = min\left\{s \in \mathbb{Z}^+ | \exists\ s \text{ colunas linearmente independentes em} H\right\}$$

onde H é a matriz de verificação de C. Com esta informação podemos provar o próximo resultado, conhecido como *Cota de Singleton*.

Lema 3.2.7. *Para qualquer código $\mathbb{F}_q^n$−linear de comprimento n, dimensão k e distância mínima d vale*

$$d - 1 \leqslant n - k \tag{3.2}$$

Demonstração. Seja H a matriz de verificação do um código C. Como $wt(C) = d(C) = d$ então qualquer $d-1$ colunas de H são $l.i.$, sendo $n-k$ o posto de H o resultado segue. □

Definição 3.2.4. *Um código $\mathbb{F}_q^n$−linear de comprimento n, dimensão k e distância mínima d é dito* MDS *(em inglês: maximum distance separable) se $d = n-k+1$.*

Questão: Existem códigos MDS?

A resposta é verdadeira. No exemplo a seguir vamos construir um código MDS e isto irá motivar nossos estudos na próxima seção.

Exemplo 3.2.4. *Considere n, k, q, d números inteiros onde $1 \leqslant k \leqslant n \leqslant q$ e q é potência de primo. Sejam $\mathbb{F} = \mathbb{F}_q$ e $\mathbb{F}[x]$ o anel de polinômios de uma variável sobre $\mathbb{F}$. Definimos o conjunto*

$$L := \{p(x) \in \mathbb{F}[x] \mid deg(p(x)) \leqslant k-1\} \cup \{0\}.$$

Tomando n pontos distintos $a_1, \ldots, a_n \in \mathbb{F}$ definimos a aplicação $\eta : L \to \mathbb{F}^n$ por $\eta(p(x)) = (p(a_1), \ldots, p(a_n))$ (um mapa definido como η é chamado aplicação! de avaliação*). É imediato a verificação de η é uma aplicação linear bem definida e injetora. Definindo $C = \mathrm{Im}(\eta)$ vemos que C é um código linear. Se $\boldsymbol{x} \in C$ com $\boldsymbol{x} = (p(a_1), \ldots, p(a_n))$ temos que $p(\boldsymbol{x})$ possui $n - wt(\boldsymbol{x})$ zeros e portanto $n - w \leqslant k - 1$, isto é, $n - d(C) \leqslant k - 1$. Segue da cota de Singleton que $n - d(C) = k - 1$. Portanto, C é MDS.*

Definição 3.2.5. *Um código $C' \subset \mathbb{F}_q^n$ é equivalente à outro código $C \subset \mathbb{F}_q^n$ se C' pode ser obtido de C por uma combinação de operações dos seguintes tipos:*

1. *multiplicação dos símbolos que aparecem em uma posição fixa por um escalar diferente de zero*

2. *permutação dos n posições de palavras-código.*

Do primeiro item da definição acima podemos escrever

$$C' = \{(\lambda_1 c_1, \ldots, \lambda_n c_n) | (c_1, \ldots, c_n \in C\} \\ e\ \lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}^n.$$

Uma propriedade interessante sobre códigos equivalentes é que estes possuem mesma dimensão e distância mínima. Portanto, da perspectiva de calcular estes parâmetros basta conhecer tais informações de um código equivalente que seja mais simples o calculo ou que já seja conhecido. Vamos destacar estes fatos enunciando o próximo resultado.

Proposição 3.2.1. *Sejam C e C' dois códigos sobre $\mathbb{F}_q$. Se C e C' são equivalentes então* $\dim(C) = \dim(C')$ *e* $d(C) = d(C')$.

Exemplo 3.2.5. *Tomando $q = 2$ e $n = 3$, o código*

$$C' := \{(0,0,0); (1,0,1); (1,0,0)\}$$

é equivalente a $C := \{(0,0,0); (0,0,1); (0,1,0)\}$ por uma permutação dos elementos de C.

3.3 Codificando e Decodificando

Nesta seção vamos considerar um $[n,k,d]-$código linear C sobre um corpo $\mathbb{F} = \mathbb{F}_q$. Como C possui dimensão k, então cada um de seus elementos podem ser representados através desta base e os valores de $\mathbb{F}$, logo C contem q^k informações distintas, ie, C possui q^k palavras código. Escolhendo uma base $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ para C sobre $\mathbb{F}$ temos que $\mathbf{u} \in C$ então existem $\lambda_1, \ldots, \lambda_k \in \mathbb{F}$ tais que

$$\mathbf{u} = \lambda_1 \mathbf{v}_1 + \cdots + \lambda_k \mathbf{v}_k.$$

Vimos ainda que C está associado a uma matriz geradora M. Dado $\mathbf{v}' = (a_1, \ldots, a_k) \in \mathbb{F}^k$ temos que $\mathbf{v}'M = a_1\mathbf{v}_1 + \cdots + a_k\mathbf{v}_k \in C$. Em outras palavras, cada elemento de C é da forma uM, para algum $\mathbf{u} \in \mathbb{F}^k$ e para cada $\mathbf{v}' \in \mathbb{F}^k$ temos que $\mathbf{v}'M \in C$

Definição 3.3.1. *Seja C um $[n, k, d]-$código com matriz geradora M. Para cada $\boldsymbol{v} \in \mathbb{F}^k$ o processo $M\boldsymbol{v}^t$ é chamado de* codificação de **v** em C*, ou simplesmente* codificação.

Exemplo 3.3.1. *Seja C um código sobre $\mathbb{F}_3$ cuja matriz geradora é dada por*

$$H := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 2 & 1 \end{pmatrix}$$

Agora considere a mensagem $\boldsymbol{u} = (1, 0, 2, 0)$, então codificando obtemos

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 2 & 1 \end{pmatrix} (1, 0, 2, 0)^t = (0, 1, 2, 2).$$

Sobre o processo de codificar uma palavra vimos que depende da escolha da base do código C. Portanto, a escolha da base incorre na dificuldade de recuperar a palavra codificada. No caso em que a matriz geradora está no formato padrão, teremos que é trivial recuperar a palavra (ou mensagem) que foi codificada.

Exemplo 3.3.2. *Seja C um código sobre $\mathbb{F}_2$ cuja matriz geradora é dada por*

$$H := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Agora considere a mensagem $\boldsymbol{u} = (1011) + (1001)$, então codificando obtemos

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} [(1, 0, 1, 1) + (1, 0, 0, 1)]^t =$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} (1, 0, 1, 1)^t + \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} (1, 0, 0, 1)^t =$$

$$(1, 1, 0) + (0, 1, 1).$$

Uma vez que a mensagem foi codificada temos que ser capazes de recuperar a mensagem que foi envida, este processo é chamado de *Decodificação*. Portanto, um sistema de codificação tem uso pratico se podemos recuperar a mensagem de forma eficiente. Vamos ver um processo bem simples de decodificação.

Dado um $[n, k, d]-$código C sobre $\mathbb{F}_q$. Para cada $\mathbf{u} \in \mathbb{F}_q^n$ podemos definir o conjunto

$$C + \mathbf{u} = \{\mathbf{x} + \mathbf{u} | \ \mathbf{x} \in C\}.$$

O conjunto $C + \mathbf{u}$ é chamado *coset*. Observamos que $C + \mathbf{u} = \mathbf{u} + C$.

Exemplo 3.3.3. *Seja* $\mathbb{F}_2$ *e* $C = \{(0,0); (0,1)\}$ *então podemos calcular alguns cosets:*

1. $C + (0,0) = \{(0,0); (0,1)\}$
2. $C + (0,1) = \{(0,1); (0,0)\}$
3. $C + (1,1) = \{(1,1); (1,0)\}$

Dentro de um coset, o vetor com o menor peso é chamado de **vetor líder**. É importante notar que nem sempre um coset terá um único vetor líder.

Exemplo 3.3.4. *Seja* $\mathbb{F}_3$ *e*

$$C = \{(0,0,0); (0,1,0); (1,2,0); (0,2,0); (1,0,0); (2,0,0); (1,1,0); (2,2,0); (2,1,0)\}$$

vamos calcular alguns cosets e vetores lideres.

1. $C+(0,0,0) = \{(0,0,0); (0,1,0); (1,2,0); (0,2,0); (1,0,0); (2,0,0); (1,1,0); (2,2,0); (2,1,0)\}$.
2. $C+(1,0,0) = \{(1,0,0); (1,1,0); (2,2,0); (1,2,0); (2,0,0); (0,0,0); (2,1,0); (0,2,0); (0,1,0)\}$.
3. $C+(1,1,0) = \{(1,1,0); (1,2,0); (2,0,0); (1,0,0); (1,0,0); (0,1,0); (2,2,0); (0,0,0); (0,2,0)\}$.
4. $C+(0,0,2) = \{(0,0,2); (0,1,2); (1,2,2); (0,2,2); (1,0,2); (2,0,2); (1,1,2); (2,2,2); (2,1,2)\}$.

Então em cada caso temos os vetores lideres:

1. $(0,0,0)$,

2. $(0, 0, 0)$,

3. $(0, 0, 0)$,

4. $(0, 0, 2)$.

Nos exemplos anteriores vemos características interessantes sobre cosets. O Exemplo sugere que um coset $C + \mathbf{u}$ tem mesma cardinalidade que C.

Sobre os cosets temos o seguinte resultado.

Proposição 3.3.1. *Seja C $[n, k, d]$−código sobre $\mathbb{F}_q$.*

a) Todo $\boldsymbol{v} \in \mathbb{F}_q^n$ então contido em algum coset de C.

b) $\#(C) = \#(C + \boldsymbol{v})$, para $\boldsymbol{v} \in \mathbb{F}_q^n$.

c) Para $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_q^n$, temos que $C + \boldsymbol{u} = C + \boldsymbol{v}$ sempre que $\boldsymbol{v} \in C + \boldsymbol{u}$.

d) Para $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_q^n$, temos que $C + \boldsymbol{u} = C + \boldsymbol{v}$ ou $C + \boldsymbol{u} \cap C + \boldsymbol{v} = \emptyset$

e) Para $\boldsymbol{u}, \boldsymbol{v}, w \in \mathbb{F}_q^n$, $\boldsymbol{u} - \boldsymbol{v} \in C \Leftrightarrow \boldsymbol{u}, \boldsymbol{v} \in C + \boldsymbol{w}$.

Demonstração. a) Segue do fato de que C é subespaço.

b) Para verificar este item, basta notar que $\mathbf{x} + \mathbf{u} = \mathbf{y} + \mathbf{u}$ em $C + \mathbf{u}$, então $\mathbf{x} = \mathbf{y}$.

c) Se $\mathbf{v} \in C + \mathbf{u}$ então $C + \mathbf{v} \subset C + \mathbf{u}$, como ambos tem mesma cardinalidade (item anterior) o item segue.

d) Se $C + \mathbf{u} \cap C + \mathbf{v} = \emptyset$ então não há o que fazer. Se $C + \mathbf{u} \cap C + \mathbf{v} \neq \emptyset$ então existe $\mathbf{x} \in C + \mathbf{u} \cap C + \mathbf{v}$. Pelo item anterior segue a igualdade.

e) Se $\mathbf{u} - \mathbf{v} \in C$ então $\mathbf{u} = \mathbf{v} + \mathbf{x} \in C + \mathbf{v}$, com $\mathbf{x} \in C$. Segue do item c) a igualdade. Por outro lado, se $\mathbf{u}, \mathbf{v} \in C + \mathbf{w}$ então temos que $\mathbf{v} - \mathbf{u} \in C$ pelo fato de ser espaço vetorial.

□

Observamos dos itens $a), b)$ e $d)$ que existem exatamente q^{n-k} cosets diferentes de C.

Pelo item $d)$ da proposição anterior vemos que se um coset for um subespaço ele necessariamente será igual à C.

Lema 3.3.1. *Sejam C $[n,k,d]-$código sobre $\mathbb{F}_q$ e $x \in \mathbb{F}_q^n$ um vetor. Se $wt(\boldsymbol{x}) \leqslant \lfloor \frac{d-1}{2} \rfloor$ então $\boldsymbol{x}$ é o único vetor líder de $C + \boldsymbol{x}$*

Em sequencia, imaginemos que **v** seja uma palavra enviada e **u** a palavra recebida. O vetor

$$\mathbf{e} = \mathbf{u} - \mathbf{v}$$

é chamado de *vetor erro*. Notamos que $\mathbf{e} = \mathbf{u} - \mathbf{v} \in C + \mathbf{u}$, logo $\mathbf{u} - e = \mathbf{v} \in C$.

Como o vetor erro é definido como a diferença entre a palavra enviada e a recebida, temos que seu peso é justamente a quantidades de erros que ocorreram. Uma forma de verificar com eficiência se algum erro ocorreu é utilizando a matriz de verificação de C.

Exemplo 3.3.5. *Seja $\mathbb{F}_3$ e*

$$C = \{(0,0,0);(0,1,0);(1,2,0);(0,2,0);(1,0,0);(2,0,0);(1,1,0);(2,2,0);(2,1,0)\}.$$

Vamos decodificar as seguintes palavra recebida $w = (2,1,2)$ Notamos que w pertence ao coset $C + (0,0,2)$. Vimos que neste coset o vetor líder é $(0,0,2)$. Logo a palavra-código transmitida mais provável é $(2,1,2) - (0,0,2) = (2,1,0)$.

Definição 3.3.2. *Considere C um $[n,k]-$código. Seja H a matriz de verificação de C, então para qualquer vetor $\boldsymbol{v} \in \mathcal{F}_q^n$ o vetor*

$$S_H(\boldsymbol{v}) = H\boldsymbol{v}^t$$

é chamado de síndrome *de $\boldsymbol{v}$. Quando não houver risco de ambiguidade, denotaremos S_H por S.*

O próximo resultado segue diretamente da definição de síndrome.

Teorema 3.3.1. *Seja C um $[n,k]-$código com matriz de verificação H. Então*

a) $S(\boldsymbol{u} + \boldsymbol{v}) = S(\boldsymbol{u}) + S(\boldsymbol{u})$, para cada $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}^n$

b) $S(\boldsymbol{u}) = \boldsymbol{0} \Leftrightarrow \boldsymbol{u} \in C$.

Demonstração.

a) Pela definição de síndrome, temos que $S(\mathbf{v}) = H\mathbf{v}^t$, logo pela linearidade de H^t temos que $S(\mathbf{v} + \mathbf{u}) = H(\mathbf{v} + \mathbf{u})^t = H(\mathbf{v})^t + H(\mathbf{u})^t = S(\mathbf{v}) + S(\mathbf{u})$.

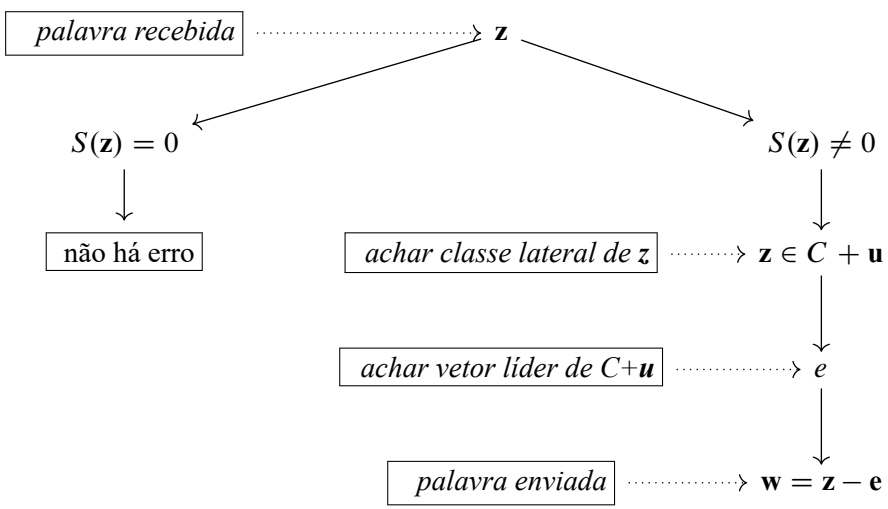
b) $S(\mathbf{v}) = 0$ então $H\mathbf{v}^t = 0$ e, do fato de H ser a matriz de verificação de C segue o resultado.

□

Do Teorema anterior podemos concluir que dois vetores possuem mesma síndrome se, e somente se, estão num mesmo coset. Logo em um coset, basta calcular a síndrome de um único vetor, com isso notamos que cosets estão em correspondência com síndromes.

Corolário 3.3.1. *Sejam C um $[n,k]-$código com matriz de verificação H e $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_q^n$. Então $S(\boldsymbol{u}) = S(\boldsymbol{v})$ se, e somente se, $\boldsymbol{u}, \boldsymbol{v} \in C + \boldsymbol{w}$ para algum $\boldsymbol{w} \in \mathbb{F}_q^n$.*

Sobre a decodificação de uma palavra: Supondo que $wt(\mathbf{z}) \leqslant \lfloor \frac{d-1}{2} \rfloor$, temos o seguinte organograma:



Exemplo 3.3.6. *Seja C um código sobre $\mathbb{F}_2$ com matriz de verificação*

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Então a síndrome de $(1,1,1,1)$ e $(0,1,0,0)$ são dadas por

$$S(1,1,1,1) = H(1,1,1,1)^t = (1,1) \text{ e}$$
$$S(0,1,0,0) = H(0,1,0,0)^t = (0,0).$$

Portanto, $(0,1,0,0) \in C$ não contém erros e $(1,1,1,1) \notin C$ contém erros.

Nesta parte final apresentaremos vários exemplos de códigos. Cada exemplo é na verdade um método para construir alguma família de códigos, que (de uma forma ou de outra) têm bastante parâmetros. Já que em muitos casos essas famílias são predecessores dos códigos algébrico-geométricos, tentamos escolher construções que são fáceis de generalizar nessa direção. Iremos enunciar resultados sem demonstrá-los, mas indicamos onde o leitor pode consultar tais demonstrações.

Exemplo 3.3.7 (Códigos Triviais)**.** *Seja n um inteiro qualquer. Os seguintes códigos são considerados "triviais":*

1. *$O\,[n, n, 1]-$código $C = \mathbb{F}_q^n$ é chamado de* código trivial.
2. *$O\,[n, n-1, 2]-$código* $C' := \left\{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \mid \sum_{i=1}^{n} a_i = 0\right\}$.
3. *$O\,[n, 1, n]-$código $C'' := \{(b, \ldots, b)\}_{b \in \mathbb{F}_q}$ é, como já vimos, chamado de código de repetição.*

Exemplo 3.3.8 (Códigos cíclicos)**.** *Um código $C \subset \mathbb{F}_q^n$ é dito* cíclico *se é invariante por mudanças cíclicas em suas coordenadas, ou seja, se $(a_1, a_2, \ldots, a_n) \in C$ então $(a_2, a_3, \ldots, a_n, a_1) \in C$.*

A seguir vamos apresentar alguns códigos conhecidos como códigos de avaliação.

Exemplo 3.3.9 (códigos de Reed–Solomon)**.** *O código $C = \mathrm{Im}(\eta)$ construído no Exemplo 3.2.4 é chamado de* Códigos de Reed–Solomon de grau k *e como vimos são MDS códigos. Este código é um $[n, k, n-k]-$código.*

Como vimos a partir de um código C, nos podemos construir um novo código calculando o dual. Com essa ideia em mente vamos agora calcular o dual de código de Reed–Solomon.

onde $Resp_a(g)$ é o resíduo de g em a.

Proposição 3.3.2. *Seja $C = \eta(p(x)) = (p(a_1), \ldots, p(a_n))$ um Códigos de Reed–Solomon de grau k. Considere $\mathcal{D}_k$ o espaço vetorial gerado pelos polinômios $g_0(x) := (x - a_1)^{-1} \cdots (a_n)^{-1}$ e $g_i = x^i g_0(x)$ com $0 \leqslant i \leqslant n - k - 2$. Então $C^{\perp} = \mathrm{Im}(\nabla)$ onde*

$$\nabla(g(x))(Resp_{a_1} g, \ldots, Resp_{a_n} g)$$

é um código.

Seja $g_0(x)$ como na proposição acima, considere a função $T(x) = p(x)g_0(x)$ onde $p(x)$ é um polinômio. Então

$$Resp(p)_{a_i} = p(a_i) * \prod_{j \mid i \neq j} (a_i - a_j)^{-1}.$$

O próximo exemplo temos a definição de condigo BCH. Como veremos no próximo capítulo, este código se relaciona com códigos do Exemplo 4.1.4 em um caso particular.

Exemplo 3.3.10 (Códigos BCH)**.** *Sejam* $n|(q^m - 1)$ *e* $\alpha \in \mathbb{F}_{q^m}$ *tal que* $\mathbb{F}_{q^m}^{\times} =< \alpha >$ *. Dados* $r, s \in \mathbb{N}$ *com* $s \geqslant 2$ *considere a matriz*

$$H := \begin{pmatrix} 1 & \alpha^r & \alpha^{2r} & \cdots & \alpha^{r(n-1)} \\ 1 & \alpha^{r+1} & \alpha^{2(r+1)} & \cdots & \alpha^{(r+1)(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{r+s-2} & \alpha^{2(r+s-2)} & \cdots & \alpha^{(r+s-2)(n-1)} \end{pmatrix}$$

Então $C = \{x \in \mathbb{F}_q^n | Hx^t = 0\}$ *é chamado de* códigos BCH *com distância designada* s.

Existem vários outros exemplos de códigos como: códigos de grupos, códigos perfeitos, códigos de Golay e outros códigos através de ferramentas que não veremos neste curso como: códigos por soma direta, produto tensorial de códigos entre outras. Deixamos como referência o texto (Golay 1948) para eventuais consultas.

4 Códigos Geométricos

4.1 Códigos Geométricos e Resultados

Neste capítulo vamos apresentar três exemplos de códigos de avaliação bem conhecidos. Dentre eles, vamos nos aprofundar no Exemplo 4.1.4. Este foco se deve ao fato de estes tipos de códigos serem construídos a partir de curvas e portanto podemos estabelecer relações entre propriedades geométricas e algébricas.

No Capítulo 1 vimos a definição de semigrupos de Weierstrass em um ponto. Aproveitamos a definição de códigos geométricos para apresentar a definição de semigrupos de Weierstrass em m pontos distintos $P_1, \ldots, P_m$. Além disso, veremos algumas caracterizações destes conjuntos bem como o conjunto de geradores minimais $\Gamma(P_1, \ldots, P_m)$. Ainda veremos uma generalização semigrupos de Weierstrass em m pontos.

Durante todo o capítulo $\mathbb{F}_q$ sempre denotará um corpo finito com q elementos e $\mathcal{X}$ uma curva projetiva, geometricamente irredutível, não singular.

Exemplo 4.1.1 (Códigos Reed–Muller de primeira ordem)**.** *Considere um linear espaço $\mathcal{L}_m$ de polinômios de grau 0 e 1 em m variáveis, então $dim\mathcal{L}_m = m + 1$. Dado $A = \{P_1, \ldots, P_n\} \subset \mathbb{F}_q^m$ tal que nenhum polinômio linear não nulo se anula em todos os pontos $P_1, \ldots, P_n$ (é portanto então, se $n > mq - l$, pois o*

número de zeros de um polinomial em m variáveis é no máximo q^{m-l}). Considerando a aplicação $\beta : \mathcal{L}_m \to \mathbb{F}_q^m$ por $\beta(f) = (f(P_1), \ldots, f(P_n))$ definimos o Códigos Reed–Muller de primeira ordem *como*

$$\mathcal{C} = \mathrm{Im}(\beta).$$

Então $\mathcal{C}$ é um $[n, m+1, n-q^{m-1}]-$código

Exemplo 4.1.2 (Códigos de Hamming)**.** *O* código de Hamming *é obtido tomando o dual do código de Reed–Muller acima e é denotado por*

$$C_H = \mathcal{C}^{\perp}.$$

Nosso próximo exemplo é o Código de Reed–Muller de ordem r, que generaliza o exemplo anterior.

Exemplo 4.1.3 (Códigos Reed–Muller de ordem r)**.** *Sejam $\mathbb{F} = \mathbb{F}_q$ um corpo finito e r, m inteiros tais que $r < m(q-1)$. Seja $\mathcal{L}_m^r$ o espaço vetorial dos polinômios de m variáveis de grau no máximo r. Tomando um conjunto $U = \{v_1, \ldots, v_n\} \subset \mathbb{F}_q^m$ consideramos a aplicação*

$$\begin{aligned} ev_U : \mathcal{L}_m^r &\to \mathbb{F}_q^n \\ p(x) &\mapsto (p(v_1), \ldots, p(v_n)) \end{aligned}$$

Então $C = \mathrm{Im}(ev_U)$ é chamado de códigos Reed–Muller de ordem r

A seguir apresentamos o exemplo que motiva toda o estudo desta seção.

Exemplo 4.1.4 (Códigos de Goppa)**.** *Sejam n e q inteiros tais que $n = q-1$ e $\alpha \in \mathbb{F}_q$ um elemento satisfazendo $< \alpha >= \left\{1, \alpha, \ldots, \alpha^{q-1}\right\} = \mathbb{F}_q^{\times}$. Para qualquer inteiro k onde $1 \leqslant k \leqslant n$ definimos o $\mathbb{F}_q-$espaço vetorial*

$$\mathcal{L}_k = \left\{ f(x) \in \mathbb{F}_q[x] \mid deg(f) \leqslant k-1 \right\}$$

e consideramos a aplicação

$$\begin{aligned} ev :& \mathcal{L}_k \to \mathbb{F}_q^n \\ & f \mapsto (f(\alpha), f(\alpha^2), \ldots, f(\alpha^n)) \end{aligned}$$

Vamos utilizar a seguinte notação:

1. *$F/\mathbb{F}_q$ um corpos de funções algébricas de gênero g;*

2. *Um divisor $D = P_1 + \cdots + P_n$, onde P_i são places distintos de grau um em $F/\mathbb{F}_q$;*

3. *G um divisor de $F/\mathbb{F}_q$ tal que* $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$.

O conjunto

$$\mathcal{C}_{\mathcal{L}}(D, G) := \{(z(P_1), \ldots, z(P_n))|\ z \in \mathcal{L}(G)\} \subset \mathbb{F}_q^n \tag{4.1}$$

é chamado de código de Goppa associado ao divisor D *(ou* Código Geométrico*).*

Seja $\mathcal{X}$ uma curva sobre $\mathbb{F}_q$ contendo pelo menos um ponto racional, ie, o conjunto dos pontos racionais de $\mathcal{X}$, denotado por $X(\mathbb{F}_q)$, é não vazio. Seja $D = P_1 + \cdots + P_n \in Div(\mathcal{X})$ com $P_i \in X(\mathbb{F}_q)$. Considere $G \in Div(\mathcal{X})$ tal que $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$. Considerando o mapa de avaliação

$$\begin{aligned} ev_D :& \mathcal{L}(G) \to \mathbb{F}_q^n \\ & f \mapsto (f(P_1), \ldots, f(P_n)) \end{aligned}$$

onde $\mathcal{L}(G) = \{0 \neq f \in X|\ (f) \geqslant -G\} \cup \{0\}$ é o espaço de Riemann–Roch associado ao divisor G.

Definição 4.1.1. *Dado $\mathcal{X}$ uma curva sobre $\mathbb{F}_q$, com $\mathcal{X}(\mathbb{F}_q) \neq \emptyset$. Seja $D = P_1 + \cdots + P_n \in Div(X)$ com $P_i \in \mathcal{X}(\mathbb{F}_q)$. Considere $G \in Div(\mathcal{X})$ tal que* $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$. *O código $C_{\mathcal{X}}(\mathcal{L}, D, G) = \mathrm{Im}(ev_D)$ é chamado* código Geométrico

Observamos que esta definição é equivalente a definição do Exemplo 4.1.4. De fato, dada uma curva $\mathcal{X}$ uma curva sobre $\mathbb{F}_q$, vimos que a esta curva está associado um corpo de funções $\mathcal{X}/\mathbb{F}_q$ (continuar). Quando não for necessário evidenciar a curva denotaremos o código $C_{\mathcal{X}}(\mathcal{L}, D, G)$ simplesmente por $C(\mathcal{L}, D, G)$

Lema 4.1.1. *Sejam k a dimensão e d a distância mínima do código $C_{\mathcal{X}}(\mathcal{L}, D, G)$. Então*

a) $k = \ell(G) - \ell(G - D)$

b) $d \geqslant n - Deg(G)$.

Demonstração. a) Observamos que aplicação ev_D é sobrejetora entre $\mathcal{L}(G)$ e $C(\mathcal{L}, D, G)$. Note ainda que $f \in ker(ev_D)$ se, e somente se, $v_P(f) > 0$ para cada $P \in \text{Supp}(D)$. Portanto, $ker(ev_D) = \mathcal{L}(G - D)$. Estes fatos juntamente com propriedades de Álgebra linear, obtemos que $k = \ell(G) - \ell(G - D)$.

b) Seja $z \in \mathcal{L}(G)$ tal que $d = d(C) = wt(C) = wt(z)$, então existem exatamente $n-d$ places, digamos $P_1, \ldots, P_{n-d}$ em D, tais que $z(P_i) = 0$, i.e., $v_{P_i}(z) > 0$. Assim, $\ell(\mathcal{L}(G - P_1 - \cdots - P_{n-d})) \geqslant 1$ e $Deg(\mathcal{L}(G - P_1 - \cdots - P_{n-d})) \geqslant 0$. Portanto, $d \geqslant n - Deg(G)$.

□

Teorema 4.1.1. *Seja $C_{\mathcal{X}}(\mathcal{L}, D, G)$ $[n, k, d]$−código e suponha que $n - Deg(G) > 0$ e g seja o gênero da curva $\mathcal{X}$. Então*

a) A aplicação ev_D é injetiva.

b) $k = \ell(G)$. Em particular, $k \geqslant Deg(G) + 1 - g$ e $k + d \geqslant n + 1 - g$

c) Se $Deg(G) > 2g - 2$, então $k = Deg(G) + 1 - g$.

d) A matriz geradora de $C_{\mathcal{X}}(\mathcal{L}, D, G)$ é dada por

$$G := \begin{pmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ x_2(P_1) & x_2(P_2) & \cdots & x_2(P_n) \\ \vdots & \vdots & \vdots & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{pmatrix}$$

onde $\beta = \{x_1, \ldots, x_k\}$ é uma base de $\mathcal{L}(G)$.

Demonstração. a) Se $n - Deg(G) < 0$, então $Deg(G - D) < 0$ e portanto $ker(ev_D) = \mathcal{L}(G - D) = 0$.

b) Segue do item *a*) e do Lema 4.1.1 que $k = \ell(G)$. Além disso, do Teorema de Riemann–Roch concluímos que $k \geqslant Deg(G) + 1 - g$ e $k + d \geqslant n + 1 - g$.

c) Se $Deg(G) > 2g - 2$ então pela Proposição 2.1.3 temos que $k = Deg(G) + 1 - g$.

d) Seja $\beta = \{x_1, \ldots, x_k\}$ é uma base de $\mathcal{G}$. Basta mostrar que $v_j = (x_j(P_1), \ldots, x_j(P_n))$ forma uma base de $C_{\mathcal{X}}(\mathcal{L}, D, G)$. Escrevendo $\sum a_i v_i$ com $a_i \in \mathbb{F}_q$ temos que $\sum a_i x_i(P_j) = 0$. Assim, $\sum a_i x_i \in \mathcal{L}(G - D)$ e portanto $a_i = 0$ para todo i.

□

Definição 4.1.2. *Seja $C_{\mathcal{X}}(\mathcal{L}, D, G)$ $[n, k, d]-$ código. O inteiro $\varrho := n - Deg(G)$ é chamado de* distância! designada.

O lema anterior mostra que a distância mínima de um código é sempre maior que a distância designada. Logo uma questão interessante que surge é saber quando $d = \varrho$ ou $d \neq \varrho$.

Notamos que se o divisor G é tal que $l(G) > 0$ e $\varrho > 0$ então $d = \varrho \Leftrightarrow$ existir um divisor positivo A tal que $A \leqslant D$, $l(G - A) > 0$ e $Deg(A) = Deg(G)$. Deixamos a prova deste fato ao leitor.

Afim de descrever o dual de um AG código, vamos definir um novo código.

Definição 4.1.3. *Sejam dois divisores G e $D = \sum_{i=1}^{m} P_i$ em um corpo de função $F/\mathbb{F}$ tais que* $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$ *e $P_i \neq P_j$ para $i \neq j$. O conjunto $C_{\Omega}(G, D) := \{(\omega_{P_1}(1), \ldots, \omega_{P_m}(1)) | \, \omega \in \Omega_F(G - D)\} \subset \mathbb{F}^m$ é um código geométrico.*

Seja P um place de $F/\mathbb{F}_q$ de grau um e ω um diferencial de Weil satisfazendo $v_P(\omega) \geqslant -1$. Se $\omega_P(1) = 0$, seja $x \in F$ tal que $v_P(x) \geqslant 0$. Sendo P um place de grau um, podemos escrever $x = u + z$ com $a \in \mathbb{F}_q$ e $v_P(y) \geqslant 1$. Então

$$\omega_P(x) = \omega_P(u) + \omega_P(y) = u\omega_P(1) = 0$$

e $v_P(\omega) \geqslant 0$.

Proposição 4.1.1. *O código $C_{\Omega}(G, D)$ satisfaz as seguintes propriedades:*

a) A dimensão de $C_{\Omega}(G, D)$ é $i(G - D) - i(G)$.

b) A distância mínima d de $C_{\Omega}(G, D)$ é tal que $d \geqslant Deg(G) + 2 - 2g$.

Demonstração. a) Consideramos a aplicação

$$ev_D : \Omega_{\mathcal{X}}(G - D) \to C(D, G)$$

dada por $e_D(w) = (w_{P_1}(1), \ldots, w_{P_n}(1))$. É imediato verificar que

$$\text{Im}(e_D(\omega) = C_\Omega(D, G) \quad \text{e} \quad ker(e_D(\omega)) = \Omega_\mathcal{X}(G)$$

Portanto, $k = i(G - D) - i(G)$.

b) Por outro lado, seja $e_D(\omega) \in C(D, G)$ tal que $wt(e_D(\omega)) = m > 0$, então $\omega_{P_i}(1) = 0$ para $i = i_1, \ldots, i_{n-m}$. Logo

$$\omega \in \Omega_\mathcal{X}(G - (D - \sum P_{i_j}))$$

Como $\Omega_\mathcal{X}(A) \neq 0$, onde $A := G - (D - \sum P_{i_j})$, temos que $Deg(A) \geqslant 2g - 2$. Assim,

$$2g - 2 \geqslant Deg(G)deg(G) - (n - (n - m)) = deg(G) - m,$$

mas como m é arbitrário segue que $d \geqslant deg(G) - (2g2)$.

□

Se nas condições da proposição anterior impormos que $Deg(G) > 2g - 2$, onde g é o gênero de F, temos que $k' = \dim(C_\Omega(D, G))$ satisfaz

$$k' = i(G - D) - i(G) \geqslant n - Deg(G) + g - 1.$$

Teorema 4.1.2. *O código dual de $\mathcal{C}_\mathcal{L}(G, D)$ é o código $C_\Omega(G, D)$.*

Proposição 4.1.2. *Considere em $F/\mathbb{F}_q$ dois divisores equivalentes G e U tais que* $\text{Supp}(G) \cap \text{Supp}(D) = \emptyset$ *e* $\text{Supp}(U) \cap \text{Supp}(D) = \emptyset$ *com* $D = \sum_{i=1}^{n} P_i$. *Então $\mathcal{C}(\mathcal{L}, D, G)$ e $\mathcal{C}(\mathcal{L}, D, U)$ são equivalentes.*

Demonstração. Como G é equivalente à U, então existe $w \in F$ tal que $G = U + (w)$ com $v_{P_i}(w) = 0$, para cada $i = 1, \ldots, n$. Definindo $u := (w(P_1), \ldots, w(P_n))$ temos a aplicação $y \mapsto yw$ que é uma bijeção entre $\mathcal{L}(G)$ e $\mathcal{L}(U)$. Portanto, $\mathcal{C}(\mathcal{L}, D, G) = u\mathcal{C}(\mathcal{L}, D, U)$. □

Uma consequência imediata do resultado anterior é.

Corolário 4.1.1. *$\mathcal{C}_\Omega(D, G)$ é equivalente à $\mathcal{C}_\Omega(D, U)$*

Como veremos no próximo resultado, qualquer código linear equivalente a um código geométrico, ele necessariamente será um código geométrico.

Proposição 4.1.3. *Seja D um divisor em $F/\mathbb{F}_q$. Todo código equivalente à $\mathcal{C}(\mathcal{L}, D, U)$ é da forma $\mathcal{C}(\mathcal{L}, D, G)$ com G e U equivalentes e* $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$ *e* $\mathrm{Supp}(U) \cap \mathrm{Supp}(D) = \emptyset$.

Demonstração. Seja C tal que $C = a\mathcal{C}(\mathcal{L}, D, U)$, onde $a = (a_1, \ldots, a_n)$. Escolhendo $z \in F$, com $z(P_i) = a_i$ temos que o divisor $G := U - (z)$ satisfaz a condições desejadas.

□

Exemplo 4.1.5. *Considere a o corpo de funções $F/\mathbb{F}_{q^{2r}}$ dado pela curva $y^q + y = x^{q^r+1}$ com gênero g. Considere P_∞ o place no infinito de F e P_0 o zero em comum das funções x e y. Em (Castellanos e Tizziotti 2014), foram calculadas algumas propriedades do código $C_\Omega(D, G)$ onde $D = \sum_{i=1}^{n} P_i$ e $G = (a+b-1)P_\infty + (c+d-1)P_0$ com $P_i \neq P_0, P_\infty$. Suponha que*

1. *$a \geqslant 1$ e $\exists f \in F$ tal que* $\mathrm{div}(f)_\infty = aP_\infty + bP_0$ *e $\ell(\mathcal{L}(aP_\infty + bP_0)) = \ell(\mathcal{L}((a-1)P_\infty + bP_0))$.*
2. *$(b, d-u-1), (b+1, d-u-1), (b+q^r+1, d-u-1), (b, d-u)$ não existem funções com divisor de polos sendo estes pontos, para cada $0 \leqslant u \leqslant min\{b-1, 2g-1-(a+b)\}$*

Então $d(C_\Omega(D, G)) \geqslant Deg(G) - 2g + 4$.

4.2 Códigos Racionais e Hermitianos

Nesta seção vamos estudar códigos racionais e códigos Hermitianos. Estas duas famílias de códigos são exemplos importantes como veremos dentro da família de códigos geométricos. Por exemplo, códigos racionais possuem uma relação com códigos de Reed–Solomon generalizados. Ao longo deste estudo, veremos algumas propriedades interessantes que estes códigos apresentam.

Seja $\mathcal{X}$ uma curva sobre $\mathbb{F}_q$. Nesta seção vamos considerar G e $D = \sum_{i=1}^{m} P_i$ divisores com $P_i \in \mathbb{F}_\mathcal{X}$ places racionais distintos dois à dois e $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$.

Definição 4.2.1. *Um código geométrico $C_F(\mathcal{L}, D, G)$ é dito ser um* código racional *se é obtido do corpo de funções racionais $F = \mathbb{F}_q(z)$.*

Teorema 4.2.1. *Se $C_F(\mathcal{L}, D, G)$ é um $[n, k, d]$−código racional sobre $\mathbb{F}_q$,então*

a) $n \leqslant q+1$.

b) $k = n \Leftrightarrow Deg(G) > n-2$. *E* $k = 0$ *se e somente se o grau de* G *é negativo.*

c) Quando $0 \leqslant Deg(G) \leqslant n-2$ *temos que* $k = Deg(G)+1$.

d) Quando $0 \leqslant Deg(G) \leqslant n-2$ *a distância mínima é exatamente* $n - Deg(G)$.

Demonstração. a) Como $\mathbb{F}_q(x)$ tem exatamente $q+1$ places de grau um, sendo eles o place no infinito e os places associados as funções $x-a$, com $a \in \mathbb{F}_q$ o resultado segue. Os itens b), c) e d) seguem do Teorema 4.1.1.

□

Para este tipo de código, quando $G = sP_\infty$ temos que o espaço de Riemann–Roch é facilmente calculado, i.e., $\mathcal{L}(sP_\infty) =< 1, x, \ldots, x^s >$, onde P_∞ é o ponto no infinito da curva racional e $0 \leqslant s \leqslant n-2$. Como os parâmetros destes códigos satisfazem $k+d = n+1$ temos que os mesmos são MDS.

Proposição 4.2.1. *Seja* $C_F(\mathcal{L}, D, G)$ *é um código racional sobre* $\mathbb{F}_q$. *Então*

a) Se $n = q+1$, *então* $C_F(\mathcal{L}, D, G)$ *é dada por*

$$C_F(\mathcal{L}, D, G) = \left\{(u_1 p(a_1), \ldots, u_n p(a_n))|\ p(z) \in \mathbb{F}_q[z] \text{ e } deg(p(z)) \leqslant k-1\right\},$$

onde $u_1, \ldots, u_n \in \mathbb{F}_q^\times$ *e* $a_1, \ldots, a_n \in \mathbb{F}_q$ *com* $a_i \neq a_j$ *para* $i \neq j$.

b) Se $n \leqslant q$ *então a matriz geradora de* $C_F(\mathcal{L}, D, G)$ *é dada por*

Demonstração. a) Seja $n = q+1$, escolhendo P_∞ como o polo de x. Assumindo que $Deg(G) = k-1$ temos que $(k-1)P_\infty - G$ possui grau zero, logo existe uma função $w \neq 0$ tal que $(k-1)P_\infty - G = \text{div}(w)$.. Como $\ell(G) = k$ e $w, wx, \ldots, wx^{k-1} \in \mathcal{L}(G)$ são linearmente independentes o resultado segue.

b) Segue de forma similar a demonstração do item anterior.

□

Na demonstração da Proposição anterior obtemos que

$$\mathcal{L}(G) = \left\{wp(x)|\mathbb{F}_q[z] \text{ e } deg(p(z)) \leqslant k-1\right\}.$$

Quando $n \leqslant q$ podemos exibir a matriz geradora M de C. Fazendo $a_i := x(P_i)$ e $v_i := w(P_i)$ obtemos que $(wp(x)(P_i) = v_i\, p(a_i)$. Então os vetores $(v_1 a_1^i, \ldots, v_m a_m^i)$ corresponde as linha da matriz M.

De forma análoga, quando $n = q+1$, obtemos que as linhas da matriz geradora são dadas por $(v_1 a_1^i, \ldots, v_{m-1} a_{m-1}^i, 0)$ e $(v_1 a_1^i, \ldots, v_{m-1} a_{m-1}^i, 1)$

Segue dos resultados anteriores que o dual de um código racional também é racional.

O estudo sobre Códigos Hermitianos são interessantes pois são códigos que retornam "boa" distância mínima e dimensão. Como veremos tais códigos são construídos a partir da curva Hermitiana sobre $\mathbb{F}_{q^2}$.

Considere $\mathcal{H}_{q^2}$ o corpo de funções dado pela equação Hermitiana $y^q + y = x^{q+1}$. Vimos que esta curva possui gênero $g = \frac{q(q-1)}{2}$. $\mathcal{H}_{q^2} = \mathbb{F}_{q^2}(y, x)$ é chamado de corpo de funções Hermitianas. Esta curva possui propriedade interessantes como: x e y possui um único polo em comum P_∞ e para cada ponto da forma $(a, b) \in \mathcal{H}_{q^2}$ existe um único place da $P_{(a,b)}$ tal que $x(P_{(a,b)}) = a$ e $y(P_{(a,b)}) = b$.

Exercício 4.2.1. *Mostre que para cada $a \in \mathbb{F}_{q^2}$ existe exatamente q elementos distintos $b \in \mathbb{F}_{q^2}$ satisfazendo a equação da curva $y^q + y = x^{q+1}$. Conclua que o número de places em $\mathcal{H}_{q^2}$ da forma $P_{(a,b)}$ é q^3.*

Seja $\mathcal{H} = K(x, y)$ com $y^q + y = x^{q+1}$ o corpo de funções Hermitiano, onde $K = \mathbb{F}_q$. Sabemos que $\mathcal{H}$ possui exatamente $q^3 + 1$ places de grau um. Vamos denotar $P_\infty \in \mathbb{P}_{K(x)}$ o place no infinito. Vimos que existe um único place $Q_\infty \in \mathbb{P}_{\mathcal{H}}$ que sobre P_∞.

Definição 4.2.2. *O* código Hermitiano *é definido como $\mathcal{H}_r := \mathcal{C}(\mathcal{L}, D, rQ_\infty)$, onde $D = \sum_{i=1}^{q^3} P_i$ com P_i racional e $P_i \neq Q_\infty$.*

Proposição 4.2.2. *O semigrupo de Weiertrass $H(Q_\infty) =< q, q+1 >$.*

Demonstração. De fato, pelo exercício 4 temos que $(x)_\infty = qQ_\infty$ e $(y)_\infty = (q+1)Q_\infty$. Logo, $q,\ q+1 \in H(Q_\infty)$ e assim $< q, q+1 > \subset H(Q_\infty)$. Como $H(Q_\infty)$ e $< q, q+1 >$ tem mesmo gênero $g = \frac{q(q-1)}{2}$ segue que $H(Q_\infty) =< q, q+1 >$. Portanto, $m(< q, q+1 >) = q$ e $c(< q, q+1 >) = q^2 - q$. □

Note que podemos calcular $l(rQ_\infty)$ para $r \in H(Q_\infty)$. observamos que se $r \geqslant q(q-1)$ então $l(rQ_\infty) = r - g + 1$. Sabemos que $H(Q_\infty) = \{0 = h_0 <$

$h_1 < \cdots < h_g = 2g, \ldots\}$ e que r é uma não lacuna se, e somente se, $l(rQ_\infty) = l((r-1)Q_\infty) + 1$. Como $l(0) = 1$ segue por indução que $l(h_i Q_\infty) = i + 1$, para cada $i = 0, \ldots, g-1$.

Como comentamos anteriormente, alguns trabalhos científicos buscam descrever uma base para o espaço de Riemann–Roch de uma curva, pois tal informação auxilia na obtenção de informações sobre outros objetos,como por exemplos, semigrupos de Weierstrass, códigos, isomorfismo, etc.. A seguir vamos calcular uma base de um caso particular da curva Hermitiana.

Vamos achar uma base para $\mathcal{L}(2qQ_\infty) = \{1, x, y, x^2\}$.

Com efeito, temos pelo item b) que $\ell(qQ_\infty) = 2$, $\ell((q+1)Q_\infty) = 3$ e $\ell(2qQ_\infty) = 4$. Segue do item a) que $x \in \mathcal{L}(qQ_\infty)$ e assim $\{1, x\}$ é uma base para $\mathcal{L}(2qQ_\infty)$. Como

$$\mathcal{L}(qQ_\infty) \subset \mathcal{L}((q+1)Q_\infty) \subset \mathcal{L}(2qQ_\infty).$$

Pelo item a) $y \in \mathcal{L}((q+1)Q_\infty)$ e $\ell((q+1)Q_\infty) = 3$ temos que $\{1, x, y\}$ é uma base para $\mathcal{L}((q+1)Q_\infty)$. Observando que $x^2 \in \mathcal{L}(2qQ_\infty)$ e que $\ell(2qQ_\infty) = 4$ concluímos que $\{1, x, y, x^2\}$ é uma base para $\mathcal{L}(2qQ_\infty)$.

Sobre a dimensão deste código temos o seguinte teorema.

Definindo $I(s) := \{n \in \mathcal{H}(Q_\infty) | \ n \leqslant s\}$, vamos calcular a dimensão do código C_r.

Teorema 4.2.2. *Sejam k a dimensão e d a distância mínima de $\mathcal{H}_r$. Se $0 \leqslant r \leqslant q^3 + q^2 - q - 2$, então vale:*

a) $k = \#(I(r))$ *se* $0 \leqslant r \leqslant q^3$.

b) $k = q^3 - \#(I(s))$, *se* $q^3 \leqslant r \leqslant q^3 + q^2 - q - 2$, *onde* $s := q^3 + q^2 - q - 2 - r$.

c) $k = r + 1 - \frac{q(q-1)}{2}$, *se* $q^2 - q - 2 \leqslant r \leqslant q^3$.

Demonstração. a) Se $0 \leqslant r \leqslant q^3$ segue imediatamente que $\dim(C_r) = \ell(rQ_\infty) = \#(I(r)$.

b) Se $q^3 \leqslant r \leqslant q^3 + q^2 - q - 2$, onde $s := q^3 + q^2 - q - 2 - r$, então $\dim(C_r) = q^3 - \dim(C_s) = q^3 - \#(I(r)$.

c) Segue do Lema 4.1.1.

□

4.3 AG Códigos, Semigrupos Numéricos e Curvas

No Capítulo 2 vimos que o conjunto de pontos de uma curva definida sobre um corpo finita é um conjunto finito. Em 1981 o matemático Ihara em (Ihara 1981) mostrou que dada uma curva $\mathcal{X}$ de gênero g definida sobre $\mathbb{F}_q$ tinha como cota para a cardinalidade de seus pontos racionais, $\mathcal{X}(\mathbb{F}_q)$, $2g\sqrt{q}+1+q$. Em outras palavras,

$$\#(\mathcal{X}(\mathbb{F}_q)) \leqslant 2g\sqrt{q}+1+q. \tag{4.2}$$

A cota acima recebe o nome de *cota de Hasse–Weil* (ou cota HW) em homenagem aos matemáticos Hasse e Weil.

Uma curva $\mathcal{X}$ de gênero g definida sobre $\mathbb{F}_q$ é dita ser uma *curva maximal* se a cota HW é atingida. É claro que tal cota somente pode ser atingida se q for da forma p^{2t} para algum número primo p.

Curvas maximais possuem propriedades interessantes, principalmente pelo fato que sabemos exatamente a quantidade de pontos racionais. Portanto, construir AG códigos.

Nesta e na próxima seção veremos exemplos de códigos construídos a partir de curvas maximais.

A curva Hermitiana $\mathcal{H}_{q^2} : y^q + y = x^{q+1}$ definida sobre $\mathbb{F}_{q^2}$ é uma curva maximal veja a demonstração em (Hirschfeld, Korchmáros e Torres 2008). Lembramos do Exemplo 2.2.5 que esta curva possui gênero $g = \frac{(q-1)q}{2}$ e portanto $\mathbb{F}_{q^2}(\mathcal{H}_{q^2}) = 1 + q^2 + q^2(q-1) = 1 + q^3$.

Exemplo 4.3.1. *Considere $\mathcal{H}_{16} : y^4 + y = x^5$, definida sobre $\mathbb{F}_{4^2}$. Então $H(P_\infty) =< 4, 5 >= \{0, 4, 5, 8, 9, 10, 12, \ldots\}$*

Um importante resultado sobre curvas maximais é enunciado no próximo resultado.

Teorema 4.3.1. *Seja $\mathcal{X}$ uma curva maximal sobre $\mathbb{F}_{q^2}$ com gênero $g > 0$. As seguintes afirmações são equivalentes:*

a) $\mathcal{X}$ é a curva Hermitiana,

b) $g > \frac{(q-1)^2}{4}$.

Em outras palavras, o resulta afirma que qualquer curva maximal com gênero $g\frac{(q-1)^2}{4}$ deve ser a própria curva Hermitiana. Este fato, sugere uma serie de perguntas acerca de curvas maximais, abaixo listamos algumas delas:

- É possível determinar todos os gêneros de curvas maximais sobre $\mathbb{F}_{q^2}$ tais que $g \leqslant \frac{(q-1)^2}{4}$?

- Se existem tais curvas, elas são "únicas"?

Na Teoria de Curvas Maximais, vários resultados sobre estas perguntas foram obtidos, por exemplo, em (ibid.). Assim, já possuímos respostas parciais para algumas perguntas.

Resumimos estes resultadas no seguinte teorema.

Teorema 4.3.2. *Seja $\mathcal{X}$ uma curva maximal sobre $\mathbb{F}_{q^2}$ com gênero $g > 0$. Então g satisfaz:*

a) $g = \frac{q(q-1)}{2}$,

b) $g = \lfloor \frac{(q-1)^2}{4} \rfloor$.

c) $g \leqslant \lfloor \frac{q^2-q+4}{6} \rfloor$.

Os dois Teoremas anteriores podem ser encontrados em (ibid.), (Fuhrmann, Garcia e Torres 1996).

A seguir vamos apresentar algumas famílias de curvas maximais sobre $\mathbb{F}_{q^2}$. Para mais exemplos e detalhes o leitor pode obter em (Hirschfeld, Korchmáros e Torres 2008).

$$\begin{aligned} \mathcal{D}_r : &\quad x^r + y^r + 1 \\ \mathcal{E}_m^1 : &\quad y^q + y - x^m \\ \mathcal{C}_n : &\quad x^n y + y^n + x \\ \mathcal{F}_0 : &\quad x^{\frac{q+1}{3}} + x^{\frac{2(q+1)}{3}} + y^{q+1} : \end{aligned}$$

No Capítulo 2 definimos semigrupos Weierstrass para um ponto, aqui discutiremos o caso particular de códigos geométricos no caso em que o divisor D é um único ponto racional. Motivamos pelo fato de que tal divisor possa ser soma de m pontos racionais, definiremos o semigrupo de Weierstrass em m pontos.

Definição 4.3.1. *Sejam $\mathcal{X}$ uma curva definida sobre $\mathbb{F}_q$ e $\mathbb{F}_q(\mathcal{X})$ o corpo de funções associado à $\mathcal{X}$. Dados $P_1, \ldots, P_m \in \mathcal{X}(\mathbb{F}_q)$ pontos racionais. O conjunto*

$$H(P_1, \ldots, P_m) := \left\{ (a_1, \ldots, a_m) \in \mathbb{N}_0^m \mid \exists h \in \mathbb{F}_q(\mathcal{X})^\times, \ \mathrm{div}(h)_\infty = \sum_{i=1}^{m} a_i P_i \right\}$$

é chamado semigrupo de Weierstrass *na $m-$upla $(P_1, \ldots, P_m)$.*

Por questões históricas, muitas vezes o conjunto $H(P_1, \ldots, P_m)$ é chamado de *semigrupo de Weierstrass clássico* na $m-$upla $(P_1, \ldots, P_m)$

Lema 4.3.1. *Sejam $\mathcal{X}$ uma curva definida sobre $\mathbb{F}_q$ e $\mathbb{F}_q(X)$ o corpo de funções associado à $\mathcal{X}$. Então*

$$H(P_1, \ldots, P_m) := \left\{ (a_1, \ldots, a_m) \in \mathbb{N}_0^m \mid \exists h \in \mathbb{F}_q(\mathcal{X})^\times, \ \mathrm{div}(h)_\infty = \sum_{i=1}^{m} a_i P_i \right\}$$

é um subsemigrupo de $\mathbb{N}_0^m$

O conjunto de lacunas de $H(P_1, \ldots, P_m)$ é definido por $G(P_1, \ldots, P_m) := \mathbb{N}_0^m \setminus H(P_1, \ldots, P_m)$ e o gênero é dado por $g(H(P_1, \ldots, P_m)) = \#(G(P_1, \ldots, P_m))$. Vale ressaltar que diferente do caso em que $m = 1$, quando $m \geqslant 2$ o valor $g(H(P_1, \ldots, P_m))$ depende da escolha dos pontos $P_1, \ldots, P_m$. Neste sentido, vamos supor que $m \geqslant 2$.

Notamos quando $m = 1$ recuperamos a definição de semigrupo de Weierstrass dada no Capítulo 2.

A seguir vamos sempre supor que $P_1, \ldots, P_m$ são pontos racionais de uma curva $\mathcal{X}$ e denotaremos $H_r := H(P_1, \ldots, P_r)$ e $G_r := G(P_1, \ldots, P_r)$ com $1 \leqslant r \leqslant m$. Em H_r vamos definir a seguinte relação de ordem parcial: dados $\mathbf{u} = (u_1, \ldots, u_r), \mathbf{v} = (v_1, \ldots, v_r) \in H_r$ dizemos que $\mathbf{u}$ é menos que $\mathbf{v}$, denotamos por $\mathbf{u} \preceq \mathbf{v}$, quando $u_i \leqslant v_i$ para todo $i = 1, \ldots, r$.

Dado $\mathbf{v} = (v_1, \ldots, v_m) \in \mathbb{N}_0^m$ definimos o conjunto

$$\bigtriangledown_i(\mathbf{v}) := \left\{ u = (u_1, \ldots, u_r) \in H_r \mid u_i = v_i \ e \ u_j \leqslant v_j, \forall j \neq i \right\}.$$

Ainda definimos o vetor $v(i) := \mathbf{v} - u_i e_i$, onde e_i é o vetor com 1 na $i-$ésima posição e zero nas demais.

Para $\mathbf{v} = (v_1, \ldots, v_m) \in \mathbb{N}_0^m$ vamos denotar por $\mathcal{L}(\mathbf{v}) = \mathcal{L}(v_1 P_1 + \cdots + v_m P_m)$ e $\ell(\mathbf{v}) = dim\,(\mathcal{L}(\mathbf{v}))$.

Lema 4.3.2. *Suponha que* $\#(\mathbb{F}_q) \geqslant m$. *Dado* $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}_0^m$ *temos que* $\ell(\boldsymbol{v}) = l(\boldsymbol{v} - e_i) + 1 \Leftrightarrow \bigtriangledown_i(\boldsymbol{v}) \neq \emptyset$.

Demonstração. Provaremos somente a ida, pois a reciproca é imediata. Com efeito, seja $w \in \mathcal{L}(\mathbf{v}) \backslash \mathcal{L}(\mathbf{v} - e_i)$. Como $\#(\mathbb{F}_q) \geqslant m$, existe $u \in \mathbb{F}_q$ tal que $(-v_{P_1}(w+u), \ldots, -v_{P_m}(w+u)) \in \bigtriangledown_i(\mathbf{v})$.

□

A prova do próximo lema pode ser encontrado em (Carvalho e Torres 2005).

Lema 4.3.3. *Suponha que* $\#(\mathbb{F}_q) \geqslant m$. *As seguintes afirmações são equivalentes*

a) $\boldsymbol{u} = (u_1, \ldots, u_m) \in H_m$.

b) $\ell(\boldsymbol{u}) = l(\boldsymbol{u} - e_i) + 1$, $\forall i = 1, \ldots, m$.

O próximo resultado é uma consequência imediata do lama anterior. Deixamos a demonstração como exercício ao leitor.

Corolário 4.3.1. *Suponha que* $\#(\mathbb{F}_q) \geqslant m$. *As seguintes afirmações são equivalentes*

a) $\boldsymbol{n} = (n_1, \ldots, n_m) \in G_m$.

b) $\ell(\boldsymbol{n}) = l(\boldsymbol{n} - e_i)$, *para algum* $i = 1, \ldots, m$.

c) $\bigtriangledown_i(\boldsymbol{n}) = \emptyset$, *para algum* $i = 1, \ldots, m$.

Dizemos que $\mathbf{n} = (n_1, \ldots, n_m) \in G_m$ é uma *lacuna de Weierstrass pura* se

$$\ell\left(\mathcal{L}\left(\sum_{i=1}^{m} n_i P_i\right)\right) = \ell\left(\mathcal{L}\left(\sum_{i=1}^{m} n_i P_i - P_j\right)\right).$$

Lema 4.3.4. *Dados* $\boldsymbol{u} = (u_1, \ldots, u_m), \boldsymbol{v} = (v_1, \ldots, v_m) \in H_m$. *Se* $w_i := max\{u_i, v_i\}$ *para cada* $i = 1, \ldots, r$ *então* $\boldsymbol{w} = (w_1, \ldots, w_m) \in H_m$.

Demonstração. Sejam $f, g \in \mathbb{F}(\mathcal{X})$ tais que $\operatorname{div}(f)_\infty = \sum_{i=1}^{m} u_i P_i$ e $\operatorname{div}(g)_\infty = \sum_{i=1}^{m} v_i P_i$. Considere t_i um parâmetro local de P_i, para cada $i = 1, \ldots, m$. Então escrevendo $h := af + bg$, com $a, b \in \mathbb{F}_q$ temos que $v_{P_i}(h) = -w_i$.

□

Corolário 4.3.2. *Seja* $\boldsymbol{u} = (u_1, \ldots, u_m) \in \mathbb{N}_0^m$ *tal que* $\bigtriangledown_i(u) \neq \emptyset$ *para algum* i. *Dado* $s \in \mathbb{N}$ *com* $s < u_i$ *se* $\boldsymbol{w} := u(i) + se_i \in H_m$ *então* $\boldsymbol{u} \in H_m$.

Demonstração. Segue do Lema 4.3.2 que existe $\mathbf{v} = (v_1, \ldots, v_m) \in H_m$ tal que $v_i = u_i$ e $v_j \leqslant u_j$, para $j \neq i$. Então aplicando o lema anterior para $\mathbf{w}$ e $\mathbf{v}$ o resultado segue. □

Lema 4.3.5. *Sejam* $\boldsymbol{u} = (u_1, \ldots, u_r), \boldsymbol{v} = (v_1, \ldots, v_r) \in H_r$. *Se* $u_i = v_i$ *para algum* $i = 1, \ldots, r$ *então existe* $\boldsymbol{t} = (t_1, \ldots, t_r) \in H_r$ *satisfazendo as seguintes propriedades:*

a) $t_j = max\{u_j, v_j\}$ *para* $i \neq j$ *e* $u_j \neq v_j$.

b) $t_j \leqslant u_j$ *para* $i \neq j$ *e* $u_j = v_j$.

c) $t_j < u_j$ *ou* $t_j = u_j = 0$.

Demonstração. Basta tomar h como no Lema 4.3.4 e usar propriedades de valorização. □

Proposição 4.3.1. *Seja* $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}_0^m$ *tal que* $v(i) \in G_m$. *Denote* $b := min\{s \in \mathbb{N} | n(i) + se_i \in H_m\}$. *Então qualquer* $\boldsymbol{u} = (u_1, \ldots, u_m) \in \mathbb{N}_0^m$ *com* $u_i = b$ *e* $u_j = v_j = 0$ *ou* $u_j < v_j$ *pertence à* G_m. *Em particular,* $b \in H(P_i)$.

Demonstração. Suponha por absurdo que $\mathbf{u} \in H_m$. Aplicando o Lema 4.3.5 para $\mathbf{u}$ e $v(i) + be_i$ obtemos que $v(i) + re_i \in H_m$para algum $s \in \mathbb{N}$ com $r < b$, o que é uma contradição. □

Exemplo 4.3.2. *Considere a extensão de Kummer* $F/\mathbb{F}_q(x)$ *dada por*

$$y^m = \prod_{i=1}^{r} (x - a_i)^s,$$

Vimos alguns exemplos de divisores deste tipo no Exemplo 2.4.3. Se tomarmos $r = 7, s = 1$ *e* $m = 5$ *então* $y^5 = \prod_{i=1}^{7}(x - a_i)$. *Se* P_1 *é totalmente ramificado. Então*

$$\Gamma(P_\infty, P_1) = \{(1,21), (2,17), (3,8), (4,4), (6,16), (7,12), (8,3), (11,11), (12,7), (16,6), (17,2), (21,1)\}.$$

Em (Shudi e Hu 2016) é possível consultar a demonstração do próximo resultado.

Teorema 4.3.3. *Considere a extensão de Kummer $F/\mathbb{F}_q(x)$ dada por $y^m = \prod_{i=1}^{r}(x-a_i)^s$ com $mdc\{m,sr\} = 1$ e $a_i \in \mathbb{F}_q$. Se os zeros P_i associados à $(x-a_i)$ são totalmente ramificados, então*

$$\Gamma(P_\infty, P_1, \ldots, P_t) = \{(mc_0 - rj, mc_1 + j, \ldots, mc_t + j) |\ 1 \leqslant j \leqslant m-1-\lfloor\frac{m}{r}\rfloor, \\ c_i \geqslant 0,\ c_0 \geqslant \lceil\frac{rj}{m}\rceil,\ \sum c_i = r-t\}$$

Sobre a relação de ordem $\preceq$, vamos definir um lub. Considere $\mathbf{u}_1, \ldots, \mathbf{u}_s \in \mathbb{N}_0^m$ com $u_i = (u_{i_1}, \ldots, u_{i_m})$ definimos o *lub* de $\mathbf{u}_1, \ldots, \mathbf{u}_s$ (em ingles "least upper bound") como

$$lub(\mathbf{u}_1, \ldots, \mathbf{u}_s) = (max\{u_{1_1}, \ldots, u_{s_1}\}, \ldots, max\{u_{1_m}, \ldots, u_{s_m}\})$$

Para $\mathbf{v} = (v_1, \ldots, v_m) \in \mathbb{N}_0^m$ definimos o conjunto

$$\nabla_i(\mathbf{v}) := \{(u_1, \ldots, u_m) \in H_m |\ v_i = u_i\}.$$

Vemos imediatamente que $\bigtriangledown_i(\mathbf{v}) \supseteq \nabla_i(\mathbf{v})$.

Proposição 4.3.2. *Seja $\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}_0^m$. Estão $\boldsymbol{v} = min\nabla_i(\boldsymbol{v})$ para algum i com respeito à $\preceq$ se, e somente se, $\boldsymbol{v} = min\nabla_i(\boldsymbol{v})$ para todo i*

Demonstração. Seja u minimal em $\{(u_1, \ldots, u_m) \in H_m |\ v_i = u_i\}$ com relação à $\preceq$ para algum i. Sem perca de generalidade podemos assumir que $i = 1$. Suponha que existe j, com $j \geqslant 2$, tal que u não é minimal em $\{(u_1, \ldots, u_m) \in H_m |\ v_j = u_j\}$. então existe $\mathbf{v} \in H_m$ tal que $\mathbf{v} \preceq \mathbf{u}$, $\mathbf{v} \neq \mathbf{u}$ e $v_j = u_j$. Logo, existe $\mathbf{w} \in H_m$ satisfazendo $w_1 = u_1$, $w_j < u_j$ e $w_s \leqslant u_s$ para $j \neq s \geqslant 2$, mas isto contradiz a minimalidade de $\mathbf{u}$. Portanto, $\mathbf{u}$ é minimal para todo $j = 1, \ldots, m$. A reciproca é imediata. □

Proposição 4.3.3. *Se $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_s \in H_m$, então $lub(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_s) \in H_m$.*

Demonstração. Podemos provar o resultado repetindo o argumento realizado no Lema 4.3.4 da seguinte forma: defina $\mathbf{w}_2 = lub\{\mathbf{u}_1, \mathbf{u}_2\}$. Pelo Lema 4.3.4 temos que $w_2 \in H_m$. Definido $\mathbf{w}_i = lub\{\mathbf{w}_{i-1}, \mathbf{u}_i\}$ temos pelo Lema 4.3.4 que $\mathbf{w}_i \in H_m$. □

Definição 4.3.2. *Seja $\mathcal{X}$ uma curva sobre $\mathbb{F}_q$ e $P_1, \ldots, P_m$ pontos racionais de $\mathcal{X}$ distintos entre si. Denote $\Gamma(P_1) = H(P_1)$ se $m = 1$ e para m*

$$\Gamma(P_1, \ldots, P_m) := \{\boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}_0^m | \boldsymbol{v} = mim\nabla_i(\boldsymbol{v}), \textit{para algum } i\}.$$

Considere a condição: (A)

$$(u_{i_1},\ldots,u_{i_k}) \in \Gamma(P_{i_1},\ldots,P_{i_k}) \text{ para algum, } \{i_1,\ldots,i_k\} \subset \{1,\ldots,m\}$$
$$satisfazendo\ i_1 < \cdots < i_k\ e\ i_{k+1} = \cdots = i_\ell = 0,\ onde$$
$$\{i_{k+1},\ldots,i_m\} \subset \{1,\ldots,\ell\} \setminus \{i_1,\ldots,i_k\}$$

Teorema 4.3.4. *$H(P_1,\ldots,P_m)$ é completamente determinado por $\Gamma(P_1,\ldots,P_m)$. Em outras palavras,*

$$H(P_1,\ldots,P_m) = \{lub(u_1,\ldots,u_m) |\ u_i \in \Gamma(P_1,\ldots,P_m)\ ou\ satisfaz\ (A)\}.$$

Demonstração. Segue da Proposição 4.3.3 a inclusão $\supseteq$. Para mostrar a contraria, suponha $\mathbf{u} \in H_m \setminus \{lub(u_1,\ldots,u_m) |\ u_i \in \Gamma(P_1,\ldots,P_m)\ ou\ satisfaz\ (A)\}$. Sem perca de generalidade podemos supor que $\mathbf{u} = (u_1,\ldots,u_m) \in \mathbb{N}_0^m$. Então $\mathbf{u}$ não é minimal em $\{\mathbf{v} \in H_m |\ u_i = v_i\}$ para todo i. Logo, existem $w_1,\ldots,w_m$ tais que $\mathbf{u} = lub\{\mathbf{w}_1,\ldots,\mathbf{w}_m\}$ e $w_1,\ldots,w_m \in \{lub(\mathbf{u}_1,\ldots,\mathbf{u}_m) |\ u_i \in \Gamma(P_1,\ldots,P_m)\}$ ou satisfazem (A).

□

Definição 4.3.3. *O Conjunto $\Gamma(P_1,\ldots,P_m)$ é chamado de* conjunto minimal de geradores *de $H(P_1,\ldots,P_m)$*

Seja $\mathcal{X}$ um curva sobre $\mathbb{F}$. Um divisor $D \in Div(\mathcal{X})$ é chamado de *discrepância* para dois pontos racionais $P, Q \in \mathcal{X}$ se

$$\mathcal{L}(D) \neq \mathcal{L}(D-P) = \mathcal{L}(D-P-Q)\ e$$
$$\mathcal{L}(D) \neq \mathcal{L}(D-Q) = \mathcal{L}(D-P-Q)$$

Teorema 4.3.5. *Seja $\boldsymbol{u} = (u_1,\ldots,u_m) \in H(P_1,\ldots,P_m)$. Então $\boldsymbol{u} \in \Gamma(P_1,\ldots,P_m)$ se, e somente se, $D = u_1P_1 + \cdots + u_mP_m$ é uma discrepância para qualquer dois pontos de $\{P_1,\ldots,P_m\}$.*

Demonstração. Seja $\mathbf{u} = (u_1,\ldots,u_m) \in \Gamma(P_1,\ldots,P_m)$, então existe $f \in \mathbb{F}_q(\mathcal{X})$ tal que $\mathrm{div}(f)_\infty = u_1P_1 + \cdots + u_mP_m$. Considere $P_i, P_j \in K := \{P_1,\ldots,uP_m\}$com $i \neq j$. Se $\mathcal{L}(D) = \mathcal{L}(D-P_i)$, então $f \in \mathcal{L}(D-P_i)$, i.e., $\mathrm{div}(f) + D - P_i \geqslant 0$, o que é uma contradição. Portanto, $\mathcal{L}(D-P_i) \neq \mathcal{L}(D)$. Agora suponha que $\mathcal{L}(D-P_i-P_j) \neq \mathcal{L}(D-P_i)$, então existe $g \in \mathcal{L}(D-P_i) \setminus \mathcal{L}(D-P_i-P_j)$ satisfazendo $\mathrm{div}(g) + D - P_i \geqslant 0$. Desta forma

$$\mathrm{div}(g)_\infty = s_1P_1 + \cdots + s_{j-1}P_{j-1} + u_jP_j + s_{j+1}P_{j+1} + \cdots + s_mP_m,$$

com $s_i \leqslant u_i - 1$ e $s_k \leqslant u_k$ para $k \in \{1, \ldots, m\} \setminus \{i, j\}$.

Portanto, $(s_1, \cdots, s_{j-1}, u_j, s_{j+1}, s_m) \in \nabla_i(\mathbf{u})$ o que contradiz o fato de que u é minimal em $\in \nabla_i(\mathbf{u})$.

Reciprocamente, se $D = u_1 P_1 + \cdots + u_m P_m$ é uma discrepância com respeito $P_i, P_j \in K$ com $i \neq j$. Seja $h \in \mathbb{F}_q(\mathcal{X})$ tal que $\mathrm{div}(h)_\infty = u_1 P_1 + \cdots + u_m P_m$. Se $\mathbf{u} = (u_1, \ldots, u_m)$ não é minimal em $\nabla_i(\mathbf{u})$ para algum i, então existe $f_i \in \mathbb{F}_q(\mathcal{X})$ com $\mathrm{div}(f_i)_\infty = n_1 P_1 + \cdots + n_m P_m$. Se $\mathbf{n} = (n_1, \ldots, n_m)$, então $s \in \nabla_i(u)$ com $\mathbf{n} \neq \mathbf{u}$ e $\mathbf{n} \preceq \mathbf{u}$. Portanto, $f_i \in \mathcal{L}(D - P_j)$ e $f_i \notin \mathcal{L}(D - P_i)$, absurdo. □

Definição 4.3.4. *Seja* $\boldsymbol{u} = (u_1, \ldots, u_m) \in G(P_1, \ldots, P_m)$. *Dizemos que* $\boldsymbol{u}$ *é uma* lacuna pura *de* $G(P_1, \ldots, P_m)$ *se* $\ell\left(\mathcal{L}\left(\sum_{i=1}^{m} u_i P_i\right)\right) = \ell\left(\mathcal{L}\left(\sum_{i=1}^{m} u_i P_i - P_j\right)\right)$ *para cada* $j = 1, \ldots, m$.

Vamos relembrar alguns fatos sobre Curva GK: Considere $q = n^3$, para $n \geqslant 2$. A curva $\mathcal{GK}$ é definida pela equações

$$\begin{aligned} z^{n^2-n+1} &= y \sum_{i=0}^{n} (-1)^{i+1} x^{i(n-1)} \\ x^n + x &= y^{n+1}, \end{aligned}$$

definida sobre $\mathbb{F}_{q^2}$. O gênero de $\mathcal{GK}$ é dado por $g = \frac{(n^3+1)(n^2-2)}{2} + 1$ e possui um único ponto no infinito $P_\infty = (1 : 0 : 0)$. Outra propriedade interessante desta curva é que ela é uma curva maximal.

Vamos denotar por $P_j := (a_j, 0, 0) \in \mathcal{GK}(\mathbb{F}_{q^2})$ tais que $a_j^n + a_j = 0$, para $j = 1, \ldots, n$. $Q_j := (a_j, b_j, 0) \in \mathcal{GK}(\mathbb{F}_{q^2})$ tais que $a_j^n + a_j = b_j^{n+1}$ e $b_j \neq 0$, para $j = 1, \ldots, n^3 - n$. Usando as equações da curva $\mathcal{GK}$ podemos exibir funções satisfazendo

$$\begin{aligned} (z) &= \sum_{j=1}^{n^3-n} Q_j + \sum_{j=1}^{n} P_j - n^3 P_\infty \\ (y) &= \sum_{j=1}^{n} (n^2 - n + 1) P_j - (n^3 - n^2 + n) P_\infty \\ (x - a_j) &= (n^3 + 1)(P_j - P_\infty). \end{aligned}$$

Usando essas funções podemos provar que

$$H(P_\infty) = H(Q_i) = H(P_j) =< n^3 - n^2 + n, n^3 + 1, n^3 >,$$

para cada $i = 1, \ldots, n^3 - n$ e $j = 1, \ldots, n$.

Usando a notação acima, enunciamos o seguinte lema.

Lema 4.3.6. *Considere a curva $\mathcal{GK}$ sobre $\mathbb{F}^{q^2}$. Sejam a, b, c inteiros então*

$$\Gamma(P_\infty, P_1, \ldots, P_m) = \Gamma_{m+1},$$

onde

$$\Gamma_{m+1} := \{(n^2 - m - \sum_{s=1}^{m} j_s)c - ina - kb, j_1c + ia + k, \ldots, j_mc + ia + k)|$$

$$1 \leqslant k \leqslant a,\ 0 \leqslant i \leqslant n,\ j_s \geqslant 0 \text{ e } (n^2 - m - \sum_{s=1}^{m} j_s)c - ian - kb > 0\},$$

para $1 \leqslant m \leqslant n$.

Exemplo 4.3.3. *Usando a mesma notação do Exemplo 4.3.3 vamos calcular Γ_{m+1}. Seja $n = 2$ e considere $a = 3$, $b = 8$ e $c = 9$. Então a curva $\mathcal{GK}$ possui gênero 10 e $H(P_\infty) =< 6, 8, 9 >$. Usando o lema anterior para $m = 1$ temos que*

$$\Gamma_2 = \{9(3 - j_1) - 6i - 8k, 9j_1 + 3i + k)|i = 1, 2,\ k = 1, 2, 3, j_1 \geqslant 0$$
$$e\ 9(3 - j_1) - 6i - 8k \geqslant 0\} =$$
$$\{(1, 19), (2, 11), (3, 3), (4, 13), (5, 5), (7, 7), (10, 10), (11, 2), (13, 4), (19, 1)\}.$$

Ainda sobre a curva enunciamos o resultado a seguir onde é possível calcular lacunas puras.

Proposição 4.3.4. *Para $2 \leqslant k \leqslant a$, o vetor $((n^2 - m)c - kb, k, \ldots, k, k - 1)$ é uma lacuna pura de $\mathcal{GK}$ $P_\infty, P_1, \ldots, P_m$.*

Exemplo 4.3.4. *Considere a curva Hermitiana $y^8 + y = x^9$ definida sobre $\mathbb{F}_{64}$. Sejam P_∞ e P_0 o polo e zero em comum das funções x e y. Sabemos que $\mathcal{H}_8(P_\infty) =< 8, 9 >$. Então*

$$\Gamma(P_\infty, P_0) = A \cup \{(u,0),(0,u) | u \in \mathcal{H}_8(P_\infty)\},$$

onde

$$A := \{(1,55),(2,47),(3,39),(4,31),(5,23),(6,15),(7,7),(10,46),(11,38),(12,30),(13,22),(14,14),(15,6),(19,37),(20,29),(21,21),(22,13),(23,5),(28,28),(29,20),(30,12),(31,4),(37,19),(38,11),(39,3),(46,10),(47,2),(55,1)\}.$$

No caso geral enunciamos o seguinte Teorema.

Teorema 4.3.6. *Seja $y^q + y = x^{q+1}$ a curva Hermitiana $\mathcal{H}_q$ definida sobre $\mathbb{F}_{q^2}$. Considere os pontos racionais P_∞ e $P_i = P_{ab_i}$ de $\mathcal{H}_q$ onde $a, b_i \in \mathbb{F}_{q^2}$ com a fixado e $b_i^q + b_i = a^{q+1}$ (note que P_i denota o zero em comum das funções $x - a$ e $y - b_i$) $i = 2, \ldots, q+1$. Então $\mathcal{H}_q(P_\infty, P_2, \ldots, P_{q+1})$ é gerado pelo conjunto*

$$\Gamma = \{u = (u_1, \ldots, u_m) \in \mathbb{N}_0^m | u = (u_{i_1}, \ldots, u_{i_l}) \in S_m \text{ com } u_{i_r} = 0, \text{ para } r = l+1, \ldots, m \text{ para algum } l \in \{1, \ldots, m\},$$

onde

$$S_m := \{((q+1)(u_1 - j) + j, \ldots, (q+1)(u_m - j) + j) \in \mathbb{N}_0^m | \sum u_i = q + (m-1)(j-1),\ 1 \leqslant j \leqslant u_i \leqslant q-1,\ \forall i = 1, \ldots, m\}.$$

Sobre $H(P_1, \ldots, P_m)$ podemos obter através dos resultados anteriores informações sobre AG códigos. Para isso vamos fixar uma notação. Seja $\mathcal{X}$ uma curva definida sobre $\mathbb{F}_q$. Considere $m \in \mathbb{N}$ tal que $q > m$. Suponha que $Q_1, \ldots, Q_n$, $P_1, \ldots, P_m$ pontos racionais de $\mathcal{X}$ dois à dois distintos. Sejam $\mathbf{u} = (u_1, \ldots, u_m)$, $\mathbf{v} = (v_1, \ldots, v_m) \in \mathbb{N}_0^m$, defina o divisor $D := Q_1 + \cdots + Q_n$ e $G := (u_1 + v_1 - 1)P_1 + \cdots + (u_m + v_m - 1)P_m$. Consideramos o AG código $\mathcal{C}_\Omega(D, G)$.

Lema 4.3.7. *Sejam B, E, L e M divisores em $\mathcal{X}$ com B, E divisores efetivos. Se as condições:*

a) $E + L + M$ é um divisor canônico,

b) $\ell(L) = \ell(L + B)$,

c) $\ell(M - B) = \ell(M)$

são satisfeitas, então $Deg(B) \leqslant Deg(E)$.

Teorema 4.3.7. *Considere uma curva* $\mathcal{X}$ *de gênero* g *e o* $[n, k, d]$*−código* $\mathcal{C}_{\Omega}(D, G)$. *Se* $\boldsymbol{u} = (u_1, \ldots, u_m), \boldsymbol{v} = (v_1, \ldots, v_m)$ *são lacunas de Weierstrass puras em* $P_1, \ldots, P_m$ *então* $d \geqslant Deg(G) - 2g + m + 2$.

Demonstração. Considere os divisores

$$E = \operatorname{div}(\eta) - G + \sum_{i=1}^{m} P_i$$

$$L = \sum_{i=1}^{m} (u_i - 1) Q_i$$

$$M = \sum_{i=1}^{m} v_i Q_i - \sum_{i=1}^{w} P_i,$$

onde $\eta \in \Omega(G - D)^{\times}$, com $res(\eta) \neq 0$, para $i = 1, \ldots, w$. Defina o divisor $B := \sum_{i=1}^{m} Q_i$. Como $\ell(L) = \ell(L+B), \ell(B) = \ell(M-B)$ e $E+L+M = \operatorname{div}(\eta)$ é um divisor canônico, portanto $Deg(B) \leqslant deg(E)$ e o resultado segue. □

Se impormos condições adicionais, podemos melhorar a cota anterior.

Teorema 4.3.8. *Sejam* $\boldsymbol{w} = (w_1, \ldots, w_m), \boldsymbol{u} = (u_1, \ldots, u_m), \boldsymbol{v} = (v_1, \ldots, v_m) \in \mathbb{N}_0^m$ *tais que* $u_i \leqslant w_i \leqslant v_i$ *para cada* $i = 1, \ldots, m$ *são lacunas de Weierstrass puras em* $P_1, \ldots, P_m$ *então*

$$d \geqslant Deg(G) - 2g + m + 2 + \sum_{i=1}^{m} (v_i - u_i).$$

Demonstração. Os passos da demonstração são análogos ao do teorema anterior, basta considerar aqui o divisor $B := \sum_{i=1}^{m} (v_i - u_i - +1) Q_i$. □

Exemplo 4.3.5 ((Matthews e Peachey 2010))**.** *Seja* $\mathbb{F}_{27} = \mathbb{F}_3(w)$, *onde* $w^3 - w + 1 = 0$. *A curva norma-traço sobre* $\mathbb{F}_{27}$ *é dada pela equação* $y^9 + y^3 + y = x^{13}$.

Esta curva possui exatamente 9 places da forma $P_i = P_{0a_i}$, *onde* $a_0 = 0, a_1 = 1, a_2 = 2$, $a_3 = w$, $a_4 = w^3$, $a_5 = w^9$, $a_6 = w^{14}$, $a_7 = w^{16}$, $a_8 = w^{22}$. *Após alguns cálculos obtemos*

$$G(P_\infty) = \{1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 15, 16, 17, 19, 20, 21, 23, 24, 25, 28, 29, 30, 32, 33, 34, 37, 38, 41, 42, 43, 46, 47, 50, 51, 55, 56, 59, 60, 64, 68, 69, 73, 77, 82, 86, 95\},$$

onde P_∞ *é o ponto no infinito da curva norma-traço. Ainda*

$$G(P_i) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 27, 28, 29, 30, 31, 32, 33, 34, 40, 41, 42, 43, 44, 45, 46, 53, 54, 55, 56, 57, 66, 67, 68, 69, 79, 80, 92\}.$$

E portanto

$$\Gamma(P_\infty, P_2) = \{(1, 23), (2, 46), (3, 69), (4, 92), (5, 11), (6, 34), (7, 57), (8, 80), (10, 22), (11, 45), (12, 68), (14, 10), (15, 33), (16, 56), (17, 79), (19, 21), (20, 44), (21, 67), (23, 9), (24, 32), (25, 55), (28, 20), (29, 43), (30, 66), (32, 8), (33, 31), (34, 54), (37, 19), (38, 42), (41, 7), (42, 30), (43, 53), (46, 18), (47, 41), (50, 6), (51, 29), (55, 17), (56, 40), (59, 5), (60, 28), (64, 16), (68, 4), (69, 27), (73, 15), (77, 3), (82, 14), (86, 2), (95, 1)\}.$$

A ideia de semigrupos de Weierstrass em uma $m-$upla $(P_1, \ldots, P_m)$ possui uma generalização. Tal generalização é definida da seguinte forma: Sejam $\mathcal{X}$ uma curva definida sobre $\mathbb{F}_q$ e $\mathbb{F}_q(X)$ o corpo de funções associado à $\mathcal{X}$, considere $P_1, \ldots, P_m \in X$ pontos racionais dois à dois distintos. Denotaremos por $\mathcal{R}(P_1, \ldots, P_m)$ o anel de funções de $\mathcal{X}$ que só possuem polos em $P_1, \ldots, P_m$. Então o *semigrupos de Weierstrass generalizado* na $m-$upla $P_1, \ldots, P_m$ é definido por

$$\overline{H}(P_1, \ldots, P_m) := \left\{(-v_{P_1}(h), \ldots, -v_{P_m}(h)) \in \mathbb{Z}^m \mid h \in \mathcal{R}(P_1, \ldots, P_m)\right\},$$

onde v_{P_i} é a valorização associada à P_i.

Teorema 4.3.9. $\overline{H}(P_1, \ldots, P_m)$ *é um subsemigrupo aditivo de* $\mathbb{Z}^m$.

Demonstração. Exercício. □

Os semigrupos $\overline{H}(P_1, \ldots, P_m)$ e $H(P_1, \ldots, P_m)$ se relacionam da seguinte forma:

$$H(P_1, \ldots, P_m) = \overline{H}(P_1, \ldots, P_m) \cap \mathbb{N}_0^m.$$

Onde esta relação justifica o termo generalizado, uma vez que podemos obter o clássico através do $\overline{H}(P_1, \ldots, P_m)$.

Sejam $\mathbf{u} = (u_1, \ldots, u_m) \in \mathbb{Z}^m$ e $i = 1, \ldots, m$. Definimos o conjunto

$$\nabla_i^m(\mathbf{u}) := \left\{ v = (v_1, \ldots, v_r) \in \overline{H}(P_1, \ldots, P_m) |\, u_i = v_i \text{ e } u_j \leqslant v_j, \forall\, j \neq i \right\}.$$

Proposição 4.3.5. *Sejam $\boldsymbol{u} = (u_1, \ldots, u_m) \in \mathbb{Z}^m$ e $D = u_1 P_1 + \cdots + u_m P_m$ $(q \geqslant m)$. Então*

a) $\boldsymbol{u} \in \overline{H}(P_1, \ldots, P_m) \Leftrightarrow \ell(\boldsymbol{u}) = \ell(u - e_i) + 1$ *para cada* $i = 1, \ldots, m$.

b) $\nabla_i^m(\boldsymbol{u}) = \emptyset \Leftrightarrow \ell(\boldsymbol{u}) = \ell(u - e_i)$.

Demonstração. a) Se $\mathbf{u} \in \overline{H}(P_1, \ldots, P_m)$, então então existe $f \in \mathcal{R}(P_1, \ldots, P_m)$ tal que $v_{P_i}(f) = -u_i$ para cada $i \in I = \{1, \ldots, m\}$. Então, $f \in \mathcal{L}(\mathbf{u}) \setminus \mathcal{L}(\mathbf{u} - e_i)$ e, portanto $\ell(\mathbf{u}) - 1 = \ell(\mathbf{u} - e_i)$, para cada $i \in I$.

Reciprocamente, se $\ell(\mathbf{u}) - 1 = \ell(\mathbf{u} - e_i)$, para cada $i \in I$, existe $h_i \in \mathcal{L}(\mathbf{u}) \setminus \mathcal{L}(\mathbf{u} - e_i)$, para cada $i \in I$. Assim, $v_{P_i}(h_i) = -u_i$ e $v_{P_j}(h_i) = -u_j$ para $i \neq j$. Dado $v = (v_1, \ldots, v_m) \in \mathbb{F}_q^m$ definimos $h = \sum_{i=1}^{m} v_i h_i$. Como $q \geqslant m$ segue que $v_{P_i}(h) = -v_i$.

b) Basta notar que $h_i \in \mathcal{L}(\mathbf{u}) \setminus \mathcal{L}(\mathbf{u} - e_i) \Leftrightarrow (-v_{P_1}(f), \ldots, -v_{P_m}(f)) \in \nabla_i^m(\mathbf{u})$.

□

Como consequência do resultado anterior temos que $\mathbf{u} \in \overline{H}(P_1, \ldots, P_m)$, sempre que sua norma é maior que o dobro do gênero da curva, i.e., $|\mathbf{u}| \geqslant 2g$.

Sejam $\mathbf{u} = (u_1, \ldots, u_m) \in \mathbb{Z}^m$ e $\emptyset \neq J \subsetneq \{1, \ldots, m\}$. Definindo o conjunto

$$\nabla_J(\mathbf{u}) := \left\{ \mathbf{v} = (v_1, \ldots, v_r) \in \overline{H}(P_1, \ldots, P_m) |\, u_i = v_i \text{ e } u_j < v_j, \forall i \notin J \right\}$$

dizemos que $\mathbf{v} = (v_1, \ldots, v_r) \in \overline{H}(P_1, \ldots, P_m)$ é *absolutamente maximal* se $\nabla_J(\mathbf{v}) = \emptyset$ para todo $\emptyset \neq J \subsetneq \{1, \ldots, m\}$. Denotaremos o conjunto de todos os elementos absolutamente maximais de $\overline{H}(P_1, \ldots, P_m)$ por $\Lambda(P_1, \ldots, P_m)$.

Proposição 4.3.6. *Sejam $\boldsymbol{u} = (u_1, \ldots, u_m) \in \mathbb{Z}^m$ e $D = u_1P_1 + \cdots + u_mP_m$ $(q \geqslant m)$. As seguintes afirmações são equivalentes:*

a) $\boldsymbol{u} \in \Lambda(P_1, \ldots, P_m)$.

b) $\nabla_i^m(\boldsymbol{u}) = \{\boldsymbol{u}\}$ *para todo* $i \in \{1, \ldots, m\}$

c) $\nabla_i^m(\boldsymbol{u}) = \{\boldsymbol{u}\}$ *para algum* $i \in \{1, \ldots, m\}$

d) $\ell(D) = \ell(D - \sum_{i=1}^m P_i) + 1$.

Demonstração. $a) \Rightarrow b)$: como $\mathbf{u} \in \overline{H}(P_1, \ldots, P_m)$, então $\{\mathbf{u}\} \subset \nabla_i^m(\mathbf{u})$, para todo $i \in I = \{1, \ldots, m\}$. Se $\mathbf{w} \in \nabla_i^m(\mathbf{u})$ com $\mathbf{w} \neq \mathbf{u}$, então existe $J \subsetneq I$ o que contradiz $a)$.

$b) \Rightarrow c)$: é imediato.

$c) \Rightarrow d)$: é suficiente mostrar que $\nabla_i^m(u - \mathbf{1} - 1_J) = \emptyset$ (onde $\mathbf{1}$ denota o vetor $(1, \ldots, 1)$ e 1_{J^c} denota a $m-$upla tendo $1-$ésima coordenada se $j \in J$ e 0 caso contrário, e $e_i = 1_{\{1\}}$). Uma vez que

$$\nabla_i^m(\mathbf{u} - \mathbf{1} - 1_J) \subset \nabla_i^m(\mathbf{u}) = \{\mathbf{u}\}$$

e $\mathbf{u} \notin \nabla_i^m(\mathbf{u} - \mathbf{1} - 1_J)$ concluímos que $\nabla_i^m(u - \mathbf{1} - 1_J) = \emptyset$.

$d) \Rightarrow a)$: Note que $\ell(\mathbf{u} - e_i) = \ell(\mathbf{u} - \mathbf{1})$ para todo $i \in I$. Se $\nabla_J^m(\mathbf{u})$, para algum $\emptyset \neq J \subset I$, então

$$\ell(\mathbf{u} - e_i) \geqslant \ell(\mathbf{u} - \mathbf{1}) + 1,$$

o que é uma contradição. □

Para o próximo resultado vamos fixar a seguinte notação: $v_{P_1,\ldots,P_m}(h) = (-v_{P_1}(h), \ldots, -v_{P_m}(h))$.

Teorema 4.3.10. $\overline{H}(P_1, \ldots, P_m) = \{lub(u_1, \ldots, u_m) | \, u_1, \ldots, u_m \in \Lambda(P_1, \ldots, P_m)\}$.

Demonstração. Começamos observando que $lub(u_1, u_2) \in \overline{H}(P_1, \ldots, P_m)$ para $u_1, u_2 \in \Lambda(P_1, \ldots, P_m)$. Logo existem $f, g \in \mathcal{R}(P_1, \ldots, P_m)$ funções tais que $\mathrm{div}(f)_\infty = \sum_{i=1}^m u_{1_i} P_i$ e $\mathrm{div}(g)_\infty = \sum_{i=1}^m u_{2_i} P_i$. Como $\#(\mathbb{F}_q) \geqslant m$ temos que $v_{P_1,\ldots,P_m}(h) = lub(u_1, u_2)$, onde $h = af + bg$ com $a, b \in \mathbb{F}_q$. Finalmente, basta repetir o processo de forma indutiva. □

Exemplo 4.3.6. *Considere a curva $\mathcal{X}$ dada pela equação $y^3 + y = x^{28}$ definida sobre $\mathbb{F}_{3^6}$. Escrevendo os pontos racionais da curva como $P_{b_j} = (0 : b_j : 1)$ com $b_j \in \mathbb{F}_{3^6}$ tais que $b_j + b_j^3 = 0$ ($j = 1, 2, 3$) e P_∞ o ponto no infinito. Temos que*

$$\{(0,0,0), (25,1,1), (22,2,2), (19,3,3), (16,4,4), (13,5,5),$$
$$(10,6,6), (7,7,7), (4,8,8), (1,9,9),$$
$$(-2,10,10), (-5,11,11), (-8,12,12), (-11,13,13), (-14,14,14),$$
$$(-17,15,15), (-20,16,16), (-23,17,17), (-26,18,18),$$
$$(-29,19,19), (-32,20,20), (-35,21,21), (-38,22,22), (-41,23,23), (-44,24,24),$$
$$(-47,25,25), (-50,26,26), (-53,27,27), (-28,28,0), (0,-28,28)\}$$

gera $\overline{H}(P_\infty, P_0, P_{w^{546}})$, onde w^{546} é uma raiz primitiva de $\mathbb{F}_{3^6}$.

Para o caso particular em que $m = 1, 2$ obtemos $\overline{H}(P)$ ou $\overline{H}(P, Q)$. Vamos estudar estes dois casos particulares.

Se $m = 1$, podemos obter um cota para a distância mínima do código $\mathcal{C} = C(\mathcal{L}, D, aP)$.

Sobre códigos racionais, temos o seguinte resultado.

Teorema 4.3.11. *Sejam $n|(q^m - 1)$ e α uma raiz $n-$ésima da unidade de $\mathbb{F}_q^m$ e $F = \mathbb{F}_{q^m}(x)$. Vamos denotar P_0 o zero de z e P_∞ o polo de x, P_i o zero de $(x - \alpha^{i-1})$ para $i = 1, \ldots, n$. Definindo o divisor $D = \sum_{i=1}^{n} P_i$ e tomando inteiros a e b tais que $0 \leqslant a + b < n - 1$ temos que*

a) $C(\mathcal{L}, D, aP_0 + bP_\infty) = C(n, l, \delta)$.

b) o dual de $C(\mathcal{L}, D, aP_0 + bP_\infty)$ é o código $C(\mathcal{L}, D, -(a+1)P_0 + (n-b-1)P_\infty)$.

Demonstração. a) Basta notar que $x^a a^i$ forma uma base para $\mathcal{L}(aP_0 + bP_\infty)$ e escrever $l = -a$, $\delta = a + b + 2$.

b) Considere as funções

$$z = x^{-n} \text{ e}$$
$$f(x) = (x-1)\cdots(x-\alpha^{n-1}).$$

Então, $D-(aP_0+bP_\infty)+\mathrm{div}(z)+[\mathrm{div}(h'(x)-h(x))]-2P_\infty=(-a-1)P_0+(n-b-1)P_\infty$. Fazendo, $l=-a$ e $\delta=a+b+2$ o resultado segue.

□

A demonstração dos próximos resultados será omitida. O leitor que desejar pode consultá-los em (Martínez-Moro, Munuera e Ruano 2008).

Teorema 4.3.12. *Seja* $G=((q+1)(q-2)+a(q+1)-b)P$ *Então*

$$d(C(\mathcal{L},D,G))=\begin{cases}a(q+1)-b, & se\ b\leqslant a\\ a(q+1)-a, & se\ b>a.\end{cases}$$

Seja $\mathcal{X}$ uma curva definida sobre $\mathbb{F}_q$ com $P,Q\in X$ dois pontos racionais distintos. Para $m=2$ temos o semigrupo $\overline{H}(P,Q)$. Notamos que para um função $x\in X(\mathbb{F}_q)$ onde P é único polo e Q seu o único zero, teremos que o espaço de Riemann–Roch $\mathcal{L}(aP+bQ)=<x^{-b},\ldots,x^a>$. Desta forma, vamos denotar $P_\infty:=P$, $P_0:=Q$ e $G:=aP_\infty+bP_0$ o divisor dado pelo polo e zero de $\mathcal{X}$.

Sobre os pontos P_∞ e P_0 podemos definir o seguinte conjunto:

$$\Gamma(P_\infty,P_0):\left\{(a,b)\in\overline{H}(P_\infty,P_0)|(a,b)\text{ é minimal em }\overline{H}(P_\infty,P_0)\right\}.$$

Vamos calcular $\Gamma(P_\infty,P_0)$ para a curva Hermitiana $y^q+y=x^{q+1}$ sobre $\mathbb{F}_{q^2}$. Considere $a_0,a_1=0,1,\ldots,q$.

Teorema 4.3.13. *Seja* $G=K+aP_\infty+bP_0\geqslant K+P_\infty+P_0$*, com K um divisor canônico. Considere* $a=a_0(q+1)-a_1$*, para* $0\leqslant a_1\leqslant q$ *e* $b=b_0(q+1)-b_1$*, para* $0\leqslant b_1\leqslant q$*. Denotando* $d=d(\mathcal{C}_\Omega(G,D))$ *temos:*

a) se $a_1,b_1\leqslant a_0+b_0$ *então* $d=a+b$

b) se $b_1\leqslant a_0+b_0\leqslant a_1$ *então* $d=a+b+a_1-(a_0+b_0)$

c) se $a_1\leqslant a_0+b_0\leqslant b_1$ *então* $d=a+b+b_1-(a_0+b_0)$

d) se $a_0+b_0\leqslant a_1\leqslant b_1$ *e* $a_1<q$ *então* $d=a+b+a_1+b_1-2(a_0+b_0)$

e) se $a_0+b_0\leqslant b_1\leqslant a_1$ *e* $b_1<q$ *então* $d=a+b+a_1+b_1-2(a_0+b_0)$

f) se $a_0+b_0\leqslant b_1=a_1=q$ *então* $d=a+b+q-(a_0+b_0)$

Corpos Algébricos

Sabemos que, um corpo, como o corpo real $\mathbb{R}$ ou o corpo dos complexos $\mathbb{C}$, tem duas operações básicas, são elas: a adição e a multiplicação. Nessa parte nosso objetivos é definir essas propriedades de maneira geral e exibir algumas propriedades sobre corpos finitos.

Definição .0.5. *Um* corpo algébrico *(ou simplesmente um* corpo*) é um conjunto não vazio* $\boldsymbol{F}$ *com duas operações* " $*$ " *e* " $+$ " *chamadas: multiplicação e adição respectivamente. Tais operações devem satisfazer as seguintes propriedades: para quaisquer* $a, b, c, d \in \boldsymbol{F}$

1. $a + b \in \boldsymbol{F}$*;*
2. $a * b \in \boldsymbol{F}$*;*
3. $a + b = b + a$ *e* $c * d = d * c$ *(comutatividade);*
4. $(a + b) + c = a + (b + c)$ *e* $(a * b) * c = a * (b * c)$ *(associatividade);*
5. $(a + b) * c = a * c + b * c$ *(distributividade).*

Lema .0.8. *Seja* $\boldsymbol{F}$ *um corpo. Então para quaisquer* $a, b \in \boldsymbol{F}$

a) $a + 0 = a$*;*

b) $a * 1 = a$*;*

c) $\forall a \in \boldsymbol{F}$ *existe* $-a \in \boldsymbol{F}$ *tal que* $a + (-a) = 0$*;*

d) $\forall 0 \neq a \in \boldsymbol{F}$ *existe* $^{-1}a \in \boldsymbol{F}$ *tal que* $a * (a^{-1}) = 1$*;*

e) $a * b = 0$ *então* $a = 0$ *ou* $b = 0$*.*

f) $(-1) * a = -a$*.*

Dados dois inteiros x, m com $m \geqslant 1$ temos pelo algoritmo da divisão que $x = mq + r$ com $0 \leqslant r \leqslant m - 1$.

Definição .0.6. *Sejam* x*,* y *e* m *inteiros com* $m \geqslant 1$*. Dizemos que* x*,* y *são* congruentes modulo m *se* $x - y = mq$ *para algum inteiro* q *e, denotamos por* $x \equiv_m y$*.*

Lema .0.9. *Se* $x \equiv_m y$ *e* $z \equiv_m w$*, então*

a) $x + z \equiv_m y + w$

b) $x - z \equiv_m y - w$

c) $x * z \equiv_m y * w$

Com essas operações $\mathbb{Z}_m := \frac{\mathbb{Z}}{m\mathbb{Z}}$ é um anel.

Teorema .0.14. $\mathbb{Z}_m$ *é um corpo* $\Leftrightarrow$ m *é primo.*

A *característica* de um corpo é definida como sendo p o menor inteiro positivo tal que $1 * p = 0$. Denotamos a característica de um corpo $\mathbf{F}$ por Char($\mathbf{F}$)

Proposição .0.7. *Se* p *é a característica de um corpo, então* p *é zero ou um primo.*

Teorema .0.15. *Seja* $\boldsymbol{F}$ *um corpo finito, com* Char($\boldsymbol{F}$) $= p$*. Então* $\sharp(\boldsymbol{F}) = p^n$*, para algum número natural* $n \geqslant 1$*.*

Proposição .0.8. *Se* $\sharp(\boldsymbol{F}) = q$ *então para todo* $a \in \boldsymbol{F}$ *temos que* $a^q = a$*.*

Note que se $p(x) \in \mathbf{F}[x]$ é um polinômio de grau m e irredutível. Se a é uma raiz de $p(x)$ então o conjunto

$$\mathbf{F}[a] := \frac{\mathbf{F}[x]}{p(x)} = \{b_0 + b_1 a + ... + b_{m-1}a^{m-1} \mid b_i \in \mathbf{F}\}$$

é um corpo finito.

Definição .0.7. *Seja* $\alpha \in \boldsymbol{F}_{q^n}$. *Um* polinômio minimal *com relação à* $\boldsymbol{F}_q$ *é um polinômio mônico de menor grau* $p(x) \in \boldsymbol{F}_q[x]$ *tal que* α *é uma raiz de* $p(x)$

Teorema .0.16. *As seguintes afirmações são verdadeiras:*

a) O polinômio minimal (de um elemento de $\alpha \in \boldsymbol{F}_{q^n}$*) com relação à* $\boldsymbol{F}_q$ *existe e é único.*

b) Todo polinômio minimal é irredutível.

Lema .0.10. *Para cada* $a, b \in \boldsymbol{F}$ *com* $\mathrm{Char}(\boldsymbol{F}) = p > 0$ *e* $n \in \mathbb{N}$ *temos que*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Para mais detalhes e propriedades veja (San Ling 2004) , (Gonçalves 2017).

Álgebra Linear

Os objetos fundamentais de estudo em álgebra linear são espaços vetoriais e transformações lineares. Aqui vamos definir o que é um espaço vetorial e transformações lineares, além de enunciar algumas propriedades.

Definição .0.8. *Seja $\boldsymbol{F}$ um corpo. Um conjunto não vazio V é um* espaço vetorial *sobre $\boldsymbol{F}$ ($\boldsymbol{F}$-espaço vetorial) se possui duas aplicações, soma $+ : V \times V \to V$ e multiplicação por escalar $\cdot : \boldsymbol{F} \times V \to V$ satisfazendo: para cada $\boldsymbol{v}, \boldsymbol{u}, \boldsymbol{w} \in V$ e $a, b \in \boldsymbol{F}$*

1. $\boldsymbol{v} + \boldsymbol{u} = \boldsymbol{u} + \boldsymbol{v}$;
2. $(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w})$;
3. *Existe* $\boldsymbol{0} \in V$ *tal que* $\boldsymbol{u} + \boldsymbol{0} = \boldsymbol{u}$ *(vetor nulo);*
4. *Existe* $-\boldsymbol{u} \in V$ *tal que* $\boldsymbol{u} + (-\boldsymbol{u}) = \boldsymbol{0}$ *(vetor inverso aditivo);*
5. $a(\boldsymbol{u} + \boldsymbol{v}) = a\boldsymbol{u} + a\boldsymbol{v}$;
6. $(a + b)\boldsymbol{u} = a\boldsymbol{u} + b\boldsymbol{u}$;
7. $a(b\boldsymbol{u}) = (ab)\boldsymbol{u}$;
8. $1 \cdot \boldsymbol{u} = \boldsymbol{u}$.

Lema .0.11. *Sejam $\boldsymbol{F}$ um corpo e V $\boldsymbol{F}$-espaço vetorial. As seguintes afirmações são verdadeiras:*

a) O vetor nulo é único.

b) O vetor inverso é único.

c) $0 \cdot \boldsymbol{u} = \boldsymbol{0}$*, para todo* $\boldsymbol{u} \in V$.

d) $(-1) \cdot \boldsymbol{u} = -\boldsymbol{u}$*, para todo* $\boldsymbol{u} \in V$.

Definição .0.9. *Um subconjunto não vazio* W *de* V *é dito um* $\boldsymbol{F}$*-subespaço vetorial de* V *se:*

1. $\boldsymbol{u} + \boldsymbol{v} \in W$,
2. $a \cdot \boldsymbol{u} \in V$*, para cada* $\boldsymbol{u}, \boldsymbol{v} \in V$ *e* $a \in \boldsymbol{F}$.

Definição .0.10. *Sejam* $\boldsymbol{F}$ *um corpo e* V $\boldsymbol{F}$*-espaço vetorial. Considere* $\boldsymbol{v}_1, ..., \boldsymbol{v}_n \in V$*, uma combinação linear é um vetor da seguinte forma:*

$$\boldsymbol{w} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n,$$

onde $a_1, ..., a_n \in \boldsymbol{F}$.

Vamos denotar por $[\mathbf{v}_1, ..., \mathbf{v}_n]$ o conjunto de todas combinações lineares dos vetores $\mathbf{v}_1, ..., \mathbf{v}_n$.

Teorema .0.17. *Sejam* $\boldsymbol{F}$ *um corpo,* V $\boldsymbol{F}$*-espaço vetorial e* $\boldsymbol{v}_1, ..., \boldsymbol{v}_n \in V$*. Então* $[\boldsymbol{v}_1, ..., \boldsymbol{v}_n]$ *é um* $\boldsymbol{F}$*-subespaço vetorial de* V.

Dizemos que $\mathbf{v}_1, ..., \mathbf{v}_n$ *gera* o espaço $[\mathbf{v}_1, ..., \mathbf{v}_n]$.

Definição .0.11. *Sejam* $\boldsymbol{F}$ *um corpo,* V $\boldsymbol{F}$*-espaço vetorial e* $\boldsymbol{v}_1, ..., \boldsymbol{v}_n \in V$*. Dizemos que* $\boldsymbol{v}_1, ..., \boldsymbol{v}_n$ *é* linearmente independente *sobre* $\boldsymbol{F}$ *(ou simplesmente l.i.) se sempre que tivermos uma combinação linear sendo o vetor nulo, então todos os escalares são nulos. Em outras palavras, se*

$$a_1\boldsymbol{v}_1 + ... + a_n\boldsymbol{v}_n = 0 \tag{3}$$

então $a_1 = ... = a_n = 0$.

Caso em 3 tenhamos algum escalar não nulo, dizemos que $\mathbf{v}_1, ..., \mathbf{v}_n$ é *linearmente dependente* (ou simplesmente l.d.).

Definição .0.12. *Sejam* $\boldsymbol{F}$ *um corpo,* V $\boldsymbol{F}$*-espaço vetorial e* $\boldsymbol{v}_1, ..., \boldsymbol{v}_n \in V$*. Dizemos que* $\boldsymbol{v}_1, ..., \boldsymbol{v}_n$ *é uma* base *de* V *se* $V = [\boldsymbol{v}_1, ..., \boldsymbol{v}_n]$ *e* $\boldsymbol{v}_1, ..., \boldsymbol{v}_n$ *são linearmente independente.*

A quantidade de vetores que formam uma base para um espaço vetorial é chamado *dimensão* de V e, é denotada por $\dim(V)$.

Uma **F**-espaço vetorial V é dito ser de dimensão finita sobre **F**, se a quantidade de vetores na sua base é finita. Caso contrário é chamado de dimensão infinita.

Teorema .0.18. *Sejam $\boldsymbol{F}$ um corpo, V $\boldsymbol{F}$-espaço vetorial e $\boldsymbol{v}_1, ..., \boldsymbol{v}_n$ uma base de V. Se $\boldsymbol{w}_1, ..., \boldsymbol{w}_m$ é outra base de V, então $m = n$.*

Proposição .0.9. *Todo subespaço de um espaço vetorial de dimensão finita possui dimensão finita.*

Seja V um **F**-espaço vetorial com base $\mathbf{v}_1, ..., \mathbf{v}_n$. Sabemos que todo elemento $\mathbf{u}$ de V pode ser escrito de maneira única como combinação linear dos elementos da base de V da forma $\mathbf{u} = a_1\mathbf{v}_1 + ... + a_n\mathbf{v}_n$, com $a_i \in \mathbf{F}$. Com esta escrita podemos denotar $\mathbf{u} = (a_1, ..., a_n)$.

Definição .0.13. *Seja V um $\boldsymbol{F}$-espaço vetorial de dimensão m. Sejam $\boldsymbol{u} = (\boldsymbol{u}_1, ..., \boldsymbol{u}_m), v = (\boldsymbol{v}_1, ..., \boldsymbol{v}_m) \in V$. O* produto interno *de u por v é definido como:*

$$< \boldsymbol{u}, \boldsymbol{v} >:= \sum_{i=1}^{m} u_i v_i .$$

Dois vetores $\mathbf{u}, \mathbf{v} \in V$ são ditos *ortogonais* se $< \mathbf{u}, \mathbf{v} >= 0$. Seja $W \subset V$ um subespaço vetorial. Então o conjunto de todos os vetores ortogonais à W é denotado por

$$W^{\perp} := \{\mathbf{v} \in V | \ < \mathbf{v}, \mathbf{w} >= 0, \forall w \in W\}.$$

O conjunto $W^{\perp}$ é um subespaço vetorial de V.

Definição .0.14. *Sejam U e V dois espaços vetoriais sobre $\boldsymbol{F}$. Uma aplicação $T : V \to U$ é chamada de* transformação linear *se:*

1. $T(\boldsymbol{u} + \boldsymbol{v}) = T(\boldsymbol{u}) + T(\boldsymbol{v})$;
2. $T(a\boldsymbol{v}) = aT(\boldsymbol{v})$, *para cada $\boldsymbol{v}, \boldsymbol{u} \in V$ e $a \in \boldsymbol{F}$*

Seja $T : V \to U$ transformação linear entre espaços vetoriais. Definimos os seguintes conjuntos associados à T :

1. $\mathrm{Ker}(T) = \{\mathbf{v} \in V | \ T(\mathbf{v}) = \mathbf{0}\}$ (o *Núcleo* de T),

2. $\text{Im}(T) = \{\mathbf{w} \in U \mid \mathbf{w} = T(\mathbf{v}), \mathbf{v} \in V\}$ (a *Imagem* de T).

Teorema .0.19. *Seja $T : V \to U$ transformação linear entre espaços vetoriais. Então*

a) $\text{Ker}(T)$ *é um subespaço de* V.

b) $\text{Im}(T)$ *é um subespaço de* U.

Sejam U e V dois espaços vetoriais sobre $\mathbf{F}$. U é dito ser *isomorfo* à V se existe uma transformação linear bijetiva $T : V \to U$.

Teorema .0.20. *Sejam U e V dois espaços vetoriais sobre $\boldsymbol{F}$ isomorfos. Então* $\dim(U) = \dim(V)$.

Teorema .0.21. *Seja $T : V \to U$ transformação linear entre espaços vetoriais de dimensão finita. Então*

$$\dim(V) = \dim(\text{Ker}(T)) + \dim(\text{Im}(T)).$$

Definição .0.15. *Sejam $\boldsymbol{F}$ e $\boldsymbol{K}$ dois corpos. Se $\boldsymbol{K} \subset \boldsymbol{F}$, dizemos que $\boldsymbol{F}$ é uma* extensão do corpo *de $\boldsymbol{K}$ e denotamos por $\boldsymbol{F}/\boldsymbol{K}$. Se ainda considerarmos que $\boldsymbol{F}$ como um espaço vetorial sobre $\boldsymbol{K}$, denotamos a* dimensão *de $\boldsymbol{F}$ sobre $\boldsymbol{K}$ por* $[\boldsymbol{F} : \boldsymbol{K}]$.

Dizemos que uma extensão $\mathbf{F}/\mathbf{K}$ é *finita* se $[\mathbf{F} : \mathbf{K}] < \infty$.

Teorema .0.22. *Sejam $\boldsymbol{F'}/\boldsymbol{F}$ e $\boldsymbol{F}/\boldsymbol{K}$ duas extensões. Então* $[\boldsymbol{F'} : \boldsymbol{K}] = [\boldsymbol{F'} : \boldsymbol{F}][\boldsymbol{F} : \boldsymbol{K}]$.

Seja $\mathbf{F}/\mathbf{K}$ uma extensão. Um elemento $\alpha \in \mathbf{F}$ é dito ser *algébrico* sobre $\mathbf{K}$ se existe um polinômio $p(x) \in \mathbf{K}[x]$ tal que $p(\alpha) = 0$. Caso contrário, dizemos que α é *transcendente* sobre $\mathbf{K}$.

Definição .0.16. *Uma extensão $\boldsymbol{F}/\boldsymbol{K}$ é dita ser* algébrica *se todo elemento de $\boldsymbol{F}$ é algébrico sobre $\boldsymbol{K}$.*

Para mais detalhes e propriedades veja (Stichtenoth 1993), (Lima 2020), (J. Kirkwood e B. Kirkwood 2017).

Bibliografia

P. Beelen e N. Tutas (out. de 2006). "A generalization of the Weierstrass semigroup". *Journal of Pure and Applied Algebra* 207, pp. 243–260. MR: 2254885. Zbl: 1105.14045.

C. Carvalho e T. Kato (abr. de 2009). "On Weierstrass semigroups and sets: A review with new results". *Geometriae Dedicata* 139, pp. 195–210. MR: 2481845. Zbl: 1168.14028.

C. Carvalho e F. Torres (mai. de 2005). "On Goppa Codes and Weierstrass Gaps at Several Points". *Des. Codes Cryptography* 35, pp. 211–225. MR: 2134388. Zbl: 1070.94029 (ver p. 87).

E. Casas-Alvero (2019). *Algebraic curves, the Brill and Noether way*. Universitext. Springer, Cham, pp. xiv+224. MR: 3971541. Zbl: 1440.14001.

A. Castellanos e G. Tizziotti (fev. de 2014). "Weierstrass semigroup and codes over the curve $y^q + y = x^{q^r} + 1$". *Advances in Mathematics of Communications* 8. MR: 3180715. Zbl: 1300.14037 (ver p. 80).

— (abr. de 2017a). "On Weierstrass semigroup at m points on curves of the type $f(y) = g(x)$". *Journal of Pure and Applied Algebra* 222. MR: 3763284. Zbl: 1390.14090.

— (mai. de 2017b). "Weierstrass Semigroup and Pure Gaps at Several Points on the GK Curve". *Bulletin of the Brazilian Mathematical Society, New Series* 49. MR: 3829207. Zbl: 1403.14065.

C. Chevalley (1951). *Introduction to the theory of algebraic functions of one variable*. American Mathematical Society (AMS), Providence, RI, p. 188. MR: 0042164. Zbl: 0045.32301.

N. Childress (2009). *Class Field Theory*. Universitext. New York, NY: Springer, pp. x + 226. MR: 2462595. Zbl: 1165.11001 (ver pp. 30, 54).

F. Delgado (mar. de 1990). "The Symmetry of the Weierstrass Generalized Semigroups and Affine Embeddings". *Proceedings of The American Mathematical Society - PROC AMER MATH SOC* 108, pp. 627–627. MR: 0990420. Zbl: 0707.14029.

M. Deuring (1973). *Lectures on the Theory of Algebraic Functions of One Variable*. Lecture Notes in Mathematics. Springer, Cham, p. 155. MR: 0344231. Zbl: 0249.14008.

R. Fuhrmann, A. Garcia e F. Torres (dez. de 1996). "On Maximal Curves". *Journal of Number Theory* 67. MR: 1485426. Zbl: 0914.11036 (ver p. 85).

W. Fulton (1989). *Algebraic Curves An Introduction to Algebraic Geometry*. Redwood City, CA etc.: Addison-Wesley Publishing Company, Inc., pp. xix + 226. MR: 1042981. Zbl: 0681.14011 (ver p. 30).

A. Garcia e H. Stichtenoth (dez. de 1996). "On the Asymptotic Behaviour of Some Towers of Function Fields over Finite Fields". *Journal of Number Theory* 61, pp. 248–273. MR: 1423052. Zbl: 0893.11047.

A. Garcia, H. Stichtenoth e H.-G. Rück (jan. de 2003). "On tame towers over finite fields". *Journal für die Reine und Angewandte Mathematik* 557. Zbl: 1055.11039 (ver p. 46).

M. J. E. Golay (1948). "Notes on digital coding". MR: 4021352 (ver p. 73).

D. M. Goldschmidt (2003). *Algebraic functions and projective curves*. Graduate Texts in Mathematics. New York, NY: Springer, pp. xvi + 179. MR: 1934359. Zbl: 1034.14011.

A. Gonçalves (2017). *Introdução à Álgebra*. Projeto Euclides. Rio de Janeiro: Instituto de Matemática Pura e Aplicada (IMPA), p. 194. Zbl: 1414.16001 (ver p. 102).

V. D. Goppa (1988). *Geometry and Codes*. Dordrecht etc.: Kluwer Academic Publishers, pp. ix + 157. MR: 1029027. Zbl: 1097.14502.

J. Hirschfeld, G. Korchmáros e F. Torres (2008). *Algebraic Curves Over a Finite Field*. Applied Mathematics. Princeton, NJ: Princeton University Press, pp. xx + 696. Zbl: 1200.11042 (ver pp. 84, 85).

T. Høholdt, J. H. van Lint e R. Pellikaan (1998). *Algebraic geometry codes*. Amsterdam: Elsevier, pp. 871–961. Zbl: 0922.94015.

M. Homma (out. de 1996). "The Weierstrass semigroup of a pair of points on a curve". *Archiv der Mathematik* 67, pp. 337–348. MR: 1407338. Zbl: 0869.14015.

Y. Ihara (jan. de 1981). "Some Remarks on the Number of Rational Points of Algebraic Curves over Finite Fields". *J. Fac. Sci. Tokyo* 28. MR: 0656048. Zbl: 0509.14019 (ver p. 84).

J. Kirkwood e B. Kirkwood (2017). *Elementary Linear Algebra*. CRC Press, p. 322. Zbl: 1448.15002 (ver p. 106).

E. L. Lima (2020). *Álgebra Linear*. Matemática Universitária. Rio de Janeiro: Instituto de Matemática Pura e Aplicada (IMPA), p. 356 (ver p. 106).

F. Martinez, C. G. Moreira, N. Saldanha e E. Tengan (2018). *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. Projeto Euclides. Rio de Janeiro: Instituto de Matemática Pura e Aplicada (IMPA), p. 500. Zbl: 1414.11002 (ver p. 6).

E. Martínez-Moro, C. Munuera e D. Ruano (2008). *Advances in Algebraic Geometry Codes*. Coding Theory and Cryptology: Volume 5. Hackensack, NJ: World Scientific, pp. viii + 444. MR: 2516523. Zbl: 1155.94006 (ver p. 99).

G. Matthews (jan. de 2003). "The Weierstrass Semigroup of an m-tuple of Collinear Points on a Hermitian Curve", pp. 12–24. MR: 2092379. Zbl: 1063.14041.

— (jan. de 2005). "Codes From the Suzuki Function Field". *Information Theory, IEEE Transactions on* 50, pp. 3298–3302. MR: 2103499. Zbl: 1316.94119.

G. Matthews e J. Peachey (jan. de 2010). "Minimal generating sets of Weierstrass semigroups of certain m-tuples on the norm-trace function field". MR: 2648556. Zbl: 1226.14037 (ver pp. 44, 94).

C. Moreno (1991). *Algebraic curves over finite fields*. Cambridge Tracts in Mathematics. Cambridge University Press, pp. ix + 246. MR: 1101140. Zbl: 0733.14025.

J. Moyano-Fernández, W. Tenório e F. Torres (jun. de 2017). "Generalized Weierstrass semigroups and their Poincaré series". *Finite Fields and their Applications* 58. MR: 3934068.

R. Pellikaan e F. Torres (dez. de 1999). "On Weierstrass semigroups and the redundancy of improved geometric Goppa codes". *Information Theory, IEEE Transactions on* 45, pp. 2512–2519. MR: 1725140. Zbl: 0960.94027.

R. Pellikaan, X.-W. Wu, S. Bulygin e R. Jurrius (2018). *Codes, cryptology and curves with computer algebra*. Cambridge: Cambridge University Press, pp. xii + 597. MR: 3751341. Zbl: 1416.94003.

J. C. Rosales e P. A. Garcia-Sánchez (2009). *Numerical semigroups*. Developments in Mathematics. Springer New York, p. 18. MR: 2549780 (ver pp. 41, 42).

C. X. San Ling (2004). *Coding Theory A First Course*. Cambridge University Press, p. 222. MR: 2048591. Zbl: 1003.94031 (ver p. 102).

Y. Shudi e C. Hu (jul. de 2016). "Weierstrass Semigroups from Kummer Extensions". *Finite Fields and Their Applications* 45. MR: 3631364. Zbl: 1366.14032 (ver pp. 55, 88).

H. Stichtenoth (1993). *Algebraic function fields and codes*. Universitext. Berlin: Springer-Verlag, pp. x + 260. MR: 1251961. Zbl: 0816.14011 (ver pp. 18, 30, 34, 51, 54, 106).

W. Tenório e G. Tizziotti (set. de 2017). "Generalized Weierstrass semigroups and Riemann–Roch spaces for certain curves with separated variables". *Finite Fields and their Applications* 57. MR: 3921288. Zbl: 1431.14026.

S. G. Tsfasman M. A.; Vlăduţ (1991). *Algebraic-geometric codes*. Mathematics and its applications. Kluwer Acedemic Publishers, pp. ix+667.

G. D. Villa Salvador (2006). *Topics in the Theory of Algebraic Function Fields*. Mathematics: Theory & Applications. Boston, MA: Birkhäuser", pp. xviii + 652. MR: 2241963. Zbl: 1154.11001 (ver p. 51).

Lista de Símbolos

F_X derivada parcial em relação à X, página 2

$H(P_1, \ldots, P_m)$ semigrupo de Weierstrass na m-upla, página 85

$K[x_1, ..., x_n]$ anel de polinômios de n variáveis, página 1

$S_H(-)$ síndrome, página 70

$[F : K]$ dimensão da extensão, página 20

$\ell(D)$ dimensão do divisor, página 28

$\mathbb{C}$ corpos dos números complexos, página 16

$\mathbb{F}_q$ corpo finito, página 3

$\mathbb{P}(F)$ conjunto de todos os places, página 10

$\mathbb{P}^1$ espaço projetivo, página 30

$\mathbb{Q}$ corpos dos números racionais, página 3

$\mathbb{R}$ corpo dos números reais, página 22

$\mathcal{L}(D)$ espaço de Riemann–Roch, página 25

$\mathcal{O}$ anel de valorização, página 9

$\mathcal{X}$ curva, página 2

$\overline{H}(P_1, \ldots, P_m)$ semigrupos de Weierstrass generalizado, página 95

v_P valorização discreta em P, página 12

α Adele , página 33

ω diferencial de Weil , página 34

Ω_F módulo de diferencial de Weil , página 34

C código, página 58

c(S) condutor, página 41

d(-, -) distância de Hamming, página 57

F(S) número de Frobenius, página 41

G(S) conj. de lacunas, página 40

i(D) índice de especialidades , página 31

m(S) multiplicidade, página 40

nG cunj. n somas de lacunas de G, página 43

P Place , página 10

wt peso, página 60

Índice Remissivo

Títulos Publicados — 33º Colóquio Brasileiro de Matemática

Geometria Lipschitz das singularidades – *Lev Birbrair e Edvalter Sena*

Combinatória – *Fábio Botler, Maurício Collares, Taísa Martins, Walner Mendonça, Rob Morris e Guilherme Mota*

Códigos geométricos, uma introdução via corpos de funções algébricas – *Gilberto Brito de Almeida Filho e Saeed Tafazolian*

Topologia e geometria de 3-variedades, uma agradável introdução – *André Salles de Carvalho e Rafał Marian Siejakowski*

Ciência de dados: algoritmos e aplicações – *Luerbio Faria, Fabiano de Souza Oliveira, Paulo Eustáquio Duarte Pinto e Jayme Luiz Szwarcfiter*

Discovering Poncelet invariants in the plane – *Ronaldo A. Garcia e Dan S. Reznik*

Introdução à geometria e topologia dos sistemas dinâmicos em superfícies e além – *Víctor León e Bruno Scárdua*

Equações diferenciais e modelos epidemiológicos – *Marlon M. López-Flores, Dan Marchesin, Vítor Matos e Stephen Schecter*

Differential Equation Models in Epidemiology – *Marlon M. López-Flores, Dan Marchesin, Vítor Matos e Stephen Schecter*

A friendly invitation to Fourier analysis on polytopes – *Sinai Robins*

PI-álgebras: uma introdução à PI-teoria – *Rafael Bezerra dos Santos e Ana Cristina Vieira*

First steps into Model Order Reduction – *Alessandro Alla*

The Einstein Constraint Equations – *Rodrigo Avalos e Jorge H. Lira*

Dynamics of Circle Mappings – *Edson de Faria e Pablo Guarino*

Statistical model selection for stochastic systems with applications to Bioinformatics, Linguistics and Neurobiology – *Antonio Galves, Florencia Leonardi e Guilherme Ost*

Transfer operators in Hyperbolic Dynamics - an introduction – *Mark F. Demers, Niloofar Kiamari e Carlangelo Liverani*

A course in Hodge Theory: Periods of Algebraic Cycles – *Hossein Movasati e Roberto Villaflor Loyola*

A dynamical system approach for Lane-Emden type problems – *Liliane Maia, Gabrielle Nornberg e Filomena Pacella*

Visualizing Thurston's geometries – *Tiago Novello, Vinícius da Silva e Luiz Velho*

Scaling problems, algorithms and applications to Computer Science and Statistics – *Rafael Oliveira e Akshay Ramachandran*

An introduction to Characteristic Classes – *Jean-Paul Brasselet*

impa

Instituto de
Matemática
Pura e Aplicada

ISBN 978-65-89124-49-8