Universidade Federal do ABC

Centro de Matemática, Computação e Cognição - CMCC

Thiago Augusto S. Dourado

A Prova de Weil da Hipótese de Riemann para Corpos Finitos

Santo André

Estado de São Paulo - Brasil

Fevereiro - 2020

Universidade Federal do ABC

Centro de Matemática, Computação e Cognição - CMCC

Thiago Augusto S. Dourado

A Prova de Weil da Hipótese de Riemann para Corpos Finitos

Orientador:

Prof. Dr. Francisco César Polcino Milies

Dissertação de mestrado apresentada ao Centro de Matemática, Computação e Cognição para obtenção do título de Mestre em Matemática

Santo André

Estado de São Paulo - Brasil

Fevereiro - 2020

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Silva Dourado, Thiago Augusto
A Prova de Weil da Hipótese de Riemann para Corpos Finitos / Thiago Augusto Silva Dourado. — 2020.

142 fls.

Orientador: Francisco César Polcino Milies

Dissertação (Mestrado) — Universidade Federal do ABC, Programa de Pós-Graduação em Matemática, Santo André, 2020.

1. Funções zeta. 2. Curvas algébricas. 3. Códigos corretores de erros. I. Polcino Milies, Francisco César. II. Programa de Pós-Graduação em Matemática, 2020. III. Título.

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do(a) autor(a) e com a anuência do(a) orientador(a).

Santo André/SP 02 de junho de 2020

Assinatura do(a) autor(a):

Assinatura do(a) orientador(a):

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Avenida dos Estados, 5001 – Bairro Santa Terezinha – Santo André – SP
CEP 09210-580 · Fone: (11) 4996-0017

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato, THIAGO AUGUSTO SILVA DOURADO realizada em 17 de Fevereiro de 2020:

Prof.(a) NAZAR ARAKELIAN
UNIVERSIDADE FEDERAL DO ABC

Raul Antonio Ferraz

Prof.(a) RAUL ANTONIO FERRAZ
UNIVERSIDADE DE SÃO PAULO

André Luiz M. Pereira

Prof.(a) ANDRE LUIZ MARTINS PEREIRA
UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO

Prof.(a) EDSON RYOJI OKAMOTO IWAKI
UNIVERSIDADE FEDERAL DO ABC

Prof.(a) SAMIR ASSUENA

Prof.(a) FRANCISCO CESAR POLCINO MILIES
UNIVERSIDADE DE SÃO PAULO - Presidente

* Por ausência do membro titular, foi substituído pelo membro suplente descrito acima: nome completo, instituição e assinatura

Aos amigos do Instituo Helion,
sem os quais este trabalho não
teria sido possível.

"O que é ser de esquerda, afinal? É uma posição filosófica perante à vida, onde a solidariedade prevalece sobre o egoísmo."

Pepe Mujica

Agradecimentos

Nenhum de nós consegue chegar a um objetivo significativo, como é de fato um mestrado, sem termos pessoas nos apoiando, nos guiando e nos moldando; passando para nós experiências e nos privando de tropeços e reveses desnecessários. Por isso julgo que tão importante quanto a dissertação em si são os agradecimentos que ora dispenso de forma mais que merecida as pessoas que lhes são devidos.

Inicialmente começo agradecendo meu mestre, meu mentor e meu amigo, o meu orientador César Polcino Milies. Muitos de nós, ao atingir um objetivo acadêmico se orgulham muito do conhecido adquirido. Eu não poderia deixar de dizer que também me orgulho por isso, pois só agora sinto que atingi uma maturidade matemática capaz o suficiente de iniciar meus estudos em matemática verdadeiramente superior, mas a minha maior conquista neste período não se deu em matemática, mas sim na amizade que obtive de meu mestre Polcino. Com ele pude aprender coisas que em livro nenhum são ensinadas, sobretudo por suas ações e exemplos que me mostraram o que o ser humano deve almejar ser um dia. O meu obrigado a meu mestre e amigo.

Também agradeço aos amigos do Instituto Helion, aos quais eu dedico esta dissertação, e em especial, a Valéria Martini, que quando dúvidas me assolaram e realmente me incomodaram, ela com um conhecimento e com técnicas transcendentais como por mágica me tirou essas dúvidas e me garantiu que eu obteria essa formação, e eu acreditei nela.

Agradeço ao amigo Raul Antonio Ferraz, professor da USP que nunca poupou esforços para nos ajudar no que fosse preciso, e pelos quais sou deveras agradecido.

Por fim, mas não menos importante, agradeço ao meu núcleo familiar: minha namorada Elaine Cardoso Penha e meus pais, João Celso Dourado e Elda Maria

Silva. Os quais que, com seus esforços incansáveis, fizeram com tudo fosse possível.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior — Brasil (CAPES) — Código de Financiamento 001. Deixo então menção e agradecimento à CAPES, a qual incentiva a pesquisa de modo geral e o auxílio à formação acadêmica de estudantes e pesquisadores.

Resumo

A proposta deste trabalho é estudar a função zeta em uma curva algébrica sobre corpos finitos, provando a hipótese de Riemann nesse contexto seguindo demonstração dada por André Weil em 1941. Também são apresentados algumas aplicações desta teoria à códigos (lineares) corretos de erros; em especial constrõem-se os códigos de Goppa.

Palavras chave: Curvas algébricas, funções zeta sobre curvas algébricas, corpos finitos, códigos corretores de erros.

Abstract

The purpose of this work is to study the zeta function in an algebraic curve over finite bodies, proving the Riemann hypothesis in this context following a demonstration given by André Weil in 1941. Some applications of this theory to error-correcting code (linear) are also presented; in particular the Goppa's codes are constructed.

Key words: Algebraic curves, zeta functions over algebraic curves, finite fields, error-correcting code.

Sumário

Introdução

0.1 Função Zeta: de Euler e Riemann

A função zeta foi introduzida por Leonhard Euler, em 1740, com o intuito de resolver um importante problema da época, a saber, o *Problema da Basileia*. Em [18] ele escreve:

> *Eu falo aqui sobre as séries de frações cujos numeradores são* 1 *e, de fato, cujos denominadores são os quadrados, ou os cubos, ou outras potências, dos números naturais; deste tipo são* $1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} +$ *etc., igualmente* $1 + \frac{1}{8} + \frac{1}{27} + \frac{1}{64} +$ *etc. e analogamente para potências superiores, cujos termos gerais estão contidas na forma* $\frac{1}{x^n}$.

Posteriormente, num trabalho publicado em novembro de 1859 [60], Bernhard Riemann a estendeu aos números complexos. Nesse trabalho ele escreve:

> *Nesta investigação, meu ponto de partida é a observação de Euler, de que o produto*
>
> $$\prod \frac{1}{1 - \frac{1}{p^s}} = \sum \frac{1}{n^s},$$
>
> *onde p percorre os números primos e n todos os números naturais. A função de variável complexa s, que estas expressões definem, quando ambos são convergentes, designarei por* $\zeta(s)$.

Em seguida, Riemann explica que esta função só está definida quando $\operatorname{Re} s > 1$ e faz uma extensão analítica de ζ:

Ambas convergem somente quando a parte real de s é maior que 1*; entretanto, é fácil encontrar uma expressão da função que é válida sempre. Aplicando a equação*

$$\int_0^\infty e^{-nx} x^{s-1} dx = \frac{\Pi(s-1)}{n^s}$$

se encontra em primeiro lugar

$$\Pi(s-1)\,\zeta(s) = \int_0^\infty \frac{x^{s-1}dx}{e^x - 1}.$$

Consideramos agora a integral

$$\int \frac{(-x)^{s-1}dx}{e^x - 1}$$

estendida de $+\infty$ *a* $+\infty$ *ao longo da fronteira, percorrida no sentido positivo de um domínio que contém ao* 0 *mas a nenhuma outra descontinuidade da função integrando, vemos sem dificuldade que é igual a*

$$\left(e^{-\pi si} - e^{\pi si}\right) \int_0^\infty \frac{x^{s-1}dx}{e^x - 1},$$

sempre que na função multi-avaliada $(-x)^{s-1} = e^{(s-1)\log(-x)}$ *fixemos o valor do logaritmo de* $-x$ *de forma que seja real para o valor real negativo. Assim,*

$$-2\,\text{sen}\,\pi s \Pi(s-1)\,\zeta(s) = i \int_\infty^\infty \frac{(-x)^{s-1}dx}{e^x - 1},$$

se definimos a integral como antes.

Esta equação dá o valor da função $\zeta(s)$ *para todo número complexo s e prova que está bem definida e é finita para todos os valores de s, distintos de* 1*, e que se anulam quando s é um inteiro negativo par.*

Posteriormente, ele apresenta o que ficou conhecido como a Hipótese de Riemann:

Tomemos agora $s = \frac{1}{2} + ti$ *e*

$$\Pi\left(\frac{s}{2}\right)(s-1)\,\pi^{-\frac{s}{2}}\zeta(s) = \xi(t),$$

de forma que

$$\xi(t) = \frac{1}{2} - \left(t^2 + \frac{1}{4}\right) \int_1^\infty \psi(x)\, x^{-\frac{3}{4}} \cos\left(\frac{1}{2} t \log x\right) dx$$

ou ainda

$$\xi(t) = 4\int_1^\infty \frac{d\left(x^{\frac{3}{4}}\psi'(x)\right)}{dx} x^{-\frac{1}{4}} \cos\left(\frac{1}{2}t\log x\right) dx.$$

Esta função é finita para todos os valores finitos de t e é desenvolvível em uma série de potências em t^2 que converge muito rapidamente. Posto que para um valor de s cuja parte real seja maior que 1, $\log\zeta(s) = -\sum\log\left(1-p^{-s}\right)$ *é finito é o mesmo é válido para o logaritmo dos fatores restantes de $\xi(t)$, a função $\xi(t)$ pode anular-se somente quando a parte imaginária de t esteja entre $\frac{1}{2}i$ e $-\frac{1}{2}i$. O número de raízes de $\xi(t) = 0$, cuja parte real está compreendida entre* 0 *e T é ao redor de*

$$= \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi};$$

pois a integral $\int d\log\xi(t)$ calculada no sentido positivo ao redor do domínio dos valores de t cuja parte imaginária está entre $\frac{1}{2}i$ e $-\frac{1}{2}i$ e cuja parte real está compreendida entre 0 *e T é (salvo uma fração da ordem de $\frac{1}{T}$) igual a $\left(T\log\frac{T}{2\pi} - T\right)$ i e, por outro lado, é igual ao número de raízes de $\xi(t) = 0$ no dito domínio, multiplicado por $2\pi i$. De fato, encontramo-nos ao redor deste número de raízes reais entre estes limites, e é bastante provável que todas as raízes sejam reais. Sem dúvida seria desejável possuir uma prova rigorosa disto, mas deixei de lado a investigação de tal prova depois de algumas tentativas infrutíferas já que não é necessário para o objetivo imediato de meu estudo.*

A afirmação que todos os zeros da função $\xi(t)$ são reais é a hipótese de Riemann.

A função $\zeta(s)$ tem zeros nos números pares negativos $-2, -4, -6, \ldots$ e eles são referidos como os *zeros triviais*. Os outros zeros são os números complexos $\frac{1}{2} + i\alpha$ onde α é um zero de $\xi(t)$. Assim, em termos da função $\zeta(s)$, podemos afirmar:

Hipótese de Riemann (versão clássica). *Todos os zeros não triviais de $\zeta(s)$ tem a parte real igual a $\frac{1}{2}$.*

0.2 Um pouco de história

Vamos nos ater um pouco mais a tudo o que foi dito até agora.

A função zeta $\zeta(s)$ é uma função de uma variável complexa $s = \sigma + it$, que pode ser expressa da seguinte forma

$$\zeta(s) = \frac{1}{\Gamma(s)}\int_0^\infty \frac{x^{s-1}}{e^x - 1}dx$$

onde

$$\Gamma(s) = \int_0^\infty x^{s-1} e^{-x} dx$$

é a função gamma.

Para o caso especial em que a parte real de s é maior do que 1, $\zeta(s)$ sempre converge e mostra-se que pode ser expressa na forma:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

A função zeta de Riemann é definida como uma continuação analítica da função definida para $\sigma > 1$ pela série acima, isto é, uma função que no domínio indicado tem a forma dada, mas que no domínio em si a parte real de s se estende além do intervalo $(1, \infty)$.

A função ζ verifica o produto de Euler, isto é, se $\sigma > 1$ então

$$\zeta(s) = \prod_{p \text{ primo}} \frac{1}{1 - p^{-s}}.$$

Com efeito, cada fator (para um dado primo p) no produto acima pode ser expandido para uma série geométrica consistindo dos recíprocos de p elevado a múltiplos de s:

$$\frac{1}{1 - p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots + \frac{1}{p^{ks}} + \cdots.$$

Como $\sigma > 1$, temos que $|p^{-s}| < 1$ e a série converge absolutamente. Assim, podemos tomar um número finito de fatores, multiplicá-los e reorganizar os termos. Tomando todos os primos p menores que certo número primo q, temos

$$\left| \zeta(s) - \prod_{p \leq q} \left(\frac{1}{1 - p^{-s}} \right) \right| < \sum_{n=q+1}^{\infty} \frac{1}{n^\sigma}.$$

Pelo Teorema Fundamental da Aritmética, o produto parcial, quando expandido, dá uma soma que consiste dos termos n^{-s}, onde n é o produto dos primos menores ou iguais a q. A desigualdade resulta no fato de que apenas inteiros maiores que q podem falhar nesse produto parcial expandido. Como a diferença entre o produto parcial e $\zeta(s)$ vai para zero quando $\sigma > 1$, temos convergência nesta região.

A função zeta satisfaz também a seguinte equação funcional:

$$\zeta(s) = 2^s \pi^{s-1} \operatorname{sen}\left(\frac{\pi s}{2} \right) \Gamma(1 - s) \zeta(1 - s).$$

Esta é uma igualdade de funções meromorfas válida em todo o plano complexo. A equação relaciona valores da função zeta de Riemann nos pontos s e $1-s$, em particular relacionando inteiros positivos com inteiros negativos ímpares. Devido aos zeros da função seno, a equação funcional implica que $\zeta(s)$ tem um zero simples em cada inteiro negativo par $s=-2n$, conhecido como os zeros triviais de $\zeta(s)$. Quando s é um inteiro positivo, o produto $\operatorname{sen}\left(\frac{\pi s}{2}\right)\Gamma(1-s)$ à direita é diferente de zero porque $\Gamma(1-s)$ tem um polo simples, que cancela o zero simples do fator senoidal.

A motivação de Riemann para estudar a função zeta e seus zeros foi sua ocorrência em sua fórmula explícita para o número de primos $\pi(x)$ menor ou igual a um dado número x, publicada no artigo supramencionado. Para isso ele utiliza a função

$$\Pi(x)=\pi(x)+\frac{1}{2}\pi\left(x^{\frac{1}{2}}\right)+\frac{1}{3}\pi\left(x^{\frac{1}{3}}\right)+\frac{1}{4}\pi\left(x^{\frac{1}{4}}\right)+\frac{1}{5}\pi\left(x^{\frac{1}{5}}\right)+\frac{1}{6}\pi\left(x^{\frac{1}{6}}\right)+\cdots.$$

Usando a função de Möbius, definida para $n=1$ ou $n=\prod_{j=1}^{k}p_j^{a_j}$ (fatoração em potências de primos) dada por

$$\mu(n)=\begin{cases}1 & \text{se } n=1,\\ (-1)^k & \text{se } a_j=1 \text{ para todo } j,\\ 0 & \text{se } a_j=1 \text{ para algum } j,\end{cases}$$

e a fórmula da inversão de Möbius, a saber, se g e f são funções aritméticas satisfazendo

$$g(n)=\sum_{d|n}f(d)$$

então

$$f(n)=\sum_{d|n}\mu(d)\,g\left(\frac{n}{d}\right),$$

o número de primos pode ser recuperado pelo seguinte:

$$\begin{aligned}\pi(x)&=\sum_{n=1}^{\infty}\frac{\mu(n)}{n}\Pi\left(x^{\frac{1}{n}}\right)\\&=\Pi(x)-\frac{1}{2}\Pi\left(x^{\frac{1}{2}}\right)-\frac{1}{3}\Pi\left(x^{\frac{1}{3}}\right)-\frac{1}{5}\Pi\left(x^{\frac{1}{5}}\right)+\frac{1}{6}\Pi\left(x^{\frac{1}{6}}\right)-\cdots.\end{aligned}$$

A fórmula de Riemann é então

$$\Pi_0(x)=\operatorname{Li}(x)-\sum_{\rho}\operatorname{Li}(x^{\rho})-\log 2+\int_x^{\infty}\frac{dt}{t\left(t^2-1\right)\log t},$$

onde a soma é sobre os zeros não triviais da função zeta e onde Π_0 é uma versão ligeiramente modificada de Π que substitui seu valor em seus pontos de descontinuidade pela média de seus limites superior e inferior:

$$\Pi_0(x) = \lim_{\varepsilon \to 0} \frac{\Pi(x-\varepsilon) + \Pi(x+\varepsilon)}{2};$$

a função Li que ocorre no primeiro termo é a função logaritmo integral dada por

$$\mathrm{Li}(x) = \int_0^x \frac{dt}{\log t}.$$

A soma na fórmula de Riemann não é absolutamente convergente, mas pode ser avaliada tomando os zeros ρ na ordem do valor absoluto de sua parte imaginária. Os termos $\mathrm{Li}(x)$ envolvendo os zeros da função zeta precisam de algum cuidado em sua definição, pois Li possui pontos de ramificação em 0 e 1, e são definidos (para $x > 1$) por continuação analítica na variável complexa ρ na região $\mathrm{Re}(\rho) > 0$, ou seja, eles devem ser considerados como a exponencial integral de $\rho \log x$, isto é,

$$\mathrm{Ei}(\rho \log x) = -\int_{-\rho \log x}^{\infty} \frac{e^{-t}}{t} dt.$$

Os outros termos também correspondem a zeros: o termo dominante $\mathrm{Li}(x)$ vem do polo $s = 1$, considerado como um zero de multiplicidade -1, e os pequenos termos restantes advém dos zeros triviais. Essa fórmula diz que os zeros da função zeta de Riemann controlam as oscilações de primos em torno de suas posições "esperadas". Riemann sabia que os zeros não triviais da função zeta eram distribuídos simetricamente sobre a linha $s = \frac{1}{2} + it$, e sabia também que todos os seus zeros não triviais devem estar no intervalo $0 \leq \mathrm{Re}\, s \leq 1$. Ele verificou que alguns dos zeros estavam na linha crítica com a parte real igual a $\frac{1}{2}$ e sugeriu que todos eles estivessem; esta é *a hipótese de Riemann*.

Hardy [29] e Hardy & Littlewood [30] mostraram que existem infinitos zeros na linha crítica, considerando momentos de certas funções relacionadas à função zeta. Selberg [64] provou que pelo menos uma (pequena) porção positiva de zeros está na linha. Levinson [46] melhorou isso para um terço dos zeros relacionando os zeros da função zeta com os da sua derivada, e Conrey [13] melhorou isso ainda mais para dois quintos.

A maioria dos zeros fica perto da linha crítica. Mais precisamente, Bohr & Landau [8] mostraram que, para qualquer ε positivo, todos, menos uma porção infinitamente pequena de zeros, estão dentro de uma distância ε da linha crítica. Ivić [41] fornece várias versões mais precisas desse resultado, chamadas estimativas de densidade zero, que limitam o número de zeros em regiões com parte imaginária no máximo T e parte real no mínimo $\frac{1}{2} + \varepsilon$.

0.3 Formas de Representar a Função Zeta

0.3.1 Séries de Dirichlet

A série

$$\zeta(s) = \frac{1}{s-1} \sum_{n=1}^{\infty} \left(\frac{n}{(n+1)^s} - \frac{n-s}{n^s} \right)$$

converge para $\mathrm{Re}(s) > 0$, enquanto que

$$\zeta(s) = \frac{1}{s-1} \sum_{n=1}^{\infty} \frac{n(n+1)}{2} \left(\frac{2n+3+s}{(n+1)^{s+2}} - \frac{2n-1-s}{n^{s+2}} \right)$$

converge para todo $\mathrm{Re}(s) > -1$.

0.3.2 Funções theta

$$2\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \int_0^{\infty} (\theta(it) - 1)\, t^{\frac{s}{2}-1} dt,$$

em que

$$\theta(\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau}$$

é a função theta de Jacobi. No entanto, essa integral só converge se a parte real de s for maior que 1, mas pode ser regularizada. Isto dá a seguinte expressão para a função zeta, que é bem definida para todos os s, exceto 0 e 1:

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \frac{1}{s-1} - \frac{1}{s} + \frac{1}{2} \int_0^1 \left(\theta(it) - t^{-\frac{1}{2}} \right) t^{\frac{s}{2}-1} dt + \frac{1}{2} \int_1^{\infty} (\theta(it) - 1)\, t^{\frac{s}{2}-1} dt.$$

0.3.3 Séries de Laurent

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=0}^{\infty} \frac{(-1)^n \gamma_n}{n!} (s-1)^n.$$

A constante γ_n, chamadas constantes de Stieltjes, podem ser definidas pelo limite

$$\gamma_n = \lim_{m \to \infty} \left[\left(\sum_{k=1}^{m} \frac{(\log k)^n}{k} \right) - \frac{(\log m)^{n+1}}{n+1} \right].$$

0.3.4 Integral

Para $s \neq 1$, tem-se

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + 2\int_0^\infty \frac{\operatorname{sen}(s \arctan t)}{(1+t^2)^{\frac{s}{2}}\left(e^{2\pi t}-1\right)} dt.$$

Esta expressão é bastante usada para o cálculo numérico da função zeta.

0.3.5 Fatorial descendente

$$\zeta(s) = \frac{s}{s-1} - \sum_{n=1}^{\infty} \left(\zeta(s+n) - 1\right) \frac{s(s+1)\cdots(s+n-1)}{(n+1)!}.$$

0.3.6 Produto de Hadamard

$$\zeta(s) = \frac{e^{\left(\log(2\pi) - 1 - \frac{\gamma}{2}\right)s}}{2(s-1)\,\Gamma\left(1+\frac{s}{2}\right)} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}},$$

onde o produto é sobre os zeros não triviais ρ de ζ e a letra γ denota a constante de Euler-Mascheroni, dada por

$$\gamma = \lim_{n\to\infty} \left(-\log n + \sum_{k=1}^{n} \frac{1}{k}\right) = \int_1^\infty \left(-\frac{1}{x} + \frac{1}{\lfloor x \rfloor}\right) dx.$$

Uma expansão mais simples em termos de produto infinito é

$$\zeta(s) = \pi^{\frac{s}{2}} \frac{\prod_{\rho}\left(1 - \frac{s}{\rho}\right)}{2(s-1)\,\Gamma\left(1+\frac{s}{2}\right)}.$$

Essa forma exibe claramente o polo simples em $s = 1$ e os zeros triviais em $-2, -4, \ldots$, devido ao termo da função gamma no denominador e os zeros não triviais em $s = \rho$. (Para assegurar a convergência na última fórmula, o produto deve ser tomado sobre "pares correspondentes" de zeros, isto é, os fatores para um par de zeros da forma ρ e $1 - \rho$ devem ser combinados).

0.3.7 Séries globalmente convergentes

Em 1930, Helmut Hasse provou [32] que se $s \neq 1 + \frac{2\pi i}{\log 2}$ então as séries

$$\zeta(s) = \frac{1}{1 - 2^{1-s}} \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{(k+1)^s}$$

e

$$\zeta(s) = \frac{1}{s-1} \sum_{n=0}^{\infty} \frac{1}{n+1} \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{(k+1)^{s-1}}$$

são globalmente convergentes.

0.4 Função Zeta e Distribuição de Primos

A fórmula explícita de Riemann para o número de primos menores que um dado número em termos de uma soma sobre os zeros da função zeta de Riemann diz que a magnitude das oscilações dos primos em torno de sua posição esperada é controlada pelas partes reais dos zeros da função zeta. Em particular, o termo de erro no teorema do número primo está intimamente relacionado com a posição dos zeros. Por exemplo, se β é o limite superior das partes reais dos zeros, então

$$\pi(x) - \mathrm{Li}(x) = O\left(x^{\beta} \log x\right).$$

Já é conhecido que $\frac{1}{2} \leq \beta \leq 1$.

Von Koch [86] provou que a hipótese de Riemann implica o "melhor possível" para o erro do teorema do número primo. Uma versão precisa do resultado de Koch, devido a Schoenfeld [63], diz que a hipótese de Riemann implica

$$|\pi(x) - \mathrm{Li}(x)| < \frac{1}{8\pi} \sqrt{x} \log x \quad \text{para todo} \quad x \geq 2657.$$

Também, no mesmo artigo, Schoenfeld mostrou que

$$|\psi(x) - x| < \frac{1}{8\pi} \sqrt{x} \log^2 x \quad \text{para todo} \quad x \geq 73.2,$$

onde $\psi(x)$ é a segunda função de Chebyshev, dada por

$$\psi(x) = \sum_{\substack{p^k \leq x \\ p \text{ primo}}} \log p = \sum_{\substack{p \leq x \\ p \text{ primo}}} \left\lfloor \log_p x \right\rfloor \log p.$$

0.5 Analogia com Curvas Algébricas

O que apresentamos nesta dissertação é o análogo e sua demonstração da hipótese de Riemann para corpos finitos ou, mais precisamente, para curvas algébricas sobre corpos finitos. Isto é, tomando uma curva $\mathfrak{C}$ definida sobre o corpo $\mathbb{F}_q$, definimos a função ζ de $\mathfrak{C}$ em um número complexo s como

$$\zeta_{\mathfrak{C}}(s) = \zeta_{\mathfrak{C}/\mathbb{F}_q}(s) = \sum_{D} N(D)^{-s},$$

em que D percorre todos os divisores efetivos (*i.e.* $D > 0$) definidos sobre $\mathbb{F}_q$ de $\mathfrak{C}$, e $N(D) = q^{\mathrm{gr}(D)}$ é a norma de D com $\mathrm{gr}(D)$ o grau do divisor D. Assim, a hipótese de Riemann para corpos finitos, análoga a formulação clássica, nos diz que $\zeta_{\mathfrak{C}}(s) = 0$ então $\mathrm{Re}\, s = \frac{1}{2}$. Naturalmente o resultado não se apresenta nessa forma direta, existem algumas formas equivalentes de se enunciar a hipótese de Riemann para corpos finitos, a mais simples delas é a seguinte:

> *Seja $f(x, y)$ um polinômio irredutível a coeficientes inteiros. Para qualquer número primo p, denotamos por $N_p(f)$ o número de soluções da congruência $f(x, y) \equiv 0 \pmod{p}$. Então existe um inteiro A dependendo apenas de f tal que*
>
> $$\left|N_p(f) - p\right| \leq A\sqrt{p}.$$

0.6 Entendendo a Importância do Problema

A prova da hipótese de Riemann para corpos finitos que iremos apresentar é devida a André Weil, que a publicou nos anos quarenta e que foi um momento matemático deveras extraordinário por muitas razões: o contexto dramático em que este trabalho foi produzido e escrito por Weil, a controvérsia com o matemático Helmut Hasse que se seguiu, a história dos desenvolvimentos que o precederam, incluindo a contribuições de E. Artin, H. Hasse, F.K. Schmidt e, claro, B. Riemann e, finalmente, os desenvolvimentos prodigiosos que se seguiram, por um lado, no campo da matemática aplicada (teoria dos códigos corretores lineares) e, por outro lado, no coração da matemática pura com as famosas "Conjecturas de Weil", que orientaram e estimularam o desenvolvimento dramático da geometria algébrica durante as décadas seguintes, culminando com sua comprovação por Grothendieck e Deligne.

0.6.1 Contexto

Em 1940, em meio a Segunda Guerra Mundial, André Weil, após incidentes que ele narra em suas *Souvenirs d'Apprentissage* [89], está preso por insubordinação na prisão "Boas Novas" em Rouen. Ele ficará lá por alguns meses, trabalhará intensamente em sua matemática, se corresponderá com Henri Cartan [4], com sua irmã Simone Weil [95] e demonstrará a famosa "hipótese de Riemann para uma curva sobre um corpo finito", trabalho que ele resume em uma nota [92] de três páginas no *Proceedings of the Academy*, apresentado via Elie Cartan, na reunião de 22 de abril de 1940. O resumo desliza sob o esteio de um enunciado ("*Aqui está um lema importante*") que ele não fornece prova. Libertado da prisão e tendo conseguido ingressar nos Estados Unidos, André Weil publica uma

segunda nota [93] no *Proceedings of National Academy of Sciences*, onde simplifica sua prova, mas sempre deixando um ponto importante sem nenhuma evidência (*"Em Severi"*). A nota americana termina com o seguinte anúncio:

> *Um relato detalhado desta teoria* [...] *e da teoria "transcendental", conforme descrito na nota anterior, está sendo preparado para publicação.*

Na verdade Weil publicará em 1946, quando estava em São Paulo, *Foundations of Algebraic Geometry* [88] e em 1948 dois livros sobre curvas algébricas e variedades abelianas [90, 91] que completarão este programa, resumido por Jean-Pierre Serre em [68] como:

> *Depois de oito anos, e mais de 500 páginas, sua Nota de 1940 está finalmente justificada!*

0.6.2 Polêmica

Hasse, que havia conseguido alguns anos antes provar a chamada hipótese de Riemann para as curvas elípticas (curvas algébricas de gênero 1) [33, 34], ficou indignado com a atitude de Weil. Este último também descreveu explicitamente seus motivos e rivalidade com Hasse em uma carta a Henri Cartan, datada de 8 de abril de 1940 [4]:

> *Enviei a nota sem ter demonstrado o lema fundamental; mas estou bem claro sobre essas questões agora, para assumir o risco. Nunca escrevi nada, e quase nunca vi nada, que atinja um grau de concentração tão alto quanto essa nota. Hasse só tem que se enforcar, porque eu resolvo (sujeito ao meu lema) todos os principais problemas da teoria: 1) A hipótese de Riemann para as funções ζ desses corpos (demonstrada por Hasse para o gênero 1); 2) As séries L de Artin relativas aos caracteres das extensões algébricas desses corpos são os polinômios, cujo grau eu determino.*

Seguiu-se uma troca indireta de farpas, da qual citamos dois extratos:

> *Você tem uma ideia de um "aproveitador da guerra espiritual"? parece-me que o nosso "amigo" André Weil é tal pessoa* [...] *Isto é o que eu chamo de um jeito tipicamente judeu!*
> (Carta de Hasse a Gaston Julia, 14 de setembro de 1941)

E muitos anos mais tarde, nos comentários de suas obras, Weil escreve:

> *Devemos concluir que as mentes desses [algebristas alemães] tinham sido um tanto intoxicados pelos sucessos de seus generais?*

0.6.3 Gênese

As analogias entre os corpos numéricos (o corpo $\mathbb{Q}$ e suas extensões finitas) e os corpos de funções em um corpo finito (o corpo $\mathbb{F}_p(X)$ e suas extensões finitas) ou entre aritmética e geometria têm fascinado muitos matemáticos, talvez o primeiro sendo Kronecker. O próprio Weil estava quase obcecado com essa ideia, acrescentando-lhe um vínculo com a topologia riemanniana, ele falava de "texto trilíngue" [95]. Emil Artin introduziu [3] o análogo da funções zeta para os corpos de funções em $\mathbb{F}_q$ e a teoria foi desenvolvida pela escola alemã, notavelmente Deuring, Hasse e Schmidt [62, 33, 34], estabelecendo a racionalidade (análogo da extensão analítica), a equação funcional e, para as curvas de gênero 1, a hipótese de Riemann. O grande avanço e, em muitos aspectos, a ideia central, frutífera e inovadora de Weil é tirar o problema do arcabouço algébrico e colocá-lo em um contexto geométrico.

0.6.4 Desenvolvimentos ulteriores

Em 1949, André Weil publicou um artigo [94] sobre o número de pontos de uma variedade algébrica em um corpo finito. Este artigo propõe uma série de conjecturas (demonstradas por Grothendieck [27] e Pierre Deligne [14, 15]) que generalizam para variedades de dimensões arbitrárias as propriedades da função zeta de uma curva. Este artigo visionário irá, durante três décadas, catalisar e suscitar a maioria dos desenvolvimentos da geometria algébrica abstrata, desenvolvimentos liderados por Grothendieck e mais tarde completados por Deligne: esquemas, vigas, ciclos algébricos e teoria da interseção, cohomologia étale, etc.

A hipótese de Riemann para curvas sobre corpos finitos também será importante para as questões de telecomunicações e teoria da informação através dos "códigos de Goppa" [24], onde o chamado limitante de Hasse-Weil, dado por

$$\left|\#\mathcal{C}\left(\mathbb{F}_q\right) - (q+1)\right| \leq 2g\sqrt{q},$$

equivalente a hipótese Riemann para curvas sobre corpos finitos, desempenha um papel importante. É uma questão de construir explicitamente bons códigos (lineares) corretores de erros. A descoberta de Goppa é que alguns sistemas lineares em curvas sobre um corpo finito fornecem tais códigos. Um dos parâmetros importantes é o número de pontos racionais da curva, que deve ser o mais amplo possível, isto é, na prática aproximando o máximo possível o limite superior fornecido pelo chamado teorema de Hasse-Weil.

Capítulo 1

Extensões e Corpos Finitos

1.1 Extensões de Corpos

Definição 1.1.1 A *característica* do corpo K, denotada por $\text{car}(K)$, é o menor inteiro positivo n tal que $n1 = 1 + \cdots + 1$ (n vezes) é igual a 0; se tal n não existe, diremos que a característica de K é zero.

O homomorfismo $i : \mathbb{Z} \to K$ (K corpo) tem uma imagem que é um subanel de integridade de K, logo $\text{Ker}(i)$ é um ideal primo. Assim seja $\text{Ker}(i) = \{0\}$ e i é injetivo logo $\text{car}(K) = 0$, se existe um número primo p tal que $\text{Ker}(i) = p\mathbb{Z}$ então $\text{car}(K) = p$. No primeiro caso K contém um subanel isomorfo a $\mathbb{Z}$ logo contém um subcorpo isomorfo a $\mathbb{Q}$; no segundo caso K contém um subcorpo isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

Definição 1.1.2 Sejam L e K corpos. Diremos que L é uma *extensão* de K se $K \subset L$, escreveremos também $L|K$ para indicar este fato.

Proposição 1.1.1 *Seja $f : K \to L$ um homomorfismo de corpos, então f é injetivo.*

Demonstração: Por definição $f(1_K) = 1_L$ e por consequência, se $x \in K \setminus \{0\}$ temos $1_L = f\left(xx^{-1}\right) = f(x) f\left(x^{-1}\right)$ logo $f(x) \neq 0$. □

Quando $f : K \to L$ é um homomorfismo de corpos, podemos identificar K como um subcorpo de L; podemos também considerar L como um K-espaço vetorial e introduzir a aplicação:

$$\begin{aligned} K \times L &\to L \\ (x, y) &\mapsto f(x)\, y \end{aligned}$$

Neste contexto denotaremos $[L:K] = \dim_K L$ a dimensão de L visto como K-espaço vetorial.

Definição 1.1.3 A dimensão $[L:K]$ definida acima é dito o *grau* da extensão $L|K$.

Teorema 1.1.1 *Seja $K \subset L \subset F$ uma torre de corpos, então*

$$[F:K] = [F:L]\,[L:K]\,.$$

Demonstração: Damos a prova quando essas dimensões são finitas, de fato o enunciado e até a prova permanecem válidos com cardinais quaisquer. Consideremos $e_1, \ldots, e_m$ uma base de L sobre K e $f_1, \ldots, f_n$ uma base de F sobre L, mostraremos então que $\left\{e_i f_j \;\middle|\; 0 \leq i \leq m, 0 \leq j \leq n\right\}$ formam uma de L sobre K. Mostraremos inicialmente que este é um conjunto gerador. Seja $x \in F$, então existe $\lambda_i \in L$ tal que $x = \sum_{i=1}^{n} \lambda_i f_i$ (pois os f_j formam uma L-base de F). Além disso, existe $\alpha_{ij} \in K$ tal que $\lambda_i = \sum_{j=1}^{m} \alpha_{ij} e_j$ (pois os e_j formam uma K-base de L) e portanto $x = \sum_{i,j} \alpha_{ij} e_j f_i$. Mostraremos agora a independência linear. Seja $\alpha_{ij} \in K$ e $\sum_{i,j} \alpha_{ij} e_j f_i = 0$ então $\sum_i \left(\sum_j \alpha_{ij} e_j\right) f_i = 0$ logo $\sum_j \alpha_{ij} e_j = 0$ (pois os f_i são L-linearmente independentes) e então os α_{ij} são nulos (pois os e_j são K-linearmente independentes). □

Seja $K \subset L$ uma extensão de corpos e $\alpha \in L$. Consideremos o homomorfismo de anéis "avaliação em α" definido da seguinte maneira:

$$\begin{aligned} \mathrm{av}_\alpha : K[X] &\to L \\ P &\mapsto P(\alpha) \end{aligned}$$

Quando $\mathrm{Ker}(\mathrm{av}_\alpha) = \{0\}$, diremos que α é *transcendente* sobre K. Quando $\mathrm{Ker}(\mathrm{av}_\alpha) \neq \{0\}$, diremos que α é algébrico sobre K. Se $\mathrm{Ker}(\mathrm{av}_\alpha) = PK[X]$, chamaremos P o *polinômio minimal* de α sobre K (ele não é único, a menos que imponhamos que seja mônico).

Note que $K[\alpha]$ é o menor subanel de L contendo K e α e$K(\alpha)$ é o menor subcorpo de L contendo K e α. Por construção $K[\alpha]$ é a imagem de av_α logo é isomorfo a $K[X]\,/\,\mathrm{Ker}(\mathrm{av}_\alpha)$. Se α é transcendente, vemos que $K[\alpha] \cong K[X]$ e $K(\alpha) \cong K(X)$; em particular $K(\alpha)$ é de dimensão finita sobre K. Se α é algébrico se P seu polinômio minimal sobre K, então P é irredutível em $K[X]$ logo o ideal gerado por P é maximal e $K[\alpha] = K(\alpha) \cong K[X]\,/PK[X]$. Além disso, neste caso $[K(\alpha):K] = \mathrm{gr}(P)$. Com efeito, uma base de $K[\alpha] = K(\alpha)$ sobre K é dada por $1, \alpha, \alpha^2, \ldots, \alpha^{\mathrm{gr}(P)-1}$. Em particular, provamos o seguinte:

Proposição 1.1.2 *Seja $\alpha \in L \supset K$, então α é algébrico sobre K se e somente se $[K(\alpha):K] < \infty$. Neste caso $[K(\alpha):K]$ é o grau do polinômio minimal de α sobre K.*

Terminamos esta seção com um teorema cuja demonstração pode ser encontrado em livros básico de álgebra que tratem da teoria dos corpos.

Teorema 1.1.2 *Seja K um corpo e $P \in K[X]$ não constante.*

(i) Existe $L \supset K$ tal que L contém uma raiz de P. Ademais, se P é irredutível em $K[X]$ e se L é minimal (i.e. *se $K \subset L' \subset L$ e P possui uma raiz em L' então $L = L'$) então L é único a menos de isomorfismo e é chamado um* corpo de ruptura de P *(de fato, $L \cong K[X]/PK[X]$).*

(ii) Existe uma extensão $L \supset K$ tal que P se decompõe sobre L, ou seja, $P = a(X - \alpha_1) \cdots (X - \alpha_n)$ com $a, \alpha_1, \ldots, \alpha_n \in L$ e minimal; uma tal extensão é única a menos de isomorfismo e é chamada o corpo de decomposição de P sobre K.

1.2 Corpos Finitos

Iniciemos esta seção recordando que todo corpo F tem um único menor subcorpo, chamado o *subcorpo primo*, denotado F_p, que é a interseção de todos os seus subcorpos.

Lema 1.2.1 *Suponha que F é um corpo finito com um subcorpo K contendo q elementos. Então F é um espaço vetorial sobre K e $\#F = q^m$, onde m é a dimensão F visto como um espaço vetorial sobre K.*

Demonstração: É fácil verificar que F é um espaço vetorial sobre K usando as operações de corpo em F. Como F é finito, podemos escolher uma base $\{\beta_1, \ldots, \beta_m\}$ para F sobre K. Todo elemento α de F pode então escrito sob a forma $\alpha = a_1\beta_1 + \cdots + a_m\beta_m$, onde $a_i \in K$ para $1 \leq i \leq m$ e a sequência $a_1, \ldots, a_m$ é unicamente determinada por α. Assim existem $(\#F)^m = q^m$ sequências distintas de coeficientes, pois existem $\#K = q$ escolhas para cada a_i. □

O m que ocorre no Lema 1.2.1, que é a dimensão de F como um espaço vetorial sobre K, é chamado de *grau* de F sobre K. Ao combinar o lema com o fato de que todo corpo finito tem uma característica prima, obtemos uma caracterização do número de elementos que um corpo finito pode possuir:

Teorema 1.2.1 *Seja F um corpo finito. A cardinalidade de F é p^m, onde p é a característica de F e m o grau de F sobre seu subcorpo primo.*

Proposição 1.2.1 *Se F é um corpo finito com q elementos e $a \in F$ é não nulo, então $a^{q-1} = 1$. Assim, $a^q = a$ para todo $a \in F$.*

DEMONSTRAÇÃO: Se a é não nulo, sabemos que a é uma unidade em F. Existem $q-1$ unidades em F, logo, pelo Teorema de Lagrange, a ordem multiplicativa de a em F divide $q-1$. Portanto $a^{q-1}=1$ e $a^q=a$. Se $a=0$ então é imediato que $a^q=a$. □

Corolário 1.2.1 *Se F um corpo finito com q elementos e $a \in F \setminus \{0\}$, então o inverso de a é a^{q-2}.*

DEMONSTRAÇÃO: $a^{q-2}a = a^{q-1} = 1$. □

Corolário 1.2.2 *Se F é finito com $\#F = q$, então todo elemento de F é raiz de $X^q - X \in F[X]$.*

DEMONSTRAÇÃO: Se $a \in F$ então $a^q = a$, logo $a^q - a = 0$. □

Proposição 1.2.2 *Se F é um corpo finito com q elementos, então $X^q - X$ se fatora em $F[X]$ como $\prod_{a \in F}(X-a)$.*

DEMONSTRAÇÃO: Imediata. □

Teorema 1.2.2 (Existência e Unicidade dos Corpos Finitos) *Para todo primo p e um inteiro positivo $n \geq 1$, existe um corpo finito com p^n elementos. Qualquer corpo finito com p^n elementos é isomorfo ao corpo de decomposição de $X^{p^n} - X$ sobre F_p.*

DEMONSTRAÇÃO: Primeiro provamos a parte da existência. Suponha que a potência prima q seja da forma p^n, onde p é um primo. Considere o polinômio $r(X) = X^q - X$ como um polinômio com coeficientes no corpo F_p. Seja F o corpo de decomposição de $r(X)$ sobre F_p.

Considere o conjunto $S = \{a \in F \mid a^q - a = 0\}$. Como a derivada $r'(X)$ é identicamente -1, ela não tem raízes. Assim o teste da derivada mostra que $r(X)$ não tem raízes múltiplas, logo $\#S = q$. Como podemos ver facilmente que S é um subcorpo de F, isso significa que S é um corpo finito com $q = p^n$ elementos.

Pela Proposição 1.2.2, um corpo com q elementos é corpo de decomposição de $X^q - X$. Como sabemos da teoria clássica dos corpos, corpos de decomposição são únicos a menos de isomorfismos. □

Observação 1.2.1 O teorema anterior mostra que um corpo finito de uma determinada ordem é único a menos de isomorfismo. Assim, falamos "do" corpo finito de uma ordem específica q e escrevemos $\mathbb{F}_q$ para denotar esse corpo. Outra notação comum para um corpo de ordem q é $\mathrm{GF}(q)$, onde G significa Galois e F significa corpo (*field* em inglês). Este nome é usado em homenagem a Evariste Galois, que em 1830 foi a primeira pessoa a considerar corpos finitos em geral, por isso esses corpos são também chamado de *corpos de Galois*. Usaremos a notação $\mathbb{F}_q$ nesta dissertação.

Observação 1.2.2 Notemos que quando p é primo, o corpo $\mathbb{F}_p$ é o mesmo que (isomorfo) o anel $\mathbb{Z}/p\mathbb{Z}$ dos números inteiros módulo p. Entretanto, quando $m > 1$ o corpo finito $\mathbb{F}_{p^m}$ não é o mesmo que o anel $\mathbb{Z}/p^m\mathbb{Z}$ dos números inteiros módulo p^m, que não é um corpo.

Teorema 1.2.3 (Estrutura dos Subcorpos de $\mathbb{F}_{p^n}$) *Todo subcorpo de $\mathbb{F}_{p^n}$ tem p^m elementos, em que m é um divisor de n. Reciprocamente, para cada inteiro m dividindo n existe um único subcorpo de $\mathbb{F}_{p^n}$ de ordem p^m.*

Demonstração: Um subcorpo K de um corpo finito $\mathbb{F}_{p^n}$ deve ter p^m elementos distintos para algum inteiro positivo m com $m \leq n$. Pelo Lema 1.2.1, p^n deve ser uma potência de p^m, logo m divide n.

Por outro lado, suponha que m divide n. Então

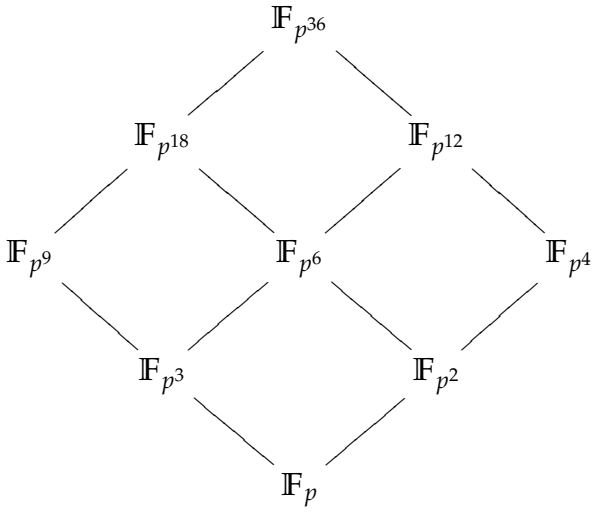
$$\left(X^{p^m-1} - X\right) \,\Big|\, \left(X^{p^n-1} - X\right),$$

e assim

$$\left(X^{p^m} - X\right) \,\Big|\, \left(X^{p^n} - X\right).$$

Segue então que cada raiz de $X^{p^m} - X$ é também uma raiz de $X^{p^n} - X$. Logo o corpo $\mathbb{F}_{p^n}$ deve conter um corpo de decomposição do polinômio $X^{p^m} - X$ sobre $\mathbb{F}_p$ e o corpo de decomposição deve ter exatamente p^m elementos distintos. Se o subcorpo não for único, isto é, se houvesse dois corpos contidos em $\mathbb{F}_{p^n}$, então sua união conteria mais do que p^m raízes do polinômio $X^{p^m} - X$ em $\mathbb{F}_{p^n}$, o que é impossível. □

Exemplo 1.2.1 (Subcorpos de $\mathbb{F}_{p^{36}}$)



Teorema 1.2.4 *O grupo multiplicativo $\mathbb{F}_q^\times$ de todos os elementos não nulos do corpo finito $\mathbb{F}_q$ é cíclico.*

DEMONSTRAÇÃO: Para o caso em que $q = 2$ é trivial. Assumamos então que $q \geq 3$. Seja $q - 1 = h > 1$ e seja sua a fatoração prima $\prod_{i=1}^{t} p_i^{r_i}$. Para cada i considere o polinômio $f_i(x) = x^{h/p_i} - 1$. Este polinômio tem grau h/p_i e, assim, tem no máximo h/p_i raízes. Como $h/p_i < h$ existe um elemento a_i de $\mathbb{F}_q$ que não é raiz de f_i, em particular $a_i \neq 1$. Seja

$$b_i = a_i^{h/p_i^{r_i}}$$

para cada $i \leq t$. Vamos mostrar que a ordem multiplicativo de b_i é $p_i^{r_i}$. Claramente

$$b_i^{p_i^{r_i}} = a_i^h = 1.$$

Assim, a ordem de b_i deve dividir $p_i^{r_i}$ e, portanto, deve ser uma potência de p_i. Suponha

$$b_i^{p_i^k} = 1$$

para algum $k \leq r_i$. Então temos

$$b_i^{p_i^{r_i-1}} = b_i^{p_i^k p_i^{r_i-(k+1)}} = 1^{p_i^{r_i-(k+1)}} = 1.$$

Isto é impossível, pois

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \quad \text{e} \quad a_i^{h/p_i} \neq 1.$$

Assim a ordem de b_i é exatamente $p_i^{r_i}$.

Finalmente, seja $b = \prod_{i=1}^{t} b_i$. Então, com base na teoria dos grupos, a ordem de b é $q-1$, pois é o mínimo múltiplo comum das ordens dos elementos b_i para $i = 1, \ldots, t$. □

Definição 1.2.1 Um elemento $\theta \in \mathbb{F}_q$ que gera multiplicativamente o grupo $\mathbb{F}_q^{\times}$ de todos os elementos diferentes de zero do corpo $\mathbb{F}_q$ é chamado de *elemento primitivo*.

Observação 1.2.3 Se θ um elemento primitivo de um corpo finito F, todo elemento não nulo de F pode ser escrito como uma potência de θ. Essa representação facilita a computação da multiplicação de elementos do corpo. Suponha, por exemplo, que $a = \theta^t$ e $b = \theta^r$, então $ab = \theta^t\theta^r = \theta^{t+r}$. É difícil, no entanto, encontrar a potência s de θ tal que $\theta^t + \theta^r = \theta^s$.

Teorema 1.2.5 (Teorema do Elemento Primitivo) *Seja $\mathbb{F}_q$ um corpo finito e seja $\mathbb{F}_r$ uma extensão finita de $\mathbb{F}_q$. Então $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_q$, e para qualquer elemento primitivo θ de $\mathbb{F}_r$ a relação $\mathbb{F}_r = \mathbb{F}_q(\theta)$ se verifica.*

Demonstração: Seja θ um elemento primitivo de $\mathbb{F}_r$. Tomemos $\alpha \in \mathbb{F}_q(\theta)$, assim $\alpha = a_0 + a_1\theta + \cdots + a_m\theta^m$, onde m é o grau de $\mathbb{F}_r$ sobre $\mathbb{F}_q$. Essa soma é um elemento de $\mathbb{F}_r$, portanto, $\alpha \in \mathbb{F}_r$. Agora observamos que $\mathbb{F}_q(\theta)$ contém $0, \theta$ e todos as potências de θ. Portanto, $\mathbb{F}_q(\theta)$ contém $\mathbb{F}_r$. □

Corolário 1.2.3 *Para qualquer potência prima q e qualquer número inteiro $n > 1$, existe um polinômio irredutível de grau n sobre $\mathbb{F}_q$.*

Demonstração: Basta tomar $f(X)$ o polinômio minimal sobre $\mathbb{F}_q$ de um elemento primitivo de $\mathbb{F}_{q^n}$. □

Exemplo 1.2.2 Considere o polinômio $f(X) = X^2 + X + l$ sobre o corpo $\mathbb{F}_2$. Como $f(X)$ não tem raiz em $\mathbb{F}_2$, $f(X)$ é irredutível sobre $\mathbb{F}_2$. Seja θ uma raiz de $f(X)$ de modo que $\theta^2 + \theta + 1 = 0$, ou seja, $\theta^2 = -(\theta + 1) = \theta + 1$. O corpo $\mathbb{F}_4 = \mathbb{F}_{2^2}$ pode ser representado como o conjunto $\{a\theta + b \mid a, b \in \mathbb{F}_2\}$. Agora, fornecemos as tabelas de adição e multiplicação para o corpo F_{2^2}:

$+$	0	1	θ	$\theta+1$
0	0	1	θ	$\theta+1$
1	1	0	$\theta+1$	θ
θ	θ	$\theta+1$	0	1
$\theta+1$	$\theta+1$	θ	1	0

$\cdot$	0	1	θ	$\theta+1$
0	0	0	0	0
1	0	1	θ	$\theta+1$
θ	0	θ	$\theta+1$	1
$\theta+1$	0	$\theta+1$	1	θ

Notemos que (depois de uma simplificação) $(\theta+1)(\theta+1) = \theta$. Notemos também que θ é um elemento primitivo do corpo $\mathbb{F}_4$, assim $\theta^1 = \theta$, $\theta^2 = \theta+1$ e $\theta^3 = 1$.

Exemplo 1.2.3 Considere o corpo $\mathbb{F}_9$, que é um espaço vetorial de dimensão 2 sobre $\mathbb{F}_3$. Considere $f(X) = X^2 + X + 2$ em $\mathbb{F}_3[X]$. Este polinômio não tem raízes em $\mathbb{F}_3$, logo é irredutível em $\mathbb{F}_3$. Seja θ uma raiz de $f(X)$, assim $\theta^2 + \theta + 2 = 0$. Logo $\theta^2 = -\theta - 2 = 2\theta + 1$. O corpo $\mathbb{F}_{3^2}$ é isomorfo ao corpo $\{a\theta + b \mid a, b \in \mathbb{F}_3\}$ com suas operações naturais. Podemos computar as tabelas de adição e multiplicação diretamente. Por exemplo, $2\theta(\theta+2) = 2\theta^2 + 4\theta = 2(\theta+1) + \theta = 2\theta + 2$. As tabelas completas de adição e multiplicação são dadas abaixo:

$+$	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
0	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
1	1	2	0	$\theta+1$	$\theta+2$	θ	$2\theta+1$	$2\theta+2$	2θ
2	2	0	1	$\theta+2$	θ	$\theta+1$	$2\theta+2$	2θ	$2\theta+1$
θ	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+2$	$2\theta+1$	0	1	2
$\theta+1$	$\theta+1$	$\theta+2$	θ	$2\theta+1$	$2\theta+2$	2θ	1	2	0
$\theta+2$	$\theta+2$	θ	$\theta+1$	$2\theta+2$	2θ	$2\theta+1$	2	0	1
2θ	2θ	$2\theta+1$	$2\theta+2$	0	1	2	θ	$\theta+1$	$\theta+2$
$2\theta+1$	$2\theta+1$	$2\theta+2$	2θ	1	2	0	$\theta+1$	$\theta+2$	θ
$2\theta+2$	$2\theta+2$	2θ	$2\theta+1$	2	0	1	$\theta+2$	θ	$\theta+1$

$\cdot$	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	θ	$\theta+1$	$\theta+2$	2θ	$2\theta+1$	$2\theta+2$
2	0	2	1	2θ	$2\theta+2$	$2\theta+1$	θ	$\theta+2$	$\theta+1$
θ	0	θ	2θ	$2\theta+1$	1	$\theta+1$	$\theta+2$	$2\theta+2$	2
$\theta+1$	0	$\theta+1$	$2\theta+2$	1	$\theta+2$	2θ	2	θ	$2\theta+1$
$\theta+2$	0	$\theta+2$	$2\theta+1$	$\theta+1$	2θ	2	$2\theta+2$	1	θ
2θ	0	2θ	θ	$\theta+2$	2	$2\theta+2$	$2\theta+1$	$\theta+1$	1
$2\theta+1$	0	$2\theta+1$	$\theta+2$	$2\theta+2$	θ	1	$\theta+1$	2	2θ
$2\theta+2$	0	$2\theta+2$	$\theta+1$	2	$2\theta+1$	θ	1	2θ	$\theta+2$

Podemos usar a tabela de multiplicação para verificar que a ordem multiplicativa de θ em $\mathbb{F}_9$ é 8, o que significa que θ é um elemento primitivo de $\mathbb{F}_9$.

Teorema 1.2.6 *Seja $N_q(n)$ o número de polinômio mônicos irredutíveis de grau n sobre $\mathbb{F}_q$. Então:*

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

Em que μ é a função de Möbius, dada pela regra:

$$\mu(n) = \begin{cases} 1 & \text{se } m = 1, \\ (-1)^k & \text{se } m = p_1 \cdots p_k, \text{ o produto de primos distintos,} \\ 0 & \text{caso contrá rio.} \end{cases}$$

Demonstração: [55, Teorema 1.6.4]. □

Hansen e Mullen [28] fornecem uma lista de polinômios primitivos (e, portanto, irredutíveis) de grau n sobre $\mathbb{F}_p$ para cada primo $p \leq 97$ com $p^n < 10^{50}$.

O próximo resultado, cuja demonstração é clara, mostra que um polinômio irredutível sobre um corpo finito é o polinômio minimal para cada uma de suas raízes.

Proposição 1.2.3 *Seja $f(X)$ um polinômio irredutível sobre $\mathbb{F}_q$ a seja α uma raiz de $f(X)$. Então para cada $h(X) \in \mathbb{F}_q[X]$, tem-se $h(\alpha) = 0$ se e somente se $f(X)$ divide $h(X)$.*

Observação 1.2.4 Essa proposição mostra que se $f(X)$ é irredutível sobre $\mathbb{F}_q$ e $f(\alpha) = 0$, então $\mathbb{F}_q(\alpha)$ contém todas as raízes de $f(X)$; portanto, $\mathbb{F}_q(\alpha) = \mathbb{F}_q(\beta)$ sempre que α e β são raízes do mesmo polinômio irredutível sobre $\mathbb{F}_q$.

Proposição 1.2.4 *Seja $f(X)$ um polinômio irredutível de grau m sobre $\mathbb{F}_q$. Então $f(X) \mid X^{q^n} - X$ se, e somente se, $m \mid n$.*

Demonstração: Suponha inicialmente que m divide n, logo $\mathbb{F}_{q^m}$ é um subcorpo de $\mathbb{F}_{q^n}$. Seja α uma raiz de $f(X)$ em seu corpo de decomposição, logo $\left[\mathbb{F}_q(\alpha) : \mathbb{F}_q\right] = m$. Assim, como m divide n, e $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, temos $\alpha^{q^n} - \alpha = 0$ em $\mathbb{F}_{q^m}$. Isto mostra que toda raiz de $f(X)$ é raiz de $X^{q^n} - X$, e portanto $f(X) \mid X^{q^n} - X$.

Para a recíproca suponha que $f(X) \mid X^{q^n} - X$. Se α uma raiz de $f(X)$, então temos a torre de corpos $\mathbb{F}_q \subset \mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^n}$. Agora, como $\left[\mathbb{F}_{q^n} : \mathbb{F}_q\right] = n$ e $\left[\mathbb{F}_q(\alpha) : \mathbb{F}_q\right] = m$, temos que necessariamente m divide n. □

O próximo teorema descreve as raízes de um polinômio irredutível sobre um corpo finito.

Teorema 1.2.7 *Seja $f(X)$ um polinômio irredutível de grau m sobre $\mathbb{F}_q$, então f tem uma raiz $\alpha \in \mathbb{F}_{q^m}$. Ademais, todas as raízes de $f(X)$ são simples e são dados por*

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}.$$

DEMONSTRAÇÃO: Seja α uma raiz de f em seu corpo de decomposição. Como $\left[\mathbb{F}_q(\alpha) : \mathbb{F}_q\right] = m$, o elemento α está em $\mathbb{F}_{q^m}$. Escrevemos $f(X) = \sum_{i=0}^{m} a_i X^i$, onde $a_i \in \mathbb{F}_q$. Seja β uma raiz qualquer de $f(X)$. Então

$$f(\beta^q) = \sum_{i=0}^{m} a_i (\beta^q)^i = \sum_{i=0}^{m} a_i \left(\beta^i\right)^q = 0.$$

Portanto β^q é uma raiz de f. Analogamente, β^{q^i} é uma raiz para todo $i > 0$.

Suponha que para $1 \leq i < j < m$ tenhamos $\beta^{q^i} = \beta^{q^j}$. Elevando ambos os lado à potência q^{m-j} obtemos

$$\beta^{q^{i+m-j}} = \beta^{q^m} = \beta.$$

Logo β é uma raiz de $X^{q^{i+m-j}} - X$, assim $m \mid i + m - j$. Desta forma, i e j são congruentes módulo m, uma contradição. □

Definição 1.2.2 Diremos que um corpo F é *perfeito* se todos os polinômios irredutíveis em $F[X]$ tem todas as suas raízes simples.

Corolário 1.2.4 *Os corpos $\mathbb{F}_q$ são perfeitos.*

Definição 1.2.3 Seja $\alpha \in \mathbb{F}_{q^m}$. Os elementos

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$$

são chamados os *conjugados* de α sobre $\mathbb{F}_q$.

Observação 1.2.5 Um elemento $\alpha \in \mathbb{F}_{q^m}$ terá m conjugados distintos se e somente se seu polinômio minimal tiver grau m. Se o polinômio minimal de α tiver grau d (que deve ser um divisor de m), os conjugados distintos de α serão

$$\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}},$$

cada um repetido exatamente m/d vezes.

Corolário 1.2.5 *Seja $\alpha \in \mathbb{F}_{q^m}$ e seja o polinômio minimal de α sobre $\mathbb{F}_q$ de grau d. Considere o conjunto*

$$\left\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\right\}$$

dos conjugados de α. Os elementos deste conjunto são distintos se $m = d$; do contrário cada conjugado é repetido m/d vezes.

O próximo resultado descreve o conjunto de automorfismos de um corpo finito.

Teorema 1.2.8 *Os automorfismos distintos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são dados pelas funções $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ onde $\sigma_j : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ é definida por*

$$\sigma_j(\alpha) = \alpha^{q^j}$$

para cada $\alpha \in \mathbb{F}_{q^m}$.

Demonstração: Mostramos acima que de β é um elemento primitivo de $\mathbb{F}_q$ e $i \neq j \in \{0, 1, \ldots, m-1\}$, então

$$\beta^{q^i} \neq \beta^{q^j}.$$

Logo, se $i \neq j$ então $\sigma_i \neq \sigma_j$.

Agora seja σ qualquer automorfismo de F_{q^m} sobre F_q e seja $f(X)$ o seu polinômio minimal sobre $\mathbb{F}_q$. Um cálculo direto mostra que σ leva β em outra raiz de $f(X)$, de modo que podemos assumir que

$$\sigma(\beta) = \beta^{q^k}.$$

Então $\sigma = \sigma_k$, pois a ação de um automorfismo de um corpo finito é completamente determinada por sua ação sobre um elemento primitivo do corpo. □

Observação 1.2.6 (Grupo de Galois) O conjunto de automorfismos de $\mathbb{F}_q$ forma um grupo com a operação de composição de funções. Este grupo é chamado *grupo de Galois de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$*, e é denotado por $\mathrm{Gal}(\mathbb{F}_{q^m}|\mathbb{F}_q)$. Este um grupo é cíclico com gerador $\sigma_1 : \alpha \mapsto \alpha^q$, o qual é chamado de *automorfismo de Frobenius*. Os conjugados de α são, portanto, os elementos aos quais α é levado por aplicações iterados da aplicação de Frobenius.

Observação 1.2.7 Observe que os subcorpos de $\mathbb{F}_{q^m}$ são exatamente os corpos do forma $\mathbb{F}_{q^n}$ em que $n \mid m$. Os subgrupos próprios do grupo Galois de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são exatamente os grupos gerados por σ_1^n onde $n \mid m$. Além disso, $\sigma_1^n(\alpha) = \alpha$ se e somente se um $\alpha \in \mathbb{F}_{q^n}$. Assim, há uma correspondência um-a-um entre os subcorpos de $\mathbb{F}_{q^m}$ e os subgrupos de seu grupo Galois. Este é um caso particular do Teorema da Correspondência de Galois.

Capítulo 2

Corpos de Funções

2.1 O Conceito de Corpo de Funções de uma Variável

Se y é transcendente sobre K, então tem-se que a interseção de todos os subcorpos de F que contém K e y é o subcorpo

$$K(y) := \left\{ \frac{p(y)}{q(y)} \in F \;\middle|\; p(X), q(X) \in K[X], q(X) \neq 0 \right\},$$

que é isomorfo ao corpo de frações dos polinômios:

$$K(X) = \left\{ \frac{p(X)}{q(X)} \;\middle|\; p(X), q(X) \in K[X], q(X) \neq 0 \right\}.$$

Isto reflete o fato de que se y é transcendente sobre K, então se comporta como "uma variável" sobre K, uma vez que para quaisquer $a_0, \ldots, a_n \in K$ tem-se que $\sum_{i=0}^{n} a_i y^i = 0$ se, e somente se, $a_i = 0$ para todo $i = 0, \ldots, n$. Esta é a ideia do conceito de corpo de funções.

Definição 2.1.1 Um *corpo de funções algébricas sobre K (de uma variável)* ou, abreviadamente, *corpo de funções* é uma extensão F de K com a propriedade de que existe um elemento $x \in F$, transcendente sobre K e tal que a extensão $F|K(x)$ é finita.

$$\begin{array}{c} F \\ \Big| \text{ extensão finita} \\ K(x) \\ \Big| \; x \text{ transcendente} \\ K \end{array}$$

Doravante assumiremos que K é *algebricamente fechado em* F, o que significa que se $f \in F$ é um elemento algébrico sobre K, então $f \in K$ (em outras palavras, exceto os elementos de K, que obviamente são algébricos sobre K, não existem outros elementos de F que sejam algébricos sobre K).

Exemplo 2.1.1 O exemplo mais básico de um corpo de funções se obtém ao tomar $F = K(X)$.

2.2 Valorizações

Definição 2.2.1 Um *anel de valorização* do corpo de funções $F|K$ é um anel $\mathcal{O}$ tal que $K \subsetneq \mathcal{O} \subsetneq F$ e, para qualquer elemento $f \in F$, tem-se $f \in \mathcal{O}$ ou $f^{-1} \in \mathcal{O}$.

Proposição 2.2.1 *Seja $\mathcal{O}$ um anel de valorização de $F|K$. Então $\mathcal{O}$ é um anel local, isto é, $\mathcal{O}$ tem um único ideal maximal $\mathfrak{p}$, a saber, o conjunto dos elementos não invertíveis de $\mathcal{O}$, ou seja, $\mathfrak{p} = \mathcal{O} \setminus \mathcal{O}^\times$, onde $\mathcal{O}^\times$ denota o conjunto dos elementos invertíveis de $\mathcal{O}$.*

Demonstração: Vamos provar inicialmente que $\mathfrak{p}$ é um ideal. De imediato temos que $0 \in \mathfrak{p}$. Seja $z \in \mathfrak{p}$ e $f \in \mathcal{O}$, se $zf = u \in \mathcal{O}^\times$ temos que $\left(zu^{-1}\right) f = 1$ e $f \in \mathcal{O}^\times$, logo $z = uf^{-1} \in \mathcal{O}^\times$, o que é um absurdo, portanto, $zf \in \mathfrak{p}$. Dados $f, g \in \mathfrak{p} \setminus \{0\}$ temos que $f/g \in \mathcal{O}$ ou $g/f \in \mathcal{O}$; suponhamos $f/g \in \mathcal{O}$, logo $1 + f/g \in \mathcal{O}$ e $f + g = g\,(1 + f/g) \in \mathfrak{p}$. Portanto $\mathfrak{p}$ é um ideal de $\mathcal{O}$.

Se $\mathfrak{m} \subset \mathcal{O}$ é um ideal não contido em $\mathfrak{p}$, então $\mathfrak{m}$ deve conter um elemento de $\mathcal{O}^\times$, de modo que $\mathfrak{m} = \mathcal{O}$. Logo $\mathfrak{p}$ é o único ideal maximal de $\mathcal{O}$. □

Proposição 2.2.2 *Seja $\mathcal{O}$ um anel de valorização de $F|K$ e seja $\mathfrak{p} \subset \mathcal{O}$ seu ideal maximal. Então vale que:*

(i) *$\mathfrak{p}$ é um ideal principal.*

(ii) *Seja $t \in \mathfrak{p}$ tal que $\mathfrak{p} = t\mathcal{O}$, então qualquer elemento não nulo $z \in F$ se escreve de maneira única como $z = t^n u$, com $n \in \mathbb{Z}$ e $u \in \mathcal{O}^\times$.*

(iii) *Sejam $t \in \mathfrak{p}$ tal que $\mathfrak{p} = t\mathcal{O}$ e $z \in F$. Então $z \in \mathcal{O}$ se, e somente se, $z = t^n u$, com $n \in \mathbb{N}$ e $u \in \mathcal{O}^\times$.*

Demonstração: Para *(i)* e *(ii)* vide [75, Teorema 1.1.6].

(iii) Se $z = t^n u$ com $u \in \mathcal{O}^\times$ e $n < 0$, então não podemos ter $z \in \mathcal{O}$ pois, neste caso, $1 = t^{-n} z u^{-1} \in \mathfrak{p}$, o que é um absurdo. A recíproca é imediata. □

Definição 2.2.2 Uma *valorização* de $F|K$ é uma função

$$v : F \to \mathbb{Z} \cup \{\infty\}$$

com as seguintes propriedades:

(i) $v(f) = \infty$ se, e somente se, $f = 0$.

(ii) $v(fh) = v(f) + v(h)$ para quaisquer $f, h \in F$.

(iii) $v(f+h) \geq \min\{v(f), v(h)\}$ para quaisquer $f, h \in F$.

(iv) Existe $t \in F$ tal que $v(t) = 1$.

(v) $v(a) = 0$ para qualquer $a \in K^{\times}$.

Observe que se $a \in K^{\times}$ e $f \in F$ então $v(af) = v(a) + v(f) = v(f)$, em particular $v(-f) = v(f)$.

Proposição 2.2.3 *Seja v uma valorização de $F|K$ e sejam $f, h \in F$. Se $v(f) \neq v(h)$, então*

$$v(f+h) = \min\{v(f), v(h)\}.$$

Demonstração: Suponhamos que $v(f) < v(h)$ e suponhamos também que $v(f+h) \neq \min\{v(f), v(h)\} = v(f)$. Da parte (iii) da Definição 2.2.2 obtemos que $v(f+h) > v(f)$ e $v(f) = v((f+h)-h) \geq \min\{v(f+h), v(-h)\} > v(f)$, uma contradição. □

A partir de trabalho de Hensel de 1897, Kürschák e Ostrowski introduziram o conceito geral de valorização motivados pelo exemplo de valorização p-ádica (vide o excelente artigo de Peter Roquette sobre história das valorizações [61]).

Exemplo 2.2.1 (Valorizações p-ádicas) Fixado um primo p. A *valorização p-ádica* sobre os números racionais é uma função $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ definida por:

$$v_p(a) = \begin{cases} m & \text{se} \quad a = p^m \frac{a'}{b'},\ \text{mdc}(a'b', p) = 1, \\ \infty & \text{se} \quad a = 0. \end{cases}$$

Note que $\mathbb{Q}$ não é corpo de funções. Neste caso, somente os itens originais de uma definição de valorização no sentido geral são satisfeitos, a saber, os itens (i), (ii) e (iii) da Definição 2.2.2. Com efeito:

(i) Por definição temos que $v_p(0) = \infty$.

(ii) Seja $v_p(a) = m$ e $v_p(b) = n$, então $a = p^m \cdot a'/b'$ e $b = p^n \cdot a''/b''$ com $\text{mdc}(a'b', p) = \text{mdc}(a''b'', p) = 1$. Temos assim que $v_p(ab) = m + n$, pois $ab = p^{m+n} \cdot a'a''/b'b''$ e $\text{mdc}(a'a''b'b'', p) = 1$.

(iii) Usando as notações do item anterior e supondo que $n < m$, como $a + b = p^n \cdot (p^{m-n}a'b'' + a''b') / b'b''$, temos que $v_p(a+b) = n = \min\{v_p(a), v_p(b)\}$.

2.3 Lugares

Definição 2.3.1 Um ideal maximal $\mathfrak{p} \subset F$ de um anel de valorização de $F|K$ diz-se um *lugar* do corpo de funções $F|K$.

Definição 2.3.2 Seja $\mathfrak{p} = t\mathcal{O}$ um lugar de $F|K$. A *valorização associada a* $\mathfrak{p}$ é uma função $v_\mathfrak{p} : F \to \mathbb{Z} \cup \{\infty\}$ definida por:

$$v_\mathfrak{p}(f) = \begin{cases} n & \text{se } f \neq 0 \text{ e } f = t^n u \text{ com } u \in \mathcal{O}^\times, \\ \infty & \text{se } f = 0. \end{cases}$$

Observação 2.3.1 Note que para qualquer gerador t' temos $v_\mathfrak{p}(t') = 1$, o que implica que a definição desta função independe da escolha do gerador de $\mathfrak{p}$. Um gerador de $\mathfrak{p}$ diz-se um *parâmetro local em* $\mathfrak{p}$.

Proposição 2.3.1 *Sejam $\mathcal{O}$ um anel de valorização do corpo de funções $F|K$, $\mathfrak{p}$ seu ideal maximal e $v_\mathfrak{p}$ a valorização associada. Então:*

(i) $\mathcal{O} = \{f \in F \mid v_\mathfrak{p}(f) \geq 0\}$.

(ii) $\mathcal{O}^\times = \{f \in F \mid v_\mathfrak{p}(f) = 0\}$.

(iii) $\mathfrak{p} = \{f \in F \mid v_\mathfrak{p}(f) > 0\}$.

Demonstração: Seja $t \in \mathfrak{p}$ tal que $\mathfrak{p} = t\mathcal{O}$.

(i) Claramente, $t^n u \in \mathcal{O}$ sempre que $n \geq 0$ e $u \in \mathcal{O}^\times$. Por outro lado, da parte *(iii)* do Teorema 2.2.2 temos que $\mathcal{O} \subset \{f \in F \mid v_\mathfrak{p}(f) \geq 0\}$.

(ii) Seja $f = t^n u \in \mathcal{O}^\times$. Como $f^{-1} = t^{-n}u^{-1} \in \mathcal{O}$, devemos ter $n \geq 0$ e $-n \geq 0$. Portanto $n = 0$.

(iii) Segue de imediato dos itens anteriores, pois $\mathfrak{p} = \mathcal{O} \setminus \mathcal{O}^\times$. □

Desta forma, um lugar determina uma valorização de $F|K$ e do item *(i)* da proposição acima vemos que existe um anel de valorização que contém um lugar dado. Não é difícil de provar o seguinte resultado, que é uma espécie de implicação inversa da proposição.

Proposição 2.3.2 *Seja $v : F \to \mathbb{Z} \cup \{\infty\}$ uma valorização de $F|K$ e seja $\mathcal{O} = \{f \in F \mid v_\mathfrak{p}(f) \geq 0\}$, então $\mathcal{O}$ é um anel de valorização de $F|K$, que tem como ideal maximal o conjunto $\mathfrak{p} = \{f \in F \mid v_\mathfrak{p}(f) > 0\}$.*

Segue-se que existe uma bijeção entre o conjunto de funções de valorizações de $F|K$ e os lugares de $F|K$. Ademais, existe uma bijeção entre o conjunto dos anéis de valorização de $F|K$ e o conjunto dos lugares de $F|K$ (isto é, os subconjuntos de f são ideais maximais dos anéis de valorização de $F|K$).

Dado que $\mathfrak{p}$ é um ideal maximal de $\mathcal{O}$, temos que $\mathcal{O}/\mathfrak{p}$ é um corpo. Definimos uma função $\pi : F \to \mathcal{O}/\mathfrak{p} \cup \{\infty\}$ da seguinte forma:

$$\begin{cases} \text{Se } z \in \mathcal{O} \text{ então } \pi(z) = z + \mathfrak{p}; \\ \text{Se } z \in F \setminus \mathcal{O} \text{ então } \pi(z) = \infty. \end{cases}$$

Como $K \cap \mathfrak{p} = \{0\}$, π é injetora, podemos identificar K com sua imagem em $\mathcal{O}/\mathfrak{p}$ e considerar $\mathcal{O}/\mathfrak{p}$ uma extensão de K. Pode-se mostrar que esta é uma extensão finita, e seu grau é dito *grau de* $\mathfrak{p}$, que denotaremos por $\operatorname{gr}(\mathfrak{p})$. Quando $\operatorname{gr}(\mathfrak{p}) = 1$ diremos que $\mathfrak{p}$ é um *lugar racional de* $F|K$. A função π definida acima chama-se a *função de classe residual em relação a* $\mathfrak{p}$ e será denotada por $\operatorname{res}_{\mathfrak{p}}$.

Dado $z \in \mathcal{O}$, é habitual escrever $z(\mathfrak{p})$, em lugar de $\bar{z}$, para denotar a classe de z no corpo $\mathcal{O}/\mathfrak{p}$, usaremos esta notação livremente daqui por diante.

Exemplo 2.3.1 Uma importante valorização de $K(X)$, geralmente denotada por v_∞ é a função definida por

$$\begin{cases} v_\infty(0) = \infty, \\ v_\infty\left(\dfrac{f(X)}{g(X)}\right) = \operatorname{gr} f(X) - \operatorname{gr} g(X) \text{ para todos } \dfrac{f(X)}{g(X)} \in K(X) \setminus \{0\}. \end{cases}$$

O anel de valorização correspondente é

$$\mathcal{O}_\infty = \left\{ \frac{f(X)}{g(X)} \in K(X) \;\middle|\; \operatorname{gr} f(X) \leq \operatorname{gr} g(X) \right\},$$

e o lugar correspondente, chamado *lugar infinito*, é

$$\mathfrak{p}_\infty = \left\{ \frac{f(X)}{g(X)} \in K(X) \;\middle|\; \operatorname{gr} f(X) < \operatorname{gr} g(X) \right\} = \frac{1}{X}\mathcal{O}_\infty,$$

logo

$$\mathcal{O}_\infty^\times = \left\{ \frac{f(X)}{g(X)} \in K(X) \;\middle|\; \operatorname{gr} f(X) = \operatorname{gr} g(X) \right\}.$$

Por fim, a função de classe residual correspondente a $\mathfrak{p}_\infty$ para

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0} \quad \text{com} \quad a_n, b_m \neq 0,$$

é determinada por

$$\mathrm{res}_{\mathfrak{p}_\infty}(z) = z(\infty) = \begin{cases} a_n/b_m & \text{se } n = m, \\ 0 & \text{se } n < m, \\ \infty & \text{se } n > m. \end{cases}$$

Vide [75, Proposição 1.2.1] para demonstração destas afirmações.

2.4 Divisores

Definição 2.4.1 Seja $\mathfrak{P} = \mathfrak{P}_F$ o conjunto dos lugares de $F|K$. Uma soma formal do tipo

$$\sum_{\mathfrak{p}\in\mathfrak{P}} n_{\mathfrak{p}}\mathfrak{p},$$

onde $n_{\mathfrak{p}} \in \mathbb{Z}$ para todo $\mathfrak{p} \in \mathfrak{P}$ e $n_{\mathfrak{p}} \neq 0$ somente para um número finito de lugares $\mathfrak{p}$, diz-se um *divisor de* $F|K$.

As demonstrações das próximas duas proposições são imediatas.

Proposição 2.4.1 *O conjunto* $\mathrm{Div}(F)$ *dos divisores de* $F|K$ *é um grupo abeliano com a soma*

$$\sum_{\mathfrak{p}\in\mathfrak{P}} n_{\mathfrak{p}}\mathfrak{p} + \sum_{\mathfrak{p}\in\mathfrak{P}} s_{\mathfrak{p}}\mathfrak{p} := \sum_{\mathfrak{p}\in\mathfrak{P}} (n_{\mathfrak{p}} + s_{\mathfrak{p}})\,\mathfrak{p}.$$

Proposição 2.4.2 *Em* $\mathrm{Div}(F)$ *tem-se definida uma ordem parcial da seguinte forma:*

$$\sum_{\mathfrak{p}\in\mathfrak{P}} n_{\mathfrak{p}}\mathfrak{p} \leq \sum_{\mathfrak{p}\in\mathfrak{P}} s_{\mathfrak{p}}\mathfrak{p} \;\Leftrightarrow\; n_{\mathfrak{p}} \leq s_{\mathfrak{p}} \text{ para todo } \mathfrak{p} \in \mathfrak{P}.$$

Com base na relação de ordem em $\mathrm{Div}(F)$ dada acima, podemos colocar a seguinte definição:

Definição 2.4.2 Um divisor $\sum_{\mathfrak{p}\in\mathfrak{P}} n_{\mathfrak{p}}\mathfrak{p}$ é dito *efetivo* (ou *positivo*) se $\sum_{\mathfrak{p}\in\mathfrak{P}} n_{\mathfrak{p}}\mathfrak{p} \geq 0$.

2.5 Grau de um Divisor

Definição 2.5.1 O *grau* do divisor $\sum_{\mathfrak{p}\in\mathfrak{P}} n_{\mathfrak{p}}\mathfrak{p}$ é definido como sendo o inteiro

$$\sum_{\mathfrak{p}\in\mathfrak{P}} n_{\mathfrak{p}} \,\mathrm{gr}(\mathfrak{p});$$

e seu *suporte* é definido como o conjunto (finito) de lugares $\mathfrak{p}$ tal que $n_{\mathfrak{p}} \neq 0$.

Definição 2.5.2 Seja $f \in F \setminus \{0\}$, o *divisor principal de* f é definido por:

$$\operatorname{div}(f) := \sum_{\mathfrak{p} \in \mathfrak{P}} v_{\mathfrak{p}}(f)\, \mathfrak{p}.$$

Observação 2.5.1 Seja $f \in F$ com $f \neq 0$. Pode-se mostrar que $v_{\mathfrak{p}}(f) \neq 0$ somente para um número finito de lugares $\mathfrak{p}$ (vide [75, Corolário 1.3.4]).

Proposição 2.5.1 *Sejam* $f, h \in F \setminus \{0\}$. *Então:*

(i) $\operatorname{div}(fh) = \operatorname{div}(f) + \operatorname{div}(h)$.

(ii) $\operatorname{div}(1) = 0$.

(iii) $\operatorname{div}\left(f^{-1}\right) = -\operatorname{div}(f)$.

Demonstração: *(i)* Aplicando a propriedade (ii) da Definição 2.2.2, obtemos:

$$\begin{aligned}\operatorname{div}(fh) &= \sum_{\mathfrak{p} \in \mathfrak{P}} v_{\mathfrak{p}}(fh)\, \mathfrak{p} = \sum_{\mathfrak{p} \in \mathfrak{P}} \left[v_{\mathfrak{p}}(f) + v_{\mathfrak{p}}(h)\right] \mathfrak{p} \\ &= \sum_{\mathfrak{p} \in \mathfrak{P}} v_{\mathfrak{p}}(f)\, \mathfrak{p} + \sum_{\mathfrak{p} \in \mathfrak{P}} v_{\mathfrak{p}}(h)\, \mathfrak{p} = \operatorname{div}(f) + \operatorname{div}(h).\end{aligned}$$

(ii) Como $1 = t^0 1$ temos, por definição, que $v_{\mathfrak{p}}(1) = 0$, logo $\operatorname{div}(1) = 0$.

(iii) Do item anterior temos que $\operatorname{div}(1) = \operatorname{div}\left(f^{-1} f\right) = 0$, logo aplicando o *(i)* obtemos:

$$\begin{aligned}\operatorname{div}\left(f^{-1} f\right) = 0 \;&\Rightarrow\; \operatorname{div}\left(f^{-1}\right) + \operatorname{div}(f) = 0 \\ &\Rightarrow\; \operatorname{div}\left(f^{-1}\right) = -\operatorname{div}(f).\end{aligned}$$

□

Corolário 2.5.1 *O conjunto de divisores principais*

$$\operatorname{Princ}(F) = \{\operatorname{div}(f) \mid f \in F \setminus \{0\}\}$$

é um grupo.

Definição 2.5.3 O grupo do corolário anterior, que é por sua vez um é um subgrupo de $\operatorname{Div}(F)$ (item *(i)* da proposição), é chamado *grupo dos divisores principais de* $F|K$.

Definição 2.5.4 (1) Se $\mathfrak{p} \in \mathfrak{P}$ é tal que $v_{\mathfrak{p}}(f) > 0$ então diz-se que $\mathfrak{p}$ é um *zero* de f. Se $v_{\mathfrak{p}}(f) < 0$ então diz-se que $\mathfrak{p}$ é um *polo* de f.

(2) Seja $f \in F$, $f \neq 0$. Definimos o *divisor de zeros de* f e o *divisor de pólos de* f, respectivamente, por:

$$\operatorname{div}_0(f) = \sum_{\substack{\mathfrak{p}\in\mathfrak{P} \\ v_{\mathfrak{p}}(f)>0}} v_{\mathfrak{p}}(f)\,\mathfrak{p} \quad \text{e} \quad \operatorname{div}_\infty(f) = \sum_{\substack{\mathfrak{p}\in\mathfrak{P} \\ v_{\mathfrak{p}}(f)<0}} (-v_{\mathfrak{p}}(f))\,\mathfrak{p}.$$

Proposição 2.5.2 *Seja $f \in F$, $f \neq 0$. Então:*

(i) $\operatorname{div}_0(f) \geq 0$ *e* $\operatorname{div}_\infty(f) \geq 0$.

(ii) $\operatorname{div}(f) = \operatorname{div}_0(f) - \operatorname{div}_\infty(f)$.

(iii) $\operatorname{gr}(\operatorname{div}_0(f)) = \operatorname{gr}(\operatorname{div}_\infty(f))$.

DEMONSTRAÇÃO: Imediato da definição. □

Teorema 2.5.1 *Todos os divisores principais tem grau zero. Mais precisamente, seja $f \in F \setminus K$, então*

$$\operatorname{gr}(\operatorname{div}_0(f)) = \operatorname{gr}(\operatorname{div}_\infty(f)) = [F : K(x)].$$

DEMONSTRAÇÃO: [75, Teorema 1.4.11]. □

2.6 Espaço de Riemann-Roch

Proposição 2.6.1 *Seja D um divisor de $F|K$. O conjunto*

$$L(D) := \{f \in F \setminus \{0\} \mid \operatorname{div}(f) + D \geq 0\} \cup \{0\}.$$

é um K-espaço vetorial.

DEMONSTRAÇÃO: Observamos inicialmente que se $D = \sum_{\mathfrak{p}\in\mathfrak{P}} n_{\mathfrak{p}}\mathfrak{p}$, então $L(D)$ pode-se ser descrito equivalentemente como o conjunto das funções f tal que $v_{\mathfrak{p}}(f) + n_{\mathfrak{p}} \geq 0$ para todo $\mathfrak{p} \in \mathfrak{P}$. Desta forma, se $f, h \in L(D)$ então

$$v_{\mathfrak{p}}(f+h) + n_{\mathfrak{p}} \geq \min\{v_{\mathfrak{p}}(f), v_{\mathfrak{p}}(h)\} + n_{\mathfrak{p}} \geq 0,$$

para todo $\mathfrak{p} \in \mathfrak{P}$, logo $f + h \in L(D)$. Da mesma forma, se $a \in K$ e $f \in L(D)$ então

$$v_{\mathfrak{p}}(af) + n_{\mathfrak{p}} = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(f) + n_{\mathfrak{p}} = \begin{cases} v_{\mathfrak{p}}(f) + n_{\mathfrak{p}} \geq 0 & \text{se} \quad a \neq 0, \\ \infty \geq 0 & \text{se} \quad a = 0, \end{cases}$$

para todo $\mathfrak{p} \in \mathfrak{P}$, logo $af \in L(D)$. Por fim, as propriedades de espaço vetorial seguem de imediato da definição de $L(D)$ e da Proposição 2.4.1. □

Definição 2.6.1 O espaço $L(D)$ da proposição anterior é chamado *espaço de Riemann-Roch associado* D.

Definição 2.6.2 Uma *série linear* referente ao divisor D, denotada por $|D|$, é um subespaço vetorial de $L(D)$. Uma série linear é dita *completa* se ela é igual a todo $L(D)$. Diremos que a série linear tem *grau* d e *dimensão* n se $\mathrm{gr}(D) = d$, e o subespaço tem dimensão $n+1$.

Definição 2.6.3 O grupo quociente

$$\mathrm{Cl}(F) = \mathrm{Div}(F) \,/\, \mathrm{Princ}(F)$$

é chamado *grupo de classes dos divisores de* $F|K$. Para um divisor $D \in \mathrm{Div}(F)$, o elemento correspondente no grupo quociente $\mathrm{Cl}(F)$ é denotado por $[D]$, a *classe de divisor* de D. Dois divisores $D, D' \in \mathrm{Div}(F)$ são ditos *equivalentes*, e escrevemos

$$D \sim D',$$

se $[D] = [D']$, isto é, $D = D' + \mathrm{div}(f)$ para algum $f \in F \setminus \{0\}$.

Observação 2.6.1 Na definição acima assumimos que $\sim$ é uma classe de equivalência. Com efeito, mostremos que de fato isso se verifica:

(i) *Reflexividade:* Se $a \in K^{\times}$, então $\mathrm{div}(a) = 0$, logo $D + \mathrm{div}(a) = D$, e assim $D \sim D$.

(ii) *Simetria:* Se $D \sim D'$ então $D' = D + \mathrm{div}(f)$ para $f \in F \setminus \{0\}$, logo $D' + \mathrm{div}\left(f^{-1}\right) = D + \mathrm{div}(f) + \mathrm{div}\left(f^{-1}\right) = D + \mathrm{div}(f) - \mathrm{div}(f) = D$, de forma que $D' \sim D$.

(iii) *Transitividade:* Se $D \sim D'$ e $D' \sim D''$, então existem $f, h \in F \setminus \{0\}$ tais que $D' = D + \mathrm{div}(f)$ e $D'' = D' + \mathrm{div}(h)$, logo $D'' = D + \mathrm{div}(f) + \mathrm{div}(h)$ e aplicando o item *(i)* da Proposição 2.5.1 concluímos que $D'' = D + \mathrm{div}(fh)$, portanto $D \sim D''$.

□

Proposição 2.6.2 *Se* D *e* D' *são divisores de* $F|K$ *tal que* $D \sim D'$*, então*

$$L(D) \cong L\left(D'\right).$$

Demonstração: Como $D \sim D'$ temos que $D' = D + \mathrm{div}(f)$ para algum $f \in F \setminus \{0\}$. Definimos então $\varphi : L(D) \to L(D')$ por:

$$h \mapsto \varphi(h) = \frac{h}{f}.$$

Seja $h \in L(D)$ então $\operatorname{div}(h) + D \geq 0$, assim

$$\operatorname{div}(h) - \operatorname{div}(f) + \operatorname{div}(f) + D = \operatorname{div}(h/f) + \operatorname{div}(f) + D \geq 0,$$

isto é, $\operatorname{div}(h/f) + D' \geq 0$, o que mostra que φ está bem definida. Mostremos que φ é um isomorfismo de K-espaços vetoriais. Com efeito:

- Sejam $h_1, h_2 \in L(D)$, então

  $$\varphi(h_1 + h_2) = \frac{h_1 + h_2}{f} = \frac{h_1}{f} + \frac{h_2}{f} = \varphi(h_1) + \varphi(h_2),$$

  logo φ é linear.

- Sejam $h_1, h_2 \in L(D)$, então

  $$\varphi(h_1) = \varphi(h_2) \;\Rightarrow\; \frac{h_1}{f} = \frac{h_2}{f} \;\Rightarrow\; h_1 = h_2,$$

  portanto φ e injetiva.

- Seja $z \in L(D')$, então $\operatorname{div}(z) + D' \geq 0$, logo

  $$\operatorname{div}(z) + \operatorname{div}(f) + D = \operatorname{div}(zf) + D \geq 0,$$

  portanto $zf \in L(D)$ e assim $\varphi(zf) = z$, isto é, φ é sobrejetiva.

□

Definição 2.6.4 Para D divisor de $F|K$, o inteiro $\ell(D) = \dim L(D)$ é chamado a *dimensão do divisor D*.

Proposição 2.6.3 *Sejam D e D' divisores com $D \sim D'$. Então*

$$\ell(D) = \ell(D') \quad e \quad \operatorname{gr}(D) = \operatorname{gr}(D').$$

Demonstração: Que $\ell(D) = \ell(D')$ segue de imediato da Proposição 2.6.2. Por outro lado, como $D' = D + \operatorname{div}(f)$ e com base no Teorema 2.5.1, temos que $\operatorname{gr}(D') = \operatorname{gr}(D) + \operatorname{gr}(\operatorname{div}(f)) = \operatorname{gr}(D)$. □

Proposição 2.6.4 *Seja D um divisor de $F|K$ tal que $\operatorname{gr}(D) < 0$, então $\ell(D) = 0$, isto é, $L(D) = \{0\}$.*

Demonstração: Suponha que existe $f \in L(D)$, $f \neq 0$, então $\operatorname{div}(f) + D \geq 0$. Temos ainda que $\operatorname{gr}(\operatorname{div}(f) + D) = \operatorname{gr}(\operatorname{div}(f)) + \operatorname{gr}(D) = \operatorname{gr}(D)$, ou seja, $\operatorname{gr}(D) \geq 0$, contrariando a hipótese. □

Proposição 2.6.5 *(i) Se $D \geq 0$ então $K \subset L(D)$.*

(ii) Se $D = 0$ então $L(D) = K$, isto é, $\ell(D) = 1$.

Demonstração: *(i)* Seja $D \geq 0$ e seja $a \in K \setminus \{0\}$. Como $v_{\mathfrak{p}}(a) = 0$ para todos os lugares $\mathfrak{p}$ de $F|K$, obtemos que $\operatorname{div}(a) = 0$, portanto $\operatorname{div}(a) + D \geq 0$ e assim $K \subset L(D)$.

(ii) Seja $D = 0$, se $f \in L(D) \cap (F \setminus K)$ então da Proposição 2.5.2*(ii)* e do Teorema 2.5.1 existe um lugar $\mathfrak{p}$ tal que $v_{\mathfrak{p}}(f) < 0$ e assim não podemos ter $\operatorname{div}(f) + 0 \geq 0$ donde $L(D) = K$. □

2.7 Gênero de um Divisor

Definição 2.7.1 O *gênero* de $F|K$ é definido por:

$$g = \max\{\operatorname{gr}(D) - \ell(D) + 1 \mid D \in \operatorname{Div}(F)\}.$$

Proposição 2.7.1 *O gênero de $F|K$ é um inteiro não negativo.*

Demonstração: Se $\operatorname{gr}(D) < 0$ existe $-D \in \operatorname{Div}(F)$ tal que $\operatorname{gr}(-D) > 0$ e $g > 0$, pois, neste caso, $\ell(D) = 0$ (Proposição 2.6.4). Por outro lado, se $D = 0$ temos $\operatorname{gr}(D) = 0$ e da Proposição 2.6.5 *(ii)* temos que $\ell(D) = 1$, assim temos que $\operatorname{gr}(0) - \ell(0) + 1 = 0$. Portanto $g \geq 0$. □

Teorema 2.7.1 (Riemann) *Seja $F|K$ um corpo de funções de gênero g. Então:*

(i) Para todo divisor $D \in \operatorname{Div}(F)$, tem-se que:

$$\ell(D) \geq \operatorname{gr}(D) + 1 - g.$$

(ii) Existe um inteiro c, dependendo unicamente do corpo de funções $F|K$, tal que se $\operatorname{gr}(D) \geq c$ então

$$\ell(D) = \operatorname{gr}(D) + 1 - g.$$

Demonstração: *(i)* Isso é justamente a definição de gênero.

(ii) Tomemos um divisor D_0 com $g = \operatorname{gr}(D_0) - \ell(D_0) + 1$ e seja $c = \operatorname{gr}(D_0) + g$. Se $\operatorname{gr}(D) \geq c$ então

$$\ell(D - D_0) \geq \operatorname{gr}(D - D_0) + 1 - g \geq c - \operatorname{gr}(D_0) + 1 - g = 1.$$

Assim existe um elemento $f \in L(D - D_0) \setminus \{0\}$. Consideremos agora o divisor $D' = D + \operatorname{div}(f)$, o qual é $\geq D_0$. Usando a Proposição 2.6.3, temos

$$\operatorname{gr}(D) - \ell(D) = \operatorname{gr}(D') - \ell(D') \geq \operatorname{gr}(D_0) - \ell(D_0) = g - 1.$$

Portanto, $\ell(D) \leq \operatorname{gr}(D) + 1 - g$. □

Exemplo 2.7.1 Vamos mostrar que o corpo de funções racionais $K(X)|K$ tem gênero $g = 0$. Para isso tomemos $\mathfrak{p}_\infty$ como no Exemplo 2.3.1 (p. 29). Considere para $r \geq 0$ o espaço vetorial $L(r\mathfrak{p}_\infty)$. Naturalmente os elementos $1, X, \ldots, X^r$ estão em $L(r\mathfrak{p}_\infty)$, logo

$$r + 1 \leq \ell(r\mathfrak{p}_\infty) = \operatorname{gr}(r\mathfrak{p}_\infty) + 1 - g = r + 1 - g.$$

De forma que $g \leq 0$. Como $g \geq 0$ para todo corpo de funções, segue a afirmação.

2.8 O Teorema de Riemann-Roch

Definição 2.8.1 Para $D \in \operatorname{Div}(F)$ o inteiro

$$\mathfrak{i}(D) = \ell(D) - \operatorname{gr}(D) + g - 1$$

é chamado *índice de especialidade* de D.

Observação 2.8.1 O Teorema de Riemann 2.7.1 garante que $\mathfrak{i}(D)$ é um inteiro não negativo, e $\mathfrak{i}(D) = 0$ se $\operatorname{gr}(D)$ é suficientemente grande.

Definição 2.8.2 Um *adele* de $F|K$ é uma aplicação

$$\begin{array}{rccc} \alpha: & \mathfrak{P} & \to & F \\ & \mathfrak{p} & \mapsto & \alpha_{\mathfrak{p}} \end{array}$$

tal que $\alpha_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}$ para quase todo $\mathfrak{p} \in \mathfrak{P}$.

Observação 2.8.2 Em geral consideramos um adele como um elemento do produto direto $\prod_{\mathfrak{p}\in\mathfrak{P}} F$ e portanto usamos a notação $\alpha = (\alpha_{\mathfrak{p}})_{\mathfrak{p}\in\mathfrak{P}}$ ou, abreviadamente, $\alpha = (\alpha_{\mathfrak{p}})$.

Definição 2.8.3 O conjunto

$$\mathfrak{A} = \mathfrak{A}_F = \{\alpha \mid \alpha \text{ é um adele de } F|K\}$$

é chamado *espaço adélico* de $F|K$.

Observação 2.8.3 O espaço adélico pode ser considerado, de forma canônica, como um espaço vetorial sobre K.

Definição 2.8.4 O *adele principal* de um elemento $f \in F$ é o adele cujos componentes são todas iguais a f.

Observação 2.8.4 A definição acima nos fornece o mergulho $F \hookrightarrow \mathfrak{A}$. As valorizações $v_{\mathfrak{p}}$ de $F|K$ estendem-se naturalmente a $\mathfrak{A}$ pondo

$$v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})$$

onde $\alpha_{\mathfrak{p}}$ é a $\mathfrak{p}$-componente do adele α. Por definição temos que $v_{\mathfrak{p}}(\alpha) \geq 0$ para quase todo $\mathfrak{p} \in \mathfrak{P}$.

Definição 2.8.5 Para $D \in \mathrm{Div}(F)$ definimos

$$\mathfrak{A}(D) = \mathfrak{A}_F(D) = \{\alpha \in \mathfrak{A} \mid v_{\mathfrak{p}}(\alpha) \geq v_{\mathfrak{p}}(D) \text{ para todo } \mathfrak{p} \in \mathfrak{P}\}.$$

Observação 2.8.5 O conjunto $\mathfrak{A}(D)$ é um subespaço de $\mathfrak{A}$.

Teorema 2.8.1 *Para qualquer divisor D tem-se que o índice de especialidade satisfaz a equação:*

$$\mathfrak{i}(D) = \dim\left(\frac{\mathfrak{A}}{\mathfrak{A}(D) + F}\right).$$

Demonstração: [75, Teorema 1.5.4] □

Observe que, embora os espaços vetoriais $\mathfrak{A}$, $\mathfrak{A}(D)$ e F sejam de dimensão infinita, o teorema afirma que o espaço quociente $\mathfrak{A}/(\mathfrak{A}(D) + F)$ tem dimensão finita sobre K. Como corolário, obtemos outra caracterização do gênero $F|K$.

Corolário 2.8.1

$$g = \dim\left(\frac{\mathfrak{A}}{\mathfrak{A}(0) + F}\right).$$

Demonstração: $\mathfrak{i}(0) = \ell(0) + \mathrm{gr}(0) + g - 1 = 1 - 0 + g - 1 = g$. □

O Teorema 2.8.1 pode ser reescrito como segue: *Para todo $D \in \mathrm{Div}(F)$ tem-se a equação:*

$$\ell(D) = \mathrm{gr}(D) + 1 - g + \dim\left(\frac{\mathfrak{A}}{\mathfrak{A}(D) + F}\right). \tag{2-1}$$

Esta é uma versão preliminar do Teorema de Riemann-Roch que apresentaremos nesta seção.

Definição 2.8.6 Um *diferencial de Weil* é uma aplicação K-linear $\omega : \mathfrak{A} \to K$ que se anula em $\mathfrak{A}(D) + F$ para algum divisor $D \in \mathrm{Div}(F)$.

Definição 2.8.7 O *módulo dos diferenciais de Weil* de $F|K$ é definido por

$$\Omega_F = \{\omega \mid \omega \text{ é um diferencial de Weil de } F|K\}.$$

Definição 2.8.8 Para $D \in \mathrm{Div}(F)$ definimos

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

Proposição 2.8.1 *O conjunto Ω_F é um K-espaço vetorial e $\Omega_F(D)$ é um subespaço de Ω_F.*

Demonstração: Se ω_1 se anula em $\mathfrak{A}(D_1) + F$ e ω_2 se anula em $\mathfrak{A}(D_2) + F$ então $\omega_1 + \omega_2$ se anula em $\mathfrak{A}(D_3)$ para qualquer divisor D_3 com $D_3 \leq D_1$ e $D_3 \leq D_2$; e $a\omega_1$ se anula em $\mathfrak{A}(D_1) + F$ para qualquer $a \in K$. A segunda parte da proposição é imediata. □

Proposição 2.8.2 *Para $D \in \mathrm{Div}(F)$ temos que*

$$\dim \Omega_F(D) = \mathfrak{i}(D).$$

Demonstração: O conjunto $\Omega_F(D)$ é canonicamente isomorfo ao espaço das formas lineares em $\mathfrak{A}/(\mathfrak{A}(D) + F)$. Como, segundo o Teorema 2.8.1, $\mathfrak{A}/(\mathfrak{A}(D) + F)$ é um espaço de dimensão finita de dimensão $\mathfrak{i}(D)$, o resultado segue. □

Corolário 2.8.2 $\Omega_F \neq 0$.

Demonstração: Para um divisor D com grau ≤ -2, temos

$$\dim \Omega_F(D) = \mathfrak{i}(D) = \ell(D) - \mathrm{gr}(D) + g - 1 \geq 1,$$

logo $\Omega_F(D) \neq 0$. □

Definição 2.8.9 Para $f \in F$ e $\omega \in \Omega_F$ definimos $f\omega : \mathfrak{A} \to K$ por

$$(f\omega)(\alpha) = \omega(f\alpha).$$

Proposição 2.8.3 *A função $f\omega$ dado na definição acima é em si um diferencial de Weil de $F|K$.*

Demonstração: De fato, como ω se anula em $\mathfrak{A}(D)+F$ então $f\omega$ se anula em $\mathfrak{A}(D+\operatorname{div}(f))+F$. □

Proposição 2.8.4 *Ω_F é um espaço vetorial sobre F de dimensão* 1.

Demonstração: [75, Proposição 1.5.9]. □

O próximo teorema associa a cada diferencial de Weil um divisor.

Teorema 2.8.2 *Para cada $\omega \in \Omega_F \setminus \{0\}$, definimos*

$$M(\omega) = \{D \in \operatorname{Div}(F) \mid \omega \text{ se anula em } \mathfrak{A}(D)+F\}.$$

Assim existe um divisor unicamente determinado $W \in M(\omega)$ tal que $D \leq W$ para todo $D \in M(\omega)$.

Demonstração: Pelo Teorema de Riemann (p. 35) existe uma constante c, dependendo unicamente do corpo de funções $F|K$, com a propriedade $\mathfrak{i}(D)=0$ para todo $D \in \operatorname{Div}(F)$ de grau $\geq c$. Como, $\dim(\mathfrak{A}/\mathfrak{A}(D)+F) = \mathfrak{i}(D)$ de acordo com o Teorema 2.8.1, temos que $\operatorname{gr}(D) < c$ para todo $D \in M(\omega)$. Portanto, podemos escolher um divisor $W \in M(\omega)$ de grau máximo.

Suponha que W não tenha a propriedade do teorema. Então existe um divisor $D_0 \in M(\omega)$ com $D_0 \not\leq W$, *i.e.* $v_{\mathfrak{q}}(D_0) > v_{\mathfrak{q}}(W)$ para algum $\mathfrak{q} \in \mathfrak{P}$.

Afirmamos que

$$W + \mathfrak{q} \in M(\omega), \qquad (*)$$

o que contradiz a maximalidade de W.

Com efeito, considere um adele $\alpha = (\alpha_{\mathfrak{p}}) \in \mathfrak{A}(W+\mathfrak{q})$. Podemos escrever $\alpha = \alpha' + \alpha''$ com

$$\alpha'_{\mathfrak{p}} = \begin{cases} \alpha_{\mathfrak{p}} & \text{para} \quad \mathfrak{p} \neq \mathfrak{q}, \\ 0 & \text{para} \quad \mathfrak{p} = \mathfrak{q}, \end{cases} \quad \text{e} \quad \alpha''_{\mathfrak{p}} = \begin{cases} 0 & \text{para} \quad \mathfrak{p} \neq \mathfrak{q}, \\ \alpha_{\mathfrak{q}} & \text{para} \quad \mathfrak{p} = \mathfrak{q}. \end{cases}$$

Então $\alpha' \in \mathfrak{A}(W)$ e $\alpha'' \in \mathfrak{A}(D_0)$, logo

$$\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0.$$

Portanto ω se anula $\mathfrak{A}(W+\mathfrak{q})+F$, e assim $(*)$ está provado.

A unicidade de W é imediata. □

A seguintes definições fazem sentido em vista do teorema anterior.

Definição 2.8.10 O divisor $\operatorname{div}(\omega)$ de um diferencial de Weil $\omega \neq 0$ é o divisor unicamente determinado de $F|K$ que satisfaz:

(i) ω se anula em $\mathfrak{A}(\operatorname{div}(\omega)) + F$, e

(ii) se ω se anula em $\mathfrak{A}(D) + F$ então $D \leq \operatorname{div}(\omega)$.

Definição 2.8.11 Para $\omega \in \Omega_F \setminus \{0\}$ e $\mathfrak{p} \in \mathfrak{P}$ definimos $v_{\mathfrak{p}}(\omega) = v_{\mathfrak{p}}(\operatorname{div}(\omega))$.

Definição 2.8.12 (1) Um lugar $\mathfrak{p}$ diz-se um *zero* (respectivamente, um *polo*) de ω se $v_{\mathfrak{p}}(\omega) > 0$ (respectivamente, $v_{\mathfrak{p}}(\omega) < 0$).

(2) O diferencial de Weil ω é dito *regular em* $\mathfrak{p}$ se $v_{\mathfrak{p}}(\omega) \geq 0$, e é dito *regular* (ou *holomorfo*) se é regular em todos os lugares $\mathfrak{p} \in \mathfrak{P}$.

Definição 2.8.13 Um divisor W é dito um *divisor canônico* de $F|K$ se $W = \operatorname{div}(\omega)$ para algum $\omega \in \Omega_F$.

Como consequência imediata dessas definições temos que:

$$\Omega_F(D) = \{\omega \in \Omega_F \mid \omega = 0 \text{ ou } \operatorname{div}(\omega) \geq D\}. \tag{2-2}$$

Desta forma,

$$\Omega_F(0) = \{\omega \in \Omega_F \mid \omega \text{ é regular}\}.$$

Assim, como consequência da Proposição 2.8.2 e da Definição 2.8.1, obtemos

$$\dim \Omega_F(0) = g.$$

Proposição 2.8.5 *(i) Para $f \in F \setminus \{0\}$ e $\omega \in \Omega_F \setminus \{0\}$ temos que*

$$\operatorname{div}(f\omega) = \operatorname{div}(f) + \operatorname{div}(\omega).$$

(ii) Quaisquer dois divisores canônicos de $F|K$ são equivalentes.

Resulta dessa proposição que os divisores canônicos de $F|K$ formam uma classe completa $[W]$ no grupo de classes de divisores $\operatorname{Cl}(F)$; esta classe é chamada de *classe canônica* de $F|K$.

Demonstração da Proposição 2.8.5: Se ω se anula em $\mathfrak{A}(D) + F$ então $f\omega$ se anula em $\mathfrak{A}(D + \operatorname{div}(f)) + F$, consequentemente

$$\operatorname{div}(\omega) + \operatorname{div}(f) \leq \operatorname{div}(f\omega).$$

da mesma forma,

$$\operatorname{div}(f\omega) + \operatorname{div}\left(f^{-1}\right) \leq \operatorname{div}\left(f^{-1}f\omega\right) = \operatorname{div}(\omega).$$

Combinando estas duas desigualdades, obtemos

$$\operatorname{div}(\omega) + \operatorname{div}(f) \leq \operatorname{div}(f\omega) \leq -\operatorname{div}\left(f^{-1}\right) + \operatorname{div}(\omega) = \operatorname{div}(\omega) + \operatorname{div}(f).$$

Isto prova o item *(i)*. O item *(ii)* segue do item *(i)* e da Proposição 2.8.4. □

Teorema 2.8.3 (Teorema da Dualidade) *Seja D um divisor arbitrário de $F|K$ e seja $W = \operatorname{div}(\omega)$ um divisor canônico de $F|K$. Então a aplicação*

$$\begin{array}{rccc} \mu: & L(W-D) & \to & \Omega_F(D) \\ & f & \mapsto & f\omega \end{array}$$

é um isomorfismo de K-espaços vetoriais. Em particular,

$$\mathfrak{i}(D) = \ell(W-D).$$

Demonstração: Para $f \in L(W-D)$ temos que

$$\operatorname{div}(f\omega) = \operatorname{div}(f) + \operatorname{div}(\omega) \geq -(W-D) + W = D,$$

logo, de acordo com a equação (2-2), $f\omega \in \Omega_F(D)$. Portanto μ é uma aplicação de $L(W-D)$ em $\Omega_F(D)$. Pode-se ver facilmente que μ é linear e injetiva. Para mostrarmos que μ é sobrejetiva, consideramos o diferencial de Weil $\omega_1 \in \Omega_F(D)$. De acordo com a Proposição 2.8.4, podemos escrever $\omega_1 = f\omega$ para algum $f \in F$. Como

$$\operatorname{div}(f) + W = \operatorname{div}(f) + \operatorname{div}(\omega) = \operatorname{div}(f\omega) = \operatorname{div}(\omega_1) \geq D,$$

obtemos que $\operatorname{div}(f) \geq -(W-D)$, logo $f \in L(W-D)$ e $\omega_1 = \mu(x)$. Provamos assim que

$$\dim \Omega_F(D) = \ell(W-D).$$

Como $\dim \Omega_F(D) = \mathfrak{i}(D)$, conforme a Proposição 2.8.2, obtemos que $\mathfrak{i}(D) = \ell(W-D)$. □

Estamos agora em condições de enunciar e demonstrar o principal resultado da teoria dos corpos de funções.

Teorema 2.8.4 (Riemann-Roch) *Seja W um divisor canônico de $F|K$. Então para cada divisor $D \in \operatorname{Div}(F)$, vale a igualdade*

$$\ell(D) = \operatorname{gr}(D) + 1 - g + \ell(W-D).$$

DEMONSTRAÇÃO: Do Teorema da Dualidade temos que $\ell(W-D) = \mathfrak{i}(D)$ e a definição de índice de especialidade de D nos diz que $\mathfrak{i}(D) = \ell(D) - \mathrm{gr}(D) + g - 1$, logo $\ell(W-D) = \ell(D) - \mathrm{gr}(D) + g - 1$, ou seja, $\ell(D) = \mathrm{gr}(D) + 1 - g + \ell(W-D)$. □

Corolário 2.8.3 *Se W é um divisor canônico, temos que*

$$\mathrm{gr}(W) = 2g - 2 \quad e \quad \ell(W) = g.$$

DEMONSTRAÇÃO: Para $D = 0$, o Teorema de Riemann-Roch e a Proposição 2.6.5*(ii)* nos dão que

$$1 = \ell(0) = \mathrm{gr}(0) + 1 - g + \ell(W-0).$$

Assim $\ell(W) = g$. Pondo $D = W$ obtemos

$$g = \ell(W) = \mathrm{gr}(W) + 1 - g + \ell(W-W) = \mathrm{gr}(W) + 2 - g.$$

Portanto $\mathrm{gr}(W) = 2g - 2$. □

Capítulo 3

Curvas Algébricas

Salvo as seções 3.7 e 3.8, em todo este capítulo K denotará um corpo algebricamente fechado.

3.1 Variedades Afins

Definição 3.1.1 O *espaço afim* n-dimensional $\mathbb{A}^n = \mathbb{A}^n(K)$ é o conjunto de todas n-uplas de elementos de K. Um elemento $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$ é dito um *ponto*, e $a_1, \ldots, a_n$ as *coordenadas* de P.

Definição 3.1.2 Seja $K[X_1, \ldots, K_n]$ um anel de polinômios em n variáveis sobre K. Um subconjunto $\mathfrak{V} \subset \mathbb{A}^n$ é dito um *conjunto algébrico* se existe $M \subset K[X_1, \ldots, X_n]$ tal que

$$\mathfrak{V} = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ para todo } F \in M\}.$$

Definição 3.1.3 Dado um conjunto algébrico $\mathfrak{V} \subset \mathbb{A}^n$, o conjunto de polinômios

$$\mathfrak{a}(\mathfrak{V}) = \{F \in K[X_1, \ldots, X_n] \mid F(P) = 0 \text{ para todo } P \in \mathfrak{V}\}$$

é chamado *ideal de* $\mathfrak{V}$.

Observação 3.1.1 O conjunto $\mathfrak{a}(\mathfrak{V})$ é claramente um ideal de $K[X_1, \ldots, X_n]$ e, segundo o Teorema da Base de Hilbert ([22, Teorema III.5.2]), pode ser gerado por um número finito de polinômios $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$.

Em vista da observação acima temos a seguinte proposição:

Proposição 3.1.1 *Existem* $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$ *tal que*

$$\mathfrak{V} = \{P \in \mathbb{A}^n \mid F_1(P) = \cdots = F_r(P) = 0\}.$$

Definição 3.1.4 Um conjunto algébrico $\mathfrak{V} \subset \mathbb{A}^n$ é dito *irredutível* se não pode ser escrito como $\mathfrak{V} = \mathfrak{V}_1 \cup \mathfrak{V}_2$, em que $\mathfrak{V}_1$ e $\mathfrak{V}_2$ são subconjunto algébricos próprios de $\mathfrak{V}$

Proposição 3.1.2 *O conjunto algébrico* $\mathfrak{V} \subset \mathbb{A}^n$ *é irredutível se, e somente se, seu ideal correspondente* $\mathfrak{a}(\mathfrak{V})$ *é primo.*

Demonstração: Se $\mathfrak{a}(\mathfrak{V})$ não é primo, existem $F, G \in K[X_1, \ldots, X_n]$ tais que $FG \in \mathfrak{a}(\mathfrak{V})$ mas $F, G \notin \mathfrak{a}(\mathfrak{V})$. Assim, existem $P_1, P_2 \in \mathfrak{V}$ tais que $F(P_1) \neq 0$ e $G(P_2) \neq 0$, logo $F \in \mathfrak{a}(\mathfrak{V} \setminus \{P_1\})$ e $G \in \mathfrak{a}(\mathfrak{V} \setminus \{P_2\})$, portanto, $\mathfrak{V} = (\mathfrak{V} \setminus \{P_1\}) \cup (\mathfrak{V} \setminus \{P_2\})$. Invertendo os passos temos a recíproca. □

Definição 3.1.5 Uma *variedade afim* é um conjunto algébrico irredutível $\mathfrak{V} \subset \mathbb{A}^n$.

Definição 3.1.6 O *anel de coordenadas* de uma variedade $\mathfrak{V}$ é seguinte anel das classes residuais:

$$\Gamma(\mathfrak{V}) = \frac{K[X_1, \ldots, X_2]}{\mathfrak{a}(\mathfrak{V})}.$$

Proposição 3.1.3 *O anel* $\Gamma(\mathfrak{V})$ *é um domínio de integridade.*

Demonstração: Conforme a Proposição 3.1.2, $\mathfrak{a}(\mathfrak{V})$ é um ideal primo, donde, por definição, segue o resultado. □

Observação 3.1.2 Todo $f = F + \mathfrak{a}(\mathfrak{V}) \in \Gamma(\mathfrak{V})$ induz uma função $f : \mathfrak{V} \to K$ tomando $f(P) = F(P)$ para $P \in \mathfrak{V}$.

Definição 3.1.7 O corpo de frações

$$K(\mathfrak{V}) = \mathrm{cf}(\Gamma(\mathfrak{V}))$$

é dito o *corpo de funções de* $\mathfrak{V}$.

Proposição 3.1.4 *O corpo de funções* $K(\mathfrak{V})$ *contém a* K *como subcorpo.*

Demonstração: Segue da Observação 3.1.2 acima. □

Definição 3.1.8 A *dimensão de uma variedade afim* $\mathfrak{V}$ é o grau de transcendência de $K(\mathfrak{V})$ sobre K.

Proposição 3.1.5 *Para cada ponto $P \in \mathfrak{V}$, conjunto*

$$\mathcal{O}_P(\mathfrak{V}) = \left\{ f \in K(\mathfrak{V}) \;\middle|\; f = \frac{g}{h} \text{ com } g,h \in \Gamma(\mathfrak{V}) \text{ e } h(P) \neq 0 \right\}.$$

é um anel local com corpo de frações $K(\mathfrak{V})$ e cujo único ideal maximal é:

$$\mathfrak{m}_P(\mathfrak{V}) = \left\{ f \in K(\mathfrak{V}) \;\middle|\; f = \frac{g}{h} \text{ com } g,h \in \Gamma(\mathfrak{V}),\ h(P) \neq 0 \text{ e } g(P) = 0 \right\}.$$

Demonstração: Basta observar que $\mathcal{O}_P(\mathfrak{V})$ é a localização de $\Gamma(\mathfrak{V})$ em $\mathfrak{m}_P(\mathfrak{V})$ [12, Capítulo 4]. □

Definição 3.1.9 O anel $\mathcal{O}_P(\mathfrak{V})$ é chamado *anel local* de $\mathfrak{V}$.

3.2 Variedades Projetivas

Proposição 3.2.1 *A relação $\sim$ sobre $\mathbb{A}^n \setminus \{(0,\ldots,0)\}$ definida abaixo é um relação de equivalência:*

$$(a_0,\ldots,a_n) \sim (b_0,\ldots,b_n)$$
$$\Updownarrow$$
existe um elemento $\lambda \in K \setminus \{0\}$ tal que $b_i = \lambda a_i$ para $0 \leq i \leq n$.

Demonstração: $(a_0,\ldots,a_n) = (1a_0,\ldots,1a_n)$, logo $(a_0,\ldots,a_n) \sim (a_0,\ldots,a_n)$.

Se $(a_0,\ldots,a_n) \sim (b_0,\ldots,b_n)$, existe $\lambda \in K \setminus \{0\}$ tal que $b_i = \lambda a_i$ para todo i. Assim $a_i = \frac{1}{\lambda} b_i$, ou seja, $(b_0,\ldots,b_n) \sim (a_0,\ldots,a_n)$.

Se $(a_0,\ldots,a_n) \sim (b_0,\ldots,b_n)$ e $(b_0,\ldots,b_n) \sim (c_0,\ldots,c_n)$, existem elementos $\lambda_1, \lambda_2 \in K \setminus \{0\}$ tais que $b_i = \lambda_1 a_i$ e $c_i = \lambda_2 b_i$ para todo $0 \leq i \leq n$. Desta forma, $c_i = (\lambda_2 \lambda_1) a_i$ e assim $(a_0,\ldots,a_n) \sim (c_0,\ldots,c_n)$. □

Notação: A classe de equivalência de $(a_0,\ldots,a_n)$ em relação a $\sim$ é denotada por $(a_0 : \ldots : a_n)$.

Definição 3.2.1 O *espaço projetivo* n-dimensional $\mathbb{P}^n = \mathbb{P}^n(K)$ é o conjunto de todas as classes de equivalência da relação $\sim$:

$$\mathbb{P}^n = \{(a_0 : \ldots : a_n) \mid a_i \in K \text{ e não são todos nulos}\}.$$

Um elemento $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$ é um *ponto*, e $a_0,\ldots,a_n$ são as *coordenadas homogêneas* de P.

Definição 3.2.2 Um *monômio* de grau d é um polinômio $G \in K[X_0, \ldots, X_n]$ da forma

$$G = a\prod_{i=0}^{n} X_i^{d_i} \text{ com } a \in K \setminus \{0\} \text{ e } \sum_{i=1}^{n} d_i = d.$$

Um polinômio F é um *polinômio homogêneo* se F é a soma de monômios de mesmo grau. Um ideal $\mathfrak{a} \subset K[X_0, \ldots, X_n]$ que é gerado por polinômios homogêneos é chamado *ideal homogêneo*.

Definição 3.2.3 Seja $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$ e $F \in K[X_0, \ldots, X_n]$ um polinômio homogêneo. Diremos que $F(P) = 0$ se $F(a_0, \ldots, a_n) = 0$.

Observação 3.2.1 A definição acima faz sentido na seguinte medida: como

$$F(\lambda a_0, \ldots, \lambda a_n) = \lambda^d F(a_0, \ldots, a_n) \quad (\text{com } d = \text{gr}(F)),$$

temos que

$$F(a_0, \ldots, a_n) = 0 \Leftrightarrow F(\lambda a_0, \ldots, \lambda a_n) = 0.$$

Definição 3.2.4 Um subconjunto $\mathfrak{V} \subset \mathbb{P}^n$ é dito um *conjunto algébrico projetivo* se existe $M \subset K[X_1, \ldots, X_n]$ tal que

$$\mathfrak{V} = \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ para todo } F \in M\}.$$

Definição 3.2.5 Um conjunto algébrico projetivo $\mathfrak{V} \subset \mathbb{P}^n$ é dito *irredutível* se não pode ser escrito como $\mathfrak{V} = \mathfrak{V}_1 \cup \mathfrak{V}_2$, em que $\mathfrak{V}_1$ e $\mathfrak{V}_2$ são subconjunto algébricos projetivos próprios de $\mathfrak{V}$

Definição 3.2.6 O ideal $\mathfrak{a}(\mathfrak{V}) \subset K[X_0, \ldots, X_n]$, que é gerado por todos os polinômios homogêneos F com $F(P) = 0$ para todo $P \in \mathfrak{V}$, é chamado *ideal de* $\mathfrak{V}$.

Proposição 3.2.2 *O conjunto $\mathfrak{V} \subset \mathbb{P}^n$ é irredutível se, e somente se, $\mathfrak{a}(\mathfrak{V})$ é um ideal homogêneo primo em $K[X_0, \ldots, X_n]$.*

Demonstração: Análoga a demonstração da Proposição 3.1.2. □

Definição 3.2.7 Uma *variedade projetiva* é um conjunto algébrico projetivo irredutível.

Definição 3.2.8 Seja $\mathfrak{V} \subset \mathbb{P}^n$. O *anel de coordenadas homogêneas* de $\mathfrak{V}$ é definido por:

$$\Gamma_h(\mathfrak{V}) = \frac{K[X_0, \ldots, K_n]}{\mathfrak{a}(\mathfrak{V})}.$$

Proposição 3.2.3 $\Gamma_h(\mathfrak{V})$ *é um domínio de integridade contendo* K.

DEMONSTRAÇÃO: Segue de imediato, fazendo a analogia adequada, da Proposição 3.1.3 e da Observação 3.1.2. □

Definição 3.2.9 Um elemento $f \in \Gamma_h(\mathfrak{V})$ é dito uma *forma* de grau d se $f = F + \mathfrak{a}(\mathfrak{V})$ para algum polinômio homogêneo $F \in K[X_0, \ldots, X_n]$ com $\operatorname{gr}(F) = d$.

Definição 3.2.10 O *corpo de funções* de $\mathfrak{V}$ é definido por

$$K(\mathfrak{V}) = \left\{ \frac{g}{h} \;\middle|\; g, h \in \Gamma_h(\mathfrak{V}) \text{ são formas de um mesmo grau e } h \neq 0 \right\}.$$

Observação 3.2.2 $K(\mathfrak{V})$ é um subcorpo de $\operatorname{cf}(\Gamma_h(\mathfrak{V}))$, o corpo de frações de $\Gamma_h(\mathfrak{V})$.

Definição 3.2.11 A *dimensão de uma variedade projetiva* $\mathfrak{V}$ é o grau de transcendência de $K(\mathfrak{V})$ sobre K.

Seja $P = (a_0 : \ldots : a_n) \in \mathfrak{V}$ e $f \in K(\mathfrak{V})$. Escrevemos $f = g/h$ em que $g = G + \mathfrak{a}(\mathfrak{V}), h = H + \mathfrak{a}(\mathfrak{V}) \in \Gamma_h(\mathfrak{V})$ e G e H são polinômios homogêneos de grau d. Como

$$\frac{G(\lambda a_0, \ldots, \lambda a_n)}{H(\lambda a_0, \ldots, \lambda a_n)} = \frac{\lambda^d G(a_0, \ldots, a_n)}{\lambda^d H(a_0, \ldots, a_n)} = \frac{G(a_0, \ldots, a_n)}{H(a_0, \ldots, a_n)},$$

podemos definir $f(P) = \frac{G(a_0,\ldots,a_n)}{H(a_0,\ldots,a_n)} \in K$, se $H(P) \neq 0$. Então, neste caso, diremos que f está *definido* em P e chamaremos $f(P)$ o *valor* de f em P.

Proposição 3.2.4 *O anel*

$$\mathcal{O}_P(\mathfrak{V}) = \{ f \in K(\mathfrak{V}) \mid f \text{ é definida em } P \} \subset K(\mathfrak{V})$$

é um anel local cujo único maximal é

$$\mathfrak{m}_P(\mathfrak{V}) = \{ f \in \mathcal{O}_P(\mathfrak{V}) \mid f(P) = 0 \}.$$

DEMONSTRAÇÃO: Segue diretamente da Proposição 3.1.5, fazendo a analogia adequada. □

3.3 Cobrindo Variedades Projetivas por Variedades Afins

Para cada $0 \leq i \leq n$ consideramos a aplicação $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$ dada por

$$\varphi_i(a_0, \ldots, a_{n-1}) = (a_0 : \ldots : a_{i-1} : 1 : a_i : \ldots : a_{n-1}).$$

Assim sendo, φ_i é uma bijeção de $\mathbb{A}^n$ sobre o conjunto

$$\mathfrak{U}_i = \{(c_0 : \ldots : c_n) \in \mathbb{P}^n \mid c_i \neq 0\},$$

e $\mathbb{P}^n = \bigcup_{i=1}^n \mathfrak{U}_i$. Portanto temos:

Proposição 3.3.1 *O espaço projetivo $\mathbb{P}^n$ pode ser coberto por $n+1$ cópias do espaço afim $\mathbb{A}^n$.*

Seja $\mathfrak{V} \subset \mathbb{P}^n$ uma variedade projetiva, então $\mathfrak{V} = \bigcup_{i=1}^n (\mathfrak{V} \cap \mathfrak{U}_i)$. Suponha que $\mathfrak{V} \cap \mathfrak{U}_i \neq \emptyset$. Então

$$\mathfrak{V}_i = \varphi_i^{-1}(\mathfrak{V} \cap \mathfrak{U}_i) \subset \mathbb{A}^n$$

é uma variedade afim, e o ideal $\mathfrak{a}(\mathfrak{V}_i)$ é dado por

$$\mathfrak{a}(\mathfrak{V}_i) = \{F(X_0, \ldots, X_i, 1, X_{i+1}, \ldots, X_n) \mid F \in \mathfrak{a}(\mathfrak{V})\}.$$

Por conveniência restringiremo-nos no que segue ao caso $i = n$ (e $\mathfrak{V} \cap \mathfrak{U}_n \neq \emptyset$).

Definição 3.3.1 O complemento

$$\mathfrak{H}_n = \mathbb{P}^n \setminus \mathfrak{U}_n = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n \mid a_n = 0\}$$

é dito o *hiperplano (no infinito)*, e os pontos $P \in \mathfrak{V} \cap \mathfrak{H}_n$ são os *pontos no infinito* de $\mathfrak{V}$ e podem serem denotados por ∞.

Proposição 3.3.2 *Existe um K-isomorfismo natural α de $K(\mathfrak{V})$ (o corpo de funções da variedade $\mathfrak{V}$) sobre $K(\mathfrak{V}_n)$ (o corpo de funções da variedade $\mathfrak{V}_n = \varphi_n^{-1}(\mathfrak{V} \cap \mathfrak{U}_n)$).*

Demonstração: Com efeito, este isomorfismo é definido da seguinte forma: Seja $f = g/h \in K(\mathfrak{V})$, onde $f, g \in \Gamma_h(\mathfrak{V})$ são formas de mesmo grau e $h \neq 0$. Tomamos polinômios homogêneos $G, H \in K[X_0, \ldots, X_n]$ que representam g respectivamente h. Sejam $G_* = G(X_0, \ldots, X_{n-1}, 1)$ e $H_* = H(X_0, \ldots, X_{n-1}, 1)$ em $K[X_0, \ldots, X_{n-1}]$. Suas classes residuais em $\Gamma(\mathfrak{V}) = K[X_0, \ldots, X_{n-1}]/\mathfrak{a}(\mathfrak{V}_n)$ são g_* respectivamente h_*. Então $\alpha(f) = g_*/h_*$. □

Notemos que sobre o isomorfismo α da proposição anterior, o anel local de um ponto $P \in \mathfrak{V} \cap \mathfrak{U}_n$ é levado *sobre* o anel local de $\varphi_n^{-1}(P) \in \mathfrak{V}_n$.

Corolário 3.3.1 *Os anéis locais $\mathcal{O}_P(\mathfrak{V} \cap \mathfrak{U}_n)$ e $\mathcal{O}_{\varphi_n^{-1}(P)}(\mathfrak{V}_n)$ são isomorfos.*

3.4 Fecho Projetivo de uma Variedade Afim

Definição 3.4.1 Para um polinômio $F = F(X_0, \ldots, X_{n-1}) \in K[X_0, \ldots, X_{n-1}]$ de grau d, definimos

$$F^* = X_n^d F\left(\frac{X_0}{X_n}, \ldots, \frac{X_{n-1}}{X_n}\right) \in K[X_0, \ldots, X_n].$$

Proposição 3.4.1 *F^* é um polinômio homogêneo de grau d em $n+1$ variáveis.*

Demonstração: Seja $F = F_0 + F_1 + \cdots + F_d \in K[X_0, \ldots, X_n]$, em que F_i, $0 \leq i \leq d$, são polinômios homogêneos de grau i, respectivamente. Então:

$$\begin{aligned} F_0 X_n^d + F_1 X_n^{d-1} + \cdots + F_{d-1} X_n + F_d & \\ = X_n^d \left(F_0 + \frac{1}{X_n} F_1 + \cdots + \frac{1}{X_n^{d-1}} F_{d-1} + \frac{1}{X_n^d} F_d\right) & \\ = X_n^d F\left(\frac{X_0}{X_n}, \cdots, \frac{X_{n-1}}{X_n}\right) = F^*. & \end{aligned}$$

□

Definição 3.4.2 Consideremos agora a variedade $\mathfrak{V} \subset \mathbb{A}^n$ e seu ideal correspondente $\mathfrak{a}(\mathfrak{V}) \subset K[X_0, \ldots, X_{n-1}]$. Definimos a variedade projetiva $\overline{\mathfrak{V}} \subset \mathbb{P}^n$ como segue:

$$\overline{\mathfrak{V}} = \{P \in \mathbb{P}^n \mid F^*(P) = 0 \text{ para todo } F \in \mathfrak{a}(\mathfrak{V})\}.$$

A variedade $\overline{\mathfrak{V}}$ é dita o *fecho projetivo* de $\mathfrak{V}$.

Observação 3.4.1 Podemos recuperar $\mathfrak{V}$ de $\overline{\mathfrak{V}}$ pelo processo descrito na Proposição 3.3.2, a saber:

$$\mathfrak{V} = \varphi_n^{-1}\left(\overline{\mathfrak{V}} \cap \mathfrak{U}_n\right) = \left(\overline{\mathfrak{V}}\right)_n.$$

Proposição 3.4.2 *Os corpos de funções de $\mathfrak{V}$ e de $\overline{\mathfrak{V}}$ são naturalmente isomorfos, e $\mathfrak{V}$ e $\overline{\mathfrak{V}}$ têm a mesma dimensão.*

Demonstração: Decorre da Observação 3.4.1 acima e da Proposição 3.3.2. □

3.5 Aplicações Racionais e Morfismos

Definição 3.5.1 Seja $\mathfrak{V} \subset \mathbb{P}^m$ e $\mathfrak{W} \subset \mathbb{P}^n$ variedades projetivas. Suponha que $F_0, \ldots, F_n \in K[X_0, \ldots, X_m]$ são polinômios homogêneos com as seguintes propriedades:

(a) $F_0, \ldots, F_n$ têm o mesmo grau;

(b) Nem todos F_i estão em $\mathfrak{a}(\mathfrak{V})$;

(c) Para todo $H \in \mathfrak{a}(\mathfrak{W})$ tem-se $H(F_0, \ldots, F_n) \in \mathfrak{a}(\mathfrak{V})$.

Seja $Q \in \mathfrak{V}$ e assumamos que $F_i(Q) \neq 0$ para ao menos um $i \in \{0, \ldots, n\}$ (por (b) um tal ponto existe). Então o ponto $(F_0(Q) : \ldots : F_n(Q)) \in \mathbb{P}^n$ está em $\mathfrak{W}$, por (c). Seja $(G_0, \ldots, G_n)$ uma outra n-upla de polinômios homogêneos satisfazendo (a), (b) e (c). Diremos que $(F_0, \ldots, F_n)$ e $(G_0, \ldots, G_n)$ são equivalentes se

(d) $F_i G_j \equiv F_j G_i \pmod{\mathfrak{a}(\mathfrak{V})}$ para $0 \leq i, j \leq n$.

A classe de equivalência de $(F_0, \ldots, F_n)$ em relação a esta relação de equivalência é denotada por

$$\phi = (F_0 : \ldots : F_n),$$

e ϕ é dita uma *aplicação racional* de $\mathfrak{V}$ em $\mathfrak{W}$.

Definição 3.5.2 Uma aplicação racional $\phi = (F_0 : \ldots : F_n)$ é dita *regular* (ou *definida*) em um ponto $P \in \mathfrak{V}$ se existem polinômios homogêneos $G_0, \ldots, G_n \in K[X_0, \ldots, X_m]$ tais que $\phi = (G_0 : \ldots : G_n)$ e $G_i(P) \neq 0$ para ao menos um i. Então definimos

$$\phi(P) = (G_0(P) : \ldots : G_n(P)) \in \mathfrak{W},$$

que está bem definida pelas condições (a) e (b) da definição anterior.

Definição 3.5.3 Duas variedades $\mathfrak{V}_1$ e $\mathfrak{V}_2$ são ditas *birracionalmente equivalentes* se existem aplicações racionais $\phi_1 : \mathfrak{V}_1 \to \mathfrak{V}_2$ e $\phi_2 : \mathfrak{V}_2 \to \mathfrak{V}_1$ tais que $\phi_1 \circ \phi_2$ e $\phi_2 \circ \phi_1$ são aplicações identidades sobre $\mathfrak{V}_2$ e sobre $\mathfrak{V}_1$, respectivamente.

Proposição 3.5.1 *As variedades $\mathfrak{V}_1$ e $\mathfrak{V}_2$ são birracionalmente equivalentes se, e somente se, seus corpos de funções $K(\mathfrak{V}_1)$ e $K(\mathfrak{V}_2)$ são K-isomorfos.*

Demonstração: Vide [20, Proposição 12 da Seção 6.6]. □

Definição 3.5.4 Uma aplicação racional $\phi : \mathfrak{V} \to \mathfrak{W}$ que é regular em todos os pontos $P \in \mathfrak{V}$ é dito um *morfismo*. Diremos que tal aplicação é um *isomorfismo* se existe um morfismo $\psi : \mathfrak{W} \to \mathfrak{V}$ tal que $\phi \circ \psi$ e $\psi \circ \phi$ são aplicações identidade sobre $\mathfrak{W}$ e $\mathfrak{V}$, respectivamente. Neste caso, $\mathfrak{V}$ e $\mathfrak{W}$ são ditas *isomorfas*. Por fim, diremos que ϕ é *birracional* se existem abertos $V \in \mathfrak{V}$ e $W \in \mathfrak{W}$, e um isomorfismo $\varphi : V \to W$ que representa ϕ.

3.6 Curvas Algébricas

Definição 3.6.1 Uma *curva algébrica projetiva (afim)* $\mathfrak{C}$ é uma variedade projetiva (afim) de dimensão um.

A definição indica que o corpo $K(\mathfrak{C})$ das funções racionais sobre $\mathfrak{C}$ é um corpo de funções algébricas de uma variável, tal como estudado em todo Capítulo 2.

Uma *curva plana afim* é uma curva $\mathfrak{C} \subset \mathbb{A}^2$. Seu ideal $\mathfrak{a}(\mathfrak{C}) \subset K[X_0, X_1]$ é gerado por um polinômio irredutível $G \in K[X_0, X_1]$ (que é único a menos de fator constante). Reciprocamente, dado um polinômio irredutível $G \in K[X_0, X_1]$, o conjunto $\mathfrak{C} = \left\{P \in \mathbb{A}^2 \mid G(P) = 0\right\}$ é uma curva plana afim, e G gera seu ideal correspondente $\mathfrak{a}(\mathfrak{C})$. Consequentemente, o ideal de uma *curva plana projetiva* $\mathfrak{C} \subset \mathbb{P}^2$ é gerado por um polinômio homogêneo irredutível $H \in K[X_0, X_1, X_2]$.

Definição 3.6.2 O *grau* de uma curva $\mathfrak{C}$, indicado por $\mathrm{gr}(\mathfrak{C})$, é o grau de um polinômio definidor da curva.

Proposição 3.6.1 *Se* $\mathfrak{C} = \left\{P \in \mathbb{A}^2 \mid G(P) = 0\right\}$ *é uma curva plana afim de grau d, o fecho projetivo* $\overline{\mathfrak{C}} \subset \mathbb{P}^2$ *é dado pelos zeros do polinômio homogêneo*

$$G^* = X_2^d \, G\left(\frac{X_0}{X_2}, \frac{X_1}{X_2}\right).$$

Definição 3.6.3 Seja $\mathfrak{C}$ uma curva afim (projetiva) gerada pelo polinômio (homogêneo) irredutível $f \in K[X_0, \ldots, X_n]$ e seja $P \in \mathfrak{C}$. Diremos que P é um ponto *singular* de $\mathfrak{C}$ se, e somente se,

$$\frac{\partial f}{\partial X_0}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0.$$

Em caso contrário, P é dita *não singular* (ou *simples*).

Observação 3.6.1 Existe somente um número finito de pontos singulares em uma curva $\mathfrak{C}$.

Proposição 3.6.2 *Um ponto $P \in \mathfrak{C}$ é não singular se o anel local $\mathcal{O}_P(\mathfrak{C})$ é um anel de valorização* (i.e., *$\mathcal{O}_P(\mathfrak{C})$ é um domínio de ideais principais contendo exatamente um ideal maximal $\neq \{0\}$).*

Demonstração: [20, Teorema 1 da Seção 3.2.] □

Definição 3.6.4 Um curva $\mathfrak{C}$ é dito *não singular* (ou *suave* ou *lisa*) se todos os pontos são não singulares.

Definição 3.6.5 Seja $\mathfrak{C}$ uma curva não singular. O *gênero* de $\mathfrak{C}$ é definido como sendo o gênero do corpo de funções $K(\mathfrak{C})$ (Definição 2.7.1, p. 35).

Em 1839, Julius Plücker publicou um importante artigo [56] que deu origem ao seguinte teorema:

Teorema 3.6.1 (Fórmulas de Plücker) *Seja $\mathfrak{C}$ uma curva plana projetiva não singular de grau d. O gênero de $\mathfrak{C}$ é dado pela seguinte fórmula:*

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

Por outro lado, se $\mathfrak{C}$ uma curva plana projetiva qualquer de grau d, então

$$g = \frac{(d-1)(d-2)}{2} - \sum_{P \in S} \delta(P),$$

em que S é o conjunto de pontos singulares de $\mathfrak{C}$ e $\delta(P) \geq 1$ é uma medida de singularidade associada a cada $P \in S$.

Para um estudo mais aprofundado das Fórmulas de Plücker, bem como suas demonstrações veja [26, Capítulo 2, Seção 4].

Consideremos agora uma aplicação racional $\phi : \mathfrak{C}_1 \to \mathfrak{C}_2$ onde $\mathfrak{C}_1$ e $\mathfrak{C}_2$ são curvas projetivas. Temos então que:

(a) ϕ é definido em todos os pontos não singulares $P \in \mathfrak{C}$. Portanto, se $\mathfrak{C}$ é uma curva não singular, ϕ é um morfismo.

(b) Se $\mathfrak{C}$ é não singular e ϕ é não constante, então ϕ é sobrejetiva.

Proposição 3.6.3 *Seja $\mathfrak{C}$ uma curva projetiva. Então existe uma curva projetiva não singular $\mathfrak{C}'$ e um morfismo birracional $\phi' : \mathfrak{C}' \to \mathfrak{C}$. O par $(\mathfrak{C}', \phi')$ é único seguinte sentido: dada outra curva não singular $\mathfrak{C}''$ e um morfismo birracional $\phi'' : \mathfrak{C}'' \to \mathfrak{C}$, existe um único isomorfismo $\phi : \mathfrak{C}' \to \mathfrak{C}''$ tal que $\phi' = \phi'' \circ \phi$.*

DEMONSTRAÇÃO: [20, Teorema 3 da Seção 7.5] □

Definição 3.6.6 A curva $\mathfrak{C}'$ (ou mais precisamente: o par $(\mathfrak{C}', \phi')$) da proposição acima é chamado *modelo não singular* da curva $\mathfrak{C}$.

Proposição 3.6.4 *Se $\phi' : \mathfrak{C}' \to \mathfrak{C}$ é um modelo não singular de $\mathfrak{C}$ e $P \in \mathfrak{C}$ é não singular, então existe um $P' \in \mathfrak{C}'$ com $\phi'(P') = P$; para um ponto singular $P \in \mathfrak{C}$ o número de $P' \in \mathfrak{C}'$ com $\phi'(P') = P$ é finito (podendo ser um).*

DEMONSTRAÇÃO: [20, Lema 2 da Seção 7.5] □

Teorema 3.6.2 *Seja o corpo de funções algébricas de uma variável $F|K$, então existe uma curva projetiva não singular $\mathfrak{C}$ (única a menos de isomorfismo) cujo corpo de funções $K(\mathfrak{C})$ é (K-isomorfo a) F.*

DEMONSTRAÇÃO: Vamos construir $\mathfrak{C}$ da seguinte forma: tomamos $x, y \in F$ tal que $F = K(x, y)$. Seja $G(X, Y) \in K[X, Y]$ um polinômio irredutível com $G(x, y) = 0$. Seja $\mathfrak{V} = \left\{P \in \mathbb{A}^2 \mid G(P) = 0\right\}$ e $\overline{\mathfrak{V}}$ o fecho projetivo de $\mathfrak{V}$. Seja $\mathfrak{C}$ o modelo não singular de $\overline{\mathfrak{V}}$, então $K(\mathfrak{C}) \cong F$. □

Corolário 3.6.1 *Seja $\mathfrak{C}$ uma curva projetiva não singular e $F = K(\mathfrak{C})$ seu corpo de funções. Então existe uma correspondência um-a-um entre os pontos $P \in \mathfrak{C}$ e os lugares de $F|K$, dada por*

$$P \mapsto \mathfrak{m}_P(\mathfrak{C}),$$

o ideal maximal do anel local $\mathcal{O}_P(\mathfrak{C})$ (os pontos de $\mathfrak{C}$ desta correspondência são chamados pontos fechados*).*

Essa correspondência torna possível traduzir definições e resultados de corpos de funções algébricas para curvas algébricas (e vice-versa). Damos alguns exemplos abaixo:

- Um *divisor* de $\mathfrak{C}$ é uma soma formal $D = \sum_{P \in \mathfrak{C}} n_P P$ onde $n_P \in \mathbb{Z}$ e é quase sempre igual a zero. O grau de D é $\operatorname{gr}(D) = \sum_{P \in \mathfrak{C}} n_P$. Os divisores de $\mathfrak{C}$ formam um grupo aditivo $\operatorname{Div}(\mathfrak{C})$, o *grupo de divisores de* $\mathfrak{C}$.
- A *ordem de uma função racional* f em um ponto $P \in \mathfrak{C}$ é definida como $v_P(f)$, em que v_P é a valorização de $K(\mathfrak{C})$ correspondente ao anel de avaliação $\mathcal{O}_P(\mathfrak{C})$.
- O *divisor principal* $\operatorname{div}(f)$ de uma função racional $f \in K(\mathfrak{C}) \setminus \{0\}$ é $\operatorname{div}(f) = \sum_{P \in \mathfrak{C}} v_P(f) P$. O grau de um divisor principal é 0.

- Os divisores principais formam um subgrupo $\mathrm{Princ}(\mathfrak{C})$ do grupo divisor $\mathrm{Div}(\mathfrak{C})$. O grupo quociente $\mathrm{Jac}(\mathfrak{C}) = \mathrm{Div}^0(\mathfrak{C}) \,/\, \mathrm{Princ}(\mathfrak{C})$, onde $\mathrm{Div}^0(\mathfrak{C})$ é o grupo de divisores de grau 0, é chamado *jacobiano de* $\mathfrak{C}$. O grupo quociente $\mathrm{Cl}(\mathfrak{C}) = \mathrm{Div}(\mathfrak{C})/\mathrm{Princ}(\mathfrak{C})$ é chamado *grupo das classes dos divisores de* $\mathfrak{C}$. A ordem de $\mathrm{Cl}(\mathfrak{C})$ é dita o *número de classes de* $\mathfrak{C}$.
- Para $D \in \mathrm{Div}(\mathfrak{C})$, o espaço $L(D)$ é definido como no caso de corpos de funções. É um espaço vetorial de dimensão finita sobre K, cuja dimensão é dada pelo teorema de Riemann-Roch.

3.7 Variedades sobre Corpos Não Algebricamente Fechados

Assumimos até agora que K é um corpo algebricamente fechado. Agora abandonamos essa suposição e supomos apenas que K é um corpo perfeito. Seja $\overline{K} \supset K$ o fecho algébrico de K.

Definição 3.7.1 Dizemos que uma variedade afim $\mathfrak{V} \subset \mathbb{A}^n\left(\overline{K}\right)$ é *definida sobre* K, e denotado por $\mathfrak{V}/K$, se o seu ideal $\mathfrak{a}(\mathfrak{V}) \subset \overline{K}[X_1, \ldots, X_n]$ pode ser gerado pelos polinômios $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$. Se $\mathfrak{V}$ for definido sobre K, o conjunto

$$\mathfrak{V}(K) = \mathfrak{V} \cap \mathbb{A}^n(K) = \{P = (a_1, \ldots, a_n) \in \mathfrak{V} \mid a_i \in K\}$$

é chamado o conjunto dos *ponto K-racionais de* $\mathfrak{V}$.

Similarmente:

Definição 3.7.2 Uma variedade projetiva $\mathfrak{V} \subset \mathbb{P}^n\left(\overline{K}\right)$ é *definida sobre* K se $\mathfrak{a}(\mathfrak{V}) \subset \overline{K}[X_0, \ldots, X_n]$ pode ser gerado pelos polinômios $F_1, \ldots, F_r \in K[X_0, \ldots, X_n]$. Um ponto $P \in \mathfrak{V}$ é dito *K-racional* se existem coordenadas homogêneas $a_0, \ldots, a_n$ de P que estão em K, e estabelecemos

$$\mathfrak{V}(K) = \{P \in \mathfrak{V} \mid P \text{ é } K\text{-racional}\}.$$

Seja $\mathfrak{V} \subset \mathbb{A}^n\left(\overline{K}\right)$ uma variedade afim definida sobre K. Definimos então o ideal

$$\mathfrak{a}(\mathfrak{V}/K) = \mathfrak{a}(\mathfrak{V}) \cap K[X_1, \ldots, X_n]$$

e o anel das classes residuais

$$\Gamma(\mathfrak{V}/K) = \frac{K[X_1, \ldots, X_n]}{\mathfrak{a}(\mathfrak{V}/K)}.$$

O corpo de quociente

$$K(\mathfrak{V}) = \mathrm{cf}(\Gamma(\mathfrak{V}/K)) \subset \overline{K}(\mathfrak{V})$$

é dito o *corpo de funções K-racionais* de $\mathfrak{V}$. A extensão de $K(\mathfrak{V})|K$ é finitamente gerada, seu grau de transcendência é a dimensão de $\mathfrak{V}$. Pode-se definir da mesma forma o corpo das funções K-racionais de uma variedade projetiva definida sobre K.

Considere duas variedades $\mathfrak{V} \subset \mathbb{P}^m\left(\overline{K}\right)$ e $\mathfrak{W} \subset \mathbb{P}^n\left(\overline{K}\right)$. Uma aplicação racional $\phi : \mathfrak{V} \to \mathfrak{W}$ é *definida sobre K* se existirem polinômios homogêneos $F_0, \ldots, F_n \in K[X_0, \ldots, X_m]$ satisfazendo as condições (a), (b) e (c) da Definição 3.5.1 (p. 50), de modo que $\phi = (F_0 : \ldots : F_n)$.

Outra maneira de descrever pontos K-racionais, funções K-racionais etc. em uma variedade definida sobre K é a seguinte: Seja $\mathrm{Gal}\left(\overline{K}|K\right)$ o grupo Galois de $\overline{K}|K$. A ação de $\mathrm{Gal}\left(\overline{K}|K\right)$ sobre $\overline{K}$ estende-se naturalmente a uma ação nos conjuntos $\mathbb{A}^n\left(\overline{K}\right)$, $\mathbb{P}^n\left(\overline{K}\right)$, $\overline{K}[X_1, \ldots, X_n]$, $\mathfrak{V}$, $\Gamma(\mathfrak{V})$, $\overline{K}(\mathfrak{V})$ etc. Por exemplo, considere uma variedade projetiva $\mathfrak{V} \subset \mathbb{P}^n\left(\overline{K}\right)$ (definida sobre K), um ponto $P = (a_0 : \ldots : a_n) \in \mathfrak{V}$ e um automorfismo $\sigma \in \mathrm{Gal}\left(\overline{K}|K\right)$; então $\sigma(P) = (\sigma(a_0) : \ldots : \sigma(a_n))$. Vê-se então que

$$\mathfrak{V}(K) = \left\{P \in \mathfrak{V} \;\middle|\; \sigma(P) = P \text{ para todo } \sigma \in \mathrm{Gal}\left(\overline{K}|K\right)\right\},$$
$$K(\mathfrak{V}) = \left\{f \in \overline{K}(\mathfrak{V}) \;\middle|\; \sigma(f) = f \text{ para todo } \sigma \in \mathrm{Gal}\left(\overline{K}|K\right)\right\},$$

e assim por diante.

3.8 Curvas sobre Corpos Não Algebricamente Fechados

Considere uma curva projetiva $\mathfrak{C} \subset \mathbb{P}^n\left(\overline{K}\right)$ que é definida sobre K (onde K é um corpo perfeito e $\overline{K}$ é o fecho algébrico de K, como na seção anterior). Então o campo $K(\mathfrak{C})$ das funções K-racionais sobre $\mathfrak{C}$ é um corpo de funções algébricas de uma variável sobre K.

Um divisor $D = \sum_{P \in \mathfrak{C}} n_P P \in \mathrm{Div}(\mathfrak{C})$ é *definido sobre K* se $\sigma(D) = D$ para todos os $\sigma \in \mathrm{Gal}\left(\overline{K}|K\right)$ (isso significa que $n_{\sigma(P)} = n_P$ para todos os $P \in \mathfrak{C}$). Os divisores de $\mathfrak{C}$ definidos sobre K formam um subgrupo $\mathrm{Div}(\mathfrak{C}/K) \subset \mathrm{Div}(\mathfrak{C})$. Para $D \in \mathrm{Div}(\mathfrak{C}/K)$, o espaço $L_K(D)$ é dado por

$$L_K(D) = K(\mathfrak{C}) \cap L(D).$$

Este é um K-espaço vetorial de dimensão finita e sua dimensão (sobre K) é igual à dimensão de $L(D)$ (sobre $\overline{K}$).

Um divisor $Q \in \mathrm{Div}(\mathfrak{C}/K)$ com $Q > 0$ é dito um *divisor primo* de $\mathfrak{C}/K$ se Q não puder ser escrito como $Q = Q_1 + Q_2$ com divisores efetivos $Q_1, Q_2 \in \mathrm{Div}(\mathfrak{C}/K)$.

Capítulo 4

Funções Zeta e a Hipótese de Riemann para Corpos Finitos

4.1 A Função Zeta de uma Curva sobre um Corpo Finito

Definição 4.1.1 Para o número complexo s, a *função zeta* de $\mathfrak{C}$ definida sobre $\mathbb{F}_q$ é definida por

$$\zeta_{\mathfrak{C}}(s) = \zeta_{\mathfrak{C}/\mathbb{F}_q}(s) = \sum_D \frac{1}{N(D)}, \tag{4-1}$$

em que D percorre todos os divisores efetivos definidos sobre $\mathbb{F}_q$ de $\mathfrak{C}$, e $N(D) = q^{\mathrm{gr}(D)}$ é a *norma* de D.

Teorema 4.1.1 *Para* $\mathrm{Re}(s) > 1$, *a série* (4-1) *converge para a função*

$$F_0(q) = F\left(q^{-s}\right) + \frac{hq^{1-g}q^{(1-s)m}}{(q-1)\left(1-q^{e(1-s)}\right)} - \frac{h}{(q-1)\left(1-q^{-es}\right)},$$

onde:

(i) $F\left(q^{-s}\right)$ *é um polinômio em* q^{-s} *de grau no máximo* $2g-2$;

(ii) h *é o número de classes de* $\mathfrak{C}$;

(iii) g *é o gênero de* $\mathfrak{C}$;

(iv) e *é o menor grau positivo dos divisores em* $\mathrm{Div}(\mathfrak{C})$;

(v)

$$m = \begin{cases} 0 & se \quad g = 0, \\ 2g-2+e & se \quad g \geq 1. \end{cases}$$

DEMONSTRAÇÃO: A minimalidade de e implica que o grau de qualquer divisor de $\mathfrak{C}$ definido sobre $\mathbb{F}_q$ é divisível por e, mas não implica que qualquer múltiplo de e é o grau de algum divisor de $\mathfrak{C}$ definido sobre $\mathbb{F}_q$. Com efeito, temos que $e = 1$, isto será mostrado mais tarde, na Proposição 4.1.1; enquanto isso, nenhum uso é feito disso.

Os divisores efetivos de $\mathfrak{C}$ definidos sobre $\mathbb{F}_q$ são particionados em classes de divisores, dois dos quais D_1 e D_2 são equivalentes se, e somente se, existe $u \in \mathbb{F}_q(\mathfrak{C})$ tal que $D_1 = D_2 + \operatorname{div}(u)$. Cada classe consiste de todos os divisores definidos sobre $\mathbb{F}_q$ de uma série linear completa $|C|$ para um divisor C definido sobre $\mathbb{F}_q$ de $\mathfrak{C}$; isto é, ela coincide com o conjunto $|C| \cap \operatorname{Div}\left(\mathbb{F}_q(\mathfrak{C})\right)$. Pode-se mostrar que o número $n_q(|C|)$ de tais divisores definidos sobre $\mathbb{F}_q$ é

$$\frac{q^{\dim|C|+1}-1}{q-1} = \frac{q^{\ell(C)}-1}{q-1}$$

(veja [39, Teorema 8.39]).

Do Teorema de Riemann-Roch, temos:

$$\ell(C) = \begin{cases} 0 & \text{se } \operatorname{gr}(C) < 0, \\ 1 & \text{se } C \text{ é um divisor de zero}, \\ 0 & \text{se } C \text{ não é um divisor de zero e } \operatorname{gr}(C) = 0, \\ g-1 & \text{se } C \text{ não é um divisor canônico e } \operatorname{gr}(C) = 2g-2, \\ g & \text{se } C \text{ é um divisor canônico}, \\ \operatorname{gr}(C) - 1 + 1 & \text{se } \operatorname{gr}(C) > 2g-2. \end{cases}$$

A curva $\mathfrak{C}$ tem algum divisor canônico definido sobre $\mathbb{F}_q$ (vide [39, Observação 8.27]). Logo e divide $2g-2$.

Na soma abaixo, $|C|$ percorre todas as series lineares definidas sobre $\mathbb{F}_q$ de $\mathfrak{C}$ contendo algum divisor efeito definido sobre $\mathbb{F}_q$. Assim sendo:

$$\begin{aligned} \zeta_{\mathfrak{C}}(s) &= \sum_D N(D)^{-s} = \sum_{|C|} \sum_{D \in |C|} N(D)^s \\ &= \sum_{|C|} \sum_{D \in |C|} q^{-s\operatorname{gr}(D)} = \sum_{|C|} n_q(|C|)\, q^{-s\operatorname{gr}(C)}. \end{aligned}$$

Logo,

$$\begin{aligned} \zeta_{\mathfrak{C}}(s) &= \sum_{|C|} \frac{q^{-s\operatorname{gr}(C)}\left(q^{\ell(C)}-1\right)}{q-1} \\ &= (q-1)^{-1} \sum_{\operatorname{gr}(C)\geq 0} q^{\ell(C)-s\operatorname{gr}(C)} - (q-1)^{-1} \sum_{\operatorname{gr}(C)\geq 0} q^{-s\operatorname{gr}(C)}. \end{aligned}$$

Se $\operatorname{Re}(s) > 1$, então

$$\sum_{\operatorname{gr}(C)\geq 0} q^{-s\operatorname{gr}(C)} = \sum_{\operatorname{gr}(C)=ve} \sum_{v=0}^{\infty} q^{-s\operatorname{gr}(C)} h \sum_{v=0}^{\infty} q^{-sve} = \frac{h}{1-q^{-es}},$$

daí

$$\zeta_{\mathfrak{C}}(s) = (q-1)^{-1} \sum_{\operatorname{gr}(C)\geq 0} q^{\ell(C)-s\operatorname{gr}(C)} - \frac{h}{(q-1)\left(1-q^{-es}\right)}.$$

Se $g = 0$, então $\ell(C) = \operatorname{gr}(C) + 1$, e $h = 1$ (vide [39, Exemplo 8.36]). Assim, para $g = 0$,

$$\begin{aligned}
\zeta_{\mathfrak{C}}(s) &= (q-1)^{-1} \sum_{v=0}^{\infty} \sum_{\operatorname{gr}(|C|)=ve} q^{\operatorname{gr}(C)+1-s\operatorname{gr}(C)} - \frac{1}{(q-1)\left(1-q^{-es}\right)} \\
&= q(q-1)^{-1} \sum_{v=0}^{\infty} q^{e(1-s)v} - \frac{1}{(q-1)\left(1-q^{-es}\right)} \\
&= \frac{1}{(q-1)\left(1-q^{e(1-s)}\right)} - \frac{1}{(q-1)\left(1-q^{-es}\right)}.
\end{aligned}$$

Para $g \geq 1$,

$$\begin{aligned}
\zeta_{\mathfrak{C}}(s) &= (q-1)^{-1} \sum_{0\leq \operatorname{gr}(C)\leq 2g-2} q^{\ell(C)-s\operatorname{gr}(C)} \\
&\quad + (q-1)^{-1} \sum_{\operatorname{gr}(C)>2g-2} q^{\ell(C)-s\operatorname{gr}(C)} - \frac{h}{(q-1)\left(1-q^{-es}\right)} \\
&= (q-1)^{-1} \sum_{v=0}^{\frac{2g-2}{e}} q^{-esv} \sum_{i=1}^{h} q^{\ell\left(C_i^{ve}\right)} \\
&\quad + h(q-1)^{-1} \sum_{v=\frac{2g-2}{e}+1}^{\infty} q^{e(s-1)v-g+1} - \frac{h}{(q-1)\left(1-q^{-es}\right)},
\end{aligned}$$

onde $\left|C_i^{ve}\right|$ denota uma classe de divisores definidos sobre $\mathbb{F}_q$ de grau ve. Logo $\zeta_{\mathfrak{C}}(s)$ converge para

$$F_0(q) = F\left(q^{-s}\right) + \frac{hq^{1-g}q^{(1-s)m}}{(q-1)\left(1-q^{e(1-s)}\right)} - \frac{h}{(q-1)\left(1-q^{-es}\right)},$$

com

$$F\left(q^{-s}\right) = (q-1)^{-1} \sum_{v=0}^{\frac{2g-2}{e}} q^{-esv} - \sum_{i=1}^{h} q^{\ell\left(C^{ve}\right)},$$

que é um polinômio em q^{-s} de grau no máximo $2g-2$. □

O Teorema 4.1.1 mostra que $\zeta_{\mathfrak{C}}(s)$ possui um prolongamento analítico a todo plano complexo. Seus pólos de primeira ordem são de dois tipos, a saber,

$$s_u = \frac{2\pi i u}{e \log q} \quad \text{e} \quad s_v = 1 - \frac{2\pi i v}{e \log q}, \quad \text{com} \quad u, v \in \mathbb{Z}.$$

Teorema 4.1.2 (Produto de Euler) *Para* $\operatorname{Re}(s) > 1$*, o produto*

$$\prod_{P \in \mathfrak{C}} \left(1 - N(P)^{-s}\right)^{-1}, \tag{4-2}$$

em que $N(P) = q^{\operatorname{gr}(P)}$*, converge absolutamente para a função* $\zeta_{\mathfrak{C}}(s)$*. Em particular, o produto independe da ordem de seus fatores.*

Demonstração: Para qualquer $N \geq 1$,

$$\prod_{N(P) \leq N} \left(1 - N(P)^{-s}\right)^{-1} = \prod_{N(P) \leq N} \left(\sum_{n=0}^{\infty} N(P)^{-ns}\right).$$

Como o produto do lado direito tem um número finito de fatores e cada fator é uma série absolutamente convergente, segue por multiplicação que

$$\prod_{N(P) \leq N} \left(1 - N(P)^{-s}\right)^{-1} = \sum_{N(D) \leq N} N(D)^{-s} + \sum_{N(D) > N} N(D)^{-s},$$

onde o primeiro somatório do lado direito é definido sobre todos os divisores efetivos definidos sobre $\mathbb{F}_q$ com $N(D) \leq N$ enquanto que o segundo é sobre todos os divisores D definidos sobre $\mathbb{F}_q$ com $N(D) > N$ que não contém pontos fechados com $N(P) > N$. Então

$$\left| \prod_{N(P) \leq N} \left(1 - N(P)^{-s}\right)^{-1} - \sum_{N(D) \leq N} N(D)^{-s} \right| \leq \sum_{N(D) > N} N(D)^{-\operatorname{Re}(s)}.$$

A soma do lado direito pode ser vista como o erro da série convergente $\zeta_{\mathfrak{C}}(s)$, e logo tende a zero. Isto prova a convergência. A convergência absoluta segue da desigualdade:

$$\left| \sum_{n=1}^{\infty} N(D)^{-ns} \right| \leq \sum_{n=1}^{\infty} N(D)^{-n \operatorname{Re}(s)}.$$

□

O Teorema 4.1.2 implica que $\zeta_{\mathfrak{C}}(s)$ não tem zeros para $\operatorname{Re}(s) > 1$.

Proposição 4.1.1 *A curva* $\mathfrak{C}$ *possui um divisor definido sobre* $\mathbb{F}_q$ *de grau* 1.

DEMONSTRAÇÃO: Com as notações do Teorema 4.1.1 é suficiente mostrar que $e = 1$. Devido a minimalidade de e, o divisor D é definido sobre $\mathbb{F}_q$ de grau e se, e somente se, D é um ponto fechado de grau e; isto é,

$$D = P + \sigma(P) + \cdots + \sigma^{e-1}(P),$$

para algum ponto $\mathbb{F}_q$-racional de $\mathfrak{C}$, e σ é o automorfismo de Frobenius. Note que as imagens dos automorfismos de Frobenius $\overline{P}_i = \sigma^i(P)$ de P, para $i = 1, \ldots, e-1$, são também pontos $\mathbb{F}_q$-racionais de $\mathfrak{C}$. Seja

$$\overline{\zeta}_{\mathfrak{C}}(s) = \prod_{\overline{P}} \left(1 - N(\overline{P})^{-s}\right)^{-1}$$

a função zeta de $\mathfrak{C}$ considerada como uma curva sobre $\mathbb{F}_q$. Então

$$\overline{\zeta}_{\mathfrak{C}}(s) = \prod_{\overline{P}} \left(1 - q^{-se\,\mathrm{gr}(\overline{P})}\right)^{-1} = \prod_{i=1}^{e} \left(\prod_{\overline{P}_i} \left(1 - q^{-se\,\mathrm{gr}(\overline{P}_i)}\right)^{-1} \right).$$

Como $\mathrm{gr}(P) = e\,\mathrm{gr}(\overline{P}_i)$, segue-se que

$$\overline{\zeta}_{\mathfrak{C}}(s) = \prod_{i=1}^{e} \left(\prod_{P} \left(1 - q^{-se\,\mathrm{gr}(P)}\right)^{-1} \right) = \zeta_{\mathfrak{C}}(s)^e.$$

Como ambas $\zeta_{\mathfrak{C}}(s)$ e $\overline{\zeta}_{\mathfrak{C}}(s)$ têm um polo de mesma ordem 1 em $s = 1$, isto implica que $e = 1$. □

A Proposição 4.1.1 permite a possibilidade de simplificar o Teorema 4.1.1.

Teorema 4.1.3 *A função zeta de $\mathfrak{C}$ pode ser escrita como*

$$\zeta_{\mathfrak{C}}(s) = \frac{L(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})},$$

em que $L(q^{-s}) = \sum_{j=0}^{2g} a_j q^{-js}$ com $a_0 = 1$ e $a_{2g} = q^g$.

DEMONSTRAÇÃO: A prova é realizada em três partes, de acordo com g sendo tomado como 0, 1 e ≥ 2.

Para $g = 0$,

$$\zeta_{\mathfrak{C}}(s) = \frac{q}{(q-1)(1 - q^{1-s})} - \frac{q}{(q-1)(1 - q^{-s})} = \frac{1}{(1 - q^{-s})(1 - q^{1-s})}.$$

Para $g = 1$,

$$\begin{aligned}\zeta_{\mathfrak{C}}(s) &= \frac{1}{q-1}\sum_{\mathrm{gr}(C)=0} q^{\ell(C)-s\,\mathrm{gr}(C)} + \frac{hq^{1-s}}{(q-1)(1-q^{1-s})} - \frac{h}{(q-1)(1-q^{-s})} \\ &= \frac{h-1}{q-1} + \frac{q}{q-1} + \frac{hq^{1-s}}{(q-1)(1-q^{1-s})} - \frac{h}{(q-1)(1-q^{-s})} \\ &= \frac{1+(h-q-1)\,q^{-s}+q\cdot q^{-2s}}{(1-q^{1-s})(1-q^{-s})}.\end{aligned}$$

Para $g \geq 2$,

$$\begin{aligned}\zeta_{\mathfrak{C}}(s) &= \frac{1}{q-1}\sum_{\mathrm{gr}(C)=0} q^{\ell(C)-s\,\mathrm{gr}(C)} + \frac{1}{q-1}\sum_{0\leq \mathrm{gr}(C)<2g-2} q^{\ell(C)-s\,\mathrm{gr}(C)} \\ &\quad + \frac{1}{q-1}\sum_{\mathrm{gr}(C)\geq 2g-2} q^{\ell(C)-s\,\mathrm{gr}(C)} + \frac{hq^{1-g}q^{(1-s)(2g-1)}}{(q-1)(1-q^{1-s})} \\ &\quad - \frac{h}{(q-1)(1-q^{1-s})} \\ &= \frac{h+q-1}{q-1} + \frac{1}{q-1}\sum_{1\leq \mathrm{gr}(C)<2g-2} q^{\ell(C)-s\,\mathrm{gr}(C)} \\ &\quad + \frac{(h-1)\,q^{g-1-s(2g-2)}+q^{g-s(2g-2)}}{q-1} \\ &\quad + \frac{hq^{1-g}q^{(1-s)(2g-1)}}{(q-1)(1-q^{1-s})} - \frac{h}{(q-1)(1-q^{-s})} \\ &= \frac{1}{q-1}\sum_{j=1}^{2g-3} a_j q^{-js} + \frac{(h+q-1)\left(q^{g-1}q^{-2(g-1)s}+1\right)}{q-1} \\ &\quad + \frac{hq^g q^{-(2g-1)s}}{(q-1)(1-q^{1-s})} - \frac{h}{(q-1)(1-q^{-s})} \\ &= \frac{1+a_1q^{-s}+\cdots+a_{2g-1}q^{-(2g-1)s}+q^gq^{-2gs}}{(1-q^{-s})(1-q^{1-s})}.\end{aligned}$$

□

Teorema 4.1.4 (Equação Funcional) *A função zeta em $\mathfrak{C}$ satisfaz a equação*

$$\zeta_{\mathfrak{C}}(1-s) = q^{(g-1)(2s-1)}\zeta_{\mathfrak{C}}(s). \tag{4-3}$$

DEMONSTRAÇÃO: Novamente, trataremos separadamente três casos de acordo com que g seja igual a 0, 1, e ≥ 2.

Para $g = 0$,

$$\zeta_{\mathfrak{C}}(1-s) = \frac{1}{(1-q^s)(1-q^{s-1})} = q^{1-2s}\zeta_{\mathfrak{C}}(s).$$

Para $g = 1$,

$$\zeta_{\mathfrak{C}}(1-s) = \frac{1+(h-q-1)q^{s-1}+q\left(q^{2s-2}\right)}{(1-q^s)(1-q^{s-1})} = \zeta_{\mathfrak{C}}(s).$$

Para $g \geq 2$, seja

$$\zeta_{\mathfrak{C}}(s) = \zeta'_{\mathfrak{C}}(s) + \zeta''_{\mathfrak{C}}(s),$$

em que

$$\zeta'_{\mathfrak{C}}(s) = (q-1)^{-1} \sum_{1 \leq \operatorname{gr}(C) < 2g-2} q^{\ell(C)+1-s\operatorname{gr}(C)},$$

$$\zeta''_{\mathfrak{C}}(s) = 1 + \frac{1}{q^{(g-1)(2s-1)}} + \frac{h}{q-1}\left(1 + q^{(g-1)(2s-1)} + \frac{q^g q^{-(2s-1)s}}{1-q^{1-s}} - \frac{1}{1-q^{s-1}}\right).$$

Então,

$$\begin{aligned}\zeta''_{\mathfrak{C}}(1-s) &= 1 + q^{(g-1)(2s-1)} + \frac{h}{q-1}\left(1 + q^{(g-1)(2s-1)} + \frac{q^g q^{(2g-1)(s-1)}}{1-q^s} - \frac{1}{1-q^{s-1}}\right) \\ &= q^{(g-1)(2s-1)}\zeta''_{\mathfrak{C}}(s).\end{aligned}$$

Resta-nos provar que $\zeta'_{\mathfrak{C}}(s-1) = q^{(g-1)(2s-1)}\zeta'_{\mathfrak{C}}(s)$. Seja $\rho(C) = \ell(C) - \frac{1}{2}\operatorname{gr}(C)$, então

$$\zeta'_{\mathfrak{C}}(s) = \frac{1}{q-1} \sum_{1 \leq \operatorname{gr}(C) < 2g-2} q^{\ell(C)-s\operatorname{gr}(C)} + \frac{1}{q-1} \sum_{1 \leq \operatorname{gr}(C) < 2g-2} q^{\rho(C)-\frac{(2s-1)\operatorname{gr}(C)}{2}}.$$

Do Teorema de Riemann-Roch,

$$\rho(C) = \rho(W-C),$$

para um divisor canônico W definido sobre $\mathbb{F}_q$ de $\mathfrak{C}$. Logo, se C percorre todos o conjunto de todas as classes de divisores satisfazendo a condição $1 \leq \operatorname{gr}(C) < 2g-2$, então $W-C$ faz o mesmo. Portanto

$$\begin{aligned}\zeta'_{\mathfrak{C}}(s) &= \frac{1}{q-1} \sum_{1 \leq \operatorname{gr}(W-C) < 2g-2} q^{\rho(W-C)-\frac{(2s-1)(2g-2-\operatorname{gr}(C))}{2}} \\ &= \frac{1}{q-1} \sum_{1 \leq \operatorname{gr}(C) < 2g-2} q^{\rho(C)-\frac{(2s-1)(2g-2-\operatorname{gr}(C))}{2}},\end{aligned}$$

e assim:

$$\begin{aligned}\zeta'_{\mathfrak{C}}(1-s) &= \frac{1}{q-1}\sum_{1\leq \mathrm{gr}(C)<2g-2} q^{\rho(C)-\frac{(2s-1)\,\mathrm{gr}(C)}{2}} \\ &= q^{(g-1)(2s-1)}\frac{1}{q-1}\sum_{1\leq \mathrm{gr}(C)<2g-2} q^{\rho(C)-\frac{(2s-1)(2g-2-\mathrm{gr}(C))}{2}} \\ &= q^{(g-1)(2s-1)}\zeta'_{\mathfrak{C}}(s)\,.\end{aligned}$$

□

Definição 4.1.2 Para $t = q^{-s}$, definimos:

$$Z_{\mathfrak{C}}(t) = \zeta_{\mathfrak{C}}(s)\,.$$

Teorema 4.1.5 *Se $|t| < q^{-1}$, então*

$$Z_{\mathfrak{C}}(t) = \exp\left(\sum_{i=1}^{\infty}\frac{N_i t^i}{i}\right)$$

em que N_i é o número de pontos $\mathbb{F}_{q^i}$-racionais de $\mathfrak{C}$.

Demonstração: A hipótese, $|t| < q^{-1}$, se verifica se, e somente se, $\mathrm{Re}(s) > 1$. Assim, para $\mathrm{Re}(s) > 1$,

$$\zeta_{\mathfrak{C}}(s) = \prod_P\left(1-N(P)^{-s}\right)^{-1} = \prod_P\left(1-q^{-s\,\mathrm{gr}(P)}\right)^{-1} = \prod_P\left(1-t^{\mathrm{gr}(P)}\right)^{-1} = Z_{\mathfrak{C}}(t)\,.$$

Logo,

$$\begin{aligned}\log Z_{\mathfrak{C}}(t) &= -\sum_P \log\left(1-t^{\mathrm{gr}(P)}\right) = \sum_P\sum_{m=1}^{\infty}\frac{t^{m\,\mathrm{gr}(P)}}{m} \\ &= \sum_{n=1}^{\infty}\left(\sum_{m\,\mathrm{gr}(P)=n}\frac{1}{m}\right)t^n = \sum_{n=1}^{\infty}\left(\sum_{\mathrm{gr}(P)|n}\mathrm{gr}(P)\right)\frac{t^n}{n}.\end{aligned}$$

Seja $N_n^* = \sum_{\mathrm{gr}(P)|n}\mathrm{gr}(P)$. Então

$$Z_{\mathfrak{C}}(t) = \exp\left(\sum_{n=1}^{\infty}\frac{N_n^* t^n}{n}\right).$$

Isto mostra que é suficiente provar a igualdade:

$$\sum_{\mathrm{gr}(P)|n}\mathrm{gr}(P) = N_n. \tag{4-4}$$

Todo ponto Q $\mathbb{F}_{q^n}$-racional de $\mathfrak{C}$ dá origem a um ponto fechado $\mathbb{F}_q$-racional

$$P = Q + \sigma(Q) + \cdots + \sigma^{n-1}(Q)$$

de $\mathfrak{C}$ (onde σ é o automorfismo de Frobenius). Neste contexto, dois pontos $\mathbb{F}_{q^n}$-racionais de $\mathfrak{C}$ são equivalentes se definem o mesmo ponto fechado $\mathbb{F}_q$-racional de $\mathfrak{C}$. Assim o conjunto de pontos $\mathbb{F}_{q^n}$-racionais de $\mathfrak{C}$ é particionado em classes de equivalência. Se Δ é um sistema representante de tais classes, então

$$N_q^* = \sum_{P \in \Delta} \operatorname{gr}(P).$$

Por outro lado, se o ponto fechado P surge do ponto Q de $\mathfrak{C}$, isto é, se

$$P = Q + \sigma(Q) + \cdots + \sigma^{n-1}(Q)$$

então a condição $\operatorname{gr}(P) \mid n$ neste somatório significa que $\sigma^m(Q) = Q$ com $m \mid n$. Portanto Q é um ponto $\mathbb{F}_{q^m}$-racional de $\mathfrak{C}$, e a condição de divisibilidade $m \mid n$ implica que $\mathbb{F}_{q^m}$ é um subcorpo de $\mathbb{F}_{q^n}$. Deste argumento, segue a equação (4-4), como queríamos obter. □

Seja A_n denotando o número de todos os divisores efetivos definidos sobre $\mathbb{F}_{q^n}$ de $\mathfrak{C}$ de grau n. Então

$$Z_{\mathfrak{C}}(t) = 1 + \sum_{n=1}^{\infty} A_n t^n. \tag{4-5}$$

Isto segue do Teorema 4.1.2, pois como

$$\prod_P \left(1 - N(P)^{-s}\right)^{-1} = \zeta_{\mathfrak{C}}(s) = Z_{\mathfrak{C}}(t) = \prod_P \left(1 - q^{\operatorname{gr}(P)}\right)^{-1},$$

onde P percorre todos os pontos fechados $\mathbb{F}_q$-racionais de $\mathfrak{C}$, e cada fator pode ser escrito como uma série geométrica, dando origem a equação

$$\prod_P \left(1 - q^{\operatorname{gr}(P)}\right)^{-1} = \prod_P \sum_{n=0}^{\infty} t^{\operatorname{gr}(nP)} = \sum_D t^{\operatorname{gr}(D)} = 1 + \sum_{n=1}^{\infty} A_n t^n,$$

em que D percorre todos os divisores efetivos definidos sobre $\mathbb{F}_q$ de $\mathfrak{C}$.

Proposição 4.1.2 *Se $g \geq 1$, então*

$$Z_{\mathfrak{C}}(t) = G(t) + H(t),$$

com

$$G(t) = \frac{1}{q-1} \sum_{0 \leq \operatorname{gr}(C) < 2g-2} q^{\ell(C)} t^{\operatorname{gr}(C)},$$

$$H(t) = \frac{h}{q-1} \left(\frac{q^{1-g}(qt)^{2g-1}}{1-qt} - \frac{1}{1-t} \right).$$

DEMONSTRAÇÃO: Aqui vamos utilizar o fato de que

$$n_q\left(|C|\right) = \frac{q^{\dim|C|+1}-1}{q-1}$$

[39, Teorema 8.39]; e o fato de que

$$A_n = \frac{h}{q-1}\left(q^{n+1-g}-1\right) \text{ para } n > 2g-2,$$

onde h é o número de classes de $\mathfrak{C}$ e g é o gênero de $\mathfrak{C}$ [39, Proposição 8.40]. Desta forma,

$$\begin{aligned} Z_{\mathfrak{C}}(t) = \sum_{n=0}^{\infty} A_n t^n &= \sum_{\mathrm{gr}(C)\geq 0} n_q\left(|C|\right) t^{\mathrm{gr}(C)} + (q-1)^{-1} \sum_{\mathrm{gr}(C)\geq 0}\left(q^{\ell(C)}-1\right) t^{\mathrm{gr}(C)} \\ &= (q-1)^{-1} \sum_{0\leq \mathrm{gr}(C)\leq 2g-2} q^{\ell(C)} t^{\mathrm{gr}(C)} \\ &\quad + (q-1)^{-1}\left(\sum_{\mathrm{gr}(C)>2g-2} q^{\ell(C)+1-g} t^{\mathrm{gr}(C)} - \sum_{\mathrm{gr}(C)\geq 0} t^{\mathrm{gr}(C)}\right) \\ &= G(t) + H(t). \end{aligned}$$

□

O Teorema 4.1.3 mostra que a função zeta $Z_{\mathfrak{C}}(t)$ tem a forma

$$Z_{\mathfrak{C}}(t) = \frac{L(t)}{(1-t)(1-qt)}, \tag{4-6}$$

em que

$$L(t) = L_{\mathbb{F}_q}(t) = \begin{cases} 1 & \text{para } g = 0, \\ 1 + \sum_{i=1}^{2g-1} a_i t^i + q^g t^{2g} & \text{para } g \geq 1, \end{cases} \tag{4-7}$$

é o *L-polinômio* de $\mathfrak{C}$, visto como uma curva definida sobre $\mathbb{F}_q$. Note que $L(t) \in \mathbb{Z}[t]$. Para $g \geq 1$, da Proposição 4.1.2,

$$L(t) = (1-t)(1-qt)G(t) + h(q-1)^{-1}\left[q^g t^{2g-1}(1-t) - (1-qt)\right]. \tag{4-8}$$

Proposição 4.1.3 *O L-polinômio tem as seguintes propriedades:*

(i) $L(t) = q^g t^{2g} L\left((qt)^{-1}\right) = 1 + a_{2g-1} q^{g-1} t + \cdots + q^g t^{2g}$;

(ii) $a_{2g-i} = q^{g-i} a_i$ *para* $i = 0, \ldots, g$.

DEMONSTRAÇÃO: A primeira afirmação é uma consequência da equação funcional (4-3). Comparando os coeficientes de t^i, a segunda afirmação segue. □

Seja

$$L(t) = \prod_{i=1}^{2g} (1 - \omega_i t) \tag{4-9}$$

a fatoração de $L(t)$ em fatores lineares em alguma extensão finita de $\mathbb{Q}$. O seguinte resultado, de suma importância para esta dissertação, desempenha um papel essencial no estudo dos pontos $\mathbb{F}_q$-racionais de $\mathfrak{C}$.

Teorema 4.1.6 *Seja N_n o número de pontos $\mathbb{F}_{q^n}$-racionais de uma curva irredutível, não singular $\mathfrak{C}$ de gênero g definida sobre $\mathbb{F}_q$. Então*

$$N_n = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n, \tag{4-10}$$

onde $\omega_1, \ldots, \omega_{2g}$ são os recíprocos das raízes do L-polinômio de $\mathfrak{C}$.

DEMONSTRAÇÃO: Da relação

$$Z_{\mathfrak{C}}(t) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} t^n\right) = \frac{\prod_{i=1}^{2g} (1 - \omega_i t)}{(1-t)(1-qt)},$$

segue que

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{N_n}{n} t^n &= \sum_{i=1}^{2g} \log(1 - \omega_i t) - \log(1-t) - \log(1-qt) \\ &= \sum_{n=1}^{\infty} n^{-1} \left(q^n + 1 - \sum_{i=1}^{2g} \omega_i^n\right) t^n. \end{aligned}$$

E assim o resultado segue comparando os coeficientes. □

Se os números N_n são conhecidos para $n = 1, \ldots, r$ e r suficientemente grande, então os coeficientes de L-polinômio podem ser calculados pelo seguinte:

Proposição 4.1.4 *Seja $L(t) = \sum_{i=0}^{2g} a_i t^i$ o L-polinômio de $\mathfrak{C}$ definida sobre $\mathbb{F}_q$, e seja $s_n = N_n - (q^n + 1)$.*

(i) A derivada logarítmica é dada por:

$$\frac{dL(t)/dt}{L(t)} = \sum_{n=1}^{\infty} s_n t^{n-1}.$$

(ii) Para $n = 1, \ldots, g$, tem-se

$$na_n = s_n + s_{n-1}a_1 + \cdots + s_1 a_{n-1}. \tag{4-11}$$

Em particular, de $N_1, \ldots, N_g$, os coeficientes de $L(t)$ podem ser calculados usando (4-11) *e as equações*

$$\begin{cases} a_0 = 1, \\ a_{2g-n} = q^{g-n} a_n \text{ para } n = 1, \ldots, g. \end{cases}$$

Demonstração: *(i)* Usando o Teorema 4.1.6 obtemos que:

$$\begin{aligned} \frac{dL(t)/dt}{L(t)} &= \sum_{n=1}^{2g} \frac{-\omega_i}{1-\omega_n t} = \sum_{n=1}^{2g} (-\omega_i) \cdot \sum_{k=0}^{\infty} (\omega_n t)^k \\ &= \sum_{k=0}^{\infty} \left(\sum_{n=1}^{2g} -\omega_n^k \right) t^{k-1} = \sum_{k=1}^{\infty} s_k t^{k-1}. \end{aligned}$$

(ii) Do item *(i)* temos:

$$\begin{aligned} &a_1 + 2a_2 t + \cdots + (2g-1)\, a_{2g-1} t^{2g-2} + 2gqt^{2g-1} \\ &\qquad = \left(1 + a_1 t + \cdots + a_{2g-1} t^{2g-2} + 2gqt^{2g}\right) \sum_{k=1}^{\infty} s_k t^{k-1}. \end{aligned}$$

Logo (4-11) segue comparando os coeficientes de t^i para $i = 0, \ldots, g-1$. □

Exemplo 4.1.1 Seja

$$\mathfrak{C}/\mathbb{F}_2 = \left\{ (X_0, X_1, X_2) \in \mathbb{P}^3(\mathbb{F}_2) \;\middle|\; X_0^3 + X_1^3 + X_2^3 = 0 \right\}.$$

Assim

$$\mathfrak{C}(\mathbb{F}_2) = \{(0,1,1), (1,0,1), (1,1,0)\}.$$

Então

$$a_1 = s_1 = N_1 - 3 = 0.$$

Logo

$$Z_{\mathfrak{C}/\mathbb{F}_2}(t) = \frac{1+2t^2}{(1-t)(1-2t)}, \tag{4-12}$$

e

$$\sum \frac{N_i t^i}{i} = \log Z_{\mathfrak{C}/\mathbb{F}_2}(t) = \sum \frac{t^i}{i} + \sum \frac{(2t)^i}{i} + \sum \frac{(-1)^{j-1}(2t^2)^j}{j}.$$

Portanto,

$$N_h = \begin{cases} 1+2^h & \text{para} \quad h \text{ ímpar}, \\ 1+2^h+2\cdot 2^{h/2} & \text{para} \quad h \equiv 2 \pmod 4, \\ 1+2^h-2\cdot 2^{h/2} & \text{para} \quad h \equiv 0 \pmod 4. \end{cases}$$

Por fim, de (4-12) segue que

$$Z_{\mathfrak{C}/\mathbb{F}_2}(t) = 1 + 3\sum_{i>0}\left(2^i - 1\right)t^i,$$

donde tem-se que

$$A_i = 3\left(2^i - 1\right) \text{ para } i > 0.$$

4.2 Hipótese de Riemann para Corpos Finitos

Como colocado na introdução, a hipótese de Riemann diz que se s não é um zero trivial então $\zeta(s) = 0$ se, e somente se, $\mathrm{Re}(s) = \frac{1}{2}$, em que ζ é a função clássica de Riemann, dos racionais. Para o caso em que ζ está na curva $\mathfrak{C}$ definida sobre o corpo $\mathbb{F}_q$, isto se traduz no seguinte teorema:

Teorema 4.2.1 (Hipótese de Riemann para Corpos Finitos) *Os recíprocos das raízes $\omega_1, \ldots, \omega_{2g}$ do L-polinômio de uma curva não singular irredutível definida sobre $\mathbb{F}_q$ satisfaz*

$$|\omega_i| = q^{1/2}.$$

Escólio. Para ver que de fato o que diz este teorema se refere a hipótese de Riemann para uma curva definida sobre um corpo finito, observamos que se $\zeta_{\mathfrak{C}}(s) = 0$, do Teorema 4.1.3 e da equação (4-6), temos que $Z_{\mathfrak{C}}(q^{-s}) = 0$, isto é, $L(q^{-s}) = 0$ e o teorema nos diz que $|q^s| = q^{\frac{1}{2}}$, por fim, como $|q^s| = q^{\mathrm{Re}(s)}$, concluímos que $\zeta_{\mathfrak{C}}(s) = 0$ implica $\mathrm{Re}(s) = 1/2$.

Lema 4.2.1 *Se existe uma constante $c \in \mathbb{R}$ tal que, para todo $n \geq 1$,*

$$|N_n - (q^n + 1)| \leq c\sqrt{q^n}, \tag{4-13}$$

então a hipótese de Riemann para corpos finitos se verifica.

Demonstração: O Teorema 4.1.6 e a equação (4-13) implicam, para todo $n \geq 1$, que

$$\left|\sum_{i=1}^{2g}\omega_i^n\right| \leq c\sqrt{q^n}. \tag{4-14}$$

Seja agora

$$\rho = \min_{i\in\{1,\ldots,2g\}} \left\{ \left| \omega_i^{-1} \right| \right\}.$$

Então o raio de convergência da expansão em séries de potência da função meromorfa

$$H(t) = \sum_{i=1}^{2g} \frac{\omega_i t}{1-\omega_i t}$$

é ρ, e os únicos pontos de singularidades de $H(t)$ são $\omega_1^{-1}, \ldots, \omega_{2g}^{-1}$. Para $|t| < \rho$,

$$H(t) = \sum_{i=1}^{2g} \sum_{n=1}^{\infty} (\omega_i t)^n = \sum_{n=1}^{\infty} \left(\sum_{i=1}^{2g} \omega_i^n \right) t^n.$$

Por (4-14), esta é uma série convergente para $|t| < q^{-1/2}$, onde $q^{-1/2} \leq \rho$. Portanto $\sqrt{q} \geq |\omega_i|$. Por fim, $|\omega_i| = \sqrt{q}$, pois

$$\prod_{i=1}^{2g} \omega_i = q^s,$$

o qual é uma consequência imediata de (4-7) e (4-9). □

Lema 4.2.2 *Sobre as hipóteses do Teorema 4.2.1 tem-se que*

$$\left| \mathfrak{C}\left(\mathbb{F}_q\right) - (q+1) \right| \leq 2g\sqrt{q}. \tag{4-15}$$

Demonstração: Do Teorema 4.1.6 temos que

$$\#\mathfrak{C}\left(\mathbb{F}_q\right) - (q+1) = -\sum_{i=1}^{2g} \omega_i.$$

Logo, com base na equação (4-7) e a Proposição 4.1.4, tem-se que desigualdade (4-15) é uma consequência imediata do Teorema 4.2.1. □

Definição 4.2.1 A desigualdade (4-15) é chamada *limitante de Hasse-Weil*.

Como consequência dos Lemas 4.2.1 e 4.2.2 temos a seguinte equivalência da hipótese de Riemann para corpos finitos:

$$\begin{bmatrix} \text{Hipótese de Riemann para Corpos Finitos} \\ \Updownarrow \\ \text{Limitante de Hasse-Weil} \end{bmatrix} \tag{4-16}$$

Exemplo 4.2.1 No Art. 358 de *Disquisitiones Arithmeticae*, Gauss provou o seguinte teorema:

> *Suponha que* $p \equiv 1 \pmod 3$. *Então existem inteiros* A *e* B *tais que* $4p = A^2 + 27B^2$. *Se tomamos* A *tal que* $A \equiv 1 \pmod 3$, *então* A *é unicamente determinado, e*
>
> $$\#\left\{(x,y) \in \mathbb{F}_p^2 \;\middle|\; x^3 + y^3 = 1\right\} = p - 2 + A.$$

Desta forma, se

$$\mathfrak{C}\left(\mathbb{F}_p\right) = \left\{(x,y) \in \mathbb{F}_p^2 \;\middle|\; x^3 + y^3 - 1 = 0\right\},$$

temos que

$$g = \frac{(3-1)(3-2)}{2} = 1.$$

Assim, se tomarmos $p = 13$ e $A = 9$ temos que

$$\#\mathfrak{C}\left(\mathbb{F}_{13}\right) = 13 - 2 + 9 = 20,$$

e que

$$2g\sqrt{p} = 2\sqrt{13} = 2 \times 3.605551275 = 7.211102551,$$

e, portanto,

$$\left|\#\mathfrak{C}\left(\mathbb{F}_p\right) - (p+1)\right| = 6 < 2\sqrt{p}.$$

4.3 A Prova Original de Weil

Como indicamos na introdução, a prova de Weil ([92, 93]) suscitou polêmicas, pois repousa sobre um "lema-chave" que ele não havia demonstrado naquele momento, veja a este propósito a correspondência com Henri Cartan [4]. Os dois artigos repousam sobre um enunciado de positividade em geometria algébrica sobre um corpo finito cuja analogia era conhecida de Weil sobre o corpo dos números complexos, mas cuja demonstração era de natureza "transcendente", utilizando Análise Holomorfa e Topologia e, portanto, não aplicável diretamente.

Apresentamos a seguir a prova do artigo de 1941, baseada na desigualdade de Castelnuovo-Severi.

A prova de Weil utilizava um trabalho em variedades algébricas de dimensões superiores. A primeira versão (de 1940) usava uma variedade de dimensão g; a segunda versão (de 1941) requer apenas um trabalho na superfície $\mathfrak{C} \times \mathfrak{C}$.

Definimos um "divisor" em uma superfície como uma soma formal com coeficientes inteiros de curvas; o divisor de uma função é a soma de seus zeros

(contados positivamente) e de seus pólos (contados negativamente); dizemos que dois divisores são linearmente equivalentes se sua diferença é o divisor de uma função.

No plano projetivo, duas retas distintas sempre se intersectam em um ponto. Essa afirmação elementar pode ser amplamente generalizada, primeiro com o seguinte resultado.

Sejam $\mathfrak{C}_1$ e $\mathfrak{C}_2$ duas curvas (não necessariamente irredutíveis) em $\mathbb{P}^2$ de graus d_1 e d_2, sem componentes comuns, então $\mathfrak{C}_1 \cap \mathfrak{C}_2$ é finito e o número de pontos desta intersecção, computando sua multiplicidade, é $d_1 d_2$.

Este resultado clássico é conhecido como Teorema de Bézout, demonstrado por Étienne Bézout em 1779; uma demonstração moderna pode ser encontrada em [31, Corolário 7.8, p. 54].

Assim sendo, por meio do Teorema do Bézout podemos definir uma forma bilinear sobre os pares de curva de $\mathbb{P}^2$ que a duas curvas $\mathfrak{C}_1$ e $\mathfrak{C}_2$ associa $\mathfrak{C}_1 \cdot \mathfrak{C}_2 = d_1 d_2$ e que, quando as curvas se interceptam propriamente, contamos o número de pontos na interseção; definimos então $\mathfrak{C} \cdot \mathfrak{C} = \mathfrak{C}^2 = (\mathrm{gr}(\mathfrak{C}))^2$.

Podemos generalizar este processo a toda superfície $\mathcal{S}$ (lisa e projetiva) e associar a todo par de divisores (curvas) D_1 e D_2 o "número de interseção" $D_1 \cdot D_2$. Estes números são invariantes por deformação de divisores e, em particular por equivalência linear, *i.e.*, para toda função f e divisor D sobre a superfície tem-se que $D \cdot \mathrm{div}(f) = 0$; se D_1 e D_2 se interceptam propriamente, eles são iguais ao número de pontos de interseção. Mergulhemos a superfície $\mathcal{S}$ num espaço projetivo $\mathbb{P}^n$ e consideremos a interseção D de $\mathcal{S}$ com um hiperplano de $\mathbb{P}^n$: trata-se de um divisor que tem a particularidade de reencontrar todas as curvas traçadas sobre $\mathcal{S}$; um tal divisor é dito uma *seção hiperplana*.

Outra relação fundamental envolvendo números de interseção em uma superfície projetiva não singular irredutível $\mathcal{S}$ é a *desigualdade de Riemann-Roch*:

$$\ell(D) + \ell(K - D) \geq \frac{1}{2} D(D - K) + \chi(\mathcal{O}_{\mathcal{S}}); \tag{4-17}$$

aqui D é um divisor arbitrário sobre $\mathcal{S}$, K um divisor canônico e $\chi(\mathcal{O}_{\mathcal{S}})$ é um invariante dependendo somente $\mathcal{S}$ e não de D.

Teorema do Índice de Hodge. *Se D é um divisor sobre a superfície $\mathcal{S}$ e $D \cdot H = 0$, onde H é uma seção hiperplana, então $D^2 \leq 0$.*

Demonstração: Suponha que $D^2 > 0$. Provaremos que, para todos $n > 0$ suficientemente grandes, $\ell(nD) > 0$ ou $\ell(-nD) > 0$. O teorema seguirá do seguinte: se, digamos, $\ell(nD) > 0$, então nD é linearmente equivalente a um divisor efetivo, ou seja; $nD \sim D > 0$; portanto $nD \cdot H = D \cdot H > 0$, pois cada

curva intercepta um hiperplano. Daí $nD \cdot H > 0$ e também $D \cdot H > 0$, o que contradiz a hipótese.

Usando (4-17), a suposição de que $D^2 > 0$ implica que

$$\ell(nD) + \ell(K - nD) \geq c(n) \quad \text{e} \quad \ell(-nD) + \ell(K + nD) \geq c(n),$$

onde $c(n)$ cresce com n ilimitado. Se $\ell(nD) = \ell(-nD) = 0$, temos $\ell(K - nD) \geq c(n)$ e $\ell(K + nD) \geq c(n)$. Mas agora se $\ell(D_1) > 0$, sempre temos $\ell(D_1 + D_2) \geq \ell(D_2)$; assim deduzimos que $\ell(2K) \geq c(n)$, que é uma contradição óbvia. Assim o teorema é provado. □

Se D é um divisor qualquer, tomamos

$$D_1 = \left(H^2\right) D - (D \cdot H) H.$$

Assim sendo, temos que $D_1 \cdot H = 0$ e logo $D_1^2 \leq 0$, donde obtemos a desigualdade aparentemente mais geral

$$\left(D^2\right)\left(H^2\right) \leq (D \cdot H)^2.$$

Vejamos agora a desigualdade-chave utilizada por Weil.

Desigualdade de Castelnuovo-Severi. *Seja $\mathfrak{C}$ uma curva lisa projetiva e D um divisor sobre $\mathfrak{C} \times \mathfrak{C}$. Seja P um ponto de $\mathfrak{C}$, tomamos $F_1 = \mathfrak{C} \times \{P\}$ e $F_2 = \{P\} \times \mathfrak{C}$. Escrevemos $d_1 = D \cdot F_1$ e $d_2 = D \cdot F_2$. Temos então*

$$D^2 = D \cdot D \leq 2d_1 d_2.$$

Demonstração: Esta desigualdade segue do Teorema do Índice de Hodge. Inicialmente observamos que $F_1 \cdot F_2 = 1$ e que

$$F_1 \cdot F_1 = F_2 \cdot F_2 = 0.$$

No caso em que $\mathcal{S} = \mathfrak{C} \times \mathfrak{C}$, podemos tomar $H = F_1 + F_2$. Introduzindo

$$D_1 = D - d_2 F_1 - d_1 F_2$$

verificamos então que

$$D_1 \cdot H = (D - d_2 F_1 - d_1 F_2)(F_1 + F_2) = 0.$$

Portanto, obtemos que

$$0 \geq D_1^2 = D^2 - 2d_2(D \cdot F_1) - 2d_1(D \cdot F_2) + 2d_1 d_2 (F_1 \cdot F_2) = D^2 - 2d_1 d_2.$$

Assim temos exatamente a desigualdade de Castelnuovo-Severi. □

Lema 4.3.1 (Cálculo do Número de Interseção) *Seja Γ o gráfico de Frobenius $\mathfrak{C} \to \mathfrak{C}$ definido por $x \mapsto x^q$, seja Δ a diagonal de $\mathfrak{C} \times \mathfrak{C}$ e seja $N = \#\mathfrak{C}\left(\mathbb{F}_q\right)$ o número de pontos fixos do Frobenius e g o gênero de $\mathfrak{C}$. Assim sendo, temos as fórmulas:*

$$\Gamma \cdot \Delta = N, \quad \Delta^2 = 2 - 2g, \quad \Gamma^2 = q\left(2 - 2g\right),$$
$$\Gamma \cdot F_1 = q \quad e \quad \Gamma \cdot F_2 = 1.$$

Demonstração: A intersecção do gráfico Γ com Δ é igual ao número de pontos fixos do morfismo de Frobenius, logo o número de pontos definidos sobre $\mathbb{F}_q$. Como Γ é um gráfico, seu número de interseção com F_2 é igual a 1; portanto o Frobenius é de grau q (o número de antecedentes de um ponto é em geral q), logo o número de interseção com F_1 é igual a q.

O cálculo da auto-interseção da diagonal é mais delicado, faremos o cálculo em um exemplo concreto. A curva hiperelíptica $\mathfrak{C}$ dada pela equação afim $y^2 = h\left(x\right)$, onde h é um polinômio separável de grau ímpar $2g + 1$. O inteiro g é o gênero da curva possuindo um único ponto no infinito denotado por ∞ e, se tomarmos

$$Q_1 = \left(0, \sqrt{h\left(0\right)}\right), \quad Q_2 = \left(0, -\sqrt{h\left(0\right)}\right) \quad \text{e} \quad P_j = \left(a_j, 0\right),$$

onde a_j percorre os zeros de h, verificamos que

$$\operatorname{div}\left(x\right) = \left(Q_1\right) + \left(Q_2\right) - 2\left(\infty\right),$$

e, sobretudo que, tomando $f\left(Q, P\right) = x\left(P\right) - x\left(Q\right)$, temos

$$\operatorname{div}\left(f\right) = \Delta + \Delta^{-} - 2\left(\infty\right) \times \mathfrak{C} - 2\mathfrak{C} \times \left(\infty\right),$$

onde Δ^{-} é o gráfico da involução $\iota\left(x, y\right) = \left(x, -y\right)$. Obtemos então que

$$0 = \Delta \cdot \Delta + \Delta^{-} \cdot \Delta - 2\left(\left(\infty\right) \times \mathfrak{C}\right) \cdot \Delta - 2\left(\mathfrak{C} \times \left(\infty\right)\right) \cdot \Delta.$$

O número de interseção de Δ e Δ^{-} é igual ao número de pontos fixos de ι, *i.e.* $2g + 2$ (os $2g + 1$ pontos P_j e o ponto ∞), donde obtemos o cálculo

$$\Delta \cdot \Delta = 2 \cdot 2 + 2 \cdot 2 - \left(2g + 2\right) = 2 - 2g.$$

Por fim, podemos escrever Γ como a imagem recíproca da diagonal pela aplicação $\Phi \times \mathrm{Id}_{\mathfrak{C}} : \mathfrak{C} \times \mathfrak{C} \to \mathfrak{C} \times \mathfrak{C}$ e deduzimos que

$$\Gamma \cdot \Gamma = \operatorname{gr}\left(\Phi \times \mathrm{Id}_{\mathfrak{C}}\right) \Delta \cdot \Delta = q\Delta \cdot \Delta = q\left(2 - 2g\right).$$

□

Aplicamos as fórmulas do Lema 4.3.1 acima ao divisor $D = r\Gamma + s\Delta$, obtemos:

$$d_1 = D \cdot F_1 = rq + s \quad \text{e} \quad d_2 = D \cdot F_2 = r + s.$$

Desta forma, a desigualdade de Castelnuovo-Severi se escreve como

$$D \cdot D = D^2 = r^2 q\,(2 - 2g) + 2rsN + s^2\,(2 - 2g) \leq 2\,(rq + s)\,(r + s)\,,$$

donde obtemos

$$gqr^2 + (q + 1 - N)\,rs + gs^2 \geq 0.$$

Se observarmos que o discriminante da inequação em r, s deve ser negativo, obtemos a desigualdade desejada:

$$|q + 1 - N| \leq 2g\sqrt{q}.$$

Capítulo 5

Aplicação: Códigos Corretores de Goppa

5.1 Generalidades

Definição 5.1.1 Um *código linear* C sobre o alfabeto $\mathbb{F}_q$ é um subespaço vetorial de $\mathbb{F}_q^n$. Se d é a dimensão de C sobre $\mathbb{F}_q$ dizemos que C é um $[n, d]$-código.

Há várias maneiras de se descrever um código, podemos, por exemplo, dar uma base $v_1, \ldots, v_d$ de C. Neste caso, se $v_i = (v_{i1}, \ldots, v_{in})$ então a aplicação $V : \mathbb{F}_q^d \to \mathbb{F}_q^n$ dada por

$$V(a_1, \ldots, a_d) = \sum_{i=1}^{d} a_i v_i = \left(\sum_{i=1}^{d} a_i v_{i1}, \ldots, \sum_{i=1}^{d} a_i v_{in} \right)$$

é um "codificador", isto é, pensando $\mathbb{F}_q^d$ como o conjunto das palavras numa linguagem "natural" a função V nos diz como codificar as palavras.

Definição 5.1.2 A matriz $V = (v_{ij})$ que descreve a aplicação linear V é chamada a *matriz geradora* do código. Diremos que V está na *forma padrão* se

$$V = (I_d P)$$

para uma matriz P, isto é, $v_{ij} = \delta_{ij}$ para $i, j = 1, \ldots, d$ (onde $\delta_{ij} = 0$ se $i \neq j$, $\delta_{ii} = 1$). Neste caso diremos que os primeiros d símbolos ou coordenadas de $c \in C$ são os *símbolos de informação* e os restantes os *símbolos de controle*.

Porque símbolos de controle? Dado um vetor $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, para checar se $x \in C$ basta verificar se $x = V(a)$ para algum a e neste caso (estamos supondo C padrão) $x_j = a_j$, $j \leq d$ e $x_j = \sum_{i=1}^{d} a_i v_{ij} = \sum_{i=1}^{d} x_i v_{ij}$ para $j > d$. Logo, para checar se $x \in C$ basta verificar se $x_j = \sum_{i=1}^{d} x_i v_{ij}$, para $j = d+1, \ldots, n$.

Definição 5.1.3 Diremos que dois códigos C_1 e C_2 são *equivalentes* se pudermos obter C_2 a partir de C_1 por permutação das coordenadas.

Pode-se provar que todo código é equivalente a um código que pode ser gerado por uma matriz na forma padrão.

Pelo que vimos acima a informação contida numa palavra $c \in C$ depende de d coordenadas e o resto é redundância, que é usada para controle. Definimos então a *razão de informação* de C, denotada por $i(C)$, como sendo n/d. Isso medirá então a razão entre o número de coordenadas "informativas" e o número total de coordenas.

Outra maneira de descrever um código é dar uma aplicação linear sobrejetiva $H : \mathbb{F}_q^n \to \mathbb{F}_q^{n-d}$ tal que o núcleo de H é C. Neste caso temos $(x_1, \ldots, x_n) \in C$ se, e somente se, $H(x_1, \ldots, x_n) = 0$. Se $H = \left(b_{ij}\right)$ então a última equação se escreve

$$\sum_{j=1}^{n} h_{ij} x_j = 0, \quad i = 1, \ldots, n-d.$$

Definição 5.1.4 A matriz H definida acima é chamada de *matriz de controle de paridade* de C.

Se C é dado pela matriz geradora $(I_d P)$ como acima, isto é, C é padrão, é fácil calcular a matriz de controle de C. De fato, temos $x \in C$ se e somente se $x_j = \sum_{i=1}^{d} x_i v_{ij}$, $j > d$, como vimos acima, logo a matriz controle é dada por

$$\left(-{}^t P I_{n-d}\right)$$

onde ${}^t P$ é a transposta de P.

Exemplo 5.1.1 Um exemplo ilustrativo que origina o nome "controle de paridade" é o código de controle de paridade sobre $\mathbb{F}_2$ definido pela matriz geradora $(I_n 1)$ onde $1 = {}^t(1, \ldots, 1)$, isto é, $C \subset \mathbb{F}_q^{n+1}$ dado por

$$\left\{ (x_1, \ldots, x_n, x_1 + \cdots + x_n) \;\middle|\; (x_1, \ldots, x_n) \in \mathbb{F}_q^n \right\}.$$

A matriz controle de paridade de C é $(1, \ldots, 1)$. É fácil ver então que $x \in C$ se, e somente se, $\sum x_i = 0$, isto é, x tem um número par de coordenadas não nulas, daí o nome controle de paridade.

Em geral tomamos os códigos de tal modo que duas palavras do código sejam sempre bem diferentes, para que quando recebamos uma mensagem com possíveis erros poderemos decodificá-la como a palavra no código mais parecida com a mensagem recebida. Para formalizar os conceitos de "diferente" e "parecido" definimos a *norma de Hamming* em $\mathbb{F}_q^n$ pondo para $x \in \mathbb{F}_q^n$,

$$|x| = \text{número de coordenadas não nulas de } x.$$

Vale então as seguintes propriedades:

(1) $|x| = 0$ se e só se $x = 0$;

(2) $|\lambda x| = |x|$ se $\lambda \in \mathbb{F}_q$, $\lambda \neq 0$;

(3) $|x + y| \leq |x| + |y|$.

Definimos também a *distância de Hamming* pondo

$$d(x, y) = |x - y|,$$

que satisfaz:

(1′) $d(x, y) = 0$ se e só se $x = y$;

(2′) $d(x, y) = d(y, x)$;

(3′) $d(x, z) \leq d(x, y) + d(y, z)$.

Note que $d(x, y)$ é o número de coordenadas onde x e y diferem, logo $d(x, y)$ mede quão diferentes são x e y. d é uma métrica em $\mathbb{F}_q^n$.

Vamos provar que de fato as propriedades acima são verificadas.

Note que *(1′)* segue de *(1)*, *(2′)* de *(2)* (com $\lambda = -1$) e *(3′)* de *(3)*. As propriedades *(1)* e *(2)* são imediatas. Provaremos a propriedade *(3)*.

Sejam

$$I = \{i \in \{1, \ldots, n\} \mid x_i = 0\} \quad \text{e} \quad J = \{i \in \{1, \ldots, n\} \mid y_i = 0\}$$

então, por definição,

$$|x| = n - \#I \quad \text{e} \quad |y| = n - \#J.$$

Logo

$$|x| + |y| = 2n - (\#I + \#J).$$

Por outro lado, temos que $\#I + \#J = \#(I \cup J) + \#(I \cap J)$ e $\#(I \cup J) \leq n$, logo

$$|x| + |y| \geq n - (\#I \cap \#J).$$

Porém, se $i \in I \cap J$, temos que $x_i = y_i = 0$, logo $x_i + y_i = 0$. Então $x + y$ tem a i-ésima coordenada nula para $i \in I \cap J$, consequentemente

$$|x + y| \leq n - \#(I \cap J).$$

Isso conclui a demonstração. □

Já podemos então medir quanto as palavras de um código diferem umas das outras. Definimos então o *peso de um código* C, denotado por $w(C)$ pondo

$$w(C) = \min\{d(x,y) \mid x,y \in C,\ x \neq y\}.$$

Como o código é um subespaço, temos que $x - y \in C$ toda vez que $x, y \in C$, logo

$$w(C) = \min\{|x| \mid x \in C,\ x \neq 0\}.$$

Podemos então passar a correção e detecção de erros. Dizemos que um código C *corrige e erros* se para todo $y \in \mathbb{F}_q^n$ existe no máximo um único $x \in C$ com $d(x,y) \leq e$. Isso significa que ao recebermos uma mensagem y com no máximo e erros, isto é, y difere de algum elemento $x \in C$ em no máximo e coordenadas, esse elemento x sendo a mensagem enviada, então x é o único elemento de C tão próximo de y, logo podemos recuperar x a partir de y. Mais adiante veremos como implementar esse procedimento. Agora vamos ver quantos erros um código pode corrigir.

Teorema 5.1.1 *Seja C um código de peso $w(C)$, então C corrige*

$$\left\lfloor \frac{w(C)-1}{2} \right\rfloor$$

erros.

Demonstração: Seja $e = \lfloor \frac{w(C)-1}{2} \rfloor$, então $2e+1 \leq w(C)$. Suponha que C não corrija e erros, e seja $y \in \mathbb{F}_q^n$ tal que existam $x_1, x_2 \in C$, $x_1 \neq x_2$, com $d(x_1,x_2) \leq e$, $i = 1,2$. Por *(3′)* temos que

$$d(x_1,x_2) \leq d(x_1,y) + d(y,x_2) \leq 2e.$$

Por outro lado, como $x_1 \neq x_2$, pela definição de $w(C)$ temos que

$$d(x_1,x_2) \geq w(C) \geq 2e+1,$$

contradição. □

Um resultado útil para se determinar $w(C)$ é o seguinte:

Proposição 5.1.1 *Seja C um código com matriz de controle H e peso $w(C)$. Então quaisquer $w(C)-1$ colunas de H são linearmente independentes e existem $w(C)$ colunas de H linearmente dependentes.*

DEMONSTRAÇÃO: Seja s o inteiro tal que quaisquer s colunas de H são linearmente independentes e existem $s+1$ colunas de H linearmente dependentes.

Sejam $h_1, \ldots, h_n$ as colunas de H. Se $h_{i_1}, \ldots, h_{i_{s+1}}$ são linearmente dependentes, existem $c_{i_1}, \ldots, c_{i_{s+1}} \in \mathbb{F}_q$ com $\sum c_{i_j} h_{i_j} = 0$. Seja $c = (c_1, \ldots, c_n)$ definido por $c_i = c_{i_j}$ se $i \in \{i_1, \ldots, i_{s+1}\}$, $c_i = 0$ caso contrário. Então $\sum c_i h_i = 0$ e $c \in C$, porém c tem no máximo $s+1$ coordenadas não nulas, logo $w(C) \leq s+1$.

Se $w(C) < s+1$ existe $c \in C$, $c \neq 0$, com no máximo s coordenadas não nulas, digamos $c_i = 0$ se $i \neq i_1, \ldots, i_s$. Como $c \in C$, $\sum_{i=1}^{n} c_i h_i = 0$, logo $\sum_{j=1}^{s} c_{i_j} h_{i_j} = 0$ e então $h_{i_1}, \ldots, h_{i_s}$ são linearmente dependentes, isso contradiz a definição de s, logo $w(C) = s+1$, como queríamos demonstrar. □

Corolário 5.1.1 (Singleton) *Se C é um $[n,d]$-código, então*

$$w(C) \leq n - d + 1.$$

DEMONSTRAÇÃO: Seja H a matriz de controle de C. Como as colunas de H estão em $\mathbb{F}_q^{n-d}$, quaisquer $n-d+1$ colunas de H são linearmente dependentes. O resultado agora segue da proposição. □

Definição 5.1.5 Códigos com $w(C) = n - d + 1$ são chamados *códigos separáveis pela distância máxima* ou MDS (maximum distance separable).

Os códigos MDS tem uma descrição interessante com conjuntos satisfazendo certas propriedades geométricas em espaços projetivos sobre corpos finitos que discutiremos no Seção 5.4.

Passamos agora a dar um procedimento simples de decodificação.

Se C é um $[n,d]$-código dado como núcleo de $H : \mathbb{F}_q^n \to \mathbb{F}_q^{n-d}$. Se $x \in \mathbb{F}_q^n$ chamaremos $H(x)$ de *síndrome* de x. Para cada $v \in \mathbb{F}_q^{n-d}$ escolha e_v tal que $H(e_v) = v$ e tal que $|e_v|$ é mínima. e_v é chamado um líder da classe lateral $H^{-1}(v)$. e_v pode não ser único, mas fixemos um em cada classe. Se recebermos uma mensagem y, calculamos $H(y) = v$ e tomamos $c = y - e_v$ como a decodificação de y.

Note primeiro que $H(c) = H(y) - H(e_v) = v - v = 0$, logo $c \in C$. Note também que $d(c,y) = |e_v|$. Como e_v foi escolhido minimizando a norma em $H^{-1}(v)$ temos que c é o elemento de C mais próximo de y. Consequentemente, se C corrige e erros, a decodificação nos dará a mensagem enviada toda vez que a mensagem recebida tem síndrome v satisfazendo $|e_v| \leq e$. Esse processo é chamado *decodificação por semelhança máxima*.

Em geral esse procedimento é muito custoso, pois nos obriga a calcular os e_v. Códigos com propriedades particulares podem ter algoritmos de decodificação mais eficientes. Encontraremos alguns exemplos disso mais adiante.

5.2 Cotas

Quais são os melhores códigos que podemos construir? Nessa generalidade essa pergunta não está resolvida. O que podemos dizer, por outro lado, é que não podemos ser otimista demais, há limitações no que podemos conseguir.

Já provamos um tal resultado, a cota de Singleton (Corolário 5.1.1) que afirma que um $[n, d]$-código C satisfaz $w(C) \leq n - d + 1$. Passaremos agora a discutir outros resultados desse tipo.

Introduzimos algumas notações.

Se $r \leq n$ é um inteiro e $a \in \mathbb{F}_q^n$, definimos a *bola de centro a e raio r*, como o conjunto

$$B(a, r) = \left\{ x \in \mathbb{F}_q^n \;\middle|\; d(x, a) \leq r \right\}.$$

Se n e w são inteiros tais que $w \leq n$, definimos

$$A_q(n, w) = \max \left\{ \dim C \;\middle|\; C \subset \mathbb{F}_q^n, \text{ código com } w(C) = w \right\}.$$

Então, $A_q(n, w)$ é a maior dimensão possível entre os códigos de peso e comprimento w e n dados sobre $\mathbb{F}_q$ e os resultados que estamos procurando são cotas superiores para $A_q(n, w)$. Por exemplo, a cota de Singleton diz que $A_q(n, w) \leq n - w + 1$.

Seja

$$V_q(n, r) = \#B(a, r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

Essa última definição merece um comentário. Primeiro ela afirma que $\#B(a, r)$ não depende de a. De fato, a função

$$x \mapsto x - a$$

estabelece uma bijeção entre $B(a, r)$ e $B(0, r)$. Segundo, a igualdade $\#B(a, r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$. Bom, $B(0, r)$ é o conjunto dos $x \in \mathbb{F}_q^n$ com $|x| \leq r$. Mostraremos que o conjunto dos $x \in \mathbb{F}_q^n$ com $|x| = i$ tem cardinalidade $\binom{n}{i}(q-1)^i$ e isso provará o que queremos.

Como escolher x tal que $|x| = i$? Primeiro, x tem i coordenadas não nulas, temos que escolher quais as coordenadas, temos então $\binom{n}{i}$ escolhas. Agora temos que escolher o valor de cada coordenada em $\mathbb{F}_q \setminus \{0\}$, temos $q - 1$ escolhas para

cada coordenada logo $(q-1)^i$ escolhas para todas as coordenadas não nulas e o resultado segue. □

A nossa primeira cota é conhecida como *cota do empacotamento de esferas*.

Teorema 5.2.1 (Hamming)

$$A_q(n,w) \leq \log_q \left(\frac{q^n}{V_q\left(n, \left\lfloor \frac{w-1}{2} \right\rfloor\right)} \right).$$

Demonstração: Seja C um $[n,d]$-código de peso w e $e = \left\lfloor \frac{w-1}{2} \right\rfloor$. Vimos na Seção 5.1 que C corrige e erros e isso significa que as bolas $B(c,e)$, $c \in C$, são disjuntas, então

$$\sum_{c \in C} \#B(c,e) \leq \#\mathbb{F}_q^n = q^n,$$

logo

$$\#C \cdot V_q(n,e) \leq q^n,$$

mas $\#C = q^d$ e o resultado segue. □

Essa cota tem relações com o problema clássico de empacotamento de esferas. Esse problema pode ser descrito da seguinte maneira: quantas bolas de pingue-pongue cabem numa caixa dada? Evidentemente podemos formular o problema em um número qualquer de dimensões. O caso de dimensão dois foi resolvido por uma abelha há alguns milhões de anos atrás! Mas em dimensões maiores o problema é bem mais difícil.

Mas as relações não param aí e o problema se conecta com reticulados em $\mathbb{R}^n$, cristais, grupos finitos e outras coisas mais. Não trataremos dessas coisas aqui, para maiores informações sobre esse tratamento vide [78].

A técnica de empacotar esferas leva ao seguinte resultado na direção inversa do Teorema 5.2.1.

Teorema 5.2.2 (Gilbert-Varshamov) *Se $w \leq n$, então*

$$A_q(n,w) \geq \log_q \left(\frac{q^n}{V_q(n, w-1)} \right).$$

Demonstração: Suponha que d é um inteiro satisfazendo

$$d < \log_q \left(q^n / V_q(n, w-1) \right)$$

e que C é um $[n,d]$-código com $w(C) = w$. Vamos mostrar que podemos construir um código C' com dimensão $d+1$ em $\mathbb{F}_q^n$ e com $w(C) = w$.

Temos que

$$\sum_{c\in C} \#B\left(c, w-1\right) = q^d V_q\left(n, w-1\right) < q^n = \#\mathbb{F}_q^n.$$

Logo, existe $x \in \mathbb{F}_q^n$, $x \notin \bigcup_{c\in C} B\left(c, w-1\right)$. Em particular $c \notin C$ e $d\left(x, c\right) \geq w$ para todo $c \in C$. Considere o código C' gerado como espaço vetorial por C e x. Mostraremos que C' é o código desejado. Claramente a dimensão de C' é $d+1$. Calculemos $w\left(C'\right)$.

Se $c' \in C'$, $c' \neq 0$, então $c' = c + \lambda x$, $c \in C$, $\lambda \in \mathbb{F}_q$. Se $\lambda = 0$ então $c \neq 0$ e $|c'| = |c| \geq w$. Se $\lambda \neq 0$ então

$$|c'| = \left|\frac{1}{\lambda}c'\right| = \left|c + \frac{c}{\lambda}\right| = d\left(x, -\frac{c}{\lambda}\right).$$

Como $-\frac{c}{\lambda} \in C$, pois C é um subespaço linear de $\mathbb{F}_q^n$, devemos ter $d\left(x, -\frac{c}{\lambda}\right) \geq w$ pela construção de x, logo $|c'| \geq w$. Mostraremos então que $w\left(C'\right) \geq w$, porém existe $c \in C$ com $|c| = w$, como $C \subset C'$ concluímos que $w\left(C'\right) = w$.

Para provar o teorema começamos com um elemento $a \in \mathbb{F}_q^n$, $|a| = w$, e consideremos $C_1 = \left\{\lambda a \;\middle|\; \lambda \in \mathbb{F}_q\right\}$ que é um código de dimensão 1 e $w\left(C_1\right) = w$. O procedimento dado acima nos permite, se $1 < \log_q\left(q^n / V_q\left(n, w-1\right)\right)$, construir um código C_2 de peso w e dimensão 2. Sucessivamente, então construímos, se $d < \log_q\left(q^n / V_q\left(n, w-1\right)\right)$ códigos $C_1, C_2, \ldots, C_{d+1}$ tais que $w\left(C_i\right) = w$ e $\dim C_i = i$ e isso prova teorema. □

Notemos que a prova do teorema nos dá um algoritmo para construir bons códigos. Porém, na prática esse algoritmo é impraticável, pois consome muito tempo. Goppa e outros autores construíram códigos por algoritmos praticáveis e partir de uma construção devida a Goppa que produz códigos satisfazendo

$$\dim C \geq \log_q\left(\frac{q^n}{V_q\left(n, w-1\right)}\right).$$

Mais ainda, esses códigos fazem parte de uma família infinita de bons códigos. Veremos esta construção na Seção 5.5.

Voltando ao problema das cotas superiores para $A_q\left(n, w\right)$, temos ainda:

Teorema 5.2.3 (Plotkin) *Ponha $\theta = 1 - \frac{1}{q}$. Se $w > \theta n$ então*

$$A_q\left(n, w\right) \leq \log_q\left(\frac{w}{w - \theta n}\right).$$

DEMONSTRAÇÃO: Seja C um $[n,d]$-código de peso $w > n\theta$. Considere os conjuntos $\{c \in C \mid c_i \neq 0\}$, $i = 1, \ldots, n$. Dado um elemento $c \in C$ este elemento aparece em $|c|$ destes conjuntos, logo temos

$$\sum_{c \in C} |c| = \sum_{i=1}^{n} \#\{c \in C \mid c_i \neq 0\}.$$

Seja i inteiro, $1 \leq i \leq n$ e considere $D = \{c \in C \mid c_i \neq 0\}$. D é um subespaço linear de C e a codimensão de D em C é no máximo 1, logo $\dim D = d$ ou $d-1$, logo $\#D = q^d$ ou q^{d-1}. Por outro lado $\#\{c \in C \mid c_i \neq 0\} = \#C - \#D$. Logo, em qualquer hipótese, $\#\{c \in C \mid c_i \neq 0\} \leq q^d - q^{d-1} = \theta q^d$. Concluímos que

$$\sum_{c \in C} |c| \leq n\theta q^d.$$

Por outro lado, se $c \in C$, $c \neq 0$ temos $|c| \geq w$, logo

$$\sum_{c \in C} |c| \geq w\left(q^d - 1\right).$$

Segue-se então que

$$q^d \leq \frac{w}{w - \theta n}$$

e o teorema está demonstrado. □

Vamos agora comparar as cotas obtidas. Para isso é conveniente olhas as coisas assintoticamente. Para isso definimos

$$\alpha_q(\delta) = \limsup_{n \to \infty} \frac{A_q(n, \lfloor \delta n \rfloor)}{n}, \quad 0 \leq \delta \leq 1.$$

Isto é, $\alpha_q(\delta)$ é o supremo dos números α tal que exista uma sequência de códigos C_i, $i = 1, 2, \ldots$, $C_i \subset \mathbb{F}_q^{n_i}$ tais que

$$\frac{w(C_i)}{n_i} \to \delta \quad \text{e} \quad \frac{\dim C_i}{n_i} \to \alpha.$$

Isso nos permite considerar as cotas para n grande sem se ater a peculiaridades de um número finito de valores de n.

O primeiro resultado interessante sobre $\alpha_q(\delta)$ é devido a Manin ([51]): $\alpha_q(\delta)$ é uma função contínua e decrescente. A cota de Singleton nos dá

$$\alpha_q(\delta) \leq 1 - \delta.$$

A cota de Plotkin nos dá, ($\theta = 1 - \frac{1}{q}$)

$$\alpha_q(\delta) \leq 0 \quad \text{se} \quad \theta \leq \delta \leq 1,$$

logo

$$\alpha_q(\delta) = 0 \quad \text{se} \quad \theta \leq \delta \leq 1.$$

Usando a cota de Plotkin podemos deduzir o seguinte

$$\alpha_q(\delta) \leq 1 - \frac{\delta}{\theta}, \quad 0 \leq \delta \leq \theta.$$

O raciocínio é o seguinte. Suponha que C é um $[n, d]$-código de peso w com $w \leq \theta n$. Ponha $n' = \left\lfloor \frac{w-1}{\theta} \right\rfloor$ e tome um subcódigo C' de C obtido anulando $n - n'$ coordenadas.

Então podemos considerar C' como um $[n', d']$-código e $d' \geq d + n' - n$ e $w(C') = w$. Podemos aplicar o Teorema 5.2.3 a C' e obtemos

$$d' \leq \log_q \left(\frac{w(C')}{w(C') - \theta n'} \right) = \log_q \left(\frac{w}{w - n'\theta} \right).$$

Se tomarmos C uma sequência com $\frac{w}{n} \to \delta$ e $\frac{d}{n} \to \alpha$ então

$$\frac{n'}{n} \to \frac{\delta}{\theta}$$

e

$$\frac{d}{n} \leq \frac{d' + n - n'}{n} \leq \frac{1}{n} \log_q \left(\frac{w}{w - n'\theta} \right) + 1 - \frac{n'}{n},$$

e temos que

$$\frac{1}{n} \log_q \left(\frac{w}{w - n'\theta} \right) \to 0,$$

logo

$$\alpha \leq 1 - \frac{\delta}{\theta}$$

e o resultado segue.

A cota de Hamming nos dá

$$\alpha_q(\delta) \leq 1 - H_q\left(\frac{\delta}{2}\right), \quad 0 \leq \delta \leq \theta,$$

onde

$$H_q(x) = \begin{cases} 0 & \text{se} \quad x = 0, \\ x\log_q\theta - x\log_q x - (1-x)\log_q(1-x) & \text{se} \quad 0 < x \leq \theta. \end{cases}$$

Isso segue do seguinte fato que se prova facilmente através da fórmula de Stirling* (ver [80, Lema 5.1.6]):

$$\lim_{n\to\infty} \frac{\log_q V_q(n, \lfloor \lambda n \rfloor)}{n} = H_q(\lambda).$$

* $\lim\limits_{n\to+\infty} \dfrac{n!}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n} = 1.$

Das três cotas mencionadas, a pior é a de Singleton. A cota de Hamming é melhor que a de Plotkin para $0 \leq \delta \leq \delta_0$ para um certo $\delta_0 \in (0, \theta)$, para $\delta_0 \leq \delta \leq \theta$ a de Plotkin é melhor. A melhor cota conhecida, devida a Elias, é a seguinte

$$\alpha_q(\delta) \leq 1 - H_q\left(\theta - \sqrt{\theta(\theta - \delta)}\right), \quad 0 \leq \delta \leq \theta. \tag{$*$}$$

Uma prova desta cota pode ser vista em [80]. Quando $q = 2$ há uma cota melhor ainda ([50]).

Para constar, o Teorema 5.2.2 nos dá:

$$\alpha_q(\delta) \geq 1 - H_q(\delta), \quad 0 \leq \delta \leq \theta. \tag{$**$}$$

Há um espaço entre $(*)$ e $(**)$ e no presente momento não se sabe o que ocorre aí nesse espaço.

5.3 Códigos Cíclicos

Definição 5.3.1 Um *código cíclico* $C \subset \mathbb{F}_q^n$ é um código tal que $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ sempre que $(c_0, \ldots, c_{n-1}) \in C$. Isto é, C é invariante com respeito a permutações cíclicas de coordenadas.

O interesse fundamental dos códigos cíclicos é que eles admitem um representação interessante em termos de polinômios sobre $\mathbb{F}_q$ que permite a descrição de um algoritmo de decodificação muito simples.

Consideramos o anel $A = \mathbb{F}_q[x] / (x^n - 1)$, quociente de $\mathbb{F}_q[x]$ pelo ideal gerado por $x^n - 1$. Todo elemento de A pode ser representado unicamente por um polinômio $a_0 + \cdots + a_{n-1}x^{n-1}$ de grau no máximo $n - 1$ (pelo algoritmo de divisão de polinômios). Vamos identificar $\mathbb{F}_q$ com A identificando $a = (a_0, \ldots, a_{n-1})$ com $a_0 + \cdots + a_{n-1}x^{n-1} = a(x)$. Note que se $b = (a_{n-1}, a_0, \ldots, a_{n-2})$ então

$$b(x) \equiv xa(x) \pmod{x^n - 1}.$$

De fato,

$$\begin{aligned} xa(x) &= a_0x + \cdots + a_{n-1}x^n \\ &\equiv a_{n-1} + a_0x + \cdots + a_{n-2}x^{n-1} \pmod{x^n - 1}. \end{aligned}$$

Então os códigos cíclicos podem ser caracterizados como os subespaços C de A tais que

$$c(x) \in C \Rightarrow xc(x) \in C.$$

Notemos agora que se C é um código cíclico e $c(x) \in C$ então

$$xc(x) \in C, x^2c(x) \in C, \ldots,$$

logo $b(x)\,a(x) \in C$ para todo $b(x) \in A$. Bem, isto quer dizer que C é um ideal de A. Reciprocamente, se C é um ideal de A então C é um subespaço de A e $xc(x) \in C$ sempre que $c(x) \in C$, logo C é um código cíclico. Resumindo os códigos cíclicos são ideais de A. Os ideais de A tem a seguinte caracterização:

Proposição 5.3.1 *Todo ideal de A é da forma (g) onde g é um divisor mônico de $x^n - 1$. Além disso, tal g é unicamente determinado pelo ideal.*

Demonstração: Seja $\varphi : \mathbb{F}_q[x] \to A$ a aplicação canônica. Se C é um ideal de A então obviamente $\varphi^{-1}(C)$ é um ideal de $\mathbb{F}_q[x]$. Como $\mathbb{F}_q[x]$ é euclidiano $\varphi^{-1}(C)$ é principal, $\varphi^{-1}(C) = (h)$. Logo C é gerado por h em A. Escrevamos $h = fg$ onde g é um divisor mônico de $x^n - 1$ e $\operatorname{mdc}(f, x^n - 1) = 1$, isto é, g é o máximo divisor comum de h e $x^n - 1$. Mostraremos que $C = (g)$. Como f e $x^n - 1$ são coprimos existe $\overline{f}$ tal que $f\overline{f} \equiv 1 \pmod{x^n - 1}$. Seja $c \in C$, sabemos então que $c = ah = afg$ logo $c \in (g)$, isto é, $C \subset (g)$. Se mostrarmos que $g \in (h)$ então teremos $C = (h) \supset (g)$ e consequentemente $C = (g)$. De fato, $g \in (h)$ pois $\overline{f}h = \overline{f}fg \equiv g \pmod{x^n - 1}$ logo $g = \overline{f}h$ em A.

Para a unicidade suponha que $(g) = (g')$, então $g' = fg$ e $g = f'g'$ logo $ff' = 1$ e f é invertível em A. Isso implica que f é coprimo com $x^n - 1$. Como g' divide $x^n - 1$ devemos então ter que $f \in \mathbb{F}_q$ e como g e g' são mônicos, $f = 1$ e logo $g = g'$. □

Se $C = (g)$ é um código cíclico então o polinômio g é chamado o *gerador* de C e o polinômio $h(x) = (x^n - 1)/g$ é chamado o *polinômio de controle* de C. Notemos que $c(x) \in C$ se, e somente se, $h(x)\,c(x) \equiv 0 \pmod{x^n - 1}$, daí o nome de controle.

Lembramos agora que se $a(x) \in A$, $a(x) = a_0 + \cdots + a_{n-1}x^{n-1}$ então existem polinômios $b(x)$ e $r(x)$ tais que

$$a(x) = b(x)\,g(x) + r(x), \quad \operatorname{gr}(r(x)) < \operatorname{gr}(g(x)).$$

Mais ainda, $\operatorname{gr}(b(x)) < n - \operatorname{gr}(g(x))$. Seja d o grau de g. Então para todo elemento $a(x) \in C$, devemos ter $r(x) = 0$, logo $a(x) = b(x)\,g(x)$ onde $\operatorname{gr}(b(x)) < n - d$. Dai segue imediatamente que $\dim C = n - d$.

Vemos também que $g(x), xg(x), \ldots, x^{n-d-1}g(x)$ é uma base de C sobre $\mathbb{F}_q$, logo, se $g = g_0 + g_1x + \cdots + g_dx^d$, então

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & \cdots & g_d & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & \cdots & \cdots & \cdots & g_d & \cdots & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & \cdots & \cdots & g_d & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 0 & g_0 & \cdots & \cdots & \cdots & g_d \end{pmatrix}$$

é uma matriz geradora de C.

Vimos acima também que $c(x) \in C$ se, e somente se, $h(x)\,c(x) = 0$. Daí conclui-se facilmente que

$$H = \begin{pmatrix} 0 & \cdots & 0 & h_{n-d} & \cdots & h_1 & h_0 \\ 0 & \cdots & h_{n-d} & \cdots & \cdots & h_0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ h_{n-d} & \cdots & h_0 & 0 & \cdots & \cdots & 0 \end{pmatrix}$$

é uma matriz de controle de C, onde $h(x) = \frac{x^n-1}{g(x)} = \sum_{i=0}^{n-d} h_i x^i$.

De agora em diante suporemos que $\text{mdc}(n, q) = 1$.

Estudaremos agora o peso de um código cíclico, para isso introduziremos o chamado *polinômio de Mattson-Solomon* (ou *transformada de Fourier discreta*).

Seja $\overline{\mathbb{F}}_q$ o fecho algébrico de $\mathbb{F}_q$ e $\beta \in \overline{\mathbb{F}}_q$ uma raiz primitiva n-ésima da unidade e T o conjunto de polinômios de grau menor do que n com coeficientes em $\overline{\mathbb{F}}_q$. Define-se $\mathcal{F} : T \to T$ pondo

$$\mathcal{F}(a) = \sum_{j=0}^{n} a\left(\beta^j\right) x^{n-j}.$$

Lema 5.3.1

$$\mathcal{F}(a)\left(\beta^k\right) = na_k.$$

Demonstração: Calculemos $\mathcal{F}(a)\left(\beta^k\right)$:

$$\mathcal{F}(a)\left(\beta^k\right) = \sum_{j=0}^{n}\left(\sum_{i=0}^{n-1} a_i\beta^{ij}\right)\left(\beta^k\right)^{n-j} \overset{(\beta^n=1)}{=} \sum_{j=0}^{n}\sum_{i=0}^{n-1} a_i\beta^{ij}\beta^{-kj}$$
$$= \sum_{j=0}^{n}\sum_{i=0}^{n-1} a_i\beta^{j(i-k)} = \sum_{i=1}^{n-1}\left(\sum_{j=0}^{n}\beta^{j(i-k)}\right)a_i.$$

Afirmamos que:

$$\sum_{j=0}^{n}\beta^{jr} = \begin{cases} n & \text{se} \quad r = 0, \\ 0 & \text{se} \quad -n < r < n. \end{cases}$$

Desta afirmação seguirá que $A\left(\beta^k\right) = na_k$. A afirmação é trivial se $r = 0$. Nos outros casos temos

$$\sum_{j=0}^{n} \beta^{jr} = \frac{\beta^{rn} - 1}{\beta^r - 1} = \frac{\left(\beta^n\right)^r - 1}{\beta^r - 1} = 0.$$

□

Teorema 5.3.1 *Seja r o grau de* $\operatorname{mdc}\left(x^n - 1, \mathcal{F}\left(a\right)\right)$*, então* $|a| = n - r$.

Demonstração: $n - |a|$ é o número de coeficientes de $a\left(x\right)$ que são nulos. Temos que $a_k = 0$ se, e somente se, $\mathcal{F}\left(a\right)\left(\beta^k\right) = 0$, pelo Lema 5.3.1. Então $n - |a|$ é o número de raízes n-ésimas da unidade que são zeros $\mathcal{F}\left(a\right)$, isto é, o número de raízes comuns de $\mathcal{F}\left(a\right)$ e $x^n - 1$ que é o grau de $\operatorname{mdc}\left(x^n - 1, \mathcal{F}\left(a\right)\right)$, provando o teorema. □

Vamos agora estudar mais detalhadamente uma classe especial de códigos, conhecidos como códigos BCH (*i.e.*, Bose, (Ray) Chaudhuri, Hocquenghem). Seja $\beta \in \overline{\mathbb{F}}_q$ uma raiz primitiva n-ésima da unidade e denotemos por $g^{(i)}\left(x\right)$ o polinômio mínimo de β^i sobre $\mathbb{F}_q$, isto é, o polinômio mônico não nulo de menor grau com coeficientes em $\mathbb{F}_q$ que tem β^i como raiz.

Definição 5.3.2 O *código BCH* de distância designada δ é o código cíclico com polinômio gerador

$$g\left(x\right) = \operatorname{mmc}\left(g^{(1)}, \ldots, g^{(\delta-1)}\right).$$

Seja m o menor inteiro positivo tal que $q^m \equiv 1 \pmod{n}$ então $\mathbb{F}_{q^m}$ é a menor extensão de $\mathbb{F}_q$ que contém todas as raízes de $x^n - 1 = 0$. Consequentemente $\operatorname{gr}\left(g^{(i)}\right) \leq m$ para $i = 1, \ldots, n$, logo $\operatorname{gr}\left(g\right) \leq m\left(\delta - 1\right)$. Daí se conclui que

$$\dim C \geq n - m\left(\delta - 1\right).$$

O resultado seguinte nos dá uma estimativa para o peso de C e justifica o nome de distância designada.

Teorema 5.3.2

$$w\left(C\right) \geq \delta.$$

Demonstração: Seja $c\left(x\right) \in C$, $c\left(x\right) \neq 0$. Como $g\left(x\right) \mid c\left(x\right)$ e $g\left(\beta^i\right) = 0$, $i = 1, \ldots, \delta - 1$, temos $g\left(\beta^i\right) = 0$, $i = 1, \ldots, \delta$. Consequentemente, o grau de $\mathcal{F}\left(c\right)$ é no máximo $n - \delta$. Segue-se que o grau de $\operatorname{mdc}\left(\mathcal{F}\left(c\right), x^n - 1\right)$ é no máximo $n - \delta$, logo $|c| \geq \delta$ pelo Teorema 5.3.1. □

Suponha que escolhemos um código BCH de distância designada $\delta = 2t + 1$, sabemos então que esse código corrige t erros. O que torna os códigos BCH muito interessantes é que há um algoritmo de decodificação eficiente, devido a Berlekamp, que passamos a expor.

Seja $C \in A$ então um código BCH de distância designada $\delta = 2t + 1$ e β a raiz primitiva n-ésima da unidade usada para definir C.

Seja $a(x) \in A$ uma palavra recebida com no máximo t erros. Suponhamos inicialmente que conhecemos a palavra enviada $c(x)$ e seja $e(x) = a(x) - c(x)$ o erro. Definimos então, se $e(x) = e_0 + \cdots + e_{n-1}x^{n-1}$,

$$\begin{aligned} &M = \{i \mid e_i \neq 0\}, \\ &r = \#M, \\ &\ell(x) = \prod_{i \in M} \left(1 - \beta^i x\right), \\ &s(x) = \left(\sum_{i \in M} e_i \beta^i x\right) \left(\sum_{j \in M \setminus \{i\}} \left(1 - \beta^j x\right)\right). \end{aligned}$$

M é o conjunto das posições onde os erros ocorrem e r é o número de erros, que estamos supondo ser no máximo t. $\ell(x)$ é chamado o *polinômio localizador de erros*. De fato, $i \in M$ se, e somente se, $\ell\left(\beta^{-i}\right) = 0$, logo conhecendo $\ell(x)$ saberemos onde os erros estão. O polinômio $s(x)$ servirá para nos dizer qual foi o erro. De fato, se $i \in M$ temos

$$s\left(\beta^{-i}\right) = e_i \sum_{j \in M \setminus \{i\}} \left(1 - \beta^j \beta^{-i}\right) = -e_i \ell'\left(\beta^{-i}\right)$$

onde ℓ' é a derivada de ℓ. Desta equação podemos calcular e_i a partir de ℓ e s. Resumindo se conhecemos ℓ e s saberemos onde os erros ocorreram e quais foram os erros. O algoritmo consistirá então de se obter $\ell(x)$ e $s(x)$ somente a partir de $a(x)$. Se pudermos fazer isso então obtemos o processo de correção como foi feito acima.

A observação crucial é a seguinte (onde trabalhos com séries formais, ver apêndice):

$$\begin{aligned} \frac{s(x)}{\ell(x)} &= \sum_{i \in M} \frac{e_i \beta^i x}{1 - \beta^i x} = \sum_{i \in M} e_i \sum_{j=1}^{\infty} \left(\beta^i x\right)^j \\ &= \sum_{j=1}^{\infty} \left(\sum_{i \in M} e_i \beta^{ij}\right) x^j = \sum_{j=1}^{\infty} e\left(\beta^j\right) x^j. \end{aligned} \tag{$*$}$$

Por outro lado, $e\left(\beta^j\right) = a\left(\beta^j\right) - c\left(\beta^j\right) = a\left(\beta^j\right)$ para $j = 1, \ldots, \delta - 1$. Logo conhecemos os valores $e\left(\beta^j\right)$ para $1 \leq j \leq 2t$ a partir de $a(x)$ somente.

O ponto crucial agora é que, por hipótese, $r \leq t$ e como o $\mathrm{gr}(\ell), \mathrm{gr}(s) \leq r$ temos $\mathrm{gr}(\ell), \mathrm{gr}(s) \leq t$.

Seja $f(x) = \sum_{j=1}^{2t} a\left(\beta^j\right) x^j$, a equação $(*)$ se reescreve como

$$\frac{s(x)}{\ell(x)} \equiv f(x) \ \left(\mathrm{mod}\, x^{2t+1}\right). \qquad (*)$$

Como $f(x)$ é conhecido, isso nos permite determine ℓ e s. De fato,

$$s(x) - \ell(x) f(x) \equiv 0 \ \left(\mathrm{mod}\, x^{2t+1}\right),$$

como $\mathrm{mdc}(\ell, s) = 1$ e $\ell(0) = 1$, isso segue do resultado do Apêndice 5.A, no final deste capítulo.

Para mais informações sobre códigos cíclicos e códigos BCH vide [50].

5.4 Relacionado Códigos e Geometria Algébrica: Códigos MDS

O objetivo aqui é relacionar os códigos MDS (C é MDS se C é um $[n,d]$-código com $w(C) = n - d + 1$) com certos conjuntos definidos por propriedades geométricas em espaços projetivos sobre corpos finitos.

Definição 5.4.1 Uma *transformação projetiva* $f : \mathbb{P}^n \to \mathbb{P}^n$ é por definição a transformação induzida a partir de uma transformação linear

$$A : \mathbb{F}_q^{n+1} \to \mathbb{F}_q^{n+1}$$

invertível, isto é, $\det A \neq 0$. Isto é,

$$f((x_0 : \ldots : x_n)) = \left(\sum_{j=0}^{n} a_{0j} x_j : \ldots : \sum_{j=0}^{n} a_{nj} x_j\right), \quad \det\left(a_{ij}\right) \neq 0.$$

Definição 5.4.2 Um conjunto $K \subset \mathbb{P}^n$, $n \geq 2$ é chamado um *arco* se $\#K > n$ e K não contiver $n+1$ pontos contidos num mesmo hiperplano.

Exemplo 5.4.1 Um exemplo de arco é o conjunto, em $\mathbb{P}^n$, $n \leq q$, dado por:

$$K_n = \left\{ \left(1 : \lambda : \ldots : \lambda^{n-1}\right) \ \middle| \ \lambda \in \mathbb{F}_q \right\} \cup \{(0 : \ldots : 0 : 1)\}.$$

Definição 5.4.3 O arco K_n, dado no exemplo acima, diz-se uma *curva normal racional*.

Observação 5.4.1 $\#K_n = q + 1$.

Pela Proposição 5.1.1 (p. 80) se $H = \left(b_{ij}\right)$, $i = 1, \ldots, n-d$, $j = 1, \ldots, n$, é a matriz de controle de um $[n, d]$-código MDS, então qualquer menor $(n-d) \times (n-d)$ de H tem determinante não nulo, isso significa que podemos obter um arco $K = \left\{ \left(h_{1j} : \ldots : h_{n-d,j}\right) \mid j = 1, \ldots, n \right\}$ em $\mathbb{P}^{n-d-1}$. Reciprocamente, dado um arco K em $\mathbb{P}^m$ com $\#K = n$, podemos construir um código MDS em $\mathbb{F}_q^n$ de dimensão $n - m - 1$. Daí, a relação entre arcos e códigos MDS.

Vamos agora estudar mais cuidadosamente os arcos de $\mathbb{P}^n$.

Definição 5.4.4 Diremos que um arco é *completo* se não for subconjunto próprio de outro arco. Da mesma forma, diremos que um arco $K \subset \mathbb{P}^n$ é *maximal* se não houver nenhum arco em $\mathbb{P}^n$ com cardinalidade maior que $\#K$. A cardinalidade de um arco maximal será denotada por $m(n, q)$.

Começaremos tratando o caso do plano, isto é, $n = 2$.

Teorema 5.4.1 (Bose)

$$m(2, q) = \begin{cases} q+1 & \textit{se} \quad q \textit{ é ímpar}, \\ q+2 & \textit{se} \quad q \textit{ é par}. \end{cases}$$

Demonstração: Seja K um arco e $k = \#K$. As retas ℓ de $\mathbb{P}^2$ contam K em 0, 1 ou 2 pontos. Se $\#(\ell \cap K) = 1$ dizemos que ℓ é uma *unissecante* a K e se $\#(\ell \cap K) = 2$ dizemos que ℓ é uma *bissecante* a K.

Seja $P \in K$ e $t(P)$ o número de unissecantes a K que contém P. As bissecantes a K contendo P são em número de $k-1$, uma para cada $Q \in K \setminus \{P\}$. Como há $q+1$ retas passando por P concluímos que $t(P) = t = q + 2 - k$.

Como $t(P)$ foi definido como a cardinalidade de um conjunto, temos $t(P) \geq 0$, logo $k \leq q+2$. Vamos mostrar que $k \leq q+1$ se q é ímpar.

Suponha q ímpar e $k = q+2$ então $k = 0$ e logo $t(P) = 0$, para todo $P \in K$, o que significa que não há nenhuma unissecante a K. Seja $Q \in \mathbb{P}^2 \setminus K$ e m o número de retas passando por Q que intersectam K. Cada uma dessas m retas então contém exatamente dois pontos de K e esses pontos são distintos para retas distintas. Logo $k = 2m$, assim $q = 2(m-1)$ é par, absurdo.

Provamos então que

$$m(2, q) \leq \begin{cases} q+1 & \text{se} \quad q \text{ é ímpar}, \\ q+2 & \text{se} \quad q \text{ é par}. \end{cases}$$

Se q é ímpar, $\#K_2 = q+1$, logo $m(2, q) = q+1$.

Se q é par, $K_2 \cup \{(0:1:0)\}$ é um arco, como se verifica facilmente e logo $m(2, q) = q+2$. □

Notemos que K_2 é dado pelo conjunto dos pontos $(x_0 : x_1 : x_2)$ satisfazendo $x_2x_0 = x_1^2$. Um conjunto de pontos C satisfazendo uma equação $f(x_0, x_1, x_2) = 0$ onde $f \in \mathbb{F}_q[x_0, x_1, x_2]$ é um polinômio homogêneo de grau 2, irredutível sobre $\overline{\mathbb{F}}_q$ é chamado uma *cônica*. Como f tem grau 2 podemos ver que uma reta corta C no máximo em 2 pontos (ver Seção 5.5) logo toda cônica é um arco. Pode-se mostrar também que toda cônica tem $q+1$ pontos e temos:

Teorema 5.4.2 (Segre) *Se q é ímpar, todo arco maximal é uma cônica.*

Não provaremos este teorema, ver [38, Teorema 8.1.3, p. 164].

Se q é par e C é uma cônica, existe um único ponto P de $\mathbb{P}^2 \setminus C$ tal que $C \cup \{P\}$ é um arco, este ponto é dito o *núcleo de C*. Porém, o análogo ao Teorema de Segre não vale em geral, para $q \geq 8$ existem arcos maximais em $\mathbb{P}^2$ que não são da forma $C \cup \{P\}$ com C uma cônica e P seu núcleo. (Ver [38]).

Para classificar os arcos de $\mathbb{P}^2$ podemos nos restringir aos arcos completos. Esse problema ainda está em aberto, mas temos alguns resultados parciais concernentes as possíveis cardinalidades de arcos completos.

Proposição 5.4.1 *Se K é um arco completo de cardinalidade k, então*

$$\frac{k(k-1)}{2} \geq \frac{q^2+q+1}{q+1}.$$

Demonstração: Considere o conjunto de bissecantes a K, como uma bissecante está determinada pelos dois pontos de K que ela corta, K tem $k(k-1)/2$ bissecantes. Cada bissecante tem $q+1$ pontos, logo se $\#\mathbb{P}^2 > (q+1)\frac{k(k-1)}{2}$ existe $P \in \mathbb{P}^2$ que não está em nenhuma bissecante de K, logo $K \cup \{P\}$ é um arco e K não é completo. Como $\#\mathbb{P}^2 = q^2+q+1$, a proposição segue. □

Muito mais difícil é uma cota superior para a cardinalidade de um arco completo não maximal.

Teorema 5.4.3 *Se K um arco completo não maximal.*

(i) Se q é par, $\#K \leq q - \sqrt{q} + 1$.

(ii) Se q é ímpar, $\#K \leq q - \frac{\sqrt{q}}{4} + \frac{7}{4}$.

(iii) Se q é primo, $\#K \leq \frac{44q}{45} + 2$.

Os itens *(i)* e *(ii)* são devidos a Segre, ele provou-os relacionando, por um argumento engenhoso, a cardinalidade de K e o número de pontos racionais numa curva algébrica sobre um corpo finito e conclui o resultado da hipótese de Riemann para Corpos Finitos, principal teorema desta dissertação, os detalhes

do argumento de Segre podem ser visto em [38]. Thas, em [77], deu uma prova elementar do item *(i)*. O item *(iii)* foi provado por J.F. Voloch ([84]) utilizando-se dos resultados mais finos que a hipótese de Riemann que foram obtidos em [74].

Por outro lado conhecem-se arcos completos não maximais K satisfazendo

$$\#K = \left\lfloor \frac{q+\sqrt{q}}{2} \right\rfloor \quad \text{e} \quad \#K \leq q^{1-\frac{1}{10}}$$

(ver [76] e [83], onde outros exemplos também são dados). E também com $\#K = q - \sqrt{q} + 1$ se q é um quadrado (ver [19]).

E o caso $n \geq 3$? Vamos estuda-lo reduzindo-o ao caso $n = 2$. Seja $\mathfrak{V} \subset \mathbb{P}^n$ um subespaço de dimensão $n-3$ e $\mathfrak{W} \subset \mathbb{P}^n$ um subespaço de dimensão 2 tal que $\mathfrak{V} \cap \mathfrak{W} = \emptyset$. Definimos

$$\pi : \mathbb{P}^n \setminus \mathfrak{V} \to \mathfrak{W},$$

chamada a *projeção* sobre $\mathfrak{W}$ ao longo de $\mathfrak{V}$, da seguinte maneira. Dado $P \in \mathbb{P}^n \setminus \mathfrak{V}$ existe um único subespaço $\mathfrak{V}_P$ de dimensão $n-2$ contendo $\mathfrak{V}$ e P. Temos ainda que $\mathfrak{V}_P \cap \mathfrak{W}$ consiste de um único ponto e é esse ponto que chamamos $\pi(P)$.

Então $\mathfrak{W}$, como tem dimensão 2, pode ser identificado com $\mathbb{P}^2$. Seja $K \subset \mathbb{P}^n$ um arco e $P_1, \ldots, P_{n-2} \in K$, defina $\mathfrak{V}$ como o menor subespaço contendo $P_1, \ldots, P_{n-2}$ e escolha $\mathfrak{W}$ de dimensão 2 com $\mathfrak{V} \cap \mathfrak{W} = \emptyset$. Vê-se facilmente que $\pi(K \setminus \{P_1, \ldots, P_{n-2}\})$ é um arco em $\mathfrak{W} = \mathbb{P}^2$. Essa construção permitiu Thas provar o seguinte teorema:

Teorema 5.4.4 (Thas) *Suponha q ímpar, $q > (4n-5)^2$. Então:*

(i) $m(n,q) = q+1$.

(ii) Se $K \subset \mathbb{P}^n$ é um arco maximal então $K = f(K_n)$ onde f é uma transformação projetiva.

(iii) Se K é um arco completo não maximal, então $\#K \leq q - \frac{\sqrt{q}}{4} + \frac{n-1}{4}$.

A prova completa deste teorema pode ser vista em [77]. A ideia é usar projeções variando os pontos $P_1, \ldots, P_{n-2}$ como acima e usar os teoremas mencionados acima para o caso plano. No caso em que além de $q > (4n-5)^2$, q ímpar, q for primo, então podemos melhor o item *(iii)* do teorema para $\#K \leq \frac{44q}{45} + n + 2$ usando o item *(iii)* do Teorema 5.4.3.

Conjectura.

$$m(n,q) = \begin{cases} q+1 & \text{se} \quad 3 \leq n \leq q, \\ n+1 & \text{se} \quad n > q. \end{cases}$$

Além dos casos cobertos pelo item *(i)* do Teorema 5.4.4 essa conjectura foi provada apenas para $i = 3,4,5$, $q \geq n+1$ e $q \leq 11$, $n \leq q$, ver [50]. Sabe-se que em geral $m(n,q) \leq q+n-4$, ver [50]. Mais recentemente, em 2012, esta conjectura foi demonstrada S. Ball [5], no caso em que o número q é primo mas continua aberta em geral.

5.5 Códigos de Goppa

Neste capítulo descreveremos duas classes de códigos que chamaremos de códigos de Goppa. Essas duas classes serão englobadas em uma classe mais ampla na próxima seção. Esses códigos tem uma excelente performance.

5.5.1 Primeira classe

Seja $g(x) \in \mathbb{F}_{q^m}[x]$, mônico de grau t e $L = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\} \subset \mathbb{F}_{q^m}$, $g(\gamma_i) \neq 0$. Definimos o *código de Goppa* $C(L,g) \subset \mathbb{F}_q^n$ como o conjunto

$$\left\{ (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n \;\middle|\; \sum_{i=0}^{n-1} \frac{c_i}{x-\gamma_i} \equiv 0 \pmod{g(x)} \right\}.$$

A condição $\sum_{i=0}^{n-1} \frac{c_i}{x-\gamma_i} \equiv 0 \pmod{g(x)}$ significa que ao escrevermos a função racional do lado direito $\frac{a(x)}{b(x)}$, $a, b \in \mathbb{F}_{q^m}[x]$ teremos $\operatorname{mdc}(a(x), b(x)) = 1$ e $a(x)$ é divisível por $g(x)$.

Teorema 5.5.1

$$\dim C(L,g) \geq n - mt, \quad w(C(L,g)) \geq t+1.$$

Demonstração: Temos que:

$$\frac{1}{x-\gamma_i} \equiv \frac{-1}{g(\gamma_i)} \left(\frac{g(x) - g(\gamma_i)}{x-\gamma_i} \right) \pmod{g(x)},$$

logo $(c_0, \ldots, c_{n-1}) \in C(L,g)$ se, e somente se,

$$\sum_{i=0}^{n-1} c_i \frac{g(x) - g(\gamma_i)}{g(\gamma_i)(x-\gamma_i)} \equiv 0 \pmod{g(x)}, \quad i = 0, \ldots, n-1.$$

Por outro lado, $G_i(x) = \frac{g(x)-g(\gamma_i)}{g(\gamma_i)(x-\gamma_i)}$ é um polinômio de grau $t-1$, que podemos escrever como

$$G_i(x) = \sum_{j=0}^{t-1} g_{ij} x^j, \quad g_{ij} \in \mathbb{F}_{q^m}.$$

Logo, em particular, $\sum_{i=0}^{n-1} c_i G_i(x)$ é um polinômio de grau $\leq t-1$ e como $g(x)$ tem grau t, se $g(x)$ divide $\sum_{i=0}^{n-1} c_i G_i(x)$ então $\sum_{i=0}^{n-1} c_i G_i(x) = 0$, logo $(c_0, \ldots, c_{n-1}) \in C(L, g)$ se, e somente se,

$$\sum_{i=0}^{n-1} c_i g_{ij} = 0, \quad j = 0, \ldots, t-1. \tag{$*$}$$

$\mathbb{F}_{q^m}$ é um espaço m-dimensional sobre $\mathbb{F}_q$, logo tem uma base $\alpha_1, \ldots, \alpha_m$. Podemos então escrever

$$g_{ij} = \sum_{k=1}^{m} \lambda_{ijk} \alpha_k, \quad \lambda_{ijk} \in \mathbb{F}_q.$$

As equações $(*)$ se tornam então:

$$\sum_{i=0}^{n} c_i \lambda_{ijk} = 0, \quad j = 0, \ldots, t-1, \ k = 1, \ldots, m. \tag{$**$}$$

Isso mostra que $\dim C(L, g) \geq n - mt$. Escolhendo-se um subconjunto maximal linearmente independente das equações $(**)$ podemos construir uma matriz de controle para $C(L, g)$, mas não precisamos disto aqui.

Para mostrar a estimativa do peso seja $c = (c_0, \ldots, c_{n-1}) \in C(L, g)$ e $M = \{i \mid c_i \neq 0\}$, então

$$\sum_{i=0}^{n-1} \frac{c_i}{x - \gamma_i} = \sum_{i \in M} c_i \frac{\prod_{j \in M \setminus \{i\}} (x - \gamma_j)}{\prod_{i \in M} (x - \gamma_i)}.$$

O numerador desta expressão tem que ser divisível por $g(x)$, mas o grau do numerador é no máximo $\#M - 1$, logo $\#M - 1 \geq t$ ou $\#M \geq t + 1$. Porém $\#M = |c|$, logo $w(C(L, g)) \geq t + 1$, como queríamos demonstrar. □

A ideia da demonstração de que o peso de $C(L, g)$ é pelo menos $t + 1$ pode ser refinada para mostrar que existe uma sequência de códigos de Goppa tão perto quanto se queira da cota de Gilbert-Varshamov (Teorema 5.2.2, p. 83).

Teorema 5.5.2 *Existe uma sequência de códigos de Goppa sobre $\mathbb{F}_q$ que atinge assintoticamente a cota de Gilbert-Varshamov.*

DEMONSTRAÇÃO: Fixe $n = q^m, t, w$ e ponha $L = \mathbb{F}_{q^m}$. Vamos tentar construir $C(L, g)$ com peso $\geq w$ e g irredutível de grau t.

Se $c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ é tal que $|c| = j < w$ então, como na prova do Teorema 5.5.1, $g(x)$ deve dividir um polinômio de grau $j-1$. Como o polinômio de grau $j-1$ tem no máximo $\left\lfloor \frac{j-1}{t} \right\rfloor$ divisores de grau t, devemos excluir $\left\lfloor \frac{j-1}{t} \right\rfloor$ polinômios para cada $c \in \mathbb{F}_q^n$ com $|c| = j$. Temos então que excluir

$$\sum_{j=1}^{w-1} \left\lfloor \frac{j-1}{t} \right\rfloor (q-1)^j \binom{n}{j}$$

polinômios. Porém (ver Seção 5.2)

$$\sum_{j=1}^{w-1} \left\lfloor \frac{j-1}{t} \right\rfloor (q-1)^j \binom{n}{j} \leq \frac{w}{t} V_q(n, w-1).$$

Se provarmos que

$$\#\left\{ g(x) \in \mathbb{F}_{q^m}[x] \;\middle|\; \operatorname{gr}(g(x)) \leq t,\ g \text{ é irredutível} \right\} = f(t)$$

é tal que $f(t) > \frac{w}{t} V_q(n, w-1)$, então tal código existirá. Pode-se provar (ver [80]) que

$$f(t) > \frac{1}{t} q^{mt} \left(1 - q^{-\frac{1}{2mt}+1}\right).$$

Basta então exigir que

$$q^{mt} \left(1 - q^{-\frac{1}{2mt}+1}\right) > w V_q(n, w-1).$$

Se $w = \lfloor \delta n \rfloor$ e n é grande isso valerá se $\lim_{n\to\infty} \frac{mt}{n} > H_q(\delta)$. Mas $\dim C(L, g) \geq n - mt$, logo $\frac{\dim C(L,g)}{n} = 1 - \frac{mt}{n}$. Podemos então escolher t tal que $H_q(\delta) < \frac{mt}{n} < H_q(\delta) + \varepsilon$ e teremos que

$$\lim_{n\to\infty} C(L, g) \geq 1 - H_q(\delta) - \varepsilon$$

e $C(L, g)$ está próximo da cota de Gilbert-Varshamov. □

Códigos de Goppa têm também um algoritmo de decodificação similar ao dos códigos BCH.

Sejam $L = \{\gamma_0, \ldots, \gamma_{n-1}\}$ e $g \in \mathbb{F}_{q^m}[x]$, mônico de grau t, e $C = C(L, g) \subset \mathbb{F}_q^n$. Seja $r = (r_0, \ldots, r_{n-1})$ a mensagem recebida e $c = (c_0, \ldots, c_{n-1})$ a mensagem enviada, suponha que $|c - r| \leq t/2$. Seja $(e_0, \ldots, e_{n-1}) = r - c$. Definimos:

$$\begin{aligned} M &= \{i \mid e_i \neq 0\}, \\ e &= \#M, \\ \ell(x) &= \prod_{i \in M} (x - \gamma_i), \\ s(x) &= \sum_{i \in M} e_i \prod_{j \in M \setminus \{i\}} (x - \gamma_j). \end{aligned}$$

Exatamente como no caso dos códigos BCH o nosso problema é calcular ℓ e s conhecendo apenas r.

Seja

$$S(x) = \sum_{i=0}^{n-1} r_i \frac{-1}{g(\gamma_i)} \frac{g(x) - g(\gamma_i)}{x - \gamma_i}$$

então

$$S(x) \equiv \sum_{i=0}^{n-1} \frac{r_i}{x - \gamma_i} \equiv \sum_{i=0}^{n-1} \frac{e_i}{x - \gamma_i} \pmod{g(x)}.$$

Temos então:

$$\begin{aligned} S(x)\ell(x) &\equiv \sum_{i=0}^{n-1} \frac{e_i}{x - \gamma_i} \prod_{j \in M} (x - \gamma_j) \\ &\equiv \sum_{i=0}^{n-1} e_i \prod_{j \in M \setminus \{i\}} (x - \gamma_j) \\ &\equiv s(x) \pmod{g(x)}. \end{aligned}$$

$S(x)$ é conhecido, $g(x)$ também e temos que achar ℓ e s de grau $< t/2$ tais que

$$S(x)\ell(x) \equiv s(x) \pmod{g(x)}$$

e lembramos que o grau de $g(x)$ é t. Isso é uma generalização do problema tratado no caso dos códigos BCH onde tínhamos $g(x) = x^{2n+1}$. A solução neste caso é uma generalização direta do que fizemos anteriormente.

5.5.2 Segunda classe

Definimos

$$\mathfrak{V}_m = \{g \in \mathbb{F}_q[x, y] \mid \operatorname{gr}(g) \leq m\}.$$

$\mathfrak{V}_m$ é um espaço vetorial sobre $\mathbb{F}_q$ de dimensão $\binom{m+2}{2}$. Definimos também $\phi_m : \mathfrak{V}_m \to \mathbb{F}_q^N$ por

$$\phi_m(g) = (g(P_1), \ldots, g(P_N)).$$

O *código de Goppa* $C_m(f)$ é definido então como a imagem de ϕ_m.

Para analisar os códigos $C_m(f)$ vamos assumir de agora em diante que $m < N/d$.

Teorema 5.5.3 *Suponha $m < N/d$. Então:*

$$\dim C_m(f) = \begin{cases} \binom{m+2}{2} & se \quad m < d, \\ md - \dfrac{d(d-3)}{2} & se \quad m \geq d, \end{cases}$$

e $w(C_m(f)) \geq N - md$.

Demonstração: Vamos primeiro calcular $\dim C_m(f)$. Vejamos então qual é o núcleo de ϕ_m. Se $\phi_m(f) = 0$ então $f = g = 0$ tem N soluções, como estamos assumindo que $md < N$, isso implica, pelo Teorema de Bézout (vide p. 72) que f divide g. Se $m < d$ então $g = 0$ e logo ϕ_m é injetivo para $m < d$, o que prova a fórmula enunciada neste caso. Para $m \geq d$ o núcleo de ϕ_m é o conjunto $\{fh \mid h \in \mathbb{F}_q[x,y],\ \mathrm{gr}(h) \leq m-d\}$, que é isomorfo (via $fh \mapsto h$) a $\mathfrak{V}_{m-d}$ logo a dimensão do núcleo de ϕ_m é $\binom{m-d+2}{2}$, assim, para $m \geq d$,

$$\dim C_m(f) = \binom{m+2}{2} - \binom{m-d+2}{2} = md - \frac{d(d-3)}{2}.$$

Seja agora $c \in C_m(f)$ com $|c| = r$ e seja $g \in V_m$ tal que $\phi_m(g) = c$. Então g tem $N - r$ zeros em comum com f. Se $c \neq 0$ devemos ter que f não divide g, logo pelo Teorema de Bézout temos $N - r \leq md$ ou $r \geq N - md$, o que prova o teorema. □

Pelo teorema, para d e m fixos a dimensão de $C_m(f)$ não depende de N (se $N > md$), então para achar o melhor código entre os $C_m(f)$ é suficiente achar f tal que N é máximo.

5.6 Códigos de Goppa Associado a Divisores

Nesta seção daremos a construção de uma família de códigos construída por Goppa [25], relacionada com curvas sobre corpos finitos. Essa relação tem-se provada ser bastante importante para as duas áreas.

Sejam $P_1, \ldots, P_n \in \mathfrak{C}\left(\mathbb{F}_q\right)$ pontos distintos e G um divisor efetivo de $\mathfrak{C}$. Suporemos também que nenhum dos P_i está no suporte de G. Por fim, tomamos $D = \sum_{i=1}^{n} P_i$.

Definimos os códigos de Goppa $C(D,G), C'(D,G) \subset \mathbb{F}_q^n$ da seguinte maneira:

$$\begin{aligned}
&C(D,G) = \text{imagem de } \phi_{D,G},\\
&\phi_{D,G} : L(G) \to \mathbb{F}_q^n, \quad \phi_{D,G}(f) = (f(P_1), \ldots, f(P_n)),\\
&C'(D,G) = \text{imagem de } \psi_{D,G},\\
&\psi_{D,G} : \Omega'(-G+D) \to \mathbb{F}_q^n,\\
&\psi_{D,G}(\omega) = (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)),
\end{aligned}$$

em que

$$\Omega'(-G+D) = \{\omega \text{ diferencial de Weil em } \mathfrak{C} \mid \operatorname{div}(\omega) - G + D \geq 0\}$$

e $\mathrm{res}_P(\omega)$ denota o resíduo do diferencial de Weil ω em P.

O código $C(D,G)$ generaliza os códigos $C_m(f)$ da seção anterior. $C_m(f) = C(D,G)$ onde $\mathfrak{C}$ é a curva plana $f = 0$, $P_1, \ldots, P_n$ são os pontos afins de $\mathfrak{C}$ e $G = mH$ onde H é o divisor cortado pela reta no infinito em $\mathfrak{C}$.

O código $C'(D,G)$ generaliza os códigos $C(L,g)$ no caso particular em que $L \subset \mathbb{F}_q$ e $g \in \mathbb{F}_q[x]$. Neste caso $\mathfrak{C} = \mathbb{P}^1$, $L = \{P_1, \ldots, P_n\}$ e G é o divisor de zeros de g. Existe uma forma de generalizar a definição dos $C'(D,G)$ de modo a englobar todos os $C(L,g)$.

Teorema 5.6.1 (Goppa [25]) *(i) Se* $\operatorname{gr}(G) < n$, *então*

$$\begin{aligned}
&\dim C(D,G) = \ell(G) \geq \operatorname{gr}(G) + 1 - g,\\
&w(C(D,G)) \geq n - \operatorname{gr}(G).
\end{aligned}$$

(ii) Se $2g - 2 < \operatorname{gr}(G) < n + g - 1$, *então*

$$\begin{aligned}
&\dim C'(D,G) = \dim \Omega'(-G+D) \geq n - \operatorname{gr}(G) + g - 1,\\
&w\left(C'(D,G)\right) \geq \operatorname{gr}(G) - 2g + 2.
\end{aligned}$$

Se $f_1, \ldots, f_r$, $r = \ell(G)$ é uma base de $L(G)$ então a matriz $\left(f_i\left(P_j\right)\right)$ é uma matriz geradora para $C(L,G)$. Similarmente, se $\omega_1, \ldots, \omega_s$ é uma base de $\Omega'(D-G)$ então a matriz $\left(\mathrm{res}_{P_j}(\omega_i)\right)$ gera $C'(L,G)$. Quanto ao controle lembremos a fórmula dos resíduos:

$$\sum_{P \in \mathfrak{C}} \mathrm{res}_P(\omega) = 0,$$

para qualquer diferencial ω em $\mathfrak{C}$. Então temos que se $f \in L(G)$ e $\omega \in \Omega'(D-G)$:

$$0 = \sum_{P \in \mathfrak{C}} \operatorname{res}_P(f\omega) = \sum_{i=1}^{n} f(P_i) \operatorname{res}_{P_i}(\omega). \qquad (*)$$

Quando $2g-2 < \operatorname{gr}(G) < n$, contando as dimensões verifica-se rapidamente que as equações $(*)$ para $f = f_1, \ldots, f_r$ nos dá uma matriz de controle para $C'(D,G)$, isto é, a matriz de controle de $C'(D,G)$ é a matriz geradora de $C(D,G)$. Podemos ver também por $(*)$ que a matriz geradora de $C(D,G)$ é a matriz de controle de $C'(D,G)$.

Proposição 5.6.1 *Nas hipóteses do Teorema 5.6.1, se $g = 0$, os códigos $C(D,G)$ e $C'(D,G)$ são MDS.*

Demonstração: Temos, para $C(D,G)$ que, pelo Teorema 5.6.1,

$$\begin{aligned} w(C(D,G)) &\geq n - \operatorname{gr}(G) \\ &= n - (\operatorname{gr}(G)+1) + 1 \\ &\geq n - \dim C(D,G) + 1. \end{aligned}$$

Pelo Cota de Singleton (Corolário 5.1.1, p. 81), temos também

$$w(C(D,G)) \leq n - \dim C(D,G) + 1.$$

Logo a vale a igualdade e $C(D,G)$ é MDS.

A prova para $C'(D,G)$ é análoga. □

Observemos (ver [20]) que quando $g = 1$ (curva elíptica), podemos definir uma lei de grupo abeliano $\oplus$ em $\mathfrak{C}$, fixando um ponto arbitrário $0 \in \mathfrak{C}$, da seguinte maneira. Pomos $P \oplus Q = R$ se R é o único ponto de $\mathfrak{C}$ tal que $P + Q - R - 0 = \operatorname{div}(f)$ para algum ponto fecho f em $\mathfrak{C}$.

Se $G = \sum_{i=1}^{m} n_i Q_i$, definimos

$$P_G = n_1 Q_1 \oplus \cdots \oplus n_m Q_m,$$

então temos:

Teorema 5.6.2 (Driencourt-Michon [16]) *Nas hipóteses do Teorema 5.6.1, se $g = 1$, então:*

$$\dim C(D,G) = \operatorname{gr}(G) \quad e \quad \dim C'(D,G) = n - \operatorname{gr}(G).$$

Se existem $i_1, \ldots, i_r$, $r = \operatorname{gr}(G)$ e $i_1, \ldots, i_r \in \{1, \ldots, r\}$ tais que $P_G = P_{i_1} \oplus \cdots \oplus P_{i_r}$, então

$$w(C(D,G)) = n - \operatorname{gr}(G) \quad e \quad w\left(C'(D,G)\right) = \operatorname{gr}(G).$$

Caso contrário, $C(D,G)$ e $C'(D,G)$ são MDS.

Driencourt e Michon deram também no caso $g = 1$ um eficiente algoritmo de decodificação.

Suponhamos agora que $\{P_1, \ldots, P_n\} = \mathfrak{C}(\mathbb{F}_q)$. Temos então, pelo Teorema 5.6.1, que

$$\frac{\dim C + w(C)}{n} \geq 1 - \frac{g-1}{n},$$

para $C = C(D, G)$ ou $C'(D, G)$. Uma maneira de se obter bons códigos é maximizar este número. Para isso temos que maximizar n/g para $\mathbb{F}_q$ fixo. Pelo Limitante de Hasse-Weil temos

$$\frac{n}{g} \leq \frac{q+1}{g} + 2q^{1/2}.$$

Esse resultado nem sempre é o melhor possível, especialmente para g grande. De fato, Drinfeld e Vladut ([17]) mostraram que

$$\frac{n}{g} \leq q^{1/2} - 1 + f(g) \quad \text{onde} \quad f(g) \to 0 \quad \text{quando} \quad g \to \infty.$$

Por outro lado, Ihara ([40]) e Tsfasman-Vladut-Zink ([79]) construíram uma sequência de curvas para cada q quadrado, $\sqrt{q} \geq 7$, tendo $n/g \to q^{1/2} - 1$. Esses códigos são assintoticamente os melhores conhecidos, estando inclusive acima da cota de Gilbert-Varshamov. Outros autores mostraram também que estes exemplos podem ser calculados eficientemente [81].

Apêndice 5.A Séries Formais

Definição 5.A.1 Seja F um corpo. O *corpo de séries formais* $F((x))$ é o conjunto das expressões

$$\sum_{i=n}^{\infty} a_i x^i, \quad a_i \in F, \quad n \in \mathbb{Z}.$$

Note que as expressões da definição são apenas formais, não discutiremos nenhuma noção de convergência.

Definição 5.A.2 Em $F((x))$ definimos a soma e o produto de dois elementos pondo

$$\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i,$$
$$\left(\sum a_i x^i\right)\left(\sum b_i x^i\right) = \sum c_i x^i,$$

onde $c_k = \sum_{i+j=k} a_i b_j$.

Proposição 5.A.1 *Com as operações definidas acima $F((x))$ é um corpo.*

Definição 5.A.3 Se $\varphi = \sum_{i=n}^{\infty} a_i x^i \in F((x))$ e $a_n \neq 0$, dizemos que n é a *ordem de* φ, denotado por $\operatorname{ord}(\varphi)$. Se $\operatorname{ord}(\varphi) \geq 0$ dizemos que φ é *inteiro*.

Proposição 5.A.2 $\operatorname{ord}(\varphi\psi) = \operatorname{ord}(\varphi) + \operatorname{ord}(\psi)$.

Observação 5.6.1 Claramente $F[x] \subset F((x))$. Como $F((x))$ é um corpo, temos então $F(x) \subset F((x))$.

Proposição 5.A.3

$$\frac{1}{1-ax} = \sum_{i=0}^{\infty} a^i x^i.$$

Demonstração:

$$\left(\sum_{i=0}^{\infty} a^i x^i\right)(1-ax) = \sum_{i=0}^{\infty} a^i x^i - \sum_{i=1}^{\infty} a^i x^i = 1.$$

□

Definição 5.A.4 Se $\varphi \in F((x))$ e $\operatorname{ord}(\varphi) \geq n > 0$, escrevemos $\varphi \equiv 0 \pmod{x^n}$.

Teorema 5.A.1 (Padé) *Seja $\varphi \in F((x))$, $\operatorname{ord}\varphi \geq 0$ e N um inteiro positivo. Então existem $a, b \in F[x]$, $b \neq 0$ de grau no máximo N satisfazendo*

$$\operatorname{ord}(a - b\varphi) \geq 2N + 1.$$

Se a e b forem tais polinômios que além disso satisfaçam $\operatorname{mdc}(a,b) = 1$ e $b(0) = 1$ então eles são únicos com esta propriedade.

Demonstração: Escrevamos $\varphi = \sum_{i=0}^{\infty} \varphi_i x^i$, $a = \sum_{i=0}^{N} a_i x^i$ e $b = \sum_{i=0}^{N} b_i x^i$, onde os coeficientes a_i e b_i ainda estão por serem determinados. Considere o sistema de equações, equivalente a $\operatorname{ord}(a - b\varphi) \geq 2N + 1$,

$$\sum_{i+j=k} b_i \varphi_i = a_k, \quad k = 0, \ldots, N, \tag{I}$$

$$\sum_{i+j=k} b_i \varphi_i = 0, \quad k = N+1, \ldots, 2N. \tag{II}$$

O sistema (II) é um sistema de N equações mas $N+1$ incógnitas b_i, logo tem uma solução não nula $(b_0, \ldots, b_N)$ e $a_0, \ldots, a_N$ estão determinados por (I). Isso prova a primeira parte do Teorema. Quanto a unicidade sejam $a, b, \overline{a}, \overline{b}$ soluções satisfazendo todas as propriedades. Temos então que

$$\operatorname{ord}\left(a\overline{b} - b\overline{a}\right) = \operatorname{ord}\left(\overline{b}(a - b\varphi) - b\left(\overline{a} - \overline{b}\varphi\right)\right) \geq 2N + 1,$$

como o grau de $a\overline{b} - b\overline{a}$ é no máximo $2N$ isso implica $a\overline{b} - b\overline{a} = 0$ ou $a/b = \overline{a}/\overline{b}$. Como $\mathrm{mdc}\,(a,b) = \mathrm{mdc}\,(\overline{a},\overline{b}) = 1$, isso implica $a = \lambda\overline{a}$, $b = \lambda\overline{b}$, $\lambda \in F$. Como $b\,(0) = \overline{b}\,(0) = 1$, temos $\lambda = 1$ logo $a = \overline{a}$ e $b = \overline{b}$, o que prova o teorema. □

Daremos agora um algoritmo para se obter os polinômios a e b do teorema que é mais rápido que resolver o sistema linear (II). Primeiramente, façamos a observação importante que a e b dependem somente de $\varphi_0, \ldots, \varphi_{2N}$. Podemos então supor que

$$\varphi = \varphi_0 + \varphi_1 x + \cdots + \varphi_{2N} x^{2N}.$$

Definiremos polinômios $r_{-1}, r_0, \ldots, q_1, q_2, \ldots$, pelo algoritmo de Euclides, pondo

$$r_{-1} = x^{2N+1}, \quad r_0 = \varphi,$$
$$r_{i-2} = q_i r_{i-1} + r_i, \quad \mathrm{gr}\,(r_i) < \mathrm{gr}\,(r_{i-1})\,.$$

Isto é, r_i é o resto da divisão de r_{i-2} por r_{i-1}.

Definimos também os polinômios t_i, $i = -1, 0, 1, \ldots$, por

$$t_{-1} = 0, \quad t_0 = 1,$$
$$t_i = t_{i-2} - q_i t_{i-1}, \quad i \geq 1.$$

Lema 5.A.1

$$t_i \varphi \equiv r_i \ \left(\mathrm{mod}\, x^{2N+1}\right), \quad i = -1, 0, 1, \ldots.$$

Demonstração: A afirmação é óbvia para $i = -1, 0$. Supondo por indução que vale para $i-1$ e $i-2$, temos

$$t_i\varphi - r_i = \left(t_{i-2} - q_i t_{i-1}\right)\varphi - \left(r_{i-2} - q_i r_{i-1}\right)$$
$$\left(t_{i-2}\varphi - r_{i-2}\right) - q_i\left(t_{i-1}\varphi - r_{i-1}\right) \equiv 0 \ \left(\mathrm{mod}\, x^{2N+1}\right),$$

logo a afirmação verdadeira. □

Notemos agora que como os graus dos r_i decrescem e r_{-1} tem grau $2N+1$, temos que $r_i = 0$, $i > 2N$. Seja n o maior inteiro tal que $r_n \neq 0$.

Lema 5.A.2 *Existe um único j, $0 \leq j \leq n$, tal que*

$$\mathrm{gr}\left(t_j\right), \mathrm{gr}\left(r_j\right) \leq N.$$

Demonstração: Pode-se provar que $\mathrm{gr}\,(r_{i-1}) + \mathrm{gr}\,(t_i) = 2N+1$, $0 \leq i \leq n+1$.

Como $\mathrm{gr}\,(r_i)$ decresce de $2N$ a 0 para $0 \leq i \leq n$ existe um único j, $0 \leq j \leq n$, tal que

$$\mathrm{gr}\left(r_{j-1}\right) > N \quad \text{e} \quad \mathrm{gr}\left(r_j\right) \leq N,$$

então $\operatorname{gr}(t_j) = 2N + 1 - \operatorname{gr}(r_{j-1}) \leq N$. Isso mostra a existência do j como anunciado no lema. Para provar a unicidade, notemos que se $\operatorname{gr}(r_i), \operatorname{gr}(t_i) \leq N$ então

$$\operatorname{gr}(r_{i-1}) = 2N + 1 - \operatorname{gr}(t_i) > N,$$

logo $i = j$. Com isso, o lema está provado. □

O algoritmo para achar a e b no Teorema 5.A.1 então é o seguinte. Calculamos os q_i e r_i sucessivamente pelo algoritmo da divisão até que achamos j como na prova do lema, então calculamos os t_i pela sua definição recursiva e temos $a = r_j$ e $b = t_j$. O Lema 5.A.2 garante que $\operatorname{gr}(a), \operatorname{gr}(b) \leq N$ e o Lema 5.A.1 garante que $\operatorname{ord}(a - b\varphi) \geq 2N + 1$.

Os polinômios a e b do Teorema 5.A.1 são chamados de *aproximantes de Padé de ordem N de* φ. Quando $b(0) \neq 0$, a/b é chamado um quociente parcial (da fração contínua) de φ.

Referências Bibliográficas

[1] Abdón, M.; Carvalho, C.; Panario, D. *Curvas sobre Cuerpos Finitos*. ICTP-CIMPA School: AGRA III (Aritmética, Grupos y Analisis III), 9-20 de Julho de 2018, Cordoba, Argentina.

[2] Artin, E. *Algebraic Numbers and Algebraic Functions*. Gordon and Breach, Science Publishers, New York, 1967.

[3] Artin, E. Quadratische Körper im Gebiete der höheren Kongruenzen. II. Analytischer Teil. *Mathematische Zeitschrift 19 (1)* (1924), 207–246.

[4] Audin, M. *Correspondance entre Henri Cartan et André Weil (1928-1991)*. Documents mathématiques, Soc. Math. France, 2011.

[5] Ball, S. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *Journal European Math. Soc. 14* (2012), 733–748.

[6] Berlekamp, E.R. *Algebraic Coding Theory*. McGraw-Hill, New York, 1968.

[7] Berlekamp, E.R. Goppa codes. *IEEE Transactions on Information Theory 19* (1973), 590–592.

[8] Bohr, H.; Landau, E. Ein Satz über Dirichletsche Reihen mit Anwendung auf die ζ-Funktion und die L-Funktionen. *Rendiconti del Circolo Matematico di Palermo 37 (1)* (1914), 269–272.

[9] Bombieri, E. Counting points on curves over finite fields. *Séminaire Bourbaki 15* (1972-1973), 234–241.

[10] Bombieri, E. Hilbert's 8^{th} problem an analogue. *In Mathematical developments arising from Hilbert's problems, F. Browder, ed., Proc. Sym. Pure Math. vol. 28, AMS* (1976), 269–274.

[11] Bombieri, E. Problems of the millennium: The Riemann hypothesis. *Clay Mathematics Institute – Millennium Problems* (`https://www.claymath.org/sites/default/files/official_problem_description.pdf`).

[12] Borges, H.; Tengan, E. *Álgebra Comutativa em Quatro Movimentos.* Coleção Projeto Euclides, IMPA, Rio de Janeiro, 2015.

[13] Conrey, J.B. More than two fifths of the zeros of the Riemann zeta function are on the critical line. *J. Reine Angew. Math. 399* (1989), 1–16.

[14] Deligne, P. La conjecture de Weil: I. *Publications Mathématiques de l'IHÉS 43* (1974), 273–307.

[15] Deligne, P. La conjecture de Weil: II. *Publications Mathématiques de l'IHÉS 52* (1980), 137–252.

[16] Driencourt, Y.; Michon,J.F. Elliptic codes over fields of characteristic 2. *Journal of Pure and Applied Algebra 45* (1987), 15–39.

[17] Drinfeld, V.G.; Vladut, S.G. Sobre o número de pontos de uma curva algébrica (em russo). *Func. Anal. and Appl. 17* (1983), 68–69.

[18] Euler, L. De summis serierum reciprocarum. *Commentarii academiae scientiarum Petropolitanae 7* (1740), 123–134.

[19] Fischer, J.C.; Hirschfeld, J.W.P.; Thas,J.A. Complete arcs in planes of square order. *Annals of Discrete Mathematics 30* (1986), 243–250.

[20] Fulton, W. *Algebraic Curves. An Introduction to Algebraic Geometry*. Addison-Wesley, 1989.

[21] Fulton, W. *Intersection Theory.* EMG 3. Springer-Verlag, 1984.

[22] Garcia, A.; Lequain, Y. *Elementos de Álgebra.* 6ª edição, Projeto Euclides, IMPA, Rio de Janeiro, 2015.

[23] Goppa, V.D. *Geometry and Codes*. Mathematics and its applications, 24, Kluwer Academic Publishers, Dordrecht-Boston-London, 1988.

[24] Goppa, V.D. Uma nova classe de códigos corretores lineares (em russo). *Problemy Peredachi Informatsii 6* (1970), 24–30.

[25] Goppa, V.D. Algebraico-Geometric codes. *Math. URSS Izvestiya 21* (1983), 15–91.

[26] Griffiths, P.A.; Harris, J.E. *Principles of Algebraic Geometry*. Wiley (Interscience), 1978.

[27] Grothendieck, A. Formule de Lefschetz et rationalité des fonctions *L*. *Séminaire Bourbaki 9* (1965), 41–55.

[28] Hansen, T.; Mullen, G.L. Primitive polynomials over finite fields. *Math. Comp. 59* (1992), 639–643.

[29] Hardy, G.H. Sur les Zéros de la Fonction $\zeta(s)$ de Riemann. *C. R. Acad. Sci. Paris 158* (1914), 1012–1014.

[30] Hardy, G.H.; Littlewood, J.E. The zeros of Riemann's zeta-function on the critical line. *Math. Z. 10 (3-4)* (1921), 283–317.

[31] Hartshorne, R. *Algebraic Geometry*. Graduate texts in mathematics: 52. Springer Science & Business Media, 1977.

[32] Hasse, H. Ein Summierungsverfahren für die Riemannsche ζ-Reihe. *Mathematische Zeitschrift 32* (1930), 458–464.

[33] Hasse, H. Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichen Konstantenkörper. *J. Reine Angew. Math. 172* (1934), 37–54.

[34] Hasse, H. Über die Riemannsche Vermuntung in Funktionenkörper. *in Congresso Internacional de Matemática, Oslo* (1936), 183–206.

[35] Hindry, M. *Arithmétique - Primalité et codes, Théorie analytique des nombres, Equations diophantiennes, Courbes elliptiques.* Collection Tableau Noir, Calvage et Mounet, Paris, 2008.

[36] Hindry, M. La preuve par André Weil de l'hypothèse de Riemann pour une courbe sur un corps fini. *Henri Cartan & André Weil, mathématiciens du XXe siècle* (2012), 63–98.

[37] Hindry, M.; Silverman, J. *Diophantine Geometry: An Introduction*. Graduate texts in mathematics: 201. Springer Science & Business Media, 2000.

[38] Hirschfeld, J.W.P. *Projective Geometries over Finite Fields*. Clarendon Press, Oxford, 1979.

[39] Hirschfeld, J.W.P.; Korchmáros, G.; Torres, F. *Algebraic curves over finite fields*. Princeton Univ. Press, Princeton and Oxford, 2008.

[40] Ihara, Y. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Tokio, Ser. IA, Math. 28* (1981), 721–724.

[41] Ivić, A. *The Riemann Zeta Function*. John Wiley and Sons, New York, 1985.

[42] Katz, N. An overview of Deligne's proof of the Riemann hypothesis for varietes over finite fields. *Proceedings of Symposia in Pure Mathematics 28* (1976), 275–305.

[43] Lachaud, G. Les codes géométriques de Goppa. *Asterisque 133-134* (1983), 139–207.

[44] Lachaud, G. Les codes géométriques de Goppa. *Séminaire Bourbaki 27* (1984-1985), 189–207.

[45] Le Brigand, D.; Risler, J.J. Algorithme de Brill-Noether et codes de Goppa. *Bulletin de la Société Mathématique de France 116* (1988), 231–253.

[46] Levinson, N. More than one-third of the zeros of Riemann's zeta function are on $\sigma = 1/2$. *Adv. Math. 13 (4)* (1974), 383–436.

[47] Lidl, R.; Niederreiter, H. *Finite Fields*. Encyclopedia of Mathematics and its Applications, v. 20, Cambridge University Press, 1997.

[48] Lint, J.H. *Introduction to Coding Theory*. 3rd, Graduate Texts in Mathematics, 86, Springer-Verlag, Berlin-Heidelberg, 1999.

[49] Lint, J.H.; Geer, G. *Introduction to coding theory and algebraic geometry*. DMV Seminar, Vol. 12, Birkhäuser, Basel-Boston-Berlin, 1988.

[50] MacWilliams, F.J.; Sloane, N.J.A. *The Theory of Error Correcting Codes*. North Holland, Amsterdam, 1977.

[51] Manin, Yu. I. What is the maximum number of points on a curve over $\mathbb{F}_2$? *J. Fac. Sci. Tokio, Ser. IA, Math. 28* (1981), 715–720.

[52] McEliece, R.J. *The Theory of Information and Coding*. Encyclopedia of Mathematics and its Applications, 86, Cambridge University Press, 2004.

[53] Milne, J.S. The Riemann hypothesis over finite fields: From weil to the present day. *arXiv.org Submitted on 2 Sep 2015* (`https://arxiv.org/abs/1509.00797`).

[54] Moreno, C. *Algebraic curves over finite fields*. Cambridge University Press, Edinburgh and Cambridge, 1991.

[55] Mullen, G.; Mummert, C. *Finite Fields and Applications*. Student Mathematical Library, v. 41, American Mathematical Society, Providence, 2007.

[56] Plücker, J. *Theorie der algebraischen Curven*. Bei Adolph Marcus, Bonn, 1839.

[57] Polcino Milies, C. *Corpos Finitos*. Notas de Aula, UFABC, Santo André, 2017.

[58] Ribenboim, P. *The Theory of Classical Valuations*. Springer Monographs in Mathematics, Springer, 1999.

[59] Ribenobim, P. *The Riemann-Roch Theorem for Algebraic Curves.* Queen's University, Kingston, 1965.

[60] Riemann, B. Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsberichte der Berliner Akademie* (Novembro de 1859).

[61] Roquette, P. History of valuation theory – Part I. *In Valuation Theory and Its Applications, Fields Institute communications, American Mathematical Soc 1* (2002), 291–356.

[62] Schmidt, F.K. Analytische Zahlentheorie in Körpern der Charakteristik p. *Mathematische Zeitschrift 33* (1931), 1–32.

[63] Schoenfeld, L. Sharper bounds for the Chebyshev functions $b(x)$ and $\psi(x)$. II. *Mathematics of Computation 30 (134)* (1976), 337–360.

[64] Selberg, A. On the zeros of Riemann's zeta-function. *SKR. Norske Vid. Akad. Oslo I. 10* (1942), 1–59.

[65] Serre, J.P. *Algèbre Locale - Multiplicités*. Lecture Notes in Mathematics: 11. Springer Verlag, 1965.

[66] Serre, J.P. *Lectures on $N_X(p)$.* Research Notes in Mathematics, 11, CRC Press Taylor & Francis Group, 2012.

[67] Serre, J.P. Sur le nombre des points rationneles d'une courbe algébrique sur un corps fini. *C.R. Acad. Sci. Paris t. 296, Serie I* (1983), 397–402.

[68] Serre, J.P. La vie et l'œuvre d'André Weil. *Enseign. Math. 45 (1-2)* (1999), 5–16.

[69] Shafarevich, I.R. *Basic Algebraic Geometry 1.* 3rd, Springer-Verlag, New York, 2013.

[70] Silverman, J.H. *The Arithmetic of Elliptic Curves*. Second Edition, Graduate Texts in Mathematics 106, Springer-Verlag, New York, 2009.

[71] Sloane, N.J.A. Error correcting codes and cryptography. *In the Mathematical Gardner, D.A. Klarner, ed., Wadsworth, Belmont* (1981), 346–382.

[72] Stepanov, S. A. *Arithmetic of Algebraic Curves*. Translated from Russian by Irene Aleksanova, Consultants Bureau, New York, 1994.

[73] Stepanov, S. A. *Codes on Algebraic Curves.* Springer Science & Business Media, 2012.

[74] Stöhr, K.O.; Voloch, J.F. Weierstrass points and curves over finite fields. *Proc. Lon. Math. Soc. (3)52* (1986), 1–19.

[75] Stichtenoth, H. *Algebraic Function Fields and Codes.* Graduate Texts in Mathematics, 254, Springer Science & Business Media, 2009.

[76] Szönyi, T. Small complete arcs in Galois Planes. *Geom. Dedicata 18* (1985), 161–172.

[77] Thas, J.A. Normal rational curves and *k*-arcs in Galois Spaces. *Rend. di Mat. (3-4) 1* (1968), 331–334.

[78] Thompson, T.M. *From Error-Correcting Codes Through Sphere Packings to Simple Groups*. Mathematical Association of America, 1983.

[79] Tsfasfman, M.A.; Vladut, S.G.; Zink, I. Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound. *Math. Nach. 109* (1982), 21–28.

[80] Van Lint, J.H. *Introduction to Coding Theory*. Springer, New York, 1982.

[81] Vladut, S.G.; Manin, Yu. I. Linear codes and modular curves. *Journal of Soviet Mathematics 30* (1985), 2611–2643.

[82] Voloch, J.F. *Códigos Corretores de Erros.* 16º Colóquio Brasileiro de Matemática, Rio de Janeiro, 1987.

[83] Voloch, J.F. On the completeness of certain plane arcs. *Europ J. of Combinatorics 8* (1987), 453–456.

[84] Voloch, J.F. Arcs in projective planes over prime fields. *J. of Geometry 38* (1990), 198–200.

[85] Voloch, J.F. On the completeness of certain plane arcs-II. *Europ J. of Combinatorics 11* (1990), 491–496.

[86] Von Koch, N.G. Sur la distribution des nombres premiers. *Acta Mathematica 24* (1901), 158–182.

[87] Walker, J.L. *Codes and Curves*. Student Mathematical Library, v.7, American Mathematical Society, Institute for Advanced Study, 2000.

[88] Weil, A. *Foundations of Algebraic Geometry*. American Mathematical Society Colloquium Publications, 29, Providence, R.I.: American Mathematical Society, 1946.

[89] Weil, A. *Souvenirs d'Apprentissage*. Vita Mathematica, 6. Birkhäuser Verlag, Basel, 1991.

[90] Weil, A. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Hermann, Paris, 1948.

[91] Weil, A. *Variétés abéliennes et courbes algébriques*. Hermann, Paris, 1948.

[92] Weil, A. Sur les fonctions algébriques à corps de constantes fini. *C. R. Acad. Sci. Paris 210* (1940), 592–594.

[93] Weil, A. On the Riemann hypothesis in function fields. *Proc. Nat. Acad. Sci. U.S.A. 27* (1941), 345–347.

[94] Weil, A. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc. 55* (1949), 497–508.

[95] Weil, A. Une lettre et un extrait de lettre à Simone Weil. *In Œuvres scientifiques [1940a], Springer 1* (1979), 244–255.

Índice Remissivo

Notações

F_p	Corpo primo de F	13
$\operatorname{car} F$	Característica do corpo F	13
$\#F$	Cardinalidade do corpo F	13
$\mathbb{F}_q$	Corpo finito com q elementos	15
$\mathrm{GF}(q)$	Corpo de Galois com q elementos	15
$\mathbb{Z}/p\mathbb{Z}$	Anel dos inteiros módulo p	15
$\mathbb{F}_q^\times$	Grupo dos elementos não nulos do corpo $\mathbb{F}_q$	16
$K(M)$	O conjunto M adjuntado ao corpo K	17
$K(\theta_1, \ldots, \theta_k)$	O corpo K adjuntado aos elementos $\theta_1, \ldots, \theta_k$	17
$[L : K]$	Grau da extensão $L\|K$	17
$\mathrm{Gal}(\mathbb{F}_{q^m}\|\mathbb{F}_q)$	Grupo de Galois de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$	24
$\mathcal{O}$	Anel de valorização	26
v_p	Valorização p-ádica sobre os números racionais	27
$v_\mathfrak{p}$	Valorização associada ao lugar $\mathfrak{p}$	28
$\mathrm{gr}(\mathfrak{p})$	Grau do lugar $\mathfrak{p}$	29
$\mathrm{res}_\mathfrak{p}$	Função de classe residual em relação ao lugar $\mathfrak{p}$	29
$\mathfrak{P} = \mathfrak{P}_F$	Conjunto dos lugares de $F\|K$	30

$\mathrm{Div}(F)$	Conjunto dos divisores de $F\|K$	30
$\mathrm{div}(f)$	Divisor principal de f	31
$\mathrm{Princ}(F)$	Grupo dos divisores principais de $F\|K$	31
$\mathrm{div}_0(f)$	Divisor de zeros de f	32
$\mathrm{div}_\infty(f)$	Divisor de pólos de f	32
$L(D)$	Espaço de Riemann-Roch associado ao divisor D	32
$\|D\|$	Série linear referente ao divisor D	33
$\mathrm{gr}(D)$	Grau do divisor D	33
$\mathrm{Cl}(F)$	Grupo de classes dos divisores de $F\|K$	33
$D \sim D'$	O divisores D e D' são equivalentes	33
$[D]$	Classe de equivalência do divisor D	33
$\ell(D)$	Dimensão do divisor D	34
$\mathfrak{i}(D)$	Índice de especialidade do divisor D	36
$\mathfrak{A} = \mathfrak{A}_F$	Espaço adélico de $F\|K$	36
$\mathfrak{A}(D) = \mathfrak{A}_F(D)$	Subespaço (associado a D) do espaço adélico	37
ω	Diferencial de Weil	38
Ω_F	Módulos dos diferenciais de Weil de $F\|K$	38
$\Omega_F(D)$	Os diferenciais de Weil que se anulam em $\mathfrak{A}(D) + F$	38
$M(\omega)$	Conjunto dos divisores D tais que o diferenciais de Weil ω se anula em $\mathfrak{A}(D) + F$	39
$\mathbb{A}^n = \mathbb{A}^n(K)$	Espaço afim n-dimensional sobre K	43
$\mathfrak{a}(\mathfrak{V})$	Ideal da variedade $\mathfrak{V}$	43
$\Gamma(\mathfrak{V})$	Anel de coordenadas da variedade $\mathfrak{V}$	44
$K(\mathfrak{V})$	Corpo de funções da variedade $\mathfrak{V}$	44
$\mathcal{O}_P(\mathfrak{V})$	Anel local com corpo de frações $K(\mathfrak{V})$	45
$\mathfrak{m}_P(\mathfrak{V})$	Ideal maximal do anel local $\mathcal{O}_P(\mathfrak{V})$	45

$i(C)$	Razão de informação do código C	78
${}^tP$	Transposta da matriz P	78
$\|x\|$	Norma (de Hamming) do elemento x	78
$d(x,y)$	Distância (de Hamming) dos elementos x e y	79
$w(C)$	Peso do código C	80
$\lfloor x \rfloor$	Maior inteiro menor ou igual a x	80
$B(a,r)$	Bola de centro a e raio r	82
$A_q(n,w)$	Máximo da dimensão do código C, em que $C \subset \mathbb{F}_q^n$ e o peso de C é w	82
$V_q(n,r)$	Cardinalidade da bola $B(a,r)$	82
$\alpha_q(\delta)$	Limite superior, quando n tende a infinito e δ está entre 0 e 1 (inclusive), da razão $A_q(n, \lfloor \delta n \rfloor)/n$	85
$\mathbb{F}_q[x]$	Anel de polinômios com coeficientes no corpo $\mathbb{F}_q$	87
$\mathbb{F}_q[x]/(x^n-1)$	Quociente de $\mathbb{F}_q[x]$ pelo ideal gerado por x^n-1	87
$a \equiv b \pmod{n}$	a é congruente a b módulo n	87
(g)	Ideal gerado por g	88
$\mathcal{F}(a)$	Polinômio de Mattson-Solomon, ou transformada de Fourier discreta, em a	89
$\ell(x)$	Polinômio localizador de erros	91
$\det A$	Determinante da matriz A	92
K_n	Curva normal racional de $\mathbb{P}^n$	92
$m(n,q)$	Cardinalidade de um arco maximal de $\mathbb{P}^n$	93
$t(P)$	Número de unissecantes a K que contém o ponto P	93
$C(L,g)$	Código de Goppa de parâmetros L e g	96
$\mathfrak{V}_m$	Espaço vetorial dos polinômios g em $\mathbb{F}_q[x,y]$ tais que o grau de g é menor ou igual a m	100
$C_m(f)$	Código de Goppa de parâmetros m e f	100