João Rafael de Melo Ruiz

"A Hipótese de Riemann em característica p", ou "O Teorema de Riemann-Roch e as Conjecturas de Weil para Curvas Algébricas", ou ainda "Childish Steps"

Florianópolis

2019

João Rafael de Melo Ruiz

"A Hipótese de Riemann em característica p", ou "O Teorema de Riemann-Roch e as Conjecturas de Weil para Curvas Algébricas", ou ainda "Childish Steps"

Trabalho de Conclusão de Curso apresentado ao Curso de Matemática do Departamento de Matemática do Centro de Ciências Físicas e Matemáticas da Universidade Federal de Santa Catarina para obtenção de grau de Bacharel em Matemática

Universidade Federal de Santa Catarina

Orientador: Dr. Eduardo Tengan

Florianópolis

2019

Dedicado à P.B.

Agradecimentos

Agradeço a todos e todas que me acompanharam ao longo dessa jornada de 4 anos no curso de Matemática, tanto colegas de curso quanto amigos/as de outros cursos que já conhecia ou conheci ao longo desse passeio. Especifico vocês abaixo.

Agradeço, antes de todos, a minha família, em especial a meus pais, Roberto e Adriana, e a meus irmãos, Pedro e José. Vocês estiveram presentes não apenas durante minha formação enquanto matemático, mas durante toda a minha vida, apoiando minhas decisões e dando os necessários "puxões de orelha". Sou extremamente grato.

Obrigado ao professor Eduardo Tengan por ter me orientado não somente durante o ano de 2019, em que este trabalho foi escrito, mas também durante 2018 e até parte de 2017! Obrigado não apenas pelas explicações matemáticas, mas também pela paciência em explicar por vezes a mesma coisa repetidas vezes, até que eu a entendesse, e também pelos conselhos "carreirísticos", que estou levando profundamente em consideração agora que encaro a pergunta do que fazer depois de me formar.

Obrigado também ao professor Paulo Carvalho, meu primeiro orientador, com quem estudei em 2016 e 2017. Com você comecei a me formar enquanto pesquisador, processo esse que continuou com o Tengan e continuará, certamente, depois de eu me formar.

Meu muito obrigado a meus amigos Luiz e Mateus, que comigo constituíram *Os Três Pinduqueiros*[1]. São tantas aventuras pelas quais passamos que não consigo elencar qual seria mais icônico de nossa amizade. Talvez algum dos churrascos que organizamos. Talvez algum dos terraços em que subimos. Talvez alguma das vezes em que fomos no cartório. Talvez alguma das vezes que passamos longas conversas reclamando de disciplinas optativas.

Agradeço a meus amigos do grupo *convite*[2], Augusto e Camila. Apesar de não nos vermos mais todos os dias, como nos tempos do Ensino Fundamental e Médio (o que é uma ironia dada a pequeníssima distância entre nossas casas), sempre continuei considerando-os como amigos extremamente próximos, com quem pude (e posso) contar quando preciso desabafar sobre o curso, sobre optativas, ou simplesmente para ir passear na praia.

Agradeço a todos os membros e ex-membros do Centro Acadêmico Livre de Matemática, o CALMA. Foi nessa instituição, da qual fiz parte por dois (ou três, se contarmos 2019) anos, que comecei a compreender o significado de fazer algo por uma comunidade

[1] O nome, no caso, é uma variação d'Os Três Mosqueteiros, o mítico grupo de atuais professores que cursaram a graduação juntos, alterado para incluir nossa marca favorita de farofa, a *Pinduca*.

[2] Sim, estou escolhendo os conjuntos de pessoas a quem agradeço via grupos de WhatsApp. E sim, em itálicos são os nomes de tais grupos.

e de participar ativamente na luta por um mundo melhor, mesmo que apenas na escala local de um curso de graduação.

Agradeço ao professor Pinho, sob cuja tutoria trabalhei durante um ano no Programa de Educação Tutorial - PET MTM. Certamente, o PET foi uma das experiências mais formativas de que tive a oportunidade de participar durante esses quatro anos. Sou grato também às amizades que forjei nesse tempo, o pessoal da *Tomada do PET 2.6*. Pimenta, Carlinhos, Ben, Leandro, Yuri, Kendji, Jean, Graciani, Tiago e Gustavo, contem comigo pra bares, pra falar bobagem, pra ir encher o saco dos bolsistas atuais do PET, pra Zoar a Galera da Matemática... Enfim, tenho de certeza que estando com vocês, teremos bons momentos.

Obrigado a diversos professores e professoras do curso que me ensinaram durante a graduação, não apenas conteúdos matemáticos, mas também o espírito de curiosidade, paixão e admiração pela beleza da matemática que vocês demonstraram durante suas aulas. Rosilene, Morgado, Royer, Ivan, Virgínia, Melissa, Eliezer, Sergio e Marianna são alguns dos nomes que me vêm imediatamente à mente enquanto escrevo este parágrafo. Obrigado por me ajudarem a me tornar o bacharel(ando) em matemática que sou hoje!

Tendo falado de professores, não tenho como deixar de fora os trabalhadores e trabalhadoras, técnicos ou terceirizados, que tornam possível a existência da Universidade e que acompanharam a minha graduação, alguns desde o começo. Simone, Antônia e toda a equipe de limpeza do CFM, obrigado pelas conversas matinais na época em que eu era o primeiro a chegar no PET. Giana,Luciana e Jaqueline, pelo sempreótimo trabalho na Coordenadoria do curso de Matemática, e pelas eventuais conversas também quando eu ia pedir alguma informação. Eduardo Ulisses e Eduardo Krukoski também não podem ser esquecidos. Bruna, Mauro e todo mundo da Direção do CFM, obrigado pela ajuda e muitas vezes paciência com questões de estrutura, como emprestar projetores, fornecer autorização pra uso de sala em fim de semana, e ajudar a mobilizar o pessoal para fazer algo com relação à infra-estrutura do Labirinto. Continuemos a luta por condições dignas de trabalho e estudo! Obrigado ao Igor, Gabriel e toda a equipe técnica da BS-CFM, onde quase morei durante os últimos anos, essa fonte de conhecimento[3] onde devo ter pego emprestado pelo menos um total de 400 000 livros (sim, eu contei!). Obrigado, por fim, ao Levy, à Thamires e todos que trabalham/trabalharam na cantina do EFI, por tantas conversas ao longo desses anos.

Obrigado aos colegas de curso, tanto veteranos quanto calouros[4]. Vocês me recepcionaram e me acolheram quando eu estava chegando no curso, e tentei fazer o mesmo com quem chegou depois de mim. Sabe, sendo a Matemática uma atividade social, sou muito

[3] Mesmo que por vezes barulhenta demais para estudar.....

[4] Bom, quanto a colegas de curso que entraram comigo no bacharelado, sobreviveram apenas dois, a quem já dirigi agradecimentos acima.

feliz por ter percebido cedo em minha vida a necessidade de uma comunidade em que possamos compartilhar nossos problemas e angústias, mas também nossas alegrias, nossos êxitos, e ao longo de minha graduação fiz tudo o que estava em meu alcance para que essa comunidade não apenas sobrevivesse, mas também fosse saudável e fonte de ajuda a quem de nós precisássemos.

Agradeço ao Conselho Nacional de Desenvolvimento Científico e Tecnológico, que durante dois anos patrocinou meus estudos em Matemática com uma bolsa de Iniciação Científica.

"The introduction of the digit 0 or the group concept was general nonsense too, and mathematics was more or less stagnating for thousands of years because nobody was around to take such childish steps..."

Alexander Grothendieck

Resumo

O presente trabalho se propõe principalmente a expor, de maneira acessível, a demonstração de Enrico Bombieri da Hipótese de Riemann para curvas sobre corpos finitos ([Bombieri, 1974]). Primeiramente, são expostos alguns fatos e construções elementares da linguagem de esquemas, como a topologia de Zariski e a construção do feixe estrutural de um esquema afim. Em seguida, após um breve comentário sobre o Teorema de Riemann-Roch no contexto de esquemas, são apresentadas a função Zeta de uma curva definida sobre um corpo finito e as Conjecturas de Weil, que dizem respeito a essa função Zeta. São demonstradas duas das Conjecturas de Weil (de quatro) para curvas: a racionalidade da função Zeta, usando métodos da teoria de corpos de funções, e a Hipótese de Riemann.

Palavras-chave: Geometria Algébrica. Função Zeta. Conjecturas de Weil. Hipótese de Riemann. Corpos finitos.

Abstract

The present work aims mainly at exposing, in an accessible fashion, Enrico Bombieri's proof of the Riemann Hypothesis for curves over finite fields ([Bombieri, 1974]). We begin by presenting some elementary facts and constructions pertaining to the language of schemes, such as the Zariski topology and the construction of the structure sheaf of an affine scheme. After a quick commentary on the Riemann-Roch Theorem in the context of schemes, we present the Zeta function of a curve defined over a finite field and the Weil Conjectures, which concern this Zeta function. We prove two (of four) Weil Conjectures: the rationality of the Zeta function using techniques from the theory of function fields, and the Riemann Hypothesis.

Keywords: Algebraic Geometry. Zeta Function. Weil Conjectures. Riemann Hypothesis. Finite Fields.

Sumário

1 Introdução

Esta introdução, naturalmente, foi uma das últimas coisas a serem escritas neste trabalho. E também está sendo uma das mas difíceis. Como escrever uma introdução leve, que pode ser lida em uma tarde de primavera, como se lê um livro de ficção?[1] O que devo incluir aqui, e o que deve ser relegado ao corpo principal do texto? Escrevo pensando no público que não possui nenhum contato com a Geometria Algébrica, em quem já tem alguma familiaridade, ou escrevo algo que vai "clicar" à medida que se for avançando na leitura do texto?

Optei por fazer uma introdução para os leigos e leigas. Assim, aqui não veremos muitos detalhes das demonstrações que serão exploradas neste trabalho. Porém, tentei passar o espírito do que será feito, especialmente no capítulo 3.

Ainda, como problemas matemáticos não existem em um vácuo[2], vale a pena falar um pouco sobre a história do problema que será aqui resolvido, de onde ele veio e quais são os principais personagens em seu desenvolvimento. É esse nosso ponto de partida:

1.1 Como chegamos aqui?

Falando na História de um problema matemático, a primeira decisão que devemos tomar é: até onde vamos rastrear a ancestralidade das Conjecturas de Weil? Assim como muitas outras perguntas importantes dessa área do conhecimento, suas raízes podem ser traçadas até a Matemática grega de milhares de anos atrás (c.f. [Dieudonné, 1972]). No entanto, me parece desnecessário versar longamente sobre a história da Geometria Algébrica de maneira geral, sendo que este trabalho se ocupa de uma parte razoavelmente pequena dela (especificamente, as Conjecturas de Weil para curvas). Assim, escolhi um ponto de partida que será no mínimo familiar a todos e todas que lerem esta Introdução: a Hipótese de Riemann. Famosa por ser talvez o problema em aberto mais importante da Matemática, ela trata sobre um objeto chamado função Zeta de Riemann:

$$\zeta(s) \stackrel{\text{def}}{=} \sum_{n\geq 1} n^{-s} = \frac{1}{1} + \frac{1}{2^s} + \frac{1}{3^s} + \dots \tag{1.1}$$

Em princípio, essa função está definida para $s \in \mathbb{C}$, $\Re(s) > 1$. No entanto, é possível estendê-la analiticamente para $\mathbb{C}\backslash\{1\}$. Quando nos referimos à função Zeta de Riemann, normalmente é dessa extensão que estamos falando. Apesar do nome, quem originalmente a introduziu foi Euler, no século XVIII. E ele também provou que essa função admite uma

[1] E não seria a Matemática uma espécie de ficção?

[2] Apesar do que podem tentar nos dizer os físicos...

representação na forma de um produto infinito:

$$\zeta(s) = \prod_{p \in \mathbb{Z}\,\text{primo}} (1 - p^{-s})^{-1}. \tag{1.2}$$

Euler considerou ζ como uma função de uma variável real e, entre outras coisas, usou o fato de o produto em (1.2) divergir para $s = 1$ para dar uma prova do Teorema de Euclides (existem infinitos números primos)[3]: como o produto em (1.2) diverge para $s = 1$ (pela divergência da série Harmônica), ele não pode ser finito, donde existem infinitos primos.

Riemann, em seu artigo histórico *On the Number of Primes Less Than a Given Magnitude* [Riemann, 1859], considerou-a com argumentos complexos s no semiplano $\Re(s) > 1$. Nesse artigo, provou que ζ satisfaz uma equação funcional envolvendo a função Γ, e também prova que é possível expressar a quantidade de números primos menores do que um número dado em termos dos zeros da função ζ.

Visando generalizar a função Zeta de Riemann, para entender melhor o comportamento de anéis de inteiros em extensões finitas de $\mathbb{Q}$, Richard Dedekind introduziu, em seu suplemento ao livro de Dirichlet *Vorlesungen Über Zahlentheorie* [Dirichlet, 1863], uma função Zeta para esse contexto. Sejam K uma extensão finita de $\mathbb{Q}$ e $\mathcal{O}_K$ seu anel de inteiros (isto é, o fecho integral de $\mathbb{Z}$ em K). A função Zeta de Dedekind é definida como

$$\zeta(K, s) \stackrel{\text{def}}{=} \sum_{I \subseteq \mathcal{O}_K\,\text{ideal}} (N_{K/\mathbb{Q}}(I))^{-s}, \tag{1.3}$$

em que a soma percorre todos os ideais de $\mathcal{O}_K$ e $N_{K/\mathbb{Q}}(I)$ é a norma de I, definida como $|\mathcal{O}_K/I|$, de maneira que tomando $K = \mathbb{Q}$, $\zeta(\mathbb{Q}, s) = \zeta(s)$.

Para provar que $\zeta(s)$ possui uma representação como produto de Euler, é necessário apenas o fato que todo número admite uma fatoração em números primos. Ou, em termos de ideais, todo ideal admite uma fatoração em ideais primos (note que isso aponta na direção de que poderemos considerar funções Zeta de outros domínios de Dedekind) e os anéis quociente são finitos. Assim, como $\mathcal{O}_K$ é domínio de Dedekind, prova-se que

$$\zeta(K, s) = \prod_{\substack{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K \\ \mathfrak{p} \neq (0)}} (1 - (N\mathfrak{p})^{-s})^{-1}. \tag{1.4}$$

Agora damos um salto no tempo para frente, e chegamos em 1921: nesse ano Emil Artin recebeu seu doutorado em Matemática com uma tese ([Artin, 1924]) que provava vários resultados sobre anéis de inteiros de extensões finitas de $\mathbb{Q}$ para corpos de funções sobre corpos finitos (isto é, extensões finitas de corpos da forma $\mathbb{F}_q(t)$). Especificamente, Artin considerou extensões da forma $K = \mathbb{F}_q(t, v)$, em que $v^2 = P(t)$, para um polinômio

[3] Exemplificando um *overkill*: usar a divergência da função Zeta para provar que existem infinitos números primos!

separável P, de forma que o "anel de inteiros" de K (isto é, o fecho integral de $\mathbb{F}_q[t]$ em K) é $\mathbb{F}_q[t, v]$. Alguns resultados e conceitos importantes que Artin importou para esse contexto são: fundamentação da teoria de ideais nesses anéis, fatos sobre o grupo de unidades e sobre a função Zeta desses corpos, finitude do grupo de classe e existência de gênero.

Ainda, Artin calculou exemplos explícitos de funções Zeta para vários corpos de funções, e verificou nesses casos a validade da Hipótese de Riemann.

Damos novamente outro salto no tempo, em direção a 1941, ano de publicação da resposta positiva da Hipótese de Riemann para corpos de funções ([Weil, 1941]). Tendo sido preso duas vezes no passado recente (uma vez na Finlândia sob acusação de espionagem soviética e outra na França por se recusar a prestar o serviço militar obrigatório), André Weil usou esse tempo "livre" para pensar sobre a Hipótese de Riemann[4]. O artigo *On the Riemann Hypothesis in Function Fields* foi publicado pouco tempo depois de Weil conseguir fugir da França para os Estados Unidos, no meio da confusão causada pela ocupação alemã da França.

Nessa época, Weil estava também trabalhando em uma generalização da Geometria Algébrica para abarcar qualquer caso de corpo base (não apenas $\mathbb{Q}$ e $\mathbb{C}$), e já sabia que a Hipótese de Riemann para funções Zeta de corpos de funções estava intimamente relacionada com a contagem de pontos de curvas sobre corpos finitos (c.f. apêndice A deste trabalho). Assim, Weil publicou em 1949 o artigo *Numbers of Solutions of Equations in Finite Fields* ([Weil et al., 1949]), em que é definida a função Zeta de uma variedade algébrica sobre um corpo $\mathbb{F}_q$ e são enunciadas as conjecturas que nomeiam este trabalho. Dou a palavra a Weil, em [Weil et al., 1949]:

(. . .) This, and other examples which we cannot discuss here, seem to lend some support to the following conjectural statements, which are known to be true for curves, but which I have not so far been able to prove for varieties of higher dimension.

Let V be a variety without singular points, of dimension n, defined over a finite field k with q elements. Let N_ν be the number of rational points on V defined over the extension k_ν of k of degreee ν. Then we have

$$\sum_1^\infty N_\nu U^{\nu-1} = \frac{d}{dU} \log Z(U),$$

where $Z(U)$ is a rational function in U, satisfying a functional equation

$$Z\left(\frac{1}{q^n U}\right) = \pm q^{n\chi/2} U^\chi Z(U),$$

[4] Ironicamente, a prisão francesa em que Weil esteve preso, na cidade de Rouen, chamava-se *"Bonne Nouvelle"* ("boas notícias", em francês). Não consegui encontrar nenhum relato da opinião de Weil sobre essa ironia do destino, porém tendo lido um pouco sobre sua vida, acredito que ele levou-a com bom-humor.

with χ equal to the Euler-Poincaré characteristic of V (intersection number of the diagonal with itself on the product $V \times V$).

Furthermore, we have:

$$Z(U) = \frac{P_1(U)P_3(U)\dots P_{2n-1}(U)}{P_0(U)P_2(U)\dots P_{2n}(U)},$$

with $P_0(U) = 1 - U$, $P_{2n}(U) = 1 - q^n U$, and, for $1 \leq h \leq 2n-1$,

$$P_h(U) = \prod_{i=1}^{B_h}(1 - \alpha_{h_i}U)$$

where the α_{h_i} are algebraic integers of absolute value $q^{h/2}$.

Finally, let us call the degrees B_h of the polynomials $P_h(U)$ the Betti numbers of the variety V; the Euler-Poincaré characteristic χ is then expressed by the usual formula $\chi = \sum_h (-1)^h B_h$. (...)

André Weil propôs essas conjecturas em 1949. No entanto, para tomar emprestadas as palavras de Pierre Cartier em seu texto *Un pays dont on ne connaîtrait que le nom* ([Cartier, 2000]), ele enxergou a Terra Prometida, porém não podia atravessar o Mar Vermelho com os pés secos, diferente de Moisés. Ainda, ele não dispunha de uma embarcação adequada para navegar através desse Mar. Era necessário, como o próprio Weil sabia, construir uma teoria de cohomologia adequada para a Geometria Algébrica sobre corpos finitos, que tivesse propriedades parecidas com as cohomologias singular e de de Rham.

Começou-se então a jornada através do Jardim das Hespérides, cujas maçãs, de acordo com Pierre Cartier no mesmo texto, eram as Conjecturas de Weil.

O personagem principal desta parte de nossa história é um ponto fora da curva em vários sentidos: o matemático franco-alemão (posteriormente apátrida) Alexander Grothendieck. Talvez sua biografia seja até mais interessante que sua Matemática, e as duas se envolvem de maneira íntima. Grothendieck, assim como outros matemáticos franceses, lecionou no Brasil durante algum tempo, e no Vietnã durante a guerra contra os Estados Unidos. Passemos a suas contribuições matemáticas:

A primeira contribuição de Grothendieck que nos é relevante é a generalização de vários pontos de Álgebra Homológica, que permitiram a fundamentação abstrata da cohomologia de feixes e, depois disso, a cohomologia étale. Em seu artigo de 1957 *Sur quelques points d'algèbre homologique* ([Grothendieck, 1957]), conhecido popularmente como *Tôhoku paper*, Grothendieck define a noção de categoria abeliana, e lança as bases da (co)homologia de funtores derivados de maneira abstrata. Depois dessa contribuição, Grothendieck empreendeu o que talvez seja seu projeto mais conhecido: a refundação da Geometria Algébrica, pondo no centro do palco o conceito de anel, ao invés do de corpo ou de variedade algébrica. Obcecado com encontrar a noção mais geral possível de

"espaço"[5], ele criou a linguagem de esquemas e, com outros matemáticos, como Deligne, Dwork, Serre, Artin[6], e o próprio André Weil, criou uma teoria de cohomologia que satisfazia as propriedades necessárias. Usando a cohomologia Étale, Grothendieck, junto com outros matemáticos, provaram a racionalidade da função Zeta, sua equação funcional e a relação com os números de Betti. E então, finalmente, em 1973 ([Deligne, 1974]), Pierre Deligne provou a Hipótese de Riemann para funções Zeta de variedades algébricas, usando para isso as cohomologias Étale e l-ádica. Esse fato lhe rendeu a Medalha Fields de 1978.[7]

Esse, no entanto, não é o ponto final da nossa história. Depois de Deligne ter demonstrado a Hipótese de Riemann, houve mais um acontecimento no âmbito das Conjecturas de Weil: o matemático italiano e medalhista Fields Enrico Bombieri encontrou uma demonstração extremamente elementar da Hipótese de Riemann para curvas. Usando o maquinário do Teorema de Riemann-Roch, sua prova é tão elementar que está ao alcance, por exemplo, de um trabalho de conclusão de curso!

E, afinal, o que fez Bombieri para demonstrar um teorema tão difícil, de maneira tão elementar? É o que veremos, de maneira resumida, na próxima seção:

1.2 Que fazer?

Começamos com a seguinte

Definição 1.1. Seja C uma curva projetiva não-singular sobre $\mathbb{F}_q$. Sua função zeta é definida como a série formal em $\mathbb{C}[[t]]$ abaixo, em que $N_r \stackrel{\text{def}}{=} \#C\left(\mathbb{F}_{q^r}\right)$.

$$Z(C,t) \stackrel{\text{def}}{=} \exp\left(\sum_{r\geq 1} \frac{N_r}{r} t^r\right)$$

Para mais detalhes sobre o por quê de essa função Zeta ser a análoga geométrica da função Zeta de corpos de funções, c.f. o apêndice A deste trabalho.

Note que a derivada logarítmica que $Z(C,t)$ é uma função geradora da quantidade de pontos racionais de C em todas as extensões finitas de $\mathbb{F}_q$:

$$\frac{d}{dt}\log Z(C,t) = \sum_{r\geq 1} N_r t^{r-1}.$$

[5] O que levou Grothendieck a passar muitos anos de sua vida em busca da definição d'o que ele chamava de 'motif'.

[6] Este Artin é Michael, filho de Emil.

[7] É claro que precisei deixar muita coisa de fora – nomes como F.K. Schmidt, Helmut Hasse, van der Waerden, Severi e muitos outros fizeram parte do desenvolvimento tanto do nosso problema, de maneira específica, quanto da Geometria Algébrica e da Matemática como um todo, e não foram mencionados aqui. Os textos [Dieudonné, 1972], [Raynaud, 1999], [Weil, 1981], [Jackson, 2004] e [Roquette et al., 2003], entre muitos outros, são ótimas fontes para a história geral da Hipótese de Riemann e das conjecturas de Weil, e de anedotas que contei aqui.

É nesse sentido que, como mencionado na seção anterior, a função Zeta de curvas/corpos de funções possui um conteúdo geométrico. Assim, podendo ser definida uma função Zeta para variedades algébricas projetivas não-singulares de qualquer dimensão, temos as supracitadas

Conjecturas de Weil. Seja V uma variedade algébrica projetiva não-singular de dimensão n, definida sobre um corpo da forma $\mathbb{F}_q$. Então, são válidos os seguintes resultados sobre $Z(V,t)$:

- **Racionalidade**. $Z(V,t)$ é uma função racional, podendo ser escrita na forma

$$Z(V,t) = \frac{P_1(t)P_3(t)\dots P_{2n-1}(t)}{P_0(t)P_2(t)\dots P_{2n}(t)},$$

  com $P_0(t) = 1 - t$ e $P_{2n}(t) = 1 - q^n t$;

- **Equação funcional**. Z satisfaz a seguinte relação, em que χ é a caraterística de Euler-Poincaré de V:

$$Z\left(V, \frac{1}{q^n t}\right) = \pm q^{n\chi/2} t^{\chi} Z(V,t);$$

- **Hipótese de Riemann**. Sendo B_h o grau de cada P_h $(1 \leq h \leq 2n-1)$, podemos fatorar cada P_h como

$$P_h(t) = \prod_{i=1}^{B_h} (1 - \alpha_{h_i} t),$$

  com $|\alpha_{h_i}| = q^{1/2}$;

- **Números de Betti**. Os B_h expressam os números de Betti de V, isto é,

$$\chi = \sum_h (-1)^h B_h.$$

Não vamos aqui provar todas as quatro afirmações. Veremos apenas a racionalidade da função Zeta e a Hipótese de Riemann. Ainda, por uma questão de espaço-tempo, não será possível tratar essas duas conjecturas em toda sua generalidade, por isso trataremos apenas o caso mais simples de dimensão 1 (isto é, curvas), que nos permitirá usar técnicas de corpos de funções para demonstrar a racionalidade da função Zeta, e o Teorema de Riemann-Roch para demonstrar a Hipótese de Riemann.

A racionalidade da função Zeta, usando-se métodos de corpos de funções, consiste puramente de *straightforward computations*, então não falaremos dela nesta introdução. Vejamos a parte interessante: a Hipótese de Riemann. Como mencionado algumas vezes acima, a demonstração de Bombieri usa o

Teorema 1.2.1 (Riemann-Roch)**.** Sejam C uma curva[8] de gênero g sobre um corpo algebricamente fechado k e D um divisor em D. Então

$$l(D) - l(K - D) = \deg D + 1 - g,$$

para qualquer divisor canônico K em C.

Vamos abrir um pouco essas definições, para entender do que se trata esse resultado. Um divisor em uma curva C consiste de um conjunto finito de pontos $P \in C$, e números inteiros n_P a eles associados. Equivalentemente, um divisor é um elemento do grupo abeliano livre gerado pelos pontos de C:

$$\operatorname{Div} C \stackrel{\text{def}}{=} \bigoplus_{P \in C} \mathbb{Z} \cdot P.$$

Podemos transferir a noção de função meromorfa e ordem de zeros e polos de funções da teoria de superfícies de Riemann para as curvas algébricas. Veremos com um pouco mais de detalhes como fazer essa tradução de $\mathbb{C}$ para k no capítulo 2§3. Por hora, suponhamos poder falar em funções meromorfas em uma curva C. Usando a seguinte

Proposição 1.2.2. Se f é uma função meromorfa não-nula em uma curva C, então $\operatorname{ord}_P f = 0$ para quase todos os $P \in C$,

podemos definir o divisor de uma função meromorfa $f \neq 0$, como

$$\operatorname{div} f = (f) \stackrel{\text{def}}{=} \sum_{P \in C} \operatorname{ord}_P f \cdot P.$$

Podemos então começar a fazer perguntas sobre quais são as possíveis funções meromorfas em uma curva, em termos de divisores. Por exemplo, se $C = \mathbb{P}^1$, é razoável que se $(f) \geq 0$ (isto é, $\operatorname{ord}_P f \geq 0$ para todo $P \in C$), deva-se ter $f \in k$, por analogia com a teoria de superfícies de Riemann compactas. Ainda, podemos comparar (f) com outros divisores, não apenas o divisor zero: se $D \in \operatorname{Div} C$, definimos o k-espaço vetorial

$$L(D) \stackrel{\text{def}}{=} \{f \in k(C)^* \mid (f) + D \geq 0\} \cup \{0\}.$$

Sua dimensão é o número $l(D)$. À luz dessas definições, o que o Teorema de Riemann-Roch nos diz é que, ao fixar ordens mínimas para f em todos os pontos, não temos tantas escolhas possíveis.

Bombieri usou a seu favor esse fato, bem como o fato sobre superfícies de Riemann compactas (que também é válido para curvas) que uma função meromorfa possui a mesma

[8] É propositalmente vaga a definição de curva ao longo desta seção. No próximo capítulo, daremos à palavra "curva" um significado preciso em termos de esquemas, porém por enquanto consideremos "curva" como "aquele objeto geométrico que conhecemos da vida, e que satisfaz quaisquer condições técnicas que precisemos".

quantidade de zeros e polos, quando contados com multiplicidade. Assim, se conseguirmos garantir a existência de uma função meromorfa não-nula em C, que se anule nos pontos $\mathbb{F}_q$-racionais de C, teremos

$$|C(\mathbb{F}_q)| \leq \#\,\text{zeros de}\, f = \#\,\text{polos de}\, f \leq \text{ algo “bom”}.$$

E aí, teremos uma estimativa razoável para $|C(\mathbb{F}_q)|$. A partir dela, usando Teoria de Galois, conseguiremos uma cota inferior para $|C(\mathbb{F}_q)|$ e aí garantiremos que $|C\left(\mathbb{F}_q\right)|$ é “próximo o suficiente” da quantidade de pontos de $\mathbb{P}^1_{\mathbb{F}_q}$, isto é,

$$\left||C\left(\mathbb{F}_q\right)| - (q+1)\right| \leq cq^{1/2},$$

para uma constante real $c \geq 0$.

A partir disso, usando alguns detalhes da demonstração da racionalidade de $Z(C,t)$, podemos provar que as raízes de $Z(C,t)$ possuem valor absoluto igual a $q^{1/2}$.

1.3 As regras d’O Jogo

Como usualmente, os símbolos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ denotam os conjuntos de números naturais, inteiros, racionais, reais e complexos, respectivamente. Cabe deixar claro aqui que considero que $0 \in \mathbb{N}$ e que quem acredita no contrário está cometendo uma grave heresia. O termo “anel” é usado para significar a mesma coisa que “anel comutativo com unidade”[9]. Ainda, em um domínio, tem-se $0 \neq 1$. Assumo que morfismos não-nulos de anéis levam 1 em 1. Explicito aqui também que subscrevo ao Axioma da Escolha, que aparece aqui na forma do Lema de Zorn, garantindo, entre outras coisas, que todo anel não-nulo possui um ideal maximal, e que o funtor de seções globais é exato à esquerda. Categorias são denotadas sempre em negrito e sublinhado, **assim**: por exemplo, **Set**, **Ab** e **CRing** denotam as categorias de conjuntos, de grupos abelianos e de anéis (comutativos com unidade). Convenciono que a notação $\underset{\circ}{\subseteq}$ significa “é um subconjunto aberto de”. Se $R = \bigoplus_{n\in\mathbb{N}} R_n$ é um anel graduado e $f \in R$ é um elemento homogêneo de grau n, denotamos por $R_{(f)}$ o subanel de R_f composto pelos elementos de grau zero dessa localização. O mesmo para $R_{(\mathfrak{p})}$, em que $\mathfrak{p}$ é um ideal primo e homogêneo de R. Em nenhum caso a notação $R_{(f)}$ será ambígua a ponto de pensarmos que $R_{(f)}$ significa a localização de R pelo ideal (caso seja primo) (f). Se $z = a + b\,i \in \mathbb{C}$, $a, b \in \mathbb{R}$, a parte real de z é $\Re(z) \stackrel{\text{def}}{=} a$. Dada uma extensão de corpos $l \supseteq k$, seu grau é denotado por $[l : k]$, e seu grau de transcendência é denotado por $td_k l$. Se V é um espaço vetorial sobre um corpo k, o dual de V (funcionais lineares $V \to k$) é denotado por $V^\vee$.

[9] É por isso que este não poderia ser um trabalho sobre ciência política: pra nós, os ideais à direita são os mesmos que os ideais à esquerda!

2 Esquemas, ou "Algèbre Figurée"

L'Algèbre n'est qu'une Géometrie écrite, et la Géometrie n'est qu'une Algèbre figurée.
- Sophie Germain

O propósito deste primeiro capítulo será introduzir a linguagem básica dos esquemas. Criados por Alexander Grothendieck na década de 60, os esquemas revolucionaram a Geometria Algébrica de um jeito parecido com como a linguagem de variedades suaves revolucionou a Geometria Diferencial. Em mais de um aspecto as variedades e os esquemas são parecidos. Por exemplo, ambos

- permitem um estudo intrínseco dos objetos geométricos,
- modelando-os localmente por um objeto "mais simples", que conhecemos bem.

No caso de variedades, esse objeto é um $\mathbb{R}^n$. No caso de esquemas, esse objeto é o espectro de um anel comutativo. Vejamos em detalhes:

2.1 Zariski, ou "Um Espectro Ronda a Álgebra..."

Definição 2.1. Seja R um anel. Um ideal $\mathfrak{p} \subseteq R$ é dito ser primo se $R/\mathfrak{p}$ é um domínio. O conjunto de ideais primos de R é denotado por $\operatorname{Spec} R$. O comprimento n da maior cadeia possível de ideais primos,

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

é chamada de dimensão de Krull de R, denotada por $\dim R$.

Observação. Note que um ideal $\mathfrak{p} \subseteq R$ é primo se, e somente se, para $a, b \in R$, $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. Ainda, como todo corpo é domínio, todo ideal maximal é primo[1]. Finalmente, como todo anel $R \neq 0$ possui um ideal maximal, temos que se $R \neq 0$, $\operatorname{Spec} R \neq \emptyset$ (porém muitas vezes, nenhuma das quais neste trabalho, o "esquema vazio", $\operatorname{Spec} 0$, desempenha um importante papel na Geometria Algébrica).

O primeiro passo para geometrizarmos a Álgebra é munir $\operatorname{Spec} R$ de uma topologia, que recebe o nome de Topologia de Zariski. Seus fechados são definidos como sendo

$$V(I) \stackrel{\text{def}}{=} \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq I\},$$

para $I \subseteq R$ um ideal qualquer.

[1] Denotando-se por $\operatorname{Specm} R$ o espectro maximal de R, isto é, o conjunto de ideais maximais de R, temos que $\operatorname{Specm} R \subseteq \operatorname{Spec} R$.

Proposição 2.1.1. Os conjuntos da forma $V(I)$ definem os fechados de uma topologia em $\operatorname{Spec} R$. A interseção abitrária e união finita de fechados nessa topologia são dados pelas seguintes expressões:

$$\bigcap_{i\in I} V(J_i) = V\left(\sum_{i\in I} J_i\right) \qquad V(J_i)\cup V(J_k) = V(J_iJ_k).$$

Demonstração. Primeiro, note que tanto $\emptyset$ quanto $\operatorname{Spec} R$ são fechados: temos

$$V((1)) = \emptyset \qquad \text{e} \qquad V(0) = \operatorname{Spec} R.$$

Agora, note que se $V(I)$ e $V(J)$ são fechados, então

$$\begin{aligned}
\mathfrak{p} \in V(I)\cup V(J) &\iff \mathfrak{p}\in V(I) \text{ ou } \mathfrak{p}\in V(J)\\
&\iff \mathfrak{p}\supseteq I \text{ ou } \mathfrak{p}\supseteq J\\
&\iff \mathfrak{p}\supseteq IJ\\
&\iff \mathfrak{p}\in V(IJ)
\end{aligned}$$

A penúltima bi-implicação é uma condição equivalente a $\mathfrak{p}$ ser um ideal primo: um anel S é domínio se, e somente se, para quaisquer ideais $I, J \subseteq S$, $IJ = (0) \implies I = (0)$ ou $J = (0)$.

Por fim, temos $\bigcap\limits_{i\in I} V(J_i) = V\left(\sum\limits_{i\in I} J_i\right)$, afinal

$$\begin{aligned}
\mathfrak{p}\in\bigcap_{i\in I} V(J_i) &\iff \mathfrak{p}\in V(J_i), \text{ para todo } i\\
&\iff \mathfrak{p}\supseteq J_i, \text{ para todo } i\\
&\iff \mathfrak{p}\supseteq \sum_{i\in I} J_i\\
&\iff \mathfrak{p}\in V\left(\sum_{i\in I} J_i\right).
\end{aligned}$$

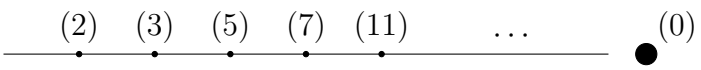
■

Agora que podemos enxergar um anel como um objeto "mais ou menos geométrico", vejamos alguns exemplos - e desenhos - para intuir melhor essa ponte entre Geometria e Álgebra.

Exemplo 2.1.2. Como $\mathbb{Z}$ é DIP, temos que $\operatorname{Spec}\mathbb{Z}$ consiste de infinitos pontos fechados, correspondendo a números primos, e um ponto "gordo", correspondendo a 0. Ainda, como a maior cadeia de ideais primos possível em $\mathbb{Z}$ é

$$(0) \subsetneq (p),$$

temos $\dim\mathbb{Z} = 1$. Visualmente, $\operatorname{Spec}\mathbb{Z}$ é uma reta discreta com um ponto denso:

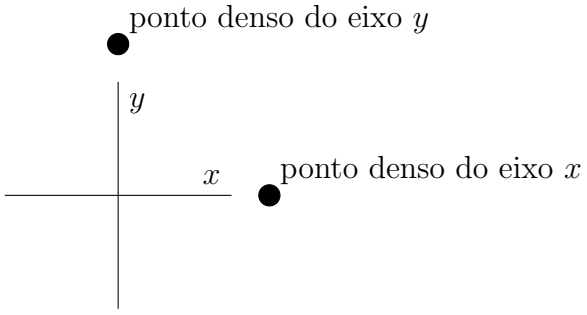


Exemplo 2.1.3. Considere o anel $R = \dfrac{\mathbb{C}[x,y]}{(xy)}$. No futuro se tornará claro que $X = \operatorname{Spec} R$ é um exemplo de esquema, e visualizaremos (não, de verdade, vamos fazer desenhos!) que ele representa a curva $xy = 0$ em $\mathbb{C}^2$, porém com mais informação do que a equação que a define consegue comportar. Por exemplo, $x^2y = 0$ define o mesmo espaço topológico, porém gostaríamos de diferenciar que o fator x está repetido nessa segunda equação.

Se $\mathfrak{p} \in X$, $0 = \overline{xy} = \overline{x}\,\overline{y} \in \mathfrak{p}$, donde $\overline{x} \in \mathfrak{p}$ ou $\overline{y} \in \mathfrak{p}$. Ou seja, temos

$$X = V((\overline{x})) \cup V((\overline{y})).$$

X é a união de dois fechados próprios, ou seja é um espaço topológico redutível. Porém esses dois fechados possuem um ponto em comum, $(\overline{x}, \overline{y})$, logo X é conexo. Pictoralmente, X consiste dos eixos coordenados em $\mathbb{C} \times \mathbb{C}$, cada um com um ponto denso $((0))$:



Assim como antes, temos $\dim R = 1$, fazendo assim sentido representar $\operatorname{Spec} R$ como a união de *retas*.

É uma boa hora para explorarmos algumas propriedades da topologia de Zariski:

Teorema 2.1.4. Seja R um anel. Então:

(a) Os conjuntos $D(h) \stackrel{\text{def}}{=} \{\mathfrak{p} \in \operatorname{Spec} R \mid h \notin \mathfrak{p}\} = \operatorname{Spec} R \backslash V((h))$, com $h \in R$, constituem uma base para a topologia de Zariski em $\operatorname{Spec} R$;

(b) Para todos $g, h \in R$, $D(h) \cap D(g) = D(hg)$;

(c) Todo morfismo de anéis $\varphi\colon R \to S$ induz uma função contínua $\operatorname{Spec}\varphi\colon \operatorname{Spec} S \to \operatorname{Spec} R$, com $(\operatorname{Spec}\varphi)(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$, de maneira que se $\varphi\colon R \to S$ e $\psi\colon S \to T$ são morfismos de anéis, então $\operatorname{Spec}\psi \circ \varphi = \operatorname{Spec}\varphi \circ \operatorname{Spec}\psi$;

(d) Se $\mathfrak{p} \in \operatorname{Spec} R$, $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$;

(e) $\operatorname{Spec} R$, com a topologia de Zariski, é um espaço topológico compacto.

Demonstração. (a) Note que como, para qualquer ideal $I \subseteq R$, temos $I = \sum_{h\in I}(h)$, é imediato que para qualquer fechado $V(I)$, temos

$$V(I) = \bigcap_{h\in I} V((h)),$$

portanto tomando os complementares, temos

$$\operatorname{Spec} R \backslash V(I) = \bigcup_{h\in I} D(h),$$

e os $D(h)$ são uma base para a topologia de Zariski.

(b) Como $(h)\cdot(g) = (hg)$, temos $V((h))\cup V((g)) = V((gh))$, e tomando complementares,

$$D(g) \cap D(h) = D(gh).$$

(c) Se $I \subseteq R$ é ideal, temos que

$$\begin{aligned} \mathfrak{p} \in (\operatorname{Spec}\varphi)^{-1}(V(I)) &\iff (\operatorname{Spec}\varphi)(\mathfrak{p}) \in V(I) \\ &\iff \varphi^{-1}(\mathfrak{p}) \supseteq I \\ &\iff \mathfrak{p} \in V((\varphi(I))). \end{aligned}$$

Portanto, como a préimagem de um fechado é fechada, $\operatorname{Spec}\varphi$ é contínua. A funtorialidade de Spec é óbvia.

(d) Como $\overline{\{\mathfrak{p}\}}$ é o menor fechado que contém $\mathfrak{p}$, e qualquer fechado contendo $\mathfrak{p}$ conterá $V(\mathfrak{p})$, é imediato que $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$.

(e) Note que se $\bigcap_{i\in I} V(J_i) = \emptyset$, temos que $V\left(\sum_{i\in I} J_i\right) = \emptyset$, o que implica que $\sum_{i\in I} J_i = (1)$ (do contrário, $\sum_{i\in I} J_i$ estaria contido em um ideal maximal $\mathfrak{m}$, que por ser primo, implicaria em $V\left(\sum_{i\in I} J_i\right) \neq \emptyset$). Portanto, existem finitos $i_1, \ldots, i_n \in I$ tais que $\bigcap_{k=i}^{n} V(J_{i_k}) = V\left(\sum_{k=1}^{n} J_{i_k}\right) = \emptyset$, isto é, da cobertura aberta $\{\operatorname{Spec} R\backslash V(J_i)\}_{i\in I}$ extraímos uma subcobertura finita $\{\operatorname{Spec} R\backslash V(J_{i_k})\}_{1\leq k\leq n}$. Portanto, $\operatorname{Spec} R$ é compacto.

■

O que o teorema anterior nos afirma é que acabamos de construir um funtor contravariante Spec: $\underline{\mathbf{CRing}}^{\mathrm{op}} \to \underline{\mathbf{Top}}$, saindo da categoria de anéis comutativos e chegando na categoria de espaços topológicos.

Da parte (d) do teorema 2.1.4, sabemos que se $\mathfrak{m} \in \operatorname{Specm} R$ (isto é, $\mathfrak{m}$ é um ideal maximal, portanto primo, de R), $\overline{\{\mathfrak{m}\}} = \{\mathfrak{m}\}$, e reciprocamente se $\overline{\{\mathfrak{m}\}} = \{\mathfrak{m}\}$, então $\mathfrak{m}$

é maximal. Os pontos de Specm R recebem o nome de "pontos fechados" de Spec R. No outro extremo, se $\overline{\{\mathfrak{p}\}} = \operatorname{Spec} R$, $\mathfrak{p}$ é dito ser um ponto genérico de Spec R. Por exemplo, se R é um domínio, (0) é um ponto genérico de Spec R.

Exemplo 2.1.5. Seja $\mathbb{A}_k^n \stackrel{\text{def}}{=} \operatorname{Spec} k[x_1, ..., x_n]$, com k um corpo. Por exemplo, consideremos $\mathbb{C}[x, y]$. Graças a um corolário do Nullstellensatz (veja abaixo) e ao fato que $\dim \mathbb{C}[x, y] = 2$, temos que $V((x-y)) = \{(x-y)\} \cup \{(x-a, y-b) \mid a, b \in \mathbb{C}, \text{ e } a-b=0\}$. Portanto, $D(x-y)$ é "o complementar da reta $x - y = 0$". De maneira mais geral, para $f \in \mathbb{C}[x, y]$, $D(f)$ é o "complementar do conjunto algébrico $f(x, y) = 0$", isto é, "o conjunto em que f nunca se anula", ou, ainda, "o domínio de $1/f$".

Teorema 2.1.6 (Um corolário do Nullstellensatz Hilberts)**.** Seja k um corpo algebricamente fechado. Então os ideais maximais de $k[x_1, \ldots, x_n]$ são da forma

$$(x_1 - a_1, \ldots, x_n - a_n),$$

com $a_i \in k$, $i = 1, \ldots, n$.

A demonstração encontra-se em [Tengan and Borges, 2015], capítulo 2§3, teorema 2.3.20 (página 65).

Como é possível depreender do exemplo acima, os abertos da topologia de Zariski são gigantes – ou melhor, seus fechados são minúsculos (em comparação com os da topologia usual, quando trabalhamos com $\mathbb{C}$). Por exemplo, no plano, os fechados próprios são pontos e curvas. Mais drasticamente, na reta (isto é, em Spec $\mathbb{C}[x]$), a topologia de Zariski coincide com a topologia cofinita.

Como vimos no exemplo acima, o complementar de $V(f)$ pode ser pensado como o domínio de $1/f$, visto como uma função $k^n \to k$. Querendo então evidenciar o papel de anéis na Geometria Algébrica, como Grothendieck fez, vemos que será necessário ter uma noção razoável de o que seria $R\left[\frac{1}{f}\right]$, para $f \in R$. Isso porque os elementos de R são pensados como funções regulares em Spec R, portanto se $1/f$ é uma função regular no complemento de $V(f)$, deveremos ter algo como "as funções regulares em $D(f)$ são exatamente $R\left[\frac{1}{f}\right]$". O que eu quero dizer com esse parágrafo é que, a partir de agora, usaremos indiscriminadamente o conceito de localização, disponível em [Atiyah and Macdonald, 1969], capítulo 3 ou, com vistas maiores ao uso na Geometria Algébrica, [Tengan and Borges, 2015], capítulo 4 e [Eisenbud, 2013], capítulo 2. Nessa linguagem, a discussão acima torna-se a seguinte

Proposição 2.1.7. Seja R um anel. Então, para $f \in R$, temos um homeomorfismo

$$D(f) \simeq \operatorname{Spec} R_f.$$

A demonstração encontra-se disponível em [Tengan and Borges, 2015], capítulo 4§3 (página 128).

2.2 As categorias LRS e SCH

Por analogia com variedades diferenciáveis ou superfícies de Riemann, é evidente que a estrutura de espaço topológico é insuficiente para termos uma noção boa de "Geometria". Assim, devemos considerar uma "estrutura funcional no espectro de um anel"[2], capítulo 1, e faremos isso por meio da identificação das "funções regulares" nesse espaço. Essa é a motivação mais elementar para (pré-)feixes. Aqui usaremos a mesma definição de [Tengan and Borges, 2015], que posteriormente pode ser generalizada no contexto da cohomologia Étale. Antes da definição, faz-se necessária uma

Observação. Seja X um espaço topológico. Os abertos de X formam um conjunto parcialmente ordenado, e como tal constituem uma categoria cujos objetos são os abertos de X e para $U, V \underset{\circ}{\subseteq} X$,

$$\mathbf{Hom}(U,V) = \begin{cases} \{U \to V\}, & U \subseteq V \\ \emptyset, & \text{caso contrário.} \end{cases}$$

Essa categoria é denotada por $\underline{\mathbf{O}}(X)$.

Definição 2.2. Seja X um espaço topológico. Um pré-feixe sobre X é um funtor contravariante saindo da categoria $\underline{\mathbf{O}}(X)$. O morfismo induzido por $U \to V$ é denotado por $\rho_{V,U}$, e sendo $\mathcal{F}$ um pré-feixe de conjuntos (isto é, $\mathcal{F}\colon \underline{\mathbf{O}}(X)^{\mathrm{op}} \to \underline{\mathbf{Set}}$), um elemento de $\mathcal{F}(U)$ é dito ser uma seção por U. Para $V \subseteq U$ e $s \in \mathcal{F}(U)$, $\rho_{U,V}(s)$ é denotado por $s\,|_V$. Uma notação comum para $\mathcal{F}(U)$ é também $\Gamma(U, \mathcal{F})$.

Intuitivamente: para um $U \underset{\circ}{\subseteq} X$ e $\mathcal{F}$ um pré-feixe sobre X, $\mathcal{F}(U)$ é "o conjunto de funções contínuas sobre U" (as aspas estão aí pois não necessariamente $\mathcal{F}(U)$ é um espaço de funções). Pré-feixes não serão muito interessantes pois eles não se comportam como estruturas funcionais o suficiente. A razão é que, quando trabalhamos com estruturas funcionais vale o chamado lema de colagem, isto é, funções contínuas/suaves definidas localmente podem ser coladas, de maneira única, a resultar numa função contínua definida globalmente. Pré-feixes não satisfazem essa propriedade: consideremos o seguinte

Exemplo 2.2.1. Seja $X = \mathbb{R}$, com a topologia usual. Podemos definir um pré-feixe em X da seguinte forma: para $U \underset{\circ}{\subseteq} \mathbb{R}$, definimos

$$\mathcal{F}(U) = \{f\colon U \to \mathbb{R} \mid f \text{ é contínua e limitada}\}.$$

Para uma inclusão de abertos $U \subseteq V$, o morfismo de restrição é a restrição do domínio. Assim, $\mathcal{F}$ é um pré-feixe. Porém funções contínuas não se colam: sejam $U_n = (-n, n)$ e $f_n \in \mathcal{F}(U_n)$ a identidade[3]. Obviamente as f_n's concordam nas interseções, porém a

[2] Para a noção de estrutura funcional, c.f. [Bredon, 2013], capítulo 2 ou [Ramanan, 2005].
[3] What a $\mathcal{F}(U_n)$ example, right?

função que elas definem em $\bigcup_{n\in\mathbb{Z}} U_n = \mathbb{R}$ é a identidade, que não é limitada. Assim, funções contínuas não se colam.

Pensando nesse problema, temos a seguinte

Definição 2.3. Um feixe sobre um espaço topológico X é um pré-feixe $\mathcal{F}$ sobre X que satisfaz o seguinte "axioma de feixe": dados $U \underset{\circ}{\subseteq} X$ e uma cobertura $\{U_i\}_{i\in I}$ aberta de U, o diagrama

$$\mathcal{F}(U) \to \prod_{i\in I} \mathcal{F}(U_i) \rightrightarrows \prod_{i,j\in I} \mathcal{F}(U_i \cap U_j)$$

é um equalizador.

Pensando em feixes como estruturas funcionais, podemos nos perguntar se é possível definir uma noção de morfismo de espaços funcionalmente estruturados via feixes. Essa definição, em princípio, usa explicitamente o fato que para $U \underset{\circ}{\subseteq} X$, $\mathcal{F}(U)$ é um conjunto de *funções*: se $f\colon (X, \mathcal{F}_X) \to (Y, \mathcal{F}_Y)$ é um morfismo de espaços funcionalmente estruturados, para $U \underset{\circ}{\subseteq} Y$ e $g \in \mathcal{F}_Y(U)$, tem-se $f^{\#}(g) = g \circ f \in \mathcal{F}_X(f^{-1}(U))$. Como não necessariamente nossos feixes são feixes de funções, precisamos de uma maneira de transitar entre feixes, isto é, uma noção de morfismo de (pré-)feixes. Ora, um pré-feixe é um funtor contravariante, portanto a única definição que faz sentido é a seguinte:

Definição 2.4. Sejam $\mathcal{F}$ e $\mathcal{G}$ dois pré-feixes sobre um espaço topológico X. Um morfismo de $\mathcal{F}$ em $\mathcal{G}$ é apenas uma transformação natural $\eta\colon \mathcal{F} \to \mathcal{G}$. Explicitamente, um morfismo de pré-feixes consiste de uma coleção de morfismos $\eta_U\colon \mathcal{F}(U) \to \mathcal{G}(U)$, compatíveis com os morfismos de restrição.

Como feixes são, em particular, pré-feixes, podemos definir morfismos de feixes como sendo morfismos de pré-feixes, e é exatamente isso que faremos. Imediatamente, vê-se que os feixes sobre um espaço topológico fixado constituem uma categoria. Ou melhor, múltiplas categorias: a de feixes de grupos abelianos sobre X, a de feixes de conjuntos sobre X, a de feixes de anéis comutativos sobre X... A categoria de feixes (resp. pré-feixes) de conjuntos sobre X é denotada por $\underline{\mathbf{Sh}}(X)$ (resp. $\underline{\mathbf{PSh}}(X)$), a categoria de feixes de grupos abelianos sobre X é denotada por $\underline{\mathbf{Ab}}(X)$, e assim por diante para outras categorias.

Exemplo 2.2.2. Sejam X e Y espaços topológicos, $f\colon X \to Y$ uma função contínua e $\mathcal{F}$ um feixe em X. Note que podemos definir um feixe $f_*\mathcal{F}$ em Y por

$$(f_*\mathcal{F})(U) \overset{\text{def}}{=} \mathcal{F}(f^{-1}(U)),$$

para $U \underset{\circ}{\subseteq} Y$. Esse feixe é chamado de *pushforward* de $\mathcal{F}$ por f. Ainda, o *pushforward* age não apenas em feixes, mas também em morfismos de feixes: afinal, dado um morfismo

$\eta\colon \mathcal{F} \to \mathcal{G}$ em $\underline{\mathbf{Sh}}(X)$, podemos definir $f_*\eta\colon f_*\mathcal{F} \to f_*\mathcal{G}$ por

$$(f_*\eta)_U \stackrel{\text{def}}{=} \eta_{f^{-1}(U)}\colon f_*\mathcal{F}(U) \to f_*\mathcal{G}(U). \tag{2.1}$$

É imediata a verificação de que $f_*\eta$ é um morfismo em $\underline{\mathbf{Sh}}(Y)$. Em outras palavras (e passando por cima de algumas verificações), o *pushforward* é um funtor $f_*\colon \underline{\mathbf{Sh}}(X) \to \underline{\mathbf{Sh}}(Y)$.

A seguir terminaremos de ver as definições referentes à teoria de feixes.

Definição 2.5. Sejam $\mathcal{F}$ um feixe sobre o espaço topológico X, e $x \in X$. Definimos o talo de $\mathcal{F}$ em x como sendo

$$\mathcal{F}_x \stackrel{\text{def}}{=} \varinjlim_{\substack{U \subseteq X \\ \circ \\ U \ni x}} \mathcal{F}(U).$$

Explicitamente, $\mathcal{F}_x$ é o conjunto de classes de equivalência da forma $[U, f]$, em que $U \subseteq X$, $f \in \mathcal{F}(U)$, $U \ni x$ e $[U, f] = [V, g]$ se, e somente se, existe uma vizinhança aberta W de x contida na interseção de U e V tal que $f\mid_W = g\mid_W$.

Ou seja, $\mathcal{F}_x$ está associado ao comportamento local de funções contínuas em torno de x. Além disso, o talo herda a estrutura do feixe, isto é, se $\mathcal{F}$ é um feixe de anéis, $\mathcal{F}_x$ é um anel e assim por diante.

Informalmente, o talo é pensado como o conjunto de germes de funções em um ponto. Vejamos um exemplo, extremamente geométrico, de um fenômeno que ocorre quando trabalhamos com feixes que são estruturas funcionais:

Exemplo 2.2.3. Seja X uma variedade diferenciável, e para $U \subseteq X$, seja

$$\mathcal{D}_X(U) \stackrel{\text{def}}{=} \{f\colon U \to \mathbb{R} \mid f \text{ é } \mathcal{C}^\infty\}.$$

Então todos os talos de $\mathcal{D}$ são anéis locais. Para ver isso, tome $x \in X$ e ponha $\mathfrak{m}_x \stackrel{\text{def}}{=} \{[U, f] \in \mathcal{D}_x \mid f(x) = 0\}$. É imediato que $\mathfrak{m}_x$ é um ideal de $\mathcal{D}_x$, e se $[U, f] \in \mathcal{D}_x \backslash \mathfrak{m}_x$, existe vizinhança V de x tal que $f(y) \neq 0$ para todo $y \in V$. Portanto, $[V, f\mid_V] \in \mathcal{D}_x^\times$ e assim $\mathcal{D}_x$ é um anel local. Note ainda que, nesse caso, o talo de $\mathcal{D}$ em x é exatamente o conjunto de germes de funções diferenciáveis em x!

Ou seja, querendo modelar o comportamento de estruturas funcionais e seus germes, é interessante considerarmos apenas os feixes cujos talos são anéis locais.

Definição 2.6. Um espaço anular (também traduzido como espaço anelado ou espaço anelar) é um espaço topológico X, munido de um feixe de anéis $\mathcal{O}_X$. Um espaço localmente anular é um espaço anular em que todos os talos são anéis locais.

Como o exemplo acima ilustra, sendo $(X, \mathcal{O}_X)$ um espaço localmente anular, o ideal maximal $\mathfrak{m}_x$ de $\mathcal{O}_{X,x}$ é pensado como sendo o ideal de germes de funções que se anulam em x. Pensando nisso, construiremos a noção de morfismo de espaços (localmente) anulares. Certamente para considerarmos um morfismo nessa categoria, é necessária uma função contínua $f\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$. Trabalhando em espaços funcionalmente estrutrados, a condição que colocaríamos seria que se $U \underset{\circ}{\subseteq} Y$ e $g \in \mathcal{O}_Y(U)$, então $f^{\#}(g) \in \mathcal{O}_X(f^{-1}(U))$. No entanto, não podemos compor um elemento de $\mathcal{O}_Y(U)$ com f (afinal, os elementos de $\mathcal{O}_Y(U)$ podem muito bem não ser funções). Para remediar essa falta, notemos que a composição com f induz um morfismo $f^{\#}_U\colon \mathcal{O}_Y(U) \to f_*\mathcal{O}_X(U)$. Ou seja, temos um morfismo de feixes $f^{\#}\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$. Podemos então concluir que a definição correta é a seguinte:

Definição 2.7. Sejam $(X, \mathcal{O}_X)$ e $(Y, \mathcal{O}_Y)$ espaços anulares. Um morfismo $(f, f^{\#})\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ consiste de:

- uma função contínua $f\colon X \to Y$;
- um morfismo de feixes $f^{\#}\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$.

O último passo na construção de uma nova categoria é definir a composição de dois morfismos de espaços anulares. Se $(f, f^{\#})\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ e $(g, g^{\#})\colon (Y, \mathcal{O}_Y) \to (Z, \mathcal{O}_Z)$ são morfismos de espaços anulares, é bastante natural que a função contínua da composição seja $g \circ f$. Porém $f^{\#}\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$ é um morfismo em $\underline{\mathbf{Sh}}(Y)$, enquanto que $g^{\#}\colon \mathcal{O}_Z \to g_*\mathcal{O}_Y$ é morfismo em $\underline{\mathbf{Sh}}(Z)$. Novamente o *pushforward* induzido por uma função contínua nos salvará: definimos então

$$(g, g^{\#}) \circ (f, f^{\#}) \overset{\text{def}}{=} (g \circ f, (g_* f^{\#}) \circ g^{\#}).$$

Como a composição de morfismo de feixes é um morfismo de feixes, $(g, g^{\#}) \circ (f, f^{\#})$ é um morfismo de espaços anulares, e finalmente temos uma nova categoria, a de espaços anulares.

A princípio podemos nos sentir tentados a definir a categoria de espaços localmente anulares (**LRS**) como subcategoria plena da categoria de espaços anulares (isto é, todo morfismo de espaços anulares entre dois espaços localmente anulares é morfismo de espaços localmente anulares). Porém a nossa intuição de estruturas funcionais pede mais uma condição para essa definição abstrata: lembre que em um espaço localmente anular os talos são locais, com ideal maximal sendo pensado como germes de funções que se anulam no ponto em questão. Seja $(f, f^{\#})\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ um morfismo de espaços anulares entre os espaços localmente anulares X e Y. Em um ponto $x \in X$, temos que tanto $\mathcal{O}_{X,x}$ quanto $\mathcal{O}_{Y,f(x)}$ são anéis locais, com ideais maximais $\mathfrak{m}_x$ e $\mathfrak{m}_{f(x)}$ respectivamente. Lembre que pensamos nesses ideais como germes de funções que se anulam em x e $f(x)$,

respectivamente. Suponha $g \in \mathfrak{m}_{f(x)}$. Intuitivamente, temos algo como "g se anula em $f(x)$". O morfismo de feixes $f^{\#}\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$ induz um morfismo nos talos $f_x^{\#}\colon \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$, que é pensado como composição com f. Assim, como g "se anula em $f(x)$", queremos que $g \circ f = f^{\#}$ "se anule em x". Em outras palavras: queremos que $f_x^{\#}\left(\mathfrak{m}_{f(x)}\right) \subseteq \mathfrak{m}_x$. Trabalhando com estruturas funcionais, é fácil ver que imediatamente essa condição é satisfeita, porém na definição abstrata de feixes e de morfismos de espaços anulares ela não se verifica sempre. Por isso definimos um morfismo de espaços localmente anulares da seguinte maneira:

Definição 2.8. Um morfismo de espaços localmente anulares é um morfismo de espaços anulares $(f, f^{\#})\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$, tal que para cada ponto $x \in X$ o morfismo $f_x^{\#}\colon \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ induzido nos talos é local (isto é, $f_x^{\#}(\mathfrak{m}_{f(x)}) \subseteq \mathfrak{m}_x$).

Uma conta rápida confirma que a composição de morfismos de espaços localmente anulares, dada pela composição de morfismos de espaços anulares, é ainda um morfismo de espaços localmente anulares (no sentido que o morfismo induzido nos talos é local). Dessa forma findamos esta seção com a construção de uma nova categoria, a de espaços localmente anulares, denotada por $\underline{\mathbf{LRS}}$[4].

Para munir $\operatorname{Spec} R$ de uma "estrutura diferenciável", só precisamos agora definir um feixe sobre esse espaço. Como defini-lo? Vamos relembrar um pouco da Geometria Algébrica clássica (como exposta em [Fulton, 1989]) para termos alguma intuição. Se $V \subseteq \mathbb{A}_k^n$ é uma variedade algébrica, seu anel de funções coordenadas é definido como

$$\Gamma(V) \stackrel{\text{def}}{=} \frac{k[x_1, \ldots, x_n]}{I(V)}.$$

Toda $f \in \Gamma(V)$ induz uma função bem-definida de V em k. No entanto, dotando V da topologia de Zariski para variedades algébricas, nem sempre dado um $U \subsetneq V$, toda $f\colon U \to k$ é induzida por um polinômio globalmente definido (isto é, pertencente a $\Gamma(V)$). No entanto, tomando $f \in \Gamma(V)$ e pondo $V_f \stackrel{\text{def}}{=} \{P \in V \mid f(P) \neq 0\}$, temos o seguinte resultado (c.f. [Fulton, 1989], capítulo 6§3, proposição 5, página 71):

Teorema 2.2.4. Sejam V uma variedade afim e $f \in \Gamma(V)$. Então V_f é uma subvariedade aberta afim de V e

$$\Gamma(V_f) \simeq \Gamma(V)_f.$$

Resgatemos uma intuição anteriormente aqui discutida: como $V(f)$ é "o conjunto de zeros de f", seu complementar V_f é "o domínio de $1/f$", donde o conjunto de funções regulares em V_f consiste de todas as funções regulares definidas em V, mais a função nova $1/f$. Sem mais delongas, enunciemos o resultado essencial que garante que o resultado acima para variedades algébricas se estende para a definição de um feixe de anéis:

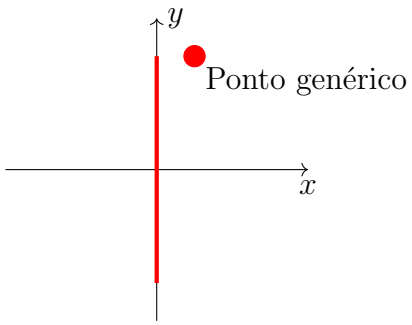
[4] Do inglês, *locally ringed spaces*.

Teorema 2.2.5. Seja R um anel. Então a associação $D(f) \mapsto R_f$ induz um feixe $\mathcal{O}_R$ em $\operatorname{Spec} R$, de tal maneira que $(\operatorname{Spec} R, \mathcal{O}_R)$ é um espaço localmente anular.

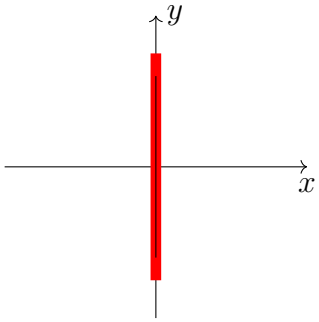
Para a demonstração, puramente mecânica, c.f. [Tengan and Borges, 2015], capítulo 15§2 (página 366). Finalmente, podemos especificar o que é um esquema:

Definição 2.9. Um esquema afim é um espaço localmente anular da forma $(\operatorname{Spec} R, \mathcal{O}_R)$ para algum anel R (ou melhor, isomorfo a um espaço localmente anular dessa forma). Um esquema é um espaço localmente anular $(X, \mathcal{O}_X)$ que admite uma cobertura por abertos U_i tal que $(U_i, \mathcal{O}_X \mid_{U_i})$ é um esquema afim para todo i.

Exemplo 2.2.6. Considere $X = \operatorname{Spec} \dfrac{\mathbb{C}[x,y]}{(x^2)}$ e $Y = \operatorname{Spec} \dfrac{\mathbb{C}[x,y]}{(x)}$. Como $\dfrac{\mathbb{C}[x,y]}{(x)}$ é o quociente do anel $\dfrac{\mathbb{C}[x,y]}{(x^2)}$ por seu nilradical (ideal de elementos nilpotentes), seus espectros são homeomorfos. Porém X e Y são esquemas completamente diferentes! Para ver isso, basta notar que $\mathcal{O}_X(X) = \dfrac{\mathbb{C}[x,y]}{(x^2)}$ possui nilpotentes, enquanto que $\mathcal{O}_Y(Y) = \dfrac{\mathbb{C}[x,y]}{(x)}$ é domínio. Como vizualizamos esses dois esquemas? Como consequência do Nullstellensatz e de $\dim \mathcal{O}_X(X) = \dim \mathcal{O}_Y(Y) = 1$, $X = Y = \{(\overline{x}, \overline{y} - a) \mid a \in \mathbb{C}\}$, donde podemos representar Y pictorialmente como



Já o esquema X será representado um pouquinho diferente: ele é visualizado fazendo-se $x^2 = 0$. Apesar de estarmos em $\mathbb{C}$, essa equação *não* é a mesma que $x = 0$; pra deixar mais claro, como em $\mathcal{O}_X(X)$, x é nilpotente, $x^2 = 0$ é a equação "x é quase igual a zero". Ou seja, ele é a reta $x = 0$ com uma "gordurinha" em volta:



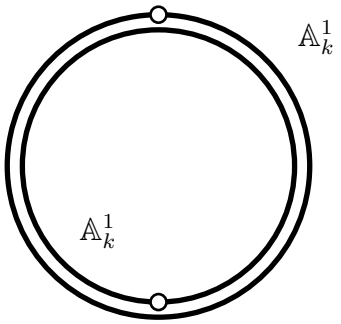
É um pouco como se o ponto genérico de Y tivesse sido espalhado pela reta como manteiga (ou geleia, se você preferir) no pão.

Exemplo 2.2.7. Seja k um corpo. Construamos a reta projetiva sobre k, $\mathbb{P}^1_k$, como um esquema. Considere os anéis $k[x]$ e $k[y]$, e o isomorfismo entre suas localizações $k[x]_x$ e $k[y]_y$ dado por $x \mapsto y^{-1}$, fornecendo assim um isomorfismo em **LRS** entre seus espectros. Note também que, pela proposição 2.1.7, o que temos na verdade é um isomorfismo entre subesquemas abertos das retas afins $\operatorname{Spec} k[x]$ e $\operatorname{Spec} k[y]$:

$$\varphi\colon \operatorname{Spec} k[x] \supseteq_{\circ} D(x) \xrightarrow{\simeq} D(y) \subseteq_{\circ} \operatorname{Spec} k[y].$$

Isso nos permite "colar as retas afins $\operatorname{Spec} k[x]$ e $\operatorname{Spec} k[y]$ ao longo dos subesquemas abertos $D(x)$ e $D(y)$" (para a construção explícita, c.f. [Tengan and Borges, 2015], capítulo 15§1). Essa construção de colagem pode ser generalizada para criar não apenas uma reta projetiva, mas o espaço projetivo $\mathbb{P}^n_k$. Isso é feito via a construção do esquema projetivo associado a um anel graduado, o Proj. Note que um ponto fechado (ideal maximal) de $D(x)$ que seja da forma $(x-a)$ $(a \neq 0)$ corresponde por φ a um ponto fechado (ideal maximal) de $D(y)$ da forma $\left(\frac{1}{y} - a\right) = (1 - ay) = \left(y - \frac{1}{a}\right)$. Ou seja, é um ponto da forma $(a\colon 1) = \left(1\colon \frac{1}{a}\right)$, assim como na reta projetiva usual! Veremos em breve um exemplo um pouco mais elaborado de que a Geometria Projetiva clássica se traduz sem perdas para a Geometria Algébrica contemporânea.

Pictorialmente, temos a seguinte situação:

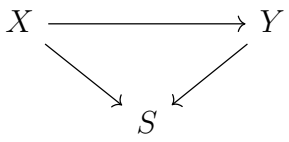


Duas cópias da reta afim $\mathbb{A}^1_k$ dispostas de maneira circular e concêntrica, em que a origem de uma é o "ponto no infinito" da outra, e vice-versa. A maneira com que essas retas estão dispostas faz com que a cada ponto de uma das cópias corresponda um único ponto da outra (com exceção das origens/pontos no infinito). Assim, a identificação das duas cartas afins "$\mathbb{A}^1_k \backslash \{0\}$" é o processo de colagem dos esquemas $\mathbb{A}^1_k$ e $\mathbb{A}^1_k$ ao longo dos subesquemas abertos $D(x)$ e $D(y)$ mencionado acima.

Comecemos agora a descrever a noção de funtor de pontos de um esquema. Basicamente, é um jeito relativo de descrever um esquema, que permite-nos simplificar algumas

demonstrações usando resultados de Teoria de Categorias (em especial o Lema de Yoneda).

Definição 2.10. Seja S um esquema. Um S-esquema, ou esquema sobre S, é um morfismo $X \to S$, em que X é um esquema[5]. Geralmente, referimo-nos a X como um esquema sobre S. Um morfismo de S-esquemas é um morfismo $X \to Y$, em que X e Y são S-esquemas, de forma que o diagrama abaixo comuta:



Os S-esquemas constituem uma categoria, denotada por $\underline{\mathbf{Sch}}/_S$. Finalmente, dado um S-esquema X, seu funtor de pontos é o funtor contravariante $X\colon \underline{\mathbf{Sch}}/_S \to \underline{\mathbf{Set}}$ dado em objetos por

$$T \longmapsto X(T) \stackrel{\text{def}}{=} \underline{\mathbf{Hom}}_{\underline{\mathbf{Sch}}/_S}(T, X)$$

e em morfismos da seguinte maneira: dado $f\colon T \to T'$ em $\underline{\mathbf{Sch}}/_S$, $X(f)\colon X(T') \to X(T)$ é dado por $X(f)(g) \stackrel{\text{def}}{=} g \circ f$.

Quando temos um esquema sobre um esquema afim, da forma $X \to \operatorname{Spec} R$, é comum se referir a X como um R-esquema, ou esquema sobre R. Ainda, é particularmente fácil descrever esquemas sobre um anel:

Teorema 2.2.8. Sejam R um anel e X um esquema. Existe uma bijeção

$$\underline{\mathbf{Hom}}_{\underline{\mathbf{Sch}}}(X, \operatorname{Spec} R) \longleftrightarrow \underline{\mathbf{Hom}}_{\underline{\mathbf{CRing}}}(R, \mathcal{O}_X(X)).$$

A demonstração encontra-se em [Tengan and Borges, 2015], capítulo 15§3 (página 384).

Corolário 2.2.9. A categoria $\underline{\mathbf{Aff.Sch}}$ de esquemas afins, é equivalente à categoria $\underline{\mathbf{CRing}}^{\text{op}}$, de anéis comutativos com as flechas invertidas.

Demonstração. O funtor $\operatorname{Spec}\colon \underline{\mathbf{CRing}} \to \underline{\mathbf{Aff.Sch}}$ já é tautologicamente essencialmente sobrejetor. Garantindo que ele seja pleno e fiel, Spec será uma equivalência de categorias. Esse fato é consequência imediata do teorema acima, que garante que existe bijeção entre $\underline{\mathbf{Hom}}_{\underline{\mathbf{Aff.Sch}}}(\operatorname{Spec} S, \operatorname{Spec} R)$ e $\underline{\mathbf{Hom}}_{\underline{\mathbf{CRing}}}(R, S)$. ■

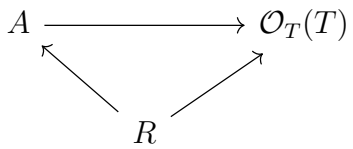
Não somente o teorema 2.2.8 caracteriza rapidamente esquemas sobre um anel, porém caracteriza também os morfismos entre $\operatorname{Spec} R$-esquemas!

[5] Na realidade, toda essa discussão de funtor de pontos pode ser feita de maneira mais geral, em uma categoria $\mathcal{C}$ qualquer. Ao invés de S-esquemas, falaríamos em S-objetos, S-morfismos, etc.

Corolário 2.2.10. Sejam A uma R-álgebra e T um R-esquema. Então temos uma bijeção

$$\underline{\mathbf{Hom}}_{\underline{\mathbf{Sch}}/R}(T, \operatorname{Spec} A) \longleftrightarrow \underline{\mathbf{Hom}}_{R-\underline{\mathbf{Alg}}}(A, \mathcal{O}_T(T)).$$

Demonstração. Basta notar que um morfismo de R-álgebras nada mais é do que um morfismo de anéis $A \to \mathcal{O}_T(T)$ fazendo comutar o diagrama:



Assim, temos a bijeção do enunciado. ■

Isso está muito abstrato. Acho que está em boa hora de um

Exemplo 2.2.11. Seja k um corpo e considere o esquema afim $X = \operatorname{Spec} R$, em que

$$R = \frac{k[x_1, ..., x_n]}{(f_1, ..., f_m)}.$$

Sendo $l \supseteq k$ uma extensão, o que seria um l-ponto de X? Ora, sabemos que existem bijeções

$$X(l) = \underline{\mathbf{Hom}}_{\underline{\mathbf{Sch}}/k}(\operatorname{Spec} l, X) = \mathbf{Hom}_{k-\mathbf{Alg}}(R, l).$$

Porém como $R = \dfrac{k[x_1, ..., x_n]}{(f_1, ..., f_m)}$, os morfismos que queremos estão em bijeção com os pontos $(a_1, ..., a_n) \in \mathbb{A}^n_l$ tais que $f_i(a_1, ..., a_n) = 0$ para todo $i = 1, ..., m$. Ou seja, os l-pontos de X são "pontos de X com valores em l"!

Vejamos um exemplo um pouco menos trivial, o supracitado Proj. Sua construção explícita pode ser encontrada em [Tengan and Borges, 2015], capítulo 15§2). Aqui, começaremos evidenciando o caráter geométrico dessa construção, e em seguida veremos um pouco do funcionamento do funtor de pontos.

Exemplo 2.2.12. Sejam $k = \mathbb{F}_q$ um corpo finito e considere o anel graduado

$$R = \frac{\mathbb{F}_q[x, y, z]}{(y^2z - x^3 + xz^2)} = k[\overline{x}, \overline{y}, \overline{z}]$$

e o esquema projetivo associado, $E = \operatorname{Proj} R$. No plano projetivo clássico, a equação $y^2z = x^3 - xz^2$ é coberta pelas cartas afins $y = 1$ e $z = 1$. Aqui, similarmente temos

$$\operatorname{Proj} R = D_+(\overline{y}) \cup D_+(\overline{z}).$$

Afinal, se $\mathfrak{p} \in \operatorname{Proj} R$ e $\mathfrak{p} \notin D_+(y) \cup D_+(z)$ temos $\mathfrak{p} \ni \overline{y}, \overline{z}$. Portanto o ideal correspondente em $k[x, y, z]$ (denotado aqui também por $\mathfrak{p}$) deve conter, além de $(y^2z - x^3 + xz^2)$, y e z.

Porém

$$\begin{aligned}\mathfrak{p} &\supseteq (y^2x - x^3 + xz^2, y, z)\\ &= (x^3, y, z),\end{aligned}$$

donde $\mathfrak{p} \supseteq (x, y, z)$, uma contradição com $\mathfrak{p} \in \operatorname{Proj} R$. Dessa forma, de fato $\operatorname{Proj} R$ é coberto pelas cartas afins $D_+(\overline{y})$ e $D_+(\overline{z})$. Os esquemas correspondentes são

$$D_+(\overline{y}) = \operatorname{Spec} R_{(\overline{y})} = \operatorname{Spec} \frac{\mathbb{F}_q\left[\frac{x}{y}, \frac{z}{y}\right]}{\left(\frac{z}{y} - \left(\frac{x}{y}\right)^3 + \left(\frac{x}{y}\right)\left(\frac{z}{y}\right)^2\right)},$$

$$D_+(\overline{z}) = \operatorname{Spec} R_{(\overline{z})} = \operatorname{Spec} \frac{\mathbb{F}_q\left[\frac{x}{z}, \frac{y}{z}\right]}{\left(\left(\frac{y}{z}\right)^2 - \left(\frac{x}{z}\right)^3 + \frac{x}{z}\right)}.$$

O subesquema aberto ao longo do qual eles são colados nada mais é do que a localização em comum

$$\operatorname{Spec} R_{(\overline{yz})}.$$

Simplificando nossa notação, os subesquemas abertos que foram colados para formar $\operatorname{Proj} R$ são

$$\operatorname{Spec} R_{(\overline{y})} = \operatorname{Spec} \frac{\mathbb{F}_q[X_1, Z_1]}{(Z_1 - X_1^3 + X_1 Z_1)}$$

em que $X_1 = \frac{x}{y}$ e $Z_1 = \frac{z}{y}$, e

$$\operatorname{Spec} R_{(\overline{z})} = \operatorname{Spec} \frac{\mathbb{F}_q[X_2, Y_2]}{(Y_2 - X_2^3 + X_2)},$$

com $X_2 = \frac{x}{z}$ e $Y_2 = \frac{y}{z}$.

Podemos exibir facilmente alguns (porém não todos os)[6] pontos desse esquema. Em $\operatorname{Spec} R_{(\overline{y})}$ existem pontos da forma

$$(X_1 - A, Z_1 - B)$$

com $A, B \in \mathbb{F}_q$ e $B = A^3 - AB$, e em $\operatorname{Spec} R_{(\overline{z})}$ existem pontos da forma

$$(X_2 - C, Y_2 - D)$$

com $C, D \in \mathbb{F}_q$ e $D^2 = C^3 - C$. Assim podemos realmente *enxergar* o esquema $\operatorname{Proj} R$ da mesma maneira que enxergamos a curva projetiva $y^2z = x^3 - xz^2$! Incrível isso, não?!

Para visualizar melhor esse esquema projetivo, também podemos usar o funtor de pontos. Agora, consideremos uma extensão k_r de grau r de k. Descrevamos $E(k_r)$.

[6] Se trocássemos k por um corpo algebricamente fechado, como por exemplo $\mathbb{C}$, aí sim os pontos aqui exibidos esgotariam os pontos fechados do esquema, graças ao Nullstellensatz.

Intuitivamente, queremos que esse conjunto consista de (ou melhor, esteja em bijeção com) pontos $(x\colon y\colon z)$ da curva elíptica. Mãos à obra:

Um k_r ponto de E, isto é, um elemento de $E(k_r)$ é um morfismo de esquemas $\operatorname{Spec} k_r \to E$. Explicitando a notação, um k_r-ponto de E é um morfismo

$$(f, f^{\#})\colon (\operatorname{Spec} k_r, \mathcal{O}_{k_r}) \longrightarrow (E, \mathcal{O}_E).$$

Agora, como $\operatorname{Spec} k_r$ é unitário, sua imagem por f em E consiste de um único ponto. Suponhamos sem perda de generalidade que $f((0)) \in D_+(\overline{y})$. Esse morfismo se fatora de maneira única em morfismos $\operatorname{Spec} k_r \to D_+(\overline{y}) \to E$. Sabendo que

$$D_+(\overline{y}) = \operatorname{Spec} R_{(\overline{y})} = \operatorname{Spec} \frac{\mathbb{F}_q[X, Z]}{(Z - X^3 + XZ^2)},$$

com $X = \frac{x}{y}$ e $Z = \frac{z}{y}$, os k_r-pontos de E cuja imagem está na carta $D_+(\overline{y})$ estão em bijeção com os morfismos de esquemas afins $\operatorname{Spec} k_r \to \operatorname{Spec} R_{(\overline{y})}$, que por sua vez correspondem a morfismos de anéis (ou melhor, $\mathbb{F}_q$-álgebras) $R_{(\overline{y})} \to k_r$. Porém o que define um morfismo

$$\frac{\mathbb{F}_q[X, Z]}{(Z - X^3 + XZ^2)} \longrightarrow k_r$$

é a escolha de $X \mapsto a$ e $Z \mapsto b$ $(a, b \in k_r)$. E essa escolha não é nem tão arbitrária: afinal, a e b estão sujeitos à condição $b - a^3 + ab^2 = 0$. Dessa forma, um ponto de $E(k_r)$ é (ou melhor, corresponde a) um ponto $(a\colon 1\colon b) \in \mathbb{P}^2_{k_r}$ satisfazendo a equação da curva. No caso em que $f((0)) \in D_+(z)$, a mesma discussão origina um ponto $(a\colon b\colon 1) \in \mathbb{P}^2_{k_r}$ que satisfaz a equação da curva. Ou seja: temos uma correspondência natural

$$E(k_r) \longleftrightarrow \{(a\colon b\colon c) \in \mathbb{P}^2_{k_r} \mid b^2c - a^3 + ac^2 = 0\}.$$

À luz desse exemplo, concluímos que se X é um k-esquema e $l \supseteq k$, o funtor de pontos é o jeito natural de se pensar a noção de "ponto de X com coordenadas em l", se quisermos que esses "pontos" (isto é, elementos de $X(l)$) correspondam de maneira direta aos "pontos" que pensávamos na Geometria Algébrica clássica (isto é, elementos de l^n que satisfazem as equações que definem X).

Pensando assim, o produto cartesiano de dois esquemas toma um novo significado. Se queremos que os "pontos" do produto cartesiano de dois esquemas seja o produto cartesiano dos "pontos" de cada um dos esquemas, é claro que o que queremos, na realidade, é um objeto cujo funtor de pontos seja o produto cartesiano dos dois funtores de pontos. Em termos mais abstratos: trabalhando com esquemas relativos, a noção certa do produto de dois esquemas é a de produto fibrado!

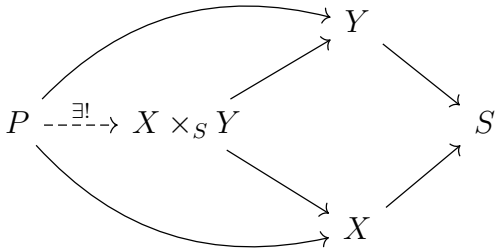
Vejamos em mais detalhe essa afirmação: sejam X e Y dois esquemas sobre um terceiro esquema S (frequentemente S será o espectro do corpo onde estão definidas as variedades X e Y, mas vamos nos manter no caso geral). À luz do fato que o funtor de pontos nos

dá a noção "certa" de ponto, se Z é o "produto certo" de X e Y, é de se esperar que o para qualquer S-esquema W, tenhamos

$$Z(W) = X(W) \times Y(W).$$

Para qualquer um que já estudou Teoria de Categorias, a conclusão óbvia dessa igualdade é a afirmação de dois parágrafos atrás: "a noção certa do produto de dois esquemas representa o produto cartesiano de seus funtores de pontos". Como isso é uma propriedade universal, ela define um objeto que, caso exista, é único a menos de isomorfismo, e denotado por $X \times_S Y$. Não será nossa preocupação aqui dar uma descrição detalhada da construção do produto fibrado em seu caso geral, apenas assumiremos sua existência. Essa demonstração pode ser encontrada em [Tengan and Borges, 2015] capítulo 15§3 (página 390)ou [Hartshorne, 2013], capítulo II§3 (página 87).

Definição 2.11. Sejam X e Y esquemas sobre S. O produto fibrado de X e Y sobre S, denotado por $X \times_S Y$, é um esquema, munido de morfismos $X \times_S Y \to X$ e $X \times_S Y \to Y$, satisfazendo a seguinte propriedade universal descrita pelo diagrama abaixo:



Vejamos alguns exemplos para nos familiarizarmos com a noção do produto fibrado.

Exemplo 2.2.13. Sejam R um anel e A e B duas R-álgebras. Os morfismos $R \to A$, $R \to B$ induzem uma estrutura de $\operatorname{Spec} R$-esquema em $\operatorname{Spec} A$ e $\operatorname{Spec} B$. Ainda, temos

$$\operatorname{Spec} A \times_{\operatorname{Spec} R} \operatorname{Spec} B \simeq \operatorname{Spec} A \otimes_R B.$$

Ou seja: o produto de dois esquemas afins sobre um esquema afim é, ele próprio, um esquema afim. Estabelecer esse fato é o primeiro passo para provar a existência de produtos fibrados em $\underline{\mathbf{Sch}}/S$.

Exemplo 2.2.14. Sejam X um esquema sobre um corpo k e l uma extensão de k. A inclusão $k \hookrightarrow l$ dá a $\operatorname{Spec} l$ uma estrutura de $\operatorname{Spec} k$-esquema. O produto

$$X \times_{\operatorname{Spec} k} \operatorname{Spec} l,$$

comumente denotado por $X \times_k l$, é chamado de mudança de base de X por l. É bastante rotineiro o ato de fazer uma mudança de base tomando o fecho algébrico. Por exemplo: considere

$$X = \operatorname{Spec} \frac{\mathbb{F}_q[x, y]}{(y^2 - x^3 + x)}.$$

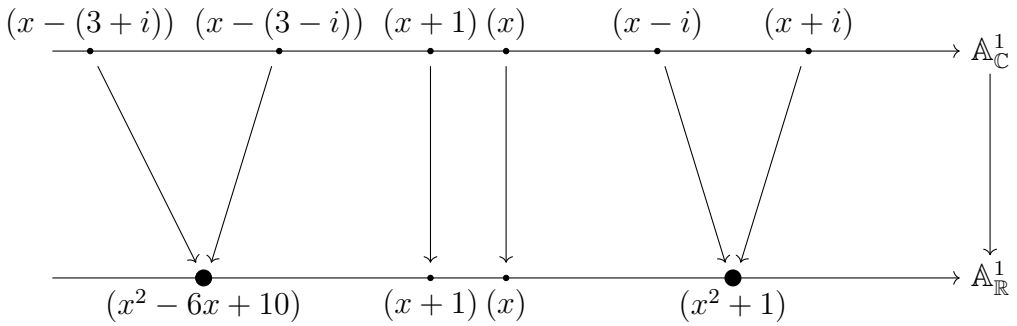
Fazendo uma mudança de base para $\overline{\mathbb{F}_q}$, à luz do exemplo anterior, vemos que o produto $\overline{X} = X \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ é o espectro do anel

$$\frac{\mathbb{F}_q[x,y]}{(y^2 - x^3 + x)} \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q} \simeq \frac{\overline{\mathbb{F}_q}[x,y]}{(y^2 - x^3 + x)}.$$

Ou seja: a mudança de base nada mais é do que fazermos uma extensão do corpo de escalares. E geometricamente (isto é, em termos de desenhos), o que significa
$X \times_{\operatorname{Spec} k} \operatorname{Spec} l$? A nossa intenção é que possamos pensar o produto fibrado como o produto cartesiano. Como $\operatorname{Spec} l = \{(0)\}$ é unitário, faz sentido imaginar que o desenho de
$X \times_{\operatorname{Spec} k} \operatorname{Spec} l$ seja o mesmo de X. No entanto, um fenômeno interessante acontece quando fazemos uma mudança de base. Para ver esse fenômeno em ação, considere a reta afim real $\mathbb{A}^1_{\mathbb{R}} \stackrel{\text{def}}{=} \operatorname{Spec} \mathbb{R}[x]$, e sua mudança de base para $\mathbb{C}$, $\mathbb{A}^1_{\mathbb{R}} \times_{\operatorname{Spec} \mathbb{R}} \operatorname{Spec} \mathbb{C} = \mathbb{A}^1_{\mathbb{C}}$. Na reta real, os pontos correspondem a polinômios irredutíveis, assim temos dois tipos de pontos:

- Pontos da forma $(x - a)$, $a \in \mathbb{R}$;
- Pontos da forma $(x^2 + ax + b)$, $a, b \in \mathbb{R}$, $x^2 + ax + b$ irredutível em $\mathbb{R}$.

Na reta complexa, no entanto, por ser $\mathbb{C}$ algebricamente fechado, o único tipo de ponto é da forma $(x - a)$, com $a \in \mathbb{C}$. Assim, algo deve acontecer com pontos do segundo tipo (chamados de "pontos duplos", por motivos que se tornarão óbvios em breve) quando fazemos a mudança de base de $\mathbb{R}$ para $\mathbb{C}$. O produto fibrado sempre vem "de fábrica" com morfismos de projeção em cada uma de suas componentes. No caso que estamos trabalhando, a projeção $\mathbb{A}^1_{\mathbb{C}} \to \mathbb{A}^1_{\mathbb{R}}$ é induzida pelo morfismo de inclusão $\mathbb{R}[x] \hookrightarrow \mathbb{C}[x]$. Assim, existem precisamente dois pontos de $\mathbb{A}^1_{\mathbb{C}}$ que são projetados para $(x^2 + 1)$: $(x + i)$ e $(x - i)$. Em desenhos, temos a seguinte situação:



Ou seja: quando fazemos a mudança de base, o ponto $(x^2 + 1)$ se "quebra" em dois pontos: $(x + i)$ e $(x - i)$! Assim, a nomenclatura de "ponto duplo" faz sentido para $(x^2 + 1)$, enquanto que os pontos da forma $(x - a)$, $a \in \mathbb{R}$ ou $a \in \mathbb{C}$, ou mais geralmente $a \in k$, são chamados de "pontos simples".

A noção de "ponto múltiplo" está intimamente relacionada com a noção de grau de um ponto. É possível imaginar que o grau de um ponto "simples" deve ser 1, o grau de um ponto duplo 2, e assim por diante. Vejamos como construir a noção de grau de um ponto:

No exemplo que acabamos de ver, essa noção está ligada à quantidade de raízes de um polinômio irredutível. Por exemplo: $x+1$ possui exatamente uma raíz queremos que seu grau seja 1. Já x^2+1 possui duas raízes, então esperamos que seu grau seja 2. Como encontrar esse 2 a partir de x^2+1? Um jeito é tomar seu corpo de decomposição, e a partir disso calcular o grau desse corpo sobre $\mathbb{R}$. Mais diretamente:

$$2 = \left[\frac{\mathbb{R}[x]}{(x^2+1)} : \mathbb{R}\right].$$

Assim como em Geometria Diferencial evitamos o quanto for possível usar coordenadas para resolver problemas em variedades, em Geometria Algébrica evitamos usar cartas afins o quanto for possível. Assim, notamos que o quociente $\dfrac{\mathbb{R}[x]}{(x^2+1)}$ pode ser escrito como o corpo residual $\kappa((x^2+1))$ do anel local de $(x^2+1) \in \mathbb{A}^1_{\mathbb{R}}$. E como $\mathbb{A}^1_{\mathbb{R}}$ é um $\mathbb{R}$-esquema, vemos que a definição a seguir condiz com o que esperamos de uma noção de grau de ponto:

Definição 2.12. Sejam X um k-esquema e $\mathfrak{p} \in X$. O grau de $\mathfrak{p}$ é definido como

$$\deg \mathfrak{p} \overset{\text{def}}{=} [\kappa(\mathfrak{p}) : k] = \left[\frac{\mathcal{O}_{X,\mathfrak{p}}}{\mathfrak{m}_{\mathfrak{p}}} : k\right].$$

Note que como sempre existe uma inclusão $k \hookrightarrow \kappa(\mathfrak{p})$, faz sentido dizer que $\kappa(\mathfrak{p})$ é uma extensão de k, de modo que o grau de um ponto está bem-definido. Ainda, note que se k é algebricamente fechado, o grau de todo ponto fechado P é igual a 1.

2.3 Riemann-Roch-Paper-Scissors!

Aqui, veremos nossa principal arma a ser usada para provar a hipótese de Riemann: o Teorema de Riemann-Roch. A sua "moral" é bastante simples: a partir do momento em que limitamos os polos de funções meromorfas a uma quantidade e ordem "aceitáveis", não temos muitos graus de liberdade. Para fins de ilustração, é conveniente olharmos o caso complexo. Se C é uma curva algébrica complexa, C é, em particular, uma superfície de Riemann, isto é, uma "variedade diferenciável complexa de dimensão (complexa) 1". Aí, se $h : C \to \mathbb{C}$ é uma função meromorfa em C, a noção de zeros e polos está bem-definida: afinal, se $V \underset{\circ}{\subseteq} \mathbb{C}$ e $h : V \to \mathbb{C}$ não possui singularidade essencial, podemos escrever

$$h(z) = (z - z_0)^n \cdot g(z),$$

em que $n \in \mathbb{Z}$, g é holomorfa em uma vizinhança de $z_0 \in V$ e $g(z_0) \neq 0$. Tal n é chamado de ordem de h em z_0. Se $n > 0$, h possui um zero de ordem n em z_0, e se $n < 0$, h possui um polo de ordem $-n$ em z_0. É um fato de Análise Complexa que o conjunto de zeros e polos de uma função meromorfa não-nula é discreto. Essa noção de zeros e polos de funções de $\mathbb{C}$ em $\mathbb{C}$ é facilmente importada para o contexto de superfícies de Riemann, donde se S é uma superfície de Riemann compacta, toda função meromorfa não-nula em S possui *finitos* zeros e polos. Portanto, considerando como $\operatorname{Div} V$ o grupo abeliano livre gerado pelos pontos de V, temos um morfismo de $K(V)$ (o corpo de funções meromorfas $V \to \mathbb{C}$) em $\operatorname{Div} V$,

$$h \longmapsto (h) = \operatorname{div} h \stackrel{\text{def}}{=} \sum_{z_0 \in U} \operatorname{ord}_{z_0} h \cdot z_0.$$

Por exemplo: na esfera de Riemann, isto é, $X = \mathbb{C} \cup \{\infty\}$, a função meromorfa z possui um zero (em 0) e um polo (em ∞). Assim, $(z) = 1 \cdot 0 - 1 \cdot \infty$. Note que z possui a mesma quantidade de zeros e polos, quando contados com multiplicidade. O mesmo fenômeno acontece com a função z^2: ela possui um zero de ordem 2 em 0, e um polo também de ordem 2 em ∞, de forma que $(z^2) = 2 \cdot 0 - 2 \cdot \infty$. Esse fenômeno pode ser sumarizado na afirmação

Toda função meromorfa em uma superfície de Riemann compacta possui a mesma quantidade de zeros e polos, quando contados com multiplicidade.

Agora, como transportar essa noção de ordem, zeros e polos, de divisores e funções meromorfas, de $\mathbb{C}$ para k? Ou melhor, do contexto de superfícies de Riemann para o de esquemas (ou pelo menos curvas)?

O primeiro passo é investigar o conceito de função. Lembre que uma função meromorfa é definida como sendo uma função definida em quase todos os pontos de uma superfície de Riemann. Ainda, por teoremas padrão de Análise Complexa, duas funções meromorfas são iguais se concordam em um aberto. Essa noção de "concordar em um aberto" traz lembranças da definição de talo de um feixe. Porém em qual ponto consideramos esse talo? Necessariamente, esse ponto deveria estar em todos os abertos do espaço topológico subjacente. No caso de $\mathbb{C}$, que é Hausdorff, isso é um problema. No entanto, para variedades algébricas, isso não é um problema: todo esquema integral (veja abaixo) possui um único ponto que pertence a todos os abertos: o ponto genérico (c.f. [Hartshorne, 2013], capítulo II§2, página 80). Assim, começamos com a seguinte

Definição 2.13. Seja X um esquema integral (isto é, para toda carta afim $\operatorname{Spec} A \underset{\circ}{\subseteq} X$, A é domínio). O conjunto de funções meromorfas de X é definido como $\mathcal{O}_{X,\eta}$, em que $\mathcal{O}_X$ é seu feixe estrutural e η seu ponto genérico. Quando X é um esquema sobre um corpo k, denotamos $\mathcal{O}_{X,\eta}$ por $k(X)$.

O conjunto de funções meromorfas é um corpo (c.f. [Hartshorne, 2013], capítulo II§3, página 91), podendo ser identificado com $Frac\, A$, em que $\operatorname{Spec} A \underset{\circ}{\subseteq} X$ é qualquer aberto afim.

Sabendo o que é uma função meromorfa, tentemos entender o que é a ordem de uma função meromorfa em um ponto. A ordem é uma propriedade local em cada ponto (fechado), portanto a ordem em $P \in X$ é uma função $\operatorname{ord}_P \colon \mathcal{O}_{X,P}^* \to \mathbb{Z}$. Ainda, a ordem satisfaz as condições de uma valorização discreta (c.f. [Atiyah and Macdonald, 1969], capítulo 9). Portanto, queremos que os talos sejam anéis de valorização discreta, com corpo de frações igual ao corpo de funções meromorfas de X. À luz da definição e teorema abaixo, é imediato trabalharmos então com esquemas integrais, não-singulares, de dimensão um, de tipo finito sobre um corpo k, que normalmente será considerado algebricamente fechado.

Definição 2.14. Seja X um esquema. Dizemos que X é regular se todos os talos são anéis locais regulares. Caso X possua dimensão 1, diremos também que X é não-singular.

Teorema 2.3.1. Seja X um esquema de tipo finito sobre um corpo k. Então, para todo ponto fechado, $P \in X$, $\dim X = \dim \mathcal{O}_{X,P}$. Ainda, seu corpo de funções meromorfas $k(X)$ é uma extensão de k e $td_k k(X) = \dim X$

A demonstração encontra-se disponível em [Hartshorne, 2013], capítulo II§3 (página 95).

Portanto, se quisermos poder falar em zeros e polos de funções meromorfas, será útil trabalharmos com um conceito de curva que garanta essas e outras coisas:

Definição 2.15. Uma curva sobre um corpo k é um esquema integral e regular C sobre k, de dimensão um e compacto, que satisfaz as seguintes condições:

- Para toda carta afim $\operatorname{Spec} A \underset{\circ}{\subseteq} C$, A é noetheriano;
- Para toda carta afim $\operatorname{Spec} A \underset{\circ}{\subseteq} C$, A é uma k-álgebra finitamente gerada;
- A projeção $C \times_{\operatorname{Spec} k} C \to C$ é um mapa fechado de espaços topológicos;
- Para qualquer k-esquema Y, o mapa de projeção $X \times_{\operatorname{Spec} k} Y \to Y$ é um mapa fechado de espaços topológicos.

O grupo de divisores de uma curva C é o grupo abeliano livre gerado pelos pontos fechados de C. Explicitamente,

$$\operatorname{Div} C \overset{\text{def}}{=} \bigoplus_{\substack{P \in C \\ P \neq \eta}} \mathbb{Z} \cdot P.$$

O grau de um divisor $D = \sum_{\substack{P \in C \\ P \neq \eta}} n_P \cdot P$ é definido como $\deg D \stackrel{\text{def}}{=} \sum n_P \cdot \deg P$. A partir de agora omitiremos o índice da soma quando falarmos de divisores, por simplicidade da notação, deixando subentendido que a soma percorre todos os pontos fechados da curva.

Proposição 2.3.2. Em uma curva C, todo talo $\mathcal{O}_{C,P}$ em um ponto $P \in C$ não-genérico é um anel de valorização discreta com corpo de frações $k(X)$. A valorização associada a $\mathcal{O}_{C,P}$ é denotada por $\operatorname{ord}_P \colon \mathcal{O}_{C,P}^* \to \mathbb{Z}$.

Demonstração. Por ser C uma curva, temos que o talo $\mathcal{O}_{C,P}$ é um domínio local, noetheriano, de dimensão 1 e normal. Ou seja, $\mathcal{O}_{C,P}$ é um domínio de Dedekind. Porém um domínio de Dedekind local é um anel de valorização discreta. Como podemos considerar os elementos de $\mathcal{O}_{C,P}$ como seções do feixe estrutural em abertos (afins) tão pequenos quanto seja necessário, porém ainda densos graças á topologia de Zariski, concluímos que $Frac\, \mathcal{O}_{C,P} = k(X)$. ■

O próximo lema garante que a definição de divisor de uma função meromorfa em X está de fato bem-definido:

Lema 2.3.3. Sejam C uma curva sobre k e $f \in k(C)^*$. Então $\operatorname{ord}_P f = 0$ para quase todos os pontos fechados P de C.

A demonstração encontra-se em [Hartshorne, 2013], capítulo II§6 (página 131).

Definição 2.16. Sejam C uma curva sobre k e $f \in k(C)^*$. O divisor de f é

$$\operatorname{div} f = (f) \stackrel{\text{def}}{=} \sum \operatorname{ord}_P f \cdot P.$$

Um divisor da forma $\operatorname{div} f$ é chamado de principal. Dois divisores são ditos serem linearmente equivalentes se possuem a mesma classe de equivalência no conúcleo do morfismo $\operatorname{div} \colon k(C)^* \to \operatorname{Div} C$. Se $\operatorname{ord}_P f \geq 0$, dizemos que f é holomorfa em P, se $\operatorname{ord}_P f > 0$, dizemos que P é um zero de ordem $\operatorname{ord}_P f$ de f, e se $\operatorname{ord}_P f < 0$, dizemos que P é um polo de ordem $-\operatorname{ord}_P f$ de f. Por fim, definimos o divisor de zeros de f como $(f)_0 \stackrel{\text{def}}{=} \sum_{\operatorname{ord}_P f > 0} \operatorname{ord}_P f \cdot P$ e o divisor de polos de f como $(f)_\infty \stackrel{\text{def}}{=} \sum_{\operatorname{ord}_P f < 0} -\operatorname{ord}_P f \cdot P$.

Damos agora um sentido "esquemático" à afirmação de que funções meromorfas em superfícies de Riemann compactas possuem a mesma quantidade de zeros e polos, quando contados com multiplicidade:

Proposição 2.3.4. Seja C uma curva sobre k. Então para toda $f \in k(C)$, $\deg \operatorname{div} f = 0$.

A demonstração encontra-se disponível em [Hartshorne, 2013], capítulo II§6 (página 132).

É necessário agora fazer um comentário sobre o valor de funções em pontos. Trabalhando em superfícies de Riemann, essa noção está muito bem-definida. Porém, dado um elemento $f \in k(C)^*$, o que seria $f(P)$ para um $P \in C$? Consideremos um caso concreto que vai nos elucidar quanto a como definir $f(P)$.

Sejam $f \in \mathbb{C}[x,y]$ um polinômio não-singular (isto é, $V(f, f_x, f_y) = \emptyset$) e $(a,b) \in V(f)$. O valor de $f(x,y)$ em (a,b) é obtido substituindo-se x por a e y por b. Ou seja, $x \mapsto a$ e $y \mapsto b$, o isomorfismo

$$\frac{\mathbb{C}[x,y]}{(x-a, y-b)} \longrightarrow \mathbb{C}$$

deve ser um bom ponto de partida. Aqui, podemos definir $f(a,b)$ como a imagem de f pelo isomorfismo acima. Porém temos um sério problema para generalizar isso: em esquemas, não temos coordenadas. Então, o anel que deveremos considerar não pode ser $\dfrac{\mathbb{C}[x,y]}{(x-a,y-b)}$. Porém, sabemos que

$$\frac{\mathbb{C}[x,y]}{(x-a,y-b)} \simeq \frac{\mathbb{C}[x,y]_{(x-a,y-b)}}{(x-a,y-b)},$$

e como $\left(\dfrac{\mathbb{C}[x,y]}{(f)}\right)_{(x-a,y-b)}$ é o anel local de $f(x,y) = 0$ em (a,b), podemos definir o valor de f em (a,b) como sendo a imagem de f no corpo residual de (a,b), e teremos uma definição que quase que pede para ser generalizada:

Definição 2.17. Sejam C uma curva sobre k, $P \in C$ fechado e $f \in \mathcal{O}_{C,P} \subseteq k(C)$. O valor de f em P é definido como a imagem de f no corpo residual de P, $\kappa(P)$.

Observação 1. No caso complexo, o valor de uma função meromorfa f em um ponto P só está bem-definido quando $\operatorname{ord}_P f \geq 0$. Em esquemas o mesmo vale: só faz sentido falar na imagem de f no corpo residual de P se $f \in \mathcal{O}_{C,P}$, isto é, $\operatorname{ord}_P f \geq 0$.

Observação 2. Assim como no caso complexo, $f(P) = 0 \iff \operatorname{ord}_P f > 0$. Afinal, uma $f \in \mathcal{O}_{C,P}$ pertence ao ideal maximal de $\mathcal{O}_{C,P}$ (isto é, é 0 em $\kappa(P)$) se, e somente se, $\operatorname{ord}_P f > 0$.

Agora, voltemos para o caso complexo para buscar inspiração para o Teorema de Riemann-Roch. Seja S uma superfície de Riemann. Uma possível pergunta a se fazer é: "quais são as funções holomorfas em S?" Bom, se S é compacta (que é mais adequado para nós como análogo para curvas, afinal da maneira que definimos, curvas são esquemas projetivos, que são sempre compactos), a resposta é: somente as constantes. Ou seja, não muitas. Consideremos novamente a esfera de Riemann, e façamos uma pergunta parecida: quais são as funções meromorfas em S que possuem polo exclusivamente em ∞, e ordem no máximo um nesse polo? Em termos de divisores, queremos conhecer o conjunto

$$\{f \in \mathbb{C}(S)^* \mid (f) \geq -1 \cdot \infty\},$$

em que temos uma ordem parcial natural induzida em $\operatorname{Div} S$ pela ordem total em $\mathbb{Z}$. Mais geralmente, dado um divisor D, definimos o seguinte espaço vetorial sobre $\mathbb{C}$:

$$L(D) \stackrel{\text{def}}{=} \{f \in \mathbb{C}(S)^* \mid (f) + D \geq 0\} \cup \{0\}.$$

Podemos então reformular as perguntas originais em um sentido matemático preciso: quanto valem

$$\dim_{\mathbb{C}} L(0) \qquad \text{e} \qquad \dim_{\mathbb{C}} L(1 \cdot \infty)?$$

Denotamos essas dimensões por $l(0)$ e $l(1 \cdot \infty)$. Mais geralmente, para um divisor D, estamos interessados no número $l(D) \stackrel{\text{def}}{=} \dim_{\mathbb{C}} L(D)$. A resposta vem na forma do Teorema de Riemann-Roch:

Teorema 2.3.5 (Teorema de Riemann-Roch para $\mathbb{C}$)**.** Seja S uma superfície de Riemann compacta de gênero g. Então, existe um divisor K, chamado de divisor canônico, tal que, para todo divisor $D \in \operatorname{Div} S$,

$$l(D) - l(K - D) = \deg D + 1 - g.$$

A demonstração encontra-se disponível em [Miranda, 1995], capítulo VI§3 (página 192).

Temos um resultado importante sobre divisores canônicos:

Corolário 2.3.6. Se K é um divisor canônico em S, então $\deg K = 2g - 2$. Portanto, se $\deg D \geq 2g - 1$, então $l(D) = \deg D + 1 - g$.

Demonstração. Tome, no Teorema de Riemann-Roch, $D = 0$. Então

$$l(0) - l(K) = 1 - g,$$

e como $l(0) = 1$, temos

$$l(K) = g.$$

Agora, tomando $D = K$ no Teorema de Riemann-Roch,

$$\deg K = l(K) - l(0) - 1 + g = g - 1 - 1 + g = 2g - 2.$$

A segunda parte do corolário se resume a provar que se $\deg D < 0$, então $l(D) = 0$. Ora, se $f \in L(D)$ e $f \neq 0$, então $(f) + D \geq 0$, donde $\deg D \geq 0$, o que é uma contradição. Portanto $l(D) = 0$ sempre que $\deg D < 0$ e assim se $\deg D \geq 2g - 1$, temos $\deg K - D < 0$ e portanto $l(D) = \deg D + 1 - g$. ∎

Vejamos, a título de exemplo, uma aplicação do Teorema de Riemann-Roch:

Exemplo 2.3.7. Seja S uma superfície de Riemann de gênero 1. Fixemos um ponto $P_0 \in S$. Como o grau de um divisor canônico em S é 0, temos que $l(n \cdot P_0) = n$, para $n \in \mathbb{N}^*$. Como $L(n \cdot P_0) \subseteq L((n+1) \cdot P_0)$, podemos escolher geradores de alguns desses espaços vetoriais:

$$\begin{aligned}
&L(1 \cdot P_0) = span\{1\};\\
&L(2 \cdot P_0) = span\{1, x\};\\
&L(3 \cdot P_0) = span\{1, x, y\};\\
&L(4 \cdot P_0) = span\{1, x, y, x^2\};\\
&L(5 \cdot P_0) = span\{1, x, y, x^2, xy\};\\
&L(6 \cdot P_0) = span\{1, x, y, x^2, xy, x^3\} = span\{1, x, y, x^2, xy, y^2\}.
\end{aligned}$$

Portanto, os elementos $1, x, y, x^2, xy, x^3, y^2$ são linearmente dependentes e devem satisfazer uma equação da forma

$$a_0 + a_1x + a_2x^2 + x^3 = a_3y + a_4xy + y^2.$$

Mediante uma mudança de variáveis, essa equação assume a familiar forma da equação de Weierstraß de uma curva elíptica:

$$y^2 = x^3 + ax + b.$$

Já temos todo o maquinário para transportar para a terra dos esquemas a pergunta a que se propõe responder o Teorema de Riemann-Roch. No entanto, a demonstração que será aqui usada pede um ferramentário muito mais elaborado da Geometria Algébrica: a cohomologia de feixes. Por não ser esse o foco principal deste trabalho, e por essa construção ser bastante extensa, vou me permitir apenas citar alguns fatos importantes de cohomologia que serão usados na prova do Riemann-Roch. Todas as construções explícitas e definições técnicas abaixo encontram-se disponíveis em [Hartshorne, 2013], ao longo do capítulo III, e [Ueno, 2003], principalmente no capítulo 7.

Comecemos pelo começo: a cohomologia de um feixe $\mathcal{F}$ de grupos abelianos sobre um esquema X é um conjunto de grupos abelianos $H^i(X, \mathcal{F})$ ($i \in \mathbb{N}$), que "são uma medida do quanto $\Gamma(X, -)$ não é um funtor exato". Trocando em miúdos:

- **Os H^i são um δ-funtor derivado de $\Gamma(X, -)$.** $H^0(X, \mathcal{F}) = \Gamma(X, \mathcal{F})$ para todo feixe $\mathcal{F}$. Ainda, dada uma sequência exata curta de feixes

$$0 \to \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \to 0,$$

existe uma sequência exata longa de grupos de cohomologia

$$\begin{aligned} 0 \to H^0(X,\mathcal{F}) \longrightarrow H^0(X,\mathcal{G}) \longrightarrow H^0(X,\mathcal{H}) \to \\ \to H^1(X,\mathcal{F}) \longrightarrow H^1(X,\mathcal{G}) \longrightarrow H^1(X,\mathcal{H}) \to \\ \to H^2(X,\mathcal{F}) \longrightarrow H^2(X,\mathcal{G}) \longrightarrow H^2(X,\mathcal{H}) \to \\ \to \dots \end{aligned}$$

- **Grothendieck Vanishing Theorem.** Se X é curva, então para todo feixe $\mathcal{F}$ sobre X e $n \geq 2$, $H^n(X,\mathcal{F}) = 0$;
- Se X é uma curva sobre um corpo algebricamente fechado k, então $H^0(X,\mathcal{O}_X) = k$;
- **Grupo de Picard.** O conjunto de classes de isomorfismo feixes $\mathcal{F}$ sobre um esquema X que possuem inverso com respeito à operação de produto tensorial (isto é, $\mathcal{G}$ tal que $\mathcal{F} \otimes \mathcal{G} = \mathcal{O}_X$) constituem um grupo, chamado de grupo de Picard de X e denotado por $\mathrm{Pic}(X)$. Ainda, dado $\mathcal{F} \in \mathrm{Pic}(X)$, $\mathcal{F}^{-1} = \mathcal{F}^\vee$ (dual de $\mathcal{F}$);
- **Morfismo de Div X em Pic X.** Seja X uma curva sobre um corpo k. Existe um morfismo $\mathrm{Div}\, X \to \mathrm{Pic}\, X$, $D \mapsto \mathcal{O}_X(D)$, de tal maneira que $\mathcal{O}_X(D)(X) = \{f \in k(X) \mid (f) + D \geq 0\} \cup \{0\}$;
- **Finitude.** Se X é uma curva sobre um corpo k e $D \in \mathrm{Div}(X)$, então todos os $H^i(X,\mathcal{O}_X(D))$ são k-espaços vetoriais de dimensão finita;
- **Dualidade de Serre + Divisores canônicos.** Se X é uma curva sobre um corpo algebricamente fechado, então existe uma classe de equivalência linear de divisores (chamados de divisores canônicos) tal que, para todo divisor canônico K e feixe $\mathcal{F}$ localmente livre existe um pareamento perfeito de espaços vetoriais

$$H^1(X,\mathcal{F}) \times H^0(X,\mathcal{F}^\vee \otimes_{\mathcal{O}_X} \mathcal{O}_X(K)) \longrightarrow k;$$

De posse desses fatos, será até fácil provar o Teorema de Riemann-Roch para esquemas:

Teorema 2.3.8 (Teorema de Riemann-Roch para esquemas)**.** Sejam C uma curva sobre um corpo algebricamente fechado k e K um divisor canônico em C. Então, para todo divisor D em C,

$$l(D) - l(K - D) = \deg D + 1 - g.$$

Antes de prová-lo, farei um comentário sobre a definição de gênero de um esquema, e outro com um resultado preliminar. Comecemos pelo comentário:

A noção de gênero perpassa diversas áreas da Matemática, então existem várias definições possíveis de gênero, e espera-se que quando mais de uma definição se aplique,

elas coincidam. No nosso caso, tomamos a definição 'original" importada do estudo de superfícies de Riemann: lá, o gênero de S costumeiramente é definido como a dimensão do espaço vetorial de 1-formas diferenciais em S. Trazendo para a linguagem esquemática (ou melhor, "curvática sobre um corpo algebricamente fechado"), temos um gênero definido por

$$g \stackrel{\text{def}}{=} \dim_k H^0(C, \omega_C).$$

Aqui, ω_C é um feixe chamado de feixe canônico da curva. É este o análogo esquemático do conjunto de formas diferenciais em uma superfície de Riemann compacta. No casoque estamos trabalhando, para todo feixe canônico K, tem-se $\omega_C = \mathcal{O}_C(K)$.

Passemos ao resultado preliminar:

Lema 2.3.9. Sejam C uma curva de gênero g sobre um corpo algebricamente fechado k e $D \geq 0$ um divisor. Então

$$\chi(\mathcal{O}_C(D)) = \deg D + 1 - g,$$

em que para um feixe $\mathcal{F}$, $\chi(\mathcal{F})$ é sua característica de Euler, definida por $\chi(\mathcal{F}) \stackrel{\text{def}}{=} \sum_{i \geq 0} (-1)^i \dim_k H^i(C, \mathcal{F})$ (quando esta soma fizer sentido, i.e. for finita).

Demonstração. Provaremos isso por indução em $\deg D$. O caso $\deg D = 0$ implica $D = 0$, afinal $D \geq 0$, e aí temos

$$\chi(\mathcal{O}_C) = \dim_k H^0(C, \mathcal{O}_C) - \dim_k H^1(C, \mathcal{O}_C) = 1 - g,$$

afinal pela Dualidade de Serre temos que $\dim_k H^1(C, \mathcal{O}_C) = \dim_k H^0(C, \mathcal{O}_C^\vee \otimes \mathcal{O}_C(K))$ para algum (qualquer,na verdade) divisor canônico K. Usando a lei de grupo de $\operatorname{Pic} X$, $\mathcal{O}_C^\vee \otimes \mathcal{O}_C(K) = \mathcal{O}_C(K) = \omega_C$ e assim $\dim_k H^1(C, \mathcal{O}_C) = g$.

Agora, suponha que o lema valha para D e seja $E \in C$ um ponto fechado. Provemos que o resultado vale para $D + E$. Temos a seguinte sequência exata curta:

$$0 \to \mathcal{O}_C(D) \longrightarrow \mathcal{O}_C(D + E) \longrightarrow k_E \to 0,$$

em que k_E é um feixe *skyscraper* sobre E. Como a característica de Euler é aditiva em sequências exatas curtas de feixes (por pura e simples Álgebra Linear), temos que

$$\chi(\mathcal{O}_C(D + E)) = \chi(\mathcal{O}_C(D)) + \chi(k_E).$$

Sendo k_E um feixe *skyscraper*, temos $\chi(k_E) = 1$: como dim $supp k_E = 0$, então $H^i(X, k_E) = 0$ para todo $i > 0$. Assim, $\chi(k_E) = \dim_k H^0(X, k_E) = \dim_k k = 1$. No entanto, nossa hipótese de indução é de que

$$\chi(\mathcal{O}_C(D)) = \deg D + 1 - g,$$

assim temos que $\chi(\mathcal{O}_C(D + E)) = \deg D + 1 - g + 1 = \deg(D + E) + 1 - g$, provando assim o lema. ∎

Esse lema, na verdade, prova alguns casos do Teorema de Riemann-Roch, como veremos na demonstração:

Demonstração do Teorema 2.3.8. Note que, para qualquer divisor D, temos

$$\mathcal{O}_C(D)^\vee \otimes \omega_C \simeq \mathcal{O}_C(-D) \otimes \mathcal{O}_C(K) \simeq \mathcal{O}_C(K-D).$$

Assim, usando a Dualidade de Serre, concluímos que

$$\begin{aligned}\chi(\mathcal{O}_C(D)) &= \dim_k H^0(C, \mathcal{O}_C(D)) - \dim_k H^1(C, \mathcal{O}_C(D)) \\ &= l(D) - \dim_k H^0(C, \mathcal{O}_C(D)^\vee \otimes \omega_C) \\ &= l(D) - \dim_k H^0(C, \mathcal{O}_C(K-D)) \\ &= l(D) - l(K-D).\end{aligned}$$

Portanto, o lema anterior garante que o Teorema de Riemann-Roch vale para divisores positivos. Provemos que ele vale para qualquer divisor por indução na quantidade de polos de D. Em outras palavras: Escrevendo $D = D_+ - D_-$, com $D_\pm \geq 0$ e $supp\, D_+ \cap supp\, D_- = \emptyset$, faremos indução em $\deg D_-$. O caso $\deg D_- = 0$ (isto é, $D_- = 0$) já foi provado, então seja $D = D_+ - D_-$ e suponha que o teorema vale para todos os divisores E com $\deg E_- < \deg D_-$. Seja $P \in C$ um ponto fechado no suporte de D_-, e ponha $E = D + P$, de forma que $E_- = D_- - P$ e o teorema vale para E. Pela mesma argumentação do lema anterior com o feixe *skyscraper* k_E, vê-se que

$$\chi(\mathcal{O}_C(E)) = \chi(\mathcal{O}_C(D)) + 1.$$

Como o teorema vale para E, temos

$$\begin{aligned}\chi(\mathcal{O}_C(D)) &= \chi(\mathcal{O}_C(E)) - 1 \\ &= \deg E + 1 - g - 1 \\ &= \deg D + 1 + 1 - g - 1 \\ &= \deg D + 1 - g.\end{aligned}$$

■

O mesmo corolário que vimos para superfícies de Riemann se aplica a esquemas. A demonstração consiste nas mesmas palavras, na mesma ordem, da demonstração do caso complexo, sem alteração nenhuma.

Corolário 2.3.10. O grau de qualquer divisor canônico em uma curva C de gênero g é $2g-2$. Portanto, se $\deg D \geq 2g-1$, então $l(D) = \deg D + 1 - g$.

3 Conjecturas de Weil, ou "Le Jardin des Hespérides"

Les pommes du jardin des Hespérides sont ces fameuses conjectures qu'André Weil énonce en 1949 (...).
- Pierre Cartier

No apêndice A deste trabalho, é evidenciado que a função Zeta de uma curva algébrica,

$$Z(C,t) \stackrel{\text{def}}{=} \exp\left(\sum_{r\geq 1} \frac{|C(\mathbb{F}_{q^r})|}{r} t^r\right),$$

contém muita informação quanto à quantidade de pontos racionais dessa curva. Afinal, os números $N_r = |C(\mathbb{F}_{q^r})|$ são a quantidade de pontos $\mathbb{F}_{q^r}$-racionais de C,de forma que a derivada logarítmica de $Z(C,t)$ é uma função geradora desses números:

$$\frac{d}{dt}\log Z(C,t) = \sum_{r\geq 1} N_r t^{r-1}.$$

Por exemplo:

Exemplo 3.1. Calculemos $Z(\mathbb{P}^1_{\mathbb{F}_q}, t)$. Uma análise combinatória agradavelmente leve nos garante que $|\mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_{q^r})| = q^r + 1$. Portanto, temos que

$$\begin{aligned}\sum_{r\geq 1} |\mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_{q^r})| t^{r-1} &= \sum_{r\geq 1} q^r t^{r-1} + \sum_{r\geq 1} t^{r-1} \\ &= q\frac{1}{1-qt} + \frac{1}{1-t}.\end{aligned}$$

Portanto, "integrando formalmente",

$$\sum_{r\geq 1} \frac{|\mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_{q^r})|}{r} t^r = -\log(1-qt) - \log(1-t) = \log\left(\frac{1}{(1-t)(1-qt)}\right),$$

donde

$$Z(\mathbb{P}^1_{\mathbb{F}_q}, t) = \frac{1}{(1-t)(1-qt)}.$$

Agora, como toda curva é um recobrimento de $\mathbb{P}^1$, graças ao Teorema de Normalização de Noether (c.f. [Tengan and Borges, 2015], capítulo 9§1, página 232), faz sentido esperar que a função Zeta de uma curva não seja extremamente diferente dessa função. Especificamente, trataremos as seguintes conjecturas:

Conjecturas de Weil. Seja C uma curva sobre um corpo finito $\mathbb{F}_q$. Então:

- **Racionalidade** A função Zeta de C é racional, e tem a seguinte forma:
$$Z(C,t) = \frac{L(t)}{(1-t)(1-qt)},$$
com $L \in \mathbb{Z}[t]$ de grau $2g$, em que g é o gênero da curva.

- **Hipótese de Riemann** Os zeros, em $\mathbb{C}$, da função Zeta de C têm valor absoluto $q^{-1/2}$. Em outras palavras, fatorando-se L em $\mathbb{C}$ como
$$L(t) = \prod_{i=1}^{2g}(1-\alpha_i t),$$
temos $|\alpha_i| = q^{1/2}$.

A maior parte deste capítulo será dedicada à demonstração da Hipótese de Riemann. Começamos pela parte "fácil", a demonstração da racionalidade da função Zeta. Ela toma vantagem do fato que, para fins de funções zeta, podemos trocar "curva algébrica" por "corpo de função", sem nenhuma mudança, de forma que a demonstração da racionalidade da função Zeta se dará no contexto de corpos de funções (para os principais pontos dessa linguagem, c.f. o apêndice A deste trabalho). Em seguida, passaremos à prova da Hipótese de Riemann: é esta a demonstração principal deste trabalho. Ela se baseia em encontrar uma função meromorfa na curva, que se anule nos pontos $\mathbb{F}_q$-racionais, e tenha polos controlados. Usando-se o fato que funções meromorfas possuem a mesma quantidade de zeros e polos, conseguiremos uma cota superior para $|C(\mathbb{F}_q)|$ que garantirá a Hipótese de Riemann. A título de aplicação, principalmente do produto fibrado, depois da racionalidade da função Zeta veremos brevemente a construção dos morfismos de Frobenius em um esquema. Depois disso, veremos a demonstração de Bombieri da cota superior para $|C(\mathbb{F}_q)|$. Em seguida, veremos como a partir dessa cota superior obter uma cota inferior para $|C(\mathbb{F}_q)|$, e assim provar a Hipótese de Riemann. Sem mais delongas:

3.1 Racionalidade da Função Zeta

Aqui, usaremos a definição da função Zeta de uma curva via seu corpo de funções. Para mais detalhes sobre como se dá essa tradução, c.f. o apêndice A deste trabalho. Usando esse maquinário, a demonstração da racionalidade da função Zeta se torna bastante direta. Lembremos de algumas definições. Seja K/k um corpo de funções.

- O grupo de divisores de K é definido comoo grupo abeliano livre gerado pelos ideais maximais de anéis de valorização discreta contidos em$K$ e contendo k (este conjunto é denotado por $\mathbb{P}_K$). Este grupo é denotado porDiv K, e temos um morfismo óbvio $\deg \operatorname{Div} K \to \mathbb{Z}$;

- Dado $f \in K^*$,podemos definir $(f) = \operatorname{div} f \stackrel{\text{def}}{=} \sum_{P \in \mathbb{P}_K} \operatorname{ord}_P f \in \operatorname{Div} K$, que dá origem a um morfismo $\operatorname{div}\colon K^* \to \operatorname{Div}^0 K \stackrel{\text{def}}{=} \ker \deg$;
- O grupo de classe $\mathcal{C}_K$ de K é definido como o conúcleo de $\operatorname{div}\colon K^* \to \operatorname{Div} K$;
- O número de classe de K (normalmente denotado por h_K) é definido como a quantidade de elementos do conúcleo de $\operatorname{div}\colon K^* \to \operatorname{Div}^0 K$ (sim,$h - K$ é sempre finito);
- Dado um divisor A, podemos considerar o espaço vetorialsobre k $L(A) \stackrel{\text{def}}{=} \{f \in K^* \mid (f) + A \geq 0\} \cup \{0\}$. A dimensão $\dim A$ deste espaço é sempre finita, e descrita pelo Teorema de Riemann-Roch para corpos de funções;
- Geometricamente, se K é o corpo de funções de uma curva C definida sobre k, então $\mathcal{C}_K \simeq \operatorname{Pic} C$ e $\mathcal{C}_K^0 \simeq \operatorname{Pic}^0 C$.

Comecemos enunciando o resultado principal desta seção:

Teorema 3.1.1. Seja K/k um corpo de funções e assuma que existe divisor de grau 1 em K. Então a função Zeta de K é da forma

$$Z(K,t) = \frac{1}{(1-t)(1-qt)},$$

se o gênero g de K for nulo[1], e caso $g \geq 1$, $Z(K,t) = F(t) + G(t)$, em que

$$F(t) = \frac{1}{q-1} \sum_{\substack{\overline{C} \in \mathcal{C}_K \\ 0 \leq \deg C \leq 2g-2}} q^{l(C)} t^{\deg C}$$

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

Note que tanto se $g = 0$ quanto se $g \geq 1$, $Z(K,t)$ é uma função racional, da forma

$$Z(K,t) = \frac{P(t)}{(1-t)(1-qt)}, \tag{3.1}$$

em que P é um polinômio com coeficientes racionais e de grau igual a $2g$. Ainda, como

$$P(t) = (1-t)(1-qt)\, Z(K,t) \ \in \mathbb{Z}[[t]] \cap \mathbb{Q}[t],,$$

tem-se que $P \in \mathbb{Z}[t]$. Como, evidentemente, $P(0) = 1$, quando $g \geq 1$ podemos fatorar P como

$$P(t) = \prod_{i=1}^{2g} (1 - \alpha_i t),$$

[1] Note que isso faz todo sentido: o gênero é invariante por birracionalidade, então não é de se surpreender que toda curva de gênero zero possua a mesma função zeta que $\mathbb{P}^1$.

com todos os α_i não-nulos. Ao longo das próximas sessões nos ocuparemos de provar a hipótese de Riemann: $|\alpha_i| = \sqrt{q}$ para todo i. Por hora, vamos nos ater a verificar a racionalidade da função Zeta. Antes, relembremos que definimos os coeficientes da série da função Zeta de um corpo de funções como

$$A_n \stackrel{\text{def}}{=} |\{A \in \operatorname{Div} K \mid A \geq 0 \,\text{e}\, \deg A = n\}|.$$

Demonstração da Racionalidade da Função Zeta. Usaremos o lema A.9. Usando a definição via corpos de função, a demonstração da racionalidade é bastante *straightforward* no caso de gênero nulo: tem-se

$$\begin{aligned} Z(K,t) &= \sum_{n\geq 0} A_n t^n = \frac{h_K}{q-1} \sum_{n\geq 0} (q^{n+1}-1)t^n \\ &= \frac{h_K}{q-1}\left(q\sum_{n\geq 0}(qt)^n - \sum_{n\geq 0} t^n\right) \\ &= \frac{h_K}{q-1}\left(\frac{q}{1-qt} - \frac{1}{1-t}\right). \end{aligned}$$

Basta agora provar que o número de classe de um corpo de funções de gênero zero é um, isto é, se $A \in \operatorname{Div}(K)$ tem grau zero, então $A = div\, x$ para algum $x \in K^\times$. Isso é consequência do Teorema de Riemann-Roch para corpos de funções: como $2g-2 < 0$, temos $\dim A = 1$, isto é, existe $0 \neq x \in L(A)$ (ou seja, $div\, x \geq -A$). Como $\deg div\, x = 0$, segue que $div\, x = -A$, donde $A = div\, x^{-1}$. Ou seja,

$$\begin{aligned} Z(K,t) &= \frac{1}{q-1}\left(\frac{q}{1-qt} - \frac{1}{1-t}\right) \\ &= \frac{1}{q-1}\left(\frac{q(1-t)-(1-qt)}{(1-qt)(1-t)}\right) = \frac{1}{q-1}\left(\frac{q-1}{(1-t)(1-qt)}\right) \\ &= \frac{1}{(1-t)(1-qt)}. \end{aligned}$$

Provemos agora o caso $g \geq 1$. Usaremos aqui o lema A.9, bem como o Teorema de

Riemann-Roch para corpos de funções:

$$\begin{aligned}
Z(K,t) &= \sum_{n\geq 0} A_n t^n = \sum_{0\leq n\leq 2g-2} A_n t^n + \sum_{n>2g-2} A_n t^n \\
&= \sum_{\substack{\overline{C}\in\mathcal{C}_K \\ 0\leq \deg C\leq 2g-2}} |\{A\in\overline{C} \mid A\geq 0\}| t^{\deg C} + \sum_{n\geq 2g-1} \frac{h}{q-1}(q^{n+1-g}-1)t^n \\
&= \sum_{\substack{\overline{C}\in\mathcal{C}_K \\ 0\leq \deg C\leq 2g-2}} \frac{1}{q-1}(q^{l(C)}-1)t^{\deg C} + \sum_{n\geq 2g-1} \frac{h}{q-1}(q^{n+1-g}-1)t^n \\
&= F(t) - \sum_{0\leq n\leq 2g-2} \frac{h}{q-1}t^n + \frac{h}{q-1}\sum_{n\geq 2g-1}(q^{n+1-g}-1)t^n \\
&= F(t) + \frac{h}{q-1}\left(q^{1-g}\sum_{n\geq 2g-1} q^n t^n - \sum_{n\geq 0} t^n\right) \\
&= F(t) + \frac{h}{q-1}\left(q^g t^{2g-1}\frac{1}{1-qt} - \frac{1}{1-t}\right) \\
&= F(t) + G(t).
\end{aligned}$$

■

Uma consequência interessante da racionalidade da função Zeta, nos termos em que enunciamo-la, é que conhecendo seu denominador,quando apresentada da maneira como em (3.1), sabemos precisamente quantos pontos $\mathbb{F}_q$-racionais nossa curva possui. Afinal, sabemos que se C é uma curva sobre $k=\mathbb{F}_q$ e $K=k(C)$ seu corpo de funções, então $|C(\mathbb{F}_q)| = A_1$, em que $A_1 = |\{A\in \operatorname{Div} K \mid A\geq 0 \text{ e } \deg A = 1\}|$. Assim, da igualdade

$$P(t) = \prod_{i=1}^{2g}(1-\alpha_i t) = (1-t)(1-qt)\sum_{n\geq 0} A_n t^n,$$

o coeficiente de grau 1 de P é, por um lado, igual a $-\sum \alpha_i$ e, por outro, $A_1 - q - 1$, donde concluímos que

$$|C(\mathbb{F}_q)| - (q+1) = -\sum_{i=1}^{2g}\alpha_i.$$

Ainda, é válido um resultado análogo para extensões de $\mathbb{F}_q$. Sendo a função Zeta de C (ou melhor, de K) escrita como

$$Z(K,t) = \frac{\prod_{i=1}^{2g}(1-\alpha_i t)}{(1-t)(1-qt)} = \exp\left(\sum_{m\geq 1}\frac{N_m}{m}t^m\right),$$

podemos usar essas duas expressões da função Zeta para concluir que

$$t\frac{d}{dt}\log Z(K,t) = \sum_{m\geq 1} N_m t^m = \sum_{m\geq 1}\left(1+q^m - \sum_{i=1}^{2g}\alpha_i^m\right)t^m,$$

e assim, comparando-se os coeficientes dessas duas séries, temos que

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r.$$

Ou seja:

$$|C(\mathbb{F}_{q^r})| = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r.$$

Esse fato facilita muito nossa vida. Vejamos isso com um

Exemplo 3.1.2. Considere a quártica de Klein sobre $\mathbb{F}_5$:

$$C = \text{Proj}\, \frac{\mathbb{F}_5[x,y,z]}{(x^3y + y^3z + z^3x)}.$$

O gênero de C é $g = 3$, de modo que seu polinômio L tem grau 6 e pode ser escrito como

$$L(t) = \prod_{i=1}^{3} (1 - \alpha_i t)(1 - \overline{\alpha_i} t), .$$

com $\alpha_k = a_k + -b_k$.

Acabamos de verificar que

$$N_r = 5^r + 1 - 2\,\Re\left(\alpha_1^r + \alpha_2^r + \alpha_3^r\right).$$

Podemos calcular alguns valores de N_r, para r pequeno, usando um *software* como PARI-GP: temos

$$\begin{aligned} N_1 &= 6 \\ N_2 &= 26 \\ N_3 &= 126 \end{aligned}$$

e as relações entre as raízes de L e N_r se tornam

$$\begin{cases} a_1 + a_2 + a_3 = 0 \\ a_1^2 + a_2^2 + a_3^2 - (b_1^2 + b_2^2 + b_3^3) = 0 \\ a_1^3 + a_2^3 + a_3^3 - 3(a_1 b_1^2 + a_2 b_2^2 + a_3 b_3^3) = 0 \end{cases}$$

Assumindo a Hipótese de Riemann, isto é, supondo que $a_j^2 + b_j^2 = 5$, as relações entre os a_j e os N_r se tornam, ao substituirmos $b_j^2 = 5 - a_j^2$,

$$\begin{cases} a_1 + a_2 + a_3 = 0 \\ a_1^2 + a_2^2 + a_3^2 = \dfrac{15}{2} \\ a_1^3 + a_2^3 + a_3^3 = 0 \end{cases}$$

O que faremos agora é construir um polinômio $p(t)$ cúbico com raízes a_1, a_2 e a_3, de forma que seus coeficientes sejam

$$p(t) = t^3 - S_1(a_1, a_2, a_3)^2 t + S_2(a_1, a_2, a_3)t - S_3(a_1, a_2, a_3),$$

em que S_j são os polinômios simétricos elementares. Note que temos que $S_1 = S_1(a_1, a_2, a_3) = 0$. Como $S_1^2 = a_1^2 + a_2^2 + a_3^2 + 2S_2$, temos que $S_2 = -\frac{15}{4}$. E, por fim, como

$$0 = S_1^2 = 6a_1a_2a_3,$$

temos que o polinômio mônico com raízes a_1, a_2 e a_3 é

$$p(t) = t^3 - \frac{15}{4}t = x\left(x - \frac{\sqrt{15}}{2}\right)\left(x + \frac{\sqrt{15}}{2}\right),$$

de modo que

$$\begin{aligned} a_1 &= 0 \\ a_2 &= \frac{\sqrt{15}}{2} \\ a_3 &= -\frac{\sqrt{15}}{2} \end{aligned}$$

Por fim, como $(1 - \alpha_j t)(1 - \overline{\alpha_j} t) = 1 - 2a_j t + 5t^2$, o polinômio L da quártica de Klein é

$$\begin{aligned} L(t) &= (1 + 5t^2)(1 + \sqrt{15}t + 5t^2)(1 - \sqrt{15}t + 5t^2) \\ &= (1 + 5t^2)((1 + 5t^2)^2 - 15t^2). \end{aligned}$$

3.2 φrobenii

Seja $k = \mathbb{F}_q$ um corpo finito de característica p. Em característica positiva vale o "sonho de todo estudante de Álgebra"

$$(a + b)^p = a^p + b^p,$$

para todo $a, b \in k$. Assim, o mapa de Frobenius de ordem q, $x \mapsto x^q$, é um endomorfismo. E mais: como k é finito e esse mapa é injetor, ele é automaticamente sobrejetor, ou seja um automorfismo.

E é claro que esse mapa é bem-definido para qualquer corpo de característica p, digamos, um fecho algébrico $\overline{k}$ fixo de k. Por que considerar essa versão estendida do mapa de Frobenius? Ora, note que pelo Teorema de Lagrange, para todo $a \in \mathbb{F}_q$,

$$a^q = a,$$

de forma que $x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$. Ou seja, os pontos fixos do mapa de Frobenius de ordem q em $\overline{k}$ são precisamente os pontos de $\mathbb{F}_q$. Podemos usar esse fato para substituir o problema de encontrar pontos $\mathbb{F}_q$-racionais de uma variedade pelo de achar pontos fixos de um mapa. Se $C \subseteq \mathbb{P}^2_{\overline{k}}$ é uma curva dada pela equação $f(x, y, z) = 0$ (no sentido clássico, isto é, um fechado irredutível do espaço projetivo), então podemos definir um mapa

$$\begin{aligned} \mathbb{P}^2_{\overline{k}} &\longrightarrow \mathbb{P}^2_{\overline{k}} \\ (a\colon b\colon c) &\longmapsto (a^q\colon b^q\colon c^q) \end{aligned}$$

que fixa exatamente os pontos de $\mathbb{P}^2_{\overline{k}}$ com coordenadas em $\mathbb{F}_q$. Ainda, esse mapa leva C não em C, mas em $C^{(q)}$, a curva em $\mathbb{P}^2_{\overline{k}}$ dada por $f^{(q)}(x, y, z) = 0$, em que $f^{(q)}$ é o polinômio obtido ao elevar cada coeficiente de f à q-ésima potência[2]. Assim, a questão de encontrar pontos $\mathbb{F}_q$-racionais de C se reduz à questão de achar pontos fixos por este mapa de Frobenius. Nesta seção, veremos como exatamente esse mapa é construído para esquemas.

Para simplicidade consideraremos apenas o caso plano afim, porém é fácil ver, pela construção de esquemas e de produtos fibrados, que o caso afim é suficiente.

Seja $X = \operatorname{Spec} \dfrac{\overline{\mathbb{F}_q}[x, y]}{(f)}$ uma curva afim, um esquema sobre $K = \overline{\mathbb{F}_q}$. O mapa de Frobenius de ordem q, $K \to K$, induz um morfismo de esquemas na direção contrária, nos dando os seguintes diagramas, um em **Aff.Sch** e o outro em **CRing**:

$$\begin{array}{ccc} & & X \\ & & \downarrow \\ \operatorname{Spec} K & \longrightarrow & \operatorname{Spec} K \end{array} \qquad\qquad \begin{array}{ccc} & & \dfrac{K[x, y]}{(f)} \\ & & \uparrow \\ K & \longleftarrow & K \end{array}$$

Sabemos que o produto fibrado $X^{(q)} \overset{\text{def}}{=} X \times_{\operatorname{Spec} K} \operatorname{Spec} K$ é isomorfo ao esquema afim $\operatorname{Spec}\left(\dfrac{K[x, y]}{(f)} \otimes_K K\right)$. A estrutura deste produto tensorial não é muito óbvia, graças à estrutura de K-álgebra que demos a K, então para evitar confusão escreveremos L para nos referir a K como uma K-álgebra cuja estrutura de álgebra vem do morfismo de Frobenius. O diagrama à direita então é

$$\begin{array}{ccc} & & \dfrac{K[x, y]}{(f)} \\ & & \uparrow \\ L & \longleftarrow & K \end{array}$$

[2] Note que se $f \in \mathbb{F}_q[x, y, z]$, então $f^{(q)} = f$ e o mapa de Frobenius leva C em C.

Verifiquemos que nossa notação $X^{(q)}$ condiz com a definição dada na discussão ao começo deste seção, isto é, que $X^{(q)}$ é uma curva afim dada pelo polinômio $f^{(q)}$. Seja

$$\begin{aligned}\xi\colon \frac{K[x,y]}{(f)} \otimes_K L &\longrightarrow \frac{L[x,y]}{(f^{(q)})}\\ \overline{g} \otimes a &\longmapsto \overline{ag^{(q)}}\end{aligned}$$

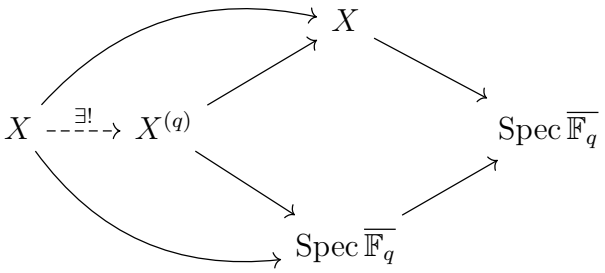
Provando que ξ está bem-definida, seu inverso será óbvio e postanto será um isomorfismo de K-álgebras. A única coisa que precisamos checar é que o morfismo

$$\begin{aligned}K[x,y] \otimes_K L &\longrightarrow L[x,y]\\ g \otimes a &\longmapsto ag^{(q)}\end{aligned}$$

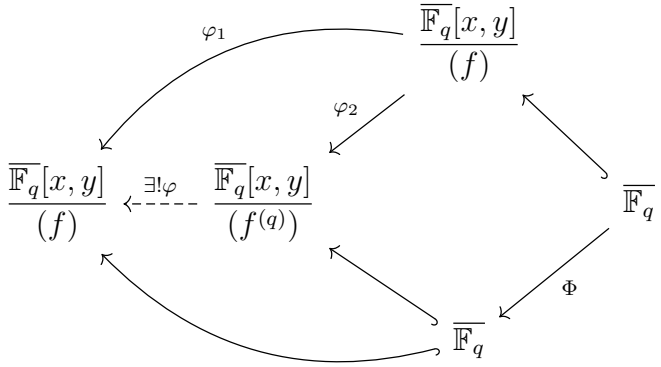
leva $f \otimes 1$ em $f^{(q)}$. Por linearidade, basta observar que $ax^iy^j \otimes 1 = x^iy^j \otimes a^q \mapsto a^q x^i y^j$. Portanto o mapa ξ dado acima é um isomorfismo e

$$X^{(q)} \simeq \operatorname{Spec} \frac{\overline{\mathbb{F}_q}[x,y]}{(f^{(q)})}.$$

Isso confirma que estamos no caminho certo, e que escolhemos uma "boa" definição de $X^{(q)}$. Nossa próxima tarefa é definir o morfismo de Frobenius que eleva toda coordenada em K à q-ésima potência. Como $X^{(q)}$ é um produto fibrado, estamos inclinados a considerar o seguinte diagrama fibrado

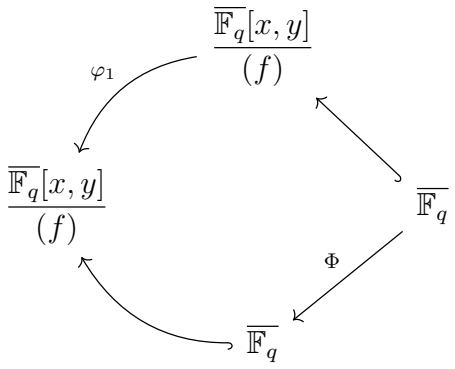


Este diagrama é, na melhor das hipóteses, ambíguo. Qual é a flecha $X \to X$? É a identidade? E a flecha $X \to \operatorname{Spec} \overline{\mathbb{F}_q}$, é o morfismo estrutural? Para elucidar essas questões, consideremos o diagrama dual em **CRing** e comecemos a dar nome aos bois:

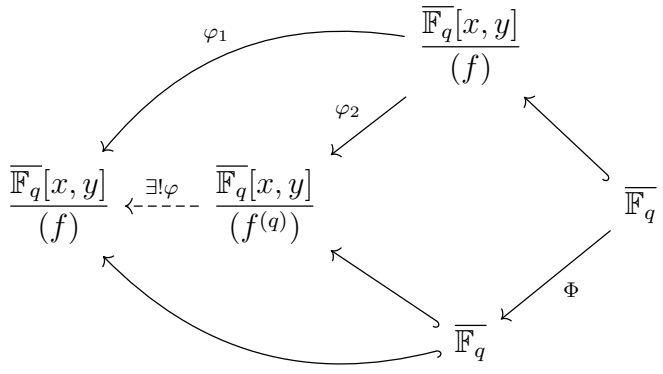


Nesse diagrama, as flechas "$\hookrightarrow$" são inclusões, e Φ é o morfismo de Frobenius em $\overline{\mathbb{F}_q}$. Precisamos, antes de encontrar φ, entender quem devem[3] ser os morfismos φ_1 e φ_2. O mapa φ_2 é facilmente conhecido, da nossa demonstração do isomorfismo $\dfrac{K[x,y]}{(f)} \otimes_K L \simeq \dfrac{L[x,y]}{(f^{(q)})}$: $\varphi_2(ax^iy^j) = a^q x^i y^j$.

Claramente se $a \in \overline{\mathbb{F}_q}$, devemos ter $\varphi_1(a) = a^q$, afinal o diagrama



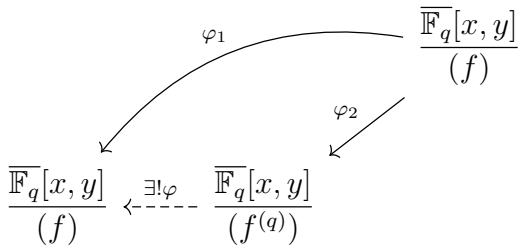
é comutativo. Agora, temos uma liberdade real em como escolher φ_1: não estamos limitados a uma única φ_1 possível, e naturalmente diferentes escolhas de φ_1 vão originar diferentes morfismos $\Phi\colon X \to X^{(q)}$. Escolhamos então φ_1 como $\varphi_1(g) = g^q$.[4] Agora, voltemos a considerar o diagrama comutativo em **CRing**, agora sabendo quem são os envolvidos:



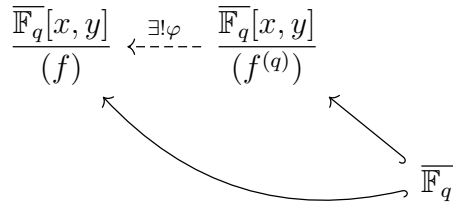
Como, necessariamente, o diagrama

[3] No sentido "quem devem ser φ_1 e φ_2 para que o morfismo induzido seja o que desejamos".

[4] Veremos num futuro breve que esta é uma escolha acertada (isto é, que induz um "morfismo de Frobenius em X" do jeito que esperaríamos). Por hora, peço a paciência do leitor em aceitar uma definição um pouco arbitrária.



comuta, devemos ter $\varphi(x) = x^q$ e $\varphi(y) = y^q$. Por outro lado a comutatividade do diagrama



nos impõe que, para $a \in \overline{\mathbb{F}_q}$, $\varphi(a) = a$. Assim, o morfismo φ que induz localmente o morfismo de $\overline{\mathbb{F}_q}$-álgebras correspondente a $X \to X^{(q)}$ é

$$\begin{aligned} \varphi\colon \frac{\overline{\mathbb{F}_q}[x,y]}{(f^{(q)})} &\longrightarrow \frac{\overline{\mathbb{F}_q}[x,y]}{(f)} \\ \overline{x} &\longrightarrow \overline{x}^q \\ \overline{y} &\longrightarrow \overline{y}^q \end{aligned}$$

Note que $\overline{0} = \overline{f^{(q)}} \mapsto \overline{f^q} = \overline{0}$, ou seja, este mapa φ está bem-definido.

Definição 3.2. Seja X um esquema sobre K. O morfismo de Frobenius absoluto de ordem q em X é o morfismo $\mathrm{Frob}_X\colon X \to X$ induzido, em qualquer carta afim $\operatorname{Spec} A \underset{\circ}{\subseteq} X$, por $a \mapsto a^q$. O morfismo de Frobenius relativo de ordem q em X é o morfismo $\mathrm{Frob}_{X/K}\colon X \to X^{(q)}$ que induzimos nos diagramas acima.

Observação 1. Apesar de termos visto em detalhes apenas o caso afim, um argumento simples de localização e colagem mostra que esses morfismos $a \mapsto a^q$ concordam nas interseções de cartas afins em um esquema X, portanto são colados de maneira única para dar o Frobenius absoluto em X.

Observação 2. Essa construção pode ser feita não apenas para esquemas sobre um fecho algébrico de um corpo finito, mas para esquemas sobre um esquema de caracterísica p, que são esquemas S em que, para toda carta afim $\operatorname{Spec} A \underset{\circ}{\subseteq} S$, $p \cdot 1_A = 0_A$. Para mais detalhes, c.f. [Liu, 2002], capítulo 3§2.4.

Verifiquemos que o mapa de Frobenius relativo age nos pontos K-racionais de X da maneira que esperamos, isto é, elevando todas as coordenadas à q-ésima potência.

Como antes, vamos considerar apenas o caso plano e afim $X = \operatorname{Spec} \dfrac{K[x,y]}{(f)}$, $K = \overline{\mathbb{F}_q}$. O mapa de anéis correspondendo ao Frobenius relativo é, como vimos,

$$\begin{aligned} \operatorname{Frob}_{X/K} \colon \frac{\overline{\mathbb{F}_q}[x,y]}{(f^{(q)})} &\longrightarrow \frac{\overline{\mathbb{F}_q}[x,y]}{(f)} \\ \overline{x} &\longmapsto \overline{x}^q \\ \overline{y} &\longmapsto \overline{y}^q \end{aligned}$$

Portanto, se $(x-a, y-b)$ é um ponto fechado de $\operatorname{Spec} \dfrac{\overline{\mathbb{F}_q}[x,y]}{(f^{(q)})}$, então $\Phi(\overline{x}-a^q) = \overline{x}^q - a^q = (\overline{x}-a)^q \in (\overline{x}-a, \overline{y}-b)$, e similarmente $\operatorname{Frob}_{X/K}(\overline{y}-b^q) \in (\overline{x}-a, \overline{y}-b)$, dando-nos que $(\overline{x}-a^q, \overline{y}-b^q) \subseteq \Phi^{-1}(\overline{x}-a, \overline{y}-b)$. Por maximalidade, essa inclusão é uma igualdade e para qualquer ponto $\overline{\mathbb{F}_q}$-racional de X,

$$\operatorname{Frob}_{X/K}(\overline{x}-a, \overline{y}-b) = (\overline{x}-a^q, \overline{y}-b^q).$$

Note que se tivéssemos começado considerando uma curva sobre $\mathbb{F}_q$, isto é, $f \in \mathbb{F}_q[x,y]$, então $f^{(q)} = f$, e o morfismo de Frobenius relativo é um endomorfismo de X.

3.3 Stepanov-Bombieri

Nesta seção estabeleceremos uma cota superior para a quantidade de pontos racionais de uma curva. A demonstração aqui presente foi criada por Enrico Bombieri, em [Bombieri, 1974], generalizando uma técnica introduzida por Sergei Stepanov em [Stepanov, 1969]. Seu mérito está em ter simplificado radicalmente a demonstração da Hipótese de Riemann, reduzindo-a a Álgebra Linear e colocando-a ao alcance, por exemplo, de um trabalho de conclusão de curso. Inclusive, na demonstração aqui apresentada foram feitas ainda mais algumas simplificações que não aparecem no artigo original de Bombieri.

O coração da prova está em encontrar uma função meromorfa f que possua polos controlados e apenas em um ponto $\mathbb{F}_q$-racional fixo de C, e se anule em todos os outros pontos de $C(\mathbb{F}_q)$. Assim, usando o fato que f possui o mesmo número de zeros e polos, poderemos concluir que

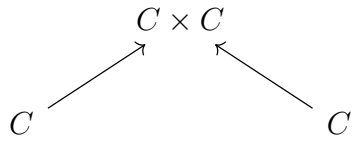
$$|C(\mathbb{F}_q)| - 1 \leq (f)_0 = (f)_\infty \leq \text{ algo "bom"},$$

dando-nos a cota superior $|C(\mathbb{F}_q)| \leq 1+$ algo "bom". Para encontrar tal f, usaremos basicamente Álgebra Linear e o Teorema de Riemann-Roch. Moralmente, o que faremos é o seguinte: seja C uma curva sobre $\mathbb{F}_q$. Mediante uma mudança de base, consideraremos que C é um esquema sobre $\overline{\mathbb{F}_q}$, com o morfismo de Frobenius relativo de ordem q sendo um endomorfismo em C. Denote-o por Φ. Note que os pontos $\mathbb{F}_q$-racionais de C são

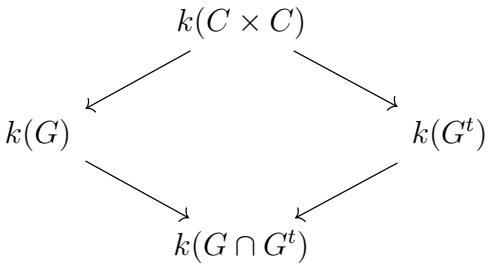
precisamente os pontos fixos de Φ. Considere agora o "gráfico" e o "gráfico transposto" de Φ,

$$\begin{aligned} G\colon C &\longrightarrow C \times C \\ a &\longmapsto (a, \Phi(a)) \\ G^t\colon C &\longrightarrow C \times C \\ a &\longmapsto (\Phi(a), a) \end{aligned}$$

Note que quando os dois gráficos se cruzam, isto é, se $G(a) = G^t(b)$ para dois pontos $a, b \in C$, então a e b são pontos fixos de Φ^2, portanto $a, b \in C(\mathbb{F}_{q^2})$. Assim, na realidade, para contar pontos $\mathbb{F}_q$-racionais, vale a pena considerar q como potência par de p, possuindo então o morfismo de Frobenius relativo de ordem q uma "raiz quadrada", $\sqrt{\Phi}$. Consideremos agora que G e G^t são o "gráfico" e o"gráfico transposto" de $\sqrt{\Phi}$, de forma que $G \cap G^t = C(\mathbb{F}_q)$. Temos o seguinte diagrama:



E, ao considerarmos G e G^t como "curvas na superfície $C \times_{\overline{\mathbb{F}_q}} C$", temos (intuitivamente apenas) o seguinte diagrama de "corpos de funções" (com as setas sendo apenas restrições)



Lembre de nosso plano: queremos uma função que se anule nos pontos $\mathbb{F}_q$-racionais da curva. Porém, "$k(G \cap G^t) = k(C(\mathbb{F}_q))$", ou seja, queremos uma função em $k(C \times C)$, não identicamente nula, que tenha imagem zero pela composição das setas. Garantiremos isso provando que existe $f \in k(C \times C)$ que, restrita a G, não é zero, porém o é restrita a G^t.

Suponha que $C(\mathbb{F}_q) \neq \emptyset$ (caso contrário, a cota superior vale trivialmente). Seja P_0 um ponto $\mathbb{F}_q$-racional de C, e ponha

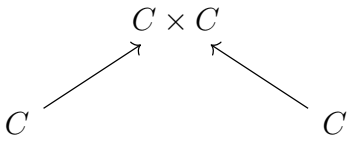
$$R_m \stackrel{\text{def}}{=} L(m \cdot P_0) = \{f \in k(C) \mid (f) + m \cdot P_0 \geq 0\} \cup \{0\},$$

para $m \in \mathbb{N}$.

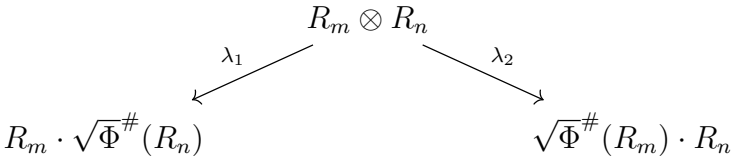
Podemos fazer algumas afirmações sobre os espaços R_m, todas ou óbvias ou consequências formais do Teorema de Riemann-Roch:

- $\dim R_{m+1} - \dim R_m \leq 1$;
- $m + 1 - g \leq \dim R_m \leq m + 1$, e se $m \geq 2g - 1$, então $\dim R_m = m + 1 - g$;
- $\sqrt{\Phi}^{\#}(R_m) \subseteq (R_m)^{\sqrt{q}} \subseteq R_{m\sqrt{q}}$.[5]

Moralmente, $k(C) = k(C) \otimes k(C)$, e a restrição induzida pelo "gráfico" de $\sqrt{\Phi}$ é simplesmente a composição com $\sqrt{\Phi}$ na segunda coordenada, analogamente para o "gráfico transposto". Em outras palavras, o diagrama



induz (heuristicamente) um diagrama



Aqui, temos $\lambda_1(f \otimes g) = f\sqrt{\Phi}^{\#}(g)$ e $\lambda_2(f \otimes g) = \sqrt{\Phi}^{\#}(f)g$.

Agora, querendo uma função que se anule no "gráfico", porém não no "gráfico transposto", vamos garantir que existe um morfismo $R_m \cdot \sqrt{\Phi}^{\#}(R_n) \to \sqrt{\Phi}^{\#}(R_m) \cdot R_n$ com núcleo não-trivial. Para isso, precisaremos do seguinte

Lema 3.3.1. Se $m < \sqrt{q}$, então λ_1 é injetor.

Demonstração. Consideremos uma base de R_m formada por elementos $f_1, \ldots, f_d$ tais que as ordens dos f_k em P_0 sejam todas distintas. Essa base pode ser obtida de maneira indutiva: suponha que tenhamos $f_1 \in R_1 \subseteq R_m$. Então ou $R_2 = R_1$ ou existe $f_2 \in R_2$ com $\operatorname{ord}_{P_0} f_2 = 2$. No segundo caso, que é o caso um pouco problemático, ou $R_3 = R_2 = R_1$ ou existe $f_3 \in R_3$ com $\operatorname{ord}_{P_0} f_3 = 3$. E assim por diante até termos a dita base. Similarmente, tomemos uma base de R_n formada por elementos $g_1, \ldots g_r$ tais que as ordens dos g_j em P_0 sejam todas distintas. Então os elementos $\lambda_1(f_k \otimes g_j) = f_k\sqrt{\Phi}^{\#}(g_j)$ são linearmente independentes: afinal, $\operatorname{ord}_{P_0} f_k\sqrt{\Phi}^{\#}(g_j) = \operatorname{ord}_{P_0} f_k + \sqrt{q}\operatorname{ord}_{P_0} g_j$, e agora é uma afirmação simples de aritmética: temos números $m_1, \ldots, m_d, n_1, \ldots, n_r \in \mathbb{N}$ tais que $0 \leq m_k \leq \sqrt{q}$ para todo k, os m_k todos distintos entre si, idem para os n_j. A afirmação em questão é que os números $m_k + n_j\sqrt{q}$ são todos distintos entre si. Isso é

[5] Aqui cabe a seguinte observação: no segundo capítulo, muito falamos sobre a heurística de "valor de função em um ponto", e "composição com funções suaves". Aqui essa heurística adquire um significado preciso, nas linhas de "$g \circ f = f^{\#}(g)$". Verificar o sentido preciso dessa igualdade é um exercício de abrir definições.

trivialmente verdadeiro: se $m_k + n_j\sqrt{q} = m_{k'} + n_{j'}\sqrt{q}$, então $|m_k - m_{k'}| = |n_j - n_{j'}|\sqrt{q}$, e como $0 \leq |m_k - m_{k'}| \leq m < \sqrt{q}$, temos $|m_k = m_{k'}| = |n_j - n_{j'}| = 0$, e assim $k = k'$ e $j = j'$. Finalmente, então, os elementos $\lambda_1(f_k \otimes g_j)$ são linearmente independentes, e assim temos λ_1 injetor. ■

Considere então a composição

$$\lambda\colon \lambda_1(R_m \otimes R_n) \longrightarrow R_m \otimes R_n \longrightarrow \sqrt{\Phi}^{\#}(R_m) \cdot R_n \subseteq R_{m\sqrt{q}+n}.$$

Pelo lema 3.3.1, a dimensão do domínio de λ é, no mínimo, $(m+1-g)(n+1-g)$. Ainda, a dimensão do contradomínio de λ, supondo $m, n \geq g$, é igual a $m\sqrt{q}+n+1-g$. Portanto, se conseguirmos garantir que

$$(m+1-g)(n+1-g) > m\sqrt{q}+n+1-g,$$

teremos que $\ker\lambda \neq \{0\}$. Agora, seja $0 \neq F = \sum_i f_i \cdot g_i \circ \sqrt{\Phi} \in \ker\lambda$. Então, para um $x \in C(\mathbb{F}_q)$, $x \neq P_0$, temos

$$\begin{aligned} F(x) &= \sum_i f_i(x) \cdot g_i(\sqrt{\Phi}(x)) = \sum_i f_i(\sqrt{\Phi}(\sqrt{\Phi}(x))) \cdot g_i(\sqrt{\Phi}(x)) \\ &= \left(\sum_i f_i \circ \sqrt{\Phi} \cdot g_i\right)(\sqrt{\Phi}(x)) = (\lambda F)(\sqrt{\Phi}(x)) = 0. \end{aligned}$$

Portanto, $\deg(F)_0 \geq |C(\mathbb{F}_q)| - 1$. No entanto, como $Im(\lambda_1) \subseteq R_{m+n\sqrt{q}}$, temos $\deg(F)_\infty \leq m + n\sqrt{q}$, ou seja, concluímos que para m, n adequados,

$$|C(\mathbb{F}_q)| \leq m + n\sqrt{q} + 1.$$

A demonstração do teorema a seguir é apenas uma questão de escolher adequadamente m e n:

Teorema 3.3.2. Seja C uma curva de gênero g definida sobre um corpo finito $\mathbb{F}_q$, com q quadrado perfeito. Suponha que $q > (g+1)^4$. Então

$$|C(\mathbb{F}_q)| \leq (q+1) + (2g+1)q^{1/2}.$$

Demonstração. Basta escolher m e n satisfazendo as seguintes condições que lhes foram impostas na discussão anterior:

- $m < \sqrt{q}$;
- $m, n \geq g$;
- $(m+1-g)(n+1-g) > m\sqrt{q}+n+1-g$.

É fácil verificar que a escolha explícita

$$m = \left\lfloor \frac{g}{g+1}\sqrt{q} \right\rfloor + g + 1, \qquad n = \sqrt{q} + 2g$$

satisfaz as três condições, portanto

$$|C(\mathbb{F}_q)| \leq m + n\sqrt{q} + 1 \leq (q+1) + (2g+1)q^{1/2}.$$

■

Corolário 3.3.3. Suponha que C seja uma curva de gênero g sobre um corpo finito $\mathbb{F}_q$, tal que q é um quadrado perfeito estritamente maior que $(g+1)^4$. Então, para todo $r \geq 1$,

$$|C(\mathbb{F}_{q^r})| \leq (q^r + 1) + (2g+1)q^{r/2}.$$

3.4 A Hipótese de Riemann

Aqui, transformaremos a cota superior obtida na seção anterior em uma cota inferior, e juntaremos essas duas para provar a Hipótese de Riemann.

Teorema 3.4.1 (Hipótese de Riemann)**.** Sejam C uma curva sobre um corpo finito $\mathbb{F}_q$ e $\alpha \in \mathbb{C}$ uma raíz de $Z(C,t)$. Então $|\alpha^{-1}| = q^{1/2}$.

Isso será feito usando uma série de reduções a casos mais simples A primeira dessas reduções é que não precisamos prová-la para $\mathbb{F}_q$, bastando prová-la para *alguma* extensão de $\mathbb{F}_q$.

Redução 1. Seja $K/\mathbb{F}_q$ um corpo de funções e considere sua função Zeta

$$Z(K,t) = \frac{L(t)}{(1-t)(1-qt)},$$

bem como a função Zeta de seu compósitum com $\mathbb{F}_{q^r}$, K_r,

$$Z(K_r,t) = \frac{L_r(t)}{(1-t)(1-q^r t)}.$$

Sendo $L(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$, então temos $L_r(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t)$.

A demonstração encontra-se disponível em [Stichtenoth, 2009], capítulo V§1 (página 166).

Perceba que esse resultado nos permite provar a Hipótese de Riemann não para uma curva C sobre $\mathbb{F}_q$, mas para a curva C_r obtida via mudança de base para $\mathbb{F}_{q^r}$: afinal, $|\alpha_i| = q^{1/2}$ se, e somente se, $|\alpha_i^r| = q^{r/2}$ para algum $r \geq 1$. Na prática, isso nos permite supor q tão grande quanto necessário. Por exemplo, podemos supor q quadrado perfeito e $q > (g+1)^4$, permitindo-nos assim usar a cota superior dada em 3.3.2.

Redução 2. Considere uma curva C definida sobre $\mathbb{F}_q$. Suponha que existe uma constante $c \in \mathbb{R}$ tal que, para todo $r \geq 1$,

$$||C(\mathbb{F}_{q^r})| - q^r - 1| \leq cq^{r/2}.$$

Então a hipótese de Riemann é válida para C.

Demonstração. Comecemos notando que a primeira redução, quando acompanhada da conclusão do final da seção 1 deste capítulo, nos garante que $|C(\mathbb{F}_{q^r})| - q^r - 1 = -\sum_{i=1}^{2g} \alpha_i^r$. Portanto, nossa hipótese é de que

$$\left| \sum_{i=1}^{2g} \alpha_i^r \right| \leq cq^{r/2},$$

para todo $r \geq 1$. A prova basear-se-á no raio de convergência (em torno de $z_0 = 0$) da função meromorfa em $\mathbb{C}$

$$M(z) = \sum_{i=1}^{2g} \frac{\alpha_i z}{1 - \alpha_i z},$$

que é $\rho = \min\{|\alpha_i|^{-1} \mid i = 1, \ldots, 2g\}$. Note que para $|z| < \rho$,

$$M(z) = \sum_{i=1}^{2g} \sum_{r \geq 1} (\alpha_i z)^r = \sum_{r \geq 1} c_r z^r,$$

em que

$$c_r = \sum_{i=1}^{2g} \alpha_i^r.$$

Portanto, como o raio de convergência ρ dessa série satisfaz

$$\rho^{-1} = \limsup |c_r|^{1/r} \leq q^{1/2},$$

temos que $|\alpha_i| \leq q^{1/2}$ para todo i. No entanto, como o produto de todos os α_i é precisamente igual a q^g (basta olhar a expressão explícita para $Z(C, t)$ que foi dada na seção 1 deste capítulo), temos que $|\alpha_i| = q^{1/2}$ para todo $i = 1, \ldots, 2g$. ■

Juntando essas duas reduções, se provarmos que existe uma constante $c \in \mathbb{R}_{>0}$ tal que, para todo $r \gg 1$,

$$|C(\mathbb{F}_{q^r})| > q^r + 1 - cq^{r/2},$$

provaremos a hipótese de Riemann. E é essa cota inferior que buscaremos provar nesta seção, transformando a cota superior de 3.3.2 em uma cota inferior.

Comecemos percebendo que sempre podemos encontrar um morfismo de C para $\mathbb{P}^1 = \mathbb{P}^1_k$ ($k = \overline{\mathbb{F}_q}$). Afinal, $k(C)$ é uma extensão finitamente gerada de k, que é um corpo perfeito, donde $k(C)$ é separavelmente gerada (c.f. [Hartshorne, 2013], capítulo I§4, página

27), isto é, pode ser fatorada como $k(C) \supseteq k(t) \supseteq k$, com $k(C)/k(t)$ separável. Aí o morfismo $k(t) \hookrightarrow k(C)$ equivale, na categoria de curvas, a um morfismo (dominante) $C \to \mathbb{P}^1_k$. Assim, temos a seguinte situação:

$$\begin{array}{ccc} C & & k(C) \\ \downarrow & & \uparrow \\ \mathbb{P}^1 & & k(t) \end{array}$$

Comecemos com um ponto racional $x \in \mathbb{P}^1(\mathbb{F}_q)$. Como a extensão $k(C)/k(t)$ é algébrica (pois $td_k k(C) = 1$) e finitamente gerada (pois $k(C)$ é finitamente gerado sobre k), essa extensão é finita de grau $n = [k(C)\colon k]$. Assumamos, por hora, que ela seja Galois. Nesse caso, o grupo de Galois $G = Gal(k(C)/k(t))$ age transitivamente na fibra de x (c.f. [Tengan and Borges, 2015], capítulo 11§1, página 273). Como o morfismo de Frobenius relativo mantém um elemento de C dentro da fibra de sua imagem, temos que para todo $y \in C$, existe $\eta \in G$, chamado de substituição de Frobenius de G em y, tal que

$$\phi(y) = \eta y.$$

Pondo e como o índice de ramificação de x, f seu grau (que, na realidade, é $= 1$ por ser ponto racional) e g a quantidade de primos de C em sua fibra, sabemos por Álgebra Comutativa que $n = efg$ (c.f. [Tengan and Borges, 2015] capítulo 11§4, página 286 para uma versão mais geral ou [Samuel and Zariski, 1975] capítulos V§9, página 290). Ou seja, supondo x não-ramificado (o que, em particular, significa que $e = 1$), a fibra de qualquer ponto racional de $\mathbb{P}^1$, não ramificado em C, tem precisamente $|G|$ elementos. Pondo agora $\nu(\eta)$ como a quantidade de pontos de C, cuja imagem em $\mathbb{P}^1$ é um ponto $\mathbb{F}_q$-racional, e com substituição de Frobenius η, sobre cada ponto não-ramificado de $\mathbb{P}^1$ existem $|G|$ pontos de C, e como os pontos não-ramificados são finitos, temos que

$$\sum_{\eta \in G} \nu(\eta) = |G| \cdot |\mathbb{P}^1(\mathbb{F}_q)| + N,$$

em que N é uma constante positiva (dada em função da quantidade de pontos ramificados).

Agora, a mesma argumentação com o Teorema de Riemann-Roch e os produtos tensoriais que nos deu a cota superior nos fornece a cota

$$\nu(\eta) \leq (q+1) + (2g+1)q^{1/2}.$$

Como os pontos $\mathbb{F}_q$-racionais de C são precisamente aqueles sobre pontos $\mathbb{F}_q$-racionais

de $\mathbb{P}^1$ com substituição de Frobenius identidade (de G), temos que

$$\begin{aligned}|C(\mathbb{F}_q)| &\geq |G| \cdot |\mathbb{P}^1(\mathbb{F}_q)| + N - \sum_{\substack{\eta \in G \\ \eta \neq Id}} (q+1) + (2g+1)q^{1/2} \\ &\geq n \cdot |\mathbb{P}^1(\mathbb{F}_q)| + N - (n-1)\left((q+1) + (2g+1)q^{1/2}\right) \\ &\geq (q+1) + N - (n-1)(2g+1)q^{1/2} \\ &\geq (q+1) - (n-1)(2g+1)q^{1/2}.\end{aligned}$$

Caso a extensão $k(C)/k(t)$ não seja Galois, tomamos simplesmente o fecho Galois de $k(C)$ sobre $k(t)$, que consiste de adicionar os (finitos) conjugados de elementos de $k(C)$, e procedemos normalmente com a prova. Para detalhes, c.f. o artigo de Bombieri, [Bombieri, 1974].

Em suma: a Hipótese de Riemann é válida para curvas sobre corpos finitos, e nosso trabalho deu algum resultado. Ufa!

A Corpos de Funções e Curvas Algébricas

Aqui desenvolveremos um pouco a linguagem a ser utilizada na demonstração da racionalidade da função Zeta, a dizer, a de corpos de funções. É possível ter um apanhado geral da teoria de curvas algébricas (do ponto de vista da Geometria Algébrica clássica) em [Fulton, 1989], bem como introduções à teoria de corpos de funções em [Rosen, 2013] e, principalmente, [Stichtenoth, 2009]. Comecemos pelo começo:

Definição A.1. Seja k um corpo. Um corpo de funções algébricas de dimensão 1 sobre k (doravante simplesmente um corpo de funções sobre k) é uma extensão de k, finitamente gerada e com grau de transcendência 1.

Exemplo A.2. $K = k(x)$ é um corpo de funções sobre k. Note que $K = k(\mathbb{P}^1_k)$, isto é, K é (isomorfo a)o corpo de funções da reta projetiva.

Exemplo A.3. Considere $K = k(x, y)$ em que $y^2 = x^3 - x$, isto é,

$$K = \operatorname{Frac} \frac{k[x, y]}{(y^2 - x^3 + x)}.$$

Como K é uma extensão finita de $k(x)$, K é um corpo de funções sobre k.

Definição A.4. Seja K/k um corpo de funções. Um lugar de K é o ideal maximal de um anel de valorização discreta contido em K cujo corpo de frações seja K e contendo k. O grau de um lugar P é definido[1] como $\deg P \stackrel{\text{def}}{=} [\kappa(P) \colon k]$. Por fim, o conjunto de lugares de K é $\mathbb{P}_K$.

Exemplo A.5. Considere o corpo de funções meromorfas em uma curva elíptica $K = \operatorname{Frac} \frac{k[x, y]}{(y^2 - x^3 + x)}$ e um lugar P correspondente a um ponto k-racional dela, isto é $P = (\overline{x} - \alpha, \overline{y} - \beta)$ com $\beta^2 = \alpha^3 - \alpha$. Note que o anel de valorização de P é $k[\overline{x}, \overline{y}]_{(\overline{x}-\alpha, \overline{y}-\beta)}$, assim $\deg P = 1$.

Na realidade, temos uma equivalência de categorias entre curvas projetivas não-singulares sobre um corpo, com morfismos dominantes de variedades algébricas, e corpos de funções sobre esse mesmo corpo, com morfismos sendo os morfismos de corpos (c.f. [Hartshorne, 2013], capítulo I§6, página 45) e, nesse contexto, lugares de grau 1 correspondem exatamente aos pontos k-racionais da curva.

Vamos explicitar essa correspondência sem abrir todos os detalhes: todo corpo de funções é da forma $k(C)$, em que C é uma curva projetiva não-singular sobre k. Sem

[1] Temos um morfismo óbvio $k \to \kappa(P)$, logo podemos tratar $k \subseteq \kappa(P)$. Ainda, essa extensão é finita, de maneira que $[\kappa(P) \colon k] < \infty$.

muita perda de generalidade, assumamos que C é uma curva plana e, por birracionalidade, podemos assumir que C é afim, em outras palavras,

$$C = \operatorname{Spec} \frac{k[x,y]}{(f)},$$

em que $V(f, f_x, f_y) = \emptyset$.

Agora, **não é** verdade que todos os ideais maximais de $R = \dfrac{k[x,y]}{(f)}$ sejam da forma $(x-a, y-b)$ com (a,b) pontos racionais da curva. Por exemplo, tomando $k = \mathbb{Q}$ e $f(x,y) = x^2 + y^2 + 1$, (x^2+1, y) é um ideal maximal de R, porém é um lugar de $K = \operatorname{Frac} \dfrac{k[x,y]}{(f)}$ de grau 2. E por que grau 2? Ora, por ser exatamente o grau do ponto (x^2+1, y)! No seguinte sentido: quando consideramos (x^2+1) em $\dfrac{\mathbb{C}[x,y]}{(f)}$, ele se fatora como $(x+i)(x-i)$, "quebrando-se em $2 = \deg(x^2+1, y)$". Ou seja, o grau de um lugar codifica se ele é um ponto racional ou, caso não seja, sua "potencialidade enquanto pontos múltiplos"!

O próximo passo para usarmos o Teorema de Riemann-Roch é criarmos uma linguagem razoável de divisores:

Definição A.6. Seja K/k um corpo de funções. O grupo de divisores de K é

$$\operatorname{Div} K \stackrel{\text{def}}{=} \bigoplus_{P \in \mathbb{P}_K} \mathbb{Z} \cdot P,$$

isto é, o grupo abeliano livre gerado pelos lugares de K. A ordem total em $\mathbb{Z}$ induz uma ordem parcial em $\operatorname{Div} K$. Dizemos que um divisor $A \in \operatorname{Div} K$ é efetivo, ou positivo, se $A \geq 0$.

Dada uma $f \in K^\times$, o divisor de f é

$$(f) = \operatorname{div} f \stackrel{\text{def}}{=} \sum_{P \in \mathbb{P}_K} \nu_P(f) \cdot P,$$

em que ν_P é a valorização discreta a cujo anel de valorização P é associado[2]. O conúcleo de $\operatorname{div}\colon K^\times \to \operatorname{Div} K$ é o grupo de classe de K, $\mathcal{C}_K$.

Possuindo uma linguagem razoável de divisores, estamos quase prontos para enunciar o Teorema de Riemann-Roch. Para um divisor $D \in \operatorname{Div} K$, considere o k-espaço vetorial

$$L(D) \stackrel{\text{def}}{=} \{f \in K^\times \mid (f) + D \geq 0\} \cup \{0\}.$$

Assim como nos Teoremas de Riemann-Roch para superfícies de Riemann e para curvas, estamos interessados em calcular $l(D) \stackrel{\text{def}}{=} \dim_k L(D)$. O Teorema de Riemann-Roch para corpos de funções nos diz, então, o seguinte:

[2] Para uma demonstração de que div está bem-definido (em outras palavras, que toda $0 \neq f \in K^\times$ possui um número finito de zeros e polos), c.f. [Stichtenoth, 2009], capítulo 1§3 (página 14).

Teorema A.7 (Teorema de Riemann-Roch para Corpos de Funções)**.** Seja K/k um corpo de funções de gênero[3] g, com k integralmente fechado em K. Então existe um divisor (na verdade, uma classe de divisores, chamados de divisores canônicos de K/k) $W \in \operatorname{Div} K$ tal que, para todo $D \in \operatorname{Div} K$,

$$l(D) - l(W - D) = \deg D + 1 - g.$$

Para a demonstração, c.f. [Stichtenoth, 2009], capítulo I§5 (página 28).

Assim como para superfícies de Riemann e para esquemas, temos a seguinte consequência puramente formal do Teorema de Riemann-Roch:

Corolário A.8. O grau de qualquer divisor canônico em K/k é $2g - 2$.

Passamos agora à consideração da função Zeta de um corpo de funções sobre um corpo finito $\mathbb{F}_q$, que é considerado integralmente fechado em K, que veremos em instantes ser igual à função Zeta da curva projetiva e não-singular a ele associado. Lembre que $\operatorname{Div}(K)$ é o grupo de divisores de K, o grupo abeliano livre gerado pelos lugares de K, e o conúcleo do morfismo $\operatorname{div}\colon K^\times \to \operatorname{Div}(K)$ é definido como sendo o grupo de classe de K, $\mathcal{C}_K$. Por fim, definimos também o grupo de divisores de grau zero, módulo equivalência linear, como $\mathcal{C}_K^0$. Este grupo é finito (c.f. [Stichtenoth, 2009], capítulo V§1, página 159), e sua ordem $h = h_K$ é definida como sendo o número de classe de K.

Comecemos com um lema contendo alguns números importantes para nossa demonstração. A partir de agora sempre assumiremos que uma curva algébrica possui ao menos um ponto racional, ou, uma condição um pouco mais fraca, que existe $A \in \operatorname{Div} K$ com grau 1[4].

Lema A.9. Seja K/k um corpo de funções de gênero g sobre um corpo finito $k = \mathbb{F}_q$ e ponha

$$A_n \stackrel{\text{def}}{=} |\{A \in \operatorname{Div}(K) \mid A \geq 0, \text{ e } \deg A = n\}|.$$

Então, para $\overline{D} \in \mathcal{C}_K$,

$$|\{A \in \overline{D} |\, A \geq 0\}| = \frac{1}{q-1}\left(q^{l(D)} - 1\right).$$

Ainda, para $n > 2g - 2$,

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

em que $h = h_K$ é o número de em que $h = h_K$ é o número de classe de K,isto é, a quantidade de elementos de $\mathcal{C}_K^0$.

[3] No contexto de corpos de funções, o gênero g é definido como o máximo de $\deg D + 1 - l(D)$, com D percorrendo todos os divisores de K/k. Esse número é finito, c.f. [Stichtenoth, 2009], capítulo I§4 (página 20).

[4] Essa condição mais fraca é supérflua, pois é sempre verdadeira. No entanto, sua demonstração é um pouco mais complicada, c.f. [Stichtenoth, 2009],capítulo V§1 (página 164).

classe de K,isto é, a quantidade de elementos de $\mathcal{C}_K^0$.

Demonstração. Note que $A \in \overline{D}$ e $A \geq 0$ se, e somente se, $A = D + (x)$, com $x \in L(D)$, $x \neq 0$. Ainda, $D + (x) = D + (y)$ se, e somente se, $x = \alpha y$ para algum $\alpha \in \mathbb{F}_q$ não-nulo. Ou seja: os elementos de

$$\{A \in \overline{D} |\, A \geq 0\}$$

estão em bijeção com a projetivização do espaço $L(D)$. Ora, a projetivização de um espaço vetorial de dimensão $l(D)$ sobre $\mathbb{F}_q$ possui exatamente

$$\frac{1}{q-1}\left(q^{l(C)} - 1\right)$$

elementos, dando assim a primeira parte do lema.

Da finitude do grupo $\mathcal{C}_K^0$, temos que existem precisamente h classes de equivalência de divisores de grau n (módulo equivalência linear), dadas por $\overline{D_1}, \ldots, \overline{D_h} \in \mathcal{C}_K$. Aí, como qualquer divisor A de grau n está em exatamente uma classe de equivalência $\overline{D_i}$, e pela primeira parte desse lema,

$$A_n = \sum_{i=1}^{h} |\{A \in \overline{D_i} \mid A \geq 0\}| = \sum_{i=1}^{h} \frac{1}{q-1}\left(q^{l(D_i)} - 1\right) = \frac{h}{q-1}\left(q^{n+1-g} - 1\right).$$

■

Definição A.10. Seja K/k um corpo de funções sobre um corpo finito $k = \mathbb{F}_q$. A função Zeta de K é definida como sendo a série formal em $\mathbb{Z}[[t]]$

$$Z(K,t) \stackrel{\text{def}}{=} \sum_{n \geq 0} A_n t^n.$$

Primeiramente: é bom garantirmos que essa função Zeta corresponde realmente à função Zeta de uma curva algébrica, como definida no terceiro capítulo desse texto, no sentido que $Z(k(C),t) = Z(C,t)$. Faremos isso por meio de uma representação específica que a função Zeta possui, a dizer, o produto de Euler. Por ser este um produto infinito, existem questões de convergência às quais devemos prestar atenção. No entanto, para manter a brevidade desse apêndice, referencio o leitor interessado a conferir os detalhes em [Stichtenoth, 2009], capítulo V (esp. páginas 162 e 163).

Proposição A.11. $Z(K,t) = \sum_{\substack{A \in \operatorname{Div} K \\ A \geq 0}} t^{\deg A}$.

Demonstração. Note que, dividindo-se a soma do lado direito da igualdade por grau, a quantidade de parcelas da forma t^n é, tautologicamente, $|\{A \in \operatorname{Div} K \mid A \geq 0 \text{ e } \deg A = n\}|$.

Portanto,

$$\sum_{\substack{A\in\operatorname{Div} K\\ A\geq 0}} t^{\deg A} = \sum_{n\geq 0} |\{A\in \operatorname{Div} K \mid A\geq 0 \text{ e } \deg A = n\}|\, t^n$$
$$= \sum_{n\geq 0} A_n t^n = Z(K,t).$$

■

Lema A.12. A função Zeta acima definida admite uma representação na forma de um produto infinito

$$Z(K,t) = \prod_{P\in\mathbb{P}_K} (1-t^{\deg P})^{-1}.$$

Demonstração. Temos:

$$\prod_{P\in\mathbb{P}_K} (1-t^{\deg P})^{-1} = \prod_{P\in\mathbb{P}_K}\sum_{n\geq 0} t^{n\deg P}$$
$$= \prod_{P\in\mathbb{P}_K}\sum_{n\geq 0} t^{\deg nP}$$
$$= \sum_{A\geq 0} t^{\deg A} = \sum_{n\geq 0} A_n t^n = Z(K,t).$$

A única igualdade merecedora de escrutínio é a antepenúltima, isto é,

$$\prod_{P\in\mathbb{P}_K}\sum_{n\geq 0} t^{\deg nP} = \sum_{A\geq 0} t^{\deg A}.$$

Podemos concluir sua veracidade pois cada parcela à direita é da forma $t^{\deg A} = t^{\deg n_1P_1+\ldots+\deg n_kP_k}$, para divisores $P_i\in\mathbb{P}_L$ $(i=1,\ldots,k)$ e $n_1\geq 0$. Daí, temos

$$t^{\deg A} = t^{\deg n_1P_1}\ldots t^{\deg n_kP_k},$$

que aparece na soma à esquerda ao considerarmos a parcela em que, em quase todos os fatores do produto infinito tomamos $n=0$, e nos P_i, tomamos a parcela n_kP_k da soma, dando assim nosso divisor A. Assim, é fácil ver que a igualdade acima faz sentido, provando assim que a função Zeta admite representação como produto de Euler. ■

Agora, estamos em condição de provar que essa noção de função Zeta condiz com a função Zeta de uma curva algébrica:

Teorema A.13. Ponha $b_d \overset{\text{def}}{=} |\{P\in\mathbb{P}_K \mid \deg P = d\}|$ e $N_r \overset{\text{def}}{=} \sum_{d|r} d\, b_d$. Então

$$Z(K,t) = \exp\left(\sum_{r\geq 1}\frac{N_r}{r}t^r\right).$$

Demonstração. Note que da representação de $Z(K,t)$ como um produto de Euler e da definição de b_d, temos

$$\log Z(K,t) = \sum_{d\geq 1} b_d \left(-\log(1-t^d)\right).$$

Como $-\log(1-x) = \sum_{r\geq 1} x^r/r$, vê-se que

$$\begin{aligned}\log Z(K,t) &= \sum_{d\geq 1} b_d \left(\sum_{r\geq 1} \frac{t^{rd}}{r}\right) \\ &= \sum_{d\geq 1}\sum_{r\geq 1} d\, b_d \frac{t^{dr}}{dr}\end{aligned}$$

Dividindo-se as parcelas por expoente de t, vemos que o coeficiente de t^m são da forma

$$\sum_{d|m} \frac{d\, b_d}{m} = \frac{N_m}{m},$$

donde é imediato confirmar que

$$\log Z(K,t) = \sum_{m\geq 1} \frac{N_m}{m} t^m.$$

■

A única coisa que precisamos agora garantir é que de fato N_r é a quantidade de pontos $\mathbb{F}_{q^r}$-racionais da curva que tem K como corpo de funções. A heurística por trás disso é a seguinte: um lugar $P \in \mathbb{P}_K$ de grau d se "quebra" em d lugares de grau 1 quando passamos à extensão $K_d \stackrel{\text{def}}{=} \mathbb{F}_{q^d} \cdot K$. Assim, o "ponto não-racional" P (quando $\deg P = d > 1$) origina d pontos racionais na extensão de grau d de K. E aí, quando consideramos uma extensão de um grau fixo r, precisamos contar todos os pontos com coordenadas em extensões intermediárias de K_r, isto é,

$$|C(\mathbb{F}_{q^r})| = \sum_{d|r} d\, b_d.$$

De maneira mais precisa, temos a seguinte

Proposição A.14. $N_r = |\{P \in \mathbb{P}_{K_r} \mid \deg P = 1\}|$.

Demonstração. Usaremos a redução 1 da seção 3.4 deste trabalho. Explicitamente, se $K/\mathbb{F}_q$ é um corpo de funções com gênero g e função Zeta

$$Z(K,t) = \frac{L(t)}{(1-t)(1-qt)},$$

em que $L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$, então

$$Z(K_r, t) = \frac{L_r(t)}{(1-t)(1-q^r t)},$$

em que $L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t)$. Assim, sendo $A_1 = |\{P \in \mathbb{P}_{K_r} \mid \deg P = 1\}|$, temos

$$A_1 = q^r + 1 - \sum \alpha_i^r.$$

Precisamos provar agora que a expressão à direita da igualdade acima é igual a N_r. Para tanto, consideremos duas expressões da função Zeta,

$$Z(K, t) = \frac{\prod_{i=1}^{2g}(1 - \alpha_i t)}{(1-t)(1-qt)} = \exp\left(\sum_{m \geq 1} \frac{N_m}{m} t^m\right).$$

Usando essas duas expressões da função Zeta, temos

$$t\frac{d}{dt}Z(K, t) = \sum_{m \geq 1} N_m t^m = \sum_{m \geq 1}\left(1 + q^m - \sum_{i=1}^{2g} \alpha_i^m\right) t^m,$$

donde comparando os coeficientes dessas duas séries em t^m, concluímos que

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r.$$

■

E agora, finalmente, podemos garantir que $|C(\mathbb{F}_{q^r})| = N_r$: afinal, se C é uma curva definida sobre $\mathbb{F}_q$ com corpo de funções K, então o corpo de funções de C_r, a extensão de C a $\mathbb{F}_{q^r}$, é precisamente K_r. Em outras palavras: acabamos de provar que se C é uma curva definida sobre $\mathbb{F}_q$ com corpo de funções $K/\mathbb{F}_q$, então

$$Z(C, t) = Z(K, t).$$

Ou seja: a Hipótese de Riemann para curvas sobre corpos finitos (ou, mais geralmente, as conjecturas de Weil) têm uma íntima relação com a Hipótese de Riemann (aquela que vale um milhão de dólares). Daí, é possível se perguntar se não conseguiríamos uma a partir da outra. A resposta é: talvez! Um ramo de pesquisa que está sendo desenvolvido nesse instante é a chamada "geometria sobre $\mathbb{F}_1$". A ideia é que se for desenvolvida uma teoria que dê um significado bom à ideia de uma "curva sobre o corpo com um elemento", poderemos enxergar $\mathbb{Z}$ como uma curva sobre esse corpo, e aí a Hipótese de Riemann seria uma consequência meramente formal da Hipótese de Riemann para $\mathbb{Z}$ como uma curva. Para uma introdução contando os primeiros passos dessa teoria, c.f. [Connes and Consani, 2008].

Referências

[Artin, 1924] Artin, E. (1924). Quadratische körper im gebiete der höheren kongruenzen. i,ii. *Mathematische Zeitschrift*, 19(1):153–206,207–246.

[Atiyah and Macdonald, 1969] Atiyah, M. and Macdonald, I. (1969). Introduction to commutative algebra, addisonwesley. *Reading, MA*.

[Bombieri, 1974] Bombieri, E. (1974). Counting points on curves over finite fields. In *Séminaire Bourbaki vol. 1972/73 Exposés 418–435*, pages 234–241. Springer.

[Bredon, 2013] Bredon, G. E. (2013). *Topology and geometry*, volume 139. Springer Science & Business Media.

[Cartier, 2000] Cartier, P. (2000). Alexander grothendieck–un pays dont on ne connaîtrait que le nom. *Inference–International Review of Science*, pages 1–27.

[Connes and Consani, 2008] Connes, A. and Consani, C. (2008). On the notion of geometry over f_1. *arXiv preprint arXiv:0809.2926*.

[Deligne, 1974] Deligne, P. (1974). La conjecture de weil. i. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 43(1):273–307.

[Dieudonné, 1972] Dieudonné, J. (1972). The historical development of algebraic geometry. *The American Mathematical Monthly*, 79(8):827–866.

[Dirichlet, 1863] Dirichlet, P. L. (1863). *Vorlesungen Über Zahlentheorie*. Ripol ClassiC.

[Eisenbud, 2013] Eisenbud, D. (2013). *Commutative Algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media.

[Fulton, 1989] Fulton, W. (1989). *Algebraic curves: an introduction to algebraic geometry*. Addison-Wesley.

[Grothendieck, 1957] Grothendieck, A. (1957). Sur quelques points d'algèbre homologique. *Tohoku Mathematical Journal, Second Series*, 9(2):119–183.

[Hartshorne, 2013] Hartshorne, R. (2013). *Algebraic geometry*, volume 52. Springer Science & Business Media.

[Jackson, 2004] Jackson, A. (2004). Comme appelé du néant—as if summoned from the void: the life of alexandre grothendieck. *Notices of the AMS*, 51(4).

[Liu, 2002] Liu, Q. (2002). *Algebraic geometry and arithmetic curves*, volume 6. Oxford University Press on Demand.

[Miranda, 1995] Miranda, R. (1995). *Algebraic curves and Riemann surfaces*, volume 5. American Mathematical Soc.

[Ramanan, 2005] Ramanan, S. (2005). *Global calculus*, volume 65. American Mathematical Soc.

[Raynaud, 1999] Raynaud, M. (1999). André weil and the foundations of algebraic geometry. *Notices of the AMS*, 46(8).

[Riemann, 1859] Riemann, B. (1859). On the number of primes less than a given magnitude. *Monatsberichte der Berliner Akademie*, pages 1–10.

[Roquette et al., 2003] Roquette, P. et al. (2003). The riemann hypothesis in characteristic p, its origin and development. *preprint available at http://www. rzuser. uni-heidelberg. de/ci3*.

[Rosen, 2013] Rosen, M. (2013). *Number theory in function fields*, volume 210. Springer Science & Business Media.

[Samuel and Zariski, 1975] Samuel, P. and Zariski, O. (1975). *Commutative algebra*. Springer.

[Stepanov, 1969] Stepanov, S. A. (1969). On the number of points of a hyperelliptic curve over a finite prime field. *Mathematics of the USSR-Izvestiya*, 3(5):1103.

[Stichtenoth, 2009] Stichtenoth, H. (2009). *Algebraic function fields and codes*, volume 254. Springer Science & Business Media.

[Tengan and Borges, 2015] Tengan, E. and Borges, H. (2015). Algebra comutativa em quatro movimentos. *Projeto Euclides, IMPA, Rio de Janeiro*.

[Ueno, 2003] Ueno, K. (2003). *Algebraic geometry 3, volume 218 of Translations of Mathematical Monographs*, volume 3. American Mathematical Society.

[Weil, 1941] Weil, A. (1941). On the riemann hypothesis in function-fields. *Proceedings of the National Academy of Sciences of the United States of America*, 27(7):345.

[Weil, 1981] Weil, A. (1981). Sur les origines de la géométrie algébrique. *Compositio mathematica*, 44(1-3):395–406.

[Weil et al., 1949] Weil, A. et al. (1949). Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc*, 55(5):497–508.