UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

Roberto Alvarenga Jr.

Teorema de Riemann-Roch, Morfismos de Frobenius e a Hipótese de Riemann

São José do Rio Preto
2014

Roberto Alvarenga Jr.

Teorema de Riemann-Roch, Morfismos de Frobenius e a Hipótese de Riemann

Dissertação apresentada para obtenção do título de Mestre em Matemática, área de Geometria Algébrica, junto ao Programa de Pós Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus São José do Rio Preto.

Orientador: Prof. Dr. Parham Salehyan

São José do Rio Preto
2014

Roberto Alvarenga Jr.

Teorema de Riemann-Roch, Morfismos de Frobenius e a Hipótese de Riemann

Dissertação apresentada para obtenção do título de Mestre em Matemática, área de Geometria Algébrica, junto ao Programa de Pós Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus São José do Rio Preto.

BANCA EXAMINADORA

Prof. Dr. Parham Salehyan
Professor Assistente Doutor
UNESP - São José do Rio Preto
Orientador

Prof. Dr. Eduardo Tengan
Professor Associado - SMA
Livre-Docente (MS5) - RDIDP
ICMC-USP-São Carlos

Prof. Dr. Trajano Pires da Nóbrega Neto
Professor Adjunto
UNESP - São José do Rio Preto

Aos meus pais,
Roberto e Elza,
dedico.

Agradecimentos

Agradeço a todos que contribuíram de alguma forma para minha formação. Em especial agradeço:
Ao Prof. Dr. Parham Salehyan, pela excelente e valiosa orientação desde a graduação. Pelos conhecimentos transmitidos, pela disponibilidade, atenção e dedicação indispensáveis para não só a concretização deste trabalho mas também para minha formação matemática.
Ao Prof. Dr João Carlos, pelo conhecimento transmitido, incentivo e pelas tão valiosas conversas matemáticas ou não.
Aos verdadeiros mestres Enio Ricardo Crema e Danilo Marangão, fontes de inspiração desde meu primeiro dia de graduação.
À Banca Examinadora, por terem aceito o meu convite.
Aos meus pais Roberto e Elza, minha eterna gratidão pelo amor incondicional e pelos sacrifícios realizados afim de que minha única preocupação sempre fosse os estudos.
Aos meus irmãos Weinner e Isabella pela preciosidade na minha vida.
À minha noiva Natália, agradeço o apoio inestimável, companheirismo, carinho e cuidado.
Aos grandes amigos que ganhei durante todo esse tempo, em especial: Jhony, Juliana, Letícia, Liliam, Rafael, Ricardo, Robson, Rodrigo, Vanessa, Victor e Wanderson.
À FAPESP, pelo apoio financeiro.

"E mesmo que meus passos sejam falsos, mesmo que os meus caminhos sejam errados, mesmo que meu jeito de levar a vida incomoda, eu sei quem sou e sei pelo que devo lutar. Se você acha que meu orgulho é grande, é porque nunca viu o tamanho da minha fé!".

Tião Carreiro

Resumo

O objetivo desde trabalho é estimar um cota para o número de pontos racionais de uma curva. Observando as várias semelhanças entre o anel dos inteiros e o anel dos polinômios em uma variável, iremos usar ferramentas da teoria dos números para resolver um problema da geometria algébrica. Desta fusão nasce uma das mais nobres áreas da matemática: a geometria aritmética. Fazendo uso do célebre teorema de Riemann-Roch e das ferramentas da teoria dos números demonstraremos a hipótese de Riemann para a função-zeta de uma curva não singular e qual consequência tal hipótese tem para a contagem de pontos racionais de uma curva.

Palavras-chave: Geometria Algébrica, Geometria Aritmética, Teorema de Riemann-Roch, Hipótese de Riemann e Funções-Zeta.

Abstract

The aim of this work is to estimate a bound for the number of rational points of a curve. Observing the various similarities between the ring of integers and the ring of polynomials in one variable, we use tools from number theory to solve a problem of algebraic geometry. From this merger is born one of the noblest areas of mathematics: arithmetic geometry. Making use of the famous Riemann-Roch's theorem and tools of number theory we demonstrate the Riemann hypothesis for the zeta-function of a nonsingular curve and which consequence this hypothesis has to count rational points on a curve.

Keywords: *Algebraic Geometry, Arithmetic Geometry, Riemann-Roch's theorem, Riemann Hypothesis and Zeta-Functions*

Sumário

Introdução

O objetivo principal deste trabalho é dar boas estimativas para o número de pontos racionais de uma *curva completa não singular* definida sobre um corpo finito. Para isto, estudaremos numa maneira unificada, alguns conceitos e ferramentas fundamentais na teoria dos números, álgebra comutativa e geometria algébrica e mostraremos a analogia e relação profunda entre estas áreas. Introduziremos nos cinco primeiros capítulos ferramentas que serão úteis para a resolução deste problema nos ultimos três capítulos. Veremos que tal estimativa decorre diretamente do análogo da *hipótese de Riemann*, para o caso de curvas sobre corpos finitos. Para alcançar tal objetivo, entre outos assuntos estudaremos: da teoria dos números: fecho integral, discriminante e ramificações, grupo de classe de ideais; da álgebra comutativa: localizações, domínios de Dedekind, valorizações; da geometria algébrica e aritmética: curvas algébricas, teorema de Riemann-Roch, funções-zeta e a hipótese de Riemann.

No capítulo zero introduziremos alguns resultados clássicos que serão úteis no decorrer do texto. São resultados conhecidos e básicos da álgebra comutativa e da teoria de curvas planas afins, por isso serão apenas enunciados com referências para suas demonstrações.

Começaremos nosso estudo com um assunto clássico da teoria dos números: *o fecho integral* de um anel. Como frequentemente acontece na história da matemática, definições abstratas são dadas a partir de concretos exemplos bem entendidos. A definição de fecho integral dada num cenário abstrato de álgebra comutativa por Noether por volta de 1927 veio somente após casos concretos de corpos de números e corpos de funções estudados em grandes detalhes. No primeiro capítulo, dada uma extensão de anéis, veremos quando um elemento é integral sobre o anel de base e, assim, definiremos o fecho integral de um anel. Após a definição do fecho integral de um anel, buscaremos responder quais propriedades o fecho integral herda do anel. Daremos exemplos que contextualizarão estas definições para o caso de corpos de números e o caso de corpos de funções. Além disso, introduziremos alguns outros conceitos de álgebra, tais como produto de ideais e

domínios de Dedekind.

O segundo capítulo é caracterizado por reunir conceitos e resultados da teoria dos números, álgebra comutativa e teoria de Galois. O primeiro objetivo deste capítulo é demonstrar um teorema sobre fatoração única de ideais, cujo enunciado é dado no primeiro capítulo. Definiremos na segunda seção o *índice de ramificação* e o *grau residual* associados a um ideal e a uma extensão de seu anel, além disso, daremos uma fórmula que associará estes dois números com o grau da extensão. Depois estudaremos os conceitos de *ramificação* e *não ramificação* de um ideal e usaremos tal conceito para dar, em alguns casos, a fatoração explicita de ideais no fecho integral de seu anel. Definidos tais conceitos acima, estudaremos como eles se comportam em dois casos particulares de extensão do corpo de frações do anel dado, discutiremos o caso de extensões simples e de extensões de Galois. Terminaremos este capítulo contextualizando a teoria de Galois para o caso de curvas planas.

Para dar sequência no estudo do capítulo anterior e fornecer alguns critérios para um ideal ser ramificado ou não, estudaremos no terceiro capítulo *os discriminantes*. Discutiremos neste capítulo as diversas definições de discriminante e veremos quais consequências possui sobre o estudo de tais ideais. Com essa ferramenta, veremos quando um *ponto* sobre uma curva é ramificado no fecho integral do anel dos polinômios, numa extensão do corpo de funções polinomiais em uma variável. Mais geralmente, usaremos os conceitos de discriminante para definir o discriminante de uma base e o *ideal discriminante*, que nos fornecerá um importante critério para saber quando um ideal é ramificado no fecho integral de seu anel. Finalizaremos este capítulo introduzindo uma generalização de norma de um elemento para um ideal, este conceito será usado no próximo capítulo.

No quarto capítulo, estudaremos um invariante associado a um domínio de Dedekind, o *grupo de classe de ideais*. O principal objetivos é mostrar que este grupo é finito nos casos dos fechos integrais de $\mathbb{Z}$ e $k[x]$, com k um corpo finito. Para isto, primeiramente definiremos quando um domínio possui quocientes finitos e mostraremos que nos dois casos mencionados acima, os domínios possuem quocientes finitos. Assim, teremos condições de mostrar a finitude para o caso do fecho integral de $\mathbb{Z}$. Para o caso do fecho integral de $k[x]$, introduziremos os importantes conceitos que serão úteis para mostrar a finitude do grupo de classe de ideais neste caso e que também serão úteis nos próximos capítulos, trata-se das *valorizações* e *valores absolutos*. Encerraremos o capítulo demonstrando a finitude do grupo de classe de ideais para o caso de $k[x]$ com k corpo finito.

Estudados nos primeiros quatro capítulos algumas ferramentas da teoria dos números e álgebra comutativa, iniciaremos no quinto capítulo o estudo de *curvas projetivas planas* e *curvas completas não singulares*. Este último por sinal, é uma classe de objetos algébricos (geométricos) que contém as curvas projetivas planas, por este motivo, discutiremos os

resultados nos próximos capítulos para essa classe mais ampla. Começaremos o capítulo definindo curvas projetivas e logo em seguida trataremos o caso das *cônicas*. Entendido bem este caso, passaremos a estudar as funções sobre uma curva projetiva. Definiremos o *corpo das funções* sobre uma curva e em seguida caracterizaremos as valorizações sobre uma curva, que não será nada mais do que as valorizações do corpo de funções sobre uma curva. Em seguida, começaremos nosso estudo sobre as *curvas completas não singulares*. Usando as ações do grupo de Galois de uma extensão caracterizaremos as curvas projetivas e afins planas em termo de domínios locais principais contidos nos corpos de funções e do conjunto das valorizações discretas destes corpos. Estudaremos ainda como relacionar duas curvas completas através de uma aplicação, para isso, definiremos um *morfismo* de curvas completas e estudaremos quando um ponto de um curva é um ponto de ramificação de um morfismo dado, fazendo aqui, forte analogia com o capítulo dois. Já visando o objetivo principal, definiremos na penúltima seção, o *corpo de definição* de um ponto de uma curva completa e o conceito de *pontos racionais* de uma curva. Por fim, discutiremos na última seção deste capítulo o *divisor do grupo de classe*. Estudamos no quarto capítulo o grupo de classe de ideais para um domínio de Dedekind, aqui associaremos a uma curva completa, um grupo abeliano chamado do *grupo de classe divisor* ou *grupo de Picard*, este grupo desempenhará um papel importantíssimo no próximo capítulo, como por exemplo na prova da racionalidade da *função-zeta*.

Agora, com *quase todas* as ferramentas em mãos, atacaremos nos últimos três capítulos o problema de contar o números de pontos racionais de uma curva completa não singular sobre um corpo finito.

Como dissemos acima, uma boa estimativa para o número de pontos racionais de uma curva sobre um corpo finito está diretamente ligado com a versão para curvas sobre corpos finitos da chamada hipótese de Riemann. Tal hipótese afirma que os zeros da *função-zeta de Riemann* compreendidos em um determinando conjunto possuem todos o mesmo módulo. Dito isto, dedicaremos o sexto capítulo ao estudo das funções-zeta de Riemann. Iniciaremos com a definição geral da função-zeta e algumas propriedades. Em seguida, associaremos a um domínio de Dedekind com quocientes finitos uma função-zeta, usaremos fortemente o fato deste domínio possuir fatoração única de ideais e a norma de um ideal(discutida anteriormente) para dar a esta função-zeta uma caracterização chamada de *produto de Euler*. Estudado os casos acima, definiremos a função-zeta para: uma curva afim plana não singular, curva projetiva plana não singular e finalmente para uma curva completa não singular. Definida a função-zeta para uma curva completa não singular discutiremos como a hipótese de Riemann neste caso implica em boas estimativas para o número de pontos racionais desta curva. Além disso, mostraremos (utilizando o teorema de Riemann-Roch) a racionalidade da função-zeta de uma curva completa e

daremos explicitamente sua forma para o caso das cúbicas.

O sétimo capítulo é dedicado aos teoremas de Riemann, em especial ao teorema de Riemann-Roch. Este teorema terá suma importância na prova de que a hipótese de Riemann vale para o caso de curvas sobre corpos finitos, sem contar que ele é usado fortemente na prova da racionalidade da função-zeta. A motivação para este teorema é verificar se existe uma função racional sobre um curva com zeros e polos pré-determinados. A afirmação do teorema de Riemann-Roch é uma identidade cujo um dos termos é um inteiro positivo associado a curva dada, chamado *gênero*. A determinação do gênero de uma curva completa dada será o motivo de estudo nas duas última seções deste capítulo, primeiro investigaremos como determinar o gênero de uma curva plana não singular e em seguida de uma curva completa através da *fórmula de Riemann-Hurwitz*.

No oitavo e último capítulo, adicionaremos a *priori* alguns conceitos que serão úteis para o desfecho do problema central deste trabalho e a *posteriori* demonstraremos a validade da hipótese de Riemann para curvas sobre corpos finitos, e assim, dar boas estimativas para o número de pontos racionais de uma curva sobre um corpo finito. Começaremos discutindo alguns casos de extensões inseparáveis, em seguida definiremos e estudaremos conceitos importantes tais como: morfismos, endomorfismos e elementos de Frobenius. Assim teremos condições de na última seção provar a hipótese de Riemann para o caso citado acima. Esta prova será feita em dois passos, primeiro mostraremos um resultado onde sob certas condições a hipótese de Riemann é garantida e depois mostraremos que tais condições são sempre verificadas.

Capítulo

0

Preliminares

Reservamos este capítulo inicial para listar algumas definições e resultados básicos da álgebra comutativa e das curvas planas.

0.1 Álgebra Comutativa

Nesta seção listaremos alguns resultados da álgebra comutativa que serão utilizados ao longo deste trabalho.

0.1.1 Lema de Gauss e Mais

Introduziremos agora alguns resultados importantes devido a Gauss. Seja A um domínio fatorial com corpo de frações K. Diremos que um elemento de K é o *conteúdo* de $f \in K[y]$ e denotaremos por $\text{cont}(f)$ o elemento que, a menos de um inversível de A, satisfazer $f(y) = \text{cont}(f)f_1(y)$ tal que $f_1(y) \in A[y]$ e o maior divisor comum dos coeficientes de f_1 seja um. O polinômio $f_1(y)$ é único a menos de um inversível em A e é chamado de *polinômio primitivo* associado a f.

Lema 0.1.1 *(Versão de Gauss) Sejam A um domínio fatorial, K seu corpo de frações e g, h polinômios mônicos em $K[x]$. Se os coeficientes de g e h não estão todos em A, então os coeficientes de gh não podem estar todos em A.*

Lema 0.1.2 *(Versão Moderna) Seja A um domínio fatorial com corpo de frações K. Sejam $g, h \in K[x]$. Então o* $\text{cont}(gh) = \text{cont}(g)\text{cont}(h)$.

Corolário 0.1.1 *Seja $f(y) \in A[y]$ fatorável em $K[y]$ como $f(y) = g(y)h(y)$, com $g, h \in K[y]$. Escreva $g(y) = \text{cont}(g)g_1(y)$ e $h(y) = \text{cont}(h)h_1$, com $g_1, h_1 \in A[y]$. Então $f(y) = \text{cont}(f)g_1h_1$ é um fatoração de $f(y)$ em $A[y]$.*

As demonstrações desses fatos podem ser encontradas em [1] , página 181.

Lema 0.1.3 *Seja A um domínio de dimensão um. Seja $M \subseteq A$ um ideal maximal gerado por dois elementos x e y. São equivalentes:*

1. *A_M é um domínio de ideais principais.*
2. *Existem dois elementos $u, v \in A$ tal que $ux + vy = 0$ onde pelo menos um dos elementos u, v não pertencem a M.*
3. *x ou y gera MA_M.*

Demonstração: *Veja [6], página 70.*

Proposição 0.1.1 *Seja A um anel. As seguintes afirmações são equivalentes:*

(1) *Todo ideal de A é principal.*

(2) *Todo ideal primo de A é principal.*

Demonstração: *Veja [6], página 68.*

Lema 0.1.4 *Seja $E|k$ uma extensão de grau n. Suponha que existe $\alpha \in E$ tal que $E = k(\alpha)$. Seja $g = \min_k(\alpha) \in k[y]$. São equivalentes:*

1. *$E|k$ é separável.*
2. *g tem n raízes distintas em $\overline{k}$.*
3. *$(g, g') = 1$.*
4. *$g' \neq 0$.*
5. *Se $\mathrm{char}(k) = 0$ ou $\mathrm{char}(k) = p > 0$, então $g \neq h^p$ em $\overline{k}[y]$ para qualquer $h \in \overline{k}[y]$.*
6. *$g'(\alpha) \neq 0$.*

Demonstração: *Veja [6], página 376.*

Lema 0.1.5 *Sejam $J \subseteq I$ dois ideais do anel A. Então $J = I$ se, e somente se, $J_M = I_M$ para todo ideal maximal M de A que contém J.*
Demonstração: *Veja [6], página 87.* ■

Proposição 0.1.2 *Seja A um domínio comutativo. Então*

$$A = \bigcap_{P \in \mathrm{Spec}(A)} A_P = \bigcap_{P \in \mathrm{Max}(A)} A_P.$$

Demonstração: *Veja [6], página 74.*

0.1.2 Módulos Noetherianos

Teorema 0.1.1 *Seja A um anel comutativo. Seja M um $A-$módulo qualquer. As seguintes afirmações são equivalentes:*

1. *Todo submódulo de M é finitamente gerado como $A-$módulo.*
2. *Todo cadeia crescente $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$ de submódulos de M é estacionária, isto é, existe n tal que $M_n = M_{n+1} = \cdots$.*
3. *Todo subconjunto não vazio de submódulos de M tem elemento maximal.*

Demonstração: *Veja [6], página 23.*

Definição 0.1.1 *Um $A-$módulo M é chamado de Noetheriano se satisfaz as propriedades equivalentes do teorema anterior.*

Um anel A é Noetheriano se, e somente se, é um $A-$módulo Noetheriano. De fato, os submódulos de A como $A-$módulo são seus ideais.

0.1.3 Sequências Exatas

Definição 0.1.2 *Um conjunto de $A-$módulos $\{M_i\}_{i\in\mathbb{Z}}$ e um conjunto de homomorfismo de $A-$módulos $\xi_i : M_i \longrightarrow M_{i+1}$ são chamados de* sequência *ou* complexo *se* $\mathrm{Im}(\xi_{i-1}) \subseteq \ker(\xi_i)$. *Uma sequência*

$$\cdots \to M_{i-1} \overset{\xi_{i-1}}{\to} M_i \overset{\xi_i}{\to} M_{i+1} \to \cdots$$

de $A-$módulos e $A-$módulos homomorfismo é exata *em M_i se* $\mathrm{Im}(\xi_{i-1}) = \ker(\xi_i)$. *A sequência é exata se é exata em cada M_i.*

Definição 0.1.3 *Uma* sequencia exata curta *é uma sequência exata de cinco termos da forma*

$$0 \to M' \overset{f}{\to} M \overset{g}{\to} M'' \to 0.$$

Equivalentemente, uma sequência de cinco termos como acima é um sequência exata curta se f é injetiva, g sobrejetiva e $\mathrm{Ker}(g) = Im(f)$.

Lema 0.1.6 *Seja $0 \to M' \overset{f}{\to} M \overset{g}{\to} M'' \to 0$ uma sequência exata de $A-$módulos. Se M' e M'' são finitamente gerados, então M é finitamente gerado. Além disso, se M é um $A-$módulo finitamente gerado, então M'' também é um $A-$módulo finitamente gerado.*
Demonstração: *Veja [6], página 25.*

Proposição 0.1.3 *Seja $0 \to M' \overset{f}{\to} M \overset{g}{\to} M'' \to 0$ uma sequência exata de $A-$módulos. Então M é Noetheriano se, e somente se, M' e M'' são Noetherianos.*
Demonstração: *Veja [6], página 25.*

Corolário 0.1.2 *Seja $\{M_i\}_{i=1}^n$ um conjunto de $A-$módulos Noetherianos. Então, o $A-$módulo $M = \bigoplus_{i=1}^n M_i$ é Noetheriano.*
Demonstração: *Veja [6], página 25.*

Proposição 0.1.4 *Seja $M' \xrightarrow{f} M \xrightarrow{g} M''$ uma sequência de $A-$módulos. As seguintes afirmações são equivalentes:*

(1) *A sequência $M' \xrightarrow{f} M \xrightarrow{g} M''$ é exata em M.*

(2) *A sequência $M'_P \xrightarrow{f_P} M_P \xrightarrow{g_P} M''_P$ é exata em M_P para todo $P \in \mathrm{Spec}(A)$.*

(3) *A sequência $M'_P \xrightarrow{f_P} M_P \xrightarrow{g_P} M''_P$ é exata em M_P para todo $P \in \mathrm{Max}(A)$.*

Demonstração: *Veja [6], página 73.*

Corolário 0.1.3 *Sejam $f : M \to N$ uma aplicação de $A-$módulos. A aplicação f é injetiva (resp. sobrejetica) se, e somente se, as aplicações f_P são injetivas (resp. sobrejetiva) para todo $P \in \mathrm{Max}(A)$.*
Demonstração: *Veja [6], página 73.*

Lema 0.1.7 *Sejam P um ideal primo e I, J dois ideais tais que $IJ \subseteq P$, então $I \subseteq P$ ou $J \subseteq P$.*
Demonstração: *Veja [6], página 89.*

Lema 0.1.8 *Seja A um anel. Sejam $I_1, \ldots, I_n$ ideais de A tais que I_i e I_j são coprimos se $i \neq j$. Então,*

(1) *$I_1 \cdots I_s$ é coprimo com I_{s+1}, para $s = 1, \ldots, n-1$.*

(2) *$I_1 \cdots I_n = I_1 \cap \ldots \cap I_n$.*

Demonstração: *Veja [6], página 89.*

0.2 Curvas Planas

Sejam $k \subseteq F \subseteq \overline{k}$ corpos. Seja $f \in k[x, y]$ um polinômio em duas variáveis com coeficientes em k. Defina $Z_f(F) := \{(a, b) \in F \times F | f(a, b) = 0\}$.

Definição 0.2.1 *O conjunto $Z_f(\overline{k})$ é chamado de* curva afim plana *, e $Z_f(F)$ é o conjunto dos pontos com coordenadas em F da curva afim plana definida por f.*

Definição 0.2.2 *Seja k um corpo. Uma* curva afim *sobre k é um par $(\mathrm{Max}(A), A)$. Onde A é uma $k-$álgebra finitamente gerado de dimensão um. Quando A é um domínio a curva $(\mathrm{Max}(A), A)$ é chamada* integral.

0.2.1 Anel de Funções

Seja $f \in \overline{k}[x,y]$ irredutível. Considere a curva afim plana definida por f $Z_f(\overline{k})$ e o anel $\overline{C}_f := \overline{k}[x,y]/\langle f\rangle$. Estes dois objetos estão fortemente relacionados. Considerando em $Z_f(\overline{k})$ e $\overline{k}$ a topologia de Zariski, podemos ver o anel $\overline{C}_f$ como o anel das funções contínuas sobre a curva $Z_f(\overline{k})$.

Proposição 0.2.1 *Seja $f \in \overline{k}[x,y]$ irredutível. Um conjunto não vazio $C \subseteq Z_f(\overline{k})$ é fechado com a topologia de Zariski se, e somente se, é a união finita de pontos de $Z_f(\overline{k})$ ou $C = Z_f(\overline{k})$.*
Demonstração: *Veja [6], página 40.*

Corolário 0.2.1 *Seja $f \in \overline{k}[x,y]$ irredutível. Sejam g e h dois polinômios tais que $\boldsymbol{g=h}$ como funções em $Z_f(\overline{k})$. Então $f|g-h$. Em particular, g e h definem o mesmo elemento em $\overline{C}_f$.*
Demonstração: *Veja [6], página 43.*

Tomando $Z_f(\overline{k})$ e $\overline{k}$ com a topologia de Zariski. Seja $C(Z_f(\overline{k}),\overline{k})$ o conjunto das funções contínuas de $Z_f(\overline{k})$ em $\overline{k}$. O corolário 0.2.1 mostra que a aplicação

$$i_f : \overline{C}_f \longrightarrow C(Z_f(\overline{k}),\overline{k})$$

que leva um polinômio g na função polinomial $\mathbf{g}$ definida por g é injetiva.

Definição 0.2.3 *Seja $f \in \overline{k}[x,y]$ irredutível de modo que $\overline{C}_f$ é um domínio. Denotaremos por $\overline{k}(Z_f)$ o corpo de frações de $\overline{C}_f$. Chamaremos este corpo de* corpo das funções racionais *da curva afim definida por f. Os elementos de $\overline{k}(Z_f)$ são chamados de funções racionais de $Z_f(\overline{k})$.*

Lema 0.2.1 *Seja $\alpha \in \overline{k}(Z_f)^*$. Existe uma quantidade finita de pontos $P_1,\ldots,P_s \in Z_f(\overline{k})$ tal que α define um aplicação contínua α: $Z_f(\overline{k}) \setminus P_1,\ldots,P_s \to \overline{k}$.*
Demonstração: *Veja [6], página 44.*

0.2.2 Pontos e Ideais Maximais

Aqui, estabeleceremos uma relação entre os pontos da curva $Z_f(\overline{k})$ e os maximais de $\overline{C}_f$. Seja

$$I_f : Z_f(\overline{k}) \longrightarrow \mathrm{Max}(\overline{C}_f)$$

que leva um ponto (a,b) nas funções de $\overline{C}_f$ que se anulam em (a,b). Para cada ponto em $Z_f(\overline{k})$ o conjunto $I_f(a,b)$ é de fato um maximal de $\overline{C}_f$, logo nossa aplicação I_f está bem definida. Quando dizemos que um função se anula em um ponto estamos dizendo que:

Definição 0.2.4 *Seja $\overline{g} \in \overline{C}_f$. O* valor *de $\overline{g}$ no ponto $(a,b) \in Z_f(\overline{k})$ é o elemento $g(a,b) \in \overline{k}$, onde $g \in \overline{k}[x,y]$ é tal que sua classe em $\overline{C}_f$ é $\overline{g}$.*

Lema 0.2.2 *Seja $f \in k[x,y] \setminus k$. Então $\langle f\rangle \notin \mathrm{Max}(k[x,y])$.*
Demonstração: *Veja [6], página 46.*

Corolário 0.2.2 *Seja $f \in \overline{k}[x,y]$ irredutível. M é um ideal maximal de $\overline{C}_f := \overline{k}[x,y]/\langle f\rangle$ se, e somente se, M é gerado pela imagem de $\langle x-a, y-b\rangle \trianglelefteq \overline{k}[x,y]$ em $\overline{C}_f$, com $f(a,b)=0$. Seja $I_f(a,b)$ o ideal de $\overline{C}_f$ gerado pelas imagens de $x-a$ e $y-b$ em $\overline{C}_f$. A aplicação*

$$I_f : (a,b) \mapsto I_f(a,b)$$

é uma bijeção entre $Z_f(\overline{k})$ e $\mathrm{Max}(\overline{C}_f)$.
Demonstração: *Veja [6], página 47.*

0.2.3 Morfismos de Curvas

Seja $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$ um aplicação entre duas curvas. A aplicação φ define unicamente duas aplicações

$$\varphi_1, \varphi_2 : Z_f(\overline{k}) \longrightarrow \overline{k}$$

tal que $\varphi(a,b) := (\varphi_1(a,b), \varphi_2(a,b))$.

Definição 0.2.5 *A aplicação $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$ entre duas curvas planas é um* morfismo de curvas planas afins *se existem $\alpha, \beta \in \overline{k}[x,y]$ tais que $\varphi_1(a,b) = \alpha(a,b)$ e $\varphi_2(a,b) = \beta(a,b)$. Além disso, se existe $\psi : Z_g(\overline{k}) \to Z_f(\overline{k})$ um morfismo tal que $\varphi \circ \psi = \mathrm{id}_{Z_g(\overline{k})}$ e $\psi \circ \varphi = \mathrm{id}_{Z_f(\overline{k})}$, então diremos que φ é um isomorfismo.*

Lema 0.2.3 *Seja $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$ um morfismo de curvas planas. Considere $Z_f(\overline{k})$ e $Z_g(\overline{k})$ com a topologia de Zariski. Então φ é uma aplicação contínua.*
Demonstração: *Veja [6], página 48.*

0.2.4 Pontos Singulares

Definição 0.2.6 *Um ponto $(a,b) \in Z_f(\overline{k})$ é um* ponto singular *se $(\partial f/\partial x)(a,b) = (\partial f/\partial y)(a,b) = 0$. Se existe $(a,b) \in Z_f(\overline{k})$ ponto singular diremos que a curva $Z_f(\overline{k})$ é singular. Caso contrário diremos que $Z_f(\overline{k})$ é não singular.*

Seja $\ell(x,y) = f_x(a,b)(x-a) + f_y(a,b)(y-b)$, onde f_x, f_y são as derivadas parciais de f. Quando $(a,b) \in Z_f(\overline{k})$ é não singular, a reta $Z_\ell(\overline{k})$ é chamada de *reta tangente* de $Z_f(\overline{k})$ no ponto (a,b).

Proposição 0.2.2 *O ponto $(a,b) \in Z_f(\overline{k})$ é não singular se, e somente se, o ideal maximal de $(\overline{C}_f)_M$ é gerado por um elemento.*
Demonstração: *Veja [6], página 67.*

Proposição 0.2.3 *Seja $f \in \overline{k}[x,y]$ irredutível. A curva $Z_f(\overline{k})$ é não singular se, e somente se, o domínio $\overline{C}_f$ é tal que sua localização em todo ideal maximal é um domínio local de ideais principais.*
Demonstração: *Veja [6], página 69.*

.

Capítulo

1

O Fecho Integral

Neste capítulo introduziremos alguns conceitos tais como, elementos e fecho integrais, produto de ideais e domínios de Dedekind. Apresentaremos vários resultados e propriedades que envolvem estes conceitos.

Durante este capítulo a tripla (A, K, L) sempre representa uma extensão de corpos $L|K$ e A um subanel de K.

1.1 Elementos Integrais

Sejam $L|K$ uma extensão finita de corpos e $\alpha \in L$. Pela finitude da extensão, α é algébrico sobre K. Denotaremos o polinômio minimal de α sobre K por $\min_K \alpha$.

Lema 1.1.1 *Sejam $L|K$ uma extensão de Galois e $G = \mathrm{Gal}(L|K)$ seu grupo de Galois. Seja $R \subseteq L$ um subanel tal que $\sigma(R) = R$ para todo $\sigma \in G$. Então para todo $r \in R$, os coeficientes de $\min_K r$ pertencem a $R \cap K$.*

Demonstração: *Como a extensão $L|K$ é de Galois, logo normal, todas as raízes de f pertencem a L. Considere $\alpha_1 = \alpha, \ldots, \alpha_n$ as raízes de f. Por [8], página 34, existem $\sigma_i \in G$ tal que $\sigma_i(\alpha) = \alpha_i, i = 1, \ldots, n$. Escreva*

$$f = \prod_{i=0}^{n} (y - \alpha_i).$$

Como $f(y) = \min_K \alpha$, por definição os coeficientes de f estão em K, uma vez que escrevemos cada α_i como $\sigma_i(\alpha)$ para algum $\sigma_i \in G$ e $\sigma_i(R) = R, \forall \sigma_i \in G$, concluímos que

cada $\alpha_i \in R, i = 1, \ldots, n$ e assim os coeficientes de f estão também em R, portanto em $K \cap R$. ■

Definição 1.1.1 *Seja A um subanel do anel L. Um elemento $\alpha \in L$ é dito integral sobre A se ele é raiz de um polinômio mônico $f(y) \in A[y]$. Quando $A = \mathbb{Z}$, o elemento α é dito um inteiro algébrico em L. Se todo elemento de L for integral sobre A, diremos que L é integral sobre A.*

Observação 1.1.1 *Nas condições do lema 1.1.1, todo elemento de R é integral sobre $R \cap K$ ou, equivalentemente, R é uma extensão integral de $R \cap K$.*

Dada a tripla (A, K, L), a duas maneiras de construir subanéis de L associados a A : R_1 o menor subanel de L que contém todos os elementos integrais sobre A; e R_2 o menor subanel de L que contém todos os subanéis de L integrais sobre A. Claramente $R_2 \subseteq R_1$. A seguir mostraremos que de fato, $R_1 = R_2$.

Antes de provarmos este fato, faremos uma observação e alguns exemplos para determinar explicitamente o conjunto dos integrais algébricos de $L|\mathbb{Q}$.

Observação 1.1.2 *Sejam K o corpo das frações de A, $L|K$ uma extensão finita e $\alpha \in L$. Claramente se $g(y) = \min_K \alpha \in A[y]$, então α é integral sobre A. Suponha agora que α é integral sobre A e seja $f(y) \in A[y]$ um polinômio mônico tal que $f(\alpha) = 0$. Então $g(y)|f(y)$ em $K[y]$. O lema 0.1.2 garante que se A é fatorial, então $g(y) \in A[y]$. Isto é, quando A é fatorial, α é integral sobre A se, e somente se,* $\min_K \alpha \in A[y]$.

Exemplo 1.1.1 *Sejam K o corpo de frações do domínio A e $\alpha \in K$, então* $\min_K \alpha = y - \alpha$. *Pela observação anterior se A é fatorial, então α é integral sobre A se, e somente se, $y - \alpha \in A[y]$, isto é, se e só se, $\alpha \in A$. Em particular os elementos de $\mathbb{Z}$ são os únicos inteiros algébricos em $\mathbb{Q}$.*

Exemplo 1.1.2 *(Corpo de Número Quadrático) Sejam $d \in \mathbb{Z}(d \neq 0, 1)$ livre de quadrado e $L = \mathbb{Q}(\sqrt{d})$. Os elementos de L integrais sobre $\mathbb{Z}$ formam o anel B, dado por:*

$$B = \begin{cases} \mathbb{Z}[\sqrt{d}] & se \quad d \equiv 2, 3(\text{mod}4), \\ \mathbb{Z}[(1+\sqrt{d})/2] & se \quad d \equiv 1(\text{mod}4). \end{cases}$$

Seja $\alpha = m + n\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. Se $n = 0$, então pelo exemplo anterior α é integral sobre $\mathbb{Z}$ se, e só se, $m \in \mathbb{Z}$. Seja $n \neq 0$, então

$$f(y) = \min_{\mathbb{Q}} \alpha = y^2 - 2my + m^2 - n^2 d.$$

Pela observação anterior α *é integral sobre* $\mathbb{Z}$ *se, e somente se,* $f(y) \in \mathbb{Z}[y]$*, isto é,* $2m, m^2 - n^2 d \in \mathbb{Z}$*. Sejam* $m = a/2$ *e* $m^2 - n^2 d = b$ *com* $a, b \in \mathbb{Z}$*.*

Suponha primeiramente $a = 2t + 1, t \in \mathbb{Z}$*. Assim,*

$$t^2 + t + 1/4 - n^2 d = b$$

$$\Rightarrow 1/4 - n^2 d = c \in \mathbb{Z}.$$

Considere $n = p/q$ *com* $(p, q) = 1$*, então*

$$q^2 - 4p^2 d = 4q^2 c \Rightarrow 4|q^2 \Rightarrow 2|q.$$

Segue que $2 \nmid p$ *e* $q = 2q_1$*, substituindo na equação acima temos,*

$$4{q_1}^2 - 4p^2 d = 16{q_1}^2 c \Rightarrow {q_1}^2 - dp^2 = 4{q_1}^2 c \quad (\star\star),$$

então ${q_1}^2 - dp^2$ *é par, portanto a duas possibilidades:*

(1) $\begin{cases} 2|{q_1}^2 \ e \\ 2|dp^2 \Rightarrow 2|d \Rightarrow d \equiv 2(\text{mod}4) \end{cases}$

(2) $\begin{cases} 2 \nmid {q_1}^2 \ e \\ 2 \nmid dp^2 \Rightarrow 2 \nmid d \Rightarrow d \equiv 1(\text{mod}4) \ ou \ d \equiv 3(\text{mod}4). \end{cases}$

CASO (1) *Então* q_1 *é par. Escreva* $q_1 = 2q_2$*, substituindo em* $(\star\star)$

$$4{q_2}^2 - dp^2 = 16c{q_2}^2 \Rightarrow 4|dp^2,$$

como d *é livre de quadrado* $4 \nmid d$*, então pelo menos* $2|p$ *o que é absurdo pois* $(p, q) = 1$ *e* $q = 2q_1$*. Assim concluímos que este caso não ocorre.*

CASO (2) *Agora consideremos* $2 \nmid {q_1}^2$ *e* $2 \nmid d$*. Suponha* $d = 4k + 3$*. Em* $(\star\star)$

$$ {q_1}^2 - p^2(4k + 3) = 4{q_1}^2 c \Rightarrow {q_1}^2 - p^2 4k - 3p^2 = 4{q_1}^2 c$$

$$\Rightarrow 4|{q_1}^2 - 3p^2 \Rightarrow {q_1}^2 \equiv 3p^2(\text{mod}4)$$

$$\Rightarrow {q_1}^2 - 3p^2 \equiv 0(\text{mod}4) \quad (\star\star\star).$$

Uma vez que $2 \nmid {q_1}^2$ *e* $2 \nmid p$*:*

$\begin{cases} q_1 \ pode \ ser \ 1 \ ou \ 3(\text{mod}4) \\ p \ pode \ ser \ 1 \ ou \ 3(\text{mod}4). \end{cases}$

Facilmente verifica-se para estes valores de q_1 *e* p *que* $(\star\star\star)$ *não tem solução, logo não pode ocorrer* $d \equiv 3(\text{mod}4)$*. Como um dos casos deve ocorrer concluímos que* $d \equiv 1(\text{mod}4)$*.*

De fato, para $d \equiv 1(\text{mod}4)$ *existem soluções para* $(\star\star\star)$, *tome por exemplo* $q_1 = p = 1$.

Observe ainda que como $q = 2q_1$ *e* $(p, q) = 1$,*então* $(p, q_1) = 1$. *A priori sabíamos que* $a^2/4 - n^2d = b \in \mathbb{Z}$, *assim* $a^2{q_1}^2 - p^2d = 4{q_1}^2$, *o que implica que* ${q_1}^2|p^2d$, *como* d *é livre de quadrados* $q_1|p^2$, *logo* $q_1|p$, *mas* $(p, q_1) = 1$ *e portanto* $q_1 = 1$.

Concluímos que quando a *é ímpar* $(m = a/2)$,*então* $q = 2$, $n = p/2$ *e* $d \equiv 1(\text{mod}4)$. *Assim o anel dos elementos integrais de* $\mathbb{Q}[\sqrt{d}]$ *sobre* $\mathbb{Z}$ *é* $\mathbb{Z}[(1+\sqrt{d})/2]$ *quando* $d \equiv 1(\text{mod}4)$ *pois dado* $\alpha = m + n\sqrt{d}$ *com* $m, n \in \mathbb{Q}$ *integral sobre* $\mathbb{Z}$ *concluímos que* $m = a/2$ *e* $n = p/2$ *com* $a, p \in \mathbb{Z}$.

Suponha agora $a = 2t, t \in \mathbb{Z}$. *Sabemos que* $d \equiv 2(\text{mod}4)$ *ou* $d \equiv 3(\text{mod}4)$. *Como* $a = 2k$, *então* $m = a/2 \in \mathbb{Z}$, *logo* $n^2d \in \mathbb{Z}$. *Escreva* $n = p/q, (p, q) = 1$, *então* $p^2d = bq^2, b \in \mathbb{Z}$, *assim* $q^2|p^2d$ *o que implica que* $q^2|d$, *uma vez que* d *é livre de quadrados concluímos que* $q = 1$, *portanto* $n \in \mathbb{Z}$. *Neste caso* $\alpha = m + n\sqrt{d}$ *com* $m, n \in \mathbb{Z}$ *o que conclui nossa descrição do anel dos elementos de* $\mathbb{Q}[\sqrt{d}]$ *integrais sobre* $\mathbb{Z}$.

Claramente $\sqrt{d}$ *e* $(1 + \sqrt{d})/2$ *são integrais sobre* $\mathbb{Z}$ *quando* $d \equiv 1(\text{mod}4)$, *de fato, seu polinômio minimal é* $y^2 - y - (d - 1)/4 \in \mathbb{Z}[y]$.

O anel $\mathbb{Z}[\sqrt{d}]$ é sempre um subanel de $\mathbb{Z}[(1 + \sqrt{d})/2]$. Quando $d \equiv 1(\text{mod}4)$, o anel $\mathbb{Z}[(1 + \sqrt{d})/2]$ possui boas propriedades aritméticas, por exemplo, este anel pode ser fatorial, ao contrário o anel $\mathbb{Z}[\sqrt{d}]$ é nunca fatorial.

Exemplo 1.1.3 *Sejam* k *um corpo,* $A = k[x], K = k(x)$ *e* $\overline{k(x)} = \overline{K}$ *o fecho algébrico de* K. *Um polinômio não constante em* $k[x]$ *é livre de quadrado se ele se fatora em* $\overline{k}[x]$ *como produto de distintos polinômios irredutíveis. Sejam* $f(x) \in k[x]$ *um polinômio livre de quadrados e* $\sqrt{f}$ *a raiz em* $\overline{K}$ *do polinômio mônico* $y^2 - f(x) \in A[y]$. *Tome* $L := K(\sqrt{f})$, *o elemento* $\sqrt{f}$ *é claramente integral sobre* $k[x]$. *E mais, todo elemento de* $k[x][\sqrt{f}]$ *é integral sobre* $k[x]$. *De fato, tome* $\alpha \in k[x][\sqrt{f}]$, *então* $\alpha = g + h\sqrt{f}$ *com* $g, h \in k[x]$, *logo* α *é raiz do polinômio* $y^2 - 2yg + g^2 - h^2f \in k[x][y]$ *e portanto todo elemento de* $k[x][\sqrt{f}]$ *é integral sobre* $k[x]$. *Agora considere* k *um corpo algebricamente fechado de característica* $\neq 2$. *Nós afirmamos que o conjunto de elementos de* $K(\sqrt{f})$ *que são integrais sobre* $k[x]$ *é igual ao anel:*

$$B := k[x][\sqrt{f}] = \{m + n\sqrt{f} | m, n \in k[x]\}.$$

A prova desta afirmação é análoga ao exemplo anterior, uma vez que o domínio A *é fatorial. Seja* $\alpha = m + n\sqrt{f} \in k(x)(\sqrt{f})$, *com* $m, n \in k(x)$. *Se* $n = 0$, *então pelo exemplo 1.1.1 tem-se que* α *é integral sobre* $k[x]$ *se, e somente se,* $m \in k[x]$. *Se* $n \neq 0$,

$$\min_{k(x)}\alpha = y^2 - 2my + m^2 - n^2f.$$

A observação 1.1.2 mostra que α é integral sobre $k[x]$ se, e somente se, $2m \in k[x]$ e $m^2 - n^2 f \in k[x]$. Uma vez que a característica de k é diferente de dois, o elemento 2 é invertível em k. Assim $2m \in k[x]$ se, e só se, $m \in k[x]$. Segue que necessariamente $n^2 f \in k[x]$. Como $n \in k(x)$, escreva $n = p/q$ com $p, q \in k[x]$ e $(p, q) = 1$, então $p^2 f = hq^2$, para algum $h \in k[x]$. Segue que $q^2 | p^2 f$, como $(p, q) = 1$, então $q^2 | f$. Uma vez que f é livre de quadrado tem-se $q = 1$. Portanto $n \in k[x]$ e $\alpha \in B$. Assim segue que B é gerado, como $k[x]-$módulo por 1 e $\sqrt{f}$.

Em ambos os exemplos acima o conjunto dos elementos integrais de L sobre A é um anel. De fato, o fecho integral é sempre um anel, a próxima proposição é o principal resultado para mostrar esse fato em geral.

Proposição 1.1.1 *Sejam A um subanel de um corpo L e $\alpha \in L$. São equivalentes:*

1. *O elemento α é integral sobre A.*
2. *O subanel $A[\alpha]$ de L, gerado por A e α é finitamente gerado como $A-$módulo.*
3. *Existe um $A-$submódulo finitamente gerado M de L tal que $\alpha M \subseteq M$.*

Demonstração: **(1 $\Rightarrow$ 2)** *Seja α integral sobre A, então existem $a_0, \ldots a_{n-1} \in A$ tais que,*

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Afirmamos que o $A-$módulo $A[\alpha]$ é gerado por $1, \alpha, \ldots, \alpha^{n-1}$. Uma vez que qualquer elemento $\beta \in A[\alpha]$ é da forma,

$$\beta = \sum_{i=0}^{m} c_i \alpha^i, \quad com\ c_i \in A, \forall i.$$

Para mostrar nossa afirmação resta mostrar que $\alpha^i, i \geqslant 1$ pode ser expressado como combinação linear de $1, \alpha, \ldots, \alpha^{n-1}$ com coeficientes A. Vamos proceder a prova por indução sobre $i \geqslant n$. Se $i = n$, então

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots + a_1\alpha - a_0 \quad (\star)$$

Para $i > n$, tome $j \leqslant i - 1$, assim por hipótese de indução α^j pode ser expressado em termos de $1, \alpha, \ldots, \alpha^{n-1}$. multiplique $(\star)$ por α^{i-n}

$$\alpha^i = -a_0\alpha^{i-n} - a_1\alpha^{i-n+1} - \ldots - a_{n-1}\alpha^{i-1}.$$

Como todos os $\alpha^j, j = i-n, \ldots, i-1$ são todos expressados em termos de $1, \alpha, \ldots, \alpha^{n-1}$, portanto concluímos que $A[\alpha]$ é gerado por $1, \alpha, \ldots, \alpha^{n-1}$ como $A-$módulo.

(2 ⇒ 3) *Basta tomar* $M = A[\alpha]$.

(3 ⇒ 1) *Sejam* $e_1, \ldots, e_n$ *os geradores de* M *como* $A-$*módulo. Como* $\alpha e_i \in M, i = 1, \ldots, n$ *podemos expressar tais elementos como combinação linear dos* $e_j, j = 1, \ldots, n$.

$$\alpha e_i = \sum_{j=1}^{n} b_{ij} e_j, b_{ij} \in A, 1 \leqslant i, j \leqslant n. \quad (\star)$$

Sejam $N := (b_{ij})_{1 \leqslant i,j \leqslant n}$ *e* $E := [e_1 \ \cdot \ \cdot \ \cdot \ e_n]^t$. *As igualdades em* $(\star)$ *implicam que* $\alpha E = NE$, *ou,* $(\alpha \mathrm{Id} - N)E = 0$. *Como* $E \neq 0$, *concluímos que* $\det(\alpha \mathrm{Id} - N) = 0$. *Então,*

$$0 = \det(\alpha \mathrm{Id} - N) = \alpha^n + \sum_{i=0}^{n-1} a_i \alpha^i,$$

onde $a_0, \ldots, a_{n-1}$ *são expressões em termo das entradas de* N, *portanto elementos de* A. *Logo* α *é integral sobre* A. ■

Corolário 1.1.1 *Seja* A *um subanel do corpo* L. *O conjunto* B *de todos os elementos de* L *integrais sobre* A *é um anel.*
Demonstração: *Todo elemento* $\alpha \in A$ *é integral sobre* A, *uma vez que o mesmo é raiz do polinômio linear* $y - \alpha \in A[y]$. *Então* $A \subseteq B$, *em particular* $0, 1 \in B$. *Para mostrar que* B *é um subanel de* L *resta mostrar que se* α *e* β *são integrais sobre* A, *então* $\alpha - \beta$ *e* $\alpha\beta$ *são integrais sobre* A. *Como* α, β *são integrais sobre* A, *os subanéis* $A[\alpha]$ *e* $A[\beta]$ *são finitamente gerados como* $A-$*módulos (proposição 1.1.1). Sejam* $e_1, \ldots, e_r$ *geradores para* $A[\alpha]$ *e* $f_1, \ldots, f_s$ *geradores para* $A[\beta]$ *como* $A-$*módulos. Tome* $M = A[\alpha, \beta]$ *subanel de* L, M *é finitamente gerado como* $A-$*módulo, de fato, o conjunto* $\{e_i f_j | 1 \leqslant i \leqslant r; 1 \leqslant j \leqslant s\}$ *é gerador de* M. *Uma vez que* $(\alpha - \beta)M \subseteq M$ *e* $(\alpha\beta)M \subseteq M$, *segue da equivalência 3* $\Leftrightarrow$ *1 da proposição 1.1.1 que* $\alpha - \beta$ *e* $\alpha\beta$ *são integrais sobre* A. ■

O corolário anterior motiva a seguinte definição chave:

Definição 1.1.2 *Seja* A *um subanel do corpo* L. *O* fecho integral B *de* A *em* L *é o anel dos elementos de* L *integrais sobre* A. *Quando* L *é um corpo numérico o fecho integral* B *de* $\mathbb{Z}$ *é chamado* o anel dos integrais algébricos *de* L. *Por vezes denotado de* $\mathcal{O}_L$.

Definição 1.1.3 *Um domínio é dito ser* integralmente fechado *se ele é igual a seu fecho integral em seu corpo de frações.*

Exemplo 1.1.4 *Os anéis* $\mathbb{Z}$ *e* $k[x]$ *são integralmente fechados. Este fato segue do exemplo 1.1.1 e da observação 1.1.2. O próximo lema fornece uma prova diferente destes fatos sem usar a observação 1.1.2.*

Exemplo 1.1.5 *Quando $d \equiv 1(\mathrm{mod}4)$ o anel $\mathbb{Z}[\sqrt{d}]$ não é integralmente fechado. De fato, o elemento $(1+\sqrt{d})/2$ é integral sobre $\mathbb{Z}[\sqrt{d}]$ pois é integral sobre $\mathbb{Z}$, mas $(1+\sqrt{d})/2$ não pertence a $\mathbb{Z}[\sqrt{d}]$. Segue do próximo lema também que o anel $\mathbb{Z}[\sqrt{d}]$ não é fatorial também.*

Lema 1.1.2 *Os domínios fatoriais são integralmente fechados.*
Demonstração: *Sejam A um domínio fatorial e K seu corpo de frações. Seja $z \in K$ integral sobre A. Sem perda de generalidade podemos supor que $z = b/c$, com b, c coprimos em A. Considere,*

$$(b/c)^n + a_{n-1}(b/c)^{n-1} + \cdots + a_1(b/c) + a_0 = 0$$

a relação integral de b/c sobre A. Então

$$-b^n = c(a_{n-1}b^{n-1} + a_{n-2}b^{n-2}c + \cdots + a_1bc^{n-2} + a_0c^{n-1}).$$

Portanto $c|b^n$. Uma vez que b, c são coprimos, concluímos que c deve ser inversível em A, o que implica que $c^{-1} \in A$, logo $z \in A$. ■

A recíproca do lema anterior de fato não é válida. Para ver isso, basta tomar $A = \mathbb{Z}[\sqrt{5}]$. Pelo exemplo 1.1.2, o fecho integral de A em $\mathbb{Q}(\sqrt{5})$ é $\mathbb{Z}[(1+\sqrt{5})/2] \neq \mathbb{Z}[\sqrt{5}]$.

A seguir mostraremos que a afirmação da observação 1.1.2 vale para domínios integralmente fechados.

Lema 1.1.3 *Sejam A um domínio integralmente fechado, K seu corpo de frações e $L|K$ uma extensão de corpos. Seja $\alpha \in L$ algébrico sobre K. Então α é integral sobre A, se, e somente se, os coeficientes de $\min_K(\alpha)$ pertencem a A.*
Demonstração: *Se $\min_K(\alpha) \in A[y]$, por definição α é integral sobre A. Para a recíproca, suponha $\alpha \in L$ integral sobre A. Sejam $f(y) \in A[y]$ um polinômio mônico tal que $f(\alpha) = 0$, M o corpo de raízes de $\min_K(\alpha)$ e $\alpha_1, \ldots, \alpha_n$ os conjugados de α em M. Como $\min_K(\alpha) = \prod_{i=1}^{n}(y - \alpha_i) | f(y)$, segue que cada $\alpha_i, i = 1, \ldots, n$ é integral sobre A. Visto que o conjunto dos elementos integrais sobre A é um subanel B de M, concluímos que os coeficiente de $\min_K(\alpha)$ pertencem a B, portanto integrais sobre A. Como A é integralmente fechado $B \cap K = A$ o qual implica que $\min_K(\alpha) \in A[y]$.* ■

Proposição 1.1.2 *Sejam $A \subseteq B \subseteq C$ domínios. Então C é integral sobre A, se,e somente se, C é integral sobre B e B integral sobre A.*
Demonstração: *Suponha C integral sobre A. Pela inclusões $A \subseteq B \subseteq C$, claramente C é integral sobre B e B é integral sobre A.*

Suponha agora C integral sobre B e B integral sobre A. Seja $\alpha \in C$, como C é integral sobre B podemos encontrar $g(y) = y^n + b_{n-1}y^{n-1} + \cdots + b_0 \in B[y]$ tal que $g(\alpha) = 0$. Tome $B' := A[b_0 \ldots, b_{n-1}]$, este é o menor subanel de C gerado por A e o conjunto $\{b_0 \ldots, b_{n-1}\}$. Afirmamos que B' é finitamente gerado como $A-$módulo. Como B é integral sobre A, os $b_i's$ são integrais sobre A. Pela proposição 1.1.1 $A[b_0]$ é finitamente gerado como $A-$módulo e por indução $A[b_0 \ldots, b_{n-1}]$ é finitamente gerado como $A-$módulo: suponha $A[b_0 \ldots, b_{n-2}]$ finitamente gerado como $A-$módulo e considere um conjunto gerador $\{e_1, \ldots, e_r\}$. Como b_{n-1} é integral sobre A, pela proposição 1.1.1, $A[b_{n-1}]$ é finitamente gerado como $A-$módulo, tome $\{f_1, \ldots, f_s\}$ um conjunto gerador para $A[b_{n-1}]$ como $A-$módulo, assim $A[b_0 \ldots, b_{n-2}, b_{n-1}]$ é gerado por $\{e_i f_j | 1 \leqslant i \leqslant r; 1 \leqslant j \leqslant s\}$ como $A-$módulo e portanto finitamente gerado. Considere agora $B'[\alpha]$ o menos subanel de C contendo B' e α. Então $B'[\alpha]$ é um $A-$módulo gerado pelo conjunto:

$$\{e_i f_j \alpha^k | 1 \leqslant i \leqslant r; 1 \leqslant j \leqslant s; 0 \leqslant k \leqslant n-1\}.$$

Uma vez que $\alpha B'[\alpha] \subseteq B'[\alpha]$, pela proposição 1.1.1, que α é integral sobre A. ■

Proposição 1.1.3 *Sejam A um domínio, K seu corpo de frações e $L|K$ uma extensão finita. Seja B o fecho integral de A em L.*

1. *Seja $\alpha \in L$. Então existe $b \in B$ e $a \in A$ tal que $\alpha = b/a$. Em particular, L é o corpo de frações de B.*
2. *O anel B é integralmente fechado.*
3. *Se A é integralmente fechado, então $B \cap K = A$.*
4. *Se $L|K$ é Galois com grupo de Galois G, então $\sigma(B) = B$ para todo $\sigma \in G$. Além disso, se A é integralmente fechado, então $A = B^G := \{b \in B | \sigma(b) = b, \forall \sigma \in G\}$.*

Demonstração: *1- Sejam $\alpha \in L$ e $g(y) = \min_K(\alpha)$. Como K é o corpo de frações de A podemos escrever:*

$$g(y) = y^n + \frac{c_{n-1}}{d_{n-1}}y^{n-1} + \cdots + \frac{c_1}{d_1}y + \frac{c_0}{d_0}, \quad c_i, d_i \in A, \forall i.$$

Tome $a := \prod_{i=0}^{n-1} d_i \in A$, uma vez que $a^n g(\alpha) = 0$,

$$(a\alpha)^n + \frac{c_{n-1}}{d_{n-1}}a(a\alpha)^{n-1} + \cdots + \frac{c_1}{d_1}a^{n-1}(a\alpha) + \frac{c_0}{d_0}a^n = 0.$$

Claramente $\frac{c_i}{d_i}a \in A, i = 0, \ldots n-1$. Assim a equação acima é a relação integral de $a\alpha$ sobre A. Então, $b = a\alpha \in B$, pois B é o fecho integral de A, logo $\alpha = b/a$ com $b \in B$ e $a \in A$ como queríamos.

2- Sejam B não integralmente fechado e B' é o fecho integral de B em L. Como B é integral sobre A e B' integral sobre B, pela proposição 1.1.2, B' é integral sobre A, o que é absurdo, pois neste caso B não seria o fecho integral de A em L. Portanto B é integralmente fechado.

3- Como B é o fecho integral de A, então $B \cap K$ é integral sobre A. Mas $B \cap K \subseteq K$ e por A ser integralmente fechado, todos os elementos de K que são integrais sobre A pertencem a A, logo $B \cap K \subseteq A$. Portanto $B \cap K = A$.

4- Sejam $\alpha \in B$ e $f(y) \in A[y]$ tal que $f(\alpha) = 0$. Tome $\sigma \in G$, então $0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$, ou seja, $\sigma(\alpha)$ é integral sobre A, portanto $\sigma(\alpha) \in B$. Pela hipótese $K = L^G$, então $B^G = L^G \cap B = K \cap B$ e quando A é integralmente fechado, pelo item (3), $B^G = B \cap K = A$ ■

Corolário 1.1.2 *Sejam A um domínio e K seu corpo de frações. Seja $L|K$ uma extensão de grau n e considere B o fecho integral de A em L. Então existe uma base $\{e_1, \ldots, e_n\}$ de L sobre K dos elementos de B.*
Demonstração: *Seja $\{f_1, \ldots, f_n\}$ uma base para L sobre K, pelo item (1) da proposição anterior podemos encontrar $c_1, \ldots, c_n \in A$ e $e_1, \ldots, e_n \in B$ tais que $f_i = e_i/c_i, i = 1, \ldots, n$. Então $\{e_1, \ldots, e_n\}$ é uma base para L sobre K contida em B.* ■

1.2 Produto de Ideais

Como foi comentado anteriormente, existem domínios que não são fatoriais e portanto não principais. Um exemplo simples é $\mathbb{Z}[\sqrt{-5}]$. De fato, basta observar que

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Demonstrar que $2, 3, (1+\sqrt{-5})$ e $(1-\sqrt{-5})$ são irredutíveis e não associados é elementar. Lembramos que por definição a e b são associados se $a = ub$ para algum u inversível. Mostraremos que os únicos inversíveis de $\mathbb{Z}[\sqrt{-5}]$ são 1 e -1. Suponha,

$$1 = (a + b\sqrt{-5})(c + d\sqrt{-5}).$$

Logo,

$$\begin{cases} ac - 5bd = 1 & (\star) \\ ad + bc = 0 & (\star\star) \end{cases}$$

Então $(a, b) = (a, d) = (c, b) = (c, d) = 1$ e $ad = -bc$. Desta última concluímos $a|c, c|a, b|d$ e $d|b$, portanto $c = \pm a$ e $b = \pm d$. Da segunda equação acima, $2(ab) = 0$, logo $a = 0$ ou

$b = 0$. Se $a = 0$, então $4 \pm 5b^2 = 1$, que é absurdo. Portanto $b = d = 0$ e $a^2 = 1$, isto é, $a = \pm 1$.

Para mostrar a irredutibilidade de $2, 3, (1+\sqrt{-5})$ e $(1-\sqrt{-5})$ usaremos a função norma definida em $\mathbb{Z}[\sqrt{-5}]$ por $N(a+b\sqrt{-5}) = a^2 - 5b^2$. Por exemplo, no caso de $1+\sqrt{-5}$, observe que $N(1+\sqrt{-5}) = 6 = 1 \cdot 6 = 2 \cdot 3$. Se $1+\sqrt{-5} = \alpha\beta$, no primeiro caso $N(\alpha) = 1$, isto é, $\alpha = \pm 1$ e no segundo caso $N(\alpha) = 2$ o que é impossível. Uma vez que os únicos elementos inversíveis de $\mathbb{Z}[\sqrt{-5}]$ são 1 e -1 claramente os elementos $2, 3, (1+\sqrt{-5}), (1-\sqrt{-5})$ não são associados. Portanto o elemento 6 tem duas fatorações distintas em $\mathbb{Z}[\sqrt{-5}]$.

A busca para substituir a propriedade de fatoração única de elementos levou Dedekind ao estudo da propriedade de *fatoração única de ideais*. Nesta seção introduziremos as definições chaves necessárias para enunciar o principal teorema de Dedekind sobre fatoração única de ideais.

Definição 1.2.1 *Dois ideais I, J de um anel A são ditos* coprimos, *se $I + J = A$. Note que isto é equivalente a existência de $x \in I$ e $y \in J$ tais que $x + y = 1$.*

Lema 1.2.1 *Se I e J são coprimos, então $IJ = I \cap J$.*
Demonstração: *Sabemos que sempre $IJ \subseteq I \cap J$. Dado $z \in I \cap J$ considere $x \in I$ e $y \in J$ tais que $x + y = 1$, então $z = zx + zy \in IJ$.* ■

Observação 1.2.1 *Sejam P, Q dois ideais primos do anel A. Se P é maximal e $Q \not\subseteq P$, então P, Q são coprimos. De fato, o ideal $P + Q$ contém estritamente o ideal P o qual é maximal, logo $P + Q = A$. Entretanto, em geral dois ideais primos não são necessariamente coprimos. Por exemplo, considere o domínio $\mathbb{Z}[x]$ e seja $p \in \mathbb{Z}$ primo. Como p é irredutível em $\mathbb{Z}[x]$ o ideal $P := \langle p \rangle$ é primo em $\mathbb{Z}[x]$. Considere agora o ideal $Q = \langle x \rangle$ em $\mathbb{Z}[x]$,uma vez que x é irredutível Q também é um ideal primo, mas o ideal $P + Q = \langle p, x \rangle \neq \mathbb{Z}[x]$. De fato, $P + Q$ é maximal pois $\mathbb{Z}[x]/\langle p, x \rangle \cong \mathbb{Z}_P$. Portanto P e Q não são coprimos.*

Definição 1.2.2 *Um domínio R é dito ter a propriedade da* fatoração única de ideais *se todo ideal não trivial I de R pode ser escrito unicamente como $I = \mathfrak{P}_1 \cdots \mathfrak{P}_s$, onde cada $\mathfrak{P}_i$ é um ideal primo, isto é, se $I = \mathfrak{Q}_1 \cdots \mathfrak{Q}_n$, então $s = n$ e $\{\mathfrak{P}_1, \ldots \mathfrak{P}_s\} = \{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_n\}$.*

Note que esta definição é parecida com a definição de fatoração única para elementos um domínio de fatoração única. Nesta nova definição ideais substituem os elementos e os ideais primos substituem os elementos irredutíveis.

Exemplo 1.2.1 *Um domínio A de ideais principais tem a propriedade de fatoração única de ideais. De fato, todo domínio de ideais principais é fatorial, veja [1], página* 112. *Sejam $I = \langle a\rangle \trianglelefteq A$ e $a = \alpha_1 \cdots \alpha_n$, onde $\alpha_i, \ldots, \alpha_n \in A$ irredutíveis. É fácil ver que $I = \langle a\rangle = \langle\alpha_1\rangle \cdots \langle\alpha_n\rangle$ e cada $\langle\alpha_i\rangle$ é primo.*

O próximo teorema cuja demonstração será feita no final deste capítulo, fornece exemplo para domínios que possuem a propriedade da fatoração única de ideais.

Teorema 1.2.1 *Seja $L|K$ uma extensão separável. Seja $A \subseteq K$ um domínio principal, então o fecho integral B de A em L tem propriedade da fatoração única de ideais.*

Um caso particular e interessante deste teorema é quando $A = \mathbb{Z}$ e $K = \mathbb{Q}$, ou seja, o fecho integral de $\mathbb{Z}$ em qualquer extensão de $\mathbb{Q}$ sempre possui a propriedade de fatoração única de ideais.

A seguir veremos um exemplo de um domínio que não possui a propriedade de fatoração única de ideais.

Exemplo 1.2.2 *Seja $\partial := \frac{1+\sqrt{5}}{2}$. Observe que $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{5}] \subseteq \mathbb{Z}[\partial]$. Mostraremos que o domínio $\mathbb{Z}[\sqrt{5}]$ não tem a propriedade da fatoração única de ideais. O ideal $\mathfrak{Q} = \langle 2\rangle$ em $\mathbb{Z}[\partial]$ é maximal. Para provar este fato basta mostrar que $\frac{\mathbb{Z}[\partial]}{\langle 2\rangle}$ é corpo. De fato,*

$$\begin{aligned}\tfrac{\mathbb{Z}[\partial]}{\langle 2\rangle} &\simeq \tfrac{\mathbb{Z}[y]/\langle y^2-y-1\rangle}{\langle 2\rangle}\\ &\simeq \tfrac{\mathbb{Z}[y]}{\langle 2, y^2-y-1\rangle}\\ &\simeq \tfrac{\mathbb{Z}_2[y]}{\langle y^2-y-1\rangle}.\end{aligned}$$

O polinômio y^2-y-1 não tem raízes em $\mathbb{Z}_2$ portanto é irredutível sobre $\mathbb{Z}_2$, e $\langle y^2-y-1\rangle$ é maximal, Assim $\frac{\mathbb{Z}_2[y]}{\langle y^2-y-1\rangle}$ é corpo, a saber $\mathbb{F}_4$. Logo $\mathfrak{Q}$ é maximal. Observe que ∂ é inversível em $\mathbb{Z}[\partial]$ pois

$$\frac{(1+\sqrt{5})}{2}\cdot\frac{(-1+\sqrt{5})}{2} = 1$$

e o inverso de ∂ é $\partial - 1$. Desde que $1-\sqrt{5} = (-\partial^{-1})\cdot 2$, observamos que $1-\sqrt{5} \in \mathfrak{Q}$. Afirmamos agora que o ideal $\mathfrak{P} = \langle 2, 1-\sqrt{5}\rangle$ é maximal em $\mathbb{Z}[\sqrt{5}]$. De fato,

$$\frac{\mathbb{Z}[\sqrt{5}]}{\mathfrak{P}} \simeq \frac{\mathbb{Z}_2[y]}{\langle 1-y, y^2-5\rangle} = \frac{\mathbb{Z}_2[y]}{\langle 1-y\rangle} \simeq \mathbb{Z}_2.$$

Considere o ideal $I := \langle 2\rangle\cdot\mathbb{Z}[\sqrt{5}]$, claramente $I \subseteq \mathfrak{P}$. Afirmamos que $\mathfrak{P}$ é o único ideal primo de $\mathbb{Z}[\sqrt{5}]$ que contém I. De fato,

$$\frac{\mathbb{Z}[\sqrt{5}]}{\langle 2\rangle} \simeq \mathbb{Z}_2[y]\langle (y-1)^2\rangle.$$

Uma vez que o ideal principal $\langle y-1\rangle$ é o único ideal primo de $\mathbb{Z}_2[y]$ que contém $\langle (y-1)^2\rangle$ segue que $\mathfrak{P}$ é o único ideal primo de $\mathbb{Z}[\sqrt{5}]$ que contém I, o que prova nossa afirmação. Desde que $\mathbb{Z}[\sqrt{5}]/I$ não é domínio e $\mathbb{Z}[\sqrt{5}]/\mathfrak{P}$ é um corpo, concluímos que $I \subsetneqq \mathfrak{P}$. Suponha que I pode ser escrito como $I = \mathfrak{P}_1 \cdots \mathfrak{P}_n$, com $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ ideais primos de $\mathbb{Z}[\sqrt{5}]$. Como $\mathfrak{P}_1 \cdots \mathfrak{P}_n \subseteq \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_n$, concluímos que $I \subseteq \mathfrak{P}_i, \forall i$. Portanto $\mathfrak{P}_i = \mathfrak{P}, \forall i$. Logo $I = \mathfrak{P}^n$. Afirmamos que $\mathfrak{P}^2 \subseteq I$:

$$\begin{aligned} \mathfrak{P}^2 &= \langle 2^2, 2(1-\sqrt{5}), (1-\sqrt{5})^2\rangle \\ &= \langle 4, 2(1-\sqrt{5}), 6-2\sqrt{5}\rangle \\ &= \langle 4, 2(1-\sqrt{5})\rangle \subseteq I, \end{aligned}$$

essa inclusão ainda é própria, isto é, $\mathfrak{P}^2 \subsetneqq I = \mathfrak{P}^n$, que é possível apenas para $n = 1$. O que é absurdo uma vez que $I \neq \mathfrak{P}$.

1.3 Anéis Noetherianos

Pelo exemplo 1.1.2 e o exemplo discutido no início da seção 1.2 concluímos que o fecho integral de um domínio principal não é sempre principal. O objetivo principal desta seção é mostrar que todos os ideais deste fecho são finitamente gerados, mais precisamente, se A é um domínio principal, K seu corpo de frações e $L|K$ uma extensão separável, então todos ideais do fecho integral de A em L são finitamente gerados.

Definição 1.3.1 *Um anel é chamado de anel* Noetherianos *se todos os ideais são finitamente gerados.*

Exemplo 1.3.1 *1. Os corpos são exemplos de anéis Noetherianos, uma vez que possuem apenas os ideais triviais.*

2. *Um domínio principal é um anel Noetheriano.*
3. *Sejam K um corpo e $R := \frac{K[x]}{\langle x^2\rangle}$. Este anel possui apenas um ideal não trivial, a saber, o ideal gerado pela classe de x, portanto Noetheriano.*
4. *Em geral, se A é anel Noetheriano e I ideal de A, então A/I é Noetheriano.*

Proposição 1.3.1 *Sejam A um anel Noetheriano e M um $A-$módulo finitamente gerado, então M é Noetheriano, isto é, todo submódulo de M é finitamente gerado.*
Demonstração: *Veja [11], página 75.*

Corolário 1.3.1 *Sejam $A \subseteq B$ anéis. Se A é Noetheriano e B é finitamente gerado como $A-$módulo, então B é Noetheriano.*
Demonstração: *Basta observar que os ideais de B são submódulos de B visto como $A-$módulo.*

Para mostrar o nosso resultado principal desta seção, precisamos da seguinte proposição.

Proposição 1.3.2 *Sejam A um domínio integralmente fechado no seu corpo de frações K, $L|K$ uma extensão separável de grau n e B o fecho integral de A em L. Considere $\{e_1, \ldots, e_n\} \subseteq B$ uma base para L sobre K. Então existe $d \in A \setminus \{0\}$ tal que o $A-$módulo B está contido no $A-$módulo livre gerado por $\frac{e_1}{d}, \ldots, \frac{e_n}{d}$, isto é,*

$$Ae_1 \oplus \cdots \oplus Ae_n \subseteq B \subseteq A\frac{e_1}{d} \oplus \cdots \oplus A\frac{e_n}{d} \subseteq L.$$

Demonstração: *A existência da base para $L|K$ contido em B foi mostrada no corolário 1.1.2. A primeira inclusão claramente é satisfeita. Seja $\alpha \in B$, como $B \subseteq L$,*

$$\alpha = x_1e_1 + \cdots + x_ne_n, \quad x_1, \ldots, x_n \in K.$$

Então para todo $d' \in A \setminus 0$,

$$\alpha = d'x_1\frac{e_1}{d'} + \cdots + d'x_n\frac{e_n}{d'}.$$

Basta mostrar a existência de um elemento $d \neq 0$ tal que $dx_i \in A, i = 1, \ldots, n$ e para todo $\alpha \in B$. Seja $\overline{K}$ o fecho algébrico de K. Pela separabilidade de $L|K$, existem n monomorfismos distintos $\sigma_1, \ldots, \sigma_n$ de L em $\overline{K}$ (veja [9], pág. 33). Seja $M := (\sigma_i(e_j))_{1 \leqslant i,j \leqslant n}$. Observe,

$$\begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} = M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Seja M^* a adjunta da matriz M. Então

$$M^* \cdot \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix} = MM^* \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \det(M)x_1 \\ \vdots \\ \det(M)x_n \end{pmatrix}.$$

Como as entradas de M^* são os determinantes das sub-matrizes $(n-1) \times (n-1)$ de M, elas são integrais sobre A. Uma vez que $\alpha \in B$, $\sigma_i(\alpha) \in B$, logo $\det(M)x_i$ é integral sobre A para todo i. Mas $\det(M) \notin K$. De fato, pela finitude de $L|K$, esta extensão é algébrica, portanto $L \subseteq \overline{K}$. Para cada i, seja η_i a extensão de σ_i a $\overline{K}$. Por outro lado, para todo i, $\eta_i(\det(M)) = \pm\det(M)$, ou seja, η_i permuta as linhas da matriz M. Isto mostra que $\det(M)$ pode não pertencer a K. Mas o elemento $d := \det^2(M) \in K$ pois é invariante sobre todo automorfismo η de $\overline{K}$ tal que $\eta|_K = \mathrm{id}_K$. Por A ser integralmente

fechado e $d \in K$ é integral sobre A, concluímos que $d \in A$ e então para todo i, $dx_i \in K$ e $dx_i = \det(M)\det(M)x_i$ é integral sobre A. Para concluir observamos que $d = \det(M) \neq 0$ uma vez que $\{e_1, \ldots, e_n\}$ é uma base para $L|K$. ■

Teorema 1.3.1 *Sejam A um domínio Noetheriano integralmente fechado no seu corpo de frações K e $L|K$ uma extensão separável. Então o fecho integral de A em L é finitamente gerado como $A-$módulo, em particular, é um anel Noetheriano.*
Demonstração: *Seja B o fecho integral de A em L. Como A é Noetheriano, pela proposição 1.3.1 para mostrar que B é um $A-$módulo finitamente gerado, basta mostrar que B é um submódulo de um $A-$módulo finitamente gerado. Pela proposição anterior, B é um $A-$submódulo do $A-$módulo $A\frac{e_1}{d} \oplus \cdots \oplus A\frac{e_n}{d}$ que é livre de posto finito. E assim completaremos nossa demonstração.* ■

Relembrando que um elemento $m \in M$, onde M é um $A-$módulo é de *torção* se existe $a \in A \setminus \{0\}$, tal que $am = 0$. Um $A-$módulo M é um módulo de torção se todo elemento de M é de torção. Por exemplo, seja I um ideal não trivial de A. O $A-$módulo A/I é sempre de torção. Se zero é o único elemento de torção de M, então M é dito *livre de torção*. Quando A é um domínio de ideais principais, qualquer $A-$módulo finitamente gerado é isomorfo a soma direta de $A-$módulos de torção finitamente gerado e $A-$módulos livres finitamente gerados, esta afirmação se deve ao *teorema de estrutura de para módulos finitamente gerados sobre domínios principais.*

Corolário 1.3.2 *Seja A um domínio de ideais principais. Seja L uma extensão separável do corpo de frações de A. Então o fecho integral B de A em L é um $A-$módulo livre de posto finito.*
Demonstração: *O teorema 1.3.1 mostra que B é um $A-$módulo finitamente gerado. Desde que B é um domínio, o $A-$módulo B não contém um elemento de torção não trivial. De fato, seja $a \in A, a \neq 0$, e seja $b \in B$. Se $ab = 0$, então $b = 0$, pois B é domínio. Assim, B é livre de torção. Portanto, pelo resultado mencionado acima sobre a estrutura desses tipos de módulos, concluímos que B é um $A-$módulo livre.* ■

O posto de B sobre A pode ser calculado usando o seguinte lema:

Lema 1.3.1 *Seja K o corpo de frações do domínio A. Seja $L|K$ uma extensão finita de grau n. Seja B o fecho integral de A em L. Se B é um $A-$módulo livre finitamente gerado, então o* posto *de B sobre A é igual a n.*
Demonstração: *Seja $\{b_1, \ldots, b_s\}$ uma base para B sobre A. Dada uma relação $K-$linear entre $b_1, \ldots, b_s$, colocando em evidência o maior divisor comum dos*

denominadores temos uma relação $A-$linear, por isso, os elementos $b_1, \ldots, b_s$ são linearmente independentes sobre K e $s \leqslant n$. A proposição 1.1.3 mostra que todo elemento de L é da forma b/a para algum $b \in B$ e $a \in A$. Dado $\alpha \in L, \alpha = b/a$ para algum $b \in B$ e $a \in A$, como $b_1, \ldots, b_s$ é base para B sobre A, $b = a_1b_1 + \cdots + a_sb_s$ e assim $\alpha = \frac{1}{a}(a_1b_1 + \cdots + a_sb_s)$. Portanto $b_1, \ldots, b_s$ gera L como $K-$espaço vetorial e assim $s = n$. ■

Definição 1.3.2 *Sejam A um subanel do corpo L e B o fecho integral de A em L. Se B é um $A-$módulo livre de posto finito, as bases de B sobre A são chamadas de* bases integrais *sobre B.*

Nas condições do lema 1.3.1 uma base integral também é uma base para L sobre K.

Exemplo 1.3.2 *Os conjuntos $\{1, \sqrt{d}\}$ e $\{1, (1+\sqrt{d})/2\}$ são bases integrais sobre $\mathbb{Z}$ para o fecho integral de $\mathbb{Z}$ em $\mathbb{Q}(\sqrt{d})$, quando $d \equiv 2, 3(\text{mod}4)$ e $d \equiv 1(\text{mod}4)$ respectivamente.*

Exemplo 1.3.3 *Sejam $k = \overline{k}$ de característica 2 e $f \in k[x] \setminus k$ sem raízes duplas em k. A extensão $L := k(x)(\sqrt{f})$ não é separável sobre $K := k(x)$ uma vez que o polinômio minimal $y^2 - f = (y - \sqrt{f})^2$ de $\sqrt{f}$ tem uma raiz dupla. Assim, o teorema 1.3.1 sobre o fecho integral B de $k[x]$ em L não se aplica. Contudo mostraremos que B é um $k[x]-$módulo livre de posto 2.*

Primeiramente descreveremos B usando o mesmo método do exemplo 1.1.3. Seja $\alpha = m + n\sqrt{f} \in L, \alpha \notin k(x)$. O polinômio minimal de α sobre $k(x)$ é

$$y^2 + 2my + m^2 - n^2f = y^2 + (m^2 + n^2f).$$

Como $k[x]$ é domínio principal, logo um domínio fatorial (veja [1] pág 112)*, pelo lema 1.1.2 é integralmente fechado e pelo lema 1.1.3 $\alpha \in B$ se, e somente se, $m^2 + n^2f \in k[x]$. Sem perda de generalidade podemos assumir que $m = a/c$ e $n = b/c$ com $a, b, c \in k[x]$ e $\text{mdc}(a, b, c) = 1$. Assim, α é integral sobre $k[x]$ se, e somente se, $c^2|a^2 + b^2f$. Como queremos descrever B, consideremos $\alpha \in B$, logo existe $h \in k[x]$ tal que $hc^2 = a^2 + b^2f$. Então*

$$h'c^2 + 2cc'h = 2aa' + 2bb'f + b^2f' \Longleftrightarrow h'c^2 = b^2f',$$

então concluímos que quando $\alpha \in B$, $c^2|b^2f'$. Consequentemente, se f' não é divisível por nenhum quadrado em $k[x]$, então $c|b$. Portanto, $b/c \in k[x]$ e assim $b\sqrt{f}/c$ é integral sobre $k[x]$. Por α e $b\sqrt{f}/c$ serem integrais sobre $k[x]$ concluímos que $\alpha - b\sqrt{f}/c = a/c \in k(x)$ também é integral sobre $k[x]$, como $k[x]$ é integralmente fechado $a/c \in k[x]$ e por $\text{mdc}(a, b, c) = 1$, segue que $c \in k^*$ e $B = k[x][\sqrt{f}]$. Logo B é gerado por $\{1, \sqrt{f}\}$ sobre

$k[x]$, ou seja, B é uma $k[x]-$módulo livre de posto dois no caos em que f' não é divisível por nenhum quadrado em $k[x]$.

Agora analisaremos o caso em que f' é divisível por algum quadrado em k[x].

Afirmação 1: *Se $f' = g^2h$, isto é, $f'' \equiv 0$, então $f' = g^2$, para algum $g \in k[x]$.*

Seja $f(x) = \sum_{i=0}^{s} a_i x^i$, então $f'(x) = \sum_{i=0}^{s-1} a_{i+1}x^i$ e $f''(x) = 0$. Como $k = \overline{k}$, k é perfeito e $\mathrm{char}(k) = 2$, então k contém a raiz quadrada de qualquer um dos seus elementos, logo $f'(x) = (\sum_{2j+1\leqslant s} \sqrt{a_{2j+1}}x^j)^2$. Isso prova nossa afirmação.

Como $k = \overline{k}$ e f' é um quadrado, podemos escreve-lo $f'(x) := (\prod_{i=1}^{t}(x-b_i)^{r_i})^2$. Os elementos

$$\alpha_i := \frac{\sqrt{f(b_i)} - \sqrt{f(x)}}{(x-b_i)^{r_i}}, i = 1, \ldots, t,$$

são integrais sobre $k[x]$. De fato, cada α_i é raiz do polinômio

$$h(y) = y^2 - \frac{f(b_i) - f(x)}{(x-b_i)^{2r_i}} \in k[x][y].$$

Observamos que b_i é raiz de multiplicidade $2r_i$ do polinômio $g(x) = f(b_i) - f(x)$, pois $g(b_i) = 0$ e $g'(x) = -f'(x) = -\prod_{i=1}^{t}(x-b_i)^{2r_i}$. Logo $(f(b_i) - f(x))/(x-b_i)^{2r_i} \in k[x]$ e α_i é integral sobre $k[x]$.

Afirmação 2: *O conjunto $\{\alpha_0 = 1, \alpha_1, \ldots, \alpha_t\}$ gera o fecho integral B sobre $k[x]$.*

De fato, seja $\alpha = m + n\sqrt{f} \in L$, como antes $\alpha \in B$ se, e somente se, $c^2 | a^2 + b^2 f$ em $k[x]$, onde $a, b, c \in k[x], m = a/c$, $n = b/c$ e $\mathrm{mdc}(a, b, c) = 1$. Assim, existe $h \in k[x]$ tal que $hc^2 = a^2 + b^2 f$, ou:

$$h'c^2 = b^2 f'.$$

Logo $c^2 = b^2 f'/h'$ e assim $c = b\sqrt{f'}/\sqrt{h'}$. Voltando em $hc^2 = a^2 + b^2 f$, tem-se $a^2(b_i) + b^2(b_i)f(b_i) = 0$, como $\mathrm{mdc}(a, b, c) = 1$ segue $b^2(b_i) \neq 0$ e então $\sqrt{f(b_i)} = a(b_i)/b(b_i)$. Portanto

$$\alpha = \frac{a + b\sqrt{f}}{c} = \frac{b(a/b + \sqrt{f})}{c} = \frac{\sqrt{h'}b(\sqrt{f(b_i)} - \sqrt{f})}{b\sqrt{f'}} = \frac{\sqrt{h'}(\sqrt{f(b_i)} - \sqrt{f})}{\sqrt{f'}},$$

como desejado.

Se provarmos que o conjunto $\{\alpha_0 = 1, \alpha_1, \ldots, \alpha_t\}$ gera o fecho integral B sobre $k[x]$, saberemos que B é um $k[x]-$módulo finitamente gerado. Desde que $k[x]$ é um domínio de ideais principais, segue do corolário 1.3.2 que B é um $k[x]-$módulo livre finitamente gerado. Pelo lema 1.3.1 B pode ser gerado sobre $k[x]$ por dois elementos. Quais ? Se $\deg(f) = 1$ ou 2, então $f' \in k$ e $B = k[x][\sqrt{f}]$. Se $\deg(f) = 3$ ou 4, então $f'(x) = (x-b)^2$ e $\{1, (\sqrt{f(b)} - \sqrt{f(x)})/(x-b)\}$ é uma base para B sobre $k[x]$. Para encontrar uma base

inteira para B sobre $k[x]$ que contém dois elementos, vamos proceder como segue. Escreva,

$$f(x) = g(x)f'(x) + r(x), \quad \textit{com } \deg(r) < \deg(f') \textit{ ou } r \equiv 0.$$

Derivando ambos os lados,

$$f'(x) = g'(x)f'(x) + g(x)f''(x) + r(x).$$

Portanto, $f'(x)(1 - g'(x)) = r'(x)$ (pois $f''(x) = 0$), isso implica que $r'(x) = 0$ e então $g'(x) = 1$. Escreva $f' = h^2\varphi$, onde $h, \varphi \in k[x]$. Assim,

$$\sqrt{g\varphi} = \frac{\sqrt{f} - \sqrt{r}}{h} \in k(x)(\sqrt{f}).$$

Pela construção, $k(x)(\sqrt{g\varphi}) = k(x)(\sqrt{f})$.

Afirmação 3: $B = k[x][\sqrt{g\varphi}]$

O elemento $\sqrt{g\varphi} = (\sqrt{f} - \sqrt{r})/h$ é integral sobre $k[x]$, desde que h^2 divide $(\sqrt{f})^2 - (\sqrt{r})^2$, disso $k[x][\sqrt{g\varphi}] \subseteq B$. Como $(g\varphi)' = g'\varphi = \varphi$, nós concluímos que $(g\varphi)'$ é livre de quadrados em $k[x]$. Portanto $k[x][\sqrt{g\varphi}]$ é integralmente fechado e assim é igual a B.

Mostraremos que B é um $k[x]-$módulo finitamente gerado. Seja $h \in k[x]$ o polinômio de grau mínimo tal que $k(x)(\sqrt{h}) = k(x)(\sqrt{f})$. Afirmamos que $\{1, \sqrt{h}\}$ é base para B sobre $k[x]$. Por construção $\sqrt{h}$ é integral sobre $k[x]$ e assim, pertence a B. Seja $\alpha := a/c + b\sqrt{h}/c \in B$, com $a, b, c \in k[x]$ e $\mathrm{mdc}(a, b, c) = 1$. Seja $\deg(c) > 0$. Subtraindo (se necessário) um elemento de $k[x] + k[x]\sqrt{f}$, podemos assumir que $\deg(c) > \deg(b), \deg(a)$. Como α é integral, existe um polinômio ℓ tal que $c^2\ell = a^2 + b^2h$, esta equação mostra que $k(x)(\sqrt{\ell}) = k(x)(\sqrt{h})$ e assim $\deg(\ell) = \deg(h)$. Por $\deg(c) > \deg(b)$, $\deg(c^2\ell) = \deg(a^2)$, mas isso não é possível uma vez que $\deg(c) > \deg(a)$. Portanto $\deg(c) = 0$ e $\{1, \sqrt{h}\}$ é uma base, como desejado.

Se k é um corpo de característica $p > 0$, estudaremos em 8.1 as propriedades do fecho integral B do anel $k[x]$ numa extensão finita e inseparável de $k(x)$. E o teorema 8.1.1 nos garantirá que o anel B é sempre um $k[x]-$módulo finitamente gerado.

1.4 Localização

Definição 1.4.1 *Seja A um anel comutativo com unidade. Um subconjunto S de A é* multiplicativo *se*

1. *$0 \notin S$ e $1 \in S$,*
2. *se $a, b \in S$, então $ab \in S$.*

Considere no conjunto $A \times S$ a seguinte relação:

$$(a, s) \approx (b, t) \Leftrightarrow \exists \lambda \in S : \lambda(at - bs) = 0.$$

Observe que quando A é domínio, a equação $\lambda(at - bs) = 0$ implica que $at - bs = 0$. Claramente a relação $\approx$ em $A \times S$ é uma relação de equivalência.

Denote por $\frac{a}{s}$ a classe de equivalência de $(a, s) \in A \times S$. Seja $S^{-1}A = A \times S/\approx$. O conjunto $S^{-1}A$ tem estrutura de anel com as seguintes operações:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{ts}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{ts}.$$

O anel $S^{-1}A$ é chamado do *anel de frações do A com respeito a S*. A aplicação

$$\begin{array}{rccc} j_S : & A & \longrightarrow & S^{-1}A \\ & a & \longmapsto & \frac{a}{1} \end{array}$$

é um homomorfismo de anéis. Quando não causar confusão denotaremos j_S simplesmente por j. A aplicação j e o anel $S^{-1}A$ satisfazem as seguintes propriedades:

1. Seja $s \in S$. O elemento $j(s) \in S^{-1}A$ é inversível e seu inverso é $\frac{1}{s}$.
2. Se A é um domínio, então j é injetiva. De fato, $j(a) = \frac{a}{1} = \frac{0}{1}$ implica que existe $\lambda \in S$ tal que $\lambda a = 0$. Como A é domínio e $\lambda \neq 0$, $a = 0$.
3. Quando A é um domínio o anel $S^{-1}A$ também é. De fato, se $\frac{a}{s} \cdot \frac{b}{t} = 0$ em $S^{-1}A$, então existe $\lambda \in S$ tal que $\lambda(ab - 0) = 0$. Por A ser domínio e $\lambda \neq 0$, $a = 0$ ou $b = 0$.
4. Quando A é domínio, o corpo de frações K de A é o anel $S^{-1}A$ com $S = A \setminus \{0\}$.

Propriedade Universal de Anéis de Frações. Sejam A um anel comutativo com unidade e $S \subseteq A$ multiplicativo. Seja $g : A \to B$ um homomorfismo de anéis tal que $g(s)$ é inversível em B para todo $s \in S$. Então existe um único homomorfismo de anéis $g' : S^{-1}A \to B$ tal que $g = g' \circ j$. Onde,

$$\begin{array}{rccc} j : & A & \longrightarrow & S^{-1}A \\ & a & \longmapsto & a/1. \end{array}$$

Proposição 1.4.1 *Se A é um domínio integralmente fechado e $S \subseteq A$ multiplicativo, então $S^{-1}A$ é um domínio integralmente fechado.*

Demonstração: *Seja K o corpo de frações de A (e de $S^{-1}A$). Seja $\alpha \in K^*$ e escreva $\alpha = \frac{a}{b}$, $a, b \in A$. Suponha que α seja integral sobre $S^{-1}A$ e considere $f(y) = y^n + \sum_{i=0}^{n-1} \frac{a_i}{s_i} y^i \in (S^{-1}A)[y]$ mônico tal que $f(\alpha) = 0$. Tome $s := \prod_{i=0}^{n-1} s_i$, assim $s^n f(\frac{a}{b}) = 0$ e*

portanto $\frac{sa}{b} \in K$ *é integral sobre* A*, pois*

$$(\frac{sa}{b})^n + \frac{a_{n-1}s}{s_{n-1}}(\frac{sa}{b})^{n-1} + \cdots + \frac{a_1 s^{n-1}}{s_1}(\frac{sa}{b}) + \frac{a_0 s^n}{s_0} = 0.$$

Como A *é integralmente fechado,* $\frac{sa}{b} \in A$*, logo* $\alpha = \frac{a}{b} \in S^{-1}A$*, como desejado.* ■

Corolário 1.4.1 *Seja* B *o fecho integral de* A *no corpo* L*. Seja* $S \subset A$ *multiplicativo. Então o anel* $S^{-1}B$ *é o fecho integral de* $S^{-1}A$ *em* L*.*
Demonstração: *Pela proposição 1.4.1* $S^{-1}B$ *é integralmente fechado em* L*. Portanto para provar este corolário devemos mostrar que todo elemento de* $S^{-1}B$ *é integral sobre* $S^{-1}A$*. Sejam* $\frac{b}{s} \in S^{-1}B$ *e* $f(y) = y^n + \sum_{i=0}^{n-1} a_i y^i \in A[y]$ *tal que* $f(b) = 0$*. Tome,*

$$g(y) := y^n + \sum_{i=0}^{n-1} \frac{a_i}{s^{n-i}} y^i \in (S^{-1}A)[y].$$

Uma vez que $g(\frac{b}{s}) = 0$*, segue que* $\frac{b}{s}$ *é integral sobre* $S^{-1}A$*.* ■

A propriedade de um domínio ser integramente fechado é local. De fato:

Corolário 1.4.2 *Seja* A *um domínio. As seguintes afirmações são equivalentes:*

(1) A *é integralmente fechado.*

(2) A_P *é integralmente fechado para todo* $P \in \mathrm{Spec}(A)$.

(3) A_P *é integralmente fechado para todo* $P \in \mathrm{Max}(A)$.

A prova pode ser vista [11].

1.5 Anéis de Dimensão Um

Definição 1.5.1 *Seja* A *um anel. Uma cadeia de ideais primos de comprimento* n *é um conjunto de* $n+1$ *ideais primos distintos* $P_0, \ldots, P_n$ *de* A *tais que* $P_n \subseteq \cdots \subseteq P_1 \subseteq P_0$*.* A altura *do ideal primo* P*,* $\ell(P)$*, é o supremo dos comprimentos das cadeias de ideais primos onde* $P_0 = P$*.* A dimensão *de* Krull *de* A *é definida por*

$$\dim A := \sup\{\ell(P) | P \text{ é ideal primo de } A\}.$$

Iremos frequentemente referir a dimensão de Krull de A simplesmente por dimensão de A.

Exemplo 1.5.1 *1.* $\dim\mathbb{Z} = 1$.

2. *Os corpos possuem dimensão zero, uma vez que em um corpo o ideal zero é o único ideal primo.*
3. *Seja k um corpo. O anel $R = k[x]/\langle x^2\rangle$ claramente não é domínio e sua dimensão é zero pois $\langle \overline{x}\rangle$ é o único ideal primo de R.*
4. *Sejam k um corpo e $R = k[x_1, \ldots, x_n]$ o anel dos polinômio s em n variáveis. Então* $\dim R = n$. *Em geral, se A for um anel Noetheriano, então* $\dim A[x_1, \ldots, x_n] = \dim A + n$. *Veja [12], corolário 10.12 pág. 240.*

Lema 1.5.1 *Seja R um domínio. Sejam $P_1 = \langle p_1\rangle$ e $P_2 = \langle p_2\rangle$ dois ideais primos não triviais e distintos de R. Então $P_1 \nsubseteq P_2$. Em particular, um domínio de ideais principais possui dimensão um.*
Demonstração: *Suponha por absurdo que $P_1 \subseteq P_2$. Então existe $a \in R$ tal que $p_1 = ap_2$. Em particular $ap_2 \in P_1$, por P_1 ser primo $p_2 \in P_1$ ou $a \in P_1$. No primeiro caso concluímos que $P_1 = P_2$ o que é impossível pois são distintos. Escreva $a = bp_1$, então $p_1(1 - bp_2) = 0$. Como R é um domínio, $p_1 = 0$ então $P_1 = \langle 0\rangle$ ou $1 - bp_2 = 0$ o que implica que $P_2 = R$ e em todos os casos temos um absurdo, logo $P_1 \nsubseteq P_2$.* ■

Lema 1.5.2 *Sejam R um domínio fatorial e $P \neq \langle 0\rangle$ um ideal primo. Então $\ell(P) = 1$ se, e somente se, P é principal.*
Demonstração: *Seja $0 \neq x \in P$, por R ser fatorial $x = up_1^{\alpha_1} \cdots p_s^{\alpha_s}$, com $\langle p_1\rangle, \ldots, \langle p_s\rangle$ ideais primos de R e u inversível. Como P é primo e $x \in P$, então $p_i \in P$ para algum $i = 1, \ldots, s$. Portanto, $\langle 0\rangle \subseteq \langle p_i\rangle \subseteq P$. Se P tem altura um, então $P = \langle p_i\rangle$. Reciprocamente, suponha P um ideal principal e que P contenha um ideal não trivial Q. Pela discussão acima existe um elemento $q \in R$ tal que $\langle q\rangle \subseteq Q \subseteq P$, pelo lema 1.5.1 concluímos que $\langle q\rangle = P$, portanto $\ell(P) = 1$.* ■

Proposição 1.5.1 *Um domínio Noetheriano fatorial tem dimensão um se, e somente se, é um domínio de ideais principais.*
Demonstração: *Seja R um domínio Noetheriano fatorial de dimensão um. Seja $P \neq \langle 0\rangle$ um ideal primo. Pela hipótese $\ell(P) = 1$, logo pelo lema 1.5.2 é principal. Agora seja $I \trianglelefteq R$, por R ser Noetheriano, I é finitamente gerado. Escreva $I = \langle a_1, \ldots, a_n\rangle$. Vamos mostrar que I é principal por indução sobre n. Se $n = 1$, então $I = \langle a_1\rangle$. Suponha que o resultado é válido para $n > 1$. Por hipótese de indução o ideal $J := \langle a_1, \ldots, a_{n-1}\rangle$ é principal, isto é, existe $a \in R$ tal que $J = \langle a\rangle$. Então $I = \langle a, a_n\rangle$. Para cada ideal primo P de R, seja p o gerador de P, assim considere $\mathcal{P}$ o conjunto de todos os geradores dos ideais primos. Usando o fato de R ser fatorial podemos escrever*

$$a = u\prod_{p\in\mathcal{P}} p^{m_p} \quad e \quad a_n = u_n\prod_{p\in\mathcal{P}} p^{n_p},$$

com u, u_n inversíveis em R e $m_p, n_p \in \mathbb{N}, \forall p \in \mathcal{P}$. Observe que m_p e n_p são zeros a menos de uma quantidade finita. Seja

$$c := \mathrm{mdc}(a, a_n) = \prod_{p \in \mathcal{P}} p^{\min(m_p, n_p)}.$$

Existem $d, d_n \in R, \mathrm{mdc}(d, d_n) = 1$ tais que $a = cd$ e $a_n = cd_n$. Afirmamos que $D := \langle d, d_n \rangle = R$. De fato, se $D \neq R$, então D está contido em algum ideal maximal $\mathfrak{P}$ de R. Como todo ideal maximal é um ideal primo, logo todo ideal maximal é também principal. Assim escreva $\mathfrak{P} = \langle p \rangle$ para algum elemento primo $p \in \mathcal{P}$. Assim $D \subseteq \langle p \rangle$, logo $p|d$ e $p|d_n$ uma contradição pelo fato de $\mathrm{mdc}(d, d_n) = 1$. Logo $D = R$ e podemos encontrar $\alpha, \beta \in R$ tal que

$$\alpha d + \beta d_n = 1.$$

Assim,

$$c = c \cdot 1 = c(\alpha d + \beta d_n) = \alpha cd + \beta c d_n \in I.$$

Como $I = \langle a, a_n \rangle \subseteq \langle c \rangle$, concluímos que $I = \langle c \rangle$ e portanto todo ideal de R é principal.

Para a recíproca, seja R um domínio de ideais principais, logo é fatorial, veja [1] *página* 112*) e claramente Noetheriano. Ainda, todo ideal primo é maximal, logo* $\dim R = 1$. ■

A proposição seguinte mostra que o fecho integral de um domínio de ideais principais também tem dimensão um.

Proposição 1.5.2 *Sejam $A \subseteq B$ domínios,* $\dim A = 1$ *e B é integral sobre A. Então* $\dim B = 1$.

Demonstração: *Basta mostrar que todo ideal primo não trivial de B possui comprimento um e para isso basta mostrar que é maximal. Sejam $\mathfrak{P}$ um ideal primo não trivial de B e $P = \mathfrak{P} \cap A$. Por $\mathfrak{P} \neq B$, $P \neq A$ é um ideal primo. Mostraremos que $P \neq \langle 0 \rangle$. Seja $\alpha \in \mathfrak{P}, \alpha \neq 0$, como α é integral sobre A existe um polinômio mônico $f \in A[y]$ de grau mínimo tal que*

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Pela minimalidade de n, $a_0 \neq 0$. De $a_0 = -\alpha^n - a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha \in \mathfrak{P}$, concluímos $a_0 \in A \cap \mathfrak{P} = P$, logo $P \supseteq \langle a_0 \rangle \neq \langle 0 \rangle$. Então $\ell(P) \geqslant 1$ e pelo fato que $\dim A = 1$*, concluímos que $\ell(P) = 1$, portanto P é maximal.*

Agora mostraremos que $\mathfrak{P}$ é maximal ou equivalentemente que $B/\mathfrak{P}$ é corpo o que completa nossa demonstração. O domínio $B/\mathfrak{P}$ contém o corpo A/P. Como todo elemento de B é integral sobre A, então todo elemento de $B/\mathfrak{P}$ é integral sobre A/P.

Seja $\gamma \in B/\mathfrak{P}$ um elemento não nulo, devemos mostrar que γ é inversível em $B/\mathfrak{P}$. Considere,

$$\gamma^n + c_{n-1}\gamma^{n-1} + \cdots + c_1\gamma + c_0 = 0$$

a relação integral de γ sobre A/P de grau mínimo. Pelo mesmo argumento feito para mostrar que $a_0 \neq 0$, $c_0 \neq 0$. Portanto, c_0 é inversível em A/P e podemos escrever

$$\gamma(-c_0^{-1}\gamma^{n-1} - c_0^{-1}c_{n-1}\gamma^{n-2} - \cdots - c_0^{-1}c_1) = 1.$$

Portanto γ é inversível e $B/\mathfrak{P}$ é corpo, como desejado. ■

Observação 1.5.1 *Sejam A e B como na proposição 1.5.2. Segue da proposição 1.5.2 e de sua demonstração que se $\mathfrak{P}$ é um ideal maximal de B, então $\mathfrak{P} \cap A = P$ é maximal em A.*

A proposição 1.5.2 vale para dimensão maior, isto é, se A e B são Noetherianos e B é integral sobre A, então $\dim(B) = \dim(A)$.

Corolário 1.5.1 *Sejam K o corpo de frações do domínio A e $L|K$ uma extensão finita. Se* $\dim A = 1$*, então B o fecho integral de A em L também tem dimensão um.*

1.6 Domínios de Dedekind

Definição 1.6.1 *Um domínio é chamado de* domínio de Dedekind *se é Noetheriano, tem dimensão um e é integralmente fechado.*

Todo domínio de ideais principais é um domínio de Dedekind, este fato segue diretamente dos lemas 1.1.2 e 1.5.1. Reunindo as afirmações do teorema 1.3.1 e da proposição 1.5.2, obtemos:

Teorema 1.6.1 *Sejam A um domínio de Dedekind, K seu corpo de frações e $L|K$ uma extensão finita e separável. Então o fecho integral B de A em L é um domínio de Dedekind.*

O seguinte e importante teorema sobre domínio de Dedekind é provado no capítulo 2.

Teorema 1.6.2 *Seja R um domínio Noetheriano de dimensão um. O anel R é um domínio de Dedekind se, e somente se, R tem a propriedade de fatoração única de ideais.*

O teorema 1.2.1 segue imediatamente dos teoremas 1.6.1 e 1.6.2.

1.7 Caso $A = \overline{k}[x]$

O objetivo desta seção é determinar o fecho integral de $\overline{k}[x]$ em algumas extensões de $\overline{k}(x)$. Mais precisamente, estamos interessados nas extensões de $\overline{k}(x)$ dadas da seguinte forma: sejam $f \in \overline{k}[x,y]$ irredutível e $Z_f(\overline{k})$ a curva afim definida por f. Pela irredutibilidade de f, $\overline{C}_f := \overline{k}[x,y]/\langle f\rangle$ é um domínio. Seja $\overline{k}(Z_f)$ o corpo de frações de $\overline{C}_f$. Observe que existe o seguinte diagrama de corpos e anéis

$$\begin{array}{ccc} \overline{k}(Z_f) & & \\ | & \diagdown & \\ \overline{k}(x) & & \overline{k}[x,y]/\langle f\rangle \\ & \diagdown & | \\ & & \overline{k}[x] \end{array}$$

Estudaremos o fecho integral de $\overline{k}[x]$ em $\overline{k}(Z_f)$.

Proposição 1.7.1 *Seja $f \in k[x,y]$ irredutível. Então* $\dim \frac{k[x,y]}{\langle f\rangle} = 1$.
Demonstração: *Pelo fato de $k[x,y]/\langle f\rangle$ ser um domínio e pelo lema 0.2.2,* $\dim k[x,y]/\langle f\rangle > 0$. *Seja $\varphi : k[x,y] \to k[x,y]/\langle f\rangle$ a aplicação quociente. Considere uma cadeia de ideais primos de $k[x,y]/\langle f\rangle$:*

$$\langle 0\rangle \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_n.$$

Então,

$$\langle 0\rangle \subsetneqq \langle f\rangle \subsetneqq \varphi^{-1}(P_1) \subsetneqq \cdots \subsetneqq \varphi^{-1}(P_n)$$

é uma cadeia de ideais primos em $k[x,y]$. Pelo exemplo 1.5.1, $n \leqslant 1$. Logo $\dim k[x,y]/\langle f\rangle = 1$ ■

Corolário 1.7.1 *Seja $f \in \overline{k}[x,y]$ irredutível. Então todo ideal primo de $\overline{C}_f$ é maximal e gerado pela imagem de $\langle x-a, y-b\rangle \trianglelefteq \overline{k}[x,y]$ em $\overline{C}_f$, para algum $(a,b) \in Z_f(\overline{k})$.*
Demonstração: *Segue diretamente do corolário 0.2.2 e da proposição 1.7.1.*

Teorema 1.7.1 *Seja $f \in \overline{k}[x,y]$ irredutível. Então $\overline{C}_f$ é integralmente fechado em $\overline{k}(Z_f)$ se, e somente se, a curva $Z_f(\overline{k})$ é não singular.*
Demonstração: *Pelo corolário 1.4.2, $\overline{C}_f$ é integralmente fechado se, e somente se, $(\overline{C}_f)_M$ é integralmente fechado para todo $M \in \mathrm{Max}(\overline{C}_f)$. O corolário 1.7.1 implica que um ideal maximal M de $\overline{C}_f$ é gerado pelas imagens de $x-a$ e $y-b$ para algum $(a,b) \in Z_f(\overline{k})$. Por 0.2.3, $(\overline{C}_f)_M$ é um domínio local de ideais principais se, e só se, o*

ponto (a, b) é não singular em $Z_f(\overline{k})$. Claro que se $(\overline{C}_f)_M$ é principal (logo fatorial), então é integralmente fechado (veja 1.1.1). Para a recíproca, veja 2.1.2. ■

Observação 1.7.1 *No caso em que $Z_f(\overline{k})$ é uma curva não singular, a proposição 1.7.1 e o teorema 1.7.1 garantem que $\overline{C}_f$ é um domínio de Dedekind.*

Corolário 1.7.2 *Seja $f \in \overline{k}[x, y]$ irredutível e mônico em y. Então $\overline{C}_f$ é o fecho integral de $\overline{k}[x]$ em $\overline{k}(Z_f)$ se, e somente se, $Z_f(\overline{k})$ é uma curva não singular.*
Demonstração: *Por 1.1.1 $\overline{C}_f$ é integral sobre sobre $\overline{k}[x]$. Portanto, $\overline{C}_f$ é o fecho integral de $\overline{k}[x]$ em $\overline{k}(Z_f)$ se, e somente se, $\overline{C}_f$ é integralmente fechado em $\overline{k}(Z_f)$. Assim, este corolário segue diretamente do teorema 1.7.1.* ■

Capítulo

2

Fatoração de Ideais

Os exemplos mais simples de anéis estudados num primeiro curso de álgebra são fatoriais, tais como $\mathbb{Z}, \mathbb{Z}[i]$ e $k[x]$. Foi somente em meados do século 19 que os matemáticos observaram que a fatoração única de elementos nem sempre é válida para anéis da forma $\mathbb{Z}[\alpha]$, onde α é um integral algébrico. Dedekind, por volta de 1871, expandiu o importante trabalho de Kummer sobre propriedades de fatoração dos anéis $\mathbb{Z}[e^{2\pi i/n}]$ e definiu a propriedade de fatoração única de ideais como uma generalização da fatoração única de elementos, como visto na seção 1.2.

Neste capítulo, primeiramente provaremos o teorema 1.6.2 que afirma que um domínio Noetheriano de dimensão um é integralmente fechado se, e somente se, tem a propriedade de fatoração única de ideais. Depois disso, tentaremos descrever explicitamente, nos anéis da forma $B = \mathbb{Z}[\alpha]$ a fatoração do ideal I gerado por um primo $p \in \mathbb{Z}$. Mais geralmente, dados um domínio de Dedekind A, uma extensão finita e separável $L|K$ de seu corpo de frações e B o fecho integral de A em L, estudaremos a fatoração em B do ideal I gerado por elementos do ideal primo P de A. O caso de extensões de Galois será tratado na seção 2.6.

Exemplo 2.0.1 *Sejam $\overline{k}$ um corpo algebricamente fechado e $f \in \overline{k}[x,y]$ irredutível. Considere $\overline{C}_f := \overline{k}[x,y]/\langle f\rangle$ e tome $a \in \overline{k}$. Seja I o ideal de $\overline{C}_f$ gerado por $x-a$. Estudaremos neste exemplo o problema de fatoração do ideal I como produto de ideais primos de $\overline{C}_f$.*

Observe inicialmente que se $x-a$ é inversível em $\overline{C}_f$, então $I = \overline{C}_f$ e nenhum ideal primo ocorre na decomposição de I. Por exemplo, $x-a$ é inversível em $\overline{k}[x,y]/\langle(x-a)y-1\rangle$ e seu inverso é y. O elemento $x-a$ é inversível em $\overline{C}_f$ se, e somente se, $f(a,y) = c \in \overline{k} \setminus 0$.

Suponha $x-a$ não inversível em $\overline{C}_f$. O primeiro passo é descrever os ideais primos de $\overline{C}_f$ que contenham I. Pois, se $I = M_1^{e_1}\cdots M_s^{e_s}$, então $I \subseteq M_i, i = 1,\ldots,s$. Seja $f(a,y) = c\prod_{i=1}^{s}(y-b_i)^{e_i} \in \overline{k}[y]$, com $b_i \neq b_j$ se $i \neq j$, então

$$f(x,y) = (x-a)g(x,y) + c\prod_{i=1}^{s}(y-b_i)^{e_i},$$

para algum $g \in \overline{k}[x,y]$. Considere o anel $\overline{C}_f/\langle x-a\rangle \cong \overline{k}[y]/\langle f(a,y)\rangle$. Como os únicos ideais maximais de $\overline{k}[y]$ que contém $f(a,y)$ são os ideais gerados por $\langle y-b_i\rangle, i = 1,\ldots,s$, segue que os únicos ideais maximais de $\overline{C}_f$ que contém $\langle x-a\rangle$ são os ideais:

$$M_i := \langle x-a, y-b_i\rangle, i = 1,\ldots,s.$$

Mostremos agora que

$$\prod_{i=1}^{s} M_i^{e_i} \subseteq IC_f.$$

Note primeiramente que o ideal $M_i^{e_i}$ é gerado pelos elementos,

$$(x-a)^{e_i}, (x-a)^{e_i-1}(y-b_i), \ldots, (y-b_i)^{e_i}.$$

Em particular, $M_i^{e_i} \subseteq \langle x-a, (y-b_i)^{e_i}\rangle$. Portanto,

$$\prod_{i=1}^{s} M_i^{e_i} \subseteq \langle x-a, \prod_{i=1}^{s}(y-b_i)^{e_i}\rangle.$$

Assim, em $\overline{C}_f$

$$0 = f(x,y) = (x-a)g(x,y) + c\prod_{i=1}^{s}(y-b_i)^{e_i},$$

ou seja, $\prod_{i=1}^{s}(y-b_i)^{e_i} \in I\overline{C}_f$ e portanto $\prod_{i=1}^{s} M_i^{e_i} \subseteq I\overline{C}_f$.

Seja $J := \prod_{i=1}^{s} M_i^{e_i}$. A igualdade $J = I\overline{C}_f$ não é verdadeira sem hipóteses adicionais. De fato, mostraremos que uma condição suficiente é que os pontos $(a,b_i), i = 1,\ldots,s$ sejam não singulares. Pelo lema 0.1.5 é suficiente mostrar que $J_{M_i} = (I\overline{C}_f)_{M_i}$, para todo $i = 1,\ldots,s$. Para encontrar qual é a localização J_{M_i}, usaremos os seguintes fatos:

Fato (1) *Seja A um anel e $S \subseteq A$ um conjunto multiplicativo. Sejam I, J dois ideais de A. Então $S^{-1}(IJ) = S^{-1}(I)S^{-1}(J)$ no anel $S^{-1}(A)$.*

Fato (2) *Se A é um anel de dimensão um e J um ideal de A que pode ser fatorado como produto de ideais maximais, digamos $J = P_1^{\alpha_1}\cdots P_s^{\alpha_s}$. Seja M um ideal maximal de A, então $J_M = (MA_M)^{\alpha_i}$ se $M = P_i$ para algum $i \in \{1,\ldots,s\}$, e $J_M = A_M$ se $M \neq P_i$ para*

todo $i = 1, \ldots, s$.

Para concluir o exemplo, primeiro suponha que $e_i = 1$, *para todo* $i = 1, \ldots, s$. *Uma vez que* $J \subseteq I\overline{C}_f \subseteq M_i$,

$$J_{M_i} = M_i(\overline{C}_f)_{M_i} \subseteq I_{M_i} \subseteq M_i(\overline{C}_f)_{M_i},$$

logo $J_{M_i} = I_{M_i}$, *para todo* $i = 1, \ldots, s$.

Considere agora as derivadas parciais de $f(x, y) \in \overline{k}[x, y]$:

$$f_x = g(x, y) + (x - a)g_x, f_y = (x - a)g_y + \sum_{i=1}^{s} \left(e_i(y - b_i)^{e_i - 1} \prod_{j \neq i} (y - b_j)^{e_j} \right).$$

Como cada ponto (a, b_i) *é um ponto não singular, então* $g(a, b_i) \neq 0$ *ou* $e_i = 1$, *para* $i = 1, \ldots, s$. *Portanto, quando* $e_i > 1$, $g(x, y) \notin M_i$, *pois* $g(a, b_i) \neq 0$. *Assim,* $g(x, y)$ *é inversível em* $(C_f)_{M_i}$. *Como,*

$$0 = (x - a)g(x, y) + c \prod (y - b_j)^{e_j} \quad em\ \overline{C}_f,$$

$$\Rightarrow x - a \in (y - b_i)^{e_i}(\overline{C}_f)_{M_i} \subseteq M_i^{e_i}(C_f)_{M_i} = J_{M_i}.$$

Logo, $J_{M_i} = (I\overline{C}_f)_{M_i}$ *quando* $e_i > 1$ *também. Portanto, pelo lema 0.1.5, concluímos a prova de que* $I\overline{C}_f = J$.

2.1 Fatoração Única de Ideais

O objetivo desta seção é provar o teorema 1.6.2. No exemplo 1.2.2 discutimos o fato do anel $\mathbb{Z}[\sqrt{5}]$ não ter a propriedade de fatoração única de ideais. Para isso, mostramos que o ideal $I := \langle 2 \rangle$ em $\mathbb{Z}[\sqrt{5}]$ não pode ser fatorado como produto de ideais primos de $\mathbb{Z}[\sqrt{5}]$ pois $P^2 \subsetneq I \subsetneq P$, onde $P := \langle 2, 1 + \sqrt{5} \rangle$ é um ideal primo de $\mathbb{Z}[\sqrt{5}]$. Inicialmente procuraremos condições sobre o anel pelas quais possua a propriedade de fatoração única de ideais. Antes disso, vale observar alguns fatos triviais neste sentido. Lembramos que todo ideal não trivial está contido num ideal maximal e isto pode ser visto como um produto de ideais primos. Por outro lado, o ideal zero num domínio é primo e está contido em qualquer ideal, ou seja, qualquer ideal num domínio contém um ideal primo. Visto estas observações, procuraremos condições pelas quais um ideal contenha um produto de ideais primos não triviais. A seguir mostraremos que uma condição suficiente é que o anel seja Noetheriano e usaremos este fato para provar o teorema 1.6.2.

Proposição 2.1.1 *Sejam* A *um anel Noetheriano e* $I \trianglelefteq A$ *não trivial. Então existem ideais primos* $P_1, \ldots, P_s$ *e* $a_1, \ldots, a_s \in \mathbb{N}$ *tais que,* $P_1^{a_1} \cdots P_s^{a_s} \subseteq I \subseteq P_1 \cap \cdots \cap P_s$.
Demonstração: *Seja* Σ *o conjunto dos ideais de* A *que não satisfazem a afirmação da*

proposição. Suponha $\Sigma \neq \emptyset$. Usando o lema de Zorn e o fato de A ser Noetheriano, Σ possui elemento maximal, digamos I. O ideal I não pode ser primo pois Σ não contém nenhum ideal primo por sua definição. Portanto, existem $x, y \in A$ tais que $xy \in I$ e $x \notin I$, $y \notin I$. Considere os ideais $I_x := \langle I, x\rangle$ e $I_y := \langle I, y\rangle$. Por construção,

$$\langle I^2, I_x, I_y, xy\rangle = I_x \cdot I_y \subseteq I \subseteq I_x \cap I_y.$$

A inclusão $I_x \cdot I_y \subseteq I$ mostra que ambos I_x e I_y são não triviais, pois $I \subsetneqq I_x$ e $I \subsetneqq I_y$. Por I ser maximal em Σ os ideais I_x e I_y não pertencem a Σ. Portanto, podemos escrever

$$P_1^{a_1} \cdots P_s^{a_s} \subseteq I \subseteq P_1 \cap \cdots \cap P_s \quad e \quad Q_1^{b_1} \cdots Q_r^{b_r} \subseteq I \subseteq Q_1 \cap \cdots \cap Q_r,$$

para alguns $P_1, \ldots, P_s, Q_1, \ldots, Q_r$ ideais primos e $a_1, \ldots, a_s, b_1, \ldots, b_r$ inteiros positivos. Então,

$$P_1^{a_1} \cdots P_s^{a_s} \cdot Q_1^{b_1} \cdots Q_r^{b_r} \subseteq I_x \cdot I_y \subseteq I \subseteq I_x \cap I_y \subseteq P_1 \cap \cdots \cap P_s \cap Q_1 \cap \cdots \cap Q_r$$

o qual mostra que $I \notin \Sigma$, absurdo. Logo $\Sigma = \emptyset$. ■

Corolário 2.1.1 *Sejam A um domínio Noetheriano de dimensão um e I um ideal não trivial. Então o conjunto dos ideais maximais que contém I é finito. Se $\{M_1, \ldots, M_s\}$ é este conjunto, então existem inteiros positivos $a_1, \ldots, a_s$ tais que $M_1^{a_1} \cdots M_s^{a_s} \subseteq I \subseteq M_1 \cdots M_s$.*

Demonstração: *Com $\dim A = 1$, todo ideal primo é maximal. A proposição 2.1.1 garante a existência dos ideais maximais $M_1, \ldots, M_s$ e inteiros $a_1, \ldots, a_s$ tais que $M_1^{a_1} \cdots M_s^{a_s} \subseteq I \subseteq M_1 \cap \cdots M_s$. Seja M um ideal maximal de A que contém I, aplicando o lema 0.1.7 à inclusão $M \supseteq M_1^{a_1} \cdots M_s^{a_s}$ concluímos que existe um inteiro $i \in \{1, \ldots, s\}$ tal que $M \supseteq M_i$. Uma vez que M_i é maximal, $M = M_i$. Portanto, o conjunto $\{M_1, \ldots, M_s\}$ é o conjunto de ideais maximais de A que contém I.* ■

Observação 2.1.1 *A prova do corolário 2.1.1 implica o seguinte e importante fato: Se um ideal I de A pode ser fatorado como produto $M_1^{a_1} \cdots M_s^{a_s}$ de ideias maximais ($a_i > 0, \forall i$), então $\{M_1, \ldots, M_s\}$ é o conjunto do ideais maximais de A que contém I. Em particular, todo ideal maximal que contém I aparece na fatoração de I.*

Proposição 2.1.2 *Seja A um domínio Noetheriano de dimensão um. As seguintes afirmações são equivalentes:*

(1) *A tem a propriedade da fatoração única de ideais.*

(2) *A_M tem a propriedade da fatoração única de ideais para todo $M \in \mathrm{Max}(A)$.*

Demonstração: (1) $\Rightarrow$ (2) *Seja* $M \in \mathrm{Max}(A)$ *e considere a aplicação natural* $\varphi : A \longrightarrow A_M$. *Seja* I *um ideal de* A_M, *como* A *tem a propriedade da fatoração única de ideais, podemos fatorar* $\varphi^{-1}(I)$ *como produto de ideais maximais:*

$$\varphi^{-1}(I) := P_1^{a_1} \cdots P_s^{a_s}.$$

Uma vez que $\varphi^{-1}(I) \subseteq M$, *pelo lema 0.1.7,* $P_i \subseteq M$, *para algum* $i = 1, \ldots, s$. *Por* P_i *ser maximal, concluímos* $M = P_i$, *assim*

$$I = (\varphi^{-1}(I))_M = (MA_M)^{a_i},$$

o que mostra que I *pode ser fatorado como produto de ideais maximais em* A_M. *Para mostrar que a fatoração é única tome* $a \geqslant 0$ *um inteiro e* $M \in \mathrm{Max}(A)$, *os ideais* M^{a+1} *e* M^a *são distintos em* A *pois o mesmo tem a propriedade da fatoração única de ideais. Como* $M^{a+1} \subseteq M^a$ *e* M *é o único ideal maximal de* A *que contém* M^{a+1}, *pelo lema 0.1.5,* $(MA_M)^{a+1} \neq (MA_M)^a$. *Assim, o anel* A_M *tem a propriedade de fatoração única de ideais.*

(2) $\Rightarrow$ (1) *Sejam* I *um ideal de* A *não trivial e* $\{M_1, \ldots, M_s\}$ *o conjunto dos ideais maximais de* A *quem contém* I *(que este conjunto é finito já foi mostrado no corolário 2.1.1). Seja* $\varphi_i : A \longrightarrow A_{M_i}$ *a aplicação natural, como* A_{M_i} *tem a propriedade da fatoração única de ideais* $\varphi_i(I) = (M_i A_{M_i})^{a_i}$ *para um único inteiro* $a_i > 0, i = 1, \ldots, s$. *Afirmamos que* $I = M_1^{a_1} \cdots M_s^{a_s}$. *Por construção,*

$$I \subseteq \varphi_1^{-1}((M_1 A_{M_1})^{a_1}) \cap \cdots \cap \varphi_s^{-1}((M_s A_{M_s})^{a_s}).$$

Desde que $M_i^{a_i} \subseteq \varphi_i^{-1}((M_i A_{M_i})^{a_i})$ *e* M_i *é o único ideal maximal de* A *que contém* $M_i^{a_i}$, *pelo lema 0.1.5,* $M_i^{a_i} = \varphi_i^{-1}((M_i A_{M_i})^{a_i})$. *Como os ideais* $M_i^{a_i}$ *e* $M_j^{a_j}$ *são coprimos se* $i \neq j$, *pelo lema 0.1.8,*

$$M_1^{a_1} \cap \cdots \cap M_s^{a_s} = M_1^{a_1} \cdots M_s^{a_s}.$$

Segue que $I \subseteq M_1^{a_1} \cdots M_s^{a_s}$. *Portanto,*

$$I_{M_i} = (M_i A_{M_i})^{a_i} = (M_1^{a_1} \cdots M_s^{a_s})_{M_i}$$

e novamente pelo lema 0.1.5, $I = M_1^{a_1} \cdots M_s^{a_s}$. *Para mostrar que está fatoração é única, note que qualquer fatoração de* I *deve ser da forma* $M_1^{b_1} \cdots M_s^{b_s}$ *(observação 2.1.1). Então* $I_{M_i} = (M_i A_{M_i})^{a_i} = (M_i A_{M_i})^{b_i}$, *que implica* $a_i = b_i, i = 1, \ldots, s$. ■

Proposição 2.1.3 *Seja* (A, M) *um domínio Noetheriano local de dimensão um. As*

seguintes afirmações são equivalentes:

(1) *A tem a propriedade da fatoração única de ideais.*

(2) *A é um domínio de ideais principais.*

(3) *A é integralmente fechado.*

Demonstração: (1) $\Rightarrow$ (2) *Pela proposição 0.1.1 e pelo fato que M é o único ideal primo de A, basta mostrar que M é principal. Seja* $x \in M \setminus M^2$. *O ideal* $\langle x \rangle$ *pode ser fatorado como produto de ideais primos de A. Como A é um domínio local de dimensão um, o ideal M é o único ideal primo de A não trivial e, portanto,* $\langle x \rangle = M$.

(2) $\Rightarrow$ (1) *É óbvia.*

(2) $\Rightarrow$ (3) *Segue diretamente do lema 1.1.2.*

(3) $\Rightarrow$ (2) *Pela proposição 0.1.1 e pelo fato que M é o único ideal primo de A, basta mostrar que M é principal. Seja* $x \in M, x \neq 0$. *Se* $\langle x \rangle = M$, *não há nada a provar. Se* $\langle x \rangle \neq M$, *pelo corolário 2.1.1 existe* $n \in \mathbb{N}$ *tal que* $M^n \subseteq \langle x \rangle$ *e* $M^{n-1} \not\subseteq \langle x \rangle$. *Sejam* $y \in M^{n-1} \setminus \langle x \rangle$ *e K o corpo de frações de A. Então* $\frac{y}{x} \in K \setminus A$ *pois* $y \notin \langle x \rangle$. *Como A é integralmente fechado,* y/x *não é integral sobre A. Por A ser Noetheriano, M é um* $A-$*módulo finitamente gerado e uma vez que* $M \subseteq K$, *pela proposição 1.1.1,* $(y/x) \cdot M \not\subseteq M$. *Assim, por construção* $yM \subseteq M^n \subseteq \langle x \rangle$, *donde concluímos* $(y/x)M \subseteq A$. *Logo,* $(y/x)M$ *é um ideal de A não contido em M, por M ser o único maximal de A,* $(y/x)M = A$. *Portanto* $M = (x/y)A$ *é um ideal principal.* ■

Agora temos todos os resultados necessários para provar o teorema 1.6.2:

Teorema 2.1.1 *Seja A um domínio Noetheriano de dimensão um. As seguintes afirmações são equivalentes:*

(1) *A é um domínio de Dedekind.*

(2) *A tem a propriedade da fatoração única de ideais.*

Demonstração: *Como A é um domínio Noetheriano de dimensão um, por definição, A é domínio de Dedekind se, e somente se, A é integralmente fechado. Pelo corolário 1.4.2, A é integralmente fechado se, e somente se,* A_M *é integralmente fechado para todo ideal maximal M de A. Portanto nosso teorema segue diretamente das proposições 2.1.2 e 2.1.3.* ■

O teorema 2.1.1 possui uma versão mais forte: *Um domínio é Dedekind se, e somente se, todo ideal é um produto de ideais primos*, veja [10], vol. I.

Seja A um domínio de Dedekind. Vamos introduzir a seguinte terminologia: sejam $I \trianglelefteq A$ e $P \in \mathrm{Max}(A)$, diremos que P *divide* I e, denotaremos por $P|I$, se I pode ser fatorado em A como $I = PJ$, para algum $J \trianglelefteq A$. Dados I e P, definimos a *ordem* de I em P por ser o inteiro $\mathrm{ord}_P(I)$ como segue: fatorando $I = P_1^{a_1} \cdots P_s^{a_s}$, então $\mathrm{ord}_P(I) := a_i$ se $P = P_i$ para algum i e $\mathrm{ord}_P(I) := 0$ se $P \neq P_i$ para todo i, neste caso diremos que P não divide I. Lembramos que pelo corolário 2.1.1, a $\mathrm{ord}_P(I) = 0$ exceto para um número finito de ideais maximais. Então podemos escrever

$$I = \prod_{P \in \mathrm{Max}(A)} P^{\mathrm{ord}_P(I)} = \prod_{P|I} P^{\mathrm{ord}_P(I)}.$$

Observe que $\mathrm{ord}_P(I)$ é um invariante local de I, ou seja, para todo $S \subseteq A$ conjunto multiplicativo tal que $S \cap P = \emptyset, \mathrm{ord}_P(I) = \mathrm{ord}_{S^{-1}P}(S^{-1}I)$.

Seja $P \in \mathrm{Spec}(A)$ tal que A_P é domínio de Dedekind. Lembrando que A_P é um anel local cujo ideal maximal é PA_P podemos definir $\mathrm{ord}_P(I)$ como sendo $\mathrm{ord}_{PA_P}(IA_P)$.

Finalizaremos esta seção com alguns resultados sobre o número de geradores de ideais num domínio de Dedekind. Nas demonstrações utilizaremos o *teorema do Resto Chinês* cuja prova pode ser encontrada em *[1]*:

Teorema 2.1.2 *Sejam A um anel comutativo, $I_1, \ldots, I_n$ ideais de A dois a dois coprimos. Sejam $y_1, \ldots, y_n \in A$. Então existe um elemento $y \in A$ tal que $y - y_j \in I_j$ para todo $j = 1, \ldots, n$.*

Corolário 2.1.2 *A aplicação natural $\varphi : A \to \prod_{i=1}^n A/I_i$ é sobrejetiva e seu núcleo é $\prod_{i=1}^n I_i$. Isto é, $A/\langle I_1 \cdots I_n \rangle \cong \prod_{i=1}^n A/I_i$.*
Demonstração: *A sobrejetividade de φ segue imediatamente do teorema 2.1.2. O núcleo de φ é $\bigcap_{i=1}^n I_i$, o qual pelo lema 0.1.8 é igual a $\prod_{i=1}^n I_i$.* ■

A prova da seguinte proposição é feita utilizando o *teorema do resto chinês* e a existência de fatoração de ideais num domínio de Dedekind, a prova detalhada pode ser encontrada em [6], página 92.

Proposição 2.1.4 *Todo ideal de um domínio de Dedekind pode ser gerado por dois elementos.*

Proposição 2.1.5 *Seja A um domínio semi-local de dimensão um que possui a propriedade da fatoração única de ideais. Então A é um domínio principal.*
Demonstração: *Seja $M \in \mathrm{Max}(A)$. Por A ter a propriedade da fatoração única de ideais, $M^2 \neq M$. Sejam $m \in M \setminus M^2$ e $M_1, \ldots, M_s$ os ideais maximais de A diferentes*

de M. Uma vez que os ideais $M^2, M_1, \ldots, M_s$ são coprimos dois a dois, o teorema 2.1.2 nos garante que existe um elemento $x \in A$ tal que $x \equiv m \mod M^2$ e $x \equiv 1 \mod M_i, \forall i$. Afirmamos que $M = \langle x \rangle$. Como $x - 1 \in M_i$, concluímos que $\langle x \rangle \not\subseteq M_i, \forall i$. Então $\langle x \rangle = M^a$ para algum $a \geqslant 0$. Por $x - m \in M^2$ e $m \in M \setminus M^2$, segue $\langle x \rangle \subseteq M$, mas $\langle x \rangle \not\subset M^2$. Assim, $\langle x \rangle = M$ e isto mostra que todo ideal maximal de A é principal. Como todo ideal de A é produto de ideals maximais, concluímos que todo ideal de A é principal. ■

2.2 Índice de Ramificação e Grau Residual

Sejam A um domínio de Dedekind e K seu corpo de frações. Seja B o fecho integral de A numa extensão finita $L|K$. Suponhamos que B seja finitamente gerado como $A-$módulo (e assim, um domínio de Dedekind). Por exemplo, pelo teorema 1.3.1 B é um $A-$módulo finitamente gerado quando a extensão $L|K$ é separável. Dado $P \in \mathrm{Max}(A)$, mostraremos que o ideal PB nunca é um ideal trivial em B. E como B é um domínio de Dedekind, o ideal PB é fatorado em B como produto $\prod_{i=1}^{s} M_i^{e_i}$ de ideais primos de B. Estabeleceremos uma relação entre os inteiros $e_1, \ldots, e_s$ e o grau da extensão. E na próxima seção, descreveremos a fatoração de PB no caso especial quando o domínio de Dedekind B é dado como $A[\alpha]$, onde α é raiz de um polinômio mônico $f \in A[y]$.

Lema 2.2.1 *Sejam A um domínio de Dedekind, K seu corpo de frações e B o fecho integral de A numa extensão finita $L|K$. Dado $P \in \mathrm{Max}(A)$, $PB \neq B$.*
Demonstração: *Inicialmente verificaremos o caso em que P é principal, ou seja, $P = \langle p \rangle$. Suponha $PB = B$, então existe $b \in B$ tal que $pb = 1$. Como $P \neq A$, segue que $b \notin A$. Seja $f(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 \in A[y]$ o polinômio mônico de grau mínimo tal que $f(b) = 0$. Como $pb = 1$,*

$$pf(b) = y^{n-1} + a_{n-1}y^{n-2} + \cdots + a_1 + a_0 p = 0,$$

absurdo pela minimalidade do grau de f. Logo $PB \neq B$. No caso geral, usando a localização reduziremos ao caso em que P é principal. Seja $S := A \setminus P$, então $PB \neq B$ se, e somente se, $S^{-1}P \cdot S^{-1}B \neq S^{-1}B$. Lembramos que $S^{-1}A = A_P$ é um domínio de ideais principais pois A é um domínio de Dedekind (veja 2.1.5). ■

Definição 2.2.1 *Nas condições do lema 2.2.1, escreva PB como produto de ideais maximais:*

$$PB = M_1^{e_1} \cdots M_s^{e_s}, \quad \textit{para alguns inteiros positivos } e_1, \ldots, e_s.$$

O inteiro $e_{M_i/P} := e_i$ *é chamado de* índice de ramificação *de* M_i *em* P .

Um caso mais frequente da definição 2.2.1 é o seguinte:

Definição 2.2.2 *Sejam* A *um domínio de Dedekind com corpo de frações* K, $L|K$ *uma extensão finita e* B *o fecho integral de* A *em* L. *Suponha* B *um* $A-$*módulo finitamente gerado. Seja* M *um ideal maximal de* B. *O ideal primo* $P := M \cap A$ *é maximal (veja 1.5.1). Chamaremos o inteiro* $\mathrm{ord}_M(PB)$ *de* índice de ramificação *de* M *sobre* P, *e denotaremos por* $e_{M/P}$.

Considere $M_i \cap A = P$, a inclusão $A \subseteq B$ induz a seguinte injeção

$$A/P \longrightarrow B/M_i, \quad \text{para } i = 1, \ldots, s.$$

Por B ser um $A-$módulo finitamente gerado, o corpo B/M_i é um extensão finita do corpo A/P. Seja $f_{M_i/P} := [B/M_i : A/P]$ a dimensão de B/M_i como $A/P-$espaço vetorial. Quando não causar confusão escreveremos apenas f_i ao invés de $f_{M_i/P}$.

Definição 2.2.3 *O corpo* A/P *é chamado de* corpo residual *de* A *em* P. *O inteiro* $f_{M_i/P}$ *é chamado de grau residual de* M_i *sobre* P.

Exemplo 2.2.1 *Sejam* $A = \mathbb{Z}$ *e* $B = \mathbb{Z}[i]$. *Tome* $P := \langle 2\rangle\mathbb{Z}$. *Em* $\mathbb{Z}[i]$, $2 = i(i-1)^2$ *e* i *é um elemento inversível. Seja* $M := \langle i-1\rangle\mathbb{Z}[i]$, *assim* $P\mathbb{Z}[i] = M^2$. *Para mostrar que* M *é maximal, basta observar* B/M *é corpo:*

$$\mathbb{Z}[i]/\langle i-1\rangle \cong (\mathbb{Z}[y]/\langle y^2+1\rangle)/\langle y-1\rangle \cong \mathbb{Z}[y]/\langle y^2+1, y-1\rangle \cong \mathbb{Z}[y]/\langle 2, y-1\rangle \cong \mathbb{Z}_2[y]/\langle y-1\rangle \cong \mathbb{Z}_2.$$

Então $\mathbb{Z}/P \cong \mathbb{Z}_2 \cong \mathbb{Z}[i]/M$. *Em particular,* $f_{M/P} = 1$. *Uma vez que* M *é maximal e* $P\mathbb{Z}[i] = M^2$, $e_{M/P} = 2$.

Sejam $q \equiv 3(\mathrm{mod}4)$ *um número primo,* $Q := \langle q\rangle\mathbb{Z}$ *e* $N := \langle q\rangle\mathbb{Z}[i]$. *Observamos que*

$$\mathbb{Z}[i]/N \cong (\mathbb{Z}[y]/\langle y^2+1\rangle)/\langle q\rangle \cong \mathbb{Z}[y]/\langle y^2+1, q\rangle \cong \mathbb{Z}_q[y]/\langle y^2+1\rangle,$$

e y^2+1 *é um polinômio irredutível em* $\mathbb{Z}_q[y]$ *se* $q \equiv 3(\mathrm{mod}4)$, *portanto* $\langle y^2+1\rangle$ *é maximal o que implica que* N *é maximal. Em particular, o corpo* $\mathbb{Z}_q[y]/\langle y^2+1\rangle$ *é um extensão de grau 2 de* $\mathbb{Z}_q$, *assim* $f_{N/Q} = 2$. *Além disso, por* N *ser maximal e* $Q\mathbb{Z}[i] = N$, $e_{N/Q} = 1$.

O índice de ramificação $e_{M/P}$ pode ser definido numa maneira mais geral. Sejam $\varphi : A \to B$ um homomorfismo de anéis, $M \in \mathrm{Spec}(B)$ e $P := \varphi^{-1}(M)$. Considere a sequência $A \xrightarrow{\varphi} B \to B_M$. A imagem de todo elemento de $A \backslash P$ é inversível em B_M. Pela *Propriedade Universal de Anéis de Frações* (proposição 1.4), existe um único homomorfismo de anéis $\varphi' : A_P \to B_M$ tal que o seguinte diagrama é comutativo

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow & & \downarrow \\ A_P & \xrightarrow{\varphi'} & B_M. \end{array}$$

Vamos assumir que B_M é um domínio local de ideais principais e assim a aplicação ord_{MB_M} estará bem definida. Se $\varphi(P)B_M \neq \langle 0 \rangle$, chamamos o inteiro $\mathrm{ord}_{MB_M}(\varphi(P)B_M)$ de índice de ramificação de M sobre P e denotamos por $e_{M/P}$. Pela unicidade de φ', este índice está bem definido.

Lema 2.2.2 *Sejam A um anel e $P \in \mathrm{Max}(A)$. Seja $S \subseteq A \setminus P$ um conjunto multiplicativo. Então os corpos $A/P \cong S^{-1}A/S^{-1}P$ como corpos.*
Demonstração: *Como $S \subseteq A \setminus P$, $S^{-1}P$ é um ideal maximal de $S^{-1}A$ e, portanto $S^{-1}A/S^{-1}P$ é corpo. Considere a composição*

$$A \xrightarrow{j} S^{-1}A \xrightarrow{\pi} (S^{-1}A/S^{-1}P).$$

Desde que $(\pi \circ j)(P) = 0$, a plicação $\pi \circ j$ se fatora em termos da aplicação $\eta : A \longrightarrow A/P$. Seja $h : A/P \longrightarrow S^{-1}A/S^{-1}P$ é o único homomorfismo de anéis tal que $h \circ \eta = \pi \circ j$. Como A/P é corpo, a aplicação h é injetiva (a aplicação h não é nula). Para mostrar a sobrejetividade, sejam $a/s + S^{-1}P$ uma classe em $S^{-1}A/S^{-1}P$ e $t \in A$ tal que $st - 1 \in P$. Afirmamos que $h(at + P) = a/s + S^{-1}P$. De fato, uma vez que $ts - 1 \in P$, $a(ts-1)/s = at/1 - a/s \in S^{-1}P$. ■

Teorema 2.2.1 *Sejam A um domínio de Dedekind com corpo de frações K e $L|K$ uma extensão finita. Seja B o fecho integral de A em L. Se B é um $A-$módulo finitamente gerado, então*

$$[L : K] = \sum_{M|PB} e_{M/P} f_{M/P}.$$

Demonstração: *Seja $PB = \prod_{i=1}^{s} M_i^{e_i}$. Desde que os ideais $M_i^{e_i}$ são dois a dois coprimos, $i = 1, \ldots, s$,*

$$B/PB \cong \prod_{i=1}^{s} B/M_i^{e_i}.$$

Cada um dos anéis B/PB e $B/M_i^{e_i}, i = 1, \ldots, s$, podem ser considerados como um $(A/P)-$espaço vetorial. Mostraremos que:

1. $\dim_{A/P}(B/PB) = [L:K],\ e$
2. $\dim_{A/P}(B/M_i^{e_i}) = e_i \cdot \dim_{A/P}(B/M_i) = e_i f_i, \forall i = 1, \ldots, s.$

Primeiramente mostraremos ambas as afirmações para o caso em que A e B são domínios de ideais principais. Como B é um $A-$módulo livre de torção (B é domínio) finitamente gerado, segue do teorema da estrutura de módulos sobre domínio de ideais principais que B é um $A-$módulo livre de posto igual a $n = [L:K]$ (lema 1.3.1). Considere $P = \langle p \rangle$ em A, então

$$B/PB \cong (A \oplus \cdots \oplus A)/(pA \oplus \cdots \oplus pA) \cong (A/P)^n.$$

Por isso, a dimensão de B/PB como $(A/P)-$álgebra é igual a n. Suponha que $P \subset M^e$, de modo que B/M^e é um $A/P-$espaço vetorial. Mostraremos por indução sobre e,

$$\dim_{A/P}(B/M^e) = e \cdot \dim_{A/P}(B/M).$$

Considere a sequência exata de $A/P-$espaços vetoriais:

$$0 \longrightarrow M^{e-1}/M^e \longrightarrow B/M^e \longrightarrow B/M^{e-1} \longrightarrow 0.$$

Pela hipótese de indução

$$\begin{aligned} \dim_{A/P}(B/M^e) &= \dim_{A/P}(B/M^{e-1}) + \dim_{A/P}(M^{e-1}/M^e) \\ &= (e-1)\dim_{A/P}(B/M) + \dim_{A/P}(M^{e-1}/M^e). \end{aligned}$$

Para concluir, mostraremos que M^{e-1}/M^e é um $B/M-$espaço vetorial de dimensão 1, portanto um $A/P-$espaço vetorial de dimensão $\dim_{A/P}(B/M)$. Sejam m o gerador do ideal maximal M de B que contém P(lembre-se que B é um domínio de ideais principais). A aplicação natural

$$\begin{array}{rccc} \pi: & B & \longrightarrow & M^{e-1}/M^e \\ & 1 & \longmapsto & \text{classe de } m^{e-1} \end{array}$$

é sobrejetiva e induz um isomorfismo de $(B/M)-$módulos:

$$B/M \cong M^{e-1}/M^e.$$

Portanto, $\dim_{B/M}(M^{e-1}/M^e) = 1$ e assim a afirmação (2) está provada quando A e B são domínios de ideais principais.

Para o caso geral, tome $S := A \setminus P$. Claramente S é um conjunto multiplicativo. Pela proposição 2.1.3 $S^{-1}A = A_P$ é um domínio de ideais principais com corpo de frações K. O fecho integral de A_P em L é $S^{-1}B$ (corolário 1.4.1). Como $M_1, \ldots, M_s$ são os únicos

ideais maximais de B que não interceptam S, segue que $S^{-1}B$ é um domínio de Dedekind semi local. A proposição 2.1.5 implica que $S^{-1}B$ é um domínio de ideais principais. Entretanto, um vez que os ideais $S^{-1}M_i, i = 1, \ldots, s$, são ideais maximais não triviais em $S^{-1}B$, concluímos que

$$(S^{-1}P)(S^{-1}B) = \prod_{i=1}^{s}(S^{-1}M_i)^{e_i}$$

é a fatoração de $(S^{-1}P)(S^{-1}B)$ em $S^{-1}B$. Portanto, como ambos $S^{-1}A$ e $S^{-1}B$ são domínios de ideais principais, pela discussão feita para o caso em que A e B eram principais, segue a identidade:

$$[L : K] = \sum_{i=1}^{s} e_i f_i^{'},$$

onde $f_i^{'} := \dim_{S^{-1}A/S^{-1}P}(S^{-1}B/S^{-1}M_i)$. Assim o teorema segue do lema 2.2.2.

2.3 Fatorações Explicitas

Nesta seção daremos um primeira aplicação do teorema 2.2.1 na proposição 2.3.1, a qual descreve explicitamente como fatorar o ideal PB quando B é um domínio de Dedekind especial da seguinte forma. Sejam A um domínio de Dedekind, $f \in A[y]$ mônico irredutível de grau n e $C_f := A[y]/\langle f\rangle$. Denote por L o corpo de frações de C_f. O corpo L é um extensão de grau n do corpo de frações K de A . O anel C_f é uma extensão inteira de A e pode ser ou não igual ao fecho integral de A em L. Seja $P \subseteq A$ um ideal maximal. A proposição 2.3.1 seguinte descreverá a fatoração do ideal PC_f em C_f quando C_f for um domínio de Dedekind.

O caso em que $A = \overline{k}[x]$ foi tratado com detalhes no exemplo 2.0.1. Vamos checar o que o teorema 2.2.1 diz neste caso. Observe,

- $A/P = \overline{k}[x]/\langle x - a\rangle \cong \overline{k}$.
- $\overline{C}_f/M_i = \overline{k}[x, y]/\langle x - a, y - b_i\rangle \cong \overline{k}$.

Em particular, $f_{M_i/P} = 1$ para todo $i = 1, \ldots, s$. Uma vez que f é um polinômio mônico em y de grau n,

$$[L : K] = \deg(f) = n = \sum_{i=1}^{s} e_i = \sum_{i=1}^{s} e_{M_i/P} f_{M_i/P},$$

que verifica o teorema 2.2.1.

Retornaremos para o problema de fatoração do ideal PC_f. Como no exemplo 2.0.1, o primeiro passo é descrever todo ideal maximal de C_f que contém P. Se $h \in A[y]$, então $\overline{h}$ denota a classe de h em $(A/P)[y]$. Seja

$$\overline{f}(y) = \prod_{i=1}^{s} \overline{g}_i(y)^{e_i},$$

onde $\overline{g}_i \in (A/P)[y]$ é irredutível e mônico para todo $i = 1, \ldots, s$. Seja $g_i \in A[y]$ mônico tal que $\deg(g_i) = \deg(\overline{g}_i)$ e sua redução em $(A/P)[y]$ é $\overline{g}_i(y)$. Podemos escrever

$$f(y) = \prod_{i=1}^{s} g_i(y)^{e_i} + h(y), h \in PA[y].$$

Sejam $g_i(\alpha)$ a imagem de $g_i(y)$ em C_f e $M_i := \langle P, g_i(\alpha)\rangle \trianglelefteq C_f$. Desde que $\overline{g}_i(y)$ é irredutível em $(A/P)[y]$, o ideal M_i é maximal, pois:

$$C_f/M_i \cong A[y]/\langle P, g_i(\alpha), f\rangle \cong (A/P)[y]/\langle \overline{g}_i\rangle \text{ que é corpo.}$$

Observe que existe uma bijeção entre o conjunto dos ideais maximais de C_f que contém PC_f e o conjunto dos ideais maximais de C_f/PC_f. Ainda, $C_f/PC_f \cong (A/P)[y]/\langle \overline{f}\rangle$. Como os únicos ideais maximais de $(A/P)[y]/\langle \overline{f}\rangle$ são os ideais gerados pelos elementos $\overline{g}_i, i = 1, \ldots, s$, concluímos:

Fato 2.3.1 *Seja A um domínio de dimensão um. Sejam $P \in \mathrm{Max}(A)$, $f \in A[y]$ mônico e $N_i := \langle P, g_i\rangle, i = 1, \ldots, s$. O conjunto $\{N_1, \ldots N_s\}$ é o conjunto dos ideais maximais de $A[y]$ que contém $\langle P, f\rangle$. O conjunto $\{M_1, \ldots, M_s\}$ é o conjunto dos ideais maximais de C_f que contém P.*

Observe:

- $[C_f/M_i : A/P] = \deg(g_i)$, e
- $[L : K] = \deg(f) = \sum_{i=1}^{s} e_i \deg(g_i)$.

Proposição 2.3.1 *Com as hipóteses e notações acima, $PC_f \supseteq M_1^{e_1} \cdots M_s^{e_s}$. Se C_f é um domínio de Dedekind, então $PC_f = M_1^{e_1} \cdots M_s^{e_s}$. Além disso, $f_{M_i/P} = \deg(g_i)$.*
Demonstração: *É claro que $M_1^{e_1} \cdots M_s^{e_s} \subseteq \langle P, g_1^{e_1}(\alpha), \ldots, g_s^{e_s}(\alpha)\rangle$. Seja $h(\alpha)$ imagem de $h(y)$ em C_f. Se $h \in PA[y]$ então $h(\alpha) \in PC_f$. Uma vez que $f(\alpha) = 0$,*

$$\prod_{i=1}^{s} g_i^{e_i}(\alpha) \in \langle h(\alpha)\rangle \subseteq PC_f.$$

Assim, $M_1^{e_1} \cdots M_s^{e_s} \subseteq PC_f$. *Assuma agora que* C_f *é um domínio de Dedekind, então o ideal* PC_f *se fatora, de acordo com o teorema 2.2.1 como,*

$$PC_f = M_1^{e_{M_1/P}} \cdots M_s^{e_{M_s/P}},$$

com $[L : K] = \sum_{i=1}^{s} e_{M_i/P} f_{M_i/P}$. *De* $PC_f \supseteq M_1^{e_1} \cdots M_s^{e_s}$, *concluímos que* $e_i \geqslant e_{M_i/P}$, *para* $i = 1, \ldots, s$. *Por construção,* $f_{M_i/P} = \deg(g_i)$ *e* $[L : K] = \sum_{i=1}^{s} e_i f_{M_i/P}$. *Portanto* $e_i = e_{M_i/P}$ *e* $PC_f = M_1^{e_1} \cdots M_s^{e_s}$. ■

Exemplo 2.3.1 Corpos de Números Quadráticos. *Seja* d *um inteiro livre de quadrado. O anel de inteiros algébricos* B *em* $\mathbb{Q}(\sqrt{d})$ *é:*

- $B = \mathbb{Z}[\sqrt{d}]$ *se* $d \equiv 2$ *ou* 3 mod4.
- $B = \mathbb{Z}[(1 + \sqrt{d})/2]$ *se* $d \equiv 1$ mod4.

Seja $p \in \mathbb{Z}$ *um número primo. Como* $\mathbb{Q}(\sqrt{d})|\mathbb{Q}$ *é finita, pela teorema 2.2.1 a fatoração do ideal* pB *é:*

$$pB = \begin{cases} P, & \text{onde } P \text{ é um ideal primo com } f_{P/\langle p\rangle} = 2; \\ P_1P_2, & \text{onde } P_1, P_2 \text{ são ideais primos distintos;} \\ P^2, & \text{onde } P \text{ é um ideal primo com } f_{P/\langle p\rangle} = 1. \end{cases}$$

A determinação de quais dos três casos ocorre para cada primo p *pode ser feita usando a proposição 2.3.1. A fatoração dos primos de* $\mathbb{Z}$ *em* B *segue abaixo:*

1. *Se* $p|d$, *então* $pB = \langle p, \sqrt{d}\rangle^2$.
2. *Se* $2 \nmid d$, *então*

$$2B = \begin{cases} \text{ideal primo}, & \text{se } d \equiv 5 \mod 8; \\ \langle 2, \frac{1+\sqrt{d}}{2}\rangle\langle 2, \frac{1-\sqrt{d}}{2}\rangle, & \text{se } d \equiv 1 \mod 8; \\ \langle 2, 1 + \sqrt{d}\rangle^2, & \text{se } d \equiv 3 \mod 4. \end{cases}$$

   E os ideais $\langle 2, \frac{1+\sqrt{d}}{2}\rangle$ *e* $\langle 2, \frac{1-\sqrt{d}}{2}\rangle$ *são distintos.*

3. *Se* $p \nmid d$ *e* p *é impar, então*

$$pB = \begin{cases} \text{ideal primo}, & \text{se } d \text{ não é um quadrado } \mathrm{mod}p; \\ \langle p, \sqrt{d} + n\rangle\langle p, \sqrt{d} - n\rangle, & \text{se } n^2 \equiv d \mod p. \end{cases}$$

   Os ideais $\langle p, \sqrt{d} + n\rangle$ *e* $\langle p, \sqrt{d} - n\rangle$ *são distintos.*

2.4 Primos Ramificados e Não Ramificados

O objetivo desta seção é introduzir o conceito de ideais ramificados e não ramificados e sua interpretação geométrica.

Definição 2.4.1 *Sejam $L|K$ uma extensão finita, A um domínio de Dedekind com corpo de frações K e B seu fecho integral em L. Suponha B um $A-$módulo finitamente gerado. Sejam $M \in \mathrm{Max}(B)$ e $P := M \cap A$. O ideal M é* ramificado *sobre P (ou sobre A) se $e_{M/P} > 1$ ou a extensão B/M é não separável sobre A/P. Se o ideal M não for ramificado sobre P, então diremos que ele é* não ramificado *sobre P ou sobre A. Um ideal maximal P de A* ramifica *em B se PB está contido em um ideal maximal M de B que é ramificado sobre A. Quando nenhum ideal maximal de B é ramificado sobre A, diremos que a extensão $B|A$ é não-ramificada.*

Quando não causar confusão chamaremos o ideal maximal de *ramificado* ou invés de *ramificado sobre A*. O conceito de uma ideal primo ramificado é definido da forma análoga. A motivação para esta definição ficará clara na proposição 2.5.1 e no corolário 2.5.1 da próxima seção. Pelos exemplos a seem discutidos, observamos que em geral é mais fácil caracterizar os ideais ramificados.

A seguir discutiremos dois exemplos de extensões $B|A$ onde toda extensão do corpo residual é separável.

Sejam B um anel de inteiros numa extensão finita de $\mathbb{Q}$ e $M \in \mathrm{Max}(B)$. O corpo B/P é finito. De fato, como B é integral sobre $\mathbb{Z}$, o ideal primo $M \cap \mathbb{Z}$ é não trivial (observação 1.5.1), assim $M \cap \mathbb{Z} = \langle p \rangle$ para algum primo $p \in \mathbb{Z}$. Portanto B/M é uma extensão finita do corpo $\mathbb{Z}/p\mathbb{Z}$ de grau $f_{P/\langle p \rangle}$, como $\mathbb{Z}/p\mathbb{Z}$ é finito segue que o corpo B/P é finito. Em particular, se B' é outro anel de inteiros contendo B, então um ideal primo M' de B' é ramificado sobre B se, e somente se, $e_{M/P} > 1$, onde $P := M' \cap B$.

Considere agora $f \in \overline{k}[x, y]$ irredutível. Sejam $\overline{C}_f = \overline{k}[x, y]/\langle f \rangle$ e $M \in \mathrm{Max}(\overline{C}_f)$. Afirmamos que o $\overline{C}_f/M \cong \overline{k}$. De fato, M é gerado pelas imagens em $\overline{C}_f$ de $\langle x - a \rangle$ e $\langle y - b \rangle$ para algum $(a, b) \in Z_f(\overline{k})$. Portanto,

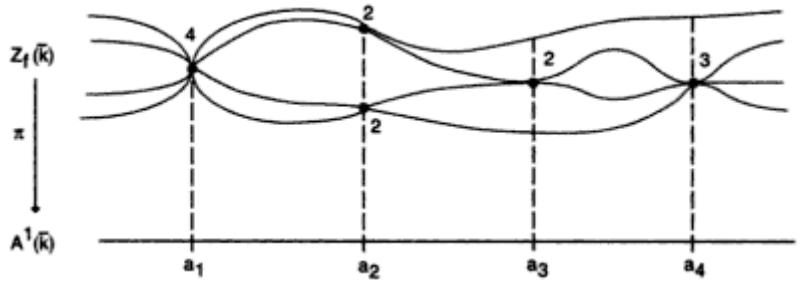
$$\overline{C}_f/M \cong \overline{k}[x, y]/\langle x - a, y - b \rangle \cong \overline{k}.$$

Assim, o corpo residual $\overline{C}_f/M$ é perfeito.

A seguir interpretamos geometricamente a definição 2.4.1. Seja f um polinômio irredutível, mônico em y tal que $\deg_y f = n > 0$. Seja $\overline{C}_f := \overline{k}[x, y]/\langle f \rangle$. Suponha a curva $Z_f(\overline{k})$ não singular e considere a inclusão $\overline{k}[x] \subseteq \overline{C}_f$. Uma vez que f é mônico em y a extensão $C_f|\overline{k}[x]$ é integral e, desde que $Z_f(\overline{k})$ é não singular, $\overline{C}_f$ é o fecho integral

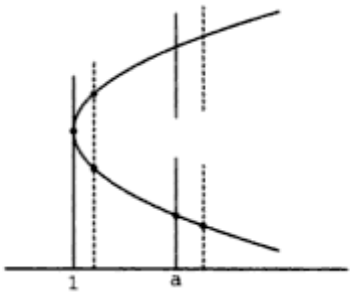
de $\overline{k}[x]$ em $\overline{k}(Z_f)$ (veja 1.7.2). A aplicação $\pi : Z_f(\overline{k}) \to \mathbb{A}^1(\overline{k})$ dada por $(a,b) \mapsto a$ é sobrejetora. Verificaremos que o conjunto de ideais primos de $\overline{k}[x]$ que ramificam em C_f está em bijeção com o conjunto dos pontos $a \in \mathbb{A}^1(\overline{k})$ tal que $\pi^{-1}(a)$ contém menos de n pontos. De fato, uma vez que todo corpo residual de $\overline{k}[x]$ é perfeito, um ideal $M = \langle x-a, y-b\rangle$ é ramificado sobre $P := \langle x-a\rangle$ se, e somente se, $e_{M/P} > 1$. Como $\sum_{M|P\overline{C}_f} e_{M/P} = n$, o ideal P ramifica em $\overline{C}_f$ se, e somente se, existem menos que n ideais maximais distintos de $\overline{C}_f$ que contém $x-a$. Assim, P ramifica em $\overline{C}_f$ se, e somente se, $\pi^{-1}(a)$ contém menos de n pontos.

Sejam $(a,b) \in Z_f(\overline{k})$ e $M := \langle x-a, y-b\rangle \in \mathrm{Max}(\overline{C}_f)$. Se $e_{M/M\cap\overline{k}[x]} > 1$, então o ponto (a,b) é chamado de *ponto de ramificação* de π. O conjunto dos pontos de ramificação é chamado de *lugar de ramificação* de π. A imagem do lugar de ramificação é chamado de *lugar dos ramos* de π. A aplicação π é chamada uma *cobertura*, uma vez que ela é sobrejetora. Se o lugar dos ramos de π é não vazio, então π é chamada *cobertura ramificada*. Seja $a \in \mathbb{A}^1(\overline{k})$, o conjunto $\pi^{-1}(a)$ é chamado de *fibra* de π sobre a. Nas condições acima sobre a aplicação $Z_f(\overline{k})$, o lugar dos ramos de π é o conjunto de pontos em $\mathbb{A}^1(\overline{k})$ tais que a fibra $\pi^{-1}(a)$ contém menos que n pontos. A figura a seguir ilustra quatro possibilidades de ramificação para uma cobertura ramificada π. O índice de ramificação é indicado próximo do ponto de $Z_f(\overline{k})$ que ramifica sobre $\mathbb{A}^1(\overline{k})$.



A terminologia de *ramificado* e *não ramificado* tem origem na geometria, como discutiremos agora.

Exemplo 2.4.1 *Sejam $f(x,y) = (y-2)^2 - (x-1)$ e $\overline{C}_f = \mathbb{C}[x,y]/\langle f\rangle$. Considere a aplicação $\pi : Z_f(\mathbb{C}) \to \mathbb{A}^1(\mathbb{C})$ correspondente a inclusão $\mathbb{C}[x] \hookrightarrow \overline{C}_f$. Como a curva $Z_f(\mathbb{C})$ é não singular, o anel $\overline{C}_f$ é o fecho integral do anel $\mathbb{C}[x]$ em $\mathbb{C}(Z_f)$. A seguinte figura é uma representação de $Z_f(\mathbb{R})$.*



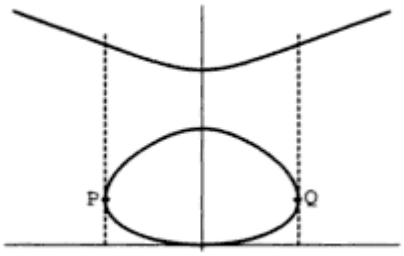
Para cada valor $a \in \mathbb{R}_{>1}$, *a reta* $x - a = 0$ *não é tangente a* $Z_f(\mathbb{R})$ *e a pré-imagem do ponto* $(a, 0) \in \mathbb{A}^1(\mathbb{R})$ *em* $Z_f(\mathbb{R})$ *consiste em dois pontos distintos* $(a, 2 + \sqrt{a-1})$ *e* $(a, 2 - \sqrt{a-1})$. *O ideal* $\langle x - a \rangle$ *se fatora em* $\overline{C}_f$ *como*

$$\langle x - a \rangle = \langle x - a, y - 2 + \sqrt{a-1} \rangle \langle x - a, y - 2 - \sqrt{a-1} \rangle.$$

Quando $a \neq 1$, *o ideal maximal* $M_{a\pm} := \langle x - a, y - 2 \pm \sqrt{a-1} \rangle$ *tem índice de ramificação igual a* 1. *A extensão dos corpos de resíduos definidos por* $M_{a\pm}$ *é trivial e, portanto, é separável. Assim, o ideal* $M_{a\pm}$ *é não ramificado sobre* $\mathbb{C}[x]$. *Quando* $a = 1$, *a reta* $x - a$ *é tangente a* $Z_f(\mathbb{R})$. *O ideal* $\langle x - 1, y - 2 \rangle$ *é ramificado sobre* $\mathbb{C}[x]$, *uma vez que ele tem índice de ramificação igual a* 2.

A terminologia ramificado/não-ramificado *pode ser explicado geometricamente do seguinte modo: Quando a reta* $x - 1 = 0$ *é levemente movida para a direita, o ponto* $(1, 2)$ *se* ramifica *em dois pontos distintos. Em outras palavras quando* $a > 1$, *podemos encontrar* $\delta > 0$ *e um pequena vizinhança* U *de* $(a, 2 - \sqrt{a-1})$ *em* $Z_f(\mathbb{R})$ *tal que a correspondência* $[a - \delta, a + \delta] \to Z_f(\mathbb{R})$, $t \mapsto \{x - t = 0\} \cap U$ *é bijeção.*

Exemplo 2.4.2 *Seja* $f(x, y) = x^2 - y(y-1)(y - \frac{3}{2})$. *A curva* $Z_f(\mathbb{C})$ *é suave e os pontos de ramificação da aplicação projeção* $\pi : Z_f(\mathbb{C}) \to \mathbb{A}^1(\mathbb{C})$ *são pontos* (a, b) *tais que* $f(a, b) = 0 = \frac{\partial f}{\partial y}(a, b)$. *Existem quatro destes tais pontos, mas apenas dois deles* P *e* Q *têm coordenadas reais.*



Seja B/A uma extensão como na definição 2.4.1, segue da mesma que um ideal maximal M de B é não ramificado sobre P se, e só se, $PB_M = MB_M$ e B/M é separável sobre A/P. Como mencionado acima, faz sentido falar de ramificação mesmo quando a extensão $B|A$ é não inteira. A definição mais geral de não ramificado dada abaixo é usado para definir pontos ramificados de um morfismo qualquer de curvas afins.

Definição 2.4.2 *Sejam $\varphi : A \to B$ um homomorfismo de anéis, $\varphi^a : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ a aplicação associada e $M \in \mathrm{Spec}(B)$. Tome $P := \varphi^{-1}(M) = \varphi^a(M)$. Diremos que M é um* ponto de ramificação *da aplicação φ^a ou que a aplicação φ^a é* ramificada *em M se, $\varphi(P)$ não gera MB_M, ou se B_M/MB_M é um extensão não separável de A_P/PA_P. Se φ^a não se ramifica em M, então diremos que ela é não ramificada em M, e M é um ponto não ramificado. O conjunto dos pontos de $\mathrm{Spec}(B)$ onde φ^a é ramificado é chamado de* lugar de ramificação *de φ^a. A imagem de φ^a $\mathrm{Spec}(A)$ do lugar de ramificação é chamado de* lugar dos ramos *de φ^a. Quando o lugar dos ramos é vazio, a aplicação φ^a é dita não ramificada.*

Sejam $f, g \in \overline{k}[x, y]$ polinômios irredutíveis e $\phi : Z_f(\overline{k}) \to Z_g(\overline{k})$ um morfismo de curvas. Observe que este morfismo é induzido pelo homomorfismo de $\overline{k}-$algebras $\pi^* : \overline{C}_g \to \overline{C}_f$. Observe também que π pode ser identificado com a aplicação $(\pi^*)^a_{|_{\mathrm{Max}(\overline{C}_f)}} : \mathrm{Max}(\overline{C}_f) \to \mathrm{Max}(\overline{C}_g)$ dada por $M \mapsto (\pi^*)^{-1}(M)$. Diremos que π é não ramificada em (a, b) se a aplicação $(\pi^*)^a$ for não ramificada em $(x - a, y - b)$. Desde que $\overline{C}_f$ é um domínio, $\ker(\pi^*)$ é um ideal primo de $\overline{C}_g$ e como $\overline{C}_g$ é um domínio de dimensão 1, há duas possibilidades: $\ker(\pi^*)$ é maximal, caso em que o morfismo π é constante, ou $\ker(\pi^*) = \langle 0 \rangle$. Suponha π^* injetivo e olhemos para $\overline{C}_g$ como subanel de $\overline{C}_f$. Pode acontecer da extensão $\overline{C}_f/\overline{C}_g$ ser não inteira. Entretanto, podemos definir o índice de ramificação de um ponto não singular $(a, b) \in Z_f(\overline{k})$ sobre $\pi(a, b)$ como segue: Seja M o ideal maximal de $\overline{C}_f$ correspondente ao ponto (a, b), então $(\overline{C}_f)_M$ é um domínio de ideais principais e a função $\mathrm{ord}_{M(\overline{C}_f)_M}$ está bem definida. Seja P o ideal maximal de C_g correspondente a $\pi(a, b)$. Uma vez que π^* é injetiva, $P(\overline{C}_f)_M \neq \langle 0 \rangle$. O *índice de ramificação* $e_{(a,b)/\pi(a,b)}$ de (a, b) sobre $\pi(a, b)$ é o inteiro $e_{M/P} := \mathrm{ord}_{M(\overline{C}_f)_M}(P(\overline{C}_f)_M)$. Se $e_{(a,b)/\pi(a,b)} > 1$, então (a, b) é um *ponto ramificado* da aplicação π e π é *ramificada* em (a, b).

2.5 Extensões Simples

Definição 2.5.1 *Seja A um subanel do anel B. A extensão de anéis $B|A$ é* simples *se existe um elemento $\alpha \in B$ tal que $B = A[\alpha]$.*

No caso de extensões de corpos, é fácil dar exemplos de extensões simples. Lembre-se que pelo teorema do elemento primitivo as extensões finitas e separáveis de corpos são

simples. No entanto, no caso de anéis existem vários exemplos de extensões que não são simples, mesmo no caso de extensões de $\mathbb{Z}$. Por exemplo, sejam

$$f(n,y) = y^3 - y^2 - ny - n^3 \in \mathbb{Z}[y]$$

e α uma raiz de f que não está em $\mathbb{Q}$. Considere a extensão $\mathbb{Q}(\alpha)|\mathbb{Q}$. Quando n é par e $27n^4 + 18n^2 - 1$ é livre de quadrado, $\mathcal{O}_{\mathbb{Q}(\alpha)} \neq \mathbb{Z}[\omega]$ para todo $\omega \in \mathcal{O}_{\mathbb{Q}(\alpha)}$. Portanto a extensão $\mathcal{O}_{\mathbb{Q}(\alpha)}|\mathbb{Z}$ não é simples.

Sejam A um domínio de Dedekind e $f \in A[y]$ mônico irredutível. O anel $C_f := A[y]/\langle f \rangle$ é uma extensão simples e inteira do anel A uma vez que é da forma $A[\alpha]$ onde α é a classe de y em C_f. Nosso objetivo nesta seção é dar uma condição suficiente para decidirmos quando a extensão simples C_f é um domínio de Dedekind.

Quando $A = \overline{k}[x]$, o teorema 1.7.1 fornece uma condição necessária e suficiente para $\overline{C}_f$ ser um domínio de Dedekind envolvendo derivadas parciais. No caso em que A é um domínio de Dedekind qualquer, não podemos usar o mesmo argumento de derivadas parciais. A seguinte proposição nos fornece uma condição suficiente para que $\overline{C}_f$ é domínio de Dedekind quando A é Dedekind.

Proposição 2.5.1 *Sejam A um domínio de Dedekind e $f \in A[y]$ irredutível e mônico. Seja α uma raiz de f no fecho algébrico de K, onde K é o corpo de frações de A. Sejam $M \in \mathrm{Max}(A[\alpha])$ e $P := M \cap A$. Seja $\overline{f}(y) = \prod_{i=1}^{s} \overline{g}_i(y)^{e_i}$ a fatoração da imagem de f em $(A/P)[y]$ em polinômios distintos, mônicos e irredutíveis. Escreva $f(y) = h(y) + \prod_{i=1}^{s} g_i(y)^{e_i}$, com $h(y) \in PA[y]$ é tal que a redução de g_i em $(A/P)[y]$ é igual a $\overline{g}_i, \forall i$. Então o ideal M é gerado pelos elementos de P e por $g_{i_0}(\alpha)$, para um único $i_0 \in \{1, \ldots, s\}$. Além disso,*

1. *As seguintes afirmações são equivalentes:*

   (i) $f'(\alpha) \notin M$.

   (ii) $e_{i_0} = 1$ e a extensão $A[\alpha]/M$ é separável sobre A/P.

2. *Seja π o gerador do ideal maximal PA_P de A_P. O anel $A[\alpha]_M$ é um domínio de ideais principais se, e somente se, $MA[\alpha]_M$ pode ser gerado por π ou por $g_{i_0}(\alpha)$.*

3. *Se $e_{i_0} = 1$, então o anel $A[\alpha]_M$ é um domínio de ideais principais e o ideal maximal $MA[\alpha]_M$ é gerado por π. Em particular, $e_{M/P} = 1$.*

4. *O anel $A[\alpha]$ é um domínio de Dedekind se, e somente se, o anel $A[\alpha]_M$ é um domínio de ideais principais para todo ideal maximal M que contenha $f'(\alpha)$. Quando f é um polinômio separável, existe somente uma quantidade finita de $M \in \mathrm{Max}(A[\alpha])$ que contém $f'(\alpha)$.*

Demonstração: *: O fato 2.3.1 implica que* $M = \langle P, g_{i_0}(\alpha)\rangle$ *para um único inteiro* $i_0 \in \{1, \ldots, s\}$. *Demonstraremos o item 1. Em* $A[\alpha]$,

$$f'(\alpha) = h'(\alpha) + \sum_{i=1}^{s} \left(e_i g_i(\alpha)^{e_i - 1} g_i^{'}(\alpha) \prod_{j \neq i} g_j(\alpha)^{e_j} \right).$$

Como $h \in PA[y]$, *segue que* $h' \in PA[y]$,*portanto* $h'(\alpha) \in PA[\alpha]$. *Então*

$$f'(\alpha) \notin M \Leftrightarrow \begin{cases} e_{i_0} = 1 \quad e \\ g_{i_0}^{'}(\alpha) \notin M. \end{cases}$$

Para concluir a prova $(i) \Leftrightarrow (ii)$, *usaremos o lema 0.1.4. Observe:*

Afirmação: *As seguintes afirmações são equivalentes*

(a) *A extensão* $A[\alpha]/M$ *é separável sobre* A/P.

(b) $g_{i_0}^{'}(\alpha) \notin M$.

Esta afirmação segue diretamente da definição de separabilidade. De fato, seja $\overline{\alpha}$ *a imagem de* α *em* $A[\alpha]/M$. *Tome* $\overline{g}_{i_0}$ *a redução de* g_{i_0} *em* $(A/P)[y]$. *Por construção o polinômio* $\overline{g}_{i_0}$ *é irredutível e mônico. O corpo* $A[\alpha]/M$ *é isomorfo a* $(A/P)(\overline{\alpha})$ *e* $\overline{g}_{i_0}$ *é o polinômio minimal de* $\overline{\alpha}$ *sobre* A/P. *A extensão* $A[\alpha]/M$ *é separável sobre* A/P *se, e somente se* $\overline{g}_{i_0}^{'}(\overline{\alpha}) \neq 0$ *em* $A[\alpha]/M$ *(veja 0.1.4). É fácil de ver que* $\overline{g}_{i_0}^{'}(\overline{\alpha}) \neq 0$ *em* $A[\alpha]/M$ *se, e somente se,* $g_{i_0}^{'}(\alpha) \notin M$. *Isso conclui a prova da afirmação anterior e consequentemente a parte* (1) *do teorema.*

Para provar 2, como $M = \langle P, g_{i_0}(\alpha)\rangle$, *concluímos* $MA[\alpha] = \langle \pi, g_{i_0}(\alpha)\rangle$. *Assim* M *é gerado por dois elementos e a parte* (2) *segue do lema 0.1.3.*

Vamos agora provar a parte 3. Suponha que $e_{i_0} = 1$. *A fim de mostrar que* $A[\alpha]_M$ *é um domínio principal, mostraremos que seu ideal maximal* $MA[\alpha]_M$ *é principal e gerado por* π. *Seja* $h \in PA[y]$, *sabemos* $h(\alpha) \in \langle \pi \rangle$. *Em* $A[\alpha]$, $h(\alpha) + g_{i_0}(\alpha)(\prod_{j \neq i_0} g_j^{e_j}(\alpha)) = 0$. *Como* $g_j(\alpha) \notin M$ *se* $j \neq i_0$, *concluímos* $g_j(\alpha)$ *é inversível em* $A[\alpha]_M$ *se* $j \neq i_0$. *Assim, em* $A[\alpha]_M$,

$$g_{i_0}(\alpha) = (\beta) \cdot h(\alpha) \in \langle \pi \rangle A[\alpha]_M, \beta \in A[\alpha]_M \text{ é inversível.}$$

O ideal maximal de $A[\alpha]_M$ *é portanto gerado por* π. *A proposição 0.1.1 implica que* $A[\alpha]_M$ *é domínio de ideais principais. Assim* $PA[\alpha]_M = MA[\alpha]_M$ *e então* $e_{M/P} = 1$.

Para provar a parte 4, usaremos o corolário 1.4.2. Utilizando a parte 3 e em seguida a parte 1, concluímos que $A[\alpha]$ *é um domínio de Dedekind se, e somente se,* $A[\alpha]_M$ *é um domínio de ideais principais para todo* $M \in \mathrm{Max}(A[\alpha])$ *que contém* $f'(\alpha)$. *Quando*

$f(y)$ é um polinômio separável, $f'(\alpha)$ é não nulo em $A[\alpha]$. Desde que $A[\alpha]$ é um domínio Noetheriano de dimensão 1*, o corolário 2.1.1 mostra que existe uma quantidade finita de ideais maximais em $A[\alpha]$ que contém $f'(\alpha)$. E isto conclui a prova da proposição.* ■

A parte dois do próximo corolário completa a caracterização dos ideais maximais de $A[\alpha]$ que são ramificados sobre A quando a extensão simples $A[\alpha]$ é um domínio de Dedekind. Podemos usar o próximo corolário também para justificar a definição de *primos ramificados* na presença de uma possível extensão inseparável do corpo residual uma vez que, como veremos a seguir, os ideais maximais com $e_{M/P} > 1$ não possuem uma caracterização simples, ao contrário dos *primos ramificados*.

Corolário 2.5.1 *Sejam A um domínio de Dedekind e $f \in A[y]$ mônico e irredutível. Tome α como a classe de y em $C_f = A[y]/\langle f(y)\rangle$. Seja $M \in \mathrm{Max}(C_f)$:*

1. *Se $f'(\alpha) \notin M$, então $(C_f)_M$ é um domínio de ideais principais e M é não ramificado sobre A.*
2. *Se C_f é um domínio de Dedekind, então M é ramificado sobre A se, e somente se, $f'(\alpha) \in M$.*

Demonstração: *Tome $P := M \cap A$. Seja $f(y) = \prod_{i=1}^{s} g_i(y)^{e_i} + h(y)$ como na proposição 2.5.1. Então $M = \langle P, g_{i_0}(\alpha)\rangle$ para um único $i_0 \in \{1, \ldots, s\}$. Assim, a parte 1 é simplesmente a proposição 2.5.1 com a terminologia da definição 2.4.1. De fato, quando $f'(\alpha) \notin M$, a parte 1 da proposição 2.5.1 mostra que $e_{i_0} = 1$ e a parte 3 mostra que $(C_f)_M$ é um domínio de ideais principais e que $e_{M/P} = 1$.*

Parte 2: Quando C_f é um domínio de Dedekind, a proposição 2.3.1 implica que $e_{M/P} = e_{i_0}$. Portanto, a afirmação que M é não ramificada se, e somente se, $f'(\alpha) \notin M$ segue da proposição 2.5.1. ■

Por fim, apresentaremos um resultado muito útil. Sejam k um corpo, $K|k(x)$ uma extensão finita e A um domínio de Dedekind com corpo de frações K. Assuma que $k \subseteq A$. Se $E|k$ é uma extensão finita, então $EK|K$ é também uma extensão finita. Denote o fecho integral de A em EK por B.

Proposição 2.5.2 *Sejam $E|k$ uma extensão finita e separável de corpos e $\alpha \in E$ tal que $E = k(\alpha)$. Então, $B = A[\alpha]$ e a extensão $B|A$ é não ramificada.*

Demonstração: *Lembre-se que a existência de α é garantida pelo teorema do elemento primitivo. Sejam $f = \min_K(\alpha) \in K[y]$ e $g = \min_k(\alpha) \in k[y]$. Uma vez que $g(\alpha) = 0$ e $k \subseteq A$, concluímos $\alpha \in B$ e portanto $A[\alpha] \subseteq B$. Claramente, $f|g$ em $K[y]$, escreva $g = fh$. Então $g'(\alpha) = f'(\alpha)h(\alpha) + f(\alpha)h'(\alpha)$. Como a extensão $E|k$ é separável, $g'(\alpha) \neq 0$ em*

$k(\alpha)$. Assim, uma vez que $k(\alpha)$ é um subcorpo de B, $f'(\alpha)$ é inversível em B e nenhum ideal maximal de B contém $f'(\alpha)$. Portanto, pela proposição 2.5.1, $A[\alpha] = B$ e $B|A$ é não ramificada. ■

2.6 Extensões de Galois

Seja A um domínio de Dedekind com corpo de frações K. Nesta seção estudaremos a fatoração dos ideais primos de A no fecho integral B de A numa extensão de Galois $L|K$. A hipótese adicional que $L|K$ é Galois nos permite, como veremos na proposição seguinte, obter mais informações a fatoração do ideal PB em B, onde $P \in \mathrm{Max}(A)$.

Seja $L|K$ um extensão de Galois finita com grupo de Galois $G = \mathrm{Gal}(L|K)$. Vimos na proposição 1.1.3 que $\sigma(B) = B$, para todo $\sigma \in G$. Considere a aplicação natural:

$$\pi : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A),$$

associada a extensão $B|A$. Seja $P \in \mathrm{Spec}(A)$, sabemos que $\pi^{-1}(P)$ é finito (veja 2.1.1), digamos $\{M_1, \ldots, M_s\}$, uma vez que $\sigma(P) = P$, concluímos que $\sigma(M_i) \in \pi^{-1}(P)$.

Proposição 2.6.1 *Seja $P \in \mathrm{Max}(A)$. Sejam M_i e M_j dois ideais maximais distintos em $\pi^{-1}(P)$. Então existe $\sigma \in G$ tal que $\sigma(M_i) = M_j$. Além disso, $e_{M_1/P} = \cdots = e_{M_s/P} = e$ e $f_{M_1/P} = \cdots = f_{M_s/P} = f$. Em particular, $PB = (M_1 \cdots M_s)^e$ e $[L : K] = efs$.*

Demonstração: *Suponha por absurdo que existam dois ideais maximais M_i e M_j em $\pi^{-1}(P)$ tal que $\sigma(M_i) \neq M_j, \forall \sigma \in G$. Sem perda de generalidade, podemos assumir que $\sigma(M_1) \neq M_s, \forall \sigma \in G$. Os ideais maximais no conjunto $\{\sigma(M_1) | \sigma \in G\} \sqcup \{M_s\}$ são dois a dois coprimos. Portanto, o teorema do resto Chinês implica que $\exists x \in B$ tal que $x \equiv 1 \mathrm{mod} \sigma(M_1), \forall \sigma \in G$, e $x \equiv 0 \mathrm{mod} M_s$. Seja $y := \prod_{\sigma \in G} \sigma(x)$. Claramente, $y \in B \cap K = A$. Afirmamos que $y \notin M_1$. De fato, se $y = \prod_{\sigma \in G} \sigma(x) \in M_1$, então existe $\sigma \in G$ tal que $\sigma(x) \in M_1$, ou equivalentemente que $x \in \sigma^{-1}(M_1)$ o que é contradição uma vez que $x \equiv 1 \mathrm{mod} \sigma(M_1)$. Portanto $y \notin M_1$ e assim, $y \notin M_1 \cap A = P$. Por outro lado, $y \in M_s \cap A = P$ pois $x \in M_s$. Esta contradição sobre y completa a demonstração a primeira parte da proposição.*

Um automorfismo $\sigma : B \to B$ induz um isomorfismo $\overline{\sigma} : B/M_1 \longrightarrow B/\sigma(M_1)$ tal que $\overline{\sigma}_{|_{A/P}} = \mathrm{id}_{A/P}$. Então $f_{M_1/P} = f_{\sigma(M_1)/P}$, para todo $\sigma \in G$. Sabemos $\{\sigma(M_1) | \sigma \in G\} = \pi^{-1}(P)$, então $f_{M_i/P} = f_{\sigma(M_1)/P}, \forall i = 1, \ldots, s$. Pela definição de índice de ramificação $PB = M_1^{e_{M_1/P}} \cdots M_s^{e_{M_s/P}}$. Portanto, para todo $\sigma \in G$,

$$\sigma(PB) = PB = \sigma(M_1)^{e_{M_1/P}} \cdots \sigma(M_s)^{e_{M_s/P}} = \sigma(M_1)^{e_{\sigma(M_1)/P}} \cdots \sigma(M_s)^{e_{\sigma(M_s)/P}}.$$

Da unicidade da fatoração, concluímos $e_{M_1/P} = e_{\sigma(M_1)/P}, \forall \sigma \in G$. *Uma vez que* $\{\sigma(M_1)|\sigma \in G\} = \pi^{-1}(P)$, $e_{M_1/P} = e_{M_i/P}, \forall i = 1, \ldots, s$. ■

Observação 2.6.1 *Seja* $L|K$ *uma extensão de Galois. Sejam* A *e* B *anéis tais que* K *é o corpo de frações de* A *e* B *é o fecho integral de* A *em* L. *Tome* $G = \mathrm{Gal}(L|K)$. *Existe uma ação natural de* G *sobre* $\mathrm{Max}(B)$ *dada por* $\sigma \cdot M = \sigma(M)$. *Sejam* $M \in \mathrm{Max}$ *e* $P = M \cap A$. *O* estabilizador *de* M *é* $D_{M/P} := \{\sigma \in G|\sigma(M) = M\}$. *É fácil verificar que* $D_{M/P}$ *é um grupo, chamado de* grupo de decomposição *de* M. *A proposição 2.6.1 afirma que a ação de* G *em* $\pi^{-1}(P)$ *é transitiva. Assim, se* $\pi^{-1}(P) = \{M_1, \ldots, M_s\}$, *então*

$$|G/D_{M/P}| = |\textit{órbita de } M| = s.$$

Em particular, $|D_{M/P}| = e_{M/P}f_{M/P}$. *Pela transitividade da ação de* G *em* $\{M_1, \ldots, M_s\}$

$$\prod_{\sigma \in G} \sigma(M) = (M_1 \cdots M_s)^{|D_{M/P}|} = PB^{f_{M/P}}.$$

Cada automorfismo $\sigma : B \to B, \sigma \in D_{M/P}$ *induz uma aplicação natural*

$$\overline{\sigma} : B/M \longrightarrow B/\sigma(M) = B/M,$$

cuja $\overline{\sigma}_{|_{A/P}} = \mathrm{id}_{A/P}$. *Seja* $\mathfrak{G}$ *o grupo de Galois de* B/M *sobre* A/P. *A aplicação* $D_{M/P} \to \mathfrak{G}$, $\sigma \mapsto \overline{\sigma}$, *é um homomorfismo de grupos cujo núcleo é* $I_{M/P} := \{\sigma \in D_{M/P}|\forall b \in B, \sigma(b) \equiv b(\mathrm{mod}M)\}$. *Este grupo é chamado de* grupo de inércia *de* M. *Observamos que,*

$$|D_{M/P}/I_{M/P}| \leqslant |\mathfrak{G}| \leqslant [B/M : A/P] = f_{M/P}.$$

O seguinte lema mostra que quando B/M *é separável sobre* A/P, *então*

$$|D_{M/P}/I_{M/P}| = f_{M/P},$$

ou, equivalentemente, que a aplicação $D_{M/P} \to \mathfrak{G}$ *é sobrejetiva. Disso segue que* $|I_{M/P}| = e_{M/P}$, *uma vez que*

$$|I_{M/P}| \cdot |D_{M/P}/I_{M/P}| \cdot |G/D_{M/P}| = |G| = e_{M/P} \cdot f_{M/P} \cdot s.$$

Lema 2.6.1 *Se a extensão* B/M *de* A/P *for separável, então é de Galois de grau* $f_{M/P}$ *e a aplicação* $D_{M/P} \to \mathfrak{G}$ *é sobrejetiva. Além disso,* M *é ramificado sobre* A *se, e só se,* $I_{M/P} \neq \{\mathrm{id}\}$.

Demonstração: *Uma vez que* B/M *é separável sobre* A/P, *toma* $\overline{\alpha} \in B/M$ *tal que* $B/M = (A/P)(\overline{\alpha})$. *Sejam* $\alpha \in B$ *tal que* $\overline{\alpha} \equiv \alpha \mathrm{mod}(M)$, $f(y) := \mathrm{min}_A\alpha \in A[y]$ *e*

$g(y) = \min_{A/P}\overline{\alpha} \in (A/P)[y]$. Desde que f se fatora completamente em $B[y]$, g se fatora completamente em $(B/M)[y]$. Então B/M é Galois sobre A/P. O teorema 2.1.2 mostra que podemos escolher escolher α tal que $\alpha \in \sigma(M), \forall\sigma \notin D_{M/P}$. Por, $f(y) = \prod_{\sigma\in H}(y - \sigma(\alpha))$ para algum $H \subseteq G$, somente as raízes não nulas mod$M$ *são os elementos de* $\sigma(\alpha)$ mod$P$, *com* $\sigma \in D_{M/P}$. *Assim, os elementos* $\overline{\sigma}(\overline{\alpha})$, $\sigma \in D_{M/P}$, *são exatamente as raízes do polinômio g. Como um isomorfismo de $(A/P)(\overline{\alpha})$ sobre A/P é unicamente determinado pela imagem de $\overline{\alpha}$, a aplicação $D_{M/P} \to \mathfrak{G}$ é sobrejetiva e $|I_{M/P}| = e_{M/P}$. Então, M é ramificado sobre P se, e somente se, $I_{M/P} \neq \{id\}$, como desejado.* ■

Vamos assumir para o restante desta seção que a extensão de corpos residuais B/M sobre A/P é separável. Quando $I_{M/P} = D_{M/P} = \{\text{id}\}$, $PB = M_1 \cdots M_{[L:K]}$ e o ideal primo P é dito *completamente decomposto* em B. Quando $I_{M/P} = D_{M/P} = G$, $PB = M^{[L:K]}$ e o ideal primo P é dito *totalmente ramificado* em B. Quando $I_{M/P} = \{\text{id}\}$ e $D_{M/P} = G$, PB é um ideal primo de B e o ideal primo P é dito *inerte* em B.

Agora seja K' um extensão intermediária entre K e L. Então $K' = L^H$ para algum H subgrupo de G. Seja $P' = M \cap B^H$, onde B^H é o fecho integral de A em K'. Sejam $e' = e_{M/P'}$, $f' = f_{M/P'}$, $s' = [L : K']/e'f'$ e analogamente $e = e_{M/P}$, $f = f_{M/P}$, $s = [L : K]/ef$. Sejam D, D' os grupos $D_{M/P}, D_{M/P'}$ e I, I' os grupos $I_{M/P}, I_{M/P'}$ respectivamente.

Segue imediatamente da definição que $D' = D \cap H$ e que $I' = I \cap H$. Em particular, se $H = D$, então $D' = \text{Gal}(L|K')$, com $|D'| = e'f'$. Neste caso $s' = 1$, de modo que M é o único primo de B além de $M \cap B^D$. Se $H = I$, então $I' = \text{Gal}(L|K')$, com $|I'| = e'$. Portanto, neste caso o ideal primo $M \cap B^I$ se ramifica totalmente em B, com índice de ramificação e, além disso o ideal primo $M \cap B^D$ é inerte em B^I.

Proposição 2.6.2 *Com as notações e hipóteses introduzidas acima,*

1. *L^I é o maior corpo intermediário K' tal que $e_{P'/P} = 1$.*
2. *L^D é o maior corpo intermediário K' tal que $e_{P'/P} = f_{P'/P} = 1$.*
3. *L^I é o menor corpo intermediário K' tal que M é totalmente ramificado sobre P'.*
4. *L^D é o menor corpo intermediário K' tal que M é o único primo de B tal que $M \cap A = P'$.*

Demonstração: *Lembre que se H e H' são dois subgrupos de G, então $L^H L^{H'} = L^{H\cap H'}$. Assim, $L^{D'} = L^D K'$ e $L^{I'} = L^I K'$. Agora, considere o seguinte diagrama de corpos*

$$\begin{array}{ccccccc} K' & \xrightarrow{s'} & K'L^D & \xrightarrow{f'} & K'L^I & \xrightarrow{e'} & L \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ K & \xrightarrow{s} & L^D & \xrightarrow{f} & L^I & \xrightarrow{e} & L \end{array}$$

1-Suponha que $e_{P'/P} = 1$. Então pela multiplicidade de índice de ramificação, $e = e'$. Como $L^I \subseteq L^I K'$, concluímos $L^I = L^I K'$ e assim $K' \subseteq L^I$.

2- Se na extensão $K'|K$, $e_{P'/P} = f_{P'/P} = 1$ pela multiplicidade do índice de ramificação e do grau residual, $e = e'$ e $f = f'$. Do diagrama anterior $L^D = L^D K'$ e assim $K' \subseteq L^D$.

3- Se M é totalmente ramificado sobre P', então $[L : K'] = e'$. Segue do diagrama que $K' = L^I K'$, tal que $L^I \subseteq K'$.

4- Se M é o único primo sobre P', então $H = \mathrm{Gal}(L|K') = D'$. Como $D' = D \cap H$, segue $H \subseteq D$, tal que $L^D \subseteq K'$. ■

Corolário 2.6.1 *Sejam $L|K$ e $L'|K$ extensões separáveis contidas no fecho algébrico $\overline{K}$ de K. Seja $\mathcal{O}_K$ um domínio de Dedekind cujo corpo de frações K. Sejam $\mathcal{O}_L, \mathcal{O}_{L'}$ e $\mathcal{O}_{LL'}$ os fechos integrais de $\mathcal{O}_K$ em L, L' e LL' respectivamente. Seja $P \in \mathrm{Max}(\mathcal{O}_K)$ e suponha que o corpo $\mathcal{O}_K/P$ é perfeito. Então P ramifica em $\mathcal{O}_{LL'}$ se, e somente se, P ramifica em $\mathcal{O}_L$ ou $\mathcal{O}_{L'}$.*

Demonstração: *Vamos assumir que P não se ramifica em $\mathcal{O}_L$ e $\mathcal{O}_{L'}$. Sejam N uma extensão de Galois em $\overline{K}$ que contenha L e L' e $\mathcal{O}_N$ o fecho integral de $\mathcal{O}_K$ em N. Seja $\mathfrak{P} \in \mathrm{Max}(\mathcal{O}_N)$ tal que $\mathfrak{P} \cap \mathcal{O}_K = P$. Pela proposição 2.6.2, $L, L' \subseteq N^{I(\mathfrak{P}'/P)}$, uma vez que os primos $\mathfrak{P} \cap \mathcal{O}_L$ e $\mathfrak{P} \cap \mathcal{O}_{L'}$ não são ramificado sobre P. Assim, $LL' \subseteq N^{I(\mathfrak{P}'/P)}$ e pela multiplicidade do índice de ramificação, P não se ramifica em $\mathcal{O}_{LL'}$.*

Reciprocamente, se P não se ramifica em $\mathcal{O}_{LL'}$, então pela multiplicidade do índice de ramificação, P não se ramifica em $\mathcal{O}_L$ e $\mathcal{O}_{L'}$. ■

Definição 2.6.1 *Suponha que A/P é um corpo finito de ordem $q = p^n$. Então B/M é Galois sobre A/P, com gerador canônico para seu grupo de Galois dado por:*

$$\begin{array}{rccc} \varphi: & B/M & \longrightarrow & B/M \\ & x & \longmapsto & x^q. \end{array}$$

Quando M é não ramificado sobre A, denotamos por $\mathrm{Frob}(M)$ *o único elemento de $D_{M/P}$ que a aplicação φ restringe a aplicação $D_{M/P} \to \mathfrak{G}$. O elemento* $\mathrm{Frob}(M)$ *é chamando de* substituição Frobenius *de M. Ele é o único elemento de G tal que*

$$\forall b \in B, \mathrm{Frob}(M)(B) \equiv b^q \mathrm{mod}(M).$$

2.7 Cobertura de Galois

Nesta seção veremos a teoria de Galois no contexto de curvas. Sejam $f \in \overline{k}[x, y]$ um polinômio irredutível e $Z_f(\overline{k})$ a curva plana associada. Seja $\overline{C}_f = \overline{k}[x, y]/\langle f \rangle$ seu anel

de funções e denote por $L = \overline{k}(Z_f)$ o corpo de frações de $\overline{C}_f$. Seja $\sigma : \overline{C}_f \to \overline{C}_f$ um automorfismo de $\overline{k}-$álgebras. Este automorfismo pode ser estendido unicamente a um automorfismo de L. Agora, seja G um grupo finito de automorfismos de $\overline{k}-$álgebras de $\overline{C}_f$ e, assim, de L. Tome

$$K := L^G = \{y \in L | \sigma(y) = y, \forall \sigma \in G\}.$$

Da teoria de Galois, segue que a extensão $L|K$ é Galois de grau $|G|$, com G o grupo de Galois. Seja,

$$A := (\overline{C}_f)^G = \{b \in C_f | \sigma(b) = b, \forall \sigma \in G\} = \overline{C}_f \cap K.$$

O conjunto $(\overline{C}_f)^G$ é o anel chamado *anel de invariantes* de C_f sob a ação de G. Nosso objetivo nesta seção é interpretar geométricamente o anel $(\overline{C}_f)^G$ como o anel de funções num quociente da curva $Z_f(\overline{k})$ por uma ação de G associada. Nesta interpretação a extensão $\overline{C}_f|(\overline{C}_f)^G$ seria correspondente a aplicação $Z_f(\overline{k}) \to Z_f(\overline{k})/G$.

Definição 2.7.1 *Sejam $f, g \in \overline{k}[x, y]$ e $\varphi : Z_f(\overline{k}) \to Z_g(\overline{k})$ uma aplicação. Esta aplicação é unicamente determinada pelas aplicações $\varphi_1, \varphi_2 : Z_f(\overline{k}) \to \overline{k}$ tais que $\varphi(a, b) = (\varphi_1(a, b), \varphi_2(a, b)) \in Z_g(\overline{k})$. A aplicação φ é um* morfismo de curvas planas afins *se existem $\gamma_1, \gamma_2 \in \overline{k}[x, y]$ tais que $\varphi_1(a, b) = \gamma_1(a, b)$ e $\varphi_2(a, b) = \gamma_2(a, b), \forall (a, b) \in Z_f(\overline{k})$.*

Observação 2.7.1 *Seja $\varphi^* : \overline{C}_g \to \overline{C}_f$ um homomorfismo de $\overline{k}-$álgebras. Observamos que φ^* induz um morfismo natural entre as curvas. Seja $\varphi_x \in \overline{k}[x, y]$ cuja classe em $\overline{C}_f$ é φ^*(classe de x). Analogamente considere $\varphi_y \in \overline{k}[x, y]$. Assim,*

$$\begin{array}{rccc} \varphi : & Z_f(\overline{k}) & \longrightarrow & Z_g(\overline{k}) \\ & (a, b) & \longmapsto & (\varphi_x(a, b), \varphi_y(a, b)) \end{array}$$

está bem definida, é um morfismo de curvas como na definição 2.7.1 e não depende da escolha de φ_x, φ_y. De fato, uma vez que g(classe de x, classe de y) $= 0$ em C_g, então em C_f :

$$\begin{array}{rcl} g(\text{classe de } \varphi_x(x, y), \text{ classe de } \varphi_y(x, y)) & = & g(\varphi^*(\text{classe de } x), \varphi^*(\text{classe de } y)) \\ & = & \varphi^*(g(\text{classe de } x, \text{ classe de } y)) \\ & = & \varphi^*(0) = 0. \end{array}$$

Logo $f | g(\varphi_x(x, y), \varphi_y(x, y))$. Assim, para todo $(a, b) \in Z_f(\overline{k}), g(\varphi_x(a, b), \varphi_y(a, b)) = 0$ e portanto $(\varphi_x(a, b), \varphi_y(a, b)) \in Z_g(\overline{k})$.

Em particular, dado um homomorfismo $\sigma : \overline{C}_f \to \overline{C}_f$, existe um morfismo de curvas

$$\begin{array}{rccc} \sigma_{Z_f(\overline{k})} : & Z_f(\overline{k}) & \longrightarrow & Z_f(\overline{k}) \\ & (a,b) & \longmapsto & (\sigma_x(a,b), \sigma_y(a,b)), \end{array}$$

onde σ_x, σ_y são polinômios em $\overline{k}[x,y]$ tal que as classes de $\sigma_x(x,y)$ e $\sigma_y(x,y)$ em $\overline{C}_f$ são σ(classe de x) e σ(classe de y) respectivamente. Note, no entanto, que a aplicação $\sigma \to \sigma_{Z_f(\overline{k})}$ não é um homomorfismo $G \to \mathrm{Aut}(Z_f(\overline{k}))$.

Observamos que existem ações naturais de G sobre $\overline{C}_f$ e $Z_f(\overline{k})$ definidas a seguir:

$$\begin{array}{ccc} G \times \overline{C}_f & \longrightarrow & \overline{C}_f \\ (\sigma, f) & \longmapsto & \sigma \cdot f := \sigma(f), \end{array}$$

e

$$\begin{array}{ccc} Z_f(\overline{k}) \times G & \longrightarrow & Z_f(\overline{k}) \\ (z, \sigma) & \longmapsto & z^\sigma := \sigma_{Z_f(\overline{k})}(z). \end{array}$$

Em geral dados um espaço topológico Z e uma grupo G de homeomorfismo de Z, há uma ação natural de G sobre Z :

$$\begin{array}{ccc} G \times Z & \longrightarrow & Z \\ (\sigma, z) & \longmapsto & \sigma(z). \end{array}$$

Portanto existe o espaço quociente:

$$Z/G := \{\text{conjunto das órbitas de } Z \text{ sob a ação de } G\}.$$

Que por sua vez é um espaço topológico munido da topologia quociente, ou seja, a topologia mais fina no conjunto Z/G que torna a aplicação quociente $\pi : Z \to Z/G$ contínua. A aplicação $\pi : Z \to Z/G$ é chamada uma *cobertura de Galois* de Z/G.

Seja F um corpo munido de uma topologia. A ação do grupo G em Z induz uma ação do grupo G no anel $C(Z,F)$ das funções contínuas de Z em F,

$$\begin{array}{ccc} C(Z,F) \times G & \longrightarrow & C(Z,F) \\ (f, \sigma) & \longmapsto & f^\sigma : = f \circ \sigma. \end{array}$$

Considere o anel das funções invariantes, ou seja,

$$C(Z,F)^G := \{f \in C(Z,F) | f^\sigma = f, \forall \sigma \in G\}.$$

A função $f : Z \to F$ pertence a $C(Z,F)^G$ se, e só se, $f(z) = f(x)$ para todo $x \in Z$ e todo $z \in Z$ que pertence a órbita de x sobre a ação de G. O anel $C(Z,F)^G$ pode ser

considerado como um anel de funções contínuas no conjunto de órbitas de G, isto é, no espaço quociente Z/G. De fato, se $g \in C(Z,F)^G$ então g define uma aplicação contínua entre os espaços topológicos Z/G e F. Ainda, $C(Z/G,F) = C(Z,F)^G$.

A seguir estudaremos um caso particular das observações anteriores, mais precisamente a ação de um grupo finito G de morfismos de uma curva $Z_f(\overline{k})$ sobre ela mesma. Considere $Z_f(\overline{k})$ com a topologia de Zariski e o quociente $Z_f(\overline{k})/G$ com a topologia quociente. Como G é um grupo finito, as órbitas de G são conjuntos finitos, segue disso que um subconjunto não trivial do quociente $Z_f(\overline{k})/G$ é fechado para a topologia quociente se, e só se, é um conjunto finito.

É natural, pensarmos se o novo espaço topológico $Z_f(\overline{k})/G$ pode ser identificado de alguma forma com uma curva plana afim. Para que isso ocorra, o quociente $Z_f(\overline{k})/G$ deveria ser homeomorfo a alguma curva plana $Z_g(\overline{k})$ dado por um homeomorfismo $\rho : Z_f(\overline{k})/G \to Z_g(\overline{k})$ tal que a composição $\rho \circ \pi : Z_f(\overline{k}) \to Z_g(\overline{k})$ seja um morfismo entre curvas planas. Em outras palavras, para tanto, a aplicação $\varphi = \rho \circ \pi$ deve ser induzida por um homomorfismo de $\overline{k}-$álgebras $\varphi^* : \overline{C}_g \to \overline{C}_f$, neste caso podemos dizer que a aplicação ρ "coloca"uma estrutura de curva plana no espaço $Z_f(\overline{k})/G$.

Vamos assumir que o homeomorfismo ρ exista. Neste caso, usando ρ podemos identificar as funções de $Z_g(\overline{k})$ com as funções de $Z_f(\overline{k})/G$. O anel das funções algébricas de $Z_f(\overline{k})$ é $\overline{C}_f$. O caso topológico citado acima sugere que a anel de funções do quociente $Z_f(\overline{k})/G$ deve ser o anel de invariantes C_f^G. Assim, a fim de colocar um estrutura de curva plana no quociente $Z_f(\overline{k})/G$, nossa discussão sugere que identifiquemos $\overline{C}_f^G$ com um anel de funções $\overline{C}_g$ de alguma curva plana $Z_g(\overline{k})$.

Proposição 2.7.1 *Sejam $Z_f(\overline{k})$ uma curva não singular e G um grupo finito de $\overline{k}-$automorfismos (como álgebra) de $\overline{C}_f$. Suponha que $\overline{C}_f^G$ seja um domínio de Dedekind. Se existe um polinômio $g \in \overline{k}[u,v]$ tal que $\overline{C}_g := \overline{k}[u,v]/\langle g\rangle \cong C_f^G$ (como $\overline{k}-$álgebra), então a aplicação quociente $\pi : Z_f(\overline{k}) \to Z_f(\overline{k})/G$ pode ser identificada com o morfismo de curvas $Z_f(\overline{k}) \to Z_g(\overline{k})$ induzido pelo $\overline{k}-$álgebra isomorfismo $\overline{C}_g \cong C_f^G \subseteq \overline{C}_f$. Mais precisamente, existe um homeomorfismo $\rho : Z_f(\overline{k})/G \to Z_g(\overline{k})$ tal que a composição $\rho \circ \pi$ é igual ao morfismo de curvas induzido pela aplicação $\overline{C}_g \to \overline{C}_f$.*

Para provar a proposição anterior, basta adaptar a proposição 2.6.1 para o contexto de ação de grupos em espaços topológicos e quocientes. Como esse não é o foco deste trabalho, para mais detalhes veja [6], página 122.

Encerramos está seção com o seguinte exemplo:

Exemplo 2.7.1 *Seja k um corpo de característica diferente de dois. Seja $f(x,y) = y^2 - g(x) \in \overline{k}[x,y]$ um polinômio irredutível. Suponha $g \in \overline{k}[x]$ livre de quadrados e assim*

a curva $Z_f(\overline{k})$ *é não singular. Sejam* $\overline{C}_f := \overline{k}[x,y]/\langle f\rangle$ *e* $L = \overline{k}(Z_f) = Cf(\overline{C}_f)$. *Considere o automorfismo de* $\overline{k}-$*álgebras*

$$\sigma : \overline{C}_f \longrightarrow \overline{C}_f,$$

dado por $x \mapsto x$ *e* $y \mapsto -y$. *A aplicação* σ *claramente tem ordem dois e se estende para uma involução de* L. *Seja* $G = \{\mathrm{id}, \sigma\}$. *O grau de* $L|L^G$ *é dois. Afirmamos que* $L^G = \overline{k}(x)$ *e que* $C_f^G = \overline{k}[x]$. *De fato,* $\overline{k}(x) \subseteq L^G$, $L \cong \overline{k}(x)(\sqrt{g(x)})$, *então* $[L : \overline{k}(x)] = 2$ *e assim,* $L^G = \overline{k}(x)$. *Para mostrar que* $C_f^G = \overline{k}[x]$, *observe que* $\{1, y\}$ *é uma base para* $\overline{C}_f$ *sobre* $\overline{k}[x]$ *e, é fácil de ver que os únicos elementos de* $\overline{C}_f$ *fixados pela ação de* σ *são os elementos de* $\overline{k}[x]$.

O automorfismo σ *induz o morfismo de curvas,*

$$\sigma_{Z_f(\overline{k})} : Z_f(\overline{k}) \longrightarrow Z_f(\overline{k})$$

com $(a,b) \mapsto (a,-b)$. *O morfismo* $\sigma_{Z_f(\overline{k})}$ *é usualmente referido como* involução hiperelítica *de* $Z_f(\overline{k})$.

Capítulo

3

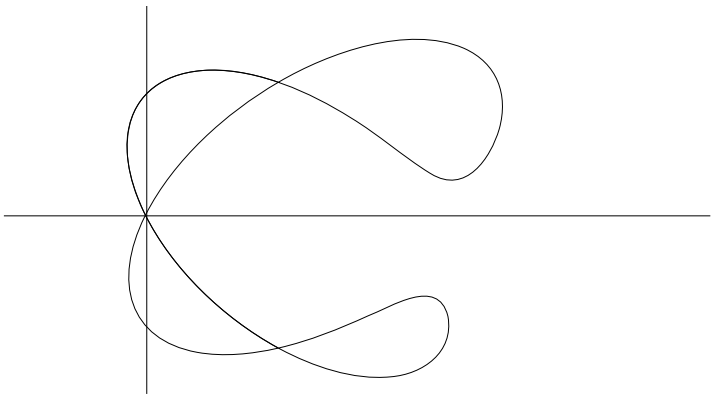
Discriminantes

Sejam A um domínio de Dedekind, K seu corpo de frações, $L|K$ uma extensão separável e B o fecho integral de A em L. Nosso objetivo neste capítulo é caracterizar os ideais $P \in \mathrm{Max}(A)$ que se ramificam em B. Para isso usaremos *os discriminantes.*

Primeiramente investigaremos quando os ideais maximais de A se ramificam numa extensão simples $B := A[\alpha]$. Neste caso, já obtivemos a descrição dos maximais de B que são ramificados sobre A. De fato, usando o corolário 2.5.1, os maximais de B que são ramificados sobre A são exatamente os que contém $f'(\alpha)$, onde $f = \min_A(\alpha)$. Mostraremos na proposição 3.0.2 que podemos caracterizar os ideais primos de A que se ramificam em B usando o discriminante de f.

Antes de tratar o caso geral onde A é um domínio de Dedekind, estudaremos o caso particular em que $A = \overline{k}[x]$ $B = \overline{C}_f = \overline{k}[x,y]/\langle f\rangle$. Onde $f \in \overline{k}[x,y]$ irredutível, mônico em y e $n := \deg_y(f) > 0$, isto garante que a aplicação natural $A \to \overline{C}_f$ é injetora. Considere a primeira projeção $\pi : Z_f(\overline{k}) \longrightarrow \mathbb{A}^1(\overline{k})$

Dado $a \in \overline{k}$, a fibra $\pi^{-1}(a)$ contém exatamente n pontos distintos se, e só se, $\partial f/\partial y(a,b) \neq 0$ para todos os pontos $(a,b) \in \pi^{-1}(a)$. Quando $\partial f/\partial y(a,b) = 0$, o ponto (a,b) é um ponto singular de $Z_f(\overline{k})$ ou a reta tangente a $Z_f(\overline{k})$ em (a,b) é vertical. Estas duas possibilidades ocorrem na seguinte curva que é uma quártica trinodal:



Suponha $\overline{C}_f$ é um domínio de Dedekind, equivalentemente, $Z_f(\overline{k})$ é uma curva suave. Neste caso $\overline{C}_f = A[\alpha]$, onde α é a classe de y em $\overline{C}_f$. Os pontos de ramificação da aplicação π são exatamente os pontos do conjunto $Z_f(\overline{k}) \cap Z_{\partial f/\partial y}(\overline{k})$. O conjunto dos pontos $a \in \mathbb{A}^1(\overline{k})$ tal que $\pi^{-1}(a)$ contém menos de n pontos (i.é, o conjunto dos pontos de ramos da aplicação π) é igual ao conjunto $\pi(Z_f(\overline{k}) \cap Z_{\partial f/\partial y}(\overline{k}))$.

Sejam $f(x,y) = a_n(x)y^n + \cdots + a_0(x)$ e $g(x,y) = b_m(x)y^m + \cdots + b_0(x)$ dois polinômios coprimos em $\overline{k}[x,y]$. Existe um polinômio (veja [6], pág. 41) $\mathrm{Res}_y(f,g)(x) \in \overline{k}[x]$ chamado *resultante* de f e g com respeito a variável y, que satisfaz a seguinte propriedade:

Fato 3.0.1 *Suponha $a_n(x) = 1$. Então $a \in \overline{k}$, então $\mathrm{Res}_y(f,g)(a) = 0$ se, e somente se, existe $b \in \overline{k}$ tal que $(a,b) \in Z_f(\overline{k}) \cap Z_g(\overline{k})$.*

No caso em que $a_n(x) = 1$ e $g(x,y) = \partial f/\partial y(x,y)$, o resultante $\mathrm{Res}_y(f, \partial f/\partial y)(x)$ é chamado o *discriminante* de $f(x,y)$ e denotaremos por $\mathrm{disc}(f)(x)$. Segue do fato 3.0.1 que a é um ponto de ramo de π se, e somente se, $\mathrm{disc}(f)(a) = 0$. Usando a correspondência entre pontos de uma curva e ideais maximais de seu anel de funções, podemos traduzir algebricamente a propriedade geométrica do discriminante:

Seja $P \in \mathrm{Max}(A)$. Então P ramifica em $\overline{C}_f$ se, e só se, $\mathrm{disc}(f) \in P$.

A próxima proposição mostra que o discriminante pode ser usado em situações mais gerais:

Proposição 3.0.2 *Sejam A um domínio de Dedekind, $f \in A[y]$ mônico e irredutível. Seja $\mathrm{disc}(f)$ o resultante de f e f'. Suponha $C_f := A[y]/\langle f \rangle$ um domínio de Dedekind. Então $P \in \mathrm{Max}(A)$ ramifica em C_f se, e somente se, $\mathrm{disc}(f) \in P$.*

Para a demonstração veja [6] página 133.

Como foi visto neste caso, disc(f) está fortemente relacionado à ramificação da extensão $A[\alpha]|A$. Uma pergunta natural é se existe alguma relação deste tipo nos casos mais gerais. O restante deste capítulo responderá positivamente esta pergunta.

3.1 Discriminante como uma Norma

Definição 3.1.1 *Sejam L um corpo e R uma $L-$álgebra de dimensão finita. Dado $r \in R$, considere $\mu_r : R \to R$, dada por $x \mapsto \mu_r(x) := rx$. Claramente μ_r é uma transformação linear de R visto como $L-$espaço vetorial. A aplicação*

$$\begin{array}{rccc} \mathrm{Norm}_{R/L}: & R & \longrightarrow & L \\ & r & \longmapsto & \det(\mu_r) \end{array}$$

é chamada da aplicação norma *de R em L. Esta aplicação é multiplicativa, isto é:*

$$\forall r, s \in R, \mathrm{Norm}_{R/L}(rs) = \mathrm{Norm}_{R/L}(r) \cdot \mathrm{Norm}_{R/L}(s).$$

A aplicação

$$\begin{array}{rccc} \mathrm{Tr}_{R/L}: & R & \longrightarrow & L \\ & r & \longmapsto & \mathrm{tr}(\mu_r) \end{array}$$

é chamada do traço *de R em L. Esta aplicação é aditiva, isto é:*

$$\forall r, s \in R, \mathrm{Tr}_{R/L}(r+s) = \mathrm{Tr}_{R/L}(r) + \mathrm{Tr}_{R/L}(s).$$

Lembre-se que norma e traço de uma transformação linear aparecem como coeficientes de seu polinômio característico, de fato, o polinômio característico de μ_r é da forma $\mathrm{char}_r(y) = y^n - \mathrm{Tr}_{R/L}(r)y^{n-1} + \cdots + (-1)^n \mathrm{Norm}_{R/L}(r)$.

Exemplo 3.1.1 *O corpo $\mathbb{Q}(i)$ é uma $\mathbb{Q}-$álgebra de dimensão dois com base $\{1, i\}$. Seja $r = a + bi \in \mathbb{Q}(i)$, na base $\{1, i\}$, a aplicação μ_r é representada pela matriz*

$$\mu_r = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Assim, $\mathrm{Norm}_{\mathbb{Q}(i)/\mathbb{Q}}(r) = a^2 + b^2 = r\overline{r}$ *e* $\mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(r) = 2a = r + \overline{r}$.

Lema 3.1.1 *Seja R uma $L-$álgebra de dimensão s. Sejam $\alpha \in R$ e $L[\alpha]$ a menor $L-$subalgebra de R que contém α. Tome $f(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_0 \in L[y]$ o polinômio minimal de α sobre L. Então $L[\alpha] \cong L[y]/\langle f \rangle$. Então R é um $L[\alpha]-$módulo R é livre de posto $[R : L[\alpha]]$ e*

1. $\mathrm{Tr}_{R/L}(\alpha) = -[R : L[\alpha]] \cdot a_{n-1} = [R : L[\alpha]] \cdot \mathrm{Tr}_{L[\alpha]/L}(\alpha)$.
2. $\mathrm{Norm}_{R/L}(\alpha) = ((-1)^n a_0)^{[R:L[\alpha]]} = (\mathrm{Norm}_{L[\alpha]/L}(\alpha))^{[R:L[\alpha]]}$.

Demonstração: *Seja* $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *uma base para* $L[\alpha]$ *sobre* L. *Seja* $\{f_1, \ldots, f_t\}$ *uma base para* R *sobre* $L[\alpha]$. *Considere a base*

$$\mathcal{B} = \{f_1, \alpha f_1, \ldots, \alpha^{n-1} f_1, \ldots, f_t, \alpha f_t, \ldots, \alpha^{n-1} f_t\}$$

para R *sobre* L. *A matriz de* μ_α *na base* $\mathcal{B}$ *é da forma*

$$\begin{pmatrix} C_\alpha & 0 & & \\ 0 & C_\alpha & 0 & \\ & 0 & \ddots & 0 \\ & & 0 & C_\alpha \end{pmatrix},$$

onde C_α *é a matriz*

$$\begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & \ddots & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ & & & 1 & -a_{n-1} \end{pmatrix}.$$

O lema segue imediatamente da representação de μ_α, *uma vez que* $\mathrm{Tr}(C_\alpha) = -a_{n-1}$ *e* $\det(C_\alpha) = (-1)^n a_0$. ■

Corolário 3.1.1 *Sejam* A *um domínio integralmente fechado no seu corpo de frações* K *e* $L|K$ *uma extensão finita. Se* $\alpha \in L$ *é integral sobre* A, *então* $\mathrm{Norm}_{L/K}(\alpha), \mathrm{Tr}_{L/K}(\alpha) \in A$.
Demonstração: *Como* L *é um* $K(\alpha)-$*espaço vetorial de dimensão* $[L : K(\alpha)]$, *podemos aplicar o lema 3.1.1. Seja* $f = \min_K(\alpha)$. *Pela hipótese* A *é integralmente fechado e pelo lema 1.1.3,* $f \in A[y]$. *Assim, este corolário segue imediatamente do lema 3.1.1.* ■

No corolário acima, a hipótese de A ser integralmente fechado é necessária. Por exemplo, dado $\alpha \in K \setminus A$ integral sobre A, $\min_K(\alpha) = y - \alpha$ e $\mathrm{Norm}_{K/K}(\alpha) = \alpha \notin A$.

Lema 3.1.2 *Seja* $L|K$ *uma extensão finita e separável de grau* s. *Sejam* $\sigma_1, \ldots, \sigma_s$ *os distintos monomorfismos de* L *em* $\overline{K}$. *Então para todo* $\alpha \in L, \mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{s} \sigma_i(\alpha)$ *e* $\mathrm{Norm}_{L/K}(\alpha) = \prod_{i=1}^{s} \sigma_i(\alpha)$.
Demonstração: *Sejam* $\alpha \in L$ *e* $f(y) = y^n + a_{n-1}y^{n-1} + a_0 = \min_K(\alpha)$. *Denote por* $\tau_1, \ldots, \tau_n$ *os monomorfismos de* $K(\alpha)$ *em* $\overline{K}$ *como sendo as restrições distintas dos*

monomorfismos $\sigma_1, \ldots, \sigma_s$. *Como* α *é separável em* L,

$$f(y) = \prod_{i=1}^{n}(y - \tau_i(\alpha)) \in \overline{K}[y],$$

com $a_{n-1} = -\sum_{i=1}^{n}\tau_i(\alpha)$ *e* $a_0 = (-1)^n \prod_{i=1}^{n}\tau_i(\alpha)$. *Para cada* $i = 1, \ldots, n$, *exatamente* $[L : K(\alpha)] = \frac{s}{n}$ *monomorfismos de* L *são iguais a* τ_i, *quando restritos a* $K(\alpha)$. *Portanto,*

1. $\sum_{j=1}^{s}\sigma_j(\alpha) = s/n\sum_{i=1}^{n}\tau_i(\alpha) = -[L : K(\alpha)]a_{n-1} = \mathrm{Tr}_{L/K}(\alpha)$.
2. $\prod_{j=1}^{s}\sigma_j(\alpha) = \prod_{i=1}^{n}\tau_i(\alpha)^{s/n} = ((-1)^n a_0)^{[L:K(\alpha)]} = \mathrm{Norm}_{L/K}(\alpha)$.

■

Teorema 3.1.1 (Transitividade do traço e da norma) *Sejam* $M|L$ *e* $L|K$ *extensões finitas. Então, para todo* $\alpha \in M$,

1. $\mathrm{Norm}_{L/K}(\mathrm{Norm}_{M/L}(\alpha)) = \mathrm{Norm}_{M/K}(\alpha)$.
2. $\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)) = \mathrm{Tr}_{M/K}(\alpha)$.

Para a demonstração veja [7], página 192.

Proposição 3.1.1 *Sejam* K *um corpo,* $f \in K[y]$ *mônico e* $L = K[y]/\langle f\rangle$. *Tome* α *a classe de* y *em* L *e* $g \in K[y]$, *então* $\mathrm{Res}(f, g) = \mathrm{Norm}_{L/K}(g(\alpha))$. *Em particular,* $\mathrm{disc}(f) = \mathrm{Norm}_{L/K}(f'(\alpha))$.

Para a demonstração veja [6], página 136.

O seguinte lema fornece algumas propriedades básicas do resultante.

Lema 3.1.3 *Sejam* A *um domínio,* $a \in A \setminus \{0\}$ *e* $f, g \in A[y]$. *Então,*

1. $\mathrm{Res}(af, g) = a^{\deg(g)}\mathrm{Res}(f, g)$.
2. $\mathrm{Res}(f, g) = (-1)^{\deg(f)\deg(g)}\mathrm{Res}(g, f)$.
3. $\mathrm{Res}(f, y - a) = (-1)^{\deg(f)}f(a)$.

   Nos próximos três itens K *é um corpo,* $f, g, h \in K[y]$ *e* $\overline{K}$ *é o fecho algébrico de* K :
4. $\mathrm{Res}(f, gh) = \mathrm{Res}(f, g)\mathrm{Res}(f, h)$.
5. *Se* $f(y) = a_n\prod_{i=1}^{n}(y - \alpha_i), g = b_m\prod_{j=1}^{m}(y - \beta_j) \in \overline{K}[y] \setminus \overline{K}$. *Então* $\mathrm{Res}(f, g) = a_n^m b_m^n \prod_{i,j}(\alpha_i - \beta_j)$.
6. *Sejam* f *mônico e* $\alpha_1, \ldots, \alpha_n$ *suas raízes, então* $\mathrm{disc}(f) = \prod_{i\neq j}(\alpha_i - \alpha_j)$.

Demonstração: *Os três primeiros itens seguem diretamente da definição. Para o item 4, escreva* $f(y) = a_n y^n + \cdots + a_0$, *pelo primeiro item,* $\mathrm{Res}(f, gh) = (a_n)^{\deg(gh)}\mathrm{Res}(f/a_n, gh)$. *Sejam* α *uma raiz de* f/a_n *e* $L = K(\alpha)$, *então*

$$\begin{aligned}\mathrm{Res}(f/a_n, gh) = \mathrm{Norm}_{L/K}(g(\alpha)h(\alpha)) &= \mathrm{Norm}_{L/K}(g(\alpha))\mathrm{Norm}_{L/K}(h(\alpha)) \\ &= \mathrm{Res}(f/a_n, g)\mathrm{Res}(f/a_n, h).\end{aligned}$$

Para o item 5, utilizando os itens 4 e depois 3,

$$\begin{aligned}\mathrm{Res}(f, g) =& \mathrm{Res}(f, b_m) \cdot \prod_{j=1}^{m} \mathrm{Res}(f, y - \beta_j) \\ =& (b_m)^n \prod_{j=1}^{m} (-1)^n f(\beta_j) \\ =& (-1)^{mn} (a_n)^m (b_m)^n \prod_{i=1}^{n}\prod_{j=1}^{m} (\beta_j - \alpha_i) \\ =& (a_n)^m (b_m)^n \prod_{i,j} (\alpha_i - \beta_j).\end{aligned}$$

Para o último, se $f' = 0$, *então por definição* $\mathrm{disc}(f) = \mathrm{Res}(f, f') = 0$. *Por outro lado como* f *não é constante, isto só acontece quando* $\mathrm{char}(K) = p > 0$. *Neste caso,* $f(y) = h(y)^p$, *para algum* $h \in \overline{K}[y]$ *e portanto* $\alpha_i = \alpha_j$ *para* $i \neq j$, *o que implica* $\prod_{i \neq j}(\alpha_i - \alpha_j) = 0$. *Suponha agora* $f' \neq 0$ *e tome* $m = \deg(f')$. *Então,*

$$\begin{aligned}\mathrm{Res}(f, f') &= (-1)^{mn}\mathrm{Res}(f', f) &&= (-1)^{mn}\textstyle\prod_{i=1}^{n} f'(\alpha_i) \\ &= \textstyle\prod_{i=1}^{n}\left(\prod_{j \neq i}(\alpha_i - \alpha_j)\right) &&= \textstyle\prod_{i \neq j}(\alpha_i - \alpha_j).\end{aligned}$$

Observação 3.1.1 *Seja* A *um domínio com corpo de frações* K. *O lema 3.1.3 mostra que,* $\mathrm{Res}(f, g) = 0$ *se, e só se,* f *e* g *possuem raiz em comum.*

3.2 Discriminante de uma Base

Definição 3.2.1 *Seja* R *uma* $L-$*álgebra de dimensão finita. Defina*

$$\begin{aligned}\mathrm{Tr} : R \times R &\longrightarrow L \\ (x, y) &\longmapsto \mathrm{Tr}_{R/L}(xy).\end{aligned}$$

Observe que Tr *é um forma $L-$bilinear, chamada da* forma do traço. *Sejam $e_1, \ldots, e_n$ elementos de uma base para R sobre L. Considere*

$$T_{\{e_1,\ldots,e_n\}} := (\mathrm{Tr}_{R/L}(e_i e_j))_{1\leqslant i,j\leqslant n}$$

como a matriz da forma Tr *na base $\{e_1, \ldots, e_n\}$. Sejam $\{f_1, \ldots, f_n\}$ outra base e C a matriz mudança de base de $\{f_1, \ldots, f_n\}$ para $\{e_1, \ldots, e_n\}$. Tome C^t a transposta de C. Então*

$$T_{\{f_1,\ldots,f_n\}} = C^t T_{\{e_1,\ldots,e_n\}} C.$$

Em particular, $\det(T_{\{f_1,\ldots,f_n\}})$ *e* $\det(T_{\{e_1,\ldots,e_n\}})$ *diferem somente por um quadrado em L, a saber,* $(\det C)^2$ *que é não nulo. Assim,* $\det(T_{\{f_1,\ldots,f_n\}}) = 0$ *se, e só se,* $\det(T_{\{e_1,\ldots,e_n\}}) = 0$.

Denotaremos por $(L^*)^2$ o subgrupo dos quadrados em L^*, observe que o conjunto dos quadrados em L não é um subgrupo do grupo aditivo de L, a menos que $\mathrm{char}(L) = 2$.

Definição 3.2.2 *O* discriminante *de* Tr *é zero se* $\det(T_{\{e_1,\ldots,e_n\}}) = 0$, *caso contrário, é igual a classe de* $\det(T_{\{e_1,\ldots,e_n\}})$ *em* $L^*/(L^*)^2$.

Proposição 3.2.1 *Seja $L|K$ uma extensão separável de grau n. Sejam $\sigma_1, \ldots, \sigma_n$ os n distintos monomorfismos de L em $\overline{K}$, o fecho algébrico de K.*

1. *Sejam $\{\alpha_1, \ldots, \alpha_n\}$ base para L/K e $M := (\sigma_i(\alpha_j))_{1\leqslant i,j\leqslant n}$. Então $T_{\{\alpha_1,\ldots,\alpha_n\}} = M^t M$.*
2. *Se $L = K(\alpha)$ para algum $\alpha \in L$ e $f = \min_K(\alpha)$ de grau n, então*

$$\mathrm{disc}(f) = \mathrm{Norm}_{L/K}(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}} \det(T_{\{1,\alpha,\ldots,\alpha^{n-1}\}}).$$

Demonstração: *1- O lema 3.1.2 implica* $\mathrm{Tr}_{L/K}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)$. *Disso segue imediatamente que* $T_{\{\alpha_1,\ldots,\alpha_n\}} = M^t M$.

2- Escreva $f(y) = \prod_{i=1}^{n}(y - \sigma_i(\alpha)) \in \overline{K}[y]$, *então*

$$\mathrm{disc}(f) = \mathrm{Norm}_{L/K}(f'(\alpha)) = \prod_{i\neq j}(\sigma_i(\alpha) - \sigma_j(\alpha)).$$

O conjunto $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base para $K(\alpha)$ sobre K. Considere a matriz

$$M := (\sigma_i(\alpha^{j-1}))_{1\leqslant i,j\leqslant n} = \begin{pmatrix} 1 & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha)^{n-1} \\ 1 & \sigma_2(\alpha) & \cdots & \sigma_2(\alpha)^{n-1} \\ \vdots & \vdots & & \\ 1 & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha)^{n-1} \end{pmatrix}.$$

Aplicando a fórmula do determinante de Vandermonde, $\det(M) = \prod_{i>j}(\sigma_i(\alpha) - \sigma_j(\alpha))$. *Em particular,*

$$\begin{aligned}\det(T_{\{1,\alpha,\ldots,\alpha^{n-1}\}}) = (\det M)^2 &= \prod_{i>j}(\sigma_i(\alpha) - \sigma_j(\alpha))^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(\sigma_i(\alpha) - \sigma_j(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} \mathrm{disc}(f).\end{aligned}$$

■

Proposição 3.2.2 *Uma extensão finita $L|K$ é separável se, e somente se, o discriminante da forma do traço* Tr *não é zero.*

Demonstração: *Suponha $L|K$ separável. Sejam $\alpha \in L$ tal que $L = K(\alpha)$ e $f = \min_K(\alpha)$. Pela separabilidade,* $\mathrm{disc}(f) \neq 0$, *portanto pelo segundo item da proposição 3.2.1,* $\det(T_{\{1,\alpha,\ldots,\alpha^{n-1}\}}) \neq 0$.

Para a recíproca suponha $L|K$ não separável. Seja $L_0 \subseteq L$ a maior extensão de K separável que está contida em L. Pela hipótese, $L_0 \neq L$, assim $\mathrm{char}(K) = p > 0$ *e $[L : L_0] = p^s$ para algum $s > 0$. Seja $\alpha \in L$, pelo lema 3.1.1*

$$\mathrm{Tr}_{L/K}(\alpha) = -[L : K(\alpha)] \cdot a_{n-1},$$

onde a_{n-1} é o coeficiente do termo y^{n-1} de $f = \min_K(\alpha)$. Se $\alpha \in L_0$, então $p|[L : K(\alpha)]$, assim $\mathrm{Tr}_{L/K}(\alpha) = 0$ em K. Se $\alpha \in L \setminus L_0$, então $f(y) = g(y^p)$ para algum $g \in K[y]$, assim, o coeficiente $a_{n-1} = 0$ e consequentemente $\mathrm{Tr}_{L/K}(\alpha) = 0$. Portanto, dada a base $\{\alpha_1, \ldots, \alpha_n\}$ para L sobre K, concluímos $T_{\{\alpha_1,\ldots,\alpha_n\}} = (0)$. ■

Seja A um domínio integralmente fechado com corpo de frações K. Sejam $L|K$ um extensão finita de grau n e B o fecho integral de A em L. Tome $\alpha_1, \ldots, \alpha_n \in L$, o *discriminante* da $n-$upla $(\alpha_1, \ldots, \alpha_n)$ é definida como o elemento:

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) := \det(T_{\{\alpha_1,\ldots,\alpha_n\}}).$$

Se $\alpha_1, \ldots, \alpha_n \in B$, então $\alpha_i\alpha_j \in B$ para todo i, j e assim $\mathrm{Tr}_{L/K}(\alpha_i\alpha_j) \in A$. Em particular, se $\{\alpha_1, \ldots, \alpha_n\}$ é uma base integral, então $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \in A$ e sua imagem em $K^*/(K*)^2$ é igual ao discriminante da forma do traço $\mathrm{Tr} : L \times L \to K$. Quando $L = K(\alpha)$, $\alpha \in B$ e $f = \min_K(\alpha)$, pelas proposições 3.2.1 e 3.2.2:

Fato 3.2.1 $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \mathrm{disc}(f)$.

Essa descrição do discriminante de um polinômio pode ser usada para dar a seguinte condição suficiente para $B = A[\alpha]$.

Lema 3.2.1 *Sejam A um domínio principal, K seu corpo de frações e $L|K$ extensão separável de grau n. Sejam B o fecho integral de A em L e $\{b_1, \ldots, b_n\}$ uma base integral. Se o* $\mathrm{disc}(b_1, \ldots, b_n)$ *é um elemento livre de quadrados de A, então $\{b_1, \ldots, b_n\}$ é uma base para B sobre A. Em particular, sejam $\alpha \in B$ com $L = K(\alpha)$ e $f = \min_K(\alpha)$. Se* $\mathrm{disc}(f)$ *for um elemento livre de quadrados de A, então $B = A[\alpha]$.*
Demonstração: *Como por hipótese A é um domínio principal, B é um $A-$módulo livre de posto n. Seja $\{c_1, \ldots, c_n\}$ uma base para o $A-$módulo B. Escreva $b_i = \sum_{j=1}^{n} \gamma_{ij} c_j$, com $\gamma_{ij} \in A$ para todo $1 \leqslant i, j \leqslant n$. Seja $d = \det((\gamma_{ij})_{1 \leqslant i,j \leqslant n}) \in A$. Então,*

$$\mathrm{disc}(b_1, \ldots, b_n) = d^2 \mathrm{disc}(c_1, \ldots, c_n).$$

Uma vez que $\mathrm{disc}(c_1, \ldots, c_n) \in A$, *e* $\mathrm{disc}(b_1, \ldots, b_n)$ *é livre de quadrados em A, concluímos que d deve ser inversível em A, assim, $\{b_1, \ldots, b_n\}$ é base para B sobre A.* ■

3.3 Ideal Discriminante

Agora, retornaremos a caracterização de ideals primos de A que ramificam em B, onde B é o fecho integral de A em alguma extensão do seu corpo de frações. Primeiro provaremos uma condição necessária para um primo P de A se ramificar em B.

Definição 3.3.1 *Sejam A domínio de Dedekind, K seu corpo de frações, $L|K$ um extensão finita e B o fecho integral de A em L. Denote por $d_{B/A}$ o ideal de B gerado por elementos da forma $f'(\alpha)$, onde $f = \min_K(\alpha)$ e $\alpha \in B$ tal que $L = K(\alpha)$. Se a extensão $L|K$ não é simples, então $d_{B/A} := \langle 0 \rangle$. O ideal $d_{B/A}$ é chamado o* ideal diferente *de B/A. Seja $\delta_{B/A}$ o ideal de A gerado por elementos da forma* $\mathrm{disc}(f)$, *onde $f = \min_K(\alpha)$ e $\alpha \in B$ é tal que $L = K(\alpha)$. Se a extensão $L|K$ não é simples, então $\delta_{B/A} := \langle 0 \rangle$.*

É importante observar que estes ideais não dependem da escolha do elemento primitivo. Quando a extensão não é separável, estes ideais são nulos.

Proposição 3.3.1 *Sejam A um domínio de Dedekind, K seu corpo de frações e B seu fecho integral na extensão $L|K$ finita e separável. Então*

1. *Se $M \in \mathrm{Max}(B)$ é ramificado sobre A, então $d_{B/A} \subseteq M$.*
2. *Se $P \in \mathrm{Max}(A)$ ramifica em B, então $\delta_{B/A} \subseteq P$.*

Em particular, existe uma quantidade finita de ideais maximais de A que ramifica em B. ***Demonstração:*** *1- Como $L|K$ é separável tome $\beta \in L$ tal que $L = K(\beta)$, pela proposição 1.1.3, $\beta = \alpha/a$ para algum $\alpha \in B$ e $a \in A$. Portanto, $L = K(\alpha)$. Seja $f = \min_K(\alpha) \in A[y]$. Por $L|K$ ser separável, $f'(\alpha) \neq 0$. Portanto, existe uma quantidade finita de ideais maximais de B que contém $f'(\alpha)$. Afirmamos que se M é ideal maximal de B que não contém $f'(\alpha)$, então M não ramifica sobre A. Seja $N := M \cap A[\alpha]$ e $P := M \cap A$. Sejam $M_1, \ldots, M_s$ os ideais obtidos na proposição 2.3.1. Então $PA[\alpha] \supseteq M_1^{e_1} \cdots M_s^{e_s}$. Sem perda de generalidade, podemos supor $N = M_1$. Uma vez que $f'(\alpha) \notin N$, a proposição 2.5.1 garante que $e_1 = 1$ e que a extensão $A[\alpha]/N$ é separável sobre A/P. Para finalizar a demonstração deste item, mostraremos que $e_{M/P} = 1$ e que B/M é separável sobre A/P, para isto, basta mostrar que $A[\alpha]_N = B_M$. De fato, como $e_1 = 1$, pela proposição 2.5.1, $A[\alpha]_N$ é um domínio de ideais principais. Como $A[\alpha]_N$ e B_M possuem o mesmo corpo de frações e $NA[\alpha]_N \subseteq MB_M$, pelo seguinte fato:*

> ***Fato 3.3.1*** *Sejam R um domínio local de ideais principais com corpo de frações K e S um domínio local com $R \subseteq S \subseteq K$. Sejam M_R e M_S os ideais maximais de R e S respectivamente. Se $M_R \subseteq M_S$, então $R = S$ (veja [6], pág. 71).*

Concluímos que $A[\alpha]_N = B_M$. Utilizando esta igualdade e o lema 2.2.2,

$$A[\alpha]/N \cong A[\alpha]_N/NA[\alpha]_N \cong B_M/MB_M \cong B/M.$$

Portanto, B/M é separável sobre A/P. Segue da proposição 2.5.1 que $PA[\alpha]_N = NA[\alpha]_N$. Logo, $PB_M = MB_M$ e $e_{M/P} = 1$. Portanto, quando $d_{B/A} \not\subseteq M$, então M não está ramificado sobre A.

2- Seja P um ideal maximal de A que ramifica em B. Por definição, existem um ideal maximal M de B que contém P e que está ramificado sobre A. Portanto, $M \supseteq d_{B/A}$. Pela proposição 3.1.1, se $L = K(\alpha)$, então $\mathrm{Norm}_{L/K}(f'(\alpha)) = \mathrm{disc}(f)$. Uma vez que a norma dos elementos M pertencem a P, concluímos $\delta_{B/A} \subseteq P$. ■

Definição 3.3.2 *Seja A um domínio integralmente fechado com corpo de frações K. Seja $L|K$ um extensão de grau n. Seja B o fecho integral de A em L. O* ideal discriminante *$\Delta_{B/A}$ é o ideal de A gerado por elementos da forma $\mathrm{disc}(b_1, \ldots, b_n)$, onde $\{b_1, \ldots, b_n\} \subseteq B$ é base de $L|K$.*

Observe que o ideal $\delta_{B/A}$ é um ideal de A gerado por elementos da forma $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1})$, onde $\alpha \in B$ e $L = K(\alpha)$. É claro que $\delta_{B/A} \subseteq \Delta_{B/A}$. Quando $B = A[\alpha]$ para algum $\alpha \in B$ e $f = \min_A(\alpha)$, então $\delta_{B/A} = \Delta_{B/A} = \mathrm{disc}(f)A$. Em geral, $\Delta_{B/A} = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)A$, onde $\{\alpha_1, \ldots, \alpha_n\}$ é base para B sobre A.

Exemplo 3.3.1 *Suponha que n é um inteiro par tal que $27n^2 + 18n^2 - 1$ é livre de quadrado. Seja α uma raiz de $f(n, y) = y^3 - y^2 - ny - n^3$. Seja $\{1, \alpha, n^2/\alpha\}$ uma base para $\mathcal{O}_{\mathbb{Q}(\alpha)}$ sobre $\mathbb{Z}$. Portanto,*

$$\Delta_{\mathcal{O}_{\mathbb{Q}(\alpha)}/\mathbb{Z}} = \text{disc}(1, \alpha, n^2/\alpha)\mathbb{Z} = \langle 27n^2 + 18n^2 - 1\rangle\mathbb{Z}.$$

Tome $w = a + b\alpha + cn^2/\alpha \in \mathcal{O}_{\mathbb{Q}(\alpha)}$,

$$\text{disc}(1, w, \ldots, w^{n-1}) = [(b^3 - c^3)n - bc(b + c)]^2\text{disc}(1, \alpha, n^2/\alpha).$$

Como $2|n$, $2|(b^3 - c^3)n - bc(b + c)$, portanto

$$\delta_{\mathcal{O}_{\mathbb{Q}(\alpha)}/\mathbb{Z}} \subseteq \langle 4\rangle\Delta_{\mathcal{O}_{\mathbb{Q}(\alpha)}/\mathbb{Z}} \subseteq \langle 2\rangle.$$

Observe que $2 \nmid 27n^2 + 18n^2 - 1$, portanto $\Delta_{\mathcal{O}_{\mathbb{Q}(\alpha)}/\mathbb{Z}} \not\subseteq \langle 2\rangle$. Segue do teorema abaixo que o ideal $\langle 2\rangle$, que divide $\delta_{\mathcal{O}_{\mathbb{Q}(\alpha)}/\mathbb{Z}}$, não ramifica em $\mathcal{O}_{\mathbb{Q}(\alpha)}$. O ideal $\langle 2\rangle$ é portanto um ideal primo não importante da extensão $\mathbb{Q}(\alpha)/\mathbb{Q}$.

Teorema 3.3.1 *Sejam A um domínio de Dedekind, K seu corpo de frações e B o fecho integral de A numa extensão finita $L|K$. Suponha B finitamente gerado como $A-$módulo. Então $P \in \text{Max}(A)$ ramifica em B se, e somente se, $\Delta_{B/A} \subseteq P$.*

Para a demonstração veja [6], página 145.

3.4 Aplicação Norma em Ideais

Nesta seção introduziremos o conceito de *norma-ideal* de um ideal. Este conceito não está diretamente ligado com as propriedades de ramificação estudadas neste capítulo, mas introduziremos este conceito aqui pois é uma generalização natural do conceito de norma de um elemento introduzida na seção 3.1. O conceito de *norma-ideal* irá desempenhar um papel fundamental no capítulo 4.

Seja A um domínio de Dedekind com corpo de frações K. Sejam $L|K$ extensão de grau n e B o fecho integral de A em L. Suponha B finitamente gerado como $A-$módulo. Denotaremos por (A, K, B, L) a quádrupla tal que A, K, B e L são como acima. Relembre que na seção 3.1, definimos a aplicação norma associada a $L|K$. Nosso objetivo nesta seção é definir a aplicação:

$$N_{B/A} : I_B := \{\text{ideais de } B\} \longrightarrow I_A := \{\text{ideais de } A\}$$

tal que, quando $L|K$ for separável, então, para todo $\alpha \in B$,

$$N_{B/A}(\alpha B) = \mathrm{Norm}_{L/K}(\alpha)A.$$

Para motivar a definição de $N_{B/A}$, suponha $L|K$ Galois com grupo de Galois $G = \{\sigma_1, \ldots, \sigma_n\}$. Pelo lema 3.1.2, $\mathrm{Norm}_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$. Esta expressão para $\mathrm{Norm}_{L/K}(\alpha)$ sugere a seguinte definição:

$$N_{B/A}(I) := \left(\prod_{i=1}^{n} \sigma_i(I)\right) \cap A.$$

Veremos a seguir que esta é, de fato, uma *boa definição* quando $L|K$ é Galois.

Lema 3.4.1 *Sejam (A, K, B, L) como definido anteriormente e $J \trianglelefteq A$. Então $J = JB \cap A$. Além disso, a aplicação $i_{B/A} : I_A \to I_B$, que $J \mapsto JB$, é injetiva.*
Demonstração: *Veja [6], página 150.*

Proposição 3.4.1 *Sejam $L|K$ de Galois e $\alpha \in B$. Então $N_{B/A}(\alpha B) = \mathrm{Norm}_{L/K}(\alpha)A$.*
Demonstração: *Pela definição de $N_{B/A}(I)$ dada acima,*

$$\begin{aligned} N_{B/A}(\alpha B) = (\textstyle\prod_{i=1}^{n} \sigma_i(\alpha)B) \cap A &= (\textstyle\prod_{i=1}^{n} \sigma_i(\alpha))B \cap A \\ &= \mathrm{Norm}_{L/K}(\alpha)B \cap A \\ &= \mathrm{Norm}_{L/K}(\alpha)A. \end{aligned}$$

■

Lema 3.4.2 *Seja (A, K, B, L) com $L|K$ Galois. Sejam $\mathfrak{P} \in \mathrm{Max}(B)$ e $P := \mathfrak{P} \cap A$. Então $N_{B/A}(\mathfrak{P}) = P^{f_{\mathfrak{P}/P}}$.*
Demonstração: *Observamos em 2.6.1 que $\prod_{\sigma \in G} \sigma(\mathfrak{P}) = (PB)^f$. Logo,*

$$N_{B/A}(\mathfrak{P}) = \left(\prod_{\sigma \in G} \sigma(\mathfrak{P})\right) \cap A = (P^f)B \cap A \overset{\text{lema 3.4.1}}{=} P^f.$$

■

Proposição 3.4.2 *Seja (A, K, B, L) com $L|K$ Galois. Seja $I = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_r^{a_r}$ um produto de ideais maximais de B. Então $N_{B/A}(I) = \prod_{i=1}^{r} N_{B/A}(\mathfrak{P}_i)^{a_i}$. Em particular, para todo $I, J \in I_B$, $N_{B/A}(IJ) = N_{B/A}(I) \cdot N_{B/A}(J)$.*
Demonstração: *Seja $\mathcal{J}_P := \{j | \mathfrak{P}_j \cap A = P\}$. Vamos reescrever I do seguinte modo:*

$$I = \prod_{P \in \mathrm{Max}(A)} \left(\prod_{j \in \mathcal{J}_P} \mathfrak{P}_j^{a_j}\right).$$

Tome $v_P := \sum_{j\in\mathcal{J}_P} a_j f_{\mathfrak{P}_j/P}$. *Então*

$$\prod_{i=1}^{n}\sigma_i(I) = \prod_{P\in\mathrm{Max}(A)}(PB)^{v_P}.$$

Uma vez que PB *é coprimo com* QB *se* P *e* Q *são ideais maximais distintos de* A,

$$\begin{array}{rcl}\left(\prod_{P\in\mathrm{Max}(A)}(PB)^{v_P}\right)\cap A & = & \left(\bigcap_{P\in\mathrm{Max}(A)}P^{v_P}B\right)\cap A \\ & = & \bigcap_{P\in\mathrm{Max}(A)}(P^{v_P}B\cap A) \\ & \overset{\textit{lema 3.4.1}}{=} & \bigcap_{P\in\mathrm{Max}(A)}P^{v_P} \\ & = & \prod_{P\in\mathrm{Max}(A)}P^{v_P} \\ & \overset{\textit{lema 3.4.2}}{=} & \prod_{i=1}^{r}N_{B/A}(\mathfrak{P}_i)^{a_i}.\end{array}$$

Portanto, $N_{B/A}(I) := (\prod_{i=1}^{n}\sigma_i(I))\cap A = \prod_{i=1}^{r}\mathrm{Norm}_{B/A}(\mathfrak{P}_i)^{a_i}$. ■

Para as extensões não Galoisianas, utilizaremos as propriedades obtidas na proposição 3.4.2 para definir a aplicação norma ideal.

Definição 3.4.1 *Seja* (A,K,B,L) *como no começo da seção. Quando* $L|K$ *não é Galois, defina a* aplicação norma-ideal $N_{B/A}: I_B \to I_A$ *por:*

1. *Se* $\mathfrak{P}\in\mathrm{Max}(B)$, *então* $N_{B/A}(\mathfrak{P}) := (\mathfrak{P}\cap A)^{f_{\mathfrak{P}/\mathfrak{P}\cap A}}$.
2. $N_{B/A}(\mathfrak{P}_1^{a_1}\cdots\mathfrak{P}_r^{a_r}) := \prod_{i=1}^{r}N_{B/A}(\mathfrak{P}_i)^{a_i}$.
3. *Por fim,* $N_{B/A}(B) := A$ *e* $N_{B/A}(\langle 0\rangle) = \langle 0\rangle$.

A aplicação $N_{B/A}: I_B \to I_A$ definida acima é claramente multiplicativa. Quando não causar confusão chamaremos a aplicação norma-ideal simplesmente por aplicação norma.

Lema 3.4.3 *Seja* (A,K,B,L). *A composição* $N_{B/A}\circ i_{B/A}: I_A \to I_A$, *é dada por* $P\mapsto P^n$. ***Demonstração:*** *É fácil de ver que* $(N_{B/A}\circ i_{B/A})(\langle 0\rangle) = \langle 0\rangle$. *Uma vez que ambos* $N_{B/A}$ *e* $i_{B/A}$ *são aplicações multiplicativas, basta mostrar o lema para* $P\in\mathrm{Max}(A)$. *Escreva* $i_{B/A}(P) = PB = \prod_{i=1}^{s}\mathfrak{P}_i^{e_i}$. *Então*

$$(N_{B/A}\circ i_{B/A})(P) = N_{B/A}(PB) = \prod_{i=1}^{s}N_{B/A}(\mathfrak{P}_i)^{e_i} = P^{\sum_{i=1}^{s}e_i f_{\mathfrak{P}_i/P}} = P^n.$$

■

Lema 3.4.4 *Sejam* $M|L$ *e* $L|K$ *extensões finitas. Sejam* A *um domínio de Dedekind com corpo de frações* K *e* B *(respectivamente* C*) o fecho integral de* A *em* L *(respectivamente,*

em M). Suponha que B e C são $A-$módulos finitamente gerados. Então $N_{C/A} = N_{B/A} \circ N_{C/B}$.

Demonstração: *Como as aplicações norma são multiplicativas, basta mostrar que para todo $\mathfrak{P} \in \mathrm{Max}(C), N_{C/A}(\mathfrak{P}) = N_{B/A}(N_{C/B}(\mathfrak{P}))$. Sejam $\mathfrak{P}_B := \mathfrak{P} \cap B$ e $\mathfrak{P}_A := \mathfrak{P} \cap A$. Pela definição da norma, $N_{C/A}(\mathfrak{P}) = \mathfrak{P}_A^{f_{\mathfrak{P}/\mathfrak{P}_A}}$ e $N_{B/A}(N_{C/B}(\mathfrak{P})) = \mathfrak{P}_A^{f_{\mathfrak{P}/\mathfrak{P}_B} f_{\mathfrak{P}/\mathfrak{P}_A}}$. O lema segue imediatamente da multiplicidade de grau residual.* ■

Proposição 3.4.3 *Seja (A, K, B, L). Então para todo $\alpha \in B$, $\mathrm{Norm}_{L/K}(\alpha)A = N_{B/A}(\alpha B)$.*

Demonstração: *Provaremos esta proposição para o caso em que $L|K$ é separável. Seja $M|L$ um extensão de Galois de L tal que $M|K$ seja de Galois também. Sejam C o fecho integral de A em L e $\alpha \in B$, então*

$$\begin{array}{rcl} N_{C/A}(\alpha C) & \overset{\text{lema 3.4.4}}{=} & N_{B/A}(N_{C/B}(\alpha C)) \\ & \overset{\text{lema 3.4.3}}{=} & N_{B/A}((\alpha B)^{[M:L]}) \\ & = & N_{B/A}(\alpha B)^{[M:L]}. \end{array}$$

Analogamente, usando a transitividade da norma, para todo $\alpha \in B$,

$$\mathrm{Norm}_{M/K}(\alpha) = \mathrm{Norm}_{L/K}(\mathrm{Norm}_{M/L}(\alpha)) = \mathrm{Norm}_{L/K}(\alpha^{[M:L]}) = \mathrm{Norm}_{L/K}(\alpha)^{[M:L]}.$$

Como $M|K$ é Galois, pela proposição 3.4.1, $N_{C/A}(\alpha C) = \mathrm{Norm}_{M/K}(\alpha)A$. Portanto, concluímos

$$N_{B/A}(\alpha B)^{[M:L]} = (\mathrm{Norm}_{L/K}(\alpha)A)^{[M:L]}.$$

Uma vez que A tem a propriedade de fatoração única de ideais, segue $B_{B/A}(\alpha B) = \mathrm{Norm}_{L/K}(\alpha)A$. ■

Observação 3.4.1 *Sejam (A, K, B, L) como no começo da seção, $\alpha \in B$ tal que $L = K(\alpha)$ e $f = \min_K(\alpha) \in A[y]$. Pela proposição 3.1.1, $\mathrm{Norm}_{L/K}(f'(\alpha)) = \mathrm{disc}(f)$. Quando B não é simples sobre A, uma afirmação análoga pode ser feita para ideais: $N_{B/A}(d_{B/A}) = \Delta_{B/A}$. Esta igualdade é provado, por exemplo em [7], página 212. A igualdade $N_{B/A}(d_{B/A}) = \Delta_{B/A}$ junto com o exemplo 3.3.1 mostram que, dado um ideal $I = \langle x_1, \ldots, x_r \rangle$ de B não é verdade, em geral, que $N_{B/A}(I) = \langle \mathrm{Norm}_{L/K}(x_1), \ldots, \mathrm{Norm}_{L/K}(x_r) \rangle$.*

Citaremos agora sem provar o seguinte teorema que pode ser encontrado em [7], 7I.

Teorema 3.4.1 *Seja (A, K, B, L) com $L|K$ separável. Sejam $M \in \mathrm{Max}(B)$ e $P := M \cap A$. Suponha B/M separável sobre A/P. Então $\mathrm{ord}_M(d_{B/A}) \geqslant e_{M/P} - 1$, ocorrendo a igualdade se, e somente se, $e_{M/P}$ e a característica de A/P são relativamente primos.*

Usando o fato que $N_{B/A}(d_{B/A}) = \Delta_{B/A}$,

$$\begin{array}{rcl} \mathrm{ord}_P(\Delta_{B/A}) & \geqslant & \sum_{M \supset P} f_{M/P}(e_{M/P} - 1) \\ & = & n - \sum_{M \supset P} f_{M/P}. \end{array}$$

Tome $A = \mathbb{Z}$ e $P = \langle p \rangle$ com $p > n$. Uma vez que $e_{M/P} \leqslant n$, $(e_{M/P}, p) = 1$. E segue do teorema 3.4.1 que

$$\mathrm{ord}_P(\Delta_{B/A}) = n - \sum_{M \supset P} f_{M/P} \leqslant n - 1.$$

Capítulo

4

Grupo de Classe de Ideais

Neste capítulo, associaremos a um domínio de Dedekind A um grupo abeliano, chamado *grupo de classe de ideais*, do $\mathrm{Cl}(A)$. Do ponto de vista algébrico, este grupo é importante pois ele mede o *quanto falta* para o anel A ser um domínio de ideais principais. Grosseiramente falando, o grupo $\mathrm{Cl}(A)$ é construído considerando primeiramente o conjunto de ideais não nulos de A e então *jogando fora* deste conjunto os ideais que são principais. Também pode-se dar uma motivação geométrica para considerar o grupo $\mathrm{Cl}(A)$ quando A é um anel de funções de uma curva sobre $\mathbb{C}$. Neste caso os elementos de ordem finita de $\mathrm{Cl}(A)$ são relacionados com espaços de cobertura da curva e assim, são relacionados com seu grupo fundamental, um importante invariante topológico associado a uma curva. Este conceito foi introduzido pela primeira vez por Kummer no caso de anéis ciclotômicos nos meados do século XIX, enquanto trabalhava sobre o último teorema de Fermat.

O resultado principal a ser estudado é sobre a finitude deste grupo em alguns casos particulares: quando A é o fecho integral de $\mathbb{Z}$ numa extensão de $\mathbb{Q}$ ou A é da forma $k[x,y]/\langle f\rangle$, onde k é um corpo finito.

O conceito de *grupo de classe* é de natureza muito diferente dos conceitos de fatoração de ideais e ramificação discutidos anteriormente. Estes conceitos são de natureza local, por exemplo para fatoração completa de um ideal I em um domínio de Dedekind A é suficiente saber a fatoração de I em cada localização A_P de A, com P ideal maximal. O conceito de *grupo de classe* por outro lado, é um conceito global. Cada localização A_P é um domínio de ideal principais e, assim, veremos que seu grupo de classe $\mathrm{Cl}(A_P)$ é trivial. Portanto, nenhuma informação do grupo de classe de A pode ser retirada a partir do conhecimento do grupo de classe de cada localização.

Seja A um domínio. O conjunto $\mathcal{M}(A)$ consistindo de todos os ideais não nulos de A munido de multiplicação de ideais é um monoide abeliano. Cujo elemento neutro é $\langle 1\rangle = A$. Este monoide é um grupo apenas quando A é corpo. O objetivo é associar outro monoide a $\mathcal{M}(A)$ que seja um grupo. Mais precisamente, associaremos um monoide a $\mathcal{M}(A)$ que será um grupo quando A for domínio de Dedekind. Seja $\mathcal{P}(A)$ o conjunto dos ideais principais não nulos de A. Claramente $\mathcal{P}(A)$ é um submonoide de $\mathcal{M}(A)$, além disso, A é domínio principal se, e só se, $\mathcal{P}(A) = \mathcal{M}(A)$. Se $\mathcal{M}(A)$ fosse grupo, $\mathcal{P}(A)$ seria um subgrupo e faria sentido considerar o quociente $\mathcal{M}(A)/\mathcal{P}(A)$ para mensurar o quão perto o anel A está de ser um domínio de ideais principais. Uma vez que $\mathcal{M}(A)$ não é um grupo em geral, mediremos o quão perto o anel A está de ser um domínio principal com um quociente de $\mathcal{M}(A)$ por uma relação de equivalência definida por $\mathcal{P}(A)$.

Definição 4.0.2 *Seja $\mathcal{M}$ um monoide com elemento neutro* 1. *Uma* relação de congruência *em M é uma relação de equivalência $\sim$ tal que, para todo $a, a', b, b' \in \mathcal{M}$ com $a \sim a$ e $a' \sim b'$, $aa' \sim bb'$.*

Dados um monoide $\mathcal{M}$ e uma relação de congruência $\sim$ em $\mathcal{M}$, o conjunto quociente $\overline{\mathcal{M}} := \mathcal{M}/\sim$ munido da seguinte operação possui estrutura de um monoide:

$$\begin{array}{ccc} \overline{\mathcal{M}} \times \overline{\mathcal{M}} & \longrightarrow & \overline{\mathcal{M}} \\ ([a],[b]) & \longmapsto & [ab]. \end{array}$$

Um exemplo de uma relação de congruência num monoide é dado da seguinte forma: Sejam $\mathcal{M}$ um monoide comutativo e $\mathcal{P}$ um submonoide de $\mathcal{M}$. Dados $a, b \in \mathcal{M}$, defina $a \sim b$ se, e somente se, existem $\alpha, \beta \in \mathcal{P}$ tais que $\alpha a = \beta b$. Em particular:

Definição 4.0.3 *Seja A um domínio comutativo. Considere a seguinte relação no monoide $\mathcal{M}(A)$:*

$$I \sim J \Longleftrightarrow \exists \alpha, \beta \in A \setminus \{0\}, \quad \langle\alpha\rangle I = \langle\beta\rangle J.$$

Observe que $\sim$ é uma relação de equivalência associada ao submonoide $\mathcal{P}(A)$ de $\mathcal{M}(A)$ e assim uma relação de congruência em $\mathcal{M}(A)$. Denotamos o monoide $\mathcal{M}(A)/\sim$ por $\mathrm{Cl}(A)$.

Quando A é um domínio de Dedekind, $\mathrm{Cl}(A)$ é um grupo cujo elemento neutro é a classe de $\langle 1\rangle$. De fato, para mostrar que $\mathrm{Cl}(A)$ é um grupo, falta mostrar que todo elemento possui um inverso. Considere $I \in \mathcal{M}(A), I \neq A$. Seja $\alpha \in I, \alpha \neq 0$. Como vimos, todo ideal não trivial de A tem uma fatoração única em produto de ideais maximais, logo podemos escrever $\langle\alpha\rangle = IJ$ para algum $J \in \mathcal{M}(A)$. Portanto, $IJ \sim \langle 1\rangle$, isto é, a classe de J é o inverso da classe de I em $\mathrm{Cl}(A)$.

Definição 4.0.4 *Seja A um domínio de Dedekind. O grupo* $\mathrm{Cl}(A)$ *é chamado do* grupo de classe ideal *de A.*

O próximo resultado mostra que a recíproca é verdadeira. Isto é, a grandeza deste grupo pode ser usando para saber o *quanto* um domínio não é principal.

Lema 4.0.5 *Seja A um domínio comutativo. Então* $\mathrm{Cl}(A)$ *é trivial se, e somente se, A é um domínio de ideais principais.*
Demonstração: *Suponha* $\mathrm{Cl}(A) = \{\langle 1\rangle\}$. *Seja $0 \neq I \trianglelefteq A$, então existem $a, b \in A \setminus \{0\}$ tais que $\langle a\rangle I = \langle b\rangle$. Em particular, $b = ac$ para algum $c \in I$. Afirmamos que $I = \langle c\rangle$. De fato, se $x \in I$, então $ax = bd$ para algum $d \in A$, ou, $a(x - cd) = 0$, como A é domínio segue que $x = cd \in \langle c\rangle$. A recíproca é imediata, basta observar que todo ideal principal é equivalente a $\langle 1\rangle$.* ■

Um monomorfismo de anéis $\varphi : A \to B$ induz a aplicação natural de monoides:

$$\begin{array}{rccc} \varphi_{\mathcal{M}}: & \mathcal{M}(A) & \longrightarrow & \mathcal{M}(B) \\ & I & \longmapsto & \varphi(I)B. \end{array}$$

Sejam $I, J \in \mathcal{M}(A)$. Se $\alpha I = \beta J$, então $\varphi(\alpha)\varphi(I)B = \varphi(\beta)\varphi(J)B$. Em particular, $\varphi_{\mathcal{M}}$ induz a aplicação:

$$\begin{array}{rccc} \varphi_{\mathcal{M}}: & \mathrm{Cl}(A) & \longrightarrow & \mathrm{Cl}(B) \\ & \text{classe de } I & \longmapsto & \text{classe de } \varphi(I)B. \end{array}$$

Quando $A \subseteq B$, denotamos esta aplicação simplesmente por $i_{B/A} : \mathrm{Cl}(A) \to \mathrm{Cl}(B)$.

Seja A um domínio de Dedekind, K seu corpo de frações, $L|K$ uma extensão finita e separável e B o fecho integral de A em L. Considere a aplicação norma-ideal como em 3.4.1:

$$\begin{array}{rccc} N_{B/A}: & \mathcal{M}(B) & \longrightarrow & \mathcal{M}(A) \\ & I & \longmapsto & N_{B/A}(I). \end{array}$$

Sejam $I, J \in \mathcal{M}(B)$, se $\alpha I = \beta J$, então pela proposição 3.4.3,

$$N_{B/A}(\alpha I) = N_{L/K}(\alpha)N_{B/A}(I) = N_{B/A}(\beta J) = N_{L/K}(\beta)N_{B/A}(J).$$

Ou seja, $N_{B/A}(I) \sim N_{B/A}(J)$ em $\mathcal{M}(A)$. Portanto a aplicação norma-ideal $N_{B/A}$ induz a aplicação natural de grupos abelianos

$$\begin{array}{rccc} N_{B/A}: & \mathrm{Cl}(B) & \longrightarrow & \mathrm{Cl}(A) \\ & [I] & \longmapsto & [N_{B/A}(I)]. \end{array}$$

O lema 3.4.3 garante que a composição $N_{B/A} \circ i_{B/A} : \mathrm{Cl}(A) \to \mathrm{Cl}(A)$ é aplicação $n-$ésima potência em $\mathrm{Cl}(A)$.

4.1 Anéis com Quocientes Finitos

Definição 4.1.1 *Diremos que um domínio de Dedekind A possui quocientes finitos se, para todo $P \in \mathrm{Max}(A)$, o corpo residual A/P é um corpo finito.*

Definição 4.1.2 *Seja A um domínio de Dedekind com quocientes finitos. Definimos a norma de um ideal $I \neq 0$ por $\|I\|_A :=$ cardinalidade de A/I.*

Observe que $\|I\|_A = 1$ se, e só se, $I = A$, e também, a priori, $\|I\|_A$ pode ser infinito. A seguir, após fazer algum exemplos, estudaremos a finitude de $\|I\|_A$.

Exemplo 4.1.1 *Seja $I = \langle a \rangle \trianglelefteq \mathbb{Z}, a \neq 0$. Então $\|I\|_{\mathbb{Z}} := |\mathbb{Z}/a\mathbb{Z}| = |a|$. Em particular, dado $\lambda \in \mathbb{R}^+$, existe uma quantidade finita de ideais $I \trianglelefteq \mathbb{Z}$ tal que $\|I\|_{\mathbb{Z}} \leqslant \lambda$.*

Exemplo 4.1.2 *O anel $A = k[x]$, onde k é um corpo finito com $q = p^r$ elementos, possui quocientes finitos. Seja $I = \langle g(x) \rangle \neq \langle 0 \rangle$. Então*

$$\|I\|_{k[x]} := |k[x]/\langle g(x) \rangle| = q^{\deg(g)}.$$

De fato, $k[x]/\langle g(x) \rangle$ é um $k-$espaço vetorial de dimensão $\deg(g)$. Dado $\lambda \in \mathbb{R}^+$, existe uma quantidade finita de ideais I em $k[x]$ tal que $\|I\|_{k[x]} \leqslant \lambda$, pois existem no máximo $q\lambda$ polinômios em $k[x]$ de grau menor ou igual a $\log(\lambda)/\log(q)$.

O próximo lema é um resultado de álgebra comutativa que nos será útil, por não ser enfoque do trabalho não será demonstrado aqui.

Lema 4.1.1 *Sejam A um domínio de Dedekind e $P \in \mathrm{Max}(A)$. Então para todo $n \in \mathbb{N}$, os $A-$módulos P^{n-1}/P^n e A/P são isomorfos. Em particular, se A/P é finito, então A/P^r é finito e $|A/P^r| = |A/P|^r$.*
Demonstração: *Veja [6], página 161.*

Lema 4.1.2 *Sejam A um domínio de Dedekind com quocientes finitos e $I \trianglelefteq A$. Então $\|I\|_A \in \mathbb{N}$ e a aplicação $\|\cdot\|_A : \mathcal{M}(A) \to \mathbb{N}$ é multiplicativa.*
Demonstração: *Seja $I := P_1^{a_1} \cdots P_r^{a_r} \trianglelefteq A$ não nulo. Pela hipótese, os quocientes $A/P_i, i = 1, \ldots, r$, são finitos. Utilizando o isomorfismo $A/I \cong A/P_1^{a_1} \times \cdots \times A/P_r^{a_r}$ e o lema 4.1.1, concluímos $\|I\|_A := \prod_{i=1}^r \|P_i\|_A^{a_i}$.* ■

Proposição 4.1.1 *Seja A um domínio de Dedekind com quocientes finitos, K seu corpo de frações e $L|K$ um extensão finita. Suponha o fecho integral B de A em L um $A-$módulo finitamente gerado. Então B é um domínio de Dedekind com quocientes finitos. Além disso, se $0 \neq I \trianglelefteq B$, então $\|I\|_B = \|N_{B/A}(I)\|_A$.*
Demonstração: *A primeira parte foi demonstrada no primeiro capítulo. Sejam $M \in \mathrm{Max}(B)$ e $P := M \cap A$. Então B/M é um $(A/P)-$espaço vetorial de dimensão $f_{M/P}$. Portanto, B/M é um corpo finito e*

$$\|M\|_B = |B/M| = |A/P|^{f_{M/P}} = \|P^{f_{M/P}}\|_A = \|N_{B/A}(M)\|_A.$$

Pela multiplicatividade de $N_{B/A}$, para todo ideal $I \trianglelefteq B$, $\|I\|_B = \|N_{B/A}(I)\|_A$. ■

Deixemos agora a teoria de anéis com quocientes finitas um pouco de lado e nos concentraremos em dois casos muito importantes: Nos próximos três lemas, A denotará $\mathbb{Z}$ ou $k[x]$, com k corpo finito. Denotaremos por L uma extensão finita do corpo de frações K de A, e B o fecho integral de A em L. Além disso, vamos supor que B é um $A-$módulo finitamente gerado e, portanto, pela proposição 4.1.1, B terá quocientes finitos.

Lema 4.1.3 *Dado $\lambda \in \mathbb{R}^+$, existe uma quantidade finita de ideais I de B com $\|I\|_B \leqslant \lambda$.*
Demonstração: *Uma vez que a função $\|\cdot\|_B$ é multiplicativa e positiva, para provar este lema, basta mostrar que existe uma quantidade finita de ideal maximais M tais que $\|M\|_B \leqslant \lambda$. Como um ideal maximal de A está contido numa quantidade finita de ideais maximais de B, e por*

$$\|M\|_B = \|M \cap A\|_A^{f_{M/M\cap A}} \geqslant \|M \cap A\|_A,$$

é suficiente mostrar que dado $\lambda \in \mathbb{R}^+$, existe uma quantidade finita de ideais maximais P de A com $\|P\|_A \leqslant \lambda$. Mas como $A = \mathbb{Z}$ ou $A = \mathbb{F}_q[x]$, a última condição é claramente satisfeita, veja o exemplo 4.1.1. ■

Observação 4.1.1 *O lema 4.1.3 vale para B um anel Noetheriano, veja [4], página 15.*

Lema 4.1.4 *O grupo $\mathrm{Cl}(B)$ é finito se, e somente se, existe $\lambda \in \mathbb{R}$, dependendo de B, tal que cada classe ideal de B contém um ideal I com $\|I\|_B \leqslant \lambda$.*
Demonstração: *Suponha o grupo $\mathrm{Cl}(B) = \{C_1, \ldots, C_h\}$ finito. Tome I_i um ideal na classe C_i e considere $\lambda := \max\{\|lI_i\|_B, i = 1, \ldots, \}$. Reciprocamente, pelo lema 4.1.3, existe uma quantidade finita de ideais I de B tal que $\|I\|_B \leqslant \lambda$. Assim, como toda classe ideal de B contém um ideal I desta forma, concluímos que $\mathrm{Cl}(B)$ é finito.* ■

Lema 4.1.5 *Seja $\lambda \in \mathbb{R}^+$. Toda classe ideal de B contém um ideal com $\|I\|_B \leqslant \lambda$ se cada ideal não nulo J de B contém um elemento α com $\|\langle\alpha\rangle\|_B \leqslant \lambda\|J\|_B$.*
Demonstração: *Seja $C \neq \langle 1\rangle$ um classe ideal de B. Fixe J um ideal na classe C^{-1}. Seja $\alpha \in J$ tal que $\|\langle\alpha\rangle\|_B \leqslant \lambda\|J\|_B$. Como $\alpha \in J$, podemos escrever $\langle\alpha\rangle = IJ$, para algum ideal I de A. Assim, $I \in C$ e a desigualdade $\|IJ\|_B = \|\langle\alpha\rangle\|_B \leqslant \lambda\|J\|_B$ mostra que $\|I\|_B \leqslant \lambda$.* ■

Teorema 4.1.1 *Seja $A = \mathbb{Z}$ ou $A = k[x]$, com k um corpo finito. Sejam L uma extensão separável de grau n do corpo de frações K de A, e B o fecho integral de A em L. Então, existe $\lambda \in \mathbb{R}^+$, dependendo somente de B, tal que todo ideal não nulo I de B contém um elemento não nulo α com $\|\langle\alpha\rangle\|_B \leqslant \lambda\|I\|_B$. Em particular, o grupo de classe ideal de B é finito.*
Demonstração: *Quando $A = \mathbb{Z}$ observe que B é livre de posto finito. Assim, tome $\{\alpha_1, \ldots, \alpha_n\}$ uma base para B sobre A e $\sigma_1, \ldots, \sigma_n$ os monomorfismos de L em $\mathbb{C}$. Seja*

$$\lambda := \prod_{i=1}^{n}\left(\sum_{j=1}^{n}|\sigma_i(\alpha_j)|\right).$$

Mostraremos que todo ideal I não nulo de B contém um elemento não nulo α tal que $\|\langle\alpha\rangle\|_B \leqslant \lambda\|I\|_B$. Sejam $I \trianglelefteq B$ e m o único inteiro positivo tal que

$$m^n \leqslant \|I\|_B < (m+1)^n.$$

Considere o seguinte conjunto de $(m+1)^n$ elementos distintos de B :

$$\left\{\sum_{j=1}^{n} m_j\alpha_j | m_j \in \mathbb{Z} \quad e \quad 0 \leqslant m_j \leqslant m, \forall j = 1, \ldots, n\right\}.$$

Como $(m+1)^n > \|I\|_B = |B/I|$, existem dois elementos distintos do conjunto anterior que são congruentes modulo I. Tomando a diferença desses dois elementos, obtemos um elemento não nulo de I da forma

$$\alpha := \sum_{j=1}^{n} m_j\alpha_j \text{ com } m_j \in \mathbb{Z} \text{ e } |m_j| \leqslant m, \forall i = 1, \ldots, n.$$

Então

$$\begin{aligned}\|\alpha B\|_B =& \|N_{B/A}(\alpha B)\|_A = |\mathrm{Norm}_{L/K}(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| \\ \leqslant& \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |m_j||\sigma_i(\alpha_j)| \right) \\ \leqslant& m^n \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |\sigma_i(\alpha_j)| \right) \\ \leqslant& \lambda \cdot \|I\|_B.\end{aligned}$$

Isto conclui a prova do teorema quando $A = \mathbb{Z}$. Para o caso em que $A = k[x]$, veja 4.4. ■

Para o caso em que $A = k[x]$ precisamos de alguns outros conceitos que introduziremos nas duas próximas seções. A prova é dada em 4.4.

Definição 4.1.3 *Seja K um corpo de números. A ordem do grupo de classe ideal* $\mathrm{Cl}(\mathcal{O}_K)$ *é chamado de* número de classe *de K e é denotado por h_K.*

Definição 4.1.4 *Dados um corpo de números K e $\sigma : K \to \mathbb{C}$ um monomorfismo. Defina $\overline{\sigma} : K \to \mathbb{C}$, com $x \mapsto \overline{\sigma(x)}$ a conjugação complexa do monomorfismo σ. Se $\overline{\sigma} = \sigma$ diremos que σ é um* monomorfismo real*, caso contrário diremos que σ é um* monomorfismo complexo*.*

Sejam r_1 a quantidade de monomorfismos reais e r_2 a quantidade de pares de monomorfismos complexos $(\sigma, \overline{\sigma})$ de K em $\mathbb{C}$. Segue da definição anterior que $[K : \mathbb{Q}] = r_1 + 2r_2$.

Seja $\mathcal{O}_K$ um anel dos inteiros algébricos, para descrever o grupo $\mathrm{Cl}(\mathcal{O}_K)$ é importante obter cotas superiores precisas para $\lambda \in \mathbb{R}^+$ encontrado no teorema 4.1.1. O próximo teorema, devido a Minkowski, cuja demonstração pode ser encontrada em [3], página 136, apresenta uma cota muito boa para λ.

Teorema 4.1.2 *Seja K um corpo de números de grau n. Seja d_K o gerador positivo do ideal discriminante $\Delta_{\mathcal{O}_K/\mathbb{Z}}$. Então toda classe de ideais de $\mathcal{O}_K$ contém um ideal I tal que*

$$\|I\|_{\mathcal{O}_K} \leqslant \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{d_K}.$$

Segue deste teorema o importante corolário:

Corolário 4.1.1 *Seja K um corpo de números. Então existe um primo $p \in \mathbb{Z}$ tal que $\langle p \rangle$ ramifica em $\mathcal{O}_K$.*
Demonstração: *Seja $[K : \mathbb{Q}] = n$. Pelo teorema 4.1.2,*

$$\sqrt{d_K} \geqslant \frac{n!}{n^n}(\frac{4}{\pi})^{r_2} \|\langle 1 \rangle\|_{\mathcal{O}_K} = \frac{n!}{n^n}(\frac{4}{\pi})^{r_2}.$$

Assim, se $n \geqslant 2$, $d_K > 1$. Logo, pelo teorema 3.3.1, todo primo p que divide d_K ramifica em $\mathcal{O}_K$. ■

4.2 Valor Absoluto e Valorizações

Definição 4.2.1 *Seja L um corpo. A aplicação $|\cdot| : L \to \mathbb{R}_{\geqslant 0}$ é chamada um* valor absoluto *de L se:*

1. $|x| = 0 \Leftrightarrow x = 0$.
2. $|xy| = |x||y|, \forall x, y \in L$.
3. $|x + y| \leqslant |x| + |y|, \forall x, y \in L$.

A condição 3 é usualmente referida como desigualdade triangular.

Seja L é um corpo. Podemos definir um valor absoluto trivial considerando que $x \mapsto 1$ se $x \neq 0$ e $0 \mapsto 0$. Se existe σ monomorfismo de L em $\mathbb{R}$($\mathbb{C}$ respectivamente) então podemos induzir em L de maneira natural um valor absoluto dado pelo valor absoluto usual de $\mathbb{R}$($\mathbb{C}$ respectivamente).

Definição 4.2.2 *Seja L um corpo. Uma* valorização *de L é um aplicação $v : L^* \to \mathbb{Z}$ tal que:*

1. $v(xy) = v(x) + v(y), \forall x, y \in L^*$(*i.é, v é um homomorfismo de grupos*).
2. $v(x + y) \geqslant \min(v(x), v(y)), \forall x, y \in L^*$.

Estendemos v para L considerando $v(0) := +\infty$.

Observação 4.2.1 *Em geral, dado um grupo abeliano totalmente ordenado Γ, uma aplicação $v : L^* \to \Gamma$ satisfazendo as propriedades 1 e 2 da definição 4.2.2 é chamada de uma* valorização *de L. Quando $\Gamma = \mathbb{Z}$, a valorização é chamada de* valorização discreta.

Observação 4.2.2 *Sejam $v : L^* \to \mathbb{Z}$ uma valorização discreta e $n \in \mathbb{N}$. A aplicação $nv : L^* \to \mathbb{Z}$, dada por $x \mapsto nv(x)$, é também um valorização discreta. Analogamente, para cada $r \in \mathbb{R}_{\geqslant 0}$, a aplicação $rv : L^* \to \mathbb{R}$ é uma valorização de L no sentido da observação 4.2.1.*

O próximo lema estabelece uma correspondência entre os conjuntos de valorizações e valores absolutos definidos sobre um corpo.

Lema 4.2.1 *Sejam $e \in \mathbb{R}_{>1}$ e v uma valorização de L. Defina*

$$\begin{array}{rcl} |\cdot|_v : L^* & \longrightarrow & \mathbb{R}_{\geqslant 0} \\ x & \longmapsto & |x|_v := e^{-v(x)}. \end{array}$$

Considere $|0|_v = 0$. Então a aplicação $|\cdot|_v$ é um valor absoluto de L.
Demonstração: *Como foi definida, $|\cdot|_v$ satisfaz as três condições da definição 4.2.1, logo é valor absoluto.* ■

Exemplo 4.2.1 *(Valorizações P-ádicas). Sejam A um domínio de Dedekind e K seu corpo de frações. Seja $P \in \mathrm{Max}(A)$. Associamos a P uma valorização sobrejetiva $v_P : K^* \to \mathbb{Z}$ como segue: se $x \in A$, escreva a fatoração do ideal $\langle x \rangle$ como*

$$\langle x \rangle := \prod_{M \in \mathrm{Max}(A)} M^{\mathrm{ord}_M(x)}.$$

Defina $v_P(x) := \mathrm{ord}_P(x)$. Se $x = a/b$, com $a, b \in A$, então

$$v_P(x) := v_P(a) - v_P(b).$$

É fácil de verificar que v_P é um valorização de K. A valorização v_P é sobrejetiva se $P \setminus P^2 \neq \emptyset$. Observe que $v_P(x) \geqslant 0$, se $x \in A$ e $v_P(x) = 0$ se, e só se, $x \notin P$.

Fato 4.2.1 *Se P e Q são dois ideais maximais distintos de A, então as valorizações sobrejetivas v_P e v_Q são distintas. De fato, seja $x \in P \setminus (P \cap Q)$, então $v_Q(x) = 0$ enquanto $v_P(x) > 0$.*

Quando A tem quocientes finito, definimos o valor absoluto padrão *$|\cdot|_P$ associado a v_P como segue:*

$$\begin{array}{rcl} |\cdot|_P : K & \longrightarrow & \mathbb{R}_{\geqslant 0} \\ x & \longmapsto & |x|_P := \ |A/P|^{-v_P(x)}, \text{se } x \neq 0, \end{array}$$

e $|0|_P = 0$. Aqui $|A/P|$ denota a cardinalidade do corpo A/P, o qual é finito pois A tem quocientes finitos.

Sejam L um extensão finita de K e B o fecho integral de A em L. Suponha B um $A-$módulo finitamente gerado. Uma vez que B é um domínio de Dedekind, podemos

associar a cada ideal maximal $\mathfrak{P}$ de B a valorização $v_{\mathfrak{P}} : L^* \to \mathbb{Z}$. Quando A tem quocientes finitos, B também tem, assim associamos a $v_{\mathfrak{P}}$ um valor absoluto $|\cdot|_{\mathfrak{P}}$:

$$\begin{array}{rccl} |\cdot|_{\mathfrak{P}} : L & \longrightarrow & \mathbb{R}_{\geqslant 0} & \\ x & \longmapsto & |\cdot|_{\mathfrak{P}} := & |B/\mathfrak{P}|^{-v_{\mathfrak{P}}(x)}, \text{ se } x \neq 0, \end{array}$$

e $|0|_{\mathfrak{P}} = 0$. O valor absoluto $|\cdot|_{\mathfrak{P}}$ é o que chamamos anteriormente de valor absoluto padrão de L associado a $\mathfrak{P}$. Quando o domínio B é considerado independentemente do domínio A, então esse valor absoluto $|\cdot|_{\mathfrak{P}}$ é certamente o mais importante valor absoluto associado a $\mathfrak{P}$. Porém, quando B é considerado como uma extensão de A, então $|\cdot|_{\mathfrak{P}}$ tem uma grande desvantagem: ele não pode estender-se a um valor absoluto $|\cdot|_P$ de K, isto é, os valores de $|x|_P$ e $|x|_{\mathfrak{P}}$ podem ser diferentes quando $x \in K$. Isto explica o porquê é mais conveniente, quando B é obtido como uma extensão de A, associar a $v_{\mathfrak{P}}$ um valor absoluto diferente. Sejam $P := \mathfrak{P} \cap A$ e $PB = \prod_{\mathfrak{P}|P} \mathfrak{P}^{e_{\mathfrak{P}/P}}$. Defina

$$\begin{array}{rccl} |\cdot|_{\mathfrak{P}} : L & \longrightarrow & \mathbb{R}_{\geqslant 0} & \\ x & \longmapsto & \left\{ \begin{array}{ll} |x|_{\mathfrak{P}} := |A/P|^{\frac{v_{\mathfrak{P}}(x)}{e_{\mathfrak{P}/P}}} & \text{se } x \neq 0; \\ 0 & \text{se } x = 0. \end{array} \right. & \end{array}$$

Fato 4.2.2 *O valos absoluto $|\cdot|_{\mathfrak{P}}$ de L estende-se ao valor absoluto $|\cdot|_P$ de K: para todo $x \in K$, $|x|_P = |x|_{\mathfrak{P}}$. De fato, se $x \in K$, então $v_{\mathfrak{P}}(x) = e_{\mathfrak{P}/P} v_P(x)$ e assim este fato segue diretamente das definições.*

Por fim, note que

$$|\cdot|_{\mathfrak{P}} = (|\cdot|_{\mathfrak{P}})^{e_{\mathfrak{P}/P} f_{\mathfrak{P}/P}}.$$

Para simplificar nossa notação, seja $n_{\mathfrak{P}/P} := e_{\mathfrak{P}/P} \cdot f_{\mathfrak{P}/P}$.

Lema 4.2.2 *Sejam A um domínio de Dedekind, K seu corpo de frações, $L|K$ uma extensão finita e B o fecho integral de A em L tal que visto como $A-$modulo é finitamente gerado. Então*

1. *$\sum_{\mathfrak{P}|P} n_{\mathfrak{P}/P} = [L : K]$.*
2. *Seja $x \in B$. Então $v_P(\mathrm{Norm}_{L/K}(x)) = \sum_{\mathfrak{P}|P} f_{\mathfrak{P}/P} v_{\mathfrak{P}}(x)$.*
3. *Suponha que A tenha quocientes finitos. Sejam $x \in L$ e $|\cdot|_P$ o valor absoluto padrão associado a $P \in \mathrm{Max}(A)$. Então $|\mathrm{Norm}_{L/K}(x)|_P = \prod_{\mathfrak{P}|P} |x|_{\mathfrak{P}}^{n_{\mathfrak{P}/P}}$.*

Demonstração: *1- Segue do teorema 2.2.1.*

2- Escreva

$$xB := \prod_{P \in \mathrm{Max}(A)} \left(\prod_{\mathfrak{P}|P} \mathfrak{P}^{v_{\mathfrak{P}}(x)} \right).$$

Por definição,

$$N_{B/A}(xB) = \prod_{P \in \mathrm{Max}(A)} P^{\sum_{\mathfrak{P}|P} f_{\mathfrak{P}/P} v_{\mathfrak{P}}(x)}.$$

Como $N_{B/A}(xB) = \mathrm{Norm}_{L/K}(x)A$ *(veja 3.4.3), segue o resultado.*

3- Uma vez que valor absoluto e aplicação norma são funções multiplicativas, é suficiente provar para $x \in B$*. Seja* $x \in B$*, usando a fatoração de* xB *e a parte 2,*

$$\prod_{\mathfrak{P}|P} |x|_{\mathfrak{P}}^{n_{\mathfrak{P}/P}} = |A/P|^{-v_P(\mathrm{Norm}_{L/K}(x))} = |\mathrm{Norm}_{L/K}|_P,$$

que concluí a prova. ■

4.3 Valor Absoluto Arquimediano e a Fórmula do Produto

Nesta seção, estudaremos os valores absolutos de um corpo K que não são obtidos a partir de uma valorização (veja lema 4.2.1). Por definição, qualquer valor absoluto satisfaz a desigualdade triangular. Seja $|\cdot|_v$ um valor absoluto associado a uma valorização v de K. Tal valor absoluto satisfaz uma desigualdade mais forte que a desigualdade triangular. De fato, de

$$v(x+y) \geqslant \min(v(x), v(y)), \forall x, y \in K,$$

concluímos

$$|x+y|_v \leqslant \max(|x|_v, |y|_v), \forall x, y \in K. \tag{4.1}$$

Definição 4.3.1 *Uma valor absoluto de* K *que satisfaz a desigualdade 4.1 é chamado de um valor absoluto não arquimediano. Caso contrário é chamado de um valor absoluto arquimediano.*

Exemplo 4.3.1 *Seja* K *um subcorpo de* $\mathbb{C}$*. Seja* $|\cdot|$ *o valor absoluto de* K *induzido pelo valor absoluto usual de* $\mathbb{C}$*. É fácil de ver que* $|\cdot|$ *é um valor absoluto arquimediano de* K*.*

Denotaremos por $|\cdot|_\infty$ o valor absoluto usual de $\mathbb{Q}$. Seja $L|\mathbb{Q}$ um corpo de números. Sejam r_1 o número de monomorfismos reais de L e r_2 o número de pares $(\sigma, \overline{\sigma})$ consistindo dos monomorfismos complexos de L e seus conjugados. A cada monomorfismo σ, associamos o valor absoluto em L, $|x|_\sigma := |\sigma(x)|_{\mathbb{R}}$ se σ é um monomorfismo real e $|x|_\sigma := |\sigma(x)|_{\mathbb{C}}$ se σ é um monomorfismo complexo. Todos estes valores absolutos são *valores absolutos arquimedianos* de L. Cada um desse valores absolutos estende $|\cdot|_\infty$, isto é, se $x \in \mathbb{Q}$, então $|x|_\infty = |x|_\sigma$ para todo $\sigma : L \to \mathbb{C}$. A proposição a seguir mostra que os $r_1 + r_2$ valores absolutos arquimedianos definidos acima são todos distintos.

Proposição 4.3.1 *Seja $L|\mathbb{Q}$ um corpo de números. Sejam $\sigma_1, \ldots, \sigma_{r_1}$ os monomorfismos reais de L e $\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}$ os monomorfismos complexos de L. Sejam $\epsilon, c_1, \ldots, c_{r_1+r_2} \in \mathbb{R}_{\geqslant 0}$. Então existe $x \in L$ tal que*

$$c_i - \epsilon \leqslant |x|_{\sigma_i} \leqslant c_i + \epsilon, \forall i = 1, \ldots, r_1 + r_2.$$

Em particular, os valores absolutos $||_{\sigma_i}$ são todos distintos para $i = 1, \ldots, r_1 + r_2$.
Demonstração: *Se σ_j é um monomorfismo complexo e $x \in L$, então as partes reais $\mathcal{R}(\sigma_j(x))$ e imaginárias $\mathcal{I}(\sigma_j(x))$ de $\sigma_j(x)$ são:*

$$\begin{array}{rcl} \mathcal{R}(\sigma_j(x)) & := & \frac{1}{2}(\sigma_j + \overline{\sigma}_j)(x), \\ \mathcal{I}(\sigma_j(x)) & := & \frac{-i}{2}(\sigma_j + \overline{\sigma}_j)(x). \end{array}$$

Considere a aplicação $\mu : L \to \mathbb{R}^n$, onde

$$\mu(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \mathcal{R}(\sigma_{r_1+1}(x)), \mathcal{I}(\sigma_{r_1+1}(x)), \ldots, \mathcal{R}(\sigma_{r_1+r_2}(x)), \mathcal{I}(\sigma_{r_1+r_2}(x))).$$

Esta aplicação é claramente $\mathbb{Q}-$linear. Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base para L sobre $\mathbb{Q}$. Afirmamos que o conjunto $\{\mu(\alpha_1), \ldots, \mu(\alpha_n)\}$ é uma base para o $\mathbb{R}-$espaço vetorial $\mathbb{R}^n$. Para mostrar esta afirmação, é suficiente mostrar que o determinante da matriz N, cujas colunas são as transpostas dos vetores $\mu(\alpha_i), i = 1, \ldots, n$ é não nulo. Uma vez que

$$\det(N)^2 = (-1/2)^{r_2} \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$$

e $\{\alpha_1, \ldots, \alpha_n\}$ é uma base para L sobre $\mathbb{Q}$, seu determinante é não nulo e assim $\det(N) \neq 0$. Em particular, uma vez que a aplicação μ é $\mathbb{Q}-$linear, ela é injetiva.

Sejam $(c_1, \ldots, c_n) \in \mathbb{R}^n$ e $\|(c_1, \ldots, c_n)\| := (\sum_{i=1}^n c_i^2)^{1/2}$ a norma usual do $\mathbb{R}^n$. Relembre que um conjunto $S \subseteq \mathbb{R}^n$ é denso se, para todo $r \in \mathbb{R}^n$ e todo $\epsilon \in \mathbb{R}_{\geqslant 0}$ existe $s \in S$ tal que $\|r - s\| < \epsilon$. Assim, segue do fato de $\mathbb{Q}$ ser denso em $\mathbb{R}$ e do fato de $\{\mu(\alpha_1), \ldots, \mu(\alpha_n)\}$ ser uma base para $\mathbb{R}^n$ que o conjunto

$$\mu(L) := \mu(\alpha_1)\mathbb{Q} + \cdots + \mu(\alpha_n)\mathbb{Q}$$

é denso em $\mathbb{R}^n$. Sejam $c_1, \ldots, c_{r_1+r_2} \in \mathbb{R}_{\geqslant 0}$ e tome

$$c := (c_1, \ldots, c_{r_1}, \frac{c_{r_1+1}}{\sqrt{2}}, \frac{c_{r_1+1}}{\sqrt{2}}, \ldots, \frac{c_{r_1+r_2}}{\sqrt{2}}, \frac{c_{r_1+r_2}}{\sqrt{2}}) \in \mathbb{R}^n.$$

Seja $\epsilon \in \mathbb{R}_{>0}$. Uma vez que $\mu(L)$ é denso, existem $q_1, \ldots, q_n \in \mathbb{Q}$ tal que

$$\| \sum_{i=1}^{n} q_i \mu(\alpha_i) - c \| < \epsilon/\sqrt{2}.$$

Seja $x := \sum_{i=1}^{n} q_i \alpha_i$, segue que

1. *Se σ_j é real, então*

$$(\sum_{i=1}^{n} q_i \sigma_j(\alpha_i) - c_j)^2 < \epsilon^2/2.$$

   Portanto, $||x|_{\sigma_j} - c_j| \leqslant |\sigma_j(x) - c_j| < \epsilon$.

2. *Se σ_j é complexo, então*

$$|\mathcal{R}(\sigma_j(x)) - c_j/\sqrt{2}| < \epsilon/\sqrt{2} \quad e \quad |\mathcal{I}(\sigma_j(x)) - c_j/\sqrt{2}| < \epsilon/\sqrt{2}.$$

   Portanto, $|\sigma_j(x) - c_j((1+i)/\sqrt{2})|_{\mathbb{C}} < \sqrt{2}(\epsilon/\sqrt{2})$ e assim, $||x|_{\sigma_j} - c_j| < \epsilon$.

■

Definição 4.3.2 *Seja $L|\mathbb{Q}$ um corpo de números. Sejam $\mathcal{O}_L$ o anel de inteiros de L e $V(L)$ o conjunto dos valores absolutos induzidos pelos monomorfismos de L junto com todo valor absoluto não-arquimediano $|\cdot|_{\mathfrak{P}}$ de L associado ao ideal maximal $\mathfrak{P}$ de $\mathcal{O}_L$.*

Dados dois valores absolutos $w, v \in V(L)$, diremos que w divide v e escreveremos $w|v$ se v é uma extensão de w. No caso de valores absolutos $P-$ádicos, vale observar: se w corresponde a $|\cdot|_{\mathfrak{P}}$ e v corresponde a $|\cdot|_p$, então $w|v$ se, e só se, o ideal maximal $\mathfrak{P}$ de $\mathcal{O}_L$ divide o ideal $p\mathcal{O}_L$.

Lembre da definição de $n_{\mathfrak{P}/\langle p \rangle}$ dada em 4.2.1. A seguir faremos uma definição análoga no caso de valores absolutos arquimedianos. Seja $|\cdot|_w$ um valor absoluto arquimediano de L, pela construção, $|\cdot|_w$ estende $|\cdot|_\infty$. Defina

$$n_{w/\infty} := \begin{cases} 1, & \text{se } |\cdot|_w = |\cdot|_\sigma, \text{ com } \sigma \text{ um monomorfismo real;} \\ 2, & \text{se } |\cdot|_w = |\cdot|_\tau, \text{ com } \tau \text{ um monomorfismo complexo.} \end{cases}$$

Em geral, usaremos a notação $n_{w/v}$ para os inteiros definidos acima e no exemplo 4.2.1.

O lema a seguir é um resultado análogo ao lema 4.2.2, para valores absolutos aquimedianos.

Lema 4.3.1 *Seja $L|\mathbb{Q}$ um corpo de números. Então $\sum_{v|\infty} n_{v/\infty} = [L:\mathbb{Q}]$. Além disso, se $x \in L$ e $|\cdot|_\infty$ o valor absoluto arquimediano de $\mathbb{Q}$, então*

$$|\mathrm{Norm}_{L/\mathbb{Q}}(x)|_\infty = \prod_{v|\infty; v\in V(L)} |x|_v^{n_{v/\infty}}.$$

Demonstração: *A primeira afirmação segue diretamente da definição de $n_{v/\infty}$. Para a segunda igualdade, note que*

$$\mathrm{Norm}_{L\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x), \forall x \in L.$$

Observe também que $|x|_\infty = |x|_{\mathbb{C}}$, para todo $x \in \mathbb{Q}$ e $|x|_{\mathbb{R}} = |x|_{\mathbb{C}}$, para todo $x \in \mathbb{R}$. Portanto,

$$\begin{aligned}
|\mathrm{Norm}_{L/K}(x)|_\infty =& |\mathrm{Norm}_{L/K}(x)|_{\mathbb{C}} \\
=& \prod_{\sigma \text{ real}} |\sigma(x)|_{\mathbb{R}} \cdot \prod_{\substack{(\tau,\overline{\tau}) \\ \tau \text{ complexo}}} |\tau(x)|_{\mathbb{C}} \cdot |\overline{\tau}(x)|_{\mathbb{C}} \\
=& \prod_{\sigma \text{ real}} |x|_\sigma \cdot \prod_{\substack{(\tau,\overline{\tau}) \\ \tau \text{ complexo}}} |x|_\tau^2.
\end{aligned}$$

■

Com a notação introduzida na definição 4.3.2, os lemas 4.2.2 e 4.3.1 implicam que, dado $v \in V(\mathbb{Q})$ e $x \in L$,

$$|\mathrm{Norm}_{L/\mathbb{Q}}(x)|_v = \prod_{w|v; w\in V(L)} |x|_w^{n_{w/v}}.$$

Proposição 4.3.2 (Fórmula do produto para corpo de números) *Sejam L um corpo de números e $x \in L^*$. Então $\prod_{w\in V(L)} |x|_w^{n_{w/v}} = 1$.*

Demonstração: *Primeiro observe que dado $x \in L^*$, $|x|_v \neq 1$ para um número finita de $v \in V(L)$. De fato, escreva $x = a/b$ com $a, b \in \mathcal{O}_L$. Como o número de ideais maximais $\mathfrak{P}$ de $\mathcal{O}_L$ que contém a ou b é finito, $|x|_{\mathfrak{P}} = |a|_{\mathfrak{P}}|b|_{\mathfrak{P}}^{-1} \neq 1$ para um número finito de ideais maximais de $\mathcal{O}_L$. Se $L = \mathbb{Q}$, escreva $x = \pm\prod_{p \text{ primo}} p^{v_p(x)}$, então $|x|_p = p^{-v_p(x)}$ e $|x|_\infty = \prod_p p^{v_p(x)}$. Logo, $\prod_{v\in V(\mathbb{Q})} |x|_v = 1$. No caso geral,*

$$\prod_{w\in V(L)} |x|_w^{n_{w/v}} = \prod_{v\in V(\mathbb{Q})} \Big(\prod_{\substack{w|v \\ w\in V(L)}} |x|_w^{n_{w/v}} \Big) = \prod_{v\in V(\mathbb{Q})} |\mathrm{Norm}_{L/\mathbb{Q}}(x)|_v = 1.$$

■

Observação 4.3.1 *Um valor absoluto num corpo L induz uma métrica. Diremos que dois valores absolutos de L são equivalentes se eles induzem a mesma topologia em L. Se L é um corpo de números, então pode-se mostrar que o conjunto $V(L)$ contém um e somente um representante de cada classe de equivalência de valores absolutos de L.*

4.4 Corpos de Funções

Nas duas últimas seções, formalizamos algumas ferramentas usadas na prova do teorema 4.1.1 para o caso de corpos de números. O objetivo desta seção é provar o teorema 4.1.1 para o caso de corpos de funções sobre um corpo finito, que é similar ao caso de corpos de números. De fato, definiremos a seguir a valorização v_∞ de $k(x)$ que é diferente de todas as valorizações $P-$ádicas associadas a um ideal maximal de $k[x]$. Iremos então estender essa valorização para uma extensão finita de $k(x)$. Veremos ainda que tal extensão possui um *fórmula do produto* análoga a fórmula do produto para os corpos de números (4.3.2).

Sejam k um corpo e $k(x)$ o corpo das funções racionais em uma variável. Para $r = f/g \in k(x)^*$, definimos o grau de r por $\deg(r) := \deg(f) - \deg(g)$ e por convenção $\deg(0) := +\infty$.

Dado $h \in k[x]$ mônico e irredutível, a valorização v_h é dada pela valorização $P-$ádica, onde $P = \langle h \rangle \in \mathrm{Max}(k[x])$. Uma valorização que não é igual a nenhuma valorização $P-$ádica é v_∞, definida por

$$\begin{array}{rccc} v_\infty : k(x) \setminus \{0\} & \longrightarrow & \mathbb{Z} \\ r & \longmapsto & -\deg(f). \end{array}$$

Fato 4.4.1 *As valorização v_P e v_∞ são distintas, onde $P = \langle f \rangle \in \mathrm{Max}(k[x])$. De fato, $v_P(f) = 1$ e $v_\infty(f) = -\deg(f) < 0$. Além disso, $v_Q(f) = 0$, se $Q \in \mathrm{Max}(k[x])$ e $Q \neq P$.*

Quando k é um corpo finito com q elementos, associamos a valorização v_∞ de $k(x)$ o valor absoluto $|f|_\infty := q^{-v_\infty(f)} = q^{\deg(f)}$.

Lema 4.4.1 *Seja k um corpo. Então $v_\infty = v_P$, onde $P := \langle 1/x \rangle k[1/x] \trianglelefteq k[1/x]$.*
Demonstração: *Considere a inclusão $k[1/x] \subseteq k(1/x) = k(x)$. O anel $k[1/x]$ é um domínio de ideais principais com corpo de frações $k(x)$. Seja $f(x) = \sum_{i=0}^{\deg(f)} a_i x^i \in k[x]$, $a_{\deg(f)} \neq 0$. Uma vez que $k(x)$ é o corpo de frações de $k[1/x]$, podemos escrever $f = g(1/x)/h(1/x)$, onde $g(1/x), h(1/x) \in k[1/x]$:*

$$\begin{array}{rcl} f(x) & = & \left(\frac{1}{x}\right)^{-\deg(f)} \left(\sum_{i=0}^{\deg(f)} a_i \frac{1}{x^{\deg(f)-i}} \right) \\ & = & \frac{a_{\deg(f)} + a_{\deg(f)-1}(\frac{1}{x}) + \cdots + a_0(\frac{1}{x})^{\deg(f)}}{(\frac{1}{x})^{\deg(f)}}. \end{array}$$

É claro que $(1/x) \nmid a_{\deg(f)} + a_{\deg(f)-1}(1/x) + \cdots + a_0(1/x)^{\deg(f)}$ *em* $k[1/x]$. *Assim, segue da definição de valorização* $P-$*ádica (4.2.1) para a valorização* v_P *associada a* $P := \langle 1/x \rangle$ *que*

$$\begin{aligned} v_P(f) := \mathrm{ord}_P(f) &= \mathrm{ord}_P(a_{\deg(f)} + a_{\deg(f)-1}(\tfrac{1}{x}) + \cdots + a_0(\tfrac{1}{x})^{\deg(f)}) - \mathrm{ord}_P((\tfrac{1}{x})^{\deg(f)}) \\ &= -\mathrm{ord}_P((1/x)^{\deg(f)}) = -\deg(f) = v_\infty(f). \end{aligned}$$

Portanto, $v_P = v_\infty$. ■

Para mostrar que $|\cdot|_\infty = |\cdot|_P$, basta notar que $k[1/x]/P \cong k$. Portanto, quando $\#k = q, |f|_P := q^{-v_P(f)} = |f|_\infty$.

Seja $L|k(x)$ um grau finito. Determinaremos o conjunto de valores absolutos $\{|\cdot|_i; i = 1, \ldots, s\}$ de L que estendem o valor absoluto $|\cdot|_\infty$ de $k(x)$. Observe que pelo lema anterior v_∞ é igual a valorização v_P, onde $P := \langle 1/x \rangle \in \mathrm{Max}(k[1/x])$. Assim, primeiramente encontraremos as valorizações de L associadas a v_∞. Estas valorizações existem mesmo quando k não é um corpo finito, como veremos a seguir. Seja B' o fecho integral de $k[1/x]$ em L. Suponha B' finitamente gerado como $k[1/x]-$modulo. Então B' é de Dedekind e podemos fatorar o ideal $(1/x)B'$ em produto de ideais maximais

$$(1/x)B' = \mathfrak{P}_1^{e_{\mathfrak{P}_1}/P} \cdots \mathfrak{P}_s^{e_{\mathfrak{P}_s}/P}.$$

Seja $v_{\mathfrak{P}_i}$ a valorização de L associada a $\mathfrak{P}_i$. Quando k é finito, B' tem quocientes finitos. Assim, denote por $|\cdot|_{\mathfrak{P}_i}$ os valores absolutos associados a $v_{\mathfrak{P}_i}, i = 1, \ldots, s$. O fato 4.2.2 mostra que cada vamos absoluto $|\cdot|_{\mathfrak{P}_i}$ de L estende o valor absoluto $|\cdot|_\infty = |\cdot|_P$ de $k(x)$. Seja

$$n_{\mathfrak{P}_i/P} = n_i := e_{\mathfrak{P}_i/P} \cdot f_{\mathfrak{P}_i/P}.$$

Pelo teorema 2.2.1, $\sum_{i=1}^s n_{\mathfrak{P}_i/P} = [L : k(x)]$. O lema 4.2.2 implica que para todo $\alpha \in B, |\mathrm{Norm}_{L/k(x)}(\alpha)|_\infty = \prod_{i=1}^s |\alpha|_{\mathfrak{P}_i}^{n_i}$. O fato 4.2.1 mostra que as valorizações $v_{\mathfrak{P}_i}$ são todas distintas.

Fato 4.4.2 *Sejam* $\mathfrak{P} \in \mathrm{Max}(B)$ *e* $i \in \{1, \ldots, s\}$. *Então* $v_{\mathfrak{P}_i} \neq v_{\mathfrak{P}}$. *De fato,*

$$(v_{\mathfrak{P}})_{|_{k[x]}} = e_{\mathfrak{P}/(\mathfrak{P}\cap k[x])} \cdot v_{\mathfrak{P}\cap k[x]} \quad e \quad (v_{\mathfrak{P}_i})_{|_{k[x]}} = e_{\mathfrak{P}_i/P} \cdot v_P.$$

Seja $f \in k[x]$ *um gerador de* $\mathfrak{P} \cap k[x]$. *Então*

$$v_{\mathfrak{P}}(f) = e_{\mathfrak{P}/(\mathfrak{P}\cap k[x])} \quad e \quad v_{e_{\mathfrak{P}/(\mathfrak{P}\cap k[x])} \cdot v_{\mathfrak{P}_i}(f)} = -\deg(f) \cdot e_{\mathfrak{P}_i/P} < 0.$$

Definição 4.4.1 *Sejam* k *um corpo finito e* $L|k(x)$ *finita. Seja* $V(L)$ *o conjunto consistindo de todos os valores absolutos* $|\cdot|_{\mathfrak{P}}$ *de* L *associados aos ideais maximais* $\mathfrak{P}$

de B, e os valores absolutos $|\cdot|_{\mathfrak{P}_i}, i = 1, \ldots, s$ que estendem o valor absoluto $|\cdot|_\infty$ de $k(x)$.

Note que quando L é um extensão finita de $k(x)$ e k é um corpo finito, o conjunto $V(L)$ consiste inteiramente de valores absolutos que são obtidos de valorizações de L. Quando L é um corpo de números, o conjunto $V(L)$ contém valores absolutos arquimedianos e assim, não consiste inteiramente de valores absolutos provenientes de valorizações.

Denotaremos um elemento de $V(L)$ por $|\cdot|_w$ ou simplesmente por w. Se $|\cdot|_w$ estende um valor absoluto $|\cdot|_v$ de $k(x)$, diremos que w divide v e denotaremos $w|v$. Se $|\cdot|_w = |\cdot|_{\mathfrak{P}}$ para algum $\mathfrak{P} \in \mathrm{Max}(B)$, considere $|\cdot|_v = |\cdot|_{\mathfrak{P}\cap k[x]}$ e $n_{w/v} = n_{\mathfrak{P}/\mathfrak{P}\cap k[x]}$. Analogamente, se $|\cdot|_w = |\cdot|_{\mathfrak{P}_i}$ para algum $i = 1, \ldots, s$, então $v = \infty$ e $n_{w/v} = n_{\mathfrak{P}_i/P}$. Com essa notação, o lema 4.2.2 afirma que, para todo $w \in V(L)$ e para todo $\alpha \in B$,

$$|\mathrm{Norm}_{L/k(x)}(\alpha)|_v = \prod_{w|v} |\alpha|_w^{n_{w/v}}.$$

Lema 4.4.2 (Fórmula produto para $\mathbb{F}_q(x)$) *Seja $f \in \mathbb{F}_q(x)^*$. Então $\prod_{v\in V(\mathbb{F}_q(x))} |f|_v = 1$.*
Demonstração: *Veja [6], página 177.*

Proposição 4.4.1 (Fórmula produto para corpos de funções sobre corpos finitos) *Sejam k um corpo finito, $L|k(x)$ uma extensão finita e $f \in L^*$. Então $\sum_{w\in V(L)} |f|_w^{n_{w/v}} = 1$.*
Demonstração: *Sejam B e B' os fechos integrais de $k[x]$ e $k[1/x]$ respectivamente. Suponha que B e B' são finitamente gerados como $k[x]$ e $k[1/x]-$modulo respectivamente. Esta hipótese adicional vale em geral, o caso em que $L|k(x)$ é separável (veja 1.3.1), o caso geral é mostrado em 8. Seja $f \in L^*$, então*

$$\begin{aligned}\sum_{w\in V(L)} |f|_w^{n_{w/v}} &= \prod_{v\in V(k(x))} \Big(\prod_{\substack{w|v \\ w\in V(L)}} |f|_w^{n_{w/v}} \Big) \\ &\overset{\text{lema 4.2.2}}{=} \prod_{v\in V(k(x))} |\mathrm{Norm}_{L/K}(f)|_v \\ &\overset{\text{lema 4.4.2}}{=} 1.\end{aligned}$$

■

Corolário 4.4.1 *Seja $|\cdot|_{\mathfrak{P}_i}, i = 1, \ldots, s$ os valores absolutos de L que estendem $|\cdot|_\infty$. Se $f \in B \setminus \{0\}$, então $\|\langle f\rangle\|_B = \prod_{i=1}^s |f|_{\mathfrak{P}_i}^{n_i}$.*
Demonstração: *Seja $f \in B$ não nulo e considere a fatoração $fB := \prod_{M\in \mathrm{Max}(B)} M^{v_M(f)}$.*

Por definição,

$$\|\langle f\rangle\|_B = |B/fB| = \prod_{M\in \mathrm{Max}(B)} |B/M|^{v_M(f)} = \frac{1}{\prod\limits_{M\in \mathrm{Max}(B)} |f|_M^{n_{M/M\cap k[x]}}}.$$

Portanto, o resultado segue imediatamente da proposição anterior. ■

Finalizaremos agora a prova do teorema 4.1.1 para o caso de corpos de funções. Sejam k um corpo de ordem q, $A = k[x]$, K o corpo de frações de A e $L|K$ uma extensão de grau n. Suponha que os fechos integrais B e B' de $k[x]$ e $k[1/x]$ são finitamente gerados como $k[x]$ e $k[1/x]-$modulos, respectivamente. Sejam $|\cdot|_i := |\cdot|_{\mathfrak{P}_i}, i = 1, \ldots, s$ valores absolutos de L que estendem o valor absoluto $|\cdot|_\infty$ de K (como em 4.4.1). Sejam $n_i := n_{\mathfrak{P}_i/P}, i = 1, \ldots, s$ as multiplicidades associadas. Uma vez que A é um domínio de ideais principais, podemos escolher uma base $\{\alpha_1, \ldots, \alpha_n\}$ para B sobre A. Seja

$$\lambda := \prod_{i=1}^{s} \Big(\sum_{j=1}^{n} |\alpha_j|_i \Big)^{n_i}.$$

Mostraremos que todo $0 \neq I \trianglelefteq B$ possui um elemento não nulo α tal que $\|\langle\alpha\rangle\|_B \leqslant \lambda \|I\|_B$. Sejam $0 \neq I \trianglelefteq B$ e $d \geqslant 0$ o único inteiro tal que $(q^d)^n \leqslant \|I\|_B < (q^{d+1})^n$. Uma vez que $(q^{d+1})^n > \|I\|_B = |B/I|$, concluímos que dois dos $(q^{d+1})^n$ elementos distintos de B da forma $\sum_{i=1}^{n} m_i\alpha_i$, com $m_i \in A$ e $|m_i|_\infty \leqslant q^d$, são congruentes módulo I. Portanto, o ideal I contém um elemento α da forma

$$\alpha = \sum_{i=1}^{n} m_i\alpha_i, \quad \text{com } m_i \in A \text{ e } |m_i|_\infty \leqslant q^d.$$

Pelo corolário 4.4.1 e as propriedades de valor absoluto, concluímos

$$\begin{aligned}
\|\langle\alpha\rangle\|_B &= \prod_{i=1}^{s} |\alpha|_i^{n_i} \\
&\leqslant \prod_{i=1}^{s} \Big(\sum_{j=1}^{n} |m_j\alpha_j|_i\Big)^{n_i} = \prod_{i=1}^{s} \Big(\sum_{j=1}^{n} |m_j|_\infty \cdot |\alpha_j|_i\Big)^{n_i}\Big) \\
&\leqslant (q^d)^{\sum_{i=1}^{s} n_i} \cdot \prod_{i=1}^{s} \Big(\sum_{j=1}^{n} |\alpha_j|_i\Big)^{n_i} = (q^d)^n \cdot \lambda \\
&\leqslant \|I\|_B \cdot \lambda.
\end{aligned}$$

Logo o teorema 4.1.1 está provado quando L é um corpo de funções sobre um corpo finito.

Capítulo

5

Curvas Projetivas e Completas

Neste capítulo estudaremos o aspecto geométrico da teoria desenvolvida nos capítulos anteriores. Comçaremos com curvas projetivas planas e curvas completas não-singulares.

Definição 5.0.2 *Seja $F \in k[X,Y,Z]$ homogêneo de grau d. O conjunto*

$$X_F(\overline{k}) := \{(a:b:c) \in \mathbb{P}^2(\overline{k}) | F(a,b,c) = 0\}$$

é chamado de curva projetiva plana. *O conjunto $X_F(k)$ é chamado de* conjunto dos pontos com coordenadas em k *ou conjunto dos* $k-$pontos racionais *da curva projetiva plana definida por F.*

Definição 5.0.3 *Seja F polinômio homogêneo de grau d. Um ponto $(a:b:c) \in X_F(\overline{k})$ é* um ponto não singular *se*

$$\text{grad}(F)(a,b,c) := \left(\frac{\partial F}{\partial X}(a,b,c), \frac{\partial F}{\partial Y}(a,b,c), \frac{\partial F}{\partial Z}(a,b,c)\right) \neq (0,0,0).$$

Lembramos que dada uma curva definida por F, sua parte afim é definida pelo conjunto dos zeros de $f(X,Y) := F(X,Y,1)$. O próximo lema estabelece a relação entre os pontos não singulares das curvas definidas por F e f.

Lema 5.0.3 *Um ponto $P = (a:b:c) \in X_F(\overline{k})$ com $c \neq 0$ é não singular se, e somente se, o ponto $(\frac{a}{c}, \frac{b}{c})$ é um ponto não singular da curva afim $Z_f(\overline{k})$.*

O resultado acima é valido *mutatis-mutandis* se $a \neq 0$ ou $b \neq 0$. Ainda, nos será útil o seguinte resultado:

Proposição 5.0.2 *Sejam k um corpo com característica diferente de dois e $F \in k[X,Y,Z]$ homogêneo de grau dois. Suponha que $X_F(\overline{k})$ é uma curva suave. Então existe $\varphi \in \mathrm{GL}_3(k)$ tal que $\varphi_{\mathbb{P}}$ induz uma bijeção entre $X_F(\overline{k})$ e a cônica na forma padrão dada pela equação $b_0X^2 + b_1Y^2 + b_2Z^2 \in k[X,Y,Z]$ com $b_0b_1b_2 \neq 0$. Além disso, se $\sqrt{b_0}, \sqrt{b_1}, \sqrt{b_2} \in k$, então existe $\psi \in \mathrm{GL}_3(k)$ tal que $\psi_{\mathbb{P}}$ induz uma bijeção entre $X_F(\overline{k})$ e a cônica dada por $X^2 + Y^2 + Z^2 = 0$.*

Para a demonstração veja [6], pág. 206.

5.1 Funções em um Curva Projetiva

Sejam $F \in \overline{k}[X,Y,Z]$ irredutível e homogêneo e $X_F(\overline{k})$ a curva projetiva associada. Pela irredutibilidade de F, $R := \overline{k}[X,Y,Z]/\langle F\rangle$ é um domínio. Seja K seu corpo de frações. Por simplicidade denotaremos simplesmente por G a classe de G em R.

Definição 5.1.1 *O* corpo das funções racionais *sobre $X_F(\overline{k})$ é $\overline{k}(X_F) := K$. Um elemento $\psi \in \overline{k}(X_F)$ é chamada de* função racional em $X_F(\overline{k})$. *Diremos que $\psi = \frac{G}{H}, (G,H) = 1$* está definida em $P \in X_F(\overline{k})$ *se $H(P) \neq 0$. Denotaremos o conjunto destes pontos por* $\mathrm{dom}(\psi)$.

Se $\psi = \frac{G}{H}$ e $(H,F) = 1$, então $\mathrm{dom}(\psi) = X_F(\overline{k}) \setminus X_H(\overline{k})$, portanto $\mathrm{dom}(\psi)$ é um subconjunto aberto(na topologia de Zariski) de $X_F(\overline{k})$. Um ponto $P \in X_F(\overline{k})$ é chamado do *polo* de ψ se $P \in X_F(\overline{k}) \setminus \mathrm{dom}(\psi)$. Dado $P \in X_F(\overline{k})$, defian

$$\mathcal{O}_P := \{\psi \in \overline{k}(X_F) | \psi \text{ está definida em } P\}.$$

Lema 5.1.1 *$\mathcal{O}_P$ é um anel local cujo ideal maximal, $\mathcal{M}_P$, é dado pelas funções racionais que se anulam em P.*
Demonstração: *É fácil ver que $\mathcal{O}_P$ é um anel. Uma vez que toda função em $\mathcal{O}_P$ que não se anula em P, possui inverso, concluímos que $\mathcal{M}_P$ é o único ideal maximal de $\mathcal{O}_P$.* ■

Lema 5.1.2 *Sejam $F \in \overline{k}[X,Y,Z]$ homogêneo e irredutível e $P, Q \in X_F(\overline{k})$ distintos. Então existe uma função $\psi \in \overline{k}(X_F)$ definida em P e Q que se anula em P mas não em Q. Em particular, $\mathcal{O}_P \neq \mathcal{O}_Q$ e não existe um domínio local $\mathcal{O} \subseteq \overline{k}(X_F)$ com ideal maximal $\mathcal{M}$ tal que $\mathcal{O} \supseteq \mathcal{O}_P \cup \mathcal{O}_Q$ e $\mathcal{M} \supseteq \mathcal{M}_P \cup \mathcal{M}_Q$.*
Demonstração: *Sejam $P = (a_0 : a_1 : a_2)$ e $Q = (b_0 : b_1 : b_2)$. Então os vetores $(a_0, a_1, a_2), (b_0, b_1, b_2)$ são linearmente independentes em $\overline{k}^3$. Sem perda de generalidade,*

seja $a_0b_1 - a_1b_0 \neq 0$. *Uma vez que* $P \neq Q \in X_F(\overline{k})$, $a_0Y - a_1X \nmid F$. *Tome uma reta projetiva* $X_\ell(\overline{k})$ *tal que* $P, Q \notin X_\ell(\overline{k})$ *e defina*

$$\psi := \frac{a_0Y - a_1X}{\ell} \in \overline{k}(X_F).$$

Claramente ψ *está definida em* P *e* Q, *e por construção* $\psi \in \mathcal{M}_P$ *e* $\psi \notin \mathcal{M}_Q$. *Como* ψ *é inversível em* $\mathcal{O}_Q$ *mas não é em* $\mathcal{O}_P$, *logo* $\mathcal{O}_P \neq \mathcal{O}_Q$.

Se existe $\mathcal{O} \supseteq \mathcal{O}_Q$, *então* ψ *é inversível em* $\mathcal{O}$ *e assim* $\psi \notin \mathcal{M}$. *Uma vez que* $\psi \in \mathcal{M}_P$, *então* $\psi \in \mathcal{M}$, *absurdo.* ■

Sejam $U \subseteq X_F(\overline{k})$ um aberto e $\mathcal{O}(U) := \bigcap_{P \in U} \mathcal{O}_P$. O conjunto $\mathcal{O}(U)$ é um anel chamado do *anel das funções definidas em* U. Note que se $P \in U$, então $\mathcal{O}(U) \subseteq \mathcal{O}_P \subseteq \overline{k}(X_F)$.

Seja $f(x, y) = F(X, Y, 1)$. Pode-se dar uma bijeção entre o conjunto $U := X_F(\overline{k}) \setminus X_Z(\overline{k})$ e a curva afim $Z_f(\overline{k})$, onde $X_Z(\overline{k})$ é dada por $Z = 0$. Identificamos em 0.2.1 o domínio $\overline{C}_f$ como o anel das funções em $Z_f(\overline{k})$ e $\overline{k}(Z_f)$ o corpo das funções racionais sobre $Z_f(\overline{k})$. Se $P \in U$, então P corresponde a um ponto em $Z_f(\overline{k})$ e assim ao ideal maximal M_P de $\overline{C}_f$. O anel local $(\overline{C}_f)_{M_P}$ é identificado como o anel das funções racionais em $Z_f(\overline{k})$ definidas em P, assim

$$\overline{C}_f \subseteq (\overline{C}_f)_{M_P} \subseteq \overline{k}(Z_f).$$

É natural perguntarmos se os corpos $\overline{k}(X_F)$ e $\overline{k}(Z_f)$ são isomorfos e similarmente, se os domínios $\mathcal{O}(U)$ e $\mathcal{O}_P$ são isomorfos a $\overline{C}_f$ e $(\overline{C}_f)_{M_P}$ respectivamente. A resposta para esta pergunta é positiva. Considere a bijeção

$$\begin{array}{rccc} \varphi_Z : & Z_f(\overline{k}) & \longrightarrow & X_F(\overline{k}) \setminus X_Z(\overline{k}) \\ & (a, b) & \longmapsto & (a : b : 1) \end{array}.$$

Observação 5.1.1 *Claramente poderíamos considerar os híperplanos* $X = 0$ *ou* $Y = 0$, *tomar* $U := X_F(\overline{k}) \setminus X_X(\overline{k})$ *ou* $X_F(\overline{k}) \setminus X_Y(\overline{k})$ *e proceder normalmente.*

Proposição 5.1.1 *Com as notações e suposições acima, a aplicação* φ_Z *induz um isomorfismo de corpos*

$$\begin{array}{rccc} \varphi_Z^* : \overline{k}(X_F) & \longrightarrow & \overline{k}(Z_f) \\ \frac{\text{classe de } G}{\text{classe de } H} & \longmapsto & \frac{\text{classe de } G(x,y,1)}{\text{classe de } H(x,y,1)}. \end{array}$$

As imagens de $\mathcal{O}(U)$ *e* $\mathcal{O}_P$ *por* φ_Z^* *são os domínios* $\overline{C}_f$ *e* $(\overline{C}_f)_{M_P}$ *respectivamente. Em particular,* P *é um ponto não singular da curva* $X_F(\overline{k})$ *se, e somente se,* $\mathcal{O}_P$ *é um domínio local de ideais principais.*

Demonstração: *É fácil ver que* φ_Z^* *está bem definida, é um homomorfismo de corpos,*

logo injetivo, e $\varphi_Z^*|_{\overline{k}} = \mathrm{id}_{\overline{k}}$. *Para a sobrejetividade, sejam* $\beta = \frac{\text{classe de } g(x,y)}{\text{classe de } h(x,y)} \in \overline{k}(Z_f)$ *e* $m := \max(\deg(g), \deg(h))$. *Tome*

$$\alpha = \frac{\text{classe de } Z^{m-\deg(g)}g(X/Z, Y/Z)}{\text{classe de } Z^{m-\deg(h)}h(X/Z, Y/Z)} \in \overline{k}(X_F),$$

então $\varphi_Z^*(\alpha) = \beta$.

Para $\varphi_Z^*(\mathcal{O}_P) = (\overline{C}_f)_{M_P}$, *seja* $P = (a_0 : a_1 : a_2) \in X_F(\overline{k}) \setminus X_Z(\overline{k})$, *então* $P = \varphi_Z(\frac{a_0}{a_2}, \frac{a_1}{a_2})$. *O ideal* M_P *em* $\overline{C}_f$ *é gerado por* $x - \frac{a_0}{a_2}$ *e* $y - \frac{a_1}{a_2}$. *Seja* $\psi \in \mathcal{O}_P$, *escreva* $\psi = G/H$. *Como* $H(a_0, a_1, a_2) \neq 0$, *então o polinômio* $H(x, y, 1)$ *não se anula em* $(\frac{a_0}{a_2}, \frac{a_1}{a_2})$ *e assim,* $H(x, y, 1) \in \overline{C}_f \setminus M_P$. *Logo,* $\varphi_Z^*(G/H) \in (\overline{C}_f)_{M_P}$. *Agora seja* $g/h \in (\overline{C}_f)_{M_P}$, *então* $h(\frac{a_0}{a_2}, \frac{a_1}{a_2}) \neq 0$. *Sejam* $g(x, y), h(x, y) \in \overline{k}[x, y]$ *cujas classes são* g *e* h *em* $(\overline{C}_f)_{M_P}$, *tome* $m = \max(\deg(g), \deg(h))$. *O polinômio* $Z^{m-\deg(h)}h(\frac{a_0}{a_2}, \frac{a_1}{a_2})$ *não se anula em* P, *assim* $\frac{g}{h} \in \varphi_Z^*(\mathcal{O}_P)$. *Portanto* $\varphi_Z^*(\mathcal{O}_P) = (\overline{C}_f)_{M_P}$.

A igualdade $\overline{C}_f = \bigcap_{M \in \mathrm{Max}(A)} (\overline{C}_f)_M$ *é satisfeita, veja 0.1.2. Uma vez que os maximais de* $\overline{C}_f$ *estão e bijeção com os pontos de* $Z_f(\overline{k})$, *logo estão em bijeção com os pontos* U. *Assim,*

$$\varphi_Z^*(\mathcal{O}(U)) = \bigcap_{M \in \mathrm{Max}(A)} (\overline{C}_f)_M = \overline{C}_f.$$

O ponto P *é não singular em* $X_F(\overline{k})$ *se, e só se,* $(\frac{a_0}{a_2}, \frac{a_1}{a_2})$ *é um ponto não singular de* $Z_f(\overline{k})$. *O ponto* $(\frac{a_0}{a_2}, \frac{a_1}{a_2})$ *é não singular em* $Z_f(\overline{k})$ *se, e só se, o anel* $(\overline{C}_f)_{M_P}$ *é um domínio local principal (veja 0.2.3). Uma vez que* $(\overline{C}_f)_{M_P} \cong \mathcal{O}_P$ *a proposição está provada.* ■

5.2 Curvas Projetivas e Valorizações

Sejam $F \in \overline{k}[X, Y, Z]$ irredutível e homogêneo, $\mathcal{V}(\overline{k}(X_f)/\overline{k})$ o conjunto das valorizações v sobrejetivas de $\overline{k}(X_f)$ tal que $v(\overline{k}^*) = \{0\}$ e $\mathcal{P}(\overline{k}(X_f)/\overline{k})$ o conjunto dos domínios locais principais $\mathcal{O} \subseteq \overline{k}(X_f)$ que contém $\overline{k}$ e cujo corpo de frações seja $\overline{k}(X_f)$. Mostraremos em 5.3.1 que a aplicação

$$\begin{array}{ccc} \mathcal{V}(\overline{k}(X_f)/\overline{k}) & \longrightarrow & \mathcal{P}(\overline{k}(X_f)/\overline{k}) \\ v & \longmapsto & \mathcal{O}_v := \{\psi \in \overline{k}(X_F)^* | v(\psi) \geqslant 0\} \cup \{0\} \end{array}$$

é uma bijeção e que $\overline{k}(X_f)$ é, de fato, o corpo de frações de $\mathcal{O}_v$.

A seguir estudaremos a relação entre os pontos de uma curva projetiva não singular e as valorizações de seu corpo de funções racionais. Sejam $X_F(\overline{k})$ uma curva plana projetiva não singular e $P \in X_F(\overline{k})$. O anel $\mathcal{O}_P \subseteq \overline{k}(X_F)$ é um domínio local de ideais principais.

Seja $\mathcal{M}_P = \langle \pi \rangle$ seu ideal maximal. A aplicação $v_P : \overline{k}(X_F)^* \to \mathbb{Z}$, $\psi \mapsto v_P(\psi) = \mathrm{ord}_\pi(\psi)$ (veja 4.2.1) é uma valorização sobrejetora tal que $\mathcal{O}_{v_P} = \mathcal{O}_P$.

Teorema 5.2.1 *Seja $X_F(\overline{k})$ uma curva plana projetiva não singular. Então as aplicações*

$$\begin{array}{ccccc} X_F(\overline{k}) & \xrightarrow{I_{\overline{k}}} & \mathcal{V}(\overline{k}(X_f)/\overline{k}) & \longrightarrow & \mathcal{P}(\overline{k}(X_f)/\overline{k}) \\ P & \longmapsto & v_P & \longmapsto & \mathcal{O}_P \end{array}$$

são bijeções.

Demonstração: *A bijetividade da aplicação $v_P \mapsto \mathcal{O}_P$ segue de 5.3.1. Seja $P \in X_F(\overline{k})$ não singular, pela proposição 5.1.1 $\mathcal{O}_P$ é um domínio local de ideais principais que contém $\overline{k}$. Logo a aplicação $I_{\overline{k}}$ está bem definida. A injetividade da aplicação $I_{\overline{k}}$ segue do lema 5.1.2. Para a sobrejetividade de $I_{\overline{k}}$ veja [6], página 217.* ■

5.3 Curva Completa Não Singular

Sejam K um corpo e $v : K^* \to (\Gamma, +, \geqslant)$ uma valorização no sentindo da observação 4.2.1. Considere

$$\mathcal{O}_v := \{\alpha \in K^* | v(\alpha) \geqslant 0\} \cup \{0\} \quad \text{e} \quad \mathcal{M}_v := \{\alpha \in K^* | v(\alpha) > 0\} \cup \{0\}.$$

Segue das propriedade das valorizações que $\mathcal{O}_v$ é um anel local de ideais principais e $\mathcal{M}_v$ seu ideal maximal. O corpo $k_v := \mathcal{O}_v/\mathcal{M}_v$ é chamado de corpo residual. Quando $\Gamma = \mathbb{Z}$, $\mathcal{O}_v$ é chamado de *anel de valorização discreta*.

Proposição 5.3.1 *Sejam K um corpo e $v : K^* \to \mathbb{Z}$ uma valorização não-trivial. Então $\mathcal{O}_v$ é um domínio local de ideais principais. Além disso, v é unicamente determinada pelo valor $v(\pi)$, onde $\langle \pi \rangle = \mathcal{M}_v$. Ainda, a aplicação $v \mapsto \mathcal{O}_v$ do conjunto das valorizações sobrejetivas de K no conjunto dos domínio locais de ideais principais contidos em K e com corpo de frações K é uma bijeção.*

Para a demonstração, veja [6], página 181.

Sejam B um domínio de Dedekind com corpo de frações L e $\mathcal{V}$ o conjunto das valorizações sobrejetivas de L. Se $U \subseteq \mathcal{V}$, então $\mathcal{O}_{\mathcal{V}(U)} := \cap_{v \in U} \mathcal{O}_v$. Seja $U_B = \{v \in \mathcal{V} | v(B) \geqslant 0\}$ a imagem de $\mathrm{Max}(B)$ na aplicação $M \mapsto v_M$ (veja 4.2.1). A proposição 5.3.2 seguinte mostra que U_B está em bijeção com $\mathrm{Max}(B)$ e que $B = \mathcal{O}_{\mathcal{V}}(U_B)$. Podemos então, recuperar o anel B conhecendo o conjunto $\mathcal{V}$ e os anéis $\mathcal{O}_{\mathcal{V}}(U)$.

Proposição 5.3.2 *Sejam A um domínio,* $\dim A = 1$ *e K seu corpo de frações. Então a aplicação $v \mapsto M_v \cap A$ está bem definida entre o conjunto das valorizações sobrejetivas de K tal que $v(A) \geqslant 0$ e* $\mathrm{Max}(A)$.

Além disso, se A é Dedekind, então essa aplicação é bijetiva. Mais precisamente, cada ideal maximal de $M \subseteq A$ define a valorização sobrejetiva v_M de K (a valorização M-ádica, veja 4.2.1) tal que $v_M(A) \geqslant 0$ e $M \mapsto v_M$ é a aplicação inversa de $v \mapsto M_v \cap A$. Ainda, $\bigcap_{\{v|v(A)\geqslant 0\}} \mathcal{O}_v = A$ e $k_{v_M} := \mathcal{O}_{v_M}/\mathcal{M}_{v_M} \cong A/M$
Demonstração: *Veja [6], página 182.*

Definição 5.3.1 *Seja $L|k$ uma extensão de corpos. Diremos que a valorização $v : L^* \to \mathbb{Z}$ é* trivial *em k se $v(k^*) = \{0\}$. Denote por $\mathcal{V}(L|k)$ o conjunto das valorizações sobrejetivas de L triviais em k.*

Definição 5.3.2 *Seja k um corpo. Diremos que corpo $L \supseteq k$ possui grau de transcendência n sobre k se existirem $x_1, \ldots, x_n \in L$ algebricamente independentes sobre k tais que L é uma extensão finita de $k(x_1, \ldots, x_n)$.*

Definição 5.3.3 *Seja k um corpo. Uma* curva completa não singular *X/k sobre k é um par $(X, k(X)|k)$ consistindo do corpo $k(X)|k$ com grau de transcendência 1 sobre k e X identificado com o conjunto $\mathcal{V}(k(X)|k)$ através de uma dada bijeção entre X e $\mathcal{V}(k(X)|k)$.*

Um elemento $P \in X$ é chamado *um ponto* e $k(X)$ é chamado do *corpo das funções racionais em X*.

Cada ponto P corresponde a uma valorização $v_P \in \mathcal{V}(k(X)|k)$ e a um domínio local de ideais principais $\mathcal{O}_P := \mathcal{O}_{v_P}$ com ideal maximal $\mathcal{M}_{v_P}$. O anel $\mathcal{O}_P$ é chamado do *anel das funções racionais definidas em P* e um elemento de $\mathcal{O}_P$ é chamado de uma *função* de K *definida em P*.

A função $\alpha \in \mathcal{O}_P$ se anula em P ou tem um zero em P se $\alpha \in \mathcal{M}_P$. O inteiro $v_P(\alpha)$ é chamado da *ordem de anulamento* de α em P. Se $\alpha \in K(X) \setminus \mathcal{O}_P$ diremos que α *tem um polo* em P e o inteiro $|v_P(\alpha)|$ é chamado de *ordem de polo* de α em P.

O *domínio* de $\alpha \in k(X)$ é o conjunto dos pontos de X onde α está definida. Se $U \subseteq X$, considere $\mathcal{O}_X(U) := \bigcap_{P\in U} \mathcal{O}_P$, chamado do *anel das funções de X definidas em U*.

Considere X com a topologia de Zariski, onde um conjunto é fechado se, e só se, é o conjunto vazio, ou X ou um conjunto finito de pontos.

Definição 5.3.4 *Um conjunto aberto $U \subseteq X$ é chamado* afim *se $\mathcal{O}_X(U)$ é um domínio de Dedekind finitamente gerado como k-álgebra e se a aplicação $U \to \mathrm{Max}(\mathcal{O}_X(U))$, com $P \mapsto \mathcal{M}_P \cap \mathcal{O}_X(U)$ está bem definida e é bijetora.*

Em outras palavras, um conjunto aberto U é chamado de *conjunto aberto afim* se está em bijeção, como acima, com a curva afim não singular $(\mathrm{Max}(\mathcal{O}_X(U)), \mathcal{O}_X(U))$.

Definição 5.3.5 *Uma* reta projetiva *sobre k é uma curva completa não singular $\mathbb{P}^1/k$ tal que seu corpo de funções $k(\mathbb{P}^1)$ é isomorfo, como $k-$álgebra, com o corpo de funções racionais em uma variável.*

Qualquer $L|k$ de grau de transcendência 1 define uma curva completa não singular X/k dada por $(\mathcal{V}(L|k), L|k)$. Para manter a interpretação geométrica do conjunto X como curva, denotamos um elemento de $X = \mathcal{V}(L|k)$ por P (ponto). Vale lembrar que de fato P é uma valorização e quando quisermos usar propriedades de valorizações usaremos v_P ao invés de P.

Se $\mathbb{P}^1/k$ é a reta projetiva associada ao corpo de funções $k(x)|k$. Denotamos usualmente por ∞ o ponto de $\mathbb{P}^1/k$ correspondente à valorização v_∞.

Proposição 5.3.3 *Sejam k um corpo e $\mathbb{P}^1/k$ a reta projetiva associada ao corpo $k(x)|k$. Então*

$$\mathbb{P}^1 = \{v_{g(x)} \mid g \in k[x],\ \textit{é irredutível e mônico}\} \cup \{v_\infty\}.$$

Demonstração: *Veja [6], página 185.*

Seja $k = \overline{k}$. Então os únicos polinômio irredutíveis em $k[x]$ são os lineares. Neste caso, usualmente denotamos v_{x-a} simplesmente por a. A proposição 5.3.3 mostra que neste caso $\mathbb{P}^1/k$ está em bijeção com $k \sqcup \{\infty\}$.

Teorema 5.3.1 *Seja X/k uma curva completa não singular associada ao corpo $k(X)|k$. Sejam $x \in k(X)$, $k(X)|k(x)$ e U o domínio de x em X. Então U é um subconjunto aberto afim de X e $\mathcal{O}_X(U)$ é igual ao fecho integral de $k[x]$ em $k(X)$. O complemento de U em X é o conjunto dos pontos P tais que $\mathcal{O}_P \supseteq k[\frac{1}{x}]_{\langle \frac{1}{x} \rangle}$.*
Demonstração: *Veja [6], página 185.*

Corolário 5.3.1 *Uma curva completa não singular X/k é a união de dois abertos afins.*
Demonstração: *Seja x como no teorema 5.3.1. Então os domínios de x e $\frac{1}{x}$ são abertos afins que cobrem X.* ■

Corolário 5.3.2 *Sejam k um corpo e $L|k(x)$ uma extensão finita. Sejam B e B' os respectivos fechos integrais de $k[x]$ e $k[1/x]$ em L. Se $\langle \frac{1}{x} \rangle B' = \prod_{i=1}^{s} \mathfrak{P}_i^{e_i}$, então*

$$\mathcal{V}(L|k) = \{v_{\mathfrak{P}} | \mathfrak{P} \in \mathrm{Max}(B)\} \cup \{v_{\mathfrak{P}_1}, \ldots, v_{\mathfrak{P}_s}\}.$$

Demonstração: *Segue do teorema 5.3.1.*

Corolário 5.3.3 *Sejam k um corpo, $L|k(x)$ um extensão finita e $v \in \mathcal{V}(L/k)$. Então $[k_v : k]$ é finito.*

Demonstração: *É fácil ver que o resultado é válido se $L = k(x)$. Sejam B o fecho integral de $k[x]$ em L e $v \in \mathcal{V}(L/k)$. Pelo teorema 5.3.1 é suficiente considerar o caso em que v é uma valorização $\mathfrak{P}-$ádica associada a algum $\mathfrak{P} \in \mathrm{Max}(B)$. Seja $P := \mathfrak{P} \cap k[x]$. Pela finitude da dimensão de $k[x]/P$ sobre k, precisamos apenas mostrar que $f_{\mathfrak{P}/P}$ é finito, pois assim*

$$[k_v : k] = [B/\mathfrak{P} : k] = [B/\mathfrak{P} : k[x]/P] \cdot [k[x]/P : k] < \infty.$$

O inteiro $f_{\mathfrak{P}/P}$ é finito quando B é um $k[x]-$modulo finitamente gerado. Quando $L|k(x)$ é separável, mostramos em 1.3.1 *que B é um $k[x]-$módulo finitamente gerado. Que B é sempre um $k[x]-$módulo finitamente gerado segue do teorema 8.1.1.* ■

Em geral não é possível identificar um curva completa não singular $X/\overline{k}$ com uma curva projetiva não singular. Mas na proposição 5.3.5 veremos que sempre existe um subconjunto denso de X que pode ser identificado com um subconjunto denso de uma curva projetiva plana.

Proposição 5.3.4 *Seja $X_F(\overline{k})$ uma curva plana projetiva com corpo de funções $\overline{k}(X_F)$.*

(i) Sejam $P \in X_F(\overline{k})$ e C o fecho integral de $\mathcal{O}_P$ em $\overline{k}(X_F)$. Então C é um domínio de Dedekind, $\mathrm{Max}(C)$ é um conjunto finito e está em bijeção com o conjunto dos domínios de ideais principais e locais $\mathcal{O} \subseteq \overline{k}(X_F)$ tal que $\mathcal{O}_P \subseteq \mathcal{O}$ e seus ideais maximais $\mathcal{M}$ satisfazem $\mathcal{M}_P \subseteq \mathcal{M}$.

(ii) Seja $\mathcal{O} \in \mathcal{P}(\overline{k}(X_F)/\overline{k})$ com ideal maximal $\mathcal{M}$. Então existe um único $P \in X_F(\overline{k})$ tal que $\mathcal{O} \supseteq \mathcal{O}_P$ e $\mathcal{M} \supseteq \mathcal{M}_P$.

Demonstração: *Veja [6], página 219.*

Proposição 5.3.5 *Seja $X/\overline{k}$ um curva completa não singular. Então existe uma curva projetiva plana $X_F(\overline{k})$ e uma aplicação sobrejetiva e contínua $\varphi : X \to X_F(\overline{k})$. Além disso, se U é o conjunto de pontos não singulares de $X_F(\overline{k})$, então U é aberto e denso em $X_F(\overline{k})$ e φ induz um homeomorfismo de $\varphi^{-1}(U)$ em U.*

Demonstração: *O corolário 8.1.2 mostra que existe $x \in \overline{k}(X)$ tal que $\overline{k}(X)|\overline{k}(x)$ é finito e separável. Sejam $\alpha \in \overline{k}(X)$ tal que $\overline{k}(X) = \overline{k}(x)(\alpha)$ e $f := \min_{\overline{k}(x)}(\alpha) \in \overline{k}(x)[y]$. Multiplicando α se necessário pelo mínimo múltiplo comum dos denominadores dos coeficientes de f, podemos assumir que $f \in \overline{k}[x][y]$. Seja $F(X,Y,Z) := Z^{\deg(f)} f(\frac{X}{Z}, \frac{Y}{Z})$ a homogenização de f. O corpo de funções racionais $\overline{k}(X_F)$ de $X_F(\overline{k})$ é igual a $\overline{k}(X)$.*

Defina $\varphi : X \to X_F(\overline{k})$ por $\varphi(\chi) = P$, onde $\mathcal{O}_\chi \supseteq \mathcal{O}_P$ e $\mathcal{M}_\chi \supseteq \mathcal{M}_P$. A proposição 5.3.4 item (ii) mostra que φ está bem definida. Para mostrar a sobrejevidade de φ, seja

$P \in X_F(\overline{k})$ não singular. Então $\mathcal{O}_P$ é um domínio local principal em $\overline{k}(X)$ contendo $\overline{k}$ e seu corpo de frações é $\overline{k}(X_F)$. Pela definição de X, existe um único ponto $\chi \in X$ tal que $\mathcal{O}_\chi = \mathcal{O}_P$. Se P for singular, seja C o fecho integral de $\mathcal{O}_P$ em $\overline{k}(X_F)$. A proposição 5.3.4 item (i) mostra que C é um domínio de Dedekind com um número finito de ideais maximais e que $\varphi^{-1}(P) = \{\chi \in X | \mathcal{O}_\chi \supseteq C\}$. Entãp $\varphi^{-1}(P) \neq \emptyset$, finito e φ é contínua. Como o conjunto S dos pontos singulares de $X_F(\overline{k})$ é finito, o conjunto $U := X_F(\overline{k}) \setminus S$ é um aberto denso em $X_F(\overline{k})$. Logo, $\varphi^{-1}(U)$ é um aberto em X e φ é um homeomorfismo de $\varphi^{-1}(U)$ em U. ■

Definição 5.3.6 *Sejam $X_F(\overline{k})$ uma curva projetiva plana e $X/\overline{k}$ uma curva completa não singular associada ao corpo de funções $\overline{k}(X_F)/\overline{k}$. Tome $\varphi : X \to X_F(\overline{k})$ a aplicação definida na proposição 5.3.5 dada por $\chi \mapsto P$, onde $\mathcal{O}_P \subseteq \mathcal{O}_\chi$ e $\mathcal{M}_P \subseteq \mathcal{M}_\chi$. O par (X, φ) é chamado de* dessingularização *da curva $X_F(\overline{k})$.*

5.4 Curvas Não Singulares e Domínios de Dedekind

Definição 5.4.1 *Seja $f \in k[x_1, \ldots, x_n]$. Diremos que f é* absolutamente irredutível *se f for irredutível em $\overline{k}[x_1, \ldots, x_n]$.*

Se f é absolutamente irredutível, então $C_f := \frac{k[x,y]}{\langle f \rangle}$ e $\overline{C}_f := \frac{\overline{k}[x,y]}{\langle f \rangle}$ são domínios. Das duas aplicações

$$\begin{aligned} \varphi : Z_f(\overline{k}) &\longrightarrow \mathrm{Max}(\overline{C}_f), \\ \varphi_k : Z_f(k) &\longrightarrow \mathrm{Max}(C_f), \end{aligned}$$

onde $(a, b) \mapsto \langle x - a, y - b \rangle$, apenas φ é uma bijeção em geral. A aplicação φ_k pode não ser sobrejetiva, por exemplo, tome $f(x, y) = x^2 + y^1 + 1 \in \mathbb{R}[x, y]$.

Discutiremos nesta seção como associar, em geral, os ideais maximais de C_f com um subconjunto de pontos de $Z_f(\overline{k})$ e quais propriedades C_f herda de $\overline{C}_f$.

Observação 5.4.1 *Dado k um corpo, sabemos da álgebra comutativa que todo ideal maximal de $k[x, y]$ pode ser gerado por dois elementos. Sejam $f \in k[x, y]$ irredutível e $(a, b) \in \overline{k}^2$. Considere*

$$\begin{aligned} \psi_{(a,b)} : C_f &\longrightarrow \overline{k} \\ \overline{g} &\longmapsto g(a, b) \end{aligned}$$

Observe que dado $M \in \mathrm{Max}(C_f)$, existe $(a, b) \in Z_f(\overline{k})$ tal que $M = \ker(\psi_{(a,b)})$.

Seja $f \in k[x, y]$ absolutamente irredutível. Mostraremos nos dois próximos resultados algumas propriedades que C_f herda de $\overline{C}_f$, mais precisamente mostraremos que se $\overline{C}_f$ for integralmente fechado e Dedekind, então C_f é também é.

Proposição 5.4.1 *Sejam k um corpo, $f \in k[x,y]$ absolutamente irredutível, $(a,b) \in Z_f(\overline{k})$ e $\overline{M} \trianglelefteq \overline{C}_f$ maximal gerado pelas imagens de $x-a$ e $y-b$. Se $M := M \cap C_f$, então o anel local $(C_f)_M$ é principal se $(\overline{C}_f)_{\overline{M}}$ é principal.*

Demonstração: *Por* 0.1.1*, afim de mostrar que um domínio local de dimensão um é principal é suficiente mostrar que seu ideal maximal é principal. Assim, sejam $(a,b) \in Z_f(\overline{k})$ e $g = \min_k(\alpha)$. Existe (veja, [6], pág. 228) $h \in k[x,y]$ tal que $M = \langle \overline{g}, \overline{h} \rangle$. Como $f \in M$, existem $\alpha, \beta \in k[x,y]$ tais que $f = \alpha g + \beta h$. Portanto, em $(C_f)_M$, $\overline{h\beta} \in \langle \overline{g} \rangle$. Pela hipótese, $(\overline{C}_f)_{\overline{M}}$ é principal, a proposição 0.2.2 mostra que, sem perda de generalidade, podemos assumir $(\partial f/\partial y(a,b)) \neq 0$. Assim,*

$$\frac{\partial f}{\partial y}(x,y) = \frac{\partial \alpha}{\partial y}(x,y)g(x) + \frac{\partial \beta}{\partial y}(x,y)h(x,y) + \beta(x,y)\frac{\partial h}{\partial y}(x,y),$$

em particular, $(\partial f/\partial y)(a,b) = \beta(a,b)(\partial h/\partial y)(a,b)$. Assim $\beta(a,b) \neq 0$, $\beta \notin M$ e $\overline{\beta}$ é inversível em $(C_f)_M$. Uma vez que $M = \langle \overline{g}, \overline{h} \rangle$, $M(C_f)_M$ é principal e gerado por $\overline{g}$. ■

Corolário 5.4.1 *Sejam k um corpo e $f \in k[x,y]$ absolutamente irredutível. Se $Z_f(\overline{k})$ é não singular, ou, equivalentemente, se $\overline{C}_f := \overline{k}[x,y]/\langle f \rangle$ é um domínio de Dedekind, então C_f é um domínio de Dedekind. Além disso, se k é um corpo finito, então C_f é um domínio com quocientes finitos.*

Demonstração: *É fácil ver que C_f é Noetheriano e pelo corolário 1.7.1,* $\dim C_f = 1$*. Pela observação 5.4.1 todo ideal maximal de C_f é da forma* $\ker(\psi_{(a,b)})/\langle f \rangle$*. A proposição 0.2.2 garante que $(\overline{C}_f)_{\overline{M}}$ é um domínio local principal se, e só se, $(a,b) \in Z_f(\overline{k})$ é não singular. Assim, segue da proposição 5.4.1 que $(C_f)_M$ é um domínio local principal para todo $M \in \mathrm{Max}(C_f)$. Pelo corolário 1.4.2 concluímos que C_f é integralmente fechado.*

Uma vez que todo ideal de C_f é da forma $M := \ker(\psi_{(a,b)})/\langle f \rangle$, o corpo residual C_f/M é isomorfo ao corpo $k(a,b)$. Assim, se k é finito, então $k(a,b)$ também é. ■

Observação 5.4.2 *A recíproca da proposição 5.4.1 vale apenas quando k é perfeito.*

5.5 Ações de Galois em Curvas

Definição 5.5.1 *Sejam $P = (a,b) \in \mathbb{A}^2(\overline{k})$ e $k(P) := k(a,b)$ o menor subcorpo de $\overline{k}$ que contém a, b e k. Este corpo é chamado do* corpo de definição *sobre k do ponto $P = (a,b)$. Diremos que P é* definido sobre *o corpo $L \subseteq \overline{k}$ se $P \in \mathbb{A}^2(L)$.*

Por construção, o ponto P é definido sobre $k(P)$ e se $P \in \mathbb{A}^2(L)$ com $k \subseteq L \subseteq \overline{k}$, então $k(P) \subseteq L$. A extensão $k(P)$ é finita sobre k desde que a e b sejam algébricos sobre k.

O grupo de Galois de $\overline{k}$ sobre k, $\mathrm{Gal}(\overline{k}|k)$, age em $\mathbb{A}^2(\overline{k})$ como segue:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{k}|k) \times \mathbb{A}^2(\overline{k}) & \longrightarrow & \mathbb{A}^2(\overline{k}) \\ (\sigma, (a,b)) & \longmapsto & (\sigma(a), \sigma(b)). \end{array}$$

Seja $f \in k[x,y]$ absolutamente irredutível. A ação de $\mathrm{Gal}(\overline{k}|k)$ em $\mathbb{A}^2(\overline{k})$ induz uma ação em $Z_f(\overline{k})$. Observamos, se $(a,b) \in Z_f(\overline{k})$, então $f(\sigma(a), \sigma(b)) = \sigma(f(a,b)) = 0$.

Seja $Z_f(\overline{k})/\mathrm{Gal}(\overline{k}|k)$ o conjunto das órbitas de $Z_f(\overline{k})$ sobre a ação de $\mathrm{Gal}(\overline{k}|k)$. Considere

$$\begin{array}{ccc} I_{\overline{k}} : Z_f(\overline{k}) & \longrightarrow & \mathrm{Max}(\overline{C}_f) \\ (a,b) & \longmapsto & \langle x-a, y-b \rangle, \end{array}$$

$$\begin{array}{ccc} \pi : \mathrm{Max}(\overline{C}_f) & \longrightarrow & \mathrm{Max}(C_f) \\ \overline{M} & \longmapsto & M := \overline{M} \cap C_f, \end{array}$$

$$\begin{array}{ccc} I_k : Z_f(\overline{k})/\mathrm{Gal}(\overline{k}|k) & \longrightarrow & \mathrm{Max}(C_f) \\ \text{órbita de } (a,b) & \longmapsto & \ker(\psi_{(a,b)}), \end{array}$$

onde $\psi_{(a,b)}$ denota a aplicação definida em 5.4.1.

Proposição 5.5.1 *Sejam k um corpo e $f \in k[x,y]$ absolutamente irredutível. A aplicação I_k é uma bijeção e o seguinte diagrama é comutativo:*

$$\begin{array}{ccc} Z_f(\overline{k}) & \xrightarrow{I_{\overline{k}}} & \mathrm{Max}(\overline{C}_f) \\ \downarrow & & \downarrow \\ Z_f(\overline{k})/\mathrm{Gal}(\overline{k}|k) & \xrightarrow{I_k} & \mathrm{Max}(C_f) \end{array}$$

Observação 5.5.1 *Sejam $k \subseteq L \subseteq \overline{k}$ extensões de Galois e $f \in k[x,y]$. Então a órbita do ponto $(a,b) \in Z_f(L)$ está contido em $Z_f(L)$. De fato, seja $\sigma \in \mathrm{Gal}(\overline{k}|k)$, uma vez que $L|k$ é de Galois, $\sigma(L) = L$, portanto $(\sigma(a), \sigma(b)) \in Z_f(L)$.*

Proposição 5.5.2 *Sejam $q = p^r$ e $\overline{\mathbb{F}}_q$ o fecho algébrico de $\mathbb{F}_q$. Denote por $\mathbb{F}_{q^n}$ o único subcorpo de $\overline{\mathbb{F}}_q$ de grau n sobre $\mathbb{F}_q$. Sejam $f \in \mathbb{F}_q[x,y]$ absolutamente irredutível e $C_f := \mathbb{F}_q[x,y]/\langle f \rangle$. Então os conjuntos $\{M \in \mathrm{Max}(C_f) \mid [C_f/M : \mathbb{F}_q] = d\}$ e $Z_f(\mathbb{F}_{q^n})$ são finitos. Além disso, se $N_n := |Z_f(\mathbb{F}_{q^n})|$ e $b_d := \#\{M \in \mathrm{Max}(C_f) \mid [C_f/M : \mathbb{F}_q] = d\}$, então $N_n = \sum_{d|n} d b_d$.*

Demonstração: *Claramente $\#Z_f(\mathbb{F}_{q^n}) < \infty$. Mostraremos que a aplicação*

$$\begin{array}{ccc} J : Z_f(\mathbb{F}_{q^n}) & \longrightarrow & \bigcup_{d|n} \{M \in \mathrm{Max}(C_f) | [C_f/M : \mathbb{F}_q] = d\} \\ (a,b) & \longmapsto & \ker(\psi_{(a,b)}) \end{array}$$

está bem definida e é sobrejetora. Sejam $(a,b) \in Z_f(\mathbb{F}_{q^n})$, $M = \ker(\psi_{(a,b)})$ *e* $d := [C_f/M : \mathbb{F}_q]$. *Como* $\mathbb{F}_q(a,b) \cong C_f/M$ *é um subcorpo de* $\mathbb{F}_{q^n}$, $d|n$ *e portanto* J *está bem definida. Seja* $M \in \mathrm{Max}(C_f)$ *tal que* $[C_f/M : \mathbb{F}_q] = d$ *e* $d|n$. *Uma vez que, a menos de isomorfismo,* $\mathbb{F}_{q^d}$ *é a único extensão de grau* d *de* $\mathbb{F}_q$, $C_f/M \cong \mathbb{F}_{q^d}$. *Por* $d|n$, $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$, *em particular, existe um monomorfismo* $\epsilon : C_f/M \to \mathbb{F}_{q^n}$. *Sejam* $a := \epsilon(x)$ *e* $b := \epsilon(y)$, *como* $f(x,y) = 0$ *em* C_f, $\epsilon(f(x,y)) = f(a,b) = 0$. *Assim,* $(a,b) \in Z_f(\mathbb{F}_{q^n})$. *É fácil ver que* $M = \ker(\psi_{(a,b)})$, *logo* J *é sobrejetora.*

Seja $(a,b) \in Z_f(\mathbb{F}_{q^n})$ *tal que* $[k(a,b) : k] = d$, *pelo lema 5.5.1 a órbita de* (a,b) *sobre a ação de* $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ *contém* d *elementos distintos. Uma vez que* $\mathbb{F}_{q^n}|\mathbb{F}_q$ *é Galois, pela observação 5.5.1 a órbita de* (a,b) *sobre a ação de* $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ *está contida em* $Z_f(\mathbb{F}_{q^n})$. *Claramente, o conjunto* $Z_f(\mathbb{F}_{q^n})$ *é igual a união disjunta das órbitas de* $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$. *A proposição 5.5.1 garante que* $J(\text{órbita de } (a,b)) \neq J(\text{órbita de } (a',b'))$ *se a órbita de* (a,b) *for diferente da órbita de* (a',b'). *Portanto, para cada* $d|n$, $Z_f(\mathbb{F}_{q^n})$ *contém* b_d *órbitas de comprimento* d. *Assim,* $N_n = \sum_{d|n} db_d$. ■

Definição 5.5.2 *Diremos que* $P = (c_0 : c_1 : c_2) \in \mathbb{P}^2(k)$ *é* definido *sobre* L *se existe* $\lambda \in \overline{k}^*$ *tal que* $\lambda c_0, \lambda c_1, \lambda c_2 \in L$.

Análogo ao caso afim, o grupo $\mathrm{Gal}(\overline{k}|k)$ age em $\mathbb{P}^2(\overline{k})$ como segue:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{k}|k) \times \mathbb{P}^2(\overline{k}) & \longrightarrow & \mathbb{P}^2(\overline{k}) \\ (\sigma, (c_0 : c_1 : c_2)) & \longmapsto & (\sigma(c_0) : \sigma(c_1) : \sigma(c_2)). \end{array}$$

Dado $F \in k[X,Y,Z]$ homogêneo, esta ação induz uma ação em $X_F(\overline{k})$. Se $P \in X_F(\overline{k})$, então $k(P)$ também é chamado do *corpo de definição* de P sobre k .

A aplicação $\varphi : \mathbb{A}^2(\overline{k}) \to \mathbb{P}^2(\overline{k})$, dada por $(a,b) \mapsto (a : b : 1)$ é *Galois-equivalente*, isto é,

$$\varphi(\sigma(P)) = \sigma(\varphi(P)),\ \forall P \in \mathbb{A}^2(\overline{k}),\ \forall \sigma \in \mathrm{Gal}(\overline{k}|k).$$

Claramente os corpos de definição de $P \in \mathbb{A}^2(\overline{k})$ sobre k e e de $\varphi(P) \in \mathbb{P}^2(\overline{k})$ são iguais.

Agora sejam $F \in k[x_0, x_1, x_2]$ homogêneo e absolutamente irredutível e $X_F(\overline{k})$ uma curva projetiva não singular. Podemos considerar os corpos $k(X_F)$ e $\overline{k}(X_F)$. Seja $\mathcal{P}(\overline{k}(X_F)/\overline{k})$ o conjunto dos domínios locais principais contendo $\overline{k}$ e com corpo de frações $\overline{k}(X_F)$. Similarmente, seja $\mathcal{P}(k(X_F)/k)$ o conjunto dos domínios locais principais contendo k com corpo de frações $k(X_F)$. Considere

$$\begin{array}{ccc} I_{\mathcal{P}} : \mathcal{P}(\overline{k}(X_F)/\overline{k}) & \longrightarrow & \mathcal{P}(k(X_F)/k) \\ \overline{\mathcal{O}} & \longmapsto & \overline{\mathcal{O}} \cap k(X_F). \end{array}$$

Seja $I_{\mathcal{V}} : \mathcal{V}(\overline{k}(X_F)/\overline{k}) \to \mathcal{V}(k(X_F)/k)$ definida por $v \mapsto I_{\mathcal{V}}(v)$, é a única valorização sobrejetiva de $k(X_F)$ associada a $v_{|_{k(X_F)}}$. Seja

$$\begin{array}{rccc} I_{\overline{k}} : X_F(\overline{k}) & \longrightarrow & \mathcal{P}(\overline{k}(X_F)/\overline{k}) \\ P & \longmapsto & \mathcal{O}_P. \end{array}$$

O teorema 5.2.1 mostra que a aplicação $I_{\overline{k}}$ é uma bijeção. Sejam $X_F(\overline{k})/\mathrm{Gal}(\overline{k}|k)$ o conjunto das órbitas de $X_F(\overline{k})$ sobre a ação de $\mathrm{Gal}(\overline{k}|k)$ e

$$\begin{array}{rccc} I_k : X_F(\overline{k})/\mathrm{Gal}(\overline{k}|k) & \longrightarrow & \mathcal{P}(k(X_F)/k) \\ \text{órbita de } P & \longmapsto & \mathcal{O}_P \cap k(X_F). \end{array}$$

O seguinte resultado é análogo da proposição 5.5.1 para o caso de curvas projetivas não singulares.

Proposição 5.5.3 *Sejam k um corpo, $F \in k[x_0, x_1, x_2]$ homogêneo e $X_F(\overline{k})$ é uma curva projetiva não singular. A aplicação I_k está bem definida e é uma bijeção. Além disso, o seguinte diagrama é comutativo:*

$$\begin{array}{ccccc} X_F(\overline{k}) & \xrightarrow{I_{\overline{k}}} & \mathcal{P}(\overline{k}(X_F)/\overline{k}) & \xrightarrow{\sim} & \mathcal{V}(\overline{k}(X_F)/\overline{k}) \\ & & \overset{I_{\mathcal{P}}}{\downarrow} & & \overset{I_{\mathcal{V}}}{\downarrow} \\ \downarrow & & & & \\ X_F(\overline{k})/\mathrm{Gal}(\overline{k}|k) & \xrightarrow{I_k} & \mathcal{P}(k(X_F)/k) & \xrightarrow{\sim} & \mathcal{V}(k(X_F)/k) \end{array}$$

Seja $P \in X_F(\overline{k})$. Então o corpo e definição de qualquer ponto da órbita de P é isomorfo sobre k ao corpo residual de $\mathcal{O}_P \cap k(X_F)$.

Lema 5.5.1 *Sejam k um corpo perfeito e $P \in \mathbb{P}^2(\overline{k})(\mathbb{A}^2(\overline{k}))$. A órbita de P sobre $\mathrm{Gal}(\overline{k}|k)$ contém exatamente $[k(P) : k]$ elementos.*
Demonstração: *Veja [6], página 335.*

Sejam q uma potência do primo p e $F \in \mathbb{F}_q[X, Y, Z]$ homogêneo. O conjunto $X_F(\mathbb{F}_{q^n})$ é finito uma vez que está contido no conjunto finito $\mathbb{P}^2(\mathbb{F}_{q^n})$ de ordem $q^{2n} + q^n + 1$. Seja $N_n := |X_F(\mathbb{F}_{q^n})|$.

Lema 5.5.2 *Sejam $F \in \mathbb{F}_q[X, Y, Z]$ homogêneo e $X_F(\overline{\mathbb{F}}_q)$ uma curva não singular. Seja b_d o número de órbitas de comprimento d de $X_F(\overline{\mathbb{F}}_q)$ sobre $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$. Então $N_n = \sum_{d|n} d b_d$.*
Demonstração: *Uma vez que $\mathbb{F}_{q^n}|\mathbb{F}_q$ é Galois, $X_F(\mathbb{F}_{q^n})$ contém a órbita de cada um de seus pontos. Se $Q \in X_F(\mathbb{F}_{q^n})$, então $\mathbb{F}_q(Q) \subseteq \mathbb{F}_{q^n}$. Assim, $\mathbb{F}_q(Q) = \mathbb{F}_{q^d}$ para algum d tal*

que $d|n$. Seja v uma órbita em $X_F(\overline{\mathbb{F}}_q)$ que contém d elementos. O lema 5.5.1 mostra que v contém um ponto P tal que $[\mathbb{F}_q(P):\mathbb{F}_q]=d$. Assim, $\mathbb{F}_q(P)=\mathbb{F}_{q^d}$ e $P\in X_F(\mathbb{F}_{q^n})$. Portanto $N_n=\sum_{d|n} db_d$. ■

5.6 Corpos de Funções

Sejam $f\in k[x,y]$ irredutível, $C_f=k[x,y]/\langle f\rangle$ e $k(Z_f)$ o corpo de frações de C_f. Nesta seção veremos como a condição de f ser absolutamente irredutível reflete em propriedades algébricas do corpo $k(Z_f)$. Primeiro observamos alguns fatos:

Fato 5.6.1 *Seja $f\in k[x,y]$.*

1. *Se $f=gh\in\overline{k}[x,y]$ tal que $g\in k[x,y]$, então $h\in k[x,y]$.*
2. *Suponha $g|f$, onde $g\in\overline{k}[x,y]$ é irredutível e que pelo menos um dos coeficientes não nulos de g pertencem a k. Seja E a extensão de k gerada pelos coeficientes de g.*
   (a) *Suponha $E|k$ separável. Seja $\{\sigma_1,\ldots,\sigma_n\}$ os representantes das classes de $\mathrm{Gal}(\overline{k}|k)/\mathrm{Gal}(\overline{k}|E)$. Então $\prod_{i=1}^n\sigma_i(g(x,y))\in k[x,y]$ e divide f.*
   (b) *Suponha $E|k$ puramente inseparável de grau p^e. Seja $r\geqslant 1$ o menor inteiro tal que $g^{p^r}\in k[x,y]$ (por definição $r\leqslant e$). Então g^{p^r} é irredutível em $k[x,y]$ e divide f.*

Proposição 5.6.1 *Sejam k um corpo, $f\in k[x,y]$, $g\in\overline{k}[x,y]$ irredutível tal que $g|f$. Suponha que pelo menos um dos coeficientes de g pertencem a k e seja E o corpo obtido pela junção a k dos coeficientes de g. Seja $E_0\subseteq E$ o subcorpo maximal de E que é separável sobre k.*

1. *Então $k(Z_f)$ contém um subcorpo isomorfo a E_0. Mais precisamente, existe um homomorfismo de corpos $\varphi:E_0\to k(Z_f)$ tal que $\varphi_{|k}=\mathrm{id}_{|k}$.*
2. *Se existe um coeficiente λ de g tal que $E=E_0(\lambda)$, então $k(Z_f)$ contém um subcorpo isomorfo a E.*

Demonstração: *Primeiro consideramos o caso em $E=E_0$, ou seja, $E|k$ é separável. Seja $\{\sigma_1,\ldots,\sigma_n\}$ o conjunto dos representantes das classes de $\mathrm{Gal}(\overline{k}|k)/\mathrm{Gal}(\overline{k}|E)$. Por 5.6.1, item 2, concluímos que $f=c\prod_{i=1}^n\sigma_i(g)\in\overline{k}[x,y]$ e a aplicação natural $i:k[x,y]/\langle f\rangle\to E[x,y]/\langle g\rangle$ é injetiva. Denote também por i a aplicação induzida entre os corpos de frações destes domínios. O resultado é válido quando $g\in\overline{k}[x]$. Seja $g\notin\overline{k}[x]$, equivalentemente, existe uma injeção $E[x]\hookrightarrow E[x,y]/\langle g\rangle$. Sejam $\deg_y(g)$ e $\deg_y(f)$ os graus de g e f em y. Por $f=c\prod_{i=1}^n\sigma_i(g)$, $n\deg_y(g)=\deg_y(f)$. Por construção*

$$[k(Z_f):k(x)]=\deg_y(f)\quad e\quad [E(Z_g):E(x)]=\deg_y(g)$$

Como $[E(x) : k(x)] = [E : k] = n$, $[E(Z_g) : k(Z_f)] = 1$ *e a aplicação* $i : k(Z_f) \to E(Z_g)$ *é um isomorfismo. Deste modo,* $k(Z_f)$ *contém um subcorpo isomorfo.*

Para o caso geral, sejam $[E : E_0] = p^e > 1$ *e* r *o menor inteiro tal que* $g^{p^r} \in E_0[x, y]$. *Então* g^{p^r} *é irredutível e divide* f *em* $E_0[x, y]$. *O corpo* E_0 *é o subcorpo de* $\overline{k}$ *obtido pela junção a* k *dos coeficientes de* g^{p^r}. *Aplicando o caso anterior para* g^{p^r}, *concluímos* $k(Z_f) \cong E_0(Z_{g^{p^r}})$ *sobre* k.

Considere o diagrama

$$\begin{array}{ccc} E_0(x)[y]/\langle g^{p^r}\rangle & \longrightarrow & E(x)[y]/\langle g\rangle \\ {\scriptstyle p^r \deg_y(g)}\uparrow & & {\scriptstyle \deg_y(g)}\uparrow \\ E_0(x) & \xrightarrow{p^e} & E(x) \end{array}$$

De $[E(x) : E_0(x)] = [E : E_0]$ *segue que* $E(x)[y]/\langle g\rangle$ *tem grau* p^{e-r} *sobre* $E_0(x)[y]/\langle g^{p^r}\rangle$. *Se existe um coeficiente* λ *de* g *tal que* $E = E_0(\lambda)$, *então* $e = r$ *e assim* $E_0(x)[y]/\langle g^{p^r}\rangle \cong E(x)[y]/\langle g\rangle$. *Portanto,* $k(Z_f) \cong E(Z_g)$ *sobre* k. *Logo,* $k(Z_f)$ *contém uma cópia de* E. ■

Proposição 5.6.2 *Sejam* k *um corpo,* $f \in k[x, y]$ *irredutível e* $E|k$ *a extensão algébrica maximal em* $k(Z_f)$. *Então* $[E : k] < \infty$ *e é número dos fatores irredutíveis de* f *em* $\overline{k}[x, y]$. *Além disso, existe um fator irredutível* g *de* f *tendo pelo menos um coeficiente em* k, *tal que* E *é gerado por* k *e os coeficientes de* g. *Seja* E_0 *a maior extensão separável de* k *em* E. *Então* $E|E_0$ *é simples e* f *é uma* $[E : E_0]-$*ésima potência em* $\overline{k}[x, y]$.

Demonstração: *É fácil verificar o resultado quando* $f \in k[x]$. *Suponha agora que* $\deg_y(f) > 0$, *tal que* $k(Z_f)|k(x)$ *é uma extensão finita. É claro que* $k(Z_f) = E(x)(y)$. *Seja* $h(x, Y) = \min_{E[x]}(y) \in E(x)[Y]$. *Claramente* $h(x, Y)|f(x, Y)$ *em* $E(x)[Y]$. *Pelo lema de Gauss, que* $g(x, Y) := \mathrm{cont}(h(x, Y))^{-1}h(x, Y) \in E[x][Y]$ *divide* $f(x, Y)$. *Assim,*

$$\deg_y(f) = [k(Z_f) : k(x)] = [k(Z_f) : E(x)][E(x) : k(x)] = \deg_y(g)[E : k].$$

Agora, sem perda de generalidade, podemos assumir que pelo menos um coeficiente não nulo de g *pertença a* k. *Sejam* F *a extensão de* k *gerada pelos coeficientes de* g *e* F_0 *a maior extensão separável de* k *em* F. *Seja* r *o menor inteiro tal que* $g^{p^r} \in F_0[x, y]$. *Sejam* $\sigma_1, \ldots, \sigma_s$ *os distintos monomorfismos de* F_0 *em* $\overline{k}$. *Por 5.6.1, item 2,* $f = c(\sigma_1(g) \cdots \sigma_s(g))^{p^r}$. *Assim,*

$$\deg_Y(f) = p^r[F_0 : k] \deg_Y(g).$$

Uma vez que $F \subseteq E$, *segue que* $F = E$ *e* $F_0 = E_0$. *Como* $[E : E_0] = p^r$, *o polinômio minimal sobre* E_0 *de pelo menos uma coeficiente* α *de* g *tem a forma* $y^{p^r} - \alpha^{p^r}$. *Portanto,* $E = E_0(\alpha)$. ■

Teorema 5.6.1 *Sejam k um corpo perfeito e $f \in k[x,y]$ irredutível. Então o corpo k é algebricamente fechado em $k(Z_f)$ se, e somente se, f é absolutamente irredutível.*
Demonstração: *Pela proposição 5.6.2, se k não é algebricamente fechado em $k(Z_f)$, então f não é absolutamente irredutível. Se f não é absolutamente irredutível, seja $g \in \overline{k}[x,y]$ um fator irredutível de f. Assuma que pelo menos um coeficiente de g pertence a k e seja E o corpo obtido pela junção a k dos coeficiente de g. Por hipótese (f irredutível), $E \neq k$. Seja $E_0 \subseteq E$ o subcorpo maximal de E que é separável sobre k. A proposição 5.6.1 mostra que $k(Z_f)$ contém um subcorpo isomorfo a E_0. Uma vez que k é perfeito, $E_0 = E$ e, portanto, $E_0 \neq k$. Então k não é algebricamente fechado em $k(Z_f)$.* ■

Teorema 5.6.2 *Sejam k um corpo e $L|k$ um extensão transcendente de grau 1. Seja $\mathcal{V}(L|k)$ o conjuntos das valorizações discretas sobrejetivas de L triviais em k. Se $k' \subseteq L$ é o maior subcorpo de L algébrico sobre k, então $[k' : k] < \infty$ e $k' = \bigcap_{v \in \mathcal{V}(L|k)} \mathcal{O}_v$.*
Demonstração: *A prova $[k' : k] < \infty$ segue de $[L : k(x)] < \infty$. Sejam $\alpha \in L$ algébrico sobre k e $v \in \mathcal{V}(L|k)$, como v é trivial em k, $v(\alpha) = 0$. Assim, $\alpha \in \mathcal{O}_v$ para todo $v \in \mathcal{V}(L|k)$. Agora seja $\alpha \in \bigcap_{v \in \mathcal{V}(L|k)} \mathcal{O}_v$, suponha que $\alpha \notin k'$. Então $[L : k(\alpha)] < \infty$. Seja B' o fecho integral de $k[\frac{1}{\alpha}]$ em L. O teorema 8.1.1 mostra que B' é um $k[\frac{1}{\alpha}]-$módulo finitamente gerado. O ideal $\langle \frac{1}{\alpha} \rangle$ em $k[\frac{1}{\alpha}]$ é não trivial e se fatora em produto de ideais maximais em B':*

$$\langle \frac{1}{\alpha} \rangle B' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s},$$

veja 2.2.1. Então $v_{\mathfrak{P}_1}(\alpha) = -v_{\mathfrak{P}_1}(\frac{1}{\alpha}) < 0$, que é impossível pelo fato que $\alpha \in \mathcal{O}_{v_{\mathfrak{P}_1}}$. Portanto $\alpha \in k'$. ■

Um fato que segue do teorema anterior é o seguinte:

Corolário 5.6.1 *Sejam k um corpo e $L|k$ uma extensão de grau de transcendência 1 e $\alpha \in L^*$. Então $\#\{v \in \mathcal{V}(L|k) | v(\alpha) \neq 0\} < \infty$.*

Agora faremos a interpretação geométrica das afirmações do teorema 5.6.2. Sejam $X_F(\overline{k})$ uma curva não singular em $\mathbb{P}^2(\overline{k})$ e $\overline{k}(X_F)$ seu corpo de funções racionais. Recorde que $\alpha = \frac{\overline{G}}{\overline{H}} \in \overline{k}(X_F)$ é definido em $P \in X_F(\overline{k})$ se $H(P) \neq 0$. O anel $\mathcal{O}_P$ é o anel das funções α definidas em P. O teorema 5.2.1 mostra que o conjunto dos pontos de $X_F(\overline{k})$ estão em bijeção com $\mathcal{V}(\overline{k}(X_F)/\overline{k})$. Em termo de funções sobre curvas, o teorema 5.6.2 afirma que as funções racionais sobre $X_F(\overline{k})$ que são definidas em todos os pontos são as funções constantes. Em outras palavras, uma função não constante α em $X_F(\overline{k})$ deve ter pelo menos um polo e um zero. De fato, o teorema 5.6.2 mostra que α e $\frac{1}{\alpha}$ devem ter polo e, o polo de $\frac{1}{\alpha}$ é um zero de α. A proposição 5.6.1 mostra que o número de zeros e polos de

α deve ser finito. O número de zeros de uma função é igual seu número de polos, como mostraremos em 5.9.1.

Agora sejam k um corpo e X/k um curva completa não singular sobre k com corpo de funções $k(X)/k$. Relembre que se $U \subseteq X$ é um aberto não vazio, então $\mathcal{O}_X(U) := \bigcap_{P \in U} \mathcal{O}_P$ é o anel de funções em U. Quando $k = \overline{k}$, o teorema 5.6.2 garante que as funções em X definidas em todos os pontos são somente as constantes. Em outras palavras, $\mathcal{O}_X(X) = k$. Em geral $k \subseteq \mathcal{O}_X(X)$ não necessariamente iguais.

Definição 5.6.1 *Seja k um corpo. O corpo $L \subseteq k$ é chamado de um* corpo de funções *sobre k se o corpo L é um corpo de transcendência de grau 1 sobre k e k é algebricamente fechado em L.*

Definição 5.6.2 *Seja k um corpo. Uma* curva completa não singular *X/k sobre k é redefinida como uma curva completa não singular como na definição 5.3.3 tal que*

$$\mathcal{O}_X(X) := \bigcap_{P \in X} \mathcal{O}_P := \bigcap_{P \in X} \mathcal{O}_{v_P} := \{x \in k(X)^* | v_P(x) \geqslant 0\} \sqcup \{0\} = k.$$

Concluímos esta seção com um resultado sobre extensão de corpos constantes. Sejam $\overline{k(X)}$ o fecho algébrico de $k(X)$ e $\overline{k}$ o fecho algébrico de k em $\overline{k(X)}$. Sejam $k' \subseteq \overline{k}$ uma extensão de k e

$$k'(X) := k' \cdot k(X) = \text{subcorpo de } \overline{k(X)} \text{ gerado por } k' \text{ e } k(X).$$

Lema 5.6.1 *Sejam k um corpo perfeito e $k(X)/k$ um corpo de funções. Se $k' \subseteq \overline{k}$ é uma extensão de k, então $k'(X)/k'$ é um corpo de funções. Além disso, se $[k' : k] < \infty$, então $[k'(X) : k(X)] = [k' : k]$.*

Definição 5.6.3 *Seja k um corpo perfeito. Com as notações acima, seja $X_{k'}/k'$ a curva completa não singular associada ao corpo de funções $k'(X)/k'$. A curva $X_{k'}/k'$ é dita ser obtida de X/k por uma extensão do corpo constante, ou por extensão de escalares ou por mudança de base. A extensão $k'(X)/k(X)$ é chamada uma extensão do corpo constante.*

O lema 5.6.1 mostra que $k'(X)/k'$ é sempre um corpo de funções quando k é perfeito. Se k não é perfeito, então a definição de extensão de escalares pode não fazer sentido. Para evitar isso, podemos definir $X_{k'}/k'$ um curva completa não singular associada ao corpo de funções $k(X) \otimes_k k'$ sobre k'.

Sejam $F \in k[x_0, x_1, x_2]$ absolutamente irredutível, homogêneo e X_F/k a curva completa não singular associada ao corpo de funções $k(X_F)/k$. Se a curva projetiva plana $X_F(\overline{k})$ é não singular, o teorema 5.2.1 afirma que $X_F(\overline{k})$ está em bijeção com o conjunto $(X_F)_{\overline{k}}$. A proposição 5.5.3 mostra que $X_F(\overline{k})/\mathrm{Gal}(\overline{k}|k)$ está em bijeção com X_F. Mostraremos uma generalização deste fato em 5.8.1.

5.7 Morfismos de Curvas Completas Não-Singulares

Sejam X/k e Y/k duas curvas completas não singulares. O conceito de morfismo não constante de curvas completas sobre k é definido abaixo. Definiremos a noção de um ponto de ramificação de um morfismo e mostraremos que o local de ramificação de um morfismo separável é finito.

Definição 5.7.1 *Sejam X/k e Y/k duas curvas completas não singulares sobre k. Um morfismo (não constante) $\varphi : X \to Y$ de curvas completas não singulares sobre k é uma aplicação dada por um homomorfismo de $k-$álgebras $\varphi^* : k(Y) \to k(X)$ do seguinte modo: se $P \in X$ corresponde à valorização v_P, então $\varphi(P)$ corresponde em Y a única valorização sobrejetiva dada por $v_P \circ \varphi$.*

Segue da definição que $\mathcal{O}_{\varphi(P)} = (\varphi^*)^{-1}(\mathcal{O}_P)$. A aplicação φ é bem definida: de fato, $\varphi^*(k(Y))$ é um corpo de funções sobre k, com $\varphi^*(k(Y)) \subseteq k(X)$. Observe que o grau da extensão do corpo de funções sobre k é finito, logo $k(X)|\varphi^*(k(Y))$ é algébrica. Seja v uma valorização em $k(X)$ correspondente ao ponto $P \in X$. Então, $v_{|_{\varphi^*(k(Y))^*}}$ pode não ser uma valorização trivial pois $k(X)|\varphi^*(k(Y))$ é algébrica.

Suponha $\varphi^* : k(Y) \to k(X)$ dada pela inclusão $k \subseteq k(Y) \subseteq k(X)$. Então $\mathcal{O}_{\varphi(P)} = \mathcal{O}_P \cap k(Y)$.

Definição 5.7.2 *Seja $\varphi : X \to Y$ um morfismo não constante de curvas completas não singulares sobre k. Seja $\varphi^* : k(Y) \to k(X)$ a extensão de corpos definida por φ. O grau $[k(X) : \varphi^*(k(Y))]$ é chamado de* grau de *φ. O morfismo φ é chamado de separável se a extensão $k(X)|\varphi^*(k(Y))$ é separável.*

Definição 5.7.3 *Duas curvas completas não singulares X/k e Y/k são isomorfas sobre k se seus corpos de funções são isomorfos como $k-$álgebras.*

Dado um isomorfismo de $k-$álgebras entre $k(X)$ e $k(Y)$, o morfismo associado entre as curvas sobre k é um isomorfismo de curvas.

Definição 5.7.4 *Diremos que σ é um* automorfismo da curva X/k *se é um morfismo de curvas sobre k associado a um automorfismo de k-álgebras $\sigma^* : k(X) \to k(X)$.*

Denote por $\mathrm{Aut}(X/k)$ o grupo dos automorfismos de uma curva completa não singular. Claramente um automorfismo tem grau 1 e é separável.

Seja $\varphi : X \to Y$ um morfismo de curvas completas não singulares sobre k. Uma vez que as curvas completas não singulares definidas pelos corpos de funções $k(Y)/k$ e $\varphi^*(k(y))$ são isomorfas, é geralmente possível reduzir o estudo de um morfismo φ ao caso em que φ é uma inclusão e $k(Y)$ visto como um subcorpo de $k(X)$.

Seja X/k uma curva completa não singular. Se $\alpha \in k(X) \setminus k$, então α não é algébrico sobre k, portanto o subcorpo $k(\alpha)$ de $k(X)$ é isomorfo ao corpo de funções racionais em uma variável sobre k. Portanto, a inclusão $k(\alpha) \subseteq k(X)$ induz um morfismo $\varphi_\alpha : X \to \mathbb{P}^1$, com $\mathcal{O}_{\varphi_\alpha(P)} := \mathcal{O}_P \cap k(\alpha)$.

Lema 5.7.1 *Sejam k um corpo e $\varphi : X \to Y$ um morfismo não constante de curvas completas não singulares sobre k. Suponha que φ é dada pela inclusão dos corpos de funções $k(Y) \subseteq k(X)$. Então existe uma cobertura de abertos afins $\{U_1, U_2\}$ de Y com as seguintes propriedades:*

1. *Seja $V_i := \varphi^{-1}(U_i), i = 1, 2$. Então V_i é um aberto afim e a inclusão $\mathcal{O}_Y(U_i) \subseteq \mathcal{O}_X(V_i)$ transforma $\mathcal{O}_X(V_i)$ em um $\mathcal{O}_Y(U_i)-$módulo finitamente gerado, para $i = 1, 2$.*
2. *A aplicação $\varphi_{|_{V_i}} : V_i \to U_i$ pode ser identificada de maneira natural com a aplicação de curvas afins $\mathrm{Max}(\mathcal{O}_X(V_i)) \to \mathrm{Max}(\mathcal{O}_Y(U_i))$ dada pela inclusão $\mathcal{O}_Y(U_i) \subseteq \mathcal{O}_X(V_i)$.*
3. *Seja $Q \in Y$. Então o fecho integral C de $\mathcal{O}_Q$ em $k(X)$ é finitamente gerado como $\mathcal{O}_Q-$módulo e um domínio de Dedekind.*

Demonstração: *Para 1 e 2, observe que: dado $\alpha \in k(Y) \setminus k$, sejam V_1, U_1 os respectivos domínios de α em X e Y. Sejam V_2 e U_2 os respectivos domínios de $\frac{1}{\alpha}$ em X e Y. É fácil ver que $\{U_1, U_2\}$ e $\{V_1, V_2\}$ são coberturas para Y e X respectivamente. Pelo teorema 5.3.1, U_1, U_2 e V_1, V_2 são abertos afins. E segue da definição que $\varphi^{-1}(U_i) = V_i, i = 1, 2$.*

Agora provemos 3. Sem perda de generalidade, podemos assumir que $Q \in U_1$ (i.é, $\alpha \in \mathcal{O}_Q \setminus k$). Por definição, C é integralmente fechado, como a extensão $C/\mathcal{O}_Q$ é integral, $\dim C = 1$. De $\alpha \in \mathcal{O}_Q$, concluímos $\mathcal{O}_Q = (\mathcal{O}_Y(U_1))_{\mathcal{M}_Q}$. Por construção, $\mathcal{O}_X(V_1)$ é o fecho integral de $\mathcal{O}_Y(U_1)$ em $k(X)$. Como $\mathcal{O}_Y(U_1) \setminus \mathcal{M}_Q$ é um subconjunto multiplicativo de $\mathcal{O}_X(V_1)$, o fecho integral de C de $\mathcal{O}_Q$ em $k(X)$ é a localização de $\mathcal{O}_X(V_1)$ num subconjunto multiplicativo. Uma vez que $\mathcal{O}_X(V_1)$ é um $\mathcal{O}_Y(U_1)-$módulo finitamente gerado, C é um $\mathcal{O}_Q-$módulo finitamente gerado. Por fim, C é Noetheriano pois $\mathcal{O}_Q$ é. ■

Sejam k um corpo e $\varphi : X \to Y$ um morfismo não constante de grau n de curvas completas não singulares sobre k. Vamos assumir que este morfismo é dado pela inclusão de corpos de funções $k(Y) \subseteq k(X)$. Sejam $P \in X$ e C o fecho integral de $\mathcal{O}_{\varphi(P)}$ em $k(X)$. Então $\mathcal{O}_P$ é a localização de C num ideal maximal. A aplicação natural $\mathcal{O}_{\varphi(P)} \to \mathcal{O}_P$ induz uma aplicação entre os corpos residuais:

$$\frac{\mathcal{O}_{\varphi(P)}}{\mathcal{M}_{\varphi(P)}} \longrightarrow \frac{\mathcal{O}_P}{\mathcal{M}_P}.$$

Por C ser finitamente gerado como $\mathcal{O}_{\varphi(P)}-$álgebra, esta extensão é finita, denotaremos seu grau por $f_{P/\varphi(P)}$ e chamaremos de *grau residual* de P em $\varphi(P)$. O índice de ramificação de φ em P (ou de P sobre $\varphi(P)$) é o inteiro e_P (denotado também por $e_{P/\varphi(P)}$) tal que $\mathcal{M}_{\varphi(P)}\mathcal{O}_P = \mathcal{M}_P^{e_P}$.

Definição 5.7.5 *Seja $\varphi : X \to Y$ um morfismo entre curvas completas não singulares. Diremos que o ponto $P \in X$ é* não ramificado *sobre Y se $e_P = 1$ e o corpo residual $\mathcal{O}_P/\mathcal{M}_P$ é separável sobre $\mathcal{O}_{\varphi(P)}/\mathcal{M}_{\varphi(P)}$. Caso contrário, é* ramificado. *A imagem do conjunto dos pontos de ramificação é chamado de* lugar dos ramos *de φ.*

Seja $Q \in Y$. A seguir daremos uma descrição para a fibra $\varphi^{-1}(Q)$. Seja C o fecho integral de $\mathcal{O}_Q$ em $k(X)$. Como $C/\mathcal{O}_Q$ é integral, todo ideal maximal de C contém $\mathcal{M}_Q$. Visto que C é um domínio de Dedekind, C é semi-local. Cada ideal maximal de C corresponde a uma valorização v_i de $k(X), i = 1, \ldots, s$. Sejam $P_1, \ldots, P_s \in X$ os pontos correspondentes e $\mathcal{O}_{P_i}, i = 1, \ldots, s$ os domínios locais principais associados a P_i's. Então

$$\varphi^{-1}(Q) = \{P_1, \ldots, P_s\}.$$

Como C é uma $\mathcal{O}_Q-$álgebra finitamente gerada, pelo teorema 2.2.1, $\sum_{P \in \varphi^{-1}(Q)} e_{P/Q} f_{P/Q} = \deg(\varphi)$. Em particular, $\#\varphi^{-1}(Q) \leq \deg(\varphi)$. De fato acabamos de provar a primeira parte da seguinte proposição:

Proposição 5.7.1 *Sejam k um corpo e $\varphi : X \to Y$ um morfismo não constante de curvas completas não singulares sobre k. Então φ é sobrejetiva com fibras finitas de cardinalidade no máximo n.*

Se φ é um morfismo separável, então o lugar dos ramos é um conjunto finito. Em particular, quando k é algebricamente fechado e φ é separável, então existe um aberto denso $U \subseteq Y$ tal que $\#\varphi^{-1}(P) = n$ para todo $P \in U$.

Demonstração: *Mostraremos agora que o lugar dos ramos é finito, escolha a cobertura aberta $\{U_1, U_2\}$ de Y como no lema 5.7.1. Uma vez que U_1 é aberto, seu complementar*

em Y é finito. Assim, para mostrar que o lugar dos ramos de φ é um conjunto finito, é suficiente mostrar que o lugar dos ramos de φ restrito a V_1 é finito. Por construção, um ponto $Q \in U_1$ é a imagem de um ponto de ramificação $P \in V_1$ se, e só se, o ideal maximal $\mathcal{M}_Q \cap \mathcal{O}_Y(U_1)$ contém o ideal discriminante da extensão da extensão $\mathcal{O}_X(V_1)/\mathcal{O}_Y(U_1)$, veja 3.3.1. Por hipótese, φ é separável, logo o ideal discriminante é um ideal não nulo. Portanto, pode haver apenas uma quantidade finita de pontos em U_1 que são imagens dos pontos de ramificação.

Para a última parte, seja U o complemento em Y do lugar dos ramos. Mostramos acima que U é sempre um aberto quando φ é separável. Supondo k ser algebricamente fechado, as fibras de φ sobre os pontos de U contém exatamente n pontos distintos. ■

5.8 Corpo de Definição

Nesta seção, consideraremos sempre k um corpo perfeito.

Definição 5.8.1 *Sejam $k \subseteq E$ corpos e $\overline{X}/E$ uma curva completa não singular. Diremos que $\overline{X}/E$ é definida sobre k se o corpo de funções $E(\overline{X})|E$ contém um corpo de funções $L|k$ tal que $EL = E(\overline{X})$. Denotaremos o corpo de funções L por $k(X)$ e X/k a curva completa não singular associada a $k(X)|k$.*

Sejam $f \in k[x, y]$ absolutamente irredutível, $\overline{k}(Z_f)|\overline{k}$ o corpo de funções associado a curva afim $Z_f(\overline{k})$ e $\overline{X}/\overline{k}$ a curva completa não singular associada. Então $\overline{X}/\overline{k}$ é definida sobre k uma vez que $\overline{k}(Z_f)|\overline{k}$ contém o corpo de funções $k(Z_f)|k$, onde $k(Z_f)$ é o corpo de frações do anel $k[x, y]/\langle f \rangle$.

Observação 5.8.1 *Sejam $\overline{X}/E$ uma curva completa não singular e $k \subseteq E$ um subcorpo. É muito difícil em geral, determinar se $\overline{X}/E$ pode ser definida sobre k. O teorema de Belyi afirma que a curva completa não singular $\overline{X}/\mathbb{C}$ pode ser definida sobre $\overline{\mathbb{Q}}$ se, e somente se, existe um morfismo $\pi : \overline{X} \to \mathbb{P}^1$ sobre $\mathbb{C}$ cujo lugar dos ramos está contida em $\{0, 1, \infty\}$. Uma análogo deste resultado foi dado por Saïdi: Sejam p um primo ímpar e E um corpo algebricamente fechado de característica p. Seja $\overline{\mathbb{F}}_p \subseteq E$ o fecho algébrico de $\mathbb{F}_p$ em E. Então a curva completa não singular $\overline{X}/E$ pode ser definida sobre $\overline{\mathbb{F}}_p$ se, e somente se, existe um morfismo $\pi : \overline{X} \to \mathbb{P}^1$ sobre E cujo lugar dos ramos está contido em $\{0, 1, \infty\}$ e o índice de ramificação de cada ponto de ramificação de π é primo com p.*

Se $\overline{X}/\overline{k}$ pode ser definida sobre k, então ela pode ser definida sobre k por vários caminhos diferentes, isto é, podem existir alguns corpos de funções não isomorfos $k(X_j)|k$ inclusos em $\overline{k}(X)$ tais que $\overline{k}k(X_j) = \overline{k}(X)$.

Se X/k e Y/k são duas curvas completas não singulares tais que $X_{\overline{k}}/\overline{k}$ e $Y_{\overline{k}}/\overline{k}$ são isomorfas como curvas não singulares sobre $\overline{k}$, então a curva Y é chamada uma *forma de torção*, ou simplesmente *torção* da curva X (ou vice-versa).

Definição 5.8.2 *Sejam k um corpo perfeito, X/k e Y/k duas curvas completas não singulares e $\pi : X \to Y$ um morfismo de curvas sobre k induzida pela inclusão $k(Y) \subseteq k(X)$. Sejam $\overline{k(X)}$ o fecho algébrico de $k(X)$, $\overline{k}$ o fecho algébrico de k em $\overline{k(X)}$ e $k'|k$ uma extensão em $\overline{k}$. Diremos que o morfismo π pode ser estendido para o morfismo $\pi_{k'} : X_{k'} \to Y_{k'}$ induzido pela inclusão $k'(Y) \subseteq k'(X)$.*

Quando $k' = \overline{k}$, denotaremos π' por $\overline{\pi}$. Quando π é dado por um homomorfismo $\pi^* : k(Y) \to k(X)$, podemos definir para qualquer extensão de corpos $i : k \to k'$ o morfismo estendido $\pi_{k'} : X_{k'} \to Y_{k'}$ por ser o morfismo associado a aplicação

$$\pi^* \otimes i : k(Y) \otimes_k k' \to k(X) \otimes_k k'.$$

Definição 5.8.3 *Sejam X/k e Y/k duas curvas completas não singulares e $\mu : X_{\overline{k}} \to Y_{\overline{k}}$ um morfismo de curvas sobre $\overline{k}$. Diremos que μ sobre a extensão $E|k$, $E \subseteq \overline{k}$, se existe um morfismo de curvas $\pi : X_E \to Y_E$ sobre E tal que $\mu = \pi_{\overline{k}}$.*

Exemplo 5.8.1 *Seja X/k uma curva completa não singular associada a $k(X) := \frac{k(x)[y]}{\langle y^n - g(x)\rangle}$, onde $g \in k[x]$ e $y^n - g(x)$ é absolutamente irredutível. Sejam $\zeta_n \in \overline{k}$ uma raiz $n-$ésima da unidade e $\mu^* : \overline{k}(X) \to \overline{k}(X)$ o automorfismo dado por $y \mapsto \zeta_n y$ e $x \mapsto x$. O morfismo associado $\mu : X_{\overline{k}} \to X_{\overline{k}}$ é definido sobre $k(\zeta_n)$. A curva $X_{\overline{k}}$ pode ser definida sobre k. Pode se mostrar que o automorfismo $\mu \in \mathrm{Aut}(X_{\overline{k}})$ não pode ser definido sobre k se $k \neq k(\zeta_n)$.*

Lema 5.8.1 *Sejam X/k e Y/k duas curvas completas não singulares e $\mu : X_{\overline{k}} \to Y_{\overline{k}}$ um morfismo sobre $\overline{k}$. Então μ pode ser definida sobre uma extensão finita de k.*
Demonstração: *Sejam $y_1, y_2, \ldots, y_s \in k(Y)$ tais que $[k(Y) : k(y_1)] < \infty$ e $k(Y) = k(y_1, \ldots, y_s)$. Escreva $\mu^*(y_j) = \sum_{i=1}^{r_j} a_{ij}\alpha_{ij}$, com $a_{ij} \in \overline{k}$ e $\alpha_{ij} \in k(X)$. Seja $E \supset k$ o corpo gerado por $a_{ij}, 1 \leqslant i \leqslant r_j, 1 \leqslant j \leqslant s$. Então $\mu^*_{|_{E(Y)}}$ é um homomorfismo $E(Y) \to E(X)$. Portanto $\mu^*_{|_{E(Y)}}$ define um morfismo $\mu_E : X_E \to Y_E$ de curvas sobre E tal que μ é o morfismo sobre $\overline{k}$ obtido de μ_E por extensão de escalares de E para $\overline{k}$.*

Dado uma curva projetiva $X_F(\overline{k})$, definimos em 5.5 o corpo de definição sobre k do ponto $P \in X_F(\overline{k})$ somente quando F define uma curva com coeficientes em k. Seja $\overline{X}/\overline{k}$ uma curva completa não singular. Em analogia com o caso das curvas projetivas, definimos abaixo o conceito de *corpo de definição* sobre k de um ponto $P \in \overline{X}$ quando a curva

$\overline{X}/\overline{k}$ é dada por uma mudança de base da curva X/k. Como no caso de curvas planas, primeiro precisamos definir uma ação do grupo $\mathrm{Gal}(\overline{k}|k)$ sobre o conjunto $\overline{X}$.

Sejam X/k uma curva completa não singular, $\overline{k(X)}$ o fecho algébrico de $k(X)$ e $\overline{k}$ o fecho algébrico de k em $\overline{k(X)}$. Considere a aplicação natural

$$\begin{array}{ccc} r : \mathrm{Gal}(\overline{k}(X)|k(X)) & \longrightarrow & \mathrm{Gal}(\overline{k}|k) \\ \sigma & \longmapsto & \sigma_{|_{\overline{k}}} \end{array}.$$

Como $\overline{k}(X) = \overline{k} \cdot k(X)$, r é injetiva. Por k ser perfeito, r é um isomorfismo de grupos (veja [6], pág. 254).

Sejam X/k uma curva completa não singular e $X_{\overline{k}}/\overline{k}$ a mudança de base de X. Identificamos $X_{\overline{k}}$ com $\mathcal{P}(\overline{k}(X)|\overline{k})$ e X com $\mathcal{P}(k(X)|k)$. Considere a seguinte ação de $\mathrm{Gal}(\overline{k}|k)$ em $X_{\overline{k}}$:

$$\forall \sigma \in \mathrm{Gal}(\overline{k}|k),\ \forall P \in X_{\overline{k}},\ \text{seja } \sigma \cdot P \text{ tal que } \mathcal{O}_{\sigma \cdot P} := \sigma(\mathcal{O}_P).$$

Em outras palavras, a ação de $\mathrm{Gal}(\overline{k}|k)$ em $\mathcal{P}(\overline{k}(X)|\overline{k})$ é $\sigma \cdot \overline{\mathcal{O}} := \sigma(\overline{\mathcal{O}})$, para todo $\sigma \in \mathrm{Gal}(\overline{k}|k)$ e para todo $\overline{\mathcal{O}} \in \mathcal{P}(\overline{k}(X)|\overline{k})$. Note que o grupo $\mathrm{Gal}(\overline{k}|k)$ age em $X_{\overline{k}}$ por permutação e não através de um morfismo de curvas, uma vez que a aplicação $\sigma : \overline{k}(X) \to \overline{k}(X)$ não é um homomorfismo de $\overline{k}-$álgebras.

Considere a aplicação $I : X_{\overline{k}} \to X$ dada por $\overline{P} \mapsto P$, onde P é detreminado pela condição $\mathcal{O}_P := \mathcal{O}_{\overline{P}} \cap k(X)$.

Proposição 5.8.1 *Seja k um corpo perfeito. Seja X/k uma curva completa não singular. A aplicação I é sobrejetiva. Então existe uma bijeção entre X e o conjunto de órbitas de $X_{\overline{k}}$ sobre a ação de* $\mathrm{Gal}(\overline{k}|k)$.

Demonstração: *Para mostrar que I está bem definida, observe que se uma valorização de $\overline{k}(X)$ é trivial em $k(X)^*$, então é trivial em k^*, portanto trivial em $\overline{k}^*$. Como $\overline{k}(X) = \overline{k}k(X)$, a mesma valorização é trivial em $\overline{k}(X)^*$. Portanto, se $\overline{\mathcal{O}}$ é um domínio local principal (i.é, corresponde a uma valorização não trivial), então $\overline{\mathcal{O}} \cap k(X)$ também é.*

Sejam $P \in X$ e v a correspondente valorização. Considere o conjunto Σ dos pares (L, w), onde $k(X) \subseteq L \subseteq \overline{k}(X)$ e $w : L^* \to \mathbb{Z}$ estende v. O conjunto Σ é munido de uma ordem parcial como segue:

$$(L, w) \leq (L', w') \Longleftrightarrow L \subseteq L' \ \ e \ \ w'_{|_{L^*}} = w.$$

As condições do lema de Zorn são satisfeitas e, portanto, Σ tem elemento maximal. Seja (M, ω) um elemento maximal de Σ. Mostraremos que $M = \overline{k}(X)$. De fato, se $M \neq \overline{k}(X)$,

então existiria $\alpha \in \overline{k} \setminus M$. Seja $\mathcal{O}_\omega$ o anel de valorização discreta associado a ω, considere a extensão $M(\alpha)|M$. Sejam B o fecho integral de $\mathcal{O}_\omega$ em $M(\alpha)$ e $\mathcal{M} \in \mathrm{Max}(B)$. Pela proposição 2.5.2, $B/\mathcal{O}_\omega$ é não ramificada. Portanto, $v_{\mathcal{M}}$ estende ω, o que é absurdo pelo fato que (M, ω) é maximal. Então I é sobrejetiva.

Seja $P \in X$. Para mostrar que a imagem inversa de P é uma órbita sobre a ação do grupo de Galois, sejam $\overline{\mathcal{O}}_1, \overline{\mathcal{O}}_2 \in \mathcal{P}(\overline{k}(X)/\overline{k})$ tais que $\overline{\mathcal{O}}_1 \cap k(X) = \mathcal{O}_P = \overline{\mathcal{O}}_2 \cap k(X)$. Considere o conjunto Θ das triplas (L_1, L_2, σ), onde $k(X) \subseteq L_1, L_2 \subseteq \overline{k}(X)$, $\sigma : L_1 \to L_2$ é um isomorfismo de corpos e $\sigma(\overline{\mathcal{O}}_1 \cap L_1) = \overline{\mathcal{O}}_2 \cap L_2$. A seguinte ordem é uma ordem parcial em Θ :

$$(L_1, L_2, \sigma) \leq (L_1^{'}, L_2^{'}, \sigma') \Longleftrightarrow L_1 \subseteq L_1^{'}, L_2 \subseteq L_2^{'} \ \ e \ \ \sigma^{'}_{|_{L_1}} = \sigma.$$

Pelo lema de Zorn, Θ possui elemento maximal, digamos (M_1, M_2, σ). Afirmamos que $M_1 = \overline{k}(X)$. De fato, se $M_1 \neq \overline{k}(X)$, então existe $\alpha \in \overline{k} \setminus M_1$. Seja N_1 a menor extensão de Galois de $M_1(\alpha)$ em $\overline{k}(X)$ que é Galois sobre M_1. Dada uma extensão σ' de σ em N_1, seja $N_2 := \sigma(N_1)$. Sejam $\mathcal{O}_2 := \overline{\mathcal{O}}_2 \cap M_2$ e B_2 o fecho integral de $\mathcal{O}_2$ em N_2. Os anéis $\sigma'(\overline{\mathcal{O}}_1 \cap N_1)$ e $\overline{\mathcal{O}}_2 \cap N_2$ são as localizações de B_2 em dois ideais maximais distintos $\mathcal{M}_1$ e $\mathcal{M}_2$, respectivamente. Pela proposição 2.6.1, existe $\tau \in \mathrm{Gal}(N_2|M_2)$ tal que $\tau(\mathcal{M}_1) = \mathcal{M}_2$, isto é $(N_1, N_2, \tau \circ \sigma') \geq (M_1, M_2, \sigma)$; absurdo pela maximalidade de (M_1, M_2, σ). Logo $M_1 = \overline{k}(X)$. Como $\sigma(\overline{k}) = \overline{k}$ e $M_2 = \overline{k}(X)$. Portanto, $\sigma \in \mathrm{Gal}(\overline{k}(X)|k(X))$, com $\sigma(\overline{\mathcal{O}}_1) = \overline{\mathcal{O}}_2$. ■

Definição 5.8.4 *Sejam X/k uma curva completa não singular e $X_{\overline{k}}/\overline{k}$ a curva completa não singular obtida por extensão de escalares em $\overline{k}$. O grupo de Galois $\mathrm{Gal}(\overline{k}|k)$ age em $X_{\overline{k}}$ como antes. Seja $P \in X_{\overline{k}}$, o* corpo de definição *de P sobre k, denotado por $k(P)$, é o subcorpo de $\overline{k}$ fixado pelo subgrupo $\mathrm{Stab}(P) := \{\sigma \in \mathrm{Gal}(\overline{k}|k) \mid \sigma(P) = P\}$. Mais precisamente,*

$$k(P) := \overline{k}^{\mathrm{Stab}(P)} = \{c \in \overline{k} \mid \sigma(c) = c, \forall \sigma \in \mathrm{Stab}(P)\}.$$

Lema 5.8.2 *Sejam k um corpo perfeito, X/k uma curva completa não singular e $P \in X_{\overline{k}}$. Então a extensão $[k(P) : k] < \infty$ e a órbita de P sobre a ação de $\mathrm{Gal}(\overline{k}|k)$ contém $[k(P) : k]$ elementos.*

Demonstração: *Sejam $\overline{\mathcal{O}}$ o domínio local principal correspondente a P, $\mathcal{O} := \overline{\mathcal{O}} \cap k(X)$ e π o gerador do ideal maximal de $\mathcal{O}$. Então, para todo $\sigma \in \mathrm{Gal}(\overline{k}|k), \sigma(\pi) = \pi \in \sigma(\overline{\mathcal{O}})$. Assim, a valorização de π, em $\sigma(\overline{\mathcal{O}})$ é positiva para todo $\sigma \in \mathrm{Gal}(\overline{k}|k)$. Segue da proposição 5.6.1 que $\#\{\sigma(\overline{\mathcal{O}})|\sigma \in \mathrm{Gal}(\overline{k}|k)\} < \infty$. Uma vez que $\mathrm{Gal}(\overline{k}|k)/\mathrm{Stab}(P)$ está*

em bijeção com a órbita de P e é finito, pelo teorema de correspondência de Galois, segue que $k(P) := \overline{k}^{\mathrm{Stab}(P)}$ é uma extensão finita de k. ■

Definição 5.8.5 *Sejam X/k uma curva completa não singular e $k'|k$ uma extensão de k em $\overline{k}$. Definimos o conjunto $X(k') := \{P \in X_{\overline{k}} \mid k(P) \subseteq k'\}$ como o conjunto dos $k'-$*pontos racionais da curva *X/k.*

Definição 5.8.6 *Sejam k um corpo, X/k uma curva completa não singular, $Q \in X$ e $\mathcal{O}_Q$ o domínio local de ideal principais (veja 5.3.1) em $k(X)$ correspondente a Q. O grau de Q, é definido por* $\deg(Q) := [\frac{\mathcal{O}_Q}{\mathcal{M}_Q} : k]$.

Definição 5.8.7 *Sejam k um corpo perfeito, X/k uma curva completa não singular e $P \in X(\overline{k})$. Definimos o grau de P por* $\deg(P) := [k(P) : k]$.

Quando k é perfeito, os graus de um ponto de $X(\overline{k})$ e de sua imagem pela aplicação natural $X_{\overline{k}} \to X$, são iguais (veja [6], pág. 256).

A seguir veremos o resultado análogo da proposição 5.5.2 para curvas completas sobre corpos finitos. Sejam $X/\mathbb{F}_q$ uma curva completa não singular e $\overline{\mathbb{F}_q(X)}$ o fecho algébrico de $\mathbb{F}_q(X)$. Sejam $\overline{\mathbb{F}}_q$ o fecho algébrico de $\mathbb{F}_q$ em $\overline{\mathbb{F}_q(X)}$ e $\mathbb{F}_{q^n}$ o único subcorpo de $\overline{\mathbb{F}}_q$ de grau n sobre $\mathbb{F}_q$.

Lema 5.8.3 *Seja $X/\mathbb{F}_q$ uma curva completa não singular. Então para todo $n \in \mathbb{N}$, $\#X(\mathbb{F}_{q^n}) < \infty$.*
Demonstração: *Tome $x \in \mathbb{F}_q(X)$ tal que $\mathbb{F}_q(X)|\mathbb{F}_q(x)$ é finita e separável. Então, aplicando o lema 4.1.3 e o teorema 5.3.1, segue o resultado.* ■

Proposição 5.8.2 *Sejam $X/\mathbb{F}_q$ uma curva completa não singular, $N_n := \#X(\mathbb{F}_{q^n})$ e $b_d := \#\{Q \in X \mid \deg(Q) = d\}$. Então $N_n := \sum_{d|n} db_d$.*
Demonstração: *A prova é análogo à proposição 5.5.2. Basta observar que o conjunto das órbitas de $X(\mathbb{F}_{q^n})$ sobre a ação de $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ está com bijeção com $\bigcup_{d|n}\{Q \in X \mid |\frac{\mathcal{O}_Q}{\mathcal{M}_Q}| = q^d\}$.* ■

Lema 5.8.4 *Seja $X/\mathbb{F}_q$ uma curva completa não singular. Fixe um inteiro $e \geqslant 1$. Sejam $k' := \mathbb{F}_{q^e}$ e $N_n^{'} := \#X_{k'}(\mathbb{F}_{q^{en}})$. Então $N_n^{'} = N_{en}$.*
Demonstração: *Segue imediatamente das definições.* ■

5.9 O Divisor do Grupo de Classe

Sejam $f \in k[x,y]$ irredutível e $C_f = k[x,y]/\langle f\rangle$. Em 4, associamos ao domínio C_f o grupo abeliano $\mathrm{Cl}(C_f)$, chamado do grupo de classe de ideais de C_f. Nesta seção, analogamente, associaremos um grupo abeliano a uma curva completa não singular X/k. O novo grupo de classe introduzido nesta seção é chamado do *grupo de Picard* de X/k, ou *o grupo de classe divisor* de X/k e será denotado por $\mathrm{Pic}(X/k)$. Antes de definir o grupo $\mathrm{Pic}(X/k)$ associado a uma curva, consideraremos o caso mais geral para um corpo qualquer L contendo um domínio de Dedekind B cujo corpo de frações é L (se $L = k(X)$, então B pode ser pensado como o anel das funções num subconjunto aberto de X). Para motivar a definição do grupo de classe associado a um corpo L, introduziremos agora a seguinte descrição alternativa para $\mathrm{Cl}(B)$: Sejam $\mathcal{V}(L)$ o conjunto de todas as valorizações não triviais e sobrejetivas de L e

$$\mathrm{Div}(B) := \bigoplus_{v\in\mathcal{V}(L),\ v(B)\geqslant 0} \mathbb{Z}x_v.$$

O grupo $\mathrm{Div}(B)$ é o grupo abeliano livre gerado pelo conjunto $\{x_v \mid v \in \mathcal{V}(L), v(B) \geq 0\}$. Um elemento $D \in \mathrm{Div}(B)$ é uma soma formal $\sum_v a_v x_v$, onde $a_v = 0$ exceto para um número finito de $v \in \mathcal{V}(L)$ tal que $v(B) \geq 0$. Seja

$$\begin{array}{rcl} \mathrm{div}_B : L^* & \longrightarrow & \mathrm{Div}(B) \\ f & \longmapsto & \displaystyle\sum_{v\in\mathcal{V}(L), v(B)\geq 0} v(f)x_v. \end{array}$$

A aplicação div_B está bem definida. De fato, todo $f \in L^*$ é um quociente de dois elementos $g, h \in B$. Uma vez que B é Noetheriano, os ideais gB e hB estão contidos numa quantidade finita de ideals maximais de B, digamos $M_1, \ldots, M_r$. A proposição 5.3.2 nos garante que toda valorização de L que é não negativa em B é uma valorização $M-$ádica, para algum $M \in \mathrm{Max}(B)$. Portanto, $v(f) = 0$ para todas as valorizações $v \in \mathcal{V}(L), v(B) \geqslant 0$, exceto possivelmente para $v_{M_1}, \ldots, v_{M_r}$.

Proposição 5.9.1 *(Descrição Aditiva do grupo de classe de ideais) Seja B um domínio de Dedekind com corpo de frações L. O homomorfismo e grupos*

$$\begin{array}{rcl} \mathrm{cl} : \mathrm{Div}(B) & \longrightarrow & \mathrm{Cl}(B) \\ x_v & \longmapsto & \textit{classe de } \mathcal{M}_v \cap B \end{array}$$

induz um isomorfismo de grupos entre $\mathrm{Div}(B)/\mathrm{div}_B(L^*)$ *e* $\mathrm{Cl}(B)$.

Demonstração: *Primeiro mostraremos que* cl *é sobrejetora. De fato, todo elemento $\mathcal{C} \in \mathrm{Cl}(B)$ é classe de algum ideal não nulo $I \subseteq B$. Por B ser Dedekind, podemos fatorar*

$I = \prod_{i=1}^{r} M_i^{a_i}$ e observe que $M_i = \mathcal{M}_{v_{M_i}} \cap B$. Então $\mathrm{cl}(\sum_i a_i x_{v_{M_i}}) =$ *classe de* $I = \mathcal{C}$. *Agora, seja $f \in L^*$, então $f = a/b$ com $a, b \in B$. Portanto,*

$$\mathrm{div}_B(f) = \mathrm{div}_B(a) - \mathrm{div}_B(b)$$

e

$$\mathrm{cl}(\mathrm{div}_B(f)) = (\textit{classe de } aB) \cdot (\textit{classe de } bB)^{-1} = \textit{classe de } B.$$

Assim, $\mathrm{div}_B(L^*) \subseteq \ker(\mathrm{cl})$. *Tome* $D \in \ker(\mathrm{cl})$, *isto é,* $\mathrm{cl}(D) = \langle 1 \rangle$. *Escreva* $D = D_0 - D_\infty$, *onde* $D_0 = \sum a_v x_v$ *e* $D_\infty = b_v x_v$ *são tais que* $a_v, b_v \geqslant 0$ *para todo* $v \in \mathcal{V}(L), v(B) \geqslant 0$. *Seja* $I_{D_0} := \prod_v (\mathcal{M}_v \cap B)^{a_v}$ *e* $I_{D_\infty} := \prod_v (\mathcal{M}_v \cap B)^{b_v}$. *Então*

$$\mathrm{cl}(D) = \textit{classe de } B = (\textit{classe de } I_{D_0}) \cdot (\textit{classe de } I_{D_\infty})^{-1}.$$

Em particular, classe de I_{D_0} = classe de I_{D_∞}. *Portanto, existem* $\alpha, \beta \in B$ *tais que* $\alpha I_{D_0} = \beta I_{D_\infty}$. *Escrevendo explicitamente a fatoração destes ideais, obtemos:*

$$\prod_v (\mathcal{M}_v \cap B)^{v(\alpha)} \prod_v (\mathcal{M}_v \cap B)^{a_v} = \prod_v (\mathcal{M}_v \cap B)^{v(\beta)} \prod_v (\mathcal{M}_v \cap B)^{b_v}.$$

A propriedade de fatoração única de ideais implica que $\mathrm{div}_B(\alpha) + D_0 = \mathrm{div}_B(\beta) + D_\infty$. *Então* $D = D_0 - D_\infty = \mathrm{div}_B(\beta/\alpha) \in \mathrm{div}_B(L^*)$. *Portanto* $\mathrm{div}_B(L^*) = \ker(\mathrm{cl})$. ■

A descrição anterior para $\mathrm{Cl}(B)$ motiva a seguinte definição:

Definição 5.9.1 *Sejam $L|k$ uma extensão de corpos e $\mathcal{V}(L|k)$ o conjunto das valorizações sobrejetivas de L que são triviais em k. Quando $\mathcal{V}(L|k) \neq \emptyset$, o grupo abeliano livre* $\mathrm{Div}(L|k)$ *gerado pelo conjunto $\{x_v | v \in \mathcal{V}(L|k)\}$,*

$$\mathrm{Div}(L|k) := \bigoplus_{v \in \mathcal{V}(L|k)} \mathbb{Z} x_v,$$

é chamado do grupo dos divisores *de $L|k$. Um elemento $D \in \mathrm{Div}(L|k)$ é da forma $D = \sum a_v x_v$, com $a_v \in \mathbb{Z}$ e $a_v = 0$ exceto para um número finito de $v \in \mathcal{V}(L|k)$. O elemento D é chamado de* um divisor *de L. Se $a_v \geqslant 0$ para todo $v \in \mathcal{V}(L|k)$, então D é chamado de um divisor* efetivo *ou* positivo.

Considere a aplicação

$$\begin{array}{rcl} \mathrm{div}_L : L^* & \longrightarrow & \mathrm{Div}(L|k) \\ f & \longmapsto & \mathrm{div}_L(f) := \sum_{v \in \mathcal{V}(L|k)} v(f) x_v. \end{array}$$

Quando não causar confusão, denotaremos a aplicação div_L simplesmente por div. A proposição 5.6.1 mostra que, quando L é uma extensão finita de $k(x)$, então a aplicação div está bem definida. Portanto a partir de agora sempre suponhamos $L|k(x)$ finita.

Definição 5.9.2 *Seja $L|k(x)$ uma extensão finita de corpos. O* grupo de Picard $\mathrm{Pic}(L|k)$ *é o quociente do grupo* $\mathrm{Div}(L|k)$ *pela imagem da aplicação* div.

A seguinte sequência de grupos abelianos é exata:

$$\langle 1\rangle \longrightarrow \bigcap_{v\in\mathcal{V}(L|k)} \mathcal{O}_v^* \longrightarrow L^* \xrightarrow{\mathrm{div}} \mathrm{Div}(L|k) \xrightarrow{\mathrm{cl}} \mathrm{Pic}(L|k) \longrightarrow \langle 0\rangle.$$

Seja $L|k(x)$ uma extensão finita. Seja B um domínio de Dedekind com corpo de frações L. Claramente quando $k \subseteq B$, $\{v \in \mathcal{V}(L)|v(B) \geqslant 0\} = \{v \in \mathcal{V}(L|k)|v(B) \geqslant 0\}$. Defina a aplicação restrição:

$$\begin{array}{ccc} \mathrm{res} : \mathrm{Div}(L|k) & \longrightarrow & \mathrm{Div}(B) \\ \displaystyle\sum_{v\in\mathcal{V}(L|k)} a_v x_v & \longmapsto & \displaystyle\sum_{v\in\mathcal{V}(L|k)\ v(B)\geqslant 0} a_v x_v \end{array}$$

Segue da definição que $\mathrm{res} \circ \mathrm{div}_L = \mathrm{div}_B$.

Relembre que, se B é um domínio de Dedekind, a proposição 0.1.2 mostra que $B = \bigcap_{v\in\mathcal{V}(L|k),v(B)\geqslant 0} \mathcal{O}_v$. Sendo assim, o próximo lema segue do fato de que $\ker(\mathrm{div}_B) = B^*$.

Lema 5.9.1 *Seja $k' := \bigcap_{v\in\mathcal{V}(L|k)} \mathcal{O}_v$. A aplicação* res *induz o seguinte diagrama comutativo com as linhas formando sequências exatas:*

$$\begin{array}{ccccccccccc} \langle 1\rangle & \longrightarrow & (k')^* & \longrightarrow & L^* & \xrightarrow{\mathrm{div}_L} & \mathrm{Div}(L|k) & \longrightarrow & \mathrm{Pic}(L|k) & \longrightarrow & \langle 0\rangle \\ & & \downarrow & & \| & & \mathrm{res}\downarrow & & \downarrow & & \\ \langle 1\rangle & \longrightarrow & B^* & \longrightarrow & L^* & \xrightarrow{\mathrm{div}_B} & \mathrm{Div}(B) & \longrightarrow & \mathrm{Cl}(B) & \longrightarrow & \langle 1\rangle \end{array}$$

Observação 5.9.1 *Sejam k um corpo, $k(X)/k$ um corpo de funções e X/k a curva completa não singular associada. Cada ponto $P \in X$ é associado a um domínio local principal $\mathcal{O}_P$ com valorização v_P. Seja*

$$\mathrm{Div}(X/k) := \bigoplus_{P\in X} \mathbb{Z}P$$

e

$$\begin{array}{ccc} \mathrm{div} : k(X)^* & \longrightarrow & \mathrm{Div}(X/k) \\ f & \longmapsto & \sum_{P\in X} v_P(f)P. \end{array}$$

Ao identificarmos X com $\mathcal{V}(k(X)|k)$, o grupo $\mathrm{Div}(X/k)$ *pode ser identificado com o grupo* $\mathrm{Div}(k(X)/k)$ *de tal modo que a aplicação* div *identifica-se com* $\mathrm{div}_{k(X)}$. *O teorema 5.6.2 mostra que* $\ker(\mathrm{div}) = k^*$. *Seja* $\mathrm{Pic}(X/k)$ *o quociente de* $\mathrm{Div}(X/k)$ *pela imagem de* div. *Por construção, a seguinte sequência é exata:*

$$\langle 1\rangle \longrightarrow k^* \longrightarrow k(X)^* \xrightarrow{\mathrm{div}} \mathrm{Div}(X/k) \xrightarrow{\mathrm{cl}} \mathrm{Pic}(X/k) \longrightarrow \langle 0\rangle.$$

Sejam $F \in \overline{k}[x_0, x_1, x_2]$ homogêneo, $X_F(\overline{k})$ a curva projetiva plana não singular definida por F e $\overline{k}(X_F)|k$ o corpo das funções de $X_F(\overline{k})$. Considere $X/\overline{k}$ a curva completa não singular associada a $\overline{k}(X_F)|k$. Ao identificar X com $X_F(\overline{k})$, um divisor $D \in \mathrm{Div}(X/\overline{k})$ pode ser pensado como um subconjunto finito de pontos de $X_F(\overline{k})$. Uma maneira de produzir divisores efetivos em $X_F(\overline{k})$ é interceptar a curva $X_F(\overline{k})$ com outra curva plana. Seja $X_H(\overline{k})$ uma curva plana que intercepta $X_F(\overline{k})$ em finitos pontos.

Definição 5.9.3 *Seja $P \in X_F(\overline{k})$. Pelo menos uma das funções $\frac{H}{x_0^{\deg H}}, \frac{H}{x_1^{\deg H}}, \frac{H}{x_2^{\deg H}} \in \overline{k}(X_F)$ pertencem a $\mathcal{O}_P$. Se $H/x_i^{\deg H} \in \mathcal{O}_P$, definimos a* multiplicidade de interseção *de $X_F(\overline{k})$ e $X_H(\overline{k})$ em P por*

$$I_P(X_F, X_H) := v_P(H/x_i^{\deg H}).$$

É fácil ver que $I_P(X_F, X_H)$ não depende da escolha de i tal que $H/x_i^{\deg H} \in \mathcal{O}_P$. Além disso, $I_P(X_F, X_H) := 0$ se $P \notin X_F(\overline{k}) \cap X_H(\overline{k})$.

Observe que $I_P(X_F, X_H) = 1$ se as curvas dadas têm retas tangentes distintas em P e é maior que 1 caso contrário. O divisor $\sum_{P\in X} I_P(X_F, X_H)P$ é chamado do *divisor interseção* de $X_F(\overline{k})$ e $X_H(\overline{k})$.

Dois divisores cujas imagens são iguais em $\mathrm{Pic}(X/k)$ são chamados de *linearmente equivalentes*. Se G e H são polinômio homogêneos de mesmo grau tais que $X_F(\overline{k}) \cap X_H(\overline{k})$ e $X_F(\overline{k}) \cap X_G(\overline{k})$ são finitos, então os divisores associados $D_1 := \sum_{P\in X} I_P(X_F, X_H)P$ e $D_2 := \sum_{P\in X} I_P(X_F, X_G)P$ são linearmente equivalentes. De fato, $D_1 - D_2 = \mathrm{div}(G/H)$.

Definição 5.9.4 *Sejam k um corpo e X/k uma curva completa não singular. Definimos a aplicação* deg *por*

$$\begin{array}{rcl} \deg : \mathrm{Div}(X/k) & \longrightarrow & \mathbb{Z} \\ \sum_{P\in X} a_P P & \longmapsto & \sum_P a_P \deg(P). \end{array}$$

O inteiro $\sum_P a_P \deg(P)$ é chamado do grau do divisor D.

Seja $\pi : X \to Y$ um morfismo de curvas completa não singulares sobre k. A proposição 5.7.1 mostra que π é sobrejetiva. Dado $P \in X$, seja $f_{P/\pi(P)} := [\mathcal{O}_P/\mathcal{M}_P : \mathcal{O}_{\pi(P)}/\mathcal{M}_{\pi(P)}]$

o grau residual. Segue da definição que

$$\deg(P) = f_{P/\pi(P)} \deg(\pi(P)).$$

Dada a extensão $k(X)|k(Y)$, associamos em 3.1 a aplicação $\mathrm{Norm}_{k(X)/k(Y)}$. Considere a seguinte aplicação *norma-divisor*

$$\begin{array}{ccc} \mathrm{Norm}_{X/Y} : \mathrm{Div}(X/k) & \longrightarrow & \mathrm{Div}(Y/k) \\ \sum_P a_P P & \longmapsto & \sum_P a_P f_{P/\pi(P)} \pi(P). \end{array}$$

Teorema 5.9.1 *Sejam k um corpo e X/k uma curva completa não singular. Então, para todo $\alpha \in k(X)^*$, $\deg(\mathrm{div}(\alpha)) = 0$.*

Para a demonstração veja [6], página 264.

Corolário 5.9.1 *Seja X/k uma curva completa não singular. A aplicação* deg : $\mathrm{Div}(X/k) \to \mathbb{Z}$ *induz um homomorfismo não trivial de grupos* deg : $\mathrm{Pic}(X/k) \to \mathbb{Z}$, *dado por* $\mathrm{cl}(D) \mapsto \deg(D)$.
Demonstração: *O fato da aplicação* deg *estar bem definida segue imediatamente do teorema 5.9.1. A aplicação* deg *é não trivial uma vez que* $\mathrm{Div}(X/k)$ *contém divisores efetivos não nulos, portanto com graus positivos.* ■

Observação 5.9.2 *Sejam X/k uma curva completa não singular e $\alpha \in k(X) \setminus k$. Então α define um morfismo não constante $\pi : X \to \mathbb{P}^1$, induzida pela extensão $k(X)|k(\alpha)$. Sejam $0 \in \mathbb{P}^1$ o ponto correspondente a $\langle\alpha\rangle-$ádica valorização de $k[\alpha]$ e $\infty \in \mathbb{P}^1$ o ponto correspondente a $\langle 1/\alpha\rangle-$ádica valorização de $k[1/\alpha]$. Se*

$$(\alpha)_0 := \sum_{P \in \pi^{-1}(0)} v_P(\alpha) P \quad e \quad (\alpha)_\infty := \sum_{P \in \pi^{-1}(\infty)} v_P(\alpha) P,$$

então

$$\mathrm{div}(\alpha) = (\alpha)_0 - (\alpha)_\infty,$$

e o teorema 2.2.1 implica que $\deg((\alpha)_0) = \deg((\alpha)_\infty) = [k(X) : k(\alpha)]$.

Sejam X/k uma curva completa não singular, $\mathrm{Div}^0(X/k)$ denotando o núcleo da aplicação deg : $\mathrm{Div}(X/k) \to \mathbb{Z}$ e $\mathrm{Pic}^0(X/k)$ o núcleo da aplicação deg : $\mathrm{Pic}(X/k) \to \mathbb{Z}$. Observe que $\mathrm{Pic}^0(X/k) = \mathrm{Div}^0(X/k)/\mathrm{div}(k(X)^*)$ e das definições segue a exatidão da sequência:

$$\langle 1\rangle \longrightarrow k^* \longrightarrow k(X)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(X/k) \longrightarrow \mathrm{Pic}^0(X/k) \longrightarrow \langle 0\rangle.$$

Proposição 5.9.2 *Seja k um corpo. Então a aplicação* $\deg : \mathrm{Pic}(k(x)/k) \to \mathbb{Z}$ *é um isomorfismo. Em particular,* $\mathrm{Pic}(\mathbb{P}^1/k) = \{0\}$.
Demonstração: *O conjunto $\mathbb{P}^1 := \mathcal{V}(k(x)/k)$ sempre contém uma valorização de grau 1, denotado por v_∞ com $v_\infty(f) = -\deg(f(x))$. Portanto, a aplicação* deg *é sobrejetora. Mostraremos* $\mathrm{Pic}(k(x)/k) \cong \mathbb{Z}\mathrm{cl}(x_{v_\infty})$. *Pela proposição 5.3.3*

$$\mathcal{V}(k(x)/k) = \{v_g \mid g \in k[x] \quad \textit{irredutível}\} \cup \{v_\infty\}.$$

Seja $g \in k[x]$ irredutível. Uma vez que

$$\mathrm{div}_{k(x)}(g(x)) = 1 \cdot x_{v_g} - (\deg(g))x_{v_\infty},$$

segue que

$$\mathrm{cl}(x_{v_g}) = (\deg(g))\mathrm{cl}(x_{v_\infty})$$

em $\mathrm{Pic}(k(x)/k)$.

Como $\mathrm{Div}(k(x)/k)$ *é gerado pelo conjunto* $\{x_v | v \in \mathcal{V}(k(x)/k)\}$, *concluímos que* $\mathrm{Pic}(k(x)/k)$ *é gerado por* $\mathrm{cl}(x_{v_\infty})$. *Observe ainda que o elemento* $\mathrm{cl}(x_{v_\infty})$ *não pode ter ordem finita em* $\mathrm{Pic}(k(x)/k)$, *pois a aplicação* deg *é um homomorfismo de grupos e* $\deg(x_{v_\infty}) = 1$. *Assim,* $\deg : \mathrm{Pic}(k(x)/k) = \mathbb{Z}\mathrm{cl}(x_{v_\infty}) \to \mathbb{Z}$ *é um isomorfismo.* ■

Em geral, quando X/k não é a reta projetiva, o grupo $\mathrm{Pic}^0(X/k)$ não é finito. Contudo, quando k é um corpo finito, o teorema abaixo mostra que $\mathrm{Pic}^0(X/k)$ é um grupo finito. A prova do seguinte teorema usa o teorema de Riemann-Roch que veremos em 7, sua prova pode ser encontrada em [6], página 266.

Teorema 5.9.2 *Sejam k um corpo finito e X/k uma curva completa não singular. Então o grupo* $\mathrm{Pic}^0(X/k)$ *é finito.*

Quando k é um corpo finito, a ordem do grupo $\mathrm{Pic}^0(X/k)$ é chamada do *número da classe* de X/k e é denotada por h . Como discutiremos em 6.4.1, a hipótese de Riemann para curvas implica em boas limitações para h.

Observação 5.9.3 *Sejam $L|k(x)$ finita e separável de corpos e B o fecho integral de $k[x]$ em L. Considere a aplicação classe* $\mathrm{cl} : \mathrm{Div}(B) \to \mathrm{Cl}(B)$. *Toda classe de ideal $\mathcal{L}$ em* $\mathrm{Cl}(B)$ *contém um ideal $I = M_1^{a_1} \cdots M_r^{a_r}$. Portanto, segue da definição do grupo de classe que todo classe de ideal $\mathcal{L}$ é igual a classe de um divisor efetivo $D = \sum_{i=1}^{r} a_i x_{v_{M_i}} \in \mathrm{Div}(B)$.*

Definição 5.9.5 *Sejam $\pi : X \to Y$ um morfismo de curvas sobre k e $\pi^* : k(Y) \to k(X)$ a associada injeção de corpos. Definimos a aplicação de grupos (novamente denotado por*

π^*) $\mathrm{Div}(Y/k) \to \mathrm{Div}(X/k)$, a aplicação pull-back *em divisores, como segue: se $Q \in Y$, então seja*

$$\pi^*(Q) := \sum_{\{P|\pi(P)=Q\}} e_{P/Q}P,$$

onde $e_{P/Q}$ é o índice de ramificação. Esta aplicação é estendida por linearidade para $\mathrm{Div}(Y/k)$.

Por fim, segue o resultado:

Lema 5.9.2 $\mathrm{Norm}_{X/Y} \circ \pi^* =$ *multiplicação por* $\deg(\pi)$.

A aplicação π^* induz um homomorfismo de grupos

$$\pi^* : \mathrm{Pic}(Y/k) \longrightarrow \mathrm{Pic}(X/k).$$

Isto segue do seguinte fato:

Fato 5.9.1

$$\forall \alpha \in k(Y)^*,\ \pi^*(\mathrm{div}_Y(\alpha)) = \mathrm{div}_X(\pi^*(\alpha)).$$

Capítulo

6

Funções-Zeta

Neste capítulo $\mathbb{F}_q$ denotará o corpo finito de $q = p^r$ elementos, para algum primo p e um inteiro $r > 1$. Seja $F \in \mathbb{F}_q[X, Y, Z]$ um polinômio homogêneo. Nosso objetivo neste capítulo é estimar a ordem do conjunto dos pontos da curva definida por F, ou em outras palavras, o conjunto das soluções da equação $F = 0$,

$$X_F(\mathbb{F}_q) := \{(a_0 : a_1 : a_2) \in \mathbb{P}^2(\mathbb{F}_q) | F(a_0, a_1, a_2) = 0\}.$$

Mais geralmente, iremos fornecer cotas muito precisas para inteiros $N_n := |X_F(\mathbb{F}_{q^n})|$, onde $\mathbb{F}_{q^n}$ denota a única extensão Galoisiana de $\mathbb{F}_q$ de grau n. Primeiramente, observe que os conjuntos $X_F(\mathbb{F}_{q^n})$ são finitos. De fato, o plano projetivo $\mathbb{P}^2(\mathbb{F}_{q^n})$ possui $\frac{(q^n)^3-1}{q^n-1} = q^{2n} + q + 1$ elementos. Uma vez que $X_F(\mathbb{F}_q^n) \subseteq \mathbb{P}^2(\mathbb{F}_{q^n})$, o conjunto $X_F(\mathbb{F}_{q^n})$ é finito para todo $n \in \mathbb{N}$, de fato $N_n \leqslant q^{2n} + q^n + 1$.

Antes de estudar algumas propriedades da sequência $\{N_n\}_{n\in\mathbb{N}}$, discutiremos nesta introdução o caso em que $\deg(F) = 2$. Suponha primeiramente que $F = L^2$, para algum polinômio homogêneo L de grau 1 em $\mathbb{F}_q[x, y, z]$. Então $X_F(\mathbb{F}_{q^n}) = X_L(\mathbb{F}_{q^n})$ e $N_n = q^n+1$. Caso $F = L_1L_2$, onde $L_1 \neq L_2$ são dois polinômios homogêneos de grau 1 em $\mathbb{F}_q[x, y, z]$, $X_F(\mathbb{F}_{q^n}) = X_{L_1}(\mathbb{F}_{q^n}) \cup X_{L_2}(\mathbb{F}_{q^n})$ e $N_n = (q^n + 1) + (q^n + 1) - 1 = 2q^n + 1$.

Se $p \neq 2$, pela proposição 5.0.2 existe uma transformação projetiva $\varphi_{\mathbb{P}} \in \mathrm{GL}_3(\mathbb{F}_q)$ tal que $\varphi_{\mathbb{P}}(X_F(\mathbb{F}_{q^n})) = X_G(\mathbb{F}_{q^n})$, e

$$G(X, Y, Z) = a_0X^2 + a_1Y^2 + a_2Z^2 \in \mathbb{F}_q[x, y, z].$$

Permutando as variáveis se preciso, podemos supor $a_0 \neq 0$ e que se $a_1 = 0$ então $a_2 = 0$.

O primeiro caso tratado acima corresponde ao caso $a_1 = a_2 = 0$, e o segundo corresponde ao caso $a_1 \neq 0, a_2 = 0$ e $a_0X^2 + a_1Y^2$ redutível em $\mathbb{F}_q[x, y, z]$.

Sejam $a_2 = 0$ e $a_0X^2 + a_1Y^2$ irredutível em $\mathbb{F}_q[x, y, z]$. Então $\sqrt{\frac{-a_0}{a_1}} \notin \mathbb{F}_q$. Uma vez que $\mathbb{F}_{q^2}$ é uma extensão quadrática de $\mathbb{F}_q$, concluímos $\mathbb{F}_{q^2} = \mathbb{F}_q\left(\sqrt{\frac{-a_0}{a_1}}\right)$. Assim, quando $2 \nmid n$, $\sqrt{\frac{-a_0}{a_1}} \notin \mathbb{F}_{q^n}$ o que implica que G é irredutível em $\mathbb{F}_{q^n}[x, y, z]$, então $X_G(\mathbb{F}_{q^n}) = \{(0 : 0 : 1)\}$ e $N_n = 1$. Quando n é par, G se fatora em fatores lineares distintos em $\mathbb{F}_{q^n}[x, y, z]$ e $|X_G(\mathbb{F}_{q^n})| = 2q^n + 1$.

Vamos agora investigar o caso em que $a_0a_1a_2 \neq 0$. Pelo lema **??**, $X_F(\overline{\mathbb{F}}_q)$ e $X_G(\overline{\mathbb{F}}_q)$ são curvas suaves. Nos casos tratados anteriormente vimos que $X_F(\overline{\mathbb{F}}_q) \neq \emptyset$. Vamos mostrar que neste caso este fato também é verdadeiro. Considere o homomorfismo de grupos $\mathbb{F}_q^* \to \mathbb{F}_q^*$, dado por $\gamma \mapsto \gamma^2$. Seu núcleo é $\{\pm 1\}$. Portanto, $\#\{\gamma^2 | \gamma \in \mathbb{F}_q^*\} = \frac{(q-1)}{2}$. Então

$$\#\{a_0\gamma^2 | \gamma \in \mathbb{F}_q\} = \frac{(q-1)}{2} + 1 = \frac{(q+1)}{2}, \quad \#\{-a_1\beta^2 - a_2 | \beta \in \mathbb{F}_q\} = \frac{(q+1)}{2}.$$

Logo existe $(c_0, c_1) \in \mathbb{F}_q \times \mathbb{F}_q$ tal que $a_0c_0^2 = -a_1c_1^2 - a_2$. Isto é $(c_0 : c_1 : 1) \in X_G(\mathbb{F}_q)$. Logo $X_G(\mathbb{F}_q) \neq \emptyset$.

Proposição 6.0.3 *Sejam $F \in \mathbb{F}_q[x, y, z]$ homogêneo de grau 2 e $X_F(\overline{\mathbb{F}}_q)$ não singular. Então $N_n = q^n + 1$.*

Demonstração: *Podemos considerar $F(x_0, x_1, x_2) = x_0^2 - x_1x_2$ (veja [5]). Assim, a aplicação abaixo é um isomorfismo de curvas desde que $X_F(\mathbb{F}_q) \neq \emptyset$*

$$\begin{array}{ccc} X_F(\mathbb{F}_q) & \longrightarrow & \mathbb{P}^1(\mathbb{F}_q) \\ (a : 1 : 0) & \longmapsto & \infty \\ (a : b : 1) & \longmapsto & a/b. \end{array}$$

Do isomorfismo anterior segue que $N_n = |X_F(\mathbb{F}_{q^n})| = |\mathbb{P}^1(\mathbb{F}_{q^n})| = q^n + 1$. Resta mostrar que $X_F(\mathbb{F}_q) \neq \emptyset$. Pela nossa discussão anterior mostramos este fato para o caso em que $p \neq 2$. Pelo teorema 6.0.3, $X_F(\mathbb{F}_q) \neq \emptyset$ também quando $p = 2$, mais precisamente veja o corolário 6.0.2. ■

Lema 6.0.3 *Sejam $i_1, \ldots, i_n$ inteiros não negativos, então*

$$\sum_{(a_1,\ldots,a_n) \in (\mathbb{F}_q)^n} (a_1^{i_1} \cdots a_n^{i_n}) = 0,$$

a menos que cada i_j é não nulo e divisível por $q - 1$.

Demonstração: *Veja [6], página 271.*

Teorema 6.0.3 *Seja $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ de grau $d < n$. Seja N_f o número de soluções em $(\mathbb{F}_q)^n$ da equação $f(X_1, \ldots, X_n) = 0$. Então $p|N_f$. Em particular, se f é um polinômio homogêneo, então $N_f \geqslant 2$.*

Demonstração: *O polinômio $F := 1 - (f(X_1, \ldots, X_n))^{q-1}$ assume valor 1 nos zeros de f. Seja $\overline{N}_f$ a classe de N_f mod$p$, consideremos $\overline{N}_f$ como um elementos de $\mathbb{F}_p \subseteq \mathbb{F}_q$. Então,*

$$\overline{N}_f = \sum_{(a_1,\ldots,a_n)\in(\mathbb{F}_q)^n} (1 - (f(X_1, \ldots, X_n))^{q-1}).$$

Seja $X_1^{i_1} \cdots X_n^{i_n}$ um monômio ocorrendo no polinômio F. Como $\deg F = d(q-1)$ e uma vez que, por hipótese, $d < n$, pelo menos um expoente i_j deve ser menor que $q-1$. Para concluir a prova deste teorema observe que o polinômio é a soma (com coeficientes) da monômios da forma $X_1^{i_1} \cdots X_n^{i_n}$, com pelo menos um expoente i_j não divisível por $q-1$ ou igual a zero. Assim, segue do lema 6.0.3 que

$$\overline{N}_f = \sum_{(a_1,\ldots,a_n)\in(\mathbb{F}_q)^n} (1 - (f(X_1, \ldots, X_n))^{q-1}) = 0.$$

Portanto, $p|N_f$. ■

Corolário 6.0.2 *Seja $F \in \mathbb{F}_q[x, y, z]$ homogêneo de grau dois. Então, $X_F(\mathbb{F}_q) \neq \emptyset$.*

Demonstração: *Uma vez que $F(0, 0, 0) = 0$ e o grau de F é menor que o número de variáveis, pelo teorema 6.0.3, existe $(c_0, c_1, c_2) \neq (0, 0, 0)$ tal que $F(c_0, c_1, c_2) = 0$.* ■

Observação 6.0.4 *A hipótese $d < n$ no teorema anterior é necessária: Seja $p > 3$ um primo. O polinômio $F(X, Y, Z) = X^{p-1} + Y^{p-1} + Z^{p-1}$ é homogêneo de grau $p - 1 \geqslant 3$ e $X_F(\mathbb{F}_p) = \emptyset$.*

No próximo exemplo veremos que o caso de curvas de graus superiores a 2 não é tão simples quanto ao casos de reta e cônicas.

Exemplo 6.0.1 *Seja $F(X, Y, Z) = Y^2Z - X^3 - DZ^3$. Se $3 \nmid p-1$, então $|X_F(\mathbb{F}_p)| = p+1$. De fato, a curva possui apenas um ponto no infinito, a saber $(0 : 1 : 0)$. Portanto $|X_F(\mathbb{F}_p)| = |Z_f(\overline{\mathbb{F}}_p)| + 1$, onde $f(x, y) = F(x, y, 1) = y^2 - (x^3 + D)$. Uma vez que $3 \nmid p-1$, todo elemento de $\mathbb{F}_p$ é um cubo. Logo, para cada $y \in \mathbb{F}_p$, a equação $x^3 = y^2 - D$ tem uma única solução. Portanto, $Z_f(\mathbb{F}_p) \cong \mathbb{F}_p$ e assim $|X_F(\mathbb{F}_p)| = p+1$. Quando $3|p-1$ e $D \neq 0$ não é possível dar uma fórmula simples e explícita para $\#Z_f(\mathbb{F}_p)$.*

Observamos que obter fórmulas explícitas para $\#Z_F(\mathbb{F}_q)$ pode não ser uma tarefa fácil. Então seria interessante se pudéssemos obter cotas para este número. Uma cota trivial é

q^2, uma vez que $Z_F(\mathbb{F}_q) \subseteq \mathbb{F}_q \times \mathbb{F}_q$. Esta cota pode ser melhorada facilmente em casos particulares. Por exemplo, sejam $p \neq 2$ e $f(x,y) = y^2 - (x^3 + a_2x^2 + a_1x + a_0)$. Claramente $|Z_f(\mathbb{F}_q)| \leqslant 2q$, uma vez que para cada valor de x temos no máximo duas opções para y.

Uma curva afim $Z_f(\overline{k})$ não singular com $f(x,y) = y^2 - g(x)$ é chamada uma *curva elíptica* se $\deg(g) = 3$ e de *curva hiperelíptica* se $\deg(g) \geqslant 4$.

Teorema 6.0.4 *Sejam $X_F(\overline{\mathbb{F}}_q)$ uma curva elíptica e $N_1 = |X_F(\mathbb{F}_q)|$. Então*

$$|N_1 - (q+1)| \leqslant 2\sqrt{q}.$$

Demonstraremos este teorema em 8.5.

Para estudar o comportamento da sequência $\{N_n\}_{n\in\mathbb{N}}$ associada a uma curva não singular $X_F(\overline{\mathbb{F}}_q)$, consideraremos a série de potências

$$\mathbf{Z}(X_F/\mathbb{F}_q, T) := \exp\left(\sum_{n=1}^{\infty} N_n \frac{T^n}{n}\right).$$

Esta série de potências é chamada da *função-zeta* da curva $X_F(\overline{\mathbb{F}}_q)$. O teorema 6.0.4 pode ser apresentado como *hipótese de Riemann para cúbicas não singulares sobre um corpo finito*. A função-zeta de uma curva e a hipótese de Riemann são apresentadas em 6.3.

6.1 A Função$-\zeta$ de Riemann

Uma série da forma $\sum_{n=1}^{\infty} a_n n^{-s}$, onde $\{a_n\}_{n\in\mathbb{N}}$ é uma sequência em $\mathbb{C}$ e $s \in \mathbb{C}$ é chamada de uma *série de Dirichlet*.

Sejam $r \in R$ e $\mathcal{H}_r := \{s \in \mathbb{C} | \mathrm{Re}(s) > r\}$. Se $\sum_{n=1}^{\infty} a_n n^{-s_0}$ converge para algum $s_0 \in \mathbb{C}$, então $\sum_{n=1}^{\infty} a_n n^{-s}$ converge para todo $s \in \mathcal{H}_{\mathrm{Re}(s_0)}$. Além disso, a série de Dirichlet converge uniformemente em qualquer subespaço compacto de $\mathcal{H}_{\mathrm{Re}(s_0)}$ e a função $s \mapsto \sum_{n=1}^{\infty} a_n n^{-s}$ é holomorfa em $\mathcal{H}_{\mathrm{Re}(s_0)}$.

Definição 6.1.1 *A série de Dirichlet $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ é chamado a* função$-\zeta$ de Riemann.

Teorema 6.1.1 *A função$-\zeta$ é uma função holomorfa $\zeta : \mathcal{H}_1 \to \mathbb{C}$ e pode ser estendida a uma função meromorfa em $\mathbb{C}$ com polo simples em $s = 1$. Além disso, $\lim_{s\to 1} \zeta(s)(s-1) = 1$.*

A seguinte conjectura, sobre os zeros da função Zeta, é chamada de hipótese de Riemann.

Conjectura 6.1.1 (Hipótese de Riemann) *Seja* $s \in \mathbb{C}$ *tal que* $\zeta(s) = 0$. *Se* $0 \leqslant \mathrm{Re}(s) \leqslant 1$, *então* $\mathrm{Re}(s) = \frac{1}{2}$.

A faixa $\{s \in \mathbb{C} | 0 \leqslant \mathrm{Re}(s) \leqslant 1\}$ é chamada de *faixa crítica* e a reta $\{s \in \mathbb{C} | \mathrm{Re}(s) = 1/2\}$ é chamada de *reta crítica* . Com essa terminologia, a hipótese de Riemann afirma que os zeros de $\zeta(s)$ na faixa crítica estão todos na reta crítica.

A função gama é uma extensão da função factorial aos números complexos. Esta função é definida por:

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} dt.$$

Para todo $n \in \mathbb{N}$, $\Gamma(n+1) = n!$, e em geral, $\Gamma(s+1) = s\Gamma(s)$. Em particular $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

Teorema 6.1.2 *(Equação Funcional da função-ζ de Riemann) Seja* $\overline{\zeta}(s) := \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$. *Então* $\overline{(\zeta)}(s) = \overline{(\zeta)}(1-s)$.

Seja K um corpo de números e para $n \in \mathbb{N}$, j_n o número de ideais de $\mathcal{O}_K$ tal que $\|I\|_{\mathcal{O}_K} := |\mathcal{O}_K/I| = n$. Pelo lema 4.1.3 j_n é um número finito para todo $n \in \mathbb{N}$.

Definição 6.1.2 *Seja* K *um corpo de números. A série de Dirichlet* $\zeta(K, s) := \sum_{n=0}^{\infty} \frac{j_n}{n^s}$ *é chamada de* função-ζ de Dedekind *do corpo de números* K.

Claramente $\zeta(\mathbb{Q}, s)$ é igual a função-ζ de Riemann.

Seja K um corpo de números. Dado um monomorfismo σ de K, o valor absoluto $|\cdot|_\sigma$ definido por σ é: $|x|_\sigma := |x|_{\mathbb{R}}$ se σ é um monomorfismo real e $|x|_\sigma := |x|_{\mathbb{C}}$ se σ é um monomorfismo complexo. Sejam $|\cdot|_1, \ldots, |\cdot|_{r_1}$ os valores absolutos de K associados aos r_1 monomorfismos reais distintos de K e $|\cdot|_{r_1+1}, \ldots, |\cdot|_{r_1+r_2}$ os valores absolutos associados aos r_2 pares de monomorfismos complexos conjugados de K. Se $\alpha \in \mathcal{O}_K^*$, a fórmula do produto 4.3.2 mostra que $\prod_{i=1}^{r_1+r_2} |\alpha|_i^{n_i} = 1$, onde $n_i = 1$ ou 2 dependendo se $|\cdot|_i$ é real ou complexo. Esta igualdade mostra que a seguinte aplicação é um homomorfismo de grupos:

$$\begin{array}{rcl} \mathrm{Log} : \mathcal{O}_K^* & \longrightarrow & \left\{(y_1, \ldots, y_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \mid \sum_{i=1}^{r_1+r_2} y_i = 0\right\} \\ \alpha & \longmapsto & (\log|\alpha|_1, \ldots, \log|\alpha|_{r_1}, \log|\alpha|_{r_1+1}^2, \ldots, \log|\alpha|_{r_1+r_2}^2). \end{array}$$

Seja $\mu(K)$ o subgrupo finito de $\mathcal{O}_K^*$ formado pelas raízes da unidade.

Teorema 6.1.3 ***(das unidade de Dirichlet)*** *O grupo* $\mathcal{O}_K^*$ *é um grupo abeliano finitamente gerado, igual ao produto do grupo finito* $\mu(K)$ *pelo grupo abeliano livre* $\mathrm{Log}(\mathcal{O}_K^*)$ *de posto* $r_1 + r_2 - 1$.

A finitude de $\mathrm{Cl}(\mathcal{O}_K)$ e o fato de $\mathcal{O}_K^*$ ser um grupo abeliano finitamente gerado, são os dois principais resultados *de finitude* da teoria algébrica dos números.

Definição 6.1.3 *Sejam $K|\mathbb{Q}$ um corpo de números e $\{u_1, \ldots, u_{r_1+r_2-1}\} \subseteq \mathcal{O}_K^*$ tal que $\{\mathrm{Log}(u_1), \ldots, \mathrm{Log}(u_{r_1+r_2-1})\}$ é uma base para o $\mathbb{Z}-$módulo $\mathrm{Log}(\mathcal{O}_K^*)$. Em particular este conjunto é linearmente independentes em $\mathbb{R}^{r_1+r_2}$. Seja M a matriz cuja $i-$ésima linha é $\mathrm{Log}(u_i)$, para todo $i = 1, \ldots, r_1 + r_2 - 1$. O regulador R_K de K é o determinante de uma submatriz $(r_1 + r_2 - 1) \times (r_1 + r_2 - 1)$ menor de M.*

Teorema 6.1.4 *Seja K um corpo de números. A função-ζ de Dedekind $\zeta(K, s)$ define uma função holomorfa $\zeta(K, s) : \mathcal{H}_1 \to \mathbb{C}$. Esta função pode ser estendida para uma função meromorfa em todo $\mathbb{C}$ com um pólo simples em $s = 1$. Além disso,*

$$\lim_{s\to 1} \zeta(K, s)(s - 1) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{\mu_K \sqrt{d_K}},$$

onde h_K é o número de classe, d_K é um gerador positivo do discriminante, μ_K é o número de raízes da unidade contidas em K, r_1 e r_2 são como na definição 4.1.4 e o regulador *R_K é definido em 6.1.3.*

Como veremos na seção seguinte, a função $\zeta(K, s)$ pode ser obtida como um produto infinito onde cada fator é dado por um ideal primo de $\mathcal{O}_K$.

Teorema 6.1.5 *(Equação Funcional da Função-ζ de Dedekind) Seja K um corpo de números. Então,*

$$\zeta(K, s) = d_K^{\frac{1}{2}-s} \left(\frac{\pi^{s-\frac{1}{2}} \Gamma(\frac{1-s}{2})}{\Gamma(\frac{s}{2})} \right)^{r_1} \left(\frac{(2\pi)^{2s-1} \Gamma(1 - s)}{\Gamma(s)} \right)^{r_2} \zeta(K, 1 - s).$$

Como no caso da função-ζ de Riemann, podemos modificar a função-ζ de Dedekind para obter uma equação funcional. Seja

$$\overline{\zeta}(K, s) := \zeta(K, s) \left(\frac{\Gamma(\frac{s}{2})}{\pi^{\frac{s}{2}}} \right)^{r_1} \left(\frac{\Gamma(s)}{(2\pi)^s} \right)^{r_2} (\sqrt{d_K})^s.$$

Então $\overline{\zeta}(K, s) = \overline{\zeta}(K, 1 - s)$.

As conjecturas que afirmam que os zeros não triviais de uma dada série de Dirichlet estão em uma reta vertical são referidas na literatura como *Generalização da Hipótese de Riemann* ou *Hipótese de Riemann Estendida.* A função-ζ de Dedekind também tem uma conjectura deste tipo. A hipótese de Riemann clássica ou estendida tem importantes consequências na teoria dos números. Por exemplo, determinar se um número é primo ou composto.

6.2 Função-ζ e o Produto de Euler

Em análogo ao caso dos corpos de números, associaremos agora um função$-\zeta$ a um domínio de Dedekind com quocientes finitos.

Definição 6.2.1 *Sejam A um domínio de Dedekind com quocientes finitos e $\mathcal{M}(A)$ o monóide dos ideais não nulos de A. Se $I \in \mathcal{M}(A)$, $\|I\| := |A/I|$. A soma formal*

$$\zeta(A, s) := \sum_{I \in \mathcal{M}(A)} \frac{1}{\|I\|^s}$$

é chamada de função-ζ de A.

Seja $j_n := \#\{I \in \mathcal{M}(A) | \|I\| = n\}$. Se $j_n < \infty$ para todo $n \in \mathbb{N}$, então reorganizando os termos da soma formal acima, podemos escrever $\zeta(A, s) = \frac{j_n}{n^s}$.

Observe que $\zeta(\mathbb{Z}, s)$ é a função-ζ de Riemann e similarmente, se K é um corpo de números e $\mathcal{O}_K$ o anel dos inteiros, então $\zeta(\mathcal{O}_K, s)$ é a função-ζ de Dedekind associada a K.

Seja A um domínio de Dedekind com quocientes finitos. Todo ideal $I \in \mathcal{M}(A)$ se fatora em produto de ideais maximais de A: $I = P_1^{a_1} \cdots P_r^{a_r}$. Podemos usar esta propriedade de fatoração única de ideais para reescrever a soma infinita $\zeta(A, s)$ como um produto infinito. Observe que

$$\frac{1}{1 - \frac{1}{\|P\|^s}} = 1 + \frac{1}{\|P\|^s} + \frac{1}{\|P\|^{2s}} + \cdots = \sum_{n=0}^{\infty} \frac{1}{\|P\|^{ns}},$$

assim

$$\sum_{I \in \mathcal{M}(A)} \frac{1}{\|I\|^s} = \prod_{P \in \mathrm{Max}(A)} \left(1 + 1 + \frac{1}{\|P\|^s} + \frac{1}{\|P\|^{2s}} + \cdots\right) = \prod_{P \in \mathrm{Max}(A)} \left(1 - \frac{1}{\|I\|^s}\right)^{-1}.$$

O lado direito da igualdade acima é às vezes chamado de fatoração de $\zeta(A, s)$ no *produto de Euler*.

Observação 6.2.1 *Seja $A = \mathbb{Z}$. A discussão acima nos permite escrever a identidade:*

$$\zeta(\mathbb{Z}, s) = \sum_{n=0}^{\infty} \frac{1}{n^s} = \prod_{p:primo} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Agora definiremos o principal objeto de estudo deste capítulo. Sejam $f \in \mathbb{F}_q[x, y]$ absolutamente irredutível e $Z_f(\overline{\mathbb{F}}_q)$ não singular. Pelo corolário 5.4.1, $C_f := \mathbb{F}_q[x, y]/\langle f \rangle$

é um domínio de Dedekind com quocientes finitos. Sejam

$$\zeta(Z_f/\mathbb{F}_q, s) := \zeta(C_f, s) = \sum_{I \in \mathcal{M}(C_f)} \frac{1}{\|I\|^s} = \prod_{M \in \mathrm{Max}(C_f)} \left(1 - \frac{1}{\|M\|^s}\right)^{-1},$$

e $b_d := \#\{M \in \mathrm{Max}(C_f) \mid [C_f/M : \mathbb{F}_q] = d\}$. Que $b_d \in \mathbb{Z}$ é provado em 5.5.2. Se $[C_f/M : \mathbb{F}_q] = d$, então $\|M\| = |C_f/M| = q^d$. Portanto

$$\zeta(Z_f/\mathbb{F}_q, s) = \prod_{d \in \mathbb{N}} \left(1 - \frac{1}{q^{sd}}\right)^{-bd}.$$

Sejam $T := q^{-s}$ e

$$\mathbf{Z}(Z_f/\mathbb{F}_q, T) := \prod_{d \in \mathbb{N}} \left(1 - T^d\right)^{-bd},$$

de modo que $\mathbf{Z}(Z_f/\mathbb{F}_q, T) = \zeta(Z_f/\mathbb{F}_q, s)$. Quando não causar confusão, denotaremos a função $\mathbf{Z}(Z_f/\mathbb{F}_q, T)$ simplesmente por $\mathbf{Z}(T)$.

6.3 A Função-ζ de uma Curva Não Singular

Sejam $f \in \mathbb{F}_q[x, y]$ absolutamente irredutível e $Z_f(\overline{\mathbb{F}}_q)$ não singular. Como visto na seção anterior, a função-ζ do anel $C_f := \mathbb{F}_q[x, y]/\langle f \rangle$ é dada por

$$\zeta(Z_f/\mathbb{F}_q, s) = \prod_{d \in \mathbb{N}} \left(1 - \frac{1}{q^{sd}}\right)^{-b_d}.$$

Seja $T := q^{-s}$ e considere a expressão

$$\mathbf{Z}(Z_f/\mathbb{F}_q, T) = \mathbf{Z}(T) := \prod_{d \in \mathbb{N}} \left(1 - T^d\right)^{-b_d}.$$

Então $\log(\mathbf{Z}(T)) = -\sum_{d \in \mathbb{N}} b_d \cdot \log(1 - T^d)$. Usando $-\log(1 - x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$, concluímos

$$\log(\mathbf{Z}(T)) = \sum_{d \in \mathbb{N}} b_d \left(\sum_{i=1}^{\infty} \frac{T^{d_i}}{i}\right), \tag{6.1}$$

ou,

$$\log(\mathbf{Z}(T)) = \sum_{n=1}^{\infty} \left(\sum_{d|n} d b_d\right) \frac{T^n}{n}. \tag{6.2}$$

Pela proposição 5.5.2, $\sum_{d|n} db_d = N_n$, onde $N_n = |Z_f(\mathbb{F}_{q^n})|$. Portanto,

$$\mathbf{Z}(Z_f/\mathbb{F}_q, T) = \exp\left(\sum_{i=1}^{\infty} N_n \frac{T^n}{n}\right).$$

Definição 6.3.1 *A série de potências $\boldsymbol{Z}(Z_f/\mathbb{F}_q, T) \in \mathbb{Q}[[T]]$ é chamada de função-zeta de uma curva afim $Z_f(\overline{\mathbb{F}}_q)$ sobre $\mathbb{F}_q$.*

Exemplo 6.3.1 *Uma vez que $|\mathbb{A}^1(\mathbb{F}_{q^n})| = q^n$,*

$$\boldsymbol{Z}(\mathbb{A}^1/\mathbb{F}_q, T) = \exp\left(\sum_{i=1}^{\infty} q^n \frac{T^n}{n}\right) = \exp(-\log(1-qT)) = (1-qT)^{-1}.$$

Exemplo 6.3.2 *Sejam $p \neq 2$, $f(x,y) = x^2 + y^2 - 1 \in \mathbb{F}_q[x,y]$ e $F(X,Y,Z) = X^2 + Y^2 - Z^2$. A curva projetiva $X_F(\overline{\mathbb{F}}_q)$ é não singular e $X_F(\mathbb{F}_q) \neq \emptyset$. A proposição 6.0.3 garante que $|X_F(\mathbb{F}_{q^n})| = q^n + 1$. Seja $i \in \overline{\mathbb{F}}_q$ a solução em $\overline{\mathbb{F}}_q$ da equação $z^2 - 1 = 0$. Então*

$$X_F(\overline{\mathbb{F}}_q) = Z_f(\overline{\mathbb{F}}_q) \sqcup \{(1:i:0), (1:-i:0)\}.$$

Se $i \in \mathbb{F}_q$, então $N_n := |Z_f(\mathbb{F}_{q^n})| = q^n - 1$. Se $i \notin \mathbb{F}_q$, então $i \in \mathbb{F}_{q^2}$ e assim

$$N_n = \begin{cases} q^n + 1, & 2 \nmid n; \\ q^n - 1, & 2|n. \end{cases}$$

Então se $i \in \mathbb{F}_q$,

$$\boldsymbol{Z}(Z_f/\mathbb{F}_q, T) = \exp\left(\sum_{i=1}^{\infty}(q^n-1)\frac{T^n}{n}\right) = \exp\left(\sum_{i=1}^{\infty}\frac{(qT)^n}{n} - \sum_{n-1}^{\infty}\frac{T^n}{n}\right) = (1-T)(1-qT)^{-1},$$

e se $i \notin \mathbb{F}_q$,

$$\begin{aligned} \boldsymbol{Z}(Z_f/\mathbb{F}_q, T) &= \exp\left(\textstyle\sum_{2\nmid n}\frac{(q^n+1)T^n}{n} + \sum_{2|n}\frac{(q^n-1)T^n}{n}\right) \\ &= \exp\left(\textstyle\sum_{n=1}^{\infty}\frac{(qT)^n}{n} + (T - \frac{T^2}{2} + \frac{T^3}{3} + \cdots)\right) \\ &= (1+T)(1-qT)^{-1}. \end{aligned}$$

Definição 6.3.2 *Sejam $F \in \mathbb{F}_q[X,Y,Z]$ homogêneo e $N_n := |X_F(\mathbb{F}_{q^n})|$. A função-zeta de $X_F(\overline{\mathbb{F}}_q)$ sobre $\mathbb{F}_q$ é a série de potências*

$$\boldsymbol{Z}(X_F/\mathbb{F}_q, T) := \exp\left(\sum_{n=1}^{\infty}\frac{N_n T^n}{n}\right).$$

Exemplo 6.3.3 *Sejam $L, F \in \mathbb{F}_q[X,Y,Z]$ homogêneos, L linear e F de grau dois tais que $X_F(\overline{\mathbb{F}}_q)$ é uma curva não singular. Pela classificação de cônicas, $F = X^2 - YZ$ e assim para todo $n \in \mathbb{N}$, $X_L(\overline{\mathbb{F}}_{q^n}) \cong X_F(\overline{\mathbb{F}}_{q^n}) \cong \mathbb{P}^1(\overline{\mathbb{F}}_{q^n})$. Logo,*

$$\boldsymbol{Z}(\mathbb{P}^1/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} \frac{(q^n+1)T^n}{n}\right) = (1-qT)^{-1}(1-T)^{-1}.$$

Seja $X_F(\overline{\mathbb{F}}_q)$ uma curva não singular. Lembre-se que grau do ponto $P \in X_F(\overline{\mathbb{F}}_q)$ é igual ao comprimento da órbita de P sobre $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$, veja 5.8.2. Se v é um órbita de $X_F(\overline{\mathbb{F}}_q)$ sobre a ação de $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$, definimos o grau da órbita v, $\deg(v)$, como sendo seu número de pontos. Seja b_d o número das órbitas de grau d da ação de $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ em $X_F(\overline{\mathbb{F}}_q)$. O lema 5.5.2 afirma que $N_n = \sum_{d|n} db_d$. Então

$$\begin{aligned} \mathbf{Z}(X_F/\mathbb{F}_q, T) &= \exp\left(\textstyle\sum_{n=1}^{\infty} N_n \frac{T^n}{n}\right) = \textstyle\prod_{d|n}(1-T^d)^{-b_d} \\ &= \prod_{v \in X_F(\overline{\mathbb{F}}_q)/\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)} (1-T^{\deg(v)})^{-1}. \end{aligned}$$

A relação entre a função-zeta de uma curva projetiva e a função-zeta da curva afim associada é descrita abaixo:

Lema 6.3.1 *Sejam $F \in \mathbb{F}_q[x_0,x_1,x_2]$ absolutamente irredutível, homogêneo e $f(x,y) = F(x,y,1)$. Sejam $v_1,\ldots,v_r$ as órbitas dos pontos no infinito de $Z_f(\overline{\mathbb{F}}_q)$ sobre a ação de* $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$. *Então*

$$\boldsymbol{Z}(X_F/\mathbb{F}_q, T) = \boldsymbol{Z}(Z_f/\mathbb{F}_q, T) \cdot \prod_{i=1}^{r} (1-T^{\deg(v_i)})^{-1}.$$

Seja $F \in \mathbb{F}_q[x_0,x_1,x_2]$ homogêneo definindo uma curva projetiva plana $X_F(\overline{\mathbb{F}}_q)$ não singular. A função-zeta desta curva foi definida como

$$\mathbf{Z}(X_F/\mathbb{F}_q, T) := \exp\left(\sum_{n=1}^{\infty} N_n \frac{T^n}{n}\right),$$

onde $N_n = |X_F(\mathbb{F}_{q^n})|$. Dado um inteiro $e > 0$, considere F como um polinômio em $\mathbb{F}_{q^e}[x_0,x_1,x_2]$. A função-zeta da curva $X_F(\overline{\mathbb{F}}_q)$, quando F é pensando como um polinômio com coeficientes em $\mathbb{F}_{q^e}$ é

$$\mathbf{Z}(X_F/\mathbb{F}_{q^e}, T) := \exp\left(\sum_{n=1}^{\infty} N_n' \frac{T^n}{n}\right),$$

onde $N_n^{'} := |X_F(\mathbb{F}_{q^{en}})| = N_{en}$. A relação entre as funções-zeta $\mathbf{Z}(X_F/\mathbb{F}_q, T)$ e $\mathbf{Z}(X_F/\mathbb{F}_{q^e}, T)$ é explicitada no resultado abaixo.

Lema 6.3.2 *Seja ξ_e um raiz $e-$ésima primitiva da unidade. Então*

$$\boldsymbol{Z}(X_F/\mathbb{F}_{q^e}, T^e) = \prod_{i=1}^{e} \boldsymbol{Z}(X_F/\mathbb{F}_q, \xi_e^i T).$$

Demonstração: *Observe que $\sum_{i=1} e(\xi_e^i)^m = e$ se $e|m$ e é zero, caso contrário. Portanto,*

$$\begin{aligned} \log\left(\prod_{i=1}^{e} \boldsymbol{Z}(X_F/\mathbb{F}_q, \xi_e^i T)\right) &= \sum_{i=1}^{e} \left(\sum_{m=1}^{\infty} N_m (\xi_e^i)^m T^m/m\right) \\ &= \sum_{m=1}^{\infty} N_m \left(\sum_{i=1}^{e} (\xi_e^i)^m\right) \frac{T^m}{m} \\ &= \sum_{n=1}^{\infty} \frac{N_{en} T^{en}}{n} = \sum_{n=1}^{\infty} \frac{N_n^{'} (T^e)^n}{n} \\ &= \log(\boldsymbol{Z}(X_F/\mathbb{F}_{q^e}, T^e)). \end{aligned}$$

■

Observação 6.3.1 *Segue da definição, que a função-zeta de uma curva projetiva pertence a $\mathbb{Q}[[T]]$. No exemplo 6.3.3, expressamos $\boldsymbol{Z}(\mathbb{P}^1/\mathbb{F}_q, T)$ como uma função racional com coeficientes em $\mathbb{Z}$. Nosso primeiro objetivo no estudo das funções-zeta de curvas, é mostrar que se $X_F(\overline{\mathbb{F}}_q)$ é não singular de grau d, então*

$$\boldsymbol{Z}(X_F/\mathbb{F}_q, T) = \frac{f(T)}{(1-qT)(1-T)}, \tag{6.3}$$

onde $f(T) \in \mathbb{Z}[T], \deg(f) = (d-1)(d-2)$. O inteiro

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

é chamado do gênero da curva $X_F(\overline{\mathbb{F}}_q)$. Segue da racionalidade da função-zeta (que provaremos em 6.4) que a sequência infinita $\{N_n\}_{n\in\mathbb{N}}$ é totalmente determinada por $2g$ inteiros $c_1, c_2, \ldots, c_{2g}$ tais que $f(T) := 1 + c_1 T + \cdots + c_{2g} T^{2g}$. Para escrever a sequência $\{N_n\}_{n\in\mathbb{N}}$ em termo dos $2g$ inteiros, escreva $f(T) = \prod_{i=1}^{2g}(1-\omega_i T) \in \overline{\mathbb{Q}}[T]$. Como $h(s) := s^{2g} f(\frac{1}{s}) \in \mathbb{Z}[s]$ é mônico de grau $2g$ e $h(\omega_i) = 0$, os elementos $\omega_1, \ldots, \omega_{2g}$ são inteiros algébricos. Então, usando 6.3

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

Assim,

$$N_n = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n. \tag{6.4}$$

Observação 6.3.2 *Como foi mencionado anteriormente, um de nossos objetivos principais é obter explicitamente estimativas para os inteiros N_n. Estas estimativas podem ser deduzidas a partir da hipótese de Riemann para curvas . Esta hipótese para as funções−ζ de Riemann $\zeta(s)$ afirma que, se $0 \leqslant \mathrm{Re}(s) \leqslant 1$ e $\zeta(s) = 0$, então $\mathrm{Re}(s) = 1/2$. Relembre que a função-zeta é dada em função de s, onde $T = q^{-s}$. Seja $s \in \mathbb{C}$, e considere a afirmação:*

$$\text{Se } 0 \leqslant \mathrm{Re}(s) \leqslant 1 \text{ e } \boldsymbol{Z}(q^{-s}) = 0, \text{ então } \mathrm{Re}(s) = 1/2. \tag{6.5}$$

Como $\boldsymbol{Z}(T) \in \mathbb{Q}[T]$, os números algébricos $1/\omega_1, \ldots, 1/\omega_{2g}$ são os únicos zeros de $\boldsymbol{Z}(T)$. Se $1/\omega_i = q^s$, então $|\omega_i|_{\mathbb{C}} = q^{\mathrm{Re}(s)}$. Note que se $\log(q) > 2\pi$, então todo $\omega \in \mathbb{C}^*$ pode ser escrito como $\omega = q^{-s}$ para algum $s \in \mathbb{C}$ com $0 \leqslant \mathrm{Re}(s) \leqslant 1$. A afirmação 6.5, se verdadeira, implicaria que $|\omega_i|_{\mathbb{C}} = q^{\frac{1}{2}}$. Assim, a hipótese se Riemann para curvas sobre corpos finitos, provada por Weil em 1940, afirma que

$$|\omega_i|_{\mathbb{C}} = \sqrt{q}, \forall i = 1, \ldots, 2g. \tag{6.6}$$

Portanto, segue de 6.4 e da hipótese de Riemann para curvas 6.6 que

$$|N_n - (q^n + 1)| \leqslant 2g\sqrt{q^n}. \tag{6.7}$$

Veremos em 8.5 que a estimativa 6.7 é essencialmente equivalente a 6.6.

Exemplo 6.3.4 *Seja $F(x_0, x_1, x_2) = x_0^4 + x_1^4 + x_2^4 \in \mathbb{F}_3[x_0, x_1, x_2]$. A curva $X_F(\overline{\mathbb{F}}_3)$ é não singular e $g = 3$. É fácil verificar que $X_F(\mathbb{F}_3) = \{(1:1:1), (2:1:1), (1:1:2), (1:2:1)\}$. O grupo $\mathbb{F}_9^*$ é cíclico de ordem 8 e, portanto, contém exatamente 4 elementos cujas potências quartas são -1. Então*

$$X_F(\mathbb{F}_9) = \{(a:b:1) | a, b \in \mathbb{F}_9, a^4 = b^4 = 1\} \cup \{(a:1:0), (1:a:0), (0:1:a) | a \in \mathbb{F}_9, a^4 = -1\}.$$

Em particular, $N_2 = 28$. A estimativa para N_2, dada pela hipótese e Riemann é alcançada neste caso: $N_2 = p^2 + 1 + 2g\sqrt{p^2} = 3^2 + 1 + 18 = 28$.

Os resultados aqui apresentados para funções-zeta de uma curva projetiva plana não singular também valem para as funções-zeta de uma curva completa não singular $X/\mathbb{F}_q$ cuja função-zeta é definida a seguir.

Definição 6.3.3 *A função-zeta de uma curva completa não singular $X/\mathbb{F}_q$ é a série de potências*

$$\boldsymbol{Z}(X/\mathbb{F}_q, T) := \prod_{P \in X} (1 - T^{\deg(P)})^{-1}$$

Sejam $b_d := \#\{P \in X \mid |\mathcal{O}_P/\mathcal{M}_P| = q^d\}$ e $N_n = |X(\mathbb{F}_{q^n})|$. A proposição 5.8.2 mostra que $N_n = \sum_{d|n} db_d$. Portanto, como em 6.1 e 6.2, concluímos que

$$\mathbf{Z}(X/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n T^n}{n}\right).$$

Sejam $e, p \in \mathbb{Z}$, p primo e $(e,p) = 1$. Dada a curva completa não singular $X/\mathbb{F}_q$, associamos por extensão de escalares a curva completa não singular $X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}$ (associada a $\mathbb{F}_{q^e}(X)|\mathbb{F}_{q^e}$). As funções-zeta destas curvas são relacionadas do seguinte modo:

Lema 6.3.3 $\boldsymbol{Z}(X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}, T^e) = \prod_{i=1}^{e} \boldsymbol{Z}(X/\mathbb{F}_q, \xi_e^i T)$.
Demonstração: *A prova deste lema é análoga ao do lema 6.3.2. Seja* $N_n^{'} := |X_{\mathbb{F}_{q^e}}(\mathbb{F}_{q^e})|$. *O fato que* $N_n^{'} = N_{ne}$ *segue do lema 5.8.4.* ■

6.4 A Racionalidade da Função-Zeta

Definição 6.4.1 *Dada X/k uma curva completa não singular, seja* $\mathrm{Eff}^d(X/k)$ *o conjunto dos dos divisores efetivos de* $\mathrm{Div}(X/k)$ *de grau d.*

Podemos escrever

$$\begin{aligned} \mathbf{Z}(X/\mathbb{F}_q, T) &:= \prod_{P \in X} (1 - T^{\deg(P)})^{-1} \\ &= \sum_{D \in \mathrm{Eff}(X/\mathbb{F}_q)} T^{\deg(D)} \\ &= \sum_{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q), \deg(\mathcal{L}) \geqslant 0} \left(\sum_{D \in \mathrm{Eff}(X/\mathbb{F}_q), \mathrm{cl}(D) = \mathcal{L}} T^{\deg(D)} \right). \end{aligned} \tag{6.8}$$

Sejam $\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q)$ e

$$E_{\mathcal{L}} := \{D \in \mathrm{Eff}(X/\mathbb{F}_q) \mid \mathrm{cl}(D) = \mathcal{L}\}.$$

O teorema de Riemann-Roch (veja 7.2.3), mostra a existência de um inteiro $g \geqslant 0$, chamado *gênero* de $X/\mathbb{F}_q$, tal que, se $\deg(\mathcal{L}) \geqslant 2g - 1$, então

$$|E_{\mathcal{L}}| = \frac{q^{\deg(\mathcal{L})+1-g} - 1}{q - 1}. \tag{6.9}$$

A racionalidade da função-zeta $\mathbf{Z}(X/\mathbb{F}_q, T)$ segue imediatamente da formula 6.9.

Teorema 6.4.1 *(**Racionalidade da função-zeta**) Seja $X/\mathbb{F}_q$ uma curva completa não singular de gênero g. Então*

$$\boldsymbol{Z}(X/\mathbb{F}_q, T) = \frac{f(T)}{(1-T)(1-qT)},$$

onde $f \in \mathbb{Z}[T]$ e $\deg f \leq 2g$. A função-zeta tem um polo simples em $T = 1$ e

$$\lim_{T\to 1}(T-1)\boldsymbol{Z}(X/\mathbb{F}_q, T) = \frac{h}{q-1},$$

onde $h := |\mathrm{Pic}^0(X/\mathbb{F}_q)|$ é o número de classe.
Demonstração: *No caso em que $g = 0$, usando 6.9, $|E_{\mathcal{L}}| = \frac{q^{\deg(\mathcal{L})+1}-1}{q-1}$ se $\deg(\mathcal{L}) \geqslant 0$, concluímos*

$$\boldsymbol{Z}(X/\mathbb{F}_q, T) = \frac{1}{(1-T)(1-qT)}.$$

Suponha $g \geqslant 1$. Segue de 6.8 que

$$\boldsymbol{Z}(X/\mathbb{F}_q, T) = \sum_{\mathcal{L}\in \mathrm{Pic}(X/\mathbb{F}_q), 0\leqslant \deg(\mathcal{L})\leqslant 2g-2} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})} + \sum_{\mathcal{L}\in \mathrm{Pic}(X/\mathbb{F}_q), \deg(\mathcal{L})\geqslant 2g-1} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})}.$$

O teorema 5.9.2 afirma que a aplicação $\deg : \mathrm{Pic}(X/\mathbb{F}_q) \to \mathbb{Z}$ tem núcleo $\mathrm{Pic}^0(X/\mathbb{F}_q)$ finito de ordem h. Portanto, para todo $d \in \mathbb{N}$, o conjunto

$$\mathrm{Pic}^d(X/\mathbb{F}_q) = \{\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q) \mid \deg(\mathcal{L}) = d\}$$

é vazio ou tem ordem h. Seja $e \in \mathbb{N}$ o único inteiro tal que $\deg(\mathrm{Pic}(X/\mathbb{F}_q)) = e\mathbb{Z}$. Então

$$\sum_{\mathcal{L}\in \mathrm{Pic}(X/\mathbb{F}_q), \deg(\mathcal{L})\leqslant 2g-2} |E_{\mathcal{L}}| x^{\frac{\deg(\mathcal{L})}{e}} \in \mathbb{Z}[x]$$

e seu grau é no máximo $2g-2$. Por 6.9,

$$\sum_{\mathcal{L}\in \mathrm{Pic}(X/\mathbb{F}_q), \deg(\mathcal{L})\geqslant 2g-1} |E_{\mathcal{L}}| T^{\deg(\mathcal{L})} = h \cdot \sum_{d, de\geqslant 2g-1} \frac{q^{de+1-g}-1}{q-1} T^{de}.$$

Seja d_0 o menor inteiro tal que $d_0 e \geqslant 2g-1$. Então

$$\frac{h}{q-1}\left(\sum_{ed\geqslant 2g-1} (q^{ed+1-g}-1)T^{ed}\right) = h \cdot \frac{u(T^e)}{(1-q^eT^e)(1^-T^e)}, \tag{6.10}$$

onde $u \in \mathbb{Z}[x]$ de grau no máximo $2g$. Assim

$$\boldsymbol{Z}(X/\mathbb{F}_q, T) = \frac{f(T^e)}{(1-q^eT^e)(1-T^e)}, \tag{6.11}$$

onde $f \in \mathbb{Z}[x]$ tem grau no máximo $2g$. Além disso, segue de 6.10 que

$$\lim_{T\to 1}(T-1)\boldsymbol{Z}(X/\mathbb{F}_q, T) = \frac{h}{(q-1)^e}.$$

Portanto, este teorema segue imediatamente da próxima proposição, cuja demostração pode ser vista em [6], página 286. ■

Proposição 6.4.1 *Seja $X/\mathbb{F}_q$ uma curva completa não singular. Então a aplicação*

$$\deg : \mathrm{Pic}(X/\mathbb{F}_q) \longrightarrow \mathbb{Z}$$

é sobrejetiva, isto é, na demonstração do teorema anterior $e = 1$.

Uma vez que $\mathbf{Z}(X/\mathbb{F}_q, 0) = 1$, segue $f(0) = 1$. Podemos portanto fatorar $f(T)$ em $\overline{\mathbb{Q}}[T]$ como

$$f(T) = \prod_{i=1}^{2g}(1-\omega_i T).$$

Notamos em 6.3.1 que os elementos $\omega_1, \ldots, \omega_{2g}$ são inteiros algébricos. Veremos em 6.5.1 que $\deg(f) = 2g$, ou seja, $\omega_i \neq 0, i = 1, \ldots, 2g$.

Corolário 6.4.1 $|\mathrm{Pic}^0(X/\mathbb{F}_q)| = h = f(1) = \prod_{i=1}^{2g}(1-\omega_i)$.

Observação 6.4.1 *A hipótese de Riemann para curvas sobre corpos finitos, cuja veracidade garante que $|\omega_i| = \sqrt{q}$, para todo $i = 1, \ldots, 2g$, fornece cotas inferior e superior para h. De fato, segue da hipótese de Riemann que*

$$(1-\sqrt{q})^{2g} \leqslant h = |\prod_{i=1}^{2g}(1-\omega_i)| \leqslant (1+\sqrt{q})^{2g}.$$

Em particular, $h > 1$ se $q > 4$.

Se $F \in \mathbb{F}_q[x_0, x_1, x_2]$ é homogêneo de grau dois, vimos em 6.0.2 que $X_F(\mathbb{F}_q) \neq \emptyset$. Já na observação 6.0.4, vimos um exemplo onde $\deg(F) > 2$ e $X_F(\mathbb{F}_q) = \emptyset$. O próximo corolário mostra a existência de algumas curvas tais que $X_F(\mathbb{F}_{q^n}) \neq \emptyset$.

Corolário 6.4.2 *Sejam $F \in \mathbb{F}_q[x_0, x_1, x_2]$ e $X_F(\overline{\mathbb{F}}_q)$ uma curva não singular. Então existe $\{P_1, \ldots, P_r\} \subseteq X_F(\overline{\mathbb{F}}_q)$ tal que $[\mathbb{F}_q(P_i) : \mathbb{F}_q], i = 1, \ldots, r$, são relativamente primos.*
Demonstração: *Seja $X/\mathbb{F}_q$ a curva completa não singular associada ao corpo de funções $\mathbb{F}_q(X_F)|\mathbb{F}_q$. A proposição 6.4.1 afirma que a aplicação $\deg : \mathrm{Pic}(X/\mathbb{F}_q) \to \mathbb{Z}$ é sobrejetiva. Portanto, existe $D = \sum_{i=1}^r a_i Q_i \in \mathrm{Div}(X/\mathbb{F}_q)$ tal que $\deg(D) = \sum_{i=1}^r a_i \deg(Q_i) = 1$. Identifique X com $X_F(\overline{\mathbb{F}}_q)/\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$. Sejam $P_1, \ldots, P_r \in X_F(\overline{\mathbb{F}}_q)$ tais que a órbita de P_i na ação de $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ corresponde a $Q_i \in X$. Então $[\mathbb{F}_q(P_i) : \mathbb{F}_q] = \deg(Q_i)$. De $\sum_{i=1}^r a_i \deg(Q_i) = 1$, concluímos que $[\mathbb{F}_q(P_i) : \mathbb{F}_q] = \deg(Q_i)$ são relativamente primos* ■

6.5 A Equação Funcional

Na seção 6.1, estabelecemos uma relação entre $\zeta(s)$ e $\zeta(s-1)$ para a função-ζ de Riemann. Nesta seção vamos estabelecer uma relação semelhante para a função-zeta $\mathbf{Z}(T)$ de uma curva não singular. Podemos considerar $\mathbf{Z}(T)$ como uma função de s, basta observar que $T = q^{-s}$. Considere a mudança de variável $q^{-1} \mapsto q^{-(1-s)}$, ou, equivalentemente $T \mapsto \frac{1}{qT}$. Pela observação 6.3.1 e pelo teorema 6.4.1,

$$\mathbf{Z}(T) = \frac{\prod_{i=1}^c (1 - \omega_i T)}{(1 - qT)(1 - T)},$$

onde $\omega_i \neq 0$ para todo $i = 1, \ldots, c$. Assim

$$\begin{aligned} \mathbf{Z}(\tfrac{1}{qT}) &= qT^2 \cdot \tfrac{1}{(1-qT)(1-T)} \cdot \textstyle\prod_{i=1}^c (1 - \frac{\omega_i}{qT}) \\ &= (-1)^c (\textstyle\prod_{i=1}^c \omega_i) \cdot (q^{1-c} T^{2-c}) \cdot \frac{\prod_{i=1}^c (1 - qT/\omega_i)}{(1-qT)(1-T)}. \end{aligned}$$

A equação funcional satisfeita pela função-zeta de uma curva não singular é obtida a partir as duas condições equivalentes abaixo.

Teorema 6.5.1 *(**Equação funcional da função-zeta**) Sejam $X/\mathbb{F}_q$ uma curva completa não singular de gênero g e $\boldsymbol{Z}(T) := \boldsymbol{Z}(X/\mathbb{F}_q, T) = \frac{f(T)}{(1-qT)(1-T)}$. Então $\deg(f) = 2g$ e são equivalentes:*

1. *$\boldsymbol{Z}(1/qT) = (qT^2)^{1-g} \boldsymbol{Z}(T)$.*
2. *$\prod_{i=1}^{2g} \omega_i = q^g$ e a aplicação $\omega_i \mapsto \frac{q}{\omega_i}$ do conjunto $\{\omega_1, \ldots, \omega_{2g}\}$ nele mesmo, está bem definida e é uma bijeção.*

A prova da equação funcional usa fortemente o teorema de Riemann-Roch 7.2.3 que veremos mais adiante, por isso daremos aqui apenas uma ideia da demonstração. O teorema de Riemann-Roch mostra a existência de um inteiro g e para cada $\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q)$, um inteiro não negativo $h^0(\mathcal{L})$ tais que

(i) $|E_{\mathcal{L}}| = \frac{q^{h^0(\mathcal{L})}-1}{q-1}$,

(ii) se $\deg(\mathcal{L}) \geqslant 2g-1$, *então* $h^0(\mathcal{L}) = \deg(L) + 1 - g$.

Além disso, o teorema de Riemann-Roch garante também a existência de um elemento $\mathcal{K} \in \mathrm{Pic}^{2g-2}(X/\mathbb{F}_q)$, *chamado da* classe canônica, *tal que para todo* $\mathcal{L} \in \mathrm{Pic}(X/\mathbb{F}_q)$,

(iii) $h^0(\mathcal{L}) = \deg(\mathcal{L}) + 1 - g + h^0(\mathcal{K} - \mathcal{L})$.

Então de $(i), (ii)$ *e principalmente* (iii), *segue a demonstração de 1 e 2. De 1, segue que* $\deg(f) = 2g$.

Observação 6.5.1 *O item 2 do teorema 6.5.1, nos permite, com uma mudança de indices de necessário, escrever o conjunto* $\{\omega_1, \ldots, \omega_{2g}\}$ *como* $\{\omega_1, \ldots, \omega_g, q/\omega_1, \ldots, q/\omega_g\}$.

Corolário 6.5.1 ***(Função-zeta de uma cúbica)*** *Sejam* $F \in \mathbb{F}_q[x_0, x_1, x_2]$ *homogêneo de grau* 3 *e* $X_F(\overline{\mathbb{F}}_q)$ *não singular. Então*

$$\boldsymbol{Z}(X/\mathbb{F}_q, T) = \frac{1 + (N_1 - q - 1)T + qT^2}{(1-T)(1-qT)}.$$

A função-zeta satisfaz a equação funcional $\boldsymbol{Z}(T) = \boldsymbol{Z}(1/qT)$. *A hipótese de Riemann vale para cúbicas não singulares se, e somente se, os zeros do polinômio* $1+(N_1-q-1)T+qT^2$ *são conjugados complexos ou se* $\sqrt{q} \in \mathbb{Z}$ *e* $\omega_1 = \omega_2 = \pm\sqrt{q}$.

Demonstração: *Provaremos em 7.3 que o gênero* g *de uma curva plana projetiva não singular de grau* d *é* $\frac{(d-1)(d-2)}{2}$, *disto segue que o gênero de uma cúbica não singular é* 1. *Do teorema 6.5.1, podemos escrever* $f(T) = (1-\omega_1 T)(1-\omega_2 T)$. *Por 6.4,* $N_1 = q+1-(\omega_1+\omega_2)$, *de modo que* $f(T) = 1 + (N_1 - q - 1)T + \omega_1\omega_2 T^2$. *Pela equação funcional 6.5.1,* $\omega_1\omega_2 = q$ *e portanto*

$$\boldsymbol{Z}(X/\mathbb{F}_q, T) = \frac{1 + (N_1 - q - 1)T + qT^2}{(1-T)(1-qT)}.$$

Uma vez que $f \in \mathbb{Z}[T]$, *se* $\omega_i \in \mathbb{C} \setminus \mathbb{R}$, *então* $\omega_2 = \overline{\omega_1} = q\omega_1$, *logo* $|\omega_1| = |\omega_2| = \sqrt{q}$. *Assim, a hipótese de Riemann vale neste caso. Se a hipótese de Riemann é verdadeira e* $\omega_1 \in \mathbb{R}$, *então* $|\omega_i| = \sqrt{q}$ *e* $\omega_i = \pm\sqrt{q}, i = 1, 2$. *Em particular,* $f(T) = (1 \pm \sqrt{q}T)^2$ *neste caso. Como* $f \in \mathbb{Z}[T]$, *logo* $\sqrt{q} \in \mathbb{Z}$. ■

Corolário 6.5.2 *Sejam* $F \in \mathbb{F}_q[x_0, x_1, x_2]$ *homogêneo de grau* 3 *e* $X_F(\overline{\mathbb{F}}_q)$ *não singular. Então* $X_F(\mathbb{F}_q) \neq \emptyset$.

Demonstração: *Basta observar que* $|X_F(\mathbb{F}_q)| = N_1 = f(1) = |\mathrm{Pic}^0(X_F/\mathbb{F}_q)| \neq 0$. ■

Observação 6.5.2 *Nas mesmas condições do corolário anterior, se $X_F(\overline{\mathbb{F}}_q)$ é uma curva singular, pode-se mostrar que*

$$q \leqslant |X_F(\mathbb{F}_q)| \leqslant q+2.$$

Em particular $|X_F(\mathbb{F}_q)| > 0$ neste caso também. Além disso, a curva completa não singular associada ao corpo de funções de $X_F(\overline{\mathbb{F}}_q)$ tem gênero zero e contém $q+1$ $\mathbb{F}_q-$pontos racionais.

Observação 6.5.3 *Seja $X_F(\overline{\mathbb{F}}_q)$ uma cúbica não singular. Quando $\omega_1+\omega_2=0$, isto é, $N_1 = q+1$, segue que $\omega_1 = \pm\sqrt{-q}$. Assim, quando $N_1 = q+1$, $N_2 = q^2+1-(\omega_1^2+\omega_2^2) = (q+1)^2$. Isto é a cota superior dada para N_2 pela hipótese de Riemann é atingida. Analogamente, a cota inferior dada pela hipótese de Riemann é atingida para N_4.*

Um exemplo de cúbica não singular onde $N_1 = q+1$, para $q=p$ foi dada no exemplo 6.0.1. Outro exemplo onde $N_1 = p+1$ é a cúbica não singular definida por $F(x_0,x_1,x_2) = x_0^3+x_1^3+x_2^3 \in \mathbb{F}_2[x_0,x_1,x_2]$.

Em geral, se $X/\mathbb{F}_q$ é uma curva completa não singular de gênero g cujo numerador da função-zeta é da forma

$$f(T) = 1+q^gT^{2g},$$

então $N_n = q^n+1$ para todo $n = 1,\ldots 2q-1$, $N_{2g} = q^{2g}+1+2gq^g$ e $N_{4g} = q^{4g}+1-2gq^{2g}$. Além disso, a hipótese de Riemann vale para esta função-zeta e as cotas siperior e inferior dadas pela hipótese de Riemann são atingidas para N_{2g} e N_{4g} respectivamente.

Capítulo

7

Os Teoremas de Riemann

Sejam k um corpo e X/k uma curva completa não singular cujo corpo de funções é $k(X)|k$. Dado $P \in X$, seja v_P a valorização associada e $\mathcal{O}_P$ o domínio local principal associado a valorização v_P. Este domínio é interpretado como o conjunto das funções f em X definidas em P, equivalentemente $v_P(f) \geqslant 0$ ou $f \equiv 0$. Seja $\mathcal{M}_P \trianglelefteq \mathcal{O}_P$ o ideal maximal das funções que se anulam em P, isto é $v_P(f) > 0$ ou $f \equiv 0$.

Seja $\{P_1, \ldots, P_s\} \subseteq X$. Uma pergunta natural é se existe uma função não constante em $k(X)$ cujo conjunto dos polos e/ou zeros esteja contido em $\{P_1, \ldots, P_s\}$? Neste capítulo estudaremos esta questão. Note que estudar a existência de uma função com zero em P é equivalente a existência de uma função com polo em P, de fato se existe $\alpha \in k(X)$ tal que $\alpha(P) = 0$, então $\frac{1}{\alpha} \in k(X)$ possui polo em P. Mais precisamente estudaremos o seguinte problema: dados $\{P_1, \ldots, P_s\} \subseteq X$ e $a_1, \ldots, a_s \in \mathbb{N}^*$, podemos encontrar uma função em $k(X)$ que tem apenas polos (ou zeros) em P_i de ordem a_i para cada $i = 1, \ldots, s$? Em geral, a reposta desta questão é negativa, no próximo exemplo veremos um caso onde a resposta é positiva. Daremos condições no decorrer do capítulo quando a resposta será positiva. Vale observar que este problema é a generalização de existência de um polinômio cujas raízes e suas respectivas multiplicidades são dadas, que claramente existe e é única a menos de uma constante (seu coeficiente líder).

Exemplo 7.0.1 *Seja $\mathbb{P}^1/\overline{k}$ a reta projetiva. Seu corpo de frações é $\overline{k}(x)$. Identificamos $\mathbb{P}^1$ com $\mathbb{A}^1(\overline{k}) \sqcup \{\infty\}$ de tal forma que $\overline{k}[x]$ é o anel das funções em $\mathbb{A}^1(\overline{k})$. Sejam $\alpha_1, \ldots, \alpha_s, \beta \in \overline{k}$ distintos e $a_1, \ldots, a_s, b \in \mathbb{N}$. A função*

$$\frac{1}{(x-\alpha_1)^{a_1} \cdots (x-\alpha_s)^{a_s}} \in \overline{k}(x)$$

tem polos somente em $\alpha_1, \ldots, \alpha_s$ *cujas ordens são* $a_1, \ldots, a_s$ *respectivamente. Suponha que* $b > \sum a_i$. *A função*

$$\frac{(x-\beta)^b}{(x-\alpha_1)^{a_1}\cdots(x-\alpha_s)^{a_s}} \in \overline{k}(x)$$

tem polos em $\alpha_1, \ldots, \alpha_s$ *de ordem* $a_1, \ldots, a_s$ *respectivamente e um polo em* ∞ *de ordem* $b - \sum a_i$. *Portanto, a resposta da questão anterior é positiva neste caso.*

Seja X/k uma curva completa não singular. Relembre que $D = \sum_{i=1}^{s} a_i P_i \in \mathrm{Div}(X)$ é efetivo ou positivo se $a_i \geqslant 0$ para todo $i = 1, \ldots, s$. Denote por O o elemento neutro de $\mathrm{Div}(X)$. Considere a seguinte relação de ordem parcial em $\mathrm{Div}(X) \setminus \{O\}$:

$$D' \geq D \iff \quad D' - D \text{ é um divisor efetivo.}$$

Em particular, D é um divisor efetivo se $D \geq O$. Para cada função $\alpha \in k(X)^*$ associamos um divisor $\mathrm{div}(\alpha) := \sum v_P(\alpha)P \in \mathrm{Div}(X)$. Por convenção, $\mathrm{div}(0) \geq D$ para todo $D \in \mathrm{Div}(X)$. Assim podemos estender a ordem parcial $\geq$ para $\mathrm{Div}(X)$. Para estudar a existência de funções com zeros e polos pré-determinados, será útil considerarmos o seguinte conjunto:

$$H^0(D) := \{\alpha \in k(X) \mid \mathrm{div}(\alpha) + D \geq 0\}.$$

Facilmente podemos verificar que $H^0(D)$ é um $k-$espaço vetorial. Veremos como estudar a resposta da pergunta feita anteriormente é relacionado ao cálculo de $\dim H^0(D)$.

Exemplo 7.0.2 *Sejam* k *um corpo algebricamente fechado e* $D = \sum_{i=1}^{s} a_i P_i \geq 0$. *Então* $H^0(D)$ *é o conjunto das funções em* $k(X)$ *com possíveis polos somente em* P_i *e de ordem no máximo* a_i, *para* $i = 1, \ldots, s$. *Em particular,* $k \subseteq H^0(D)$.

Observação 7.0.4 *Se* $D = 0$, *então* $H^0(D) = k$. *De fato, o teorema 5.6.2 mostra que as únicas funções em* $k(X)$ *que não possuem polos são as constantes. Analogamente, se* $\alpha \in k(X)^*$, *então* $H^0(\mathrm{div}(\alpha)) = \alpha^{-1}k$.

Em dois casos é muito fácil calcular $h^0(D)$. *Se* $\deg(D) < 0$, *então* $H^0(D) = \{0\}$. *Isto segue do fato que* $\deg(\mathrm{div}(\alpha) + D) = \deg(\mathrm{div}(\alpha)) + \deg(D) = \deg(D)$, *pois pelo teorema 5.9.1,* $\deg(\mathrm{div}(\alpha)) = 0$ *para todo* $\alpha \in k(X)^*$. *Se* $\deg(D) = 0$, *então* $\dim H^0(D) \leq 1$. *De fato, se* $\dim H^0(D) > 0$, *então existe uma função não nula* $\alpha \in H^0(D)$. *Assim* $\mathrm{div}(\alpha) + D \geq 0$, *uma vez que* $\deg(\mathrm{div}(\alpha) + D) = 0$, $D = -\mathrm{div}(\alpha)$, *então* $H^0(D) = \alpha k$, *ou,* $\dim H^0(D) = 1$.

Dado $D' \in \mathrm{Div}(X)$, considere o conjunto $M(D') := \{\beta \in k(X) \mid \mathrm{div}(\beta) = -D'\}$. Claramente,

$$H^0(D) = \bigcup_{D \geq D'} M(D') \bigcup \{0\}.$$

Seja $h^0(D) := \dim_k(H^0(D))$. Mostraremos que $h^0(D) < \infty$, mais precisamente, $h^0(D) \leqslant \deg(D)+1$. O resultado principal a ser provado é o teorema de Riemann-Roch, que afirma a existência de um divisor C e um inteiro g tais que $\deg(D)+1-g+h^0(C-D) = h^0(D)$.

Concluímos esta introdução relembrando a motivação aritmética para o estudo de divisores e da aplicação classe,

$$\begin{array}{ccc} \mathrm{Div}(X) & \longrightarrow & \mathrm{Pic}(X) := \mathrm{Div}(X)/\mathrm{div}(k(X)^*) \\ D & \longmapsto & \mathrm{cl}(D). \end{array}$$

Dado $\mathcal{L} \in \mathrm{Pic}(X)$, seja

$$E_{\mathcal{L}} := \{D \in \mathrm{Div}(X) | D \geq 0 \text{ e } \mathrm{cl}(D) = \mathcal{L}\}.$$

É fácil ver que $E_{\mathcal{L}} = \emptyset$ se $\deg(\mathcal{L}) < 0$, uma vez que o grau de um divisor efetivo é sempre não negativo. No capítulo anterior, provamos a *racionalidade* e a *equação funcional* da função-zeta associada a uma curva completa não singular $X/\mathbb{F}_q$, usando essencialmente boas estimativas para $\#E_{\mathcal{L}}$ quando $\deg(\mathcal{L}) > 0$. Suponha $E_{\mathcal{L}} \neq 0$ e $D \in E_{\mathcal{L}}$. A cardinalidade de $E_{\mathcal{L}}$ está relacionada com $h^0(D) = \dim_{\mathbb{F}_q} H^0(D)$, dada por:

$$\#E_{\mathcal{L}} = \frac{q^{h^0(D)}-1}{q-1}.$$

Esta fórmula é provada usando a seguinte descrição do conjunto $E_{\mathcal{L}}$, válida mesmo até quando k não é um corpo finito.

Lema 7.0.1 *Sejam k um corpo, X/k uma curva completa não singular e $\mathcal{L} \in \mathrm{Pic}(X)$. Suponha $E_{\mathcal{L}} \neq 0$ e $D \in E_{\mathcal{L}}$. A aplicação:*

$$\begin{array}{ccc} \psi_D : H^0(D) \setminus \{0\} & \longrightarrow & E_{\mathcal{L}} \\ \alpha & \longmapsto & \mathrm{div}(\alpha) + D. \end{array}$$

é sobrejetora. Além disso, o grupo k^* age em $H^0(D) \setminus \{0\}$ por

$$\begin{array}{ccc} k^* \times H^0(D) \setminus \{0\} & \longrightarrow & H^0(D) \setminus \{0\} \\ (c, \alpha) & \longmapsto & c\alpha \end{array}$$

e $E_{\mathcal{L}}$ pode ser identificado com o quociente de $H^0(D)\setminus\{0\}$ pela ação de k^*. Em particular, $E_{\mathcal{L}}$ está em bijeção com $\mathbb{P}^{h^0(D)-1}(k)$.

Demonstração: *A sobrejetividade segue pela definição. Sejam $D_0 \in E_{\mathcal{L}}$ e $\alpha \in \psi_D^{-1}(D_0)$. Resta mostrar que $\psi_D^{-1}(D_0) = \{c\alpha | c \in k^*\}$. Claramente $c\alpha \in \psi_D^{-1}(D_0)$ para todo $c \in k^*$. Seja $\beta \in \psi_D^{-1}(D_0)$, então $D_0 = \mathrm{div}(\beta) + D = \mathrm{div}(\alpha) + D$. Logo, $\mathrm{div}(\beta/\alpha) = 0$. Pelo*

teorema 5.6.2, $\beta/\alpha \in k^*$, ou, $\beta = c\alpha$ para algum $c \in k^*$. ■

Definição 7.0.1 *Sejam X/k uma curva completa não singular e $D = \sum a_P P$. Definimos a ordem de P no divisor D por* $\mathrm{ord}_P(D) := a_P$.

7.1 Teorema de Riemann

Sejam k um corpo, X/k uma curva completa não singular e $D \in \mathrm{Div}(X)$. Relembre que $H^0(D) := \{\alpha \in k(X) \mid \mathrm{div}(\alpha) \geq -D\}$. Para cada ponto $P \in X$, defina

$$\mathcal{L}(D)_P := \{\alpha \in k(X) \mid \mathrm{ord}_P(\alpha) \geqslant -\mathrm{ord}_P(D)\}.$$

Considere a seguinte aplicação de $k-$espaços vetoriais

$$\begin{array}{rcl} \varphi_D : k(X) & \longrightarrow & \displaystyle\bigoplus_{P\in X}(k(X)/\mathcal{L}(D)_P) \\ f & \longmapsto & \displaystyle\bigoplus_{P\in X}(f \mod \mathcal{L}(D)_P). \end{array}$$

Por definição, $\ker(\varphi_D) = H^0(D)$. Seja $H^1(D) := \mathrm{coker}(\varphi_D)$. Mostraremos nesta seção que $H^0(D)$ e $H^1(D)$ são ambos k-espaços vetoriais de dimensão finita.

Observação 7.1.1 *Observe que se dois divisores são linearmente equivalentes, então os espaços vetoriais H^0 e H^1 associados são isomorfos. De fato, sejam $D \in \mathrm{Div}(X)$ e $D' = D + \mathrm{div}(\alpha)$ para algum $\alpha \in k(X)^*$. O isomorfismo $m_\alpha : k(X) \to k(X)$ dado pela multiplicação por α induz o seguinte diagrama comutativo de espaços vetoriais, onde as aplicações verticais são isomorfismos:*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & H^0(D') & \longrightarrow & k(X) & \xrightarrow{\varphi_{D'}} & \bigoplus_P k(X)/\mathcal{L}(D')_P & \longrightarrow & H^1(D') & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle m_\alpha} & & \downarrow & & \downarrow{\scriptstyle \varphi_\alpha} & & \\ 0 & \longrightarrow & H^0(D) & \longrightarrow & k(X) & \xrightarrow{\varphi_D} & \bigoplus_P k(X)/\mathcal{L}(D)_P & \longrightarrow & H^1(D) & \longrightarrow & 0 \end{array}$$

Suponha que $H^0(D)$ e $H^1(D)$ têm dimensão finita e denote suas dimensões respectivamente por $h^0(D)$ e $h^1(D)$. Quando $\mathcal{L} \in \mathrm{Pic}(X/k)$, seja $h^i(\mathcal{L}) := h^i(D)$, onde D é um divisor tal que $\mathrm{cl}(D)\mathcal{L}$. A observação acima mostra que $h^i(\mathcal{L})$ não depende da escolha de D. Relembre que $h^0(O) = 1$ (7.0.4).

Definição 7.1.1 *Seja X/k uma curva completa não singular. O inteiro $h^1(O)$ é chamado do* gênero *de X e é denotado por $g = g(X)$.*

No restante desta seção mostraremos que $h^0(D) - h^1(D) - \deg(D)$ é uma constante que não depende de D. Se isto for verdade, tomando $D = \operatorname{div}(\alpha)$, $\alpha \in k(X)^*$, segue da observação 7.1.1 que

$$h^0(D) - h^1(D) - \deg(D) = h^0(O) - h^1(O) - \deg(O) = 1 - g,$$

isto é,

$$h^0(D) = \deg(D) + 1 - g + h^1(D), \tag{7.1}$$

para todo $D \in \operatorname{Div}(X)$. Uma vez que $h^1(D)$ é a dimensão de uma espaço vetorial e, portanto, um inteiro não negativo,

$$h^0(D) \geqslant \deg(D) + 1 - g, \tag{7.2}$$

para todo $D \in \operatorname{Div}(X)$. A inequação anterior é chamada *teorema de Riemann*.

Observação 7.1.2 *Seja $D \in \operatorname{Div}(X)$. O teorema de Riemann implica que, se $\deg(D) \geqslant g$, então $h^0(D) > 0$. Em particular, se $d \geqslant g$, então a aplicação*

$$\mathrm{cl}^d : \mathrm{Eff}^d(X/k) \longrightarrow \mathrm{Pic}^d(X/k)$$

introduzida em 5.9.2 é sobrejetiva.

Provaremos agora que $h^0(D) < \infty$. Sejam D e E dois divisores tais que $D \geq E$. Segue imediatamente das definições que $H^0(E) \subseteq H^0(D)$ e $\mathcal{L}(E)_P \subseteq \mathcal{L}(D)_P$, para todo $P \in X$. Denote por π_P o gerador do ideal maximal de $\mathcal{O}_P \subseteq k(X)$. Então $\mathcal{L}(D)_P = \pi_P^{-\operatorname{ord}_P(D)}\mathcal{O}_P$.

Fato 7.1.1 *Se $s \leqslant t$, então $\pi_P^t\mathcal{O}_P \subseteq \pi_P^s\mathcal{O}_P$ e $\dim_k \frac{\pi_P^s\mathcal{O}_P}{\pi_P^t\mathcal{O}_P} = (t-s)\deg(P)$.*

Fato 7.1.2 *Se $D \geq E$, então $\deg(D) - \deg(E) = \dim_k \Big(\bigoplus_P \dfrac{\mathcal{L}(D)_P}{\mathcal{L}(E)_P} \Big)$.*

Demonstração: *O fato 7.1.1 garante $\dim_k \mathcal{L}(D)_P/\mathcal{L}(E)_P = (\operatorname{ord}_P(D) - \operatorname{ord}_P(E))\deg(P)$. Como $\operatorname{ord}_P(D) = \operatorname{ord}_P(E) = 0$, a menos de uma quantidade finita de pontos em X,*

$$\dim_k \Big(\bigoplus_P \frac{\mathcal{L}(D)_P}{\mathcal{L}(E)_P} \Big) = \sum_P (\operatorname{ord}_P(D) - \operatorname{ord}_P(E))\deg(P) = \deg(P) - \deg(E).$$

■

Observação 7.1.3 *Sejam $D \geq E$ dois divisores e $\varphi_1 : H^0(E) \to H^0(E)$ a aplicação inclusão. Seja*

$$\varphi_3 : \bigoplus_P k(X)/\mathcal{L}(E)_P \longrightarrow \bigoplus_P k(X)/\mathcal{L}(D)_P$$

a aplicação sobrejetiva obtida a partir da soma direta das aplicações sobrejetivas: $\varphi_{3,P} : k(X)/\mathcal{L}(E)_P \to k(X)/\mathcal{L}(D)_P$ *induzidas pelas inclusões* $\mathcal{L}(E)_P \to \mathcal{L}(D)_P$. *Considere o diagrama*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(E) & \longrightarrow & k(X) & \xrightarrow{\varphi_E} & \bigoplus_P k(X)/\mathcal{L}(E)_P & \longrightarrow & H^1(E) & \longrightarrow 0 \\ & & \downarrow{\scriptstyle \varphi_1} & & \| & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_{E,D}} & \\ 0 & \longrightarrow & H^0(D) & \longrightarrow & k(X) & \xrightarrow{\varphi_D} & \bigoplus_P k(X)/\mathcal{L}(D)_P & \longrightarrow & H^1(D) & \longrightarrow 0 \end{array}$$

onde $\varphi_{E,D}$ *é a aplicação natural induzida por* φ_3 *entre os co-núcleos de* φ_E *e* φ_D. *Por 7.1.2,* $\dim_k \ker \varphi_3 = \deg(D) - \deg(E)$. *Então*

$$\dim_k \ker(\varphi_{E,D}) = \deg(D) - \deg(E) - \dim_k \frac{H^0(D)}{H^0(E)}. \tag{7.3}$$

Lema 7.1.1 *Seja* $D \in \mathrm{Div}(X)$, $\deg(D) \geqslant 0$. *Então* $h^0(D) \leq \deg(D) + 1$. *Em particular, para todo* $D \in \mathrm{Div}(X)$, $h^0(D) < \infty$.

Demonstração: *Por 7.0.4, se* $\deg(D) < 0$, *então* $h^0(D) = 0$ *e se* $\deg(D) = 0$, *então* $h^0(D) \leqslant 1$, *logo nestes dois casos se verifica o resultado. Para* $\deg(D) > 0$, *faremos a prova por indução sobre* $\deg(D)$. *Dado* $n \in \mathbb{N}$, *suponha o lema válido para todo divisor* E *tal que* $\deg(E) \leqslant n$. *Seja* D *uma divisor tal que* $\deg(D) = n + 1$. *Então existe* $P \in X$ *tal que* $D \geq P$. *De 7.1.1 segue que*

$$0 \leqslant \deg(D) - \deg(D - P) - \dim_k \frac{H^0(D)}{H^0(D - P)}.$$

Pela hipótese de indução $h^0(D-P) < \infty$, *logo* $h^0(D) < \infty$ *e* $h^0(D) \leqslant \deg(P)+h^0(D-P)$. *Novamente pela hipótese de indução,* $h^0(D-P) \leqslant \deg(D-P)+1 = \deg(D)-\deg(P)+1$, *portanto*

$$h^0(D) \leqslant \deg(P) + h^0(D - P) \leqslant \deg(P) + \deg(D) - \deg(P) + 1 = \deg(D) + 1.$$

■

Suponha agora $h^1(D), h^1(E) < \infty$. Pela sobrejetividade de $\varphi_{E,D}$, podemos escrever

$$\dim_k \ker(\varphi_{E,D}) = h^1(E) - h^1(D). \tag{7.4}$$

De 7.3 e 7.4, se $D \geq E$, então

$$\deg(D) - h^0(D) + h^1(D) = \deg(E) - h^0(E) + h^1(E). \tag{7.5}$$

Sejam E, D, M divisores tais que $M \geq D$ e $M \geq E$. Aplicando (7.5) para $M \geq D$ e $M \geq E$,

$$\deg(D) - h^0(D) + h^1(D) = \deg(M) - h^0(M) + h^1(M) = \deg(E) - h^0(E) + h^1(E),$$

concluindo que (7.5) vale para quaisquer dois divisores.

Teorema 7.1.1 *Sejam k um corpo e X/k uma curva completa não singular. Então para todo $D \in \mathrm{Div}(X)$, $h^1(D) < \infty$. Além disso, $h^0(D) = \deg(D) + 1 - g + h^1(D)$.*
Demonstração: *Vimos acima que 7.5 vale para qualquer par de divisores. Tome $E = O$. Concluímos $h^0(D) = \deg(D) + 1 - g + h^1(D)$. Portanto temos de mostrar $h^1(D) < \infty$.*

Sejam $D \geq E$ divisores. O primeiro passo é mostrar que $\dim_k \ker(\varphi_{E,D})$ é limitada por uma constante que independe de D e E. Mostraremos primeiro este fato no caso especial em que $E = O$ e D é múltiplo de $(\alpha)_\infty$, $\alpha \in k(X)^*$. Relembre que $\mathrm{div}(\alpha) = (\alpha)_0 - (\alpha)_\infty$. Por 5.9.2, $(\alpha)_\infty$ é um divisor efetivo e $\deg((\alpha)_\infty) := n = [k(X) : k(\alpha)]$. Seja $\{\beta_1, \ldots, \beta_n\}$ uma base para $k(X)|k(\alpha)$ contida no fecho integral de $k[x]$ em $k(X)$. Uma vez que β_i é integral sobre $k[\alpha]$, um polo P de β_i também é um polo de α: de fato, se $\alpha \in \mathcal{O}_P$, então $\mathcal{O}_P$ contém o fecho integral de $k[\alpha]$ em $k(X)$, assim $\beta_i \in \mathcal{O}_P$. Então, existe um inteiro positivo m tal que $\beta_1, \ldots, \beta_n \in H^0(m(\alpha)_\infty)$. Tome $s \in \mathbb{N}$ e considere o conjunto de $n(s+1)$ funções

$$S := \{\alpha^i \beta_j | 0 \leqslant i \leqslant s, 1 \leqslant j \leqslant n\}.$$

Como $\beta_1, \ldots, \beta_n$ são independentes sobre $k[\alpha]$, as funções em S são independentes sobre k. Uma vez que $S \subseteq H^0((m+s)(\alpha)_\infty)$, para todo $\mu \geqslant m$,

$$h^0(\mu(\alpha)_\infty) \geqslant n(\mu - m + 1). \tag{7.6}$$

Sejam $D := \mu(\alpha)_\infty$ e $E = O$. Segue de 7.3 e 7.6 que

$$\begin{aligned} \dim_k \ker(\varphi_{E,D}) &= \deg(D) - 0 - h^0(D) + 1 \\ &\leqslant \mu n - n(\mu - m + 1) + 1 \\ &= nm - n + 1. \end{aligned} \tag{7.7}$$

Assim, enquanto $\varphi_{E,D}$ depende de $\mu(\alpha)_\infty$ a dimensão de $\ker(\varphi_{E,D})$ é limitada por uma constante $c := mn - n + 1$ que não depende de μ. Também segue de 7.7 que

$$\deg(\mu(\alpha)_\infty) - h^0(\mu(\alpha)_\infty) \leqslant c. \tag{7.8}$$

Para o caso geral, dado $D \in \mathrm{Div}(X)$*, tome*

$$D_1 := \sum_{\{P|\mathrm{ord}_P((\alpha)_\infty)>0\}} \mathrm{ord}_P(D)P$$

e consider $D_2 := D - D_1$*. Se* $P \in X$ *é tal que* $\mathrm{ord}_P(D_2) \neq 0$*, então* P *não é um polo de* α*. Seja* $g_P \in k[x]$ *o minimal sobre* k *da imagem de* α *em* $\mathcal{O}_P/\mathcal{M}_P$ *(se* $\mathcal{O}_P/\mathcal{M}_P = k$*, então a imagem de* α *é* $\alpha(P)$ *e* $g_P(x) = x - \alpha(P)$*). A função* $g_P(\alpha) \in k(X)$ *pertence a* $\mathcal{M}_P$ *por definição. Seja* $a \in \mathbb{N}^*$*, a função*

$$z_a := \prod_{\{P|\mathrm{ord}_P(D_2)\neq 0\}} g_P(\alpha)^a$$

é uma função em $k(X)$ *com um zero de multiplicidade pelo menos* a *em cada ponto* P*,* $\mathrm{ord}_P(D_2) \neq 0$ *e seus possíveis polos são os polos de* α*. Tome inteiros positivos* a *e* μ *suficientemente grandes tais que* $D \leqslant \mu(\alpha)_\infty + \mathrm{div}(z_a)$*. Em 7.1.1 mostramos que* $h^i(D - \mathrm{div}(z_a)) = h^i(D), i = 1, 2$*. Logo por 7.3,*

$$0 \leqslant \deg(\mu(\alpha)_\infty) - h^0(\mu(\alpha)_\infty) - (\deg(D) - h^0(D)). \tag{7.9}$$

E segue de 7.8 e 7.9*, para todo* $D \in \mathrm{Div}(X)$

$$\deg(D) - h^0(D) \leqslant c. \tag{7.10}$$

Dados $D, E \in \mathrm{Div}(X)$*,* $D \geq E$ *e* $\varphi_{E,D} : H^1(E) \to H^1(D)$*, a igualdade 7.3 e a desigualdade 7.10 implicam que*

$$\dim_k \ker(\varphi_{E,D}) \leqslant 2c. \tag{7.11}$$

Agora mostraremos $h^1(E) < \infty$*. Caso contrário, existe uma sequência* $\{e_i\}_{i\in\mathbb{N}}$ *de elementos linearmente independentes de* $H^1(E)$*. Afirmamos que existe uma cadeia infinita de divisores* $D \geq D_1 \geq \cdots \geq D_n \geq \cdots$ *tal que* $\varphi_{E,D_n}(e_i) = 0$ *para todo* $i = 1, \ldots, n$*. A existência dessa cadeia implica que*

$$\dim_k \ker(\varphi_{E,D_n}) \geqslant n, \ \forall n \in \mathbb{N},$$

mas isso contradiz 7.11. A existência da cadeia de divisores descrita acima é feita por indução. Para todo $i \in \mathbb{N}$*, seja* $f_i \in \bigoplus_P k(X)/\mathcal{L}(E)_P$ *tal que sua imagem em* $H^1(E)$ *é* e_i*. Represente* f_i *como um vetor* $(\ldots, f_{iP}, \ldots)$*, onde* $f_{iP} \in k(X)/\mathcal{L}(E)_P$*. Sejam* $P_1, \ldots, P_s$ *os pontos onde a coordenada* f_{iP} *é diferente de zero. Seja* D_1 *um divisor tal*

que $D_1 \geq D \geq E$ e para todo $j = 1, \ldots, s$, o elemento f_{jP_j} pertence ao núcleo da aplicação natural $k(X)/\mathcal{L}(E)_{P_j} \to k(X)/\mathcal{L}(D_1)_{P_j}$. Assim, com essa escolha de D_1, $\varphi_{E,D_1}(e_1) = 0$. Repetindo o argumento anterior encontramos D_2 e assim sucessivamente até D_n, onde $\varphi_{E,D_n}(e_i) = 0$ para todo $i = 1, \ldots, n$. ■

7.2 Teorema de Riemann-Roch

Sejam k um corpo, X/k uma curva completa não singular e $D \in \mathrm{Div}(X)$. Vimos na seção anterior que $h^0(D) - \deg(D) - 1 + g = h^1(D)$. O objetivo principal desta seção é provar o teorema de Riemann-Roch: exsite um divisor K tal que $H^1(D) = H^0(K - D)$.

Dado H um $k-$espaço vetorial, denotaremos seu dual por $H^\vee := \mathrm{Hom}_k(H, K)$. Sejam $D = \sum_{P \in X} a_P P, E = \sum_{P \in X} b_P P \in \mathrm{Div}(X)$. Defina,

$$\inf(D, E) := \sum_{P \in X} \min(a_P, b_P)P \quad \text{e} \quad \sup(D, E) := \sum_{P \in X} \max(a_P, b_P)P.$$

Para provar o teorema de Riemann-Roch, construiremos um $k(X)-$espaço vetorial denotado por J, chamado do espaço de *diferenciais* em X. Considere o conjunto de todos os espaços vetoriais $H^1(D), D \in \mathrm{Div}(X)$ e o conjunto das aplicações entre esses espaços da seguinte forma:

- Se $D \geq E$, considere $\varphi_{E,D} : H^1(E) \to H^1(D)$ como em 7.1.3.
- Se $\alpha \in k(X)^*$ e $D \in \mathrm{Div}(X)$, considere $\varphi_\alpha : H^1(D + \mathrm{div}(\alpha)) \xrightarrow{\sim} H^1(D)$ como em 7.1.1.

Seja $\lambda \in H^1(D)^\vee$. Se $D \geq E$ e $\alpha \in k(X)^*$, então λ define dois novos homomorfismos:

- $\lambda \circ \varphi_{E,D} : H^1(E) \longrightarrow k$ e
- $\lambda \circ \varphi_\alpha : H^1(D + \mathrm{div}(\alpha)) \longrightarrow k$.

Com as considerações acima, definimos o $k(X)-$espaço vetorial J como segue:

$$J := \left(\bigsqcup_{D \in \mathrm{Div}(X)} H^1(D)^\vee \right) \Big/ \sim ,$$

onde $\sim$ denota a seguinte relação de equivalência: sejam $\lambda_1 \in H^1(D_1)^\vee$ e $\lambda_2 \in H^1(D_2)^\vee$, então $\lambda_1 \sim \lambda_2$ se, e somente se, existe $C \in \mathrm{Div}(X)$ tal que $D_1 \geq C, D_2 \geq C$ e $\lambda_1 \circ \varphi_{C,D_1} = \lambda_2 \circ \varphi_{C,D_2}$.

Para dar estrutura de grupo a J, observe que dados $j_1, j_2 \in J$, existem um divisor D e dois homomorfismos $\lambda_1, \lambda_2 \in H^1(D)^\vee$ tal que j_1 e j_2 são as classes de equivalência de λ_1 e λ_2 respectivamente. De fato, basta se $\lambda_1 \in H^1(D_1)^\vee$ e $\lambda_2 \in H^1(D_2)^\vee$, basta tomar $D := \inf(D_1, D_2)$. Dados $j_1, j_2 \in J$, sejam $D \in \mathrm{Div}(X)$ e $\lambda_1, \lambda_2 \in H^1(D)^\vee$ os representantes das classes de j_1 e j_2 respectivamente. Então $j_1 + j_2$ é a classe de equivalência de $\lambda_1 + \lambda_2 : H^1(D) \to k$. Assim, $(J, +)$ é um grupo e O_J é o elemento neutro, associado ao homomorfismo nulo.

A a multiplicação de um elemento de J por um elemento de $k(X)$ é definida por: $0 \cdot j = 0_J$ para todo $j \in J$, e para $\alpha \in k(X)^*$, represente j por $\lambda \in H^1(D)^\vee$ e αj pela classe de equivalência de $\lambda \circ \varphi_\alpha : H^1(D + \mathrm{div}(\alpha)) \to k$.

Teorema 7.2.1 $\dim_{k(X)} J = 1$.

Demonstração: *Sejam $j, j' \in J \setminus \{0\}$, $D \in \mathrm{Div}(X)$ e $\lambda, \lambda' \in H^1(D)^\vee$ os representantes de j, j' respectivamente. Seja E um divisor com grau suficientemente grande (veja 7.1) tal que $h^0(E) > 0$ e tome $\{\alpha_1, \ldots, \alpha_n\}$ uma base para $H^0(E)$. Então para todo $i = 1, \ldots, n$, $D + \mathrm{div}(\alpha_i) \geq D - E$. Assim, para todo $i = 1, \ldots, n$, os elementos $\alpha_i j$ e $\alpha_i j'$ são representados pelas transformações lineares*

$$\alpha_i \lambda := \lambda \circ \varphi_{\alpha_i} \circ \varphi_{D-E, D+\mathrm{div}(\alpha_i)} : H^1(D - E) \longrightarrow k,$$

$$\alpha_i \lambda' := \lambda' \circ \varphi_{\alpha_i} \circ \varphi_{D-E, D+\mathrm{div}(\alpha_i)} : H^1(D - E) \longrightarrow k.$$

Suponha j e j' linearmente independentes sobre $k(X)$ (isto é, $h^1(D) \geqslant 2$). Então $S := \{\alpha_1\lambda, \ldots, \alpha_n\lambda, \alpha_1\lambda', \ldots, \alpha_n\lambda'\}$ é um conjunto de homomorfismos linearmente independentes sobre k. De fato, sejam $c_1, \ldots, c_n$ e $d_1, \ldots, d_n$ em k tal que

$$\sum_{i=1}^{n} c_i \alpha_i \lambda + \sum_{i=1}^{n} d_i \alpha_i \lambda' = 0,$$

então

$$\left(\sum_{i=1}^{n} c_i \alpha_i \right) j + \left(\sum_{i=1}^{n} d_i \alpha_i \right) j' = 0_J.$$

Como j e j' são linearmente independentes,

$$\sum_{i=1}^{n} c_i \alpha_i = 0 \quad e \quad \sum_{i=1}^{n} d_i \alpha_i = 0 \quad \text{em } k(X).$$

Uma vez que $\{\alpha_1, \ldots, \alpha_n\}$ é uma base para $H^0(E)$, $c_i = d_i = 0$ para todo $i = 1, \ldots, n$. Assim, os elementos de S são linearmente independentes e $h^1(D - E) \geqslant 2h^0(E)$. O

teorema de Riemann (7.1) implica que

$$\begin{aligned} h^0(D-E) - \deg(D) - 1 + g &= \deg(E) + h^1(D-E) \\ &\geqslant -\deg(E) + 2h^0(E) \\ &= \deg(E) + 2 - 2g + 2h^1(E) \\ &\geqslant \deg(E) + 2 - 2g \end{aligned} \tag{7.12}$$

Como $h^0(E) \neq 0$*, podemos tomar uma cadeia infinita* $D \geq E_1 \geq E_2 \geq \cdots$ *de modo que* $h^0(E_i) > 0$ *e* $\deg(E_i) < \deg(E_{i+1})$*, para todo* $i \geqslant 1$*.De* $D \geq E_i$*, segue* $h^0(D - E_i) = 0$*. Assim, de 7.12 aplicada a cada* E_i

$$-\deg(D) - 3 + 3g \geqslant \deg(E_i),\ \forall i \in \mathbb{N}. \tag{7.13}$$

Esta última desigualdade contradiz o fato de que a sequência $\{\deg(E_i)\}_{i\in\mathbb{N}}$ *tende ao infinito. Portanto,* j *e* j' *são linearmente dependentes e assim* $\dim_k(X)J = 1$*.* ■

Teorema 7.2.2 *Sejam* k *um corpo,* X/k *uma curva completa não singular e* $j \in J \setminus \{0\}$*. Então existe um divisor* $K(j) \in \mathrm{Div}(X)$ *tal que*

- j *pode ser representado pelo homomorfismo* $\lambda : H^1(K(j)) \to k$*, e*
- $K(j)$ *é maximal com respeito a seguinte propriedade: se* $E \geq K(j)$ *é um divisor tal que* j *pode ser representado por* $\lambda' : H^1(E) \to k$*, então* $E = K(j)$*.*

Além disso, para todo $\alpha \in k(X)^*, K(\alpha j) = K(j) + \mathrm{div}(\alpha)$*. Em particular, a classe de* $K(j)$ *em* $\mathrm{Pic}(X)$ *é independente de* $j \in J \setminus \{O_J\}$ *e é chamada da* classe canônica de X*.*
Demonstração: *Seja* $\lambda : H^1(D) \to k$ *o representante de* j*. Afirmamos que* $\deg(D) \leqslant 2g + 1$*. De fato,* $\deg(D) \leqslant h^0(D) + g - 1$*. Basta mostrar* $h^0(D) \leqslant g$*. Se* $h^0(D) > 0$*, seja* $\{\alpha_1, \ldots, \alpha_n\}$ *uma base para* $H^0(D)$ *sobre* k*. Como* $D + \mathrm{div}(\alpha_i) \geq 0$*, o elemento* $\alpha_i\lambda \in J$ *é representado pela aplicação* $\alpha_i\lambda : H^1(O) \to k$*. Suponha que existem* $c_1, \ldots, c_n \in k$ *tais que* $\sum_{i=1}^n c_i\alpha_i\lambda = 0$*. Então* $\lambda \sum_{i=1}^n c_i\alpha_i = 0_J$*, ou,* $\sum_{i=1}^n c_i\alpha_i = 0$*. Uma vez que* $\alpha_1, \ldots, \alpha_n$ *são linearmente independentes sobre* k*,* $c_i = 0, i = 1, \ldots, n$ *e portanto* $\dim H^1(O)^\vee \geq h^0(D)$*.*

Agora seja D *um divisor cujo grau é máximo entre os divisores* E *tais que* j *pode ser representando por um homomorfismo* $H^1(E) \to k$*. Afirmamos que* $D \geq E$*, para todo* $E \in \mathrm{Div}(X)$ *tal que* j *pode ser representado por um homomorfismo* $H^1(E) \to k$*. De fato, seja* $\lambda : H^1(D) \to k$ *e* $\lambda' : H^1(E) \to k$ *dois representantes da classe de* j*. Considere o diagrama*

$$\begin{array}{ccc} H^1(\inf(D,E)) & \xrightarrow{\psi'} & H^1(E) \\ \overset{\psi}{\downarrow} & & \overset{\varphi'}{\downarrow} \\ H^1(D) & \xrightarrow{\varphi} & H^1(\sup(D,E)), \end{array}$$

, onde $\psi = \varphi_{\inf(D,E),D}, \psi' = \varphi_{\inf(D,E),E}$ *e* φ, φ' *definidas analogamente. Como* λ *e* λ' *representam* j*, podemos tomar* $F \in \mathrm{Div}(X), F \leq D, E$ *tal que* $\lambda \circ \varphi_{F,D} = \lambda' \circ \varphi_{F,E}$*. É fácil ver que* $\lambda \circ \psi = \lambda' \circ \psi'$ *e que existe uma única aplicação* $\lambda'' : H^1(\sup(D,E)) \to k$ *tal que* $\lambda = \lambda'' \circ \varphi$ *e* $\lambda' = \lambda'' \circ \varphi'$*. Uma vez que* $\deg(D)$ *é maximal por hipótese, segue que* $\deg(\sup(D,E)) \leqslant \deg(D)$*, o que implica* $E \leq \sup(D,E) = D$*.*

É fácil ver que para todo $\alpha \in k(X)^*, K(j) + \mathrm{div}(\alpha) = K(\alpha j)$*. Pelo teorema 7.2.1, para todos* $j, j' \in J \setminus \{0_J\}$*, as classes de* $K(j)$ *e* $K(j')$ *são iguais em* $\mathrm{Pic}(X)$*.* ■

Neste momento temos os resultados necessários para provar o teorema de Riemann-Roch para curvas.

Teorema 7.2.3 *(**Riemann-Roch**) Sejam* k *um corpo e* X/k *uma curva completa não singular. Então existe* $K \in \mathrm{Div}(X)$ *tal que para todo* $D \in \mathrm{Div}(X)$*, os* $k-$*espaços vetoriais* $H^1(D)^\vee$ *e* $H^0(K-D)$ *são isomorfos. Em particular* $h^1(D) = h^0(K-D)$ *e*

$$h^0(D) = \deg(D) + 1 - g + h^0(K-D).$$

Demonstração: *Sejam* $D \in \mathrm{Div}(X)$*,* $j \in J \setminus \{0_J\}$ *e* $K = K(j)$*. Mostraremos inicialmente que a aplicação*

$$\begin{array}{rcl} \delta : H^0(D) & \longrightarrow & \mathrm{Hom}_k(H^1(K-D), H^1(K)) \\ \alpha & \longmapsto & \varphi_\alpha \circ \varphi_{K-D,K+\mathrm{div}(\alpha)}, \quad \text{se } \alpha \neq 0; \\ 0 & \longmapsto & \text{o homomorfismo nulo} \end{array}$$

é um isomorfismo. Primeiro note que se $0 \neq \alpha \in H^0(D)$*, então* $\mathrm{div}(\alpha) \geq -D$ *e, assim,* $K + \mathrm{div}(\alpha) \geq K - D$*. Portanto, as aplicações*

$$H^1(K-D) \overset{\varphi_{K-D,K+\mathrm{div}(\alpha)}}{\longrightarrow} H^1(K+\mathrm{div}(\alpha)) \overset{\varphi_\alpha}{\longrightarrow} H^1(K)$$

estão bem definidas. É fácil ver que δ *é um homomorfismo de* $k-$*espaços vetoriais. Seja* $\lambda : H^1(K) \to k$ *um representante da classe de* j*. Mostremos que* δ *é injetiva: se* $\delta(\alpha) = 0$*, então*

$$\lambda \circ \varphi_\alpha \circ \varphi_{K-D,K+\mathrm{div}(\alpha)} = 0.$$

Assim, a classe αj *de* $\lambda \circ \varphi_\alpha$ *em* J *é a classe do* 0_J*, logo* $\alpha = 0$*. Para mostrar a sobrejetetividade, seja* $\psi \in \mathrm{Hom}_k(H^1(K-D), H^1(K)) \setminus \{0\}$*. Então* $\lambda \circ \psi \in H^1(K-D)^\vee$ *e assim a classe de* $\lambda \circ \psi$ *em* J *é igual a* $\alpha\lambda$ *para algum* $\alpha \in k^*(X)$*. Uma vez que* $K + \mathrm{div}(\alpha)$ *é um divisor maximal entre os divisores* E *com a propriedade que* $\alpha\lambda$ *pode ser representada por um homomorfismo* $H^1(E) \to k$*, segue que* $K - D \leq K + \mathrm{div}(\alpha)$*, de*

modo que $\alpha \in H^0(D)$ *e*

$$\lambda \circ \psi = \lambda \circ \varphi_\alpha \circ \varphi_{K-D,K+\mathrm{div}(\alpha)}.$$

Ou seja, $\psi = \delta(\alpha)$.

Em particular, se $D = O$, *então* $H^0(D) \cong \mathrm{Hom}_k(H^1(K-O), H^1(K))$. *Como* $h^0(O) = 1$, *concluímos que* $h^1(K) = 1$. *Tome* $\lambda : H^1(K) \to k$ *a base para* $H^1(K)$. *Este homomorfismo identifica* $\mathrm{Hom}_k(H^1(K-D), H^1(K))$ *com* $H^1(K-D)^\vee$. *Tomando* $E := K-D$, *concluímos que* $H^1(E)^\vee \cong H^0(K-E)$ *para todo divisor* $E \in \mathrm{Div}(X)$. ■

Tomando $D = O$ e $D = K$ no teorema de Riemann-Roch, concluímos: $h^0(K) = g$ e $\deg(K) = 2g-2$. A classe do divisor K em $\mathrm{Pic}(X/k)$ é chamada de *classe canônica* e um divisor na classe canônica é chamado de um *divisor canônico*.

Corolário 7.2.1 *Sejam* k *um corpo,* X/k *uma curva completa não singular e* $\mathcal{L} \in \mathrm{Pic}(X/k)$. *Se* $\deg(\mathcal{L}) \geqslant 2g-1$, *então* $h^0(\mathcal{L}) = \deg(\mathcal{L}) + 1 - g$.
Demonstração: *Seja* $D \in \mathrm{Div}(X)$ *cuja classe em* $\mathrm{Pic}(X/k)$ *é* $\mathcal{L}$. *Pela hipótese* $\deg(D) > \deg(K)$, *logo* $\deg(K-D) < 0$. *Então* $h^0(K-D) = 0$ *e o resultado segue do teorema anterior.* ■

Corolário 7.2.2 *Se* $g-1 \leqslant \deg(D) \leqslant 2g-2$, *então* $h^0(D) \leqslant g$.
Demonstração: *Pela hipótese* $0 \leqslant \deg(K-D) \leqslant g-1$. *Pelo lema 7.1.1*

$$h^0(K-D) \leqslant \deg(K-D) + 1.$$

Logo, pelo teorema de Riemann-Roch

$$h^0(D) = \deg(D)+1-g+h^0(K-D) \leqslant \deg(D)+1-g+\deg(K-D)+1 = 1-g+2g-2+1 = g.$$

■

Corolário 7.2.3 *Seja* k *um corpo. A reta projetiva* $\mathbb{P}^1/k$ *tem gênero zero.*
Demonstração: *Em 5.3.5 identificamo* $k(\mathbb{P}^1)$ *com* $k(x)$. *Seja* ∞ *o ponto correspondente a* $k[1/x]_{\langle 1/x \rangle}$. *É fácil ver que* $\{1, x, \ldots, x^n\}$ *é uma base para* $H^0(n\infty)$, *então* $h^0(n\infty) = n+1$. *Pelo corolário 7.2.1, quando* $n \gg 0$, $h^0(n\infty) = n+1-g$. *Portanto,* $g = 0$. ■

Observação 7.2.1 *Sejam* k *um corpo perfeito e* X/k *uma curva completa não singular. Considere* $\overline{k(X)}$ *o fecho algébrico de* $k(X)$ *e* $\overline{k}$ *o fecho algébrico de* k *em* $\overline{k(X)}$. *Seja* $\overline{X}/\overline{k}$ *a curva completa não singular associada ao corpo de funções* $\overline{k}(X)/\overline{k}$. *O gênero de* X, $g(X)$, *é definido por ser* $h^1(O)$ *onde* O *é o divisor nulo em* $\mathrm{Div}(X/k)$, *analogamente temos*

o gênero de $\overline{X}, g(\overline{X})$. *Afirmamos que* $g(X) = g(\overline{X})$. *De fato, se* $G = \mathrm{Gal}(\overline{k}|k)$, *pode se mostrar que* $\mathrm{Div}(X) \cong \mathrm{Div}(\overline{X})^G := \{D \in \mathrm{Div}(\overline{X}) | \sigma(D) = D\}$. *Assim, dado* $D \in \mathrm{Div}(X)$ *e seu correspondente* $\overline{D} \in \mathrm{Div}(\overline{X})^G, \deg(D) = \deg(\overline{D})$ *e* $h^0(D) = h^0(\overline{D})$. *Pelo teorema 7.1.1,*

$$g(X) = \deg(D) + 1 - h^0(D) + h^1(D)$$

e

$$g(\overline{X}) = \deg(\overline{D}) + 1 - h^0(\overline{D}) + h^1(\overline{D})$$

Tomando D *tal que* $\deg(D) \gg 0$, $h^1(D) = h^1(\overline{D}) = 0$. *Portanto* $g(X) = g(\overline{X})$.

Discutiremos brevemente o *teorema de Riemann-Roch* para corpos de números. Seja L um corpo de números. Claramente, podemos considerar o *problema de Riemann-Roch* para L, isto é, podemos perguntar sobre a existência de *funções* em L com zeros e polos pré-estabelecidos. Sejam $P_1, \ldots, P_s \in \mathrm{Max}(\mathcal{O}_L)$ e $a_1, \ldots, a_s \in \mathbb{N}$, podemos perguntar se existe um elemento $\alpha \in L$ tal que

$$\begin{array}{ll} \mathrm{ord}_{P_i}(\alpha) \geqslant -a_i, & \forall i = 1, \ldots, s, \text{ e} \\ \mathrm{ord}_P(\alpha) \geqslant 0, & \text{se } P \neq P_i, \forall i = 1, \ldots, s. \end{array}$$

Seja $D := \sum_{i=1}^{s} a_i x_{v_{P_i}} \in \mathrm{Div}(L)$. Análogo ao caso de corpo de funções, considere o conjunto

$$H^0(D) := \{\alpha \in L | \mathrm{div}_L(\alpha) \geq -D\}.$$

É fácil ver que $H^0(D) := \{\alpha \in L | \alpha P_1^{a_1} \cdots P_s^{a_s} \subseteq \mathcal{O}_L\}$. Como D é efetivo, $\mathcal{O}_L \subseteq H^0(D)$, em particular $H^0(D)$ é um grupo abeliano infinito. A priori, $H^0(D)$ não tem estrutura de $\mathbb{Q}-$espaço vetorial, ao contrário do caso de corpos de funções. Porém, com certas condições *no infinito* podemos tomar um conjunto análogo ao $H^0(D)$ (ainda denotado por $H^0(D)$) que seja finito. Considere o grupo

$$\mathrm{Div}_c(L) := \mathrm{Div}(L) \oplus \left(\bigoplus_{\sigma \in V(L) \text{ arquimediano}} \mathbb{R} x_\sigma \right)$$

Sejam $P \in \mathrm{Max}(\mathcal{O}_L)$ e $\langle p \rangle = P \cap \mathbb{Z}$. Por definição do valor absoluto $|\cdot|_P$, a inequação $v_P(\alpha) \geqslant -a$ vale se, e somente se, $|\alpha|_P \leqslant p^{a/e_{P/\langle p \rangle}}$. Seja $n_{\sigma/\infty} = 1$ ou 2, dependendo se σ é real ou complexo, respectivamente. Relembre a fórmula do produto $\prod_{w \in V(L)} |\alpha|_w^{n_{w/v}} = 1$ (4.3.2). Tomando o logaritmo nesta fórmula,

$$\sum_{w \in V(L)} n_{w/v} \log |\alpha|_w = 0.$$

A seguir, dado α, definiremos $\mathrm{div}_c(\alpha)$ e seu grau de modo que a fórmula $\deg(\mathrm{div}_c(\alpha)) = 0$ continue valendo no caso de corpos de números. Se $\alpha \in L$, então

$$\mathrm{div}_c(\alpha) := \Big(\sum v_P P\Big) \bigoplus \Big(\sum n_{\sigma/\infty} \log |\alpha|_\sigma x_\sigma\Big).$$

Se $P \in \mathrm{Max}(\mathcal{O}_L)$, seja $\deg(P) := \log |\mathcal{O}_L/P|$. Se $D = (\sum a_P P) \oplus (\sum \lambda_\sigma x_\sigma) \in \mathrm{Div}_c(L)$, então $\deg(D) := \sum a_P \deg(P) + \sum \lambda_\sigma$. Com estas definições, o logaritmo na fórmula do produto mostra que $\deg(\mathrm{div}_c(\alpha)) = 0$. Seja

$$\begin{aligned} H^0(D) &:= \{\alpha \in L \mid \mathrm{div}_c(\alpha) \geq -D\} \\ &= \{\alpha \in L \mid |\alpha|_P \leqslant p^{a_p/e_{P/\langle p\rangle}}, \forall P \text{ e } |\alpha|_\sigma \leqslant e^{\lambda_\sigma}, \forall \sigma\}. \end{aligned}$$

Com esta nova definição, $\#H^0(D) < \infty$. O teorema de Riemann-Roch para curvas explicita uma relação entre $\deg(D)$ e $h^0(D)$. Se $h^1(D) = 0$, podemos escrever o teorema de Riemann-Roch para curvas como $e^{h^0(D)} = e^{\deg(D)} \cdot e^{1-g}$.

Seja $D = \sum a_P P + \sum \lambda_\sigma x_\sigma \in \mathrm{Div}_c(L)$. Considere $|H^0(D)|$ e $\|D\| := \prod_P \|P\|^{a_P} \cdot \prod_\sigma e^{\lambda_\sigma}$ como os análogos para corpos de números dos números $e^{h^0(D)}$ e $e^{\deg(D)}$, respectivamente. O teorema análogo ao teorema de Riemann-Roch é enunciado da seguinte forma:

Teorema 7.2.4 *Seja L um corpo de números de discriminante d_L. Então para todo $\epsilon > 0$, existe uma constante $a = a(\epsilon)$ tal que para todo $D \in \mathrm{Div}_c(L)$, $\|D\| > a$,*

$$\left|\#H^0(D) - 2^{-r_1}(2\pi)^{-r_2}\|D\|\sqrt{|d_L|}\right| < \epsilon.$$

A prova pode ser encontrada em [2], capítulo 5.

7.3 Gênero de um Curva Plana Não Singular

Seja $F \in \overline{k}[x_0, x_1, x_2]$ homogêneo e irredutível de grau d. Sejam $\overline{k}(X_F)|\overline{k}$ o corpo de funções de $X_F(\overline{k})$ e $X/\overline{k}$ a curva completa não singular associada a $\overline{k}(X_F)|\overline{k}$. Definimos o *gênero geométrico* $p_g(X_F(\overline{k}))$ de $X_F(\overline{k})$ como sendo o gênero de $X/\overline{k}$.

Quando $X_F(\overline{k})$ é não singular, identificaremos X com $X_F(\overline{k})$ e chamaremos o gênero geométrico de $X_F(\overline{k})$ simplesmente por gênero de $X_F(\overline{k})$, e denotaremos por g. Nosso objetivo nesta seção é calcular g em termo de d.

Teorema 7.3.1 *Seja $F \in \overline{k}[x_0, x_1, x_2]$ homogêneo e irredutível de grau d. Suponha $X_F(\overline{k})$ não singular. Então $g = (d-1)(d-2)/2$.*
Demonstração: *Seja $D \in \mathrm{Div}(X_F(\overline{k}))$. Se $\deg(D) \geqslant 2g-1$, pelo corolário 7.2.1*

$$g = \deg(D) + 1 - h^0(D). \tag{7.14}$$

Vamos exibir um divisor D de $X_F(\overline{k})$ de grau suficientemente grande e calcular $h^0(D)$, consequentemente determinar g a partir da equação 7.14.

Sem perda de generalidade, podemos assumir que a reta no infinito, $X_{x_2}(\overline{k})$ intercepta $X_F(\overline{k})$ em d pontos distintos $P_1, \ldots, P_d$. Sejam $m \in \mathbb{N}$ e $D_m := m(P_1 + \cdots + P_d)$. Claramente $\deg(D_m) = md$. Sejam $n \in \mathbb{N}$ e V_n o espaço vetorial dos polinômios homogêneos de grau n em $\overline{k}[x_0, x_1, x_2]$ junto com o polinômio nulo. Considere a aplicação

$$\begin{array}{rcl} \varphi : V_m & \longrightarrow & H^0(D_m) \\ G & \longmapsto & \frac{\text{classe de } G}{\text{classe de } x_2^m}. \end{array}$$

Vejamos que φ está bem definida. Claramente a função G/x_2^m está definida em $X_F(\overline{k}) \setminus X_{x_2}(\overline{k})$. Mostremos que a ordem do polo $P := (c_0 : 1 : 0) \in X_F(\overline{k}) \cap X_{x_2}(\overline{k})$ de G/x_2^m é no máximo m. Em $\mathbb{P}^2(\overline{k}) \setminus X_{x_1}(\overline{k})$, a curva $X_F(\overline{k}) \setminus X_{x_1}(\overline{k})$ corresponde a curva afim $Z_{f_1}(\overline{k})$ onde $f_1(x, z) = F(x, 1, z)$. O ponto $P := (c_0 : 1 : 0)$ corresponde ao ponto $(c_0, 0.)$ O anel $\mathcal{O}_P$ é isomorfo a localização $\overline{k}[x, z]/\langle f_1 \rangle$ em $\langle x - c_o, z \rangle$. Seja v_P a valorização associada. Então

$$\begin{array}{rcl} v_P(G(x, 1, z)/z^m) & = & v_P(G(x, 1, z)) = mv_P(z) \\ & \geqslant & -mv_P(z). \end{array}$$

Uma vez que a reta $X_{x_2}(\overline{k})$ intercepta $X_F(\overline{k})$ em d pontos distintos, concluímos que $v_P(z) = 1$. Assim, $G(x, 1, z)/z^m$ é definida em P ou tem em P um polo de ordem no máximo m.

Afirmamos que φ é sobrejetora. Seja $\alpha \in H^0(D_m)$ representado por $\frac{\text{classe de } G}{\text{classe de } H} \in \overline{k}(X_F)$. Precisamos mostrar que existe $A \in \overline{k}[x_0, x_1, x_2]$ homogêneo de grau m tal que

$$\frac{\text{classe de } G}{\text{classe de } H} = \frac{\text{classe de } A}{\text{classe de } x_2^m} \in \overline{k}(X_F). \tag{7.15}$$

Neste caso $\varphi(A) = \alpha \in \alpha \in H^0(D_m)$ e

$$\frac{\text{classe de } G}{\text{classe de } H} \in \bigcap_{P \in X_F(\overline{k}) \setminus X_{x_2}(\overline{k})} \mathcal{O}_P.$$

Seja $f_2(x, y) := F(x, y, 1)$. Lembre-se que identificamos $\overline{k}(Z_{f_2})$ com $\overline{k}(X_F)$ (veja 5.1.1) e com essa identificação,

$$\frac{\text{classe de } G(x, y, 1)}{\text{classe de } H(x, y, 1)} \in \bigcap_{(a,b) \in Z_{f_2}(\overline{k})} (\overline{C}_{f_2})_{\langle x-a, y-b \rangle}.$$

Pela proposição 0.1.2,

$$\bigcap_{(a,b)\in Z_{f_2}(\overline{k})} (\overline{C}_{f_2})_{\langle x-a,y-b\rangle} = \overline{C}_{f_2}.$$

Assim, existe $a(x,y) \in \overline{k}[x,y]$ *tal que, em* $\overline{C}_{f_2}$,

$$\frac{\textit{classe de } G(x,y,1)}{\textit{classe de } H(x,y,1)} = \textit{classe de } a(x,y).$$

Seja $A(x_0,x_1,x_2) := x_2^m a(\frac{x_0}{x_2}, \frac{x_1}{x_2})$. *Então 7.15 vale para a classe de* A *e assim* φ *é sobrejetora.*

Considere agora o homomorfismo de $\overline{k}-$*espaços vetoriais*

$$\begin{array}{rccc} \psi : V_{m-d} & \longrightarrow & V_m \\ H & \longmapsto & FH. \end{array}$$

É fácil ver que ψ *é injetiva. Além disso,* $\mathrm{Im}\psi = \ker(\varphi)$, *uma vez que* $\frac{\textit{classe de } G}{\textit{classe de } x_2^m} = 0$ *em* $\overline{k}(X_F)$ *se, e só se,* $F|G$. *Então a sequência*

$$0 \longrightarrow V_{m-d} \longrightarrow V_m \longrightarrow H^0(D_m) \longrightarrow 0$$

é exata. Portanto

$$\dim_{\overline{k}} H^0(D_m) = \dim_{\overline{k}} V_m - \dim_{\overline{k}} V_{m-d}. \tag{7.16}$$

Ou,

$$\begin{array}{rcl} \dim_{\overline{k}} H^0(D_m) & = & \frac{(m+1)(m+2)}{2} - \frac{(m-d+1)(m-d+2)}{2} \\ & = & md + 1 - \frac{(d-1)(d-2)}{2}. \end{array}$$

Portanto,

$$\frac{(d-1)(d-2)}{2} = \deg(D_m) + 1 - \dim_{\overline{k}} H^0(D_m).$$

Tomando $m \gg 0$ *tal que* $\deg(D_m) > 2g-1$, *usando 7.14, concluímos*

$$g = \deg(D_m) + 1 - h^0(D_m) = \frac{(d-1)(d-2)}{2}.$$

■

Em geral a relação entre g e d é dada por uma desigualdade:

Proposição 7.3.1 *Sejam* $X_F(\overline{k})$ *uma curva projetiva plana e* $X/\overline{k}$ *a curva completa não singular associada. Então* $g(X) \leqslant \frac{(d-1)(d-2)}{2}$, *ocorrendo a igualdade se* $X_F(\overline{k})$ *é não singular.*

Para a demonstração, veja [6] página 330.

7.4 A Fórmula de Riemann-Hurwitz

Na proposição 7.3.1, vimos que quando $X_F(\overline{k})$ é singular, então o gênero da curva completa não singular associada é no máximo $(d-1)(d-2)/2$. A igualdade no entanto, ocorre se $X_F(\overline{k})$ é não singular. Em geral, o gênero de X pode ser calculado para qualquer F analisando as singularidades de $X_F(\overline{k})$. Nesta seção mencionaremos (sem provar) algumas fórmulas para gênero.

Proposição 7.4.1 *Sejam* $f(x,y) = y^n - c\prod_{i=1}^{s}(x-a_i)^{r_i}$, $\prod_{i\neq j}(a_i - a_j) \neq 0$, $c \in \overline{k}^*$ *irredutível e* $X/\overline{k}$ *a curva completa não singular associada ao corpo de funções de* $Z_f(\overline{k})$. *Fazendo uma mudança de variáveis se necessário, podemos assumir que* $n|\sum_{i=1}^{s} r_i$. *Sejam* $p = \mathrm{char}(\overline{k})$ *e* $(p,n) = 1$. *Então* $2g(X) = (s-2)(n-1) - \sum_{i=1}^{s}((r_i,n)-1)$. *Em particular, no caso de curvas hiperelíticas, ou seja,* $n = 2$, *se* $s = 2g+\epsilon$, *onde* $\epsilon = 1$ *ou* 2, *então o gênero de* X *é* g.

Observação 7.4.1 *Suponha que* $\mathrm{char}(\overline{k}) \neq 2$. *A proposição 7.4.1 mostra que, para todo inteiro* $g \geq 0$, *existe uma curva completa não singular* $X/\overline{k}$ *de gênero* g. *Como o gênero de uma curva plana projetiva não singular dada por um polinômio de grau* n *é igual* $g = \frac{(n-1)(n-2)}{2}$, *concluímos que nem todas as curvas completas não singulares tem o corpo de funções isomorfo ao corpo de funções de uma curva projetiva plana não singular. Em outras palavras, nem todas as curvas completas não singulares* são *curvas planas projetivas não singulares. Em particular, como a equação* $2 = \frac{(n-1)(n-2)}{2}$ *não tem solução inteira, nenhuma curva completa não singular de gênero* 2 *é uma curva plana não singular.*

A fórmula para o gênero da proposição 7.4.1 é consequência imediata da *fórmula de Riemann-Hurwitz*.

Teorema 7.4.1 (**Fórmula de Riemann-Hurwitz**) *Sejam* $\pi : X \to Y$ *um morfismo de curvas completas não singulares sobre* $\overline{k}$ *e* $n := \deg(\pi)$. *Suponha* $(n, \mathrm{char}(\overline{k})) = 1$. *Então*

$$2g(X) - 2 = n(2g(Y) - 2) + \sum_{P\in X}(e_P - 1),$$

onde e_P *é o índice de ramificação de* P *(i.é,* $\mathcal{M}_{\pi(P)}\mathcal{O}_P = \mathcal{M}_P^{e_P}$*).*

Capítulo

8

Morfismos de Frobenius e a Hipótese de Riemann

Nas quatro primeiras seções deste capítulo introduziremos e discutiremos alguns conceitos tais como *morfismo e endomorfismo de Frobenius* que serão uteis na última seção, onde usaremos além destes conceitos, o teorema de Riemann-Roch para provar a hipótese de Riemann para curvas completas não singulares sobre corpos finitos. A hipótese de Riemann dará cotas superior e inferior para o números de $\mathbb{F}_q-$pontos racionais de uma curva sobre um corpo finito (lembre-se 6.3.2).

8.1 Extensões Inseparáveis

Seja k um corpo de $\mathrm{char}(k) = p > 0$. Nesta seção discutiremos o teorema 1.3.1 para o caso em que a extensão corpo de função é inseparável. Neste sentido, nosso primeiro objetivo é descrever as extensões puramente inseparáveis de um corpo K, onde K é uma extensão finita de $k(x)$.

Definição 8.1.1 *Seja R um anel de característica $p > 0$. A aplicação* $\mathrm{Frob}_R : R \to R$, $r \mapsto r^p$, *é um homomorfismo de anéis chamado do* morfismo de Frobenius absoluto *de R.*

Seja k um corpo de característica $p > 0$. O homomorfismo $\mathrm{Frob}_k : k \to k$ é a identidade se, e somente se, $k = \mathbb{F}_p$. De fato, se $\mathrm{Frob}_k = \mathrm{id}_k$, então $\alpha^p - \alpha = 0$, para todo $\alpha \in k$. Como $y^p - y \in k[y]$ tem p raízes distintas em $\overline{k}$, concluímos que $2 \leqslant |k| \leqslant p$. Por outro lado, $\mathrm{char}(k) = p$, então $|k| \geqslant p$, portanto $|k| = p$.

Seja k um corpo contido em um anel R e considere R como uma $k-$álgebra. Então Frob_R é um morfismo de $k-$álgebras, se, e somente se $k = \mathbb{F}_p$. Seja $R^p = \text{ImFrob}_R$. O conjunto R^p é um subanel de R, mas não é, em geral, uma $k-$subalgebra de R (isto é, podem existir $\alpha \in k$ e $r \in R^p$ tais que $\alpha r \notin R^p$). Relembre que um corpo k é perfeito se a aplicação Frob_R é sobrejetora e assim, um isomorfismo de corpos. Assim, quando k é perfeito, R^p é uma $k-$álgebra.

A próxima proposição é o primeiro resultado para *conhcer* as extensões puramente inseparáveis e finitas de $k(x)$.

Proposição 8.1.1 *Sejam k um corpo perfeito, $\overline{k(x)}$ o fecho algébrico de $k(x)$ e $L \subseteq \overline{k(x)}$ uma extensão puramente inseparável de $k(x)$ de grau p. Denote $x^{1/p}$ a única raiz do polinômio $y^p - x$ em L. Então $L = k(x^{1/p})$ e $k(x) = L^p$.*
Demonstração: *Como $[L : k(x)] = p$, o corpo L contém uma raiz de um polinômio da forma $y^p - g(x) \in k(x)[y]$. Escreva $g(x) = \frac{\sum_{i=0}^{n} a_i x^i}{\sum_{j=0}^{m} b_j x^j}$. Por k ser perfeito, todo elemento $a \in k$ tem uma única raiz $p-$ésima em k que denotaremos por $a^{1/p}$. Em $k(x)(x^{1/p}) \cong k(x^{1/p})$,*

$$h(x) := \frac{\sum_{i=0}^{n} a_i^{1/p} (x^{1/p})^i}{\sum_{j=0}^{m} b_j^{1/p} (x^{1/p})^j}.$$

Então $h^p = g$. Como $[L : k(x)] = [k(x^{1/p}) : k(x)] = p$, e ambos contém uma raiz do polinômio irredutível $y^p - g(x)$, concluímos que $L = k(x^{1/p})$. Por k ser perfeito, $\text{Frob}_{k(x^{1/p})}(k(x^{1/p})) = k(x)$, portanto $L^p = k(x)$. ■

Seja K um corpo com característica $p > 0$. Se $\alpha \in \overline{K}$, então denotaremos por $\alpha^{1/p}$ a única raiz de $y^p - \alpha$ em $\overline{K}$. Equivalentemente, $\alpha^{1/p} = \text{Frob}_{\overline{k}}^{-1}(\alpha)$. Definimos por indução $\alpha^{1/p^n} := (\alpha^{1/p^{n-1}})^{1/p}$.

Proposição 8.1.2 *Sejam k um corpo perfeito, $K|k(x)$ finita e $L|K$ puramente inseparável de grau p^n. Então $K = L^{p^n}$. Em particular, $L = k^{1/p^n} := \{\alpha^{1/p^n} | \alpha \in K\}$.*
Demonstração: *A extensão puramente inseparável $L|K$ é obtida adicionando a K as raízes de uma quantidade finita de polinômios da forma $y^{p^{n_i}} - q_i \in K[y]$. Seja $m = \max n_i$. Como $[L : K] = p^n$, concluímos que $m \leqslant n$. É fácil ver que $L^{p^m} \subseteq K$. Afirmamos que*

$[L : L^{p^m}] = p^m$. *De fato, as aplicações $(\text{Frob}_L)^m, (\text{Frob}_K)^m$ e $(\text{Frob}_{k(x)})^m$ são*

isomorfismos de corpos:

$$\begin{array}{ccccc} L & \overset{(\mathrm{Frob}_L)^m}{\longrightarrow} & L^{p^m} & \subseteq & L \\ \uparrow & & \uparrow & & \uparrow \\ K & \overset{(\mathrm{Frob}_K)^m}{\longrightarrow} & K^{p^m} & \subseteq & K \\ \uparrow & & \uparrow & & \uparrow \\ k(x) & \overset{(\mathrm{Frob}_{k(x)})^m}{\longrightarrow} & k(x)^{p^m} & \subseteq & k(x) \end{array}$$

Assim, $[L^{p^m} : k(x)^{p^m}] = [L : k(x)]$. *Portanto,* $[L : L^{p^m}] = [k(x) : k(x)^{p^m}]$. *Por* k *ser perfeito,* $k(x)^{p^m} = k(x^{p^m})$. *Então,* $p^m = [k(x) : k(x^{p^m})] = [L : L^{p^m}]$.

Como $[L : K] \leqslant [L : L^{p^m}]$, *segue da afirmação anterior* $n \leqslant m$. *Assim,* $m = n$ *e* $L^{p^n} = K$. ■

Observação 8.1.1 *Sejam* $L = k(x, y)$ *e* $K = k(x, y^p)$. *Então* $L|K$ *é algébrica e* $[L : K] = p$. *É fácil ver que* $x^{1/p} \notin L$ *e* $L^p = k(x^p, y^p) \subsetneqq K \subsetneqq L$. *Este exemplo mostra que a hipótese de* $K|k(k)$ *ser finita não pode ser retirada da proposição anterior (ou de 8.1.2).*

Proposição 8.1.3 *Sejam* k *um corpo perfeito,* $K|k(x)$ *finita e* $L|K$ *puramente inseparável de grau* p^n. *Sejam* A *um domínio de Dedekind contendo* k *cujo corpo de frações é* K *e* B *o fecho integral de* A *em* L. *Então*

1. B *é um domínio de Dedekind e* $A = B^{p^n}$;
2. *A aplicação* $\pi : \mathrm{Max}(B) \to \mathrm{Max}(A), M \mapsto M \cap A$ *é uma bijeção;*
3. $\mathrm{Cl}(A) \cong \mathrm{Cl}(B)$. *isomorfos.*

Demonstração: *1- Observe que se* $\varphi : L \to L'$ *é um isomorfismo de corpos, então* $\varphi(B)$ *é o fecho integral de* $\varphi(A)$ *em* L'. *Seja* $\varphi := (\mathrm{Frob}_L)^n$. *Pela proposição 8.1.2,* $\varphi(L) = L^{p^n} = K$. *Então* $\varphi(B) = B^{p^n}$ *é o fecho integral de* $\varphi(A) = A^{p^n}$ *em* K. *É claro que todo elemento de* A *é integral sobre* A^{p^n}. *Assim,* $A \subseteq B^{p^n}$. *Como* A *é um domínio de Dedekind, é integralmente fechado, portanto* $A = B^{p^n}$ *e* B^{p^n} *é um domínio de Dedekind. Uma vez que* $\varphi(B)$ *é uma domínio de Dedekind e* φ *um isomorfismo, concluímos que* B *também é um domínio de Dedekind.*

2- Mostramos que $\pi : \mathrm{Max}(B) \to \mathrm{Max}(B^{p^n}), M \mapsto M \cap B^{p^n}$ *é uma bijeção. Pela observação 1.5.1,* π *está bem definida. Como* B *é o fecho integral de* $A = B^{p^n}$, *o lema 2.2.1 mostra que a sobrejetividade de* π. *Resta mostrar a injetividade. Sejam* $M_1, M_2 \in \mathrm{Max}(B)$, *se* $M_1 \cap B^{p^n} = M_2 \cap B^{p^n}$, *então para todo* $\alpha \in M_1, \alpha^{p^n} \in M_1 \cap B^{p^n} \subseteq M_2$. *Como* M_2 *é um ideal primo,* $\alpha \in M_2$. *Então* $M_1 \subseteq M_2$. *Analogamente,* $M_2 \subseteq M_1$, *portanto* $M_1 = M_2$ *e assim* π *é injetora.*

3- Um isomorfismo de anéis $\psi : R \to R'$, induz um isomorfismo de grupos $\psi_{\mathrm{Cl}} : \mathrm{Cl}(R) \to \mathrm{Cl}(R')$, dado por classe de $I \to$ classe de $\psi(I)$. *Uma vez que* $\mathrm{Frob}_B : B \to A$ *é um isomorfismo, concluímos a prova da parte 3.* ■

A proposição anterior mostra que B é Noetheriano, mas não mostra que B é um $A-$módulo finitamente gerado. Quando $L|K$ é separável, o teorema 1.3.1 garante que B é um $A-$módulo finitamente gerado. Mostraremos agora que essa afirmação vale sempre que $L|k(x)$ for finita e $A = k[x]$.

Teorema 8.1.1 *Sejam k um corpo, $L|k(x)$ finita e B o fecho integral de $k[x]$ em L. Então B é um $k[x]-$módulo finitamente gerado.*
Demonstração: *Assuma primeiro $L|k(x)$ puramente inseparável. Então $L = k(x)(h_1^{1/p^{n_1}}, \ldots, h_s^{1/p^{n_s}})$. Sejam $n = \max\{n_1, \ldots, n_s\}$, $\overline{L}$ o fecho algébrico de L e k' o subcorpo de $\overline{L}$ obtido por k , das raízes p^n-ésimas e os coeficientes de $h_i, i = 1, \ldots, s$. Tome $L' = k'(x^{1/p^n})$ e B' o fecho integral de $k[x]$ em L'. Por construção, $L \subseteq L'$. Se B' é um $k[x]-$módulo finitamente gerado, então seu $k[x]-$submódulo B também é um $k[x]-$módulo finitamente gerado, pois $k[x]$ é Noetheriano (veja 1.3.1). Mostraremos que B' é um $k[x]-$módulo finitamente gerado. É fácil ver que $k'[x]$ é o fecho integral de $k[x]$ em $k'(x)$, assim $k'[x]$ é um $k[x]-$modulo finitamente gerado. Também $k'[x^{1/p^n}]$ é o fecho integral de $k'[x]$ em L', então $k'[x^{1/p^n}]$ é um $k'[x]-$módulo finitamente gerado. Uma vez que $B' = k'[x^{1/p^n}]$, concluímos que B' é um $k[x]-$módulo finitamente gerado.*

Para o caso geral, sejam $M|L$ a menor extensão de L em $\overline{L}$ tal que $M|k(x)$ é normal e C o fecho integral de $k[x]$ em M. Se C é um $k[x]-$módulo finitamente gerado então B também é. Mostremos que C é um $k[x]-$módulo finitamente gerado. Sejam N a maior extensão puramente inseparável de $k(x)$ em M e A o fecho integral de $k[x]$ em N. Como $N|k(x)$ é puramente inseparável, por nossa discussão anterior, A é um $k[x]-$módulo finitamente gerado. Como C é o fecho integral de A em M, o teorema 1.3.1 implica que C é um $A-$módulo finitamente gerado. Portanto, C é um $k[x]-$módulo finitamente gerado. ■

O teorema anterior admite generalização trocando $k[x]$ por uma $k-$álgebra finitamente gerada cujo corpo de frações é K.

Corolário 8.1.1 *Sejam k um corpo,* $\mathrm{char}k = p > 0$, *$K|k(x)$ finita e $L|K$ puramente inseparável de grau p^n. Sejam A, B o fecho integral de $k[x]$ em K e L, respectivamente. Se $P \in \mathrm{Max}(A)$, então $PB = M^{p^n}$, para algum $M \in \mathrm{Max}(B)$. Além disso, a aplicação norma $N_{B/A} : I_B \to I_A$ está bem definida e, para todo $\alpha \in B, N_{B/A}(\alpha B) = \mathrm{Norm}_{L/K}(\alpha)A$.*
Demonstração: *Seja $P \in \mathrm{Max}(A)$. Pela proposição 8.1.3, existe um único $M \in \mathrm{Max}(B)$ tal que $M \cap A = P$. Como B é um domínio de Dedekind, $PB = M^e$, para*

algum inteiro e. Uma vez que B é um $A-$módulo finitamente gerado, o teorema 2.2.1 mostra que $e|p^n$. Afirmamos que $e = p^n$ ou, equivalentemente $[\frac{B}{M} : \frac{A}{P}] = 1$. De fato, como k é perfeito, toda extensão do corpo residual de $k[x]$ é perfeito. Como cada extensão do corpo residual de A é uma extensão finita do corpo residual de $k[x]$, concluímos que todas as extensões do corpo residual e A são perfeitas. Uma vez que $A = B^{p^n}$, a extensão $\frac{B}{M}|\frac{A}{P}$ é trivial ou puramente inseparável. Como A/P é um corpo perfeito, então $\frac{B}{M} = \frac{A}{P}$.

Como B é um $A-$modulo finitamente gerado, a aplicação norma $N_{B/A}$ está bem definida e, para todo $M \in \mathrm{Max}(B), N_{B/A}(M) = M \cap A$. Seja $\alpha \in B \setminus \{0\}$, escreva $\alpha B = \prod_{i=1}^{r} M_i^{a_i}$. Seja $m \in \mathbb{N}^*$ tal que $\alpha^{p^m} \in A$. Pelo lema 3.1.1, $\mathrm{Norm}_{L/K}(\alpha) = (\alpha^{p^m})^{p^{n-m}} = \alpha^{p^n}$.

Resta mostrar que $\alpha^{p^n} A = \prod_{i=1}^{r}(M_i \cap A)^{a_i}$. Pela injetividade de $i_{B/A} : I_A \to I_B$ (veja 3.4.1), é suficiente mostrar que $\alpha^{p^n} B = \prod_{i=1}^{r}(M_i \cap A)^{a_i} B$. Uma vez que $(M_i \cap A)B = M_i^{p^n}$, nossa afirmação segue. ■

Proposição 8.1.4 *Sejam k um corpo perfeito e $L|k(x)$ finita. Então existe $y \in L$ tal que $L = k(x)(y)$.*

Demonstração: *O número de subcorpos K com $k(x) \subseteq K \subseteq L$ é finito se, e somente se, existe $y \in L$ com $L = k(x)(y)$, veja [1], teorema V.4.6. Mostraremos então que existe uma quantidade finita destes subcorpos K. Suponha por absurdo que existem infinitos $K_i, i \in \mathbb{N}$ distintos com tal propriedade. Denote por L_0 a extensão maximal de $k(x)$ em L separável e por $K_{i,0}$ a extensão maximal de $k(x)$ em K_i separável. Como $L_0|k(x)$ é finita e separável e $K_{i,0} \subseteq L_0$, para todo $i \in \mathbb{N}$, o conjunto $\{K_{i,0} | i \in \mathbb{N}\}$ contém uma quantidade finita de corpos distintos. Assim, existe um índice i e infinitos subcorpos $K_j's$ de L tais que $K_j \cap L_0 = K_{i,0}$. Uma vez que $[L : K_{i,0}] < \infty$, podemos tomar dois índices j_1 e j_2 tal que $[K_{j_1} : K_{i,o}] = [K_{j_2} : K_{i,o}]$. Logo, pela proposição 8.1.2, $K_{j_1} = K_{j_2}$, absurdo!* ■

Corolário 8.1.2 *Sejam k um corpo perfeito e $L|k(x)$ finita e não separável. Então existe $y \in L$ tal que*

1. *$k(y)$ é isomorfo ao corpo de funções racionais em uma variável e*
2. *$L = k(x)(y)$ e $L|k(y)$ é separável.*

Demonstração: *A proposição 8.1.4 mostra a existência de $y \in L$ tal que $L = k(x)(y)$. Sem perda de generalidade, podemos assumir que y é integral sobre $k[x]$. Seja $f(x, Y) \in k[x, Y]$ o minimal (irredutível e mônico em Y) de y sobre $k[x]$. Considere agora o polinômio $f(X, Y)$ como um polinômio em X e seja $a(Y)$ seu coeficiente líder. Então $\frac{f(X,y)}{a(y)} = \min_{k(y)}(x)$. O elemento y não é algébrico sobre k. Caso contrário $k(y)|k$ seria algébrica o que implicaria $k(x, y)|k$ algébrica, absurdo. Portanto, o corpo $k(y)$ é isomorfo ao corpo de funções racionais em uma variável.*

Mostremos agora que $L|k(y)$ é separável. Como $L|k(x)$ não é separável, $f(X,Y) = g(X,Y^p)$, para algum $g \in k[X,Y]$. Se $L|k(y)$ não for separável, então $f(X,Y) = h(X^p,Y^p)$ para algum $h \in k[X,Y]$. Logo, como k é perfeito, $f(X,Y) = \widetilde{h}(X,Y)^p$ e, assim, f não seria irredutível, contradição. Portanto $L|k(y)$ é separável. ■

8.2 Morfismos de Frobenius

Nesta seção sempre k será um corpo perfeito de característica $p > 0$.

Sejam $f(x_1,\ldots,x_m) = \sum_{i_1+\cdots+i_m\leqslant d} a_{i_1\ldots i_m} x_1^{i_1}\cdots x_m^{i_m} \in k[x_1,\ldots,x_m]$ e

$$f^{(p^n)}(x_1,\ldots,x_m) := \sum_{i_1+\cdots i_m\leqslant d} (a_{i_1\ldots i_m})^{p^n} x_1^{i_1}\cdots x_m^{i_m}.$$

Observe que se k não é perfeito, $f^{(p)}$ pode ser redutível mesmo que f seja irredutível. Mas, se k é perfeito então f *irredutível* $\Leftrightarrow$ $f^{(p)}$ *irredutível.* Isto vale basicamente pelo fato que neste caso para todo $a \in k$, $a^{1/p} := \mathrm{Frob}_k^{-1}(a) \in k$.

Definição 8.2.1 *Sejam k uma corpo perfeito, $f \in \overline{k}[x,y]$ irredutível e $n \in \mathbb{N}$. Sejam $\overline{C}_f := \overline{k}[x,y]/\langle f\rangle$ e $\overline{C}_{f^{(p^n)}} := \overline{k}[x,y]/\langle f^{(p^n)}\rangle$. A aplicação*

$$\begin{array}{ccc} (\varphi_{\overline{k}}^n)^* : \overline{C}_{f^{(p^n)}} & \longrightarrow & \overline{C}_f \\ \textit{classe de } g(x,y) & \longmapsto & \textit{classe de } g(x^{p^n},y^{p^n}) \end{array}$$

é um homomorfismo de $\overline{k}-$álgebras. Esse homomorfismo de anéis de funções induz um morfismo de curvas afins

$$\begin{array}{ccc} \varphi_{\overline{k}}^n : Z_f(\overline{k}) & \longrightarrow & Z_{f^{(p^n)}}(\overline{k}) \\ (a,b) & \longmapsto & (a^{p^n},b^{p^n}) \end{array}$$

*chamado de $n-$*ésimo morfismo de Frobenius.

Seja $F \in \overline{k}[x_0,x_1,x_2]$ homogêneo e irredutível. A aplicação

$$\begin{array}{ccc} \varphi_{\overline{k}}^n : X_F(\overline{k}) & \longrightarrow & X_{F^{(p^n)}}(\overline{k}) \\ (c_0:c_1:c_2) & \longmapsto & (c_0^{p^n}:c_1^{p^n}:c_2^{p^n}) \end{array}$$

está bem definida. Apesar de não definirmos explicitamente o conceito de morfismo de curvas projetivas planas, chamaremos $\varphi_{\overline{k}}^n$ de *$n-$ésimo morfismo de Frobenius* de $X_F(\overline{k})$. Pois será um morfismo no sentido de curva completa não singular associada a $X_F(\overline{k})$. Quando $n = 1$ denotaremos $\varphi_{\overline{k}}^n$ simplesmente por $\varphi_{\overline{k}}$. Sejam $f(x,y) = F(x,y,1)$ e i :

$\mathbb{A}^2(\overline{k}) \to \mathbb{P}^2(\overline{k})$, dada por $(a,b) \mapsto (a:b:1)$. O seguinte diagrama é comutativo:

$$\begin{array}{ccc} Z_f(\overline{k}) & \xrightarrow{\varphi^n_{\overline{k}}} & Z_{f^{(p^n)}}(\overline{k}) \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} \\ X_F(\overline{k}) & \xrightarrow{\varphi^n_{\overline{k}}} & X_{F^{(p^n)}}(\overline{k}). \end{array}$$

A próxima proposição (8.2.1) motiva a definição do morfismo de Frobenius para curvas completas não singulares. Mas antes, introduziremos as seguintes notações. Seja $f \in k[x,y]$ irredutível e considere a aplicação

$$\begin{array}{ccc} (\varphi^n)^* : C_{f^{(p^n)}} & \longrightarrow & C_f \\ \text{classe de } g(x,y) & \longmapsto & \text{classe de } g(x^{p^n}, y^{p^n}). \end{array}$$

Uma vez que $f^{(p^n)}(x^{p^n}, y^{p^n}) = (f(x,y))^{p^n}$, a aplicação $(\varphi^n)^*$ está bem definida. Além disso, $(\varphi^n)^*$ é injetiva e portanto induz um homomorfismo de corpos

$$(\varphi^n)^* : k(Z_{f^{(p^n)}}) \longrightarrow k(Z_f).$$

Assuma que $f(x,y) = F(x,y,1)$. Relembre o isomorfismo de corpos

$$\begin{array}{ccc} i_{F,f} : k(X_F) & \longrightarrow & k(Z_f) \\ \frac{G(x_0,x_1,x_2)}{H(x_0,x_1,x_2)} & \longmapsto & \frac{G(x,y,1)}{H(x,y,1)}. \end{array}$$

Denote também por $(\varphi^n)^*$ a aplicação

$$\begin{array}{ccc} (\varphi^n)^* : k(X_{F^{(p^n)}}) & \longrightarrow & k(X_F) \\ \frac{G(x_0,x_1,x_2)}{H(x_0,x_1,x_2)} & \longmapsto & \frac{G(x_0^{p^n},x_1^{p^n},x_2^{p^n})}{H(x_0^{p^n},x_1^{p^n},x_2^{p^n})}. \end{array}$$

O seguinte diagrama é comutativo

$$\begin{array}{ccccc} C_{f^{(p^n)}} & \longrightarrow & k(Z_{f^{(p^n)}}) & \xrightarrow{(i_{F^{(p^n)},f^{(p^n)}})^{-1}} & k(X_{F^{(p^n)}}) \\ \downarrow{\scriptstyle (\varphi^n)^*} & & \downarrow{\scriptstyle (\varphi^n)^*} & & \downarrow{\scriptstyle (\varphi^n)^*} \\ C_f & \longrightarrow & k(Z_f) & \xrightarrow{(i_{F,f})^{-1}} & k(X_F) \end{array}$$

Proposição 8.2.1 *Sejam k um corpo perfeito, $F \in k[x_0,x_1,x_2]$ homogêneo e irredutível e $f(x,y) = F(x,y,1)$. Então*

1. $(\varphi^n)^*(C_{f^{(p^n)}}) = C_f^{p^n}$ *e*
2. $(\varphi^n)^*(k(X_{F^{(p^n)}})) = k(X_F)^{p^n}$.

Demonstração: *Uma vez que $k(Z_f)^{p^n}$ é o corpo de frações de $C_f^{p^n}$ e $k(Z_f)^{p^n} \cong k(X_F)^{p^n}$, o item 2 segue de 1. Para provar 1, observe que $\forall g \in k[x,y], (g^{(1/p^n)}(x,y))^{p^n} = g(x^{p^n}, y^{p^n})$. Portanto, toda p^n-ésima potência em C_f é a imagem de $(\varphi^n)^*$ e, vice-versa.* ■

Definiremos agora o morfismo de Frobenius associada a uma curva completa não singular. Sejam k um corpo de característica p e $K|k(x)$ finita. Considere o diagrama

$$\begin{array}{ccccc} K & \stackrel{(\mathrm{Frob}_K)^n}{\longrightarrow} & K^{p^n} \subseteq & K \\ \uparrow & & \uparrow & \uparrow \\ k(x) & \stackrel{(\mathrm{Frob}_{k(x)})^n}{\longrightarrow} & k(x)^{p^n} \subseteq & k(x). \end{array}$$

Quando k é perfeito, $k^{p^n} = k$ e $k(x)^{p^n} = k(x^{p^n})$. Uma vez que $(\mathrm{Frob}_K)^n$ é um isomorfismo e $[k(x) : k(x^{p^n})] = p^n$, segue que $[K : K^{p^n}] = p^n$. Além disso, se k é perfeito, K^{p^n} contém k e a inclusão $K^{p^n} \subseteq K$ é um morfismo de $k-$álgebras.

Definição 8.2.2 *Sejam k um corpo perfeito e $k(X)|k$ o corpo de funções da curva completa não singular X/k. Então $k(X)^{p^n}|k$ é o corpo de funções da curva completa não singular $X^{(p^n)}/k$. A inclusão $k(X)^{p^n} \subseteq k(X)$ define um morfismo de curvas completas sobre k de grau p^n,*

$$\varphi^n : X \longrightarrow X^{(p^n)},$$

*chamado de $n-$*ésimo morfismo de Frobenius *sobre k.*

Para mostrar que $k(X)^{p^n}|k$ é um corpo de funções, note primeiramente que $k(X)^{p^n}$ é uma extensão finita do corpo e funções racionais $k(y)$, onde $y = x^{p^n}$. Se $\alpha \in k(X)^{p^n}$ é algébrico sobre k, então $\alpha \in k$, pois $k(X)^{p^n} \subseteq k(X)$ e $k(X)|k$ é um corpo de funções. Assim, k é algebricamente fechado em $k(X)^{p^n}$.

Proposição 8.2.2 *Seja $\mu : X \to Y$ um morfismo de curvas completas não singulares sobre o corpo perfeito k. Então existe um único $n \in \mathbb{N}$ e um morfismo separável $\psi : X^{(p^n)} \to Y$ tais que $\mu = \psi \circ \varphi^n$.*

Demonstração: *Seja $k(X)|k(Y)$ a extensão de corpos de funções definida pelo morfismo μ. Seja $k(Y) \subseteq L_0 \subseteq k(X)$ a maior extensão separável de $k(Y)$ em $k(X)$. Então $L_0|k$ é um corpo de funções. Como $k(X)|L_0$ é puramente inseparável, a proposição 8.1.2 mostra que $L_0 = k(X)^{p^n}$ para um único $n \geqslant 0$. Portanto, $L_0 = k(X^{(p^n)})$. A extensão $k(X^{(p^n)})|k(Y)$ corresponde ao morfismo separável $\psi : X^{(p^n)} \to Y$.* ■

Diremos que um morfismo de curvas afins $\mu : Z_f(\overline{k}) \to Z_g(\overline{k})$ é *separável* se $\mu^* : \overline{C}_g \to \overline{C}_f$ é injetiva e a extensão de corpos associada $\mu^* : \overline{k}(Z_g) \to \overline{k}(Z_f)$ é separável.

Proposição 8.2.3 *Sejam $Z_f(\overline{k})$ um curva não singular e $\mu : Z_f(\overline{k}) \to Z_g(\overline{k})$ um morfismo não constante de curvas afins. Se μ não é separável, então existem $n \in \mathbb{N}$ e um morfismo separável $\psi : Z_{f^{(p^n)}}(\overline{k}) \to Z_g(\overline{k})$ tais que $\mu = \psi \circ \varphi_{\overline{k}}^n$.*

Demonstração: *Sejam $L = \overline{k}(Z_f)$ e $K = \overline{k}(Z_g)$. Denote por L_0 a maior extensão de K em L separável. Então $L|L_0$ é puramente inseparável de grau p^n, par algum $n \in \mathbb{N}$. Identifique K com um subcorpo de L pela injeção μ^*. A aplicação μ^* também nos permite identificar o anel $\overline{C}_g$ com um subanel de $\overline{C}_f$. Afirmamos que $\overline{C}_g \subseteq (\overline{C}_f)^{p^n}$. De fato, a proposição 8.1.2 mostra que $L_0 = L^{p^n}$. Assim, todo elemento $\alpha \in \overline{C}_g$ tem uma raiz p^n-ésima em L. Seja $\beta \in L$ tal que $\beta^n = \alpha$. Como $\overline{C}_f$ é integralmente fechado (pois $Z_f(\overline{k})$ é não singular) e β é integral sobre $\overline{C}_g$, concluímos que $\beta \in \overline{C}_f$. Assim, $\beta^{p^n} = \alpha \in (\overline{C}_f)^{p^n}$. A aplicação $(\varphi_{\overline{k}}^n)^* : \overline{C}_f^{(p^n)} \to (\overline{C}_f)^{p^n}$, dada por* classe de $h(x,y) \mapsto$ classe de $h(x^{p^n}, y^{p^n})$ *estabelece uma isomorfismo de $\overline{k}-$álgebras entre $\overline{C}_f^{(p^n)}$ e $(\overline{C}_f)^{p^n}$ (8.2.1). A aplicação*

$$\psi^* : \overline{C}_g \hookrightarrow (\overline{C}_f)^{p^n} \overset{((\varphi_{\overline{k}}^n)^*)^{-1}}{\longrightarrow} \overline{C}_{f^{(p^n)}}$$

é um homomorfismo de $\overline{k}-$álgebras e induz um morfismo de curvas $\psi : Z_{f^{(p^n)}}(\overline{k}) \to Z_g(\overline{k})$. Uma vez que $(\overline{C}_f)^{p^n} \subseteq L_0$ e $L_0|K$ é separável, concluímos que o morfismo ψ é um morfismo separável de curvas planas. Por construção $\psi \circ \varphi_{\overline{k}}^n = \mu$. ■

Exemplo 8.2.1 *Sejam $p > 2$ um primo e $f(x,y) = y^{2p} + x^p - x$. A curva $Z_f(\overline{k})$ é não singular. Considere a projeção $p_x : Z_f(\overline{k}) \to \mathbb{A}^1(\overline{k})$, $(a,b) \mapsto a$. Sejam $L = \overline{k}(Z_f)$ e $K = \overline{k}(x)$. A extensão $L|K$ não é separável. De fato, a maior extensão separável L_0 de K em L é isomorfa a $\overline{k}(x)[z]/\langle z^2 + x^p - x\rangle$. Além do mais, $L = L_0(\sqrt[p]{z})$ e $[L : L_0] = p$. A aplicação p_x se fatora como $p_x = \psi \circ \varphi_{\overline{k}}$, onde $\psi : Z_{f^{(p)}}(\overline{k}) \to \mathbb{A}^1(\overline{k})$, aplica $(c,d) \mapsto d^2 + c$.*

8.3 Endomorfismo de Frobenius

Sejam p um primo e $q = p^n$. Nesta seção sempre k seá o corpo finito $\mathbb{F}_q$. Seja X/k uma curva completa não singular sobre k. Pode ser que, para algum $n \in \mathbb{N}$, a curva $X^{(p^n)}/k$ seja isomorfa a curva X/k, dada pelo isomorfismo $\psi : X^{(p^n)} \to X$. Neste caso, $\psi \circ \varphi^{(p^n)}$ é um endomorfismo de X. Veremos nesta seção que, quando $k = \mathbb{F}_q$, a curva $X^{(q)}$ é sempre isomorfa a X através de um isomorfismo natural ψ. O *endomorfismo de Frobenius* definido nesta seção é então a composição $\psi \circ \varphi_{(q)}$. Começaremos definindo o endomorfismo de Frobenius para curvas projetivas planas.

Definição 8.3.1 *Sejam $k = \mathbb{F}_q$ e $H \in k[x_0, x_1, x_2]$ homogêneo e irredutível. Assim, $H^{(p^n)} = H$. O $n-$ésimo endomorfismo de Frobenius é definido por $\varphi^n = \overline{F}r : X_H(\overline{k}) \to X_H(\overline{k})$, $(c_0 : c_1 : c_2) \mapsto (c_0^q : c_1^q : c_2^q)$.*

O próximo lema determina o conjunto dos pontos fixados de $\overline{F}r$.

Lema 8.3.1 *Seja $H \in \mathbb{F}_q[x_0, x_1, x_2]$. Então $X_H(\mathbb{F}_q) = \{P \in X_H(\overline{\mathbb{F}}_q) | \overline{F}r(P) = P\}$.*
Demonstração: *Seja $P = (c_0 : c_1 : c_2) \in X_H(\mathbb{F}_q)$. Então existe $\lambda \in \overline{\mathbb{F}}_q$ tal que $\lambda c_i \in \mathbb{F}_q$, logo, $(\lambda c_i)^q = \lambda c_i$, para todo $i = 0, 1, 2$, ou, $\overline{F}r(P) = P$. Reciprocamente, se $\overline{F}r(P) = P$, então existe $\mu \in \overline{\mathbb{F}}_q$ tal que $\mu c_i^q = c_i$. Se $c_i c_j \neq 0$, então $(\frac{c_i}{c_j})^{q-1} = 1$, e $\frac{c_i}{c_j} \in \mathbb{F}_q$. Portanto, $\mathbb{F}_q(P) = \mathbb{F}_q$.* ■

Seja X/k uma curva completa não singular. Quando $k = \mathbb{F}_q$, o isomorfismo de corpos $(\mathrm{Frob}_{k(X)})^n : k(X) \to k(X)^{p^n}$ é uma isomorfismo como $k-$álgebras também, uma vez que $(\mathrm{Frob}_{k(X)})^n_{|_k} = \mathrm{id}_k$. Segue que $(\mathrm{Frob}_{k(X)})^n$ induz um isomorfismo de curvas não singulares sobre k entre $X^{(p^n)}$ e X. Sua composição com $\overline{F}r$ é endomorfismo da curva completa não singular X, chamado de *endomorfismo de Frobenius*.

Definição 8.3.2 *Sejam $k = \mathbb{F}_q$ e X/k uma curva completa não singular. O $k-$álgebra homomorfismo $\mathrm{Fr}^* : k(X) \to k(X)$, $\alpha \mapsto \alpha^q$ induz um endomorfismo $\mathrm{Fr} : X \to X$ de grau q, chamado de* endomorfismo de Frobenius *de X sobre k.*

O morfismo Fr^* pode ser estendido a $\overline{k}(X)$:

$$\begin{array}{ccc} \overline{\mathrm{Fr}}^* : \overline{k}(X) & \longrightarrow & \overline{k}(X) \\ \sum_{i=1}^s a_i \alpha_i & \longmapsto & \sum_{i=1}^s a_i \alpha_i^q, \end{array}$$

onde $a_i \in \overline{k}$ e $\alpha_i \in k(X)$, para todo $i = 1, \ldots, s$. A aplicação $\overline{\mathrm{Fr}}^*$ induz o morfismo $\overline{\mathrm{Fr}} : X_{\overline{k}} \to X_{\overline{k}}$.

O homomorfismo $\mathrm{F} : \overline{k} \to \overline{k}$, dado por $x \mapsto x^q$ é chamado de *automorfismo de Frobenius* de $\overline{k}$ sobre k. Como $F|_k = id_k$, $F \in \mathrm{Gal}(\overline{k}|k) \cong \mathrm{Gal}(\overline{k}(X)|k(X))$, então F corresponde a uma aplicação $\overline{k}(X) \to k(X)$ novamente denotada por F, dada por

$$\sum_{i=1}^s a_i \alpha_i \longmapsto \sum_{i=1}^s a_i^q \alpha_i.$$

A ação $\mathrm{Gal}(\overline{k}|k)|X_{\overline{k}}$ é dada pela regra $\mathcal{O}_{\sigma(P)} := \sigma(\mathcal{O}_P)$. Em particular, $\mathcal{O}_{\mathrm{F}(P)} := \mathrm{F}(\mathcal{O}_P)$.

Lema 8.3.2 *Seja $X/\mathbb{F}_q$ uma curva completa não singular. Então para todo $P \in X_{\overline{\mathbb{F}}_q}$, $\overline{\mathrm{Fr}}(P) = \mathrm{F}(P)$.*
Demonstração: *Seja $\mathcal{O}_P$ o anel de valorização associado a P. O ponto $\overline{\mathrm{Fr}}(P)$ corresponde ao anel de valorização $(\overline{\mathrm{Fr}}^*)^{-1}(\mathcal{O}_P)$, enquanto $\mathrm{F}(P)$ corresponde ao anel de valorização $\mathrm{F}(\mathcal{O}_P)$. Seja $\sum_{i=1}^s a_i^q \alpha_i \in \mathrm{F}(\mathcal{O}_P)$, $a_i \in \overline{\mathbb{F}}_q$ e $\alpha_i \in \mathbb{F}_q(X)$, para todo $i = 1, \ldots, s$.*

Então $\sum_{i=1}^{s} a_i\alpha_i \in \mathcal{O}_P$ *e* $(\sum_{i=1}^{s} a_i^q\alpha_i)^q \in \mathcal{O}_P$. *Assim,* $\sum_{i=1}^{s} a_i^q\alpha_i \in (\overline{\mathrm{Fr}}^*)^{-1}(\mathcal{O}_P)$. *Suponha agora que* $\sum_{i=1}^{r} b_i\beta_i \in (\mathrm{Fr}^*)^{-1}(\mathcal{O}_P)$, *com* $b_i \in \overline{\mathbb{F}}_q$ *e* $\beta_i \in \mathbb{F}_q(X)$, *para todo* $i = 1, \ldots, r$. *Então* $\sum_{i=1}^{r} b_i\beta_i^q \in \mathcal{O}_P$. *Seja* $c_i \in \overline{\mathbb{F}}_q$ *tal que* $b_i = c_i^q$, *assim* $(\sum_{i=1}^{r} c_i\beta_i)^q \in \mathcal{O}_P$. *Segue que* $\sum_{i=1}^{r} c_i\beta_i \in \mathcal{O}_P$, *portanto* $\sum_{i=1}^{r} b_i\beta_i \in \mathrm{F}(\mathcal{O}_P)$. ■

Observação 8.3.1 *Se* $Q \in X$, *então* $\mathrm{Fr}(Q) = Q$. *De fato, relembre que* $\mathcal{O}_{\mathrm{Fr}(Q)} = (\mathrm{Fr}^*)^{-1}(\mathcal{O}_Q)$. *Seja* $\alpha \in (\mathrm{Fr}^*)^{-1}(\mathcal{O}_Q)$, *então* $\alpha^q \in \mathcal{O}_Q$. *Uma vez que* $\mathcal{O}_Q$ *é integralmente fechado,* $\alpha \in \mathcal{O}_Q$. *Segue que* $\mathcal{O}_{\mathrm{Fr}(Q)} \subseteq \mathcal{O}_Q$. *Agora seja* $\beta \in \mathcal{O}_Q$, *então* $\beta^q \in \mathcal{O}_Q$. *Assim,* $\beta = (\mathrm{Fr}^*)^{-1}(\beta^q) \in (\mathrm{Fr}^*)^{-1}(\mathcal{O}_Q)$. *Então* $\mathcal{O}_{\mathrm{Fr}(Q)} = \mathcal{O}_Q$. *Portanto* $\mathrm{Fr} : X \to X$ *é a identidade sobre os pontos de* X, *mas* Fr^* *não é a identidade sobre as funções em* X.

Por outro lado, o morfismo $\overline{\mathrm{Fr}} : X_{\overline{k}} \to X_{\overline{k}}$ *não é a identidade em* $X_{\overline{k}}$. *Por exemplo, seja* $X/\mathbb{F}_q$ *a curva completa não singular associada a curva projetiva não singular* $X_H(\overline{\mathbb{F}}_q)$ *dada por* $H \in \mathbb{F}_q[x_0, x_1, x_2]$. *Então* $\overline{\mathrm{Fr}} : X_{\overline{\mathbb{F}}_q} \to X_{\overline{\mathbb{F}}_q}$ *corresponde a aplicação que aplica* $(c_0 : c_1 : c_2) \in X_H(\overline{\mathbb{F}}_q)$ *em* $(c_0^q : c_1^q : c_2^q)$.

O próximo lema é análogo ao Lema 8.3.1.

Lema 8.3.3 *Seja* $X/\mathbb{F}_q$ *uma curva completa não singular. Um ponto* $P \in X_{\overline{\mathbb{F}}_q}$ *pertence a* $X(\mathbb{F}_q)$ *se, e somente se,* $\overline{\mathrm{Fr}}(P) = P$.
Demonstração: *Seja* $k = \mathbb{F}_q$. *Por definição* $P \in X(k)$ *se, e só se,* $k(P) := \overline{k}^{\mathrm{Stab}(P)} = k$. *Pela correspondência de Galois,* $\overline{k}^{\mathrm{Stab}(P)} = k$ *se, e só se,* $\mathrm{F} \in \mathrm{Stab}(P)$. *Equivalentemente,* $P \in X(k)$ *se, e só se,* $\mathrm{F}(P) = P$. *Pelo lema 8.3.2,* $\mathrm{F}(P) = P$ *se, e só se,* $\overline{\mathrm{Fr}}(P) = P$. ■

Seja $X/\mathbb{F}_q$ uma curva completa não singular. O morfismo $\overline{\mathrm{Fr}}$ induz uma aplicação natural $\overline{\mathrm{Fr}}^* : \mathrm{Div}(X_{\overline{\mathbb{F}}_q}/\overline{\mathbb{F}}_q) \to \mathrm{Div}(X_{\overline{\mathbb{F}}_q}/\overline{\mathbb{F}}_q)$, chamado de *pull-back*. Relembre que a ação $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)|X_{\overline{\mathbb{F}}_q}$ induz uma ação natural em $\mathrm{Div}(X_{\overline{\mathbb{F}}_q}/\overline{\mathbb{F}}_q)$. Em particular, o automorfismo de Frobenius $\mathrm{F} \in \mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ e sua inversa F^{-1} agem sobre $\mathrm{Div}(X_{\overline{\mathbb{F}}_q}/\overline{\mathbb{F}}_q)$.

Lema 8.3.4 *Sejam* $X/\mathbb{F}_q$ *uma curva completa não singular. Então para todo* $Q \in X_{\overline{\mathbb{F}}_q}$, $\overline{\mathrm{Fr}}^*(Q) = q\mathrm{F}^{-1}(Q)$ *em* $\mathrm{Div}(X_{\overline{\mathbb{F}}_q}/\overline{\mathbb{F}}_q)$.
Demonstração: *Por definição,*

$$\overline{\mathrm{Fr}}^*(Q) = \sum_{\{P|\overline{\mathrm{Fr}}(P)=Q\}} e_{P/Q} \cdot P.$$

Pelo lema 8.3.2, $\overline{\mathrm{Fr}}(P) = \mathrm{F}(P)$, *para todo* $P \in X_{\overline{\mathbb{F}}_q}$. *Como* F *induz uma bijeção em* $X_{\overline{\mathbb{F}}_q}$, *concluímos que* $\{P|\overline{\mathrm{Fr}}(P) = Q\} = \mathrm{F}^{-1}(Q)$. *Considere a aplicação norma induzida por* $\overline{\mathrm{Fr}}$*:*

$$\mathrm{Norm}_{X/X} : \mathrm{Div}(X_{\overline{k}}/\overline{k}) \to \mathrm{Div}(X_{\overline{k}}/\overline{k}).$$

Uma vez que $\mathrm{Norm}_{X/X} \circ \overline{\mathrm{Fr}}^{*}$ *é a multiplicação por* q *(veja 5.9.2), concluímos que*

$$\mathrm{Norm}_{X/X} \circ \overline{\mathrm{Fr}}^{*}(Q) = e_{\mathrm{F}^{-1}(Q)/Q} f_{\mathrm{F}^{-1}(Q)/Q} \cdot Q = q \cdot Q.$$

Como $\overline{\mathbb{F}}_q$ *é algebricamente fechado,* $f_{\mathrm{F}^{-1}(Q)/Q} = 1$. *Portanto,* $e_{\mathrm{F}^{-1}(Q)/Q} = q$. ■

Corolário 8.3.1 *Seja* $f \in \overline{\mathbb{F}}_q(X)^*$. *Então* $\mathrm{div}(\overline{\mathrm{Fr}}^{*}(f)) = q\mathrm{F}^{-1}(\mathrm{div}(f))$.
Demonstração: *Segue de 5.9.1 que* $\mathrm{div}(\overline{\mathrm{Fr}}^{*}(f)) = \overline{\mathrm{Fr}}^{*}(\mathrm{div}(f))$. *Pelo lema 8.3.4,* $\overline{\mathrm{Fr}}^{*}(\mathrm{div}(f)) = q\mathrm{F}^{-1}(\mathrm{div}(f))$. ■

Exemplo 8.3.1 *Seja* $\mathbb{P}^1/\mathbb{F}_q$ *a reta projetiva associada ao corpo de funções* $\mathbb{F}_q(x)|\mathbb{F}_q$. *Identificamos* $\mathbb{P}^1_{\overline{\mathbb{F}}_q}$ *com* $\overline{\mathbb{F}}_q \sqcup \{\infty\}$. *O automorfismo de Frobenius* $\mathrm{F} \in \mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ *age sobre* $\mathbb{P}^1_{\overline{\mathbb{F}}_q}$ *levando um elemento de* $\overline{\mathbb{F}}_q$ *a potência* q *e fixando* ∞. *Seja* $f = ax - b \in \overline{\mathbb{F}}_q(x)$. *Então* $\mathrm{div}(f) = (b/a) - (\infty) \in \mathrm{Div}(\mathbb{P}^1_{\overline{\mathbb{F}}_q}/\overline{\mathbb{F}}_q)$. *Uma vez que* $\overline{\mathrm{Fr}}^{*}(ax - b) = ax^q - b$, *concluímos que*

$$\mathrm{div}(\overline{\mathrm{Fr}}^{*}(f)) = q(\sqrt[q]{b/a} - \infty).$$

Por construção, o divisor $\sqrt[q]{b/a} = \mathrm{F}^{-1}(b/a)$ *e* $(\infty) = \mathrm{F}^{-1}(\infty)$. *Portanto,*

$$\mathrm{div}(\overline{\mathrm{Fr}}^{*}(f)) = q\mathrm{F}^{-1}(\mathrm{div}(f)).$$

8.4 Elemento de Frobenius

Nesta seção, k denotará um corpo perfeito salvo menção contrária.

Definição 8.4.1 *Seja* $\pi : X \to Y$ *um morfismo de curvas completas não singulares sobre um corpo* k. *Se* $k(X)|k(Y)$ *for de Galois, diremos que* π *é uma* cobertura de Galois.

Observação 8.4.1 *Considere* $\pi : X \to Y$ *um morfismo de curvas completas não singulares sobre um corpo* k, *associado à extensão* $k(X)|k(Y)$. *Dado* $\overline{k(Y)}$ *o fecho algébrico de* $k(Y)$, *suponha* $k(X) \subseteq \overline{k(Y)}$. *Seja* $L|k(Y)$ *a menor extensão de Galois de* $k(Y)$ *em* $\overline{k(Y)}$ *que contenha* $k(X)$. *A extensão* $L|k(Y)$ *é chamada* o fecho de Galois *de* $k(X)$ *em* $\overline{k(Y)}$. *Seja* k' *o fecho algébrico de* k *em* L. *Então* $L|k'$ *é um corpo de funções. Seja* Z/k' *a curca completa não singular associada a* $L|k'$. *As inclusões* $k'(Y) \subseteq k'(X) \subseteq k'(Z)$ *induzem duas aplicações de curvas sobre* k'

$$Z \xrightarrow{\delta} X_{k'} \xrightarrow{\pi_{k'}} Y_{k'}.$$

As aplicações δ *e* $\pi_{k'} \circ \delta$ *são ambas coberturas de Galois sobre* k'.

Exemplo 8.4.1 *Sejam $f(x,y) = y^n - g(x) \in k[x,y]$ absolutamente irredutível e X/k a curva completa associada ao corpo de frações $k(X)$ de $k[x,y]/\langle f\rangle$. Vamos supor que k não contenha as $n-$ésimas raízes da unidade. Então a extensão $k(X)|k(x)$ não é de Galois e o morfismo associado $\pi : X \to \mathbb{P}^1$ não é uma cobertura de Galois. Denote por ξ_n um raiz $n-$ésima primitiva da unidade em $\overline{k(X)}$. Seja $k' := k(\xi_n)$. O fecho de Galois de $k(X)$ é o corpo $k'(X)$ e o morfismo $\pi_{k'} : X_{k'} \to \mathbb{P}^1_{k'}$ é uma cobertura de Galois sobre k'.*

Observação 8.4.2 *Seja X/k uma curva completa não singular. Observaremos agora que o quociente de uma curva completa não singular pela ação de um subgrupo finito de $\mathrm{Aut}(X/k)$ é ainda um curva completa não singular. Sejam $\pi : X \to Y$ uma cobertura de Galois de curvas completas não singulares sobre o corpo k e $G = \mathrm{Gal}(k(X)|k(Y))$. Vamos identificar G como um subgrupo de $\mathrm{Aut}(X/k)$:*

- *Para todo $\sigma \in G$ e $P \in X$, seja $\sigma(P)$ o ponto de X correspondente a pré-imagem de $\mathcal{O}_P$ pela aplicação $\sigma^{-1} : k(X) \to k(X)$. Em particular, $\mathcal{O}_{\sigma(P)} = \sigma(\mathcal{O}_P)$. O morfismo de curvas associado a σ^{-1} será denotado por $\sigma : X \to X$. Com essa notação, $\sigma^* := \sigma^{-1}$ (relembre 5.7.1). Deste modo, a ação G induz um homomorfismo de grupos $G \to \mathrm{Aut}(X/k)$. Além disso, a ação $G|X$ induz uma ação de G em $k(X)$.*
- *Para todo $\sigma \in G$ e $f \in k(X)$, seja $f^\sigma := \sigma^{-1}(f)$. Como em 2.7, se f é função em X e σ um automorfismo de X, então f^σ deve ser pensada como a função $f \circ \sigma$.*

Observe que Y pode ser identificada com o conjunto das órbitas X/G. Uma vez que cada elemento $\sigma \in \mathrm{Aut}(X/k)$ pode ser estendido a um elemento $\overline{\sigma} \in \mathrm{Aut}(X_{\overline{k}}/\overline{k})$, o grupo G pode também ser considerado um subgrupo de $\mathrm{Aut}(X_{\overline{k}}/\overline{k})$. Assim, $Y_{\overline{k}}$ pode ser identificada com o conjunto das órbitas $X_{\overline{k}}/G$.

Um caso particular da observação acima é o seguinte teorema:

Teorema 8.4.1 *Sejam X/k uma curva completa não singular e G um subgrupo de $\mathrm{Aut}(X/k)$. Seja $k(Y)$ o corpo invariante pela ação de $G|k(X)$ (i.é, $k(Y) = k(X)^G$). Então $k(Y)|k$ é um corpo de funções. Além disso, se Y/k é a curva completa não singular associada a $k(Y)|k$, o morfismo $\pi : X \to Y$ induzido por $k(Y) \subseteq k(X)$ é uma cobertura de Galois e Y/k pode ser identificado como o quociente de X pela ação de G.*

Vamos assumir que de agora em diante $k = \mathbb{F}_q$. Sejam $\pi : X \to Y$ uma cobertura de Galois de curvas completas não singulares sobre k e G o subgrupo associado de $\mathrm{Aut}(X/k)$. Tome $P \in X$ e $\sigma \in G$. O morfismo $\sigma : X \to X$ induz uma aplicação σ^* do conjunto das

funções definidas em $\sigma(P), \mathcal{O}_{\sigma(P)}$, ao conjunto das funções definidas em $P, \mathcal{O}_P$, dada por: $\sigma^* = \sigma^{-1} : \sigma(\mathcal{O}_P) \to \mathcal{O}_P$. O morfismo σ também induz a aplicação residual

$$\widetilde{\sigma}^* : \frac{\sigma(\mathcal{O}_P)}{\sigma(\mathcal{M}_P)} \longrightarrow \frac{\mathcal{O}_P}{\mathcal{M}_P}.$$

Sejam $D(P) := \{\sigma \in G | \sigma(P) = P\}, Q := \pi(P)$ e $\mathcal{G} = \mathrm{Gal}(\frac{\mathcal{O}_P}{\mathcal{M}_P} | \frac{\mathcal{O}_Q}{\mathcal{M}_Q})$. Note que a aplicação $D(P) \to \mathcal{G}$, dada por $\sigma \mapsto \widetilde{\sigma}^*$, não é um homomorfismo de grupos, uma vez que $(\sigma\tau)^* = \tau^*\sigma^*$. Como $k = \mathbb{F}_q$, o grupo $\mathcal{G}$ tem um gerador canônico: o automorfismo de Frobenius de $\frac{\mathcal{O}_P}{\mathcal{M}_P}$ sobre $\frac{\mathcal{O}_Q}{\mathcal{M}_Q}$ dado por $x \mapsto x^{q^{\deg(Q)}}$. Se P não for ramificado sobre Q, então $D(P) \cong \mathcal{G}$, veja 2.6.1.

Definição 8.4.2 *Com as considerações acima, todo $\sigma \in D(P)$ é chamado de* elemento de Frobenius *em P da cobertura de Galois π, e sua imagem $\widetilde{\sigma}^*$, de automorfismo de Frobenius de $\mathcal{O}_P/\mathcal{M}_P$ sobre $\mathcal{O}_Q/\mathcal{M}_Q$.*

Sejam B o fecho integral de $\mathcal{O}_Q$ em $k(X)$ e $M := \mathcal{M}_P \cap B$. A decomposição do grupo D_M, definida em 2.6.1, é igual a $D(P)$. O homomorfismo de grupos $D(M) \to \mathcal{G}$ definido em 2.6.1 é igual a aplicação $D(P) \to \mathcal{G}$, definida anteriormente, composta com a aplicação $\mathrm{inv} : \mathcal{G} \to \mathcal{G}$, que aplica $\tau \mapsto \tau^{-1}$. Portanto, a substituição de Frobenius, definida em 2.6.1, é a inversa do elemento de Frobenius em P.

Sejam X/k uma curva completa não singular, $\mathrm{Fr} : X \to X$ o endomorfismo de Frobenius e $P \in X$. Relembre que $\mathrm{Fr}(P) = P$ e que $\mathrm{Fr}^* : \mathcal{O}_P \to \mathcal{O}_P$ induz no corpo residual $\frac{\mathcal{O}_P}{\mathcal{M}_P}$, o automorfismo de Frobenius, que leva um elemento a potência q.

Agora seja $\pi : X \to Y$ uma cobertura de Galois com grupo G de curvas completas não singulares sobre k. Sejam $P \in X$ e $\pi(P) = Q$. Suponha P não ramificado sobre Q e $\sigma \in D(P)$ o elemento de Frobenius em P. Por definição, $\sigma(P) = P$ e σ^* induz, no corpo residual $\frac{\mathcal{O}_P}{\mathcal{M}_P}$, o automorfismo de Frobenius de $\frac{\mathcal{O}_P}{\mathcal{M}_P}$ sobre $\frac{\mathcal{O}_Q}{\mathcal{M}_Q}$, isto é, a aplicação que leva um elemento de $\frac{\mathcal{O}_P}{\mathcal{M}_P}$ a potência $|\frac{\mathcal{O}_Q}{\mathcal{M}_Q}|$. Se $\frac{\mathcal{O}_Q}{\mathcal{M}_Q} = k$, então $\sigma(P) = \mathrm{Fr}(P) = P$, e os automorfismos do corpo residual $\frac{\mathcal{O}_P}{\mathcal{M}_P}$ induzidos por σ e Fr são iguais.

Definição 8.4.3 *Estenda cada automorfismo $\sigma \in G$ para um automorfismo $\overline{\sigma}$ de $X_{\overline{\mathbb{F}}_q}$. Sejam $\overline{P} \in X_{\overline{\mathbb{F}}_q}$ e P sua imagem em X sobre a aplicação quociente pela ação de* $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$. *O* elemento de Frobenius *em $\overline{P}$ pela cobertura de Galois π é o automorfismo $\overline{\sigma}$ tal que σ é o elemento de Frobenius em P.*

Observe que $\overline{\sigma}(\overline{P}) = \overline{\mathrm{Fr}}(\overline{P})$. O seguinte lema será útil na prova da hipótese de Riemann para curvas. Sejam $\sigma \in G$ e defina o conjunto $\mathcal{N}_1(X/Y, \sigma)$ por

$$\left\{\overline{P} \in X_{\overline{k}} \mid \ \overline{\pi}(\overline{P}) \in Y(\mathbb{F}_q),\ \overline{P} \text{ não é ramificado sobre } \overline{\pi}(\overline{P}) \ \text{ e } \overline{\sigma} \text{ é o elemento de Frobenius em } \overline{P}\right\}.$$

Como as fibras de $\overline{\pi}$ e $Y(\mathbb{F}_{q^n})$ são conjuntos finitos, concluímos que $\mathcal{N}_1(X/Y,\sigma)$ é finito. Denote por $N_1(X/Y,\sigma)$ a ordem de $\mathcal{N}_1(X/Y,\sigma)$.

Seja $n \in \mathbb{N}$ e denote por $\pi_{\mathbb{F}_{q^n}} : X_{\mathbb{F}_{q^n}} \to Y_{\mathbb{F}_{q^n}}$ o morfismo estendido. Podemos considerar o conjunto $\mathcal{N}_1(X_{\mathbb{F}_{q^n}}/Y_{\mathbb{F}_{q^n}},\sigma)$. Note que o endomorfismo de Frobenius de $X_{\mathbb{F}_{q^n}}/\mathbb{F}_{q^n}$ é igual a $n-$ésima potência do endomorfismo de Frobenius de $X/\mathbb{F}_q$ estendido a $X_{\mathbb{F}_{q^n}}$.

Lema 8.4.1 *Seja $\pi : X \to Y$ uma cobertura de Galois com grupo G de curvas completas não singulares sobre k. Então existe uma constante C tal que, para todo $n \in \mathbb{N}$,*

$$\left| \sum_{\sigma \in G} N_1(X_{\mathbb{F}_{q^n}}/Y_{\mathbb{F}_{q^n}},\sigma) - |G||Y(\mathbb{F}_{q^n})| \right| \leqslant C.$$

Demonstração: *Uma vez que o elemento de Frobenius de um ponto não ramificado é único, os conjuntos $\mathcal{N}_1(X_{\mathbb{F}_{q^n}}/Y_{\mathbb{F}_{q^n}},\sigma), \sigma \in G$, são dois a dois disjuntos. Cada conjunto $\mathcal{N}_1(X_{\mathbb{F}_{q^n}}/Y_{\mathbb{F}_{q^n}},\sigma)$ contém somente pontos não ramificados da cobertura $\pi_{\overline{\mathbb{F}}_q}$. Portanto,*

$$\sum_{\sigma \in G} N_1(X_{\mathbb{F}_{q^n}}/Y_{\mathbb{F}_{q^n}},\sigma) = |G||U_n|,$$

onde U_n denota o subconjunto dos $\mathbb{F}_{q^n}-$pontos racionais no complementar do lugar dos ramos de $\pi_{\overline{\mathbb{F}}_q}$ em $Y(\overline{\mathbb{F}}_q)$. Como o morfismo $\pi_{\overline{\mathbb{F}}_q}$ é separável, seu lugar dos ramos é um conjunto finito, de cardinalidade m independente de n. Basta tomar $C = m|G|$. ■

8.5 Hipóteses de Riemann

Retornaremos nesta seção ao problema de contar os $\mathbb{F}_q-$pontos racionais de uma curva sobre corpos finitos e provaremos o análogo da hipótese de Riemann.

Sejam $X/\mathbb{F}_q$ uma curva completa não singular e $N_n := |X(\mathbb{F}_{q^n})|$. Mostramos em 6.4.1 que

$$\mathbf{Z}(X/\mathbb{F}_q,T) := \exp\left(\sum_{n=1}^{\infty} N_n \frac{T^n}{n}\right) = \frac{\prod_{i=1}^{2g}(1-\omega_i T)}{(1-T)(1-qT)},$$

onde $\omega_1,\ldots,\omega_{2g}$ são inteiros algébricos tais que $\omega_{2g-i} = \frac{q}{\omega_i}$. Assumiremos, sem perda de generalidade que $|\omega_1|_{\mathbb{C}} \leqslant \cdots \leqslant |\omega_{2g}|_{\mathbb{C}}$. Explicamos em 6.3.2 a relação entre a hipótese de Riemann para curvas cobre corpos finitos e a afirmação:

$$|\omega_i|_{\mathbb{C}} = \sqrt{q}, \forall i = 1,\ldots,2g. \tag{8.1}$$

Pela fórmula $N_n = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n$, concluímos que 8.1 implica que

$$|N_n - (q^n + 1)| = |\sum_{i=1}^{2g} \omega_i^n| \leqslant 2g\sqrt{q^n}. \tag{8.2}$$

Lema 8.5.1 *Seja $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ tais que $|\lambda_1| = \cdots = |\lambda_s| = 1$. Então para todo $\epsilon > 0$, existem inteiros $n \gg 0$ tais que $|\lambda_1^n + \cdots + \lambda_s^n| \geqslant s - \epsilon$.*

Em outras palavras, $\lambda_1^n, \ldots, \lambda_s^n$ estão muito perto do número 1.

Lema 8.5.2 *Sejam $\omega_1, \ldots, \omega_s \in \mathbb{C}$, $|\omega_1| \leqslant \cdots \leqslant |\omega_s|$. Então para todo $\epsilon > 0$, existem inteiros $n \gg 0$ tais que $|\omega_1^n + \cdots + \omega_s^n| \geqslant (1 - 2\epsilon)|\omega_s|^n$.*
Demonstração: *Seja $\ell < s$ tal que $|\omega_\ell| < |\omega_{\ell+1}| = \cdots = |\omega_s|$. Pelo lema 8.5.1, existem inteiros $n \gg 0$ tais que*

$$\begin{aligned} |\omega_s^n + \cdots + \omega_1^n| &\geqslant |\omega_s^n + \cdots + \omega_{\ell+1}^n| - |\omega_\ell^n + \cdots + \omega_1^n| \\ &\geqslant |\omega_s|^n(s - \ell - \epsilon) - \ell|\omega_\ell|^n \\ &\geqslant |\omega_s|^n(1 - \epsilon) - |\omega_\ell|^n(s - 1). \end{aligned}$$

Se $n \gg 0$, então $|\omega_\ell|^n(s-1) < \epsilon|\omega_s|^n$, o que termina a demontração. ■

Como veremos agora, a hipótese de Riemann segue de uma afirmação aparentemente mais fraca que 8.2.

Lema 8.5.3 *Se existem constantes C_0, C_1 e um inteiro $d \geqslant 1$ tais que para todo $n \in \mathbb{N}$,*

$$|N_{dn} - (q^{dn} + 1)| = |\sum_{i=1}^{2g} \omega_i^{dn}| \leqslant C_0 + C_1\sqrt{q^{dn}}, \tag{8.3}$$

então vale a hipótese de Riemann 8.1.
Demonstração: *Claramente $C_1 \geqslant 0$. Uma vez que $C_0 + C_1\sqrt{q^{dn}} \leqslant (|C_0| + C_1)\sqrt{q^{dn}}$, podemos assumir que existe uma constante C tal que $|N_{dn} - (q^{dn} + 1)| \leqslant C\sqrt{q^{dn}}$. Pelo lema 8.5.2, para inteiros $n \gg 0$,*

$$C\sqrt{q^{dn}} \geqslant |\omega_{2g}^{dn} + \cdots + \omega_1^{dn}| \geqslant (1 - 2\epsilon)|\omega_{2g}^d|^n.$$

Ou, $\frac{|\omega_{2g}^d|}{\sqrt{q^d}} \leqslant |\frac{C}{1-2\epsilon}|^{1/n}$. Por outro lado, $\lim_{n\to\infty} |\frac{C}{1-2\epsilon}|^{1/n} = 1$, então $|\omega_{2g}| \leqslant \sqrt{q}$. Como $\omega_1 = \frac{q}{\omega_{2g}}$ e $|\omega_1| \leqslant |\omega_{2g}|$, concluímos $|\omega_i| = \sqrt{q}$, para todo $i = 1, \ldots, 2g$. ■

A seguir provaremos que as hipóteses do lema 8.5.3 são sempre verificadas. Primeiro obtermos uma cota superior para N_1 quando $q \gg g$.

Teorema 8.5.1 *Seja $X/\mathbb{F}_q$ uma curva completa não singular com gênero g. Se $q = p^\alpha$, α par e $q > (g+1)^4$, então $N_1 < q + 1 + (2g+1)\sqrt{q}$.*

Demonstração: *Seja $\overline{Q} \in X(\overline{\mathbb{F}}_q)$ um $\mathbb{F}_q-$ponto racional. A órbita de $\overline{Q}$ da ação de $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ é somente o ponto $\overline{Q}$. O ponto $\overline{Q}$ corresponde ao ponto $Q \in X$, com $\frac{\mathcal{O}_Q}{\mathcal{M}_Q} = \mathbb{F}_q$. No que segue, sempre identificaremos um $\mathbb{F}_q-$ponto racional $\overline{Q}$ de X com seu ponto correspondente $Q \in X$. Tome $P \in X$ com $\frac{\mathcal{O}_P}{\mathcal{M}_P} = \mathbb{F}_q$. Observe que se tal ponto não existe, então o teorema já é válido. Nosso objetivo é construir uma função f em $\mathbb{F}_q(X)$ com um único polo em P e com zeros em todos os outros $\mathbb{F}_q-$pontos racionais de X. Tal função f tem portanto um número de zeros limitado inferiormente por uma expressão em termos de $N_1 - 1$. Isto é,*

$$\textit{uma expressão em termos de } (N_1 - 1) \leqslant \#\textit{ polos de } f.$$

Uma escolha cuidadosa de f fornecerá uma cota para o número de polos de f de tal modo que a desigualdade acima seja satisfeita. Seja $H_m := \{f \in \mathbb{F}_q(X) | \mathrm{div}(f) \geq -mP\} = H^0(mP)$. Como mP é efetivo, $H_m \neq \{0\}$. Seja $H_m^{p^\mu} = \{f^{p^\mu} | f \in H_m\}$. Se A e B são subconjuntos de H_m e H_n respectivamente, denote por AB o subespaço de H_{m+n} gerado pelos elementos fh, com $f \in A$ e $h \in B$. É fácil ver que $H_\ell^{p^\mu} H_m^q \subseteq H_{\ell p^\mu + mq}$. Então o número dos polos de $f \in H_\ell^{p^\mu} H_m^q \backslash \{0\}$, é no máximo $\ell p^\mu + mq$. Considere $f = \sum_{i=1}^r w_i s_i^q \in H_\ell^{p^\mu} H_m^q$, $w_i \in H_\ell^{p^\mu}$ e $s_i \in H_m$, para todo $i = 1, \ldots, r$. Suponha que exista $f \neq 0$ tal que

$$\delta(f) := \sum_{i=1}^{r} w_i s_i = 0.$$

Então f se anula em todos os $\mathbb{F}_q-$pontos racionais de X exceto em P. De fato, seja $Q \neq P$ um $\mathbb{F}_q-$ponto racional. Então por definição $|\frac{\mathcal{O}_Q}{\mathcal{M}_Q}| = q$, como $w_i s_i \in \mathcal{O}_Q$, para todo $i = 1, \ldots, r$, então

$$\sum_{i=1}^{r} w_i s_i^q \equiv \sum_{i=1}^{r} w_i s_i = 0 \mod \mathcal{M}_Q.$$

Segue que $f \in \mathcal{M}_Q$ para todo $\mathbb{F}_q-$ponto racional $Q \in X \setminus \{P\}$. Suponha $p^\mu < q$, de modo que toda função em $H_\ell^{p^\mu} H_m^q$ é uma $p^\mu-$ésima potência. Então f tem pelo menos $p^\mu(N_1 - 1)$ zeros. Assim, uma vez que f tem o máximo $\ell p^\mu + mq$ polos, concluímos que $p^\mu(N_1 - 1) \leqslant \ell p^\mu + mq$ ou, equivalentemente,

$$N_1 \leqslant \ell + \frac{mq}{p^\mu} + 1. \tag{8.4}$$

Mostraremos agora que existem ℓ, m e μ tais que exista uma função não nula f com $\delta(f) = 0$. Provado este fato, escolheremos cuidadosamente os inteiros ℓ, m e μ de modo que a desigualdade $N_1 \leqslant q + 1 + (2g+1)\sqrt{q}$ siga imediatamente de 8.4. O grau do ponto

P é 1, assim

$$\dim_{\mathbb{F}_q}(H_{m+1}) \leqslant \dim_{\mathbb{F}_q}(H_m) + 1.$$

Então podemos tomar uma base $\{s_1, \ldots, s_r\}$ para o $\mathbb{F}_q-$espaço vetorial H_m tal que

$$\mathrm{ord}_P(s_i) \geqslant \mathrm{ord}_P(s_{i-1}) + 1, \forall i = 2, \ldots, r$$

(considere a base associada as inclusões $H_0 \subseteq H_1 \subseteq \cdots H_m$ e inverta a numeração). Como $p^\mu < q$, $H_m^{p^\mu}$ é um $\mathbb{F}_q-$espaço vetorial. É fácil ver que $\{s_1^{p^\mu}, \ldots, s_r^{p^\mu}\}$ é uma base para $H_m^{p^\mu}$. Considere a aplicação

$$\begin{array}{rcl} \delta : H_\ell^{p^\mu} H_m^q & \longrightarrow & H_\ell^{p^\mu} H_m \\ f = \sum_{i=1}^r w_i s_i^q & \longmapsto & \sum_{i=1}^r w_i s_i. \end{array}$$

Para mostrar que δ está bem definida é suficiente mostrar que existe uma única maneira de escrever $f \in H_\ell^{p^\mu} H_m^q$ como uma soma $\sum_{i=1}^r w_i s_i^q$ com $w_i \in H_\ell^{p^\mu}$, para todo $i = 1, \ldots, r$. Provaremos este fato supondo que $\ell p^\mu < q$. Assuma que $\rho \in \{1, \ldots, r\}$ tal que $w_\rho \neq 0$ e $\sum_{i=\rho}^r w_i s_i^q = 0$. Então

$$\begin{array}{rcl} \mathrm{ord}_P(w_\rho s_\rho^q) & = & \mathrm{ord}_P(-\sum_{i=\rho+1}^r w_i s_i^q) \\ & \geqslant & \min\limits_{i>\rho}\{\mathrm{ord}_P(w_i s_i^q)\} \\ & \geqslant & -\ell p^\mu + q\mathrm{ord}_P(s_{\rho+1}), \end{array}$$

pois $w_i \in H_\ell^{p^\mu}$ e $\mathrm{ord}_P(s_{\rho+1}) \leqslant \mathrm{ord}_P(s_i)$ se $i \geqslant \rho + 1$. Assim,

$$\begin{array}{rcl} \mathrm{ord}_P(w_\rho) & \geqslant & -\ell p^\mu + q[\mathrm{ord}_P(s_{\rho+1}) - \mathrm{ord}_P(s_\rho)] \\ & \geqslant & -\ell p^\mu + q > 0. \end{array}$$

Então w_ρ tem um zero e um polo em P e $w_\rho = 0$, contradizendo nossa afirmação. Assim a aplicação δ está bem definida. É fácil ver que δ é um homomorfismo de $\mathbb{F}_q-$espaços vetoriais. Note que o fato de qualquer $f \in H_\ell^{p^\mu} H_m^q$ poder ser escrito unicamente da forma $f = \sum_{i=1}^r w_i s_i^q$ para alguns $w_i \in H_\ell^{p^\mu}$ (quando $\ell p^\mu < q$) mostra que

$$\dim_{\mathbb{F}_q}(H_\ell^{p^\mu} H_m^q) = \dim_{\mathbb{F}_q}(H_\ell^{p^\mu}) \cdot \dim_{\mathbb{F}_q}(H_m^q).$$

De $H_\ell^{p^\mu} H_m^q \subseteq H_{\ell p^\mu + m}$, concluímos que

$$\dim \ker(\delta) \geqslant \dim H_\ell^{p^\mu} \cdot \dim H_m^q - \dim H_{\ell p^\mu + m}. \tag{8.5}$$

Pelo teorema de Riemann-Roch $\dim H_\ell^{p^\mu} = \dim H_\ell \geqslant \max(1, \ell + 1 - g)$. Analogamente, $\dim H_m^q \geqslant \max(1, m + 1 - g)$. Se $\ell, m \geqslant g$, então $\ell p^\mu + m \geqslant 2g - 1$ e pelo teorema de

Riemann-Roch $\dim H_{\ell p^\mu+m} = \ell p^\mu + m + 1 - g$. *Neste caso, pela desigualdade 8.5,*

$$\dim \ker(\delta) \geqslant (\ell + 1 - g)(m + 1 - g) - (\ell p^\mu + m + 1 - g). \tag{8.6}$$

Tome $\mu = \frac{\alpha}{2}$ *e* $m = \sqrt{q} + 2g$, *claramente* $m \geqslant g$. *Com essas escolhas para* μ *e* m, *8.6 mostra que* $\ker(\delta) \neq \{0\}$ *se* $\ell > g + g\sqrt{q}/(g+1)$. *Com tal* ℓ, *a desigualdade* $\ell \geqslant g$ *é satisfeita. Uma vez que também queremos* $\ell p^\mu < q$, *ou, equivalentemente,* $\ell < \sqrt{q}$, *precisamos encontrar um inteiro* ℓ *com*

$$g + \frac{g\sqrt{q}}{g+1} < \ell < \sqrt{q}.$$

Tal inteiro ℓ *existe se, e só se,* $g + \frac{g\sqrt{q}}{g+1} + 1 < \sqrt{q}$, *ou, equivalente, se* $(g+1)^2 < \sqrt{q}$. *Pelas hipóteses, esta desigualdade é satisfeita. Tome* $\ell \in \mathbb{N}$ *tal que* $g + \frac{g\sqrt{q}}{g+1} < \ell < \sqrt{q}$. *Então de 8.4, concluímos que*

$$N_1 \leqslant \ell + \frac{mq}{p^\mu} + 1 < \sqrt{q} + (\sqrt{q} + 2g)\sqrt{q} + 1 = q + 1 + \sqrt{q}(2g+1).$$

■

Daremos agora uma cota inferior para o inteiro N_n associado a curva X/k, onde $k = \mathbb{F}_q$. Seja $\pi : X \to Y$ uma cobertura de Galois sobre k. Considere o grupo $G := \mathrm{Gal}(k(X)|k(Y))$ como o grupo dos automorfismo de X sobre k. Dado $\sigma \in G$, relembre de $\mathcal{N}_1(X/Y, \sigma)$ definido em 8.4.3). Denote por $N_1(X/Y, \sigma)$ a ordem do conjunto $\mathcal{N}_1(X/Y, \sigma)$. O passo importante para prova da cota inferior do número de $\mathbb{F}_q-$pontos racionais de uma curva é a seguinte variação do teorema 8.5.1.

Teorema 8.5.2 *Sejam* $\pi : X \to Y$ *uma cobertura de Galois sobre* $\mathbb{F}_q$ *e* G *o subgrupo de* $\mathrm{Aut}(X/k)$ *associado. Tome* $\sigma \in G$ *e denote por* g *o gênero de* X. *Suponha* $q = p^\alpha$, α *par e* $q > (g+1)^4$. *Então* $N_1(X/Y, \sigma) \leqslant q + 1 + (2g+1)\sqrt{q}$.

Demonstração: *A prova deste teorema é igual à prova do teorema 8.5.1. Por isso apenas indicaremos as mudanças necessárias. Seja* $\overline{P} \in X_{\overline{k}} \cap \mathcal{N}_1(X/Y, \sigma)$. *Se tal ponto não existe, então o resultado já é válido. Por definição,* $\overline{\sigma}(\overline{P}) = \overline{\mathrm{Fr}}(\overline{P})$. *Considere o endomorfismo* $\psi := \sigma^{-1} \circ \mathrm{Fr}$ *de* X. *Claramente* $\mathcal{N}_1(X/Y, \sigma)$ *está contido no conjunto dos elementos de* $X_{\overline{k}}$ *fixados por* $\overline{\psi}$.

Considere os seguintes espaços de funções em $X_{\overline{k}}/\overline{k}$, $H_m := H^0(m\overline{P})$ *e* $H_m^{p^\mu} := \{f^{p^\mu} | f \in H_m\}$. *Por construção, qualquer função não constante em* $\overline{\psi}^*(H_m)$ *tem um polo em* $\overline{P}$. *O corolário 8.3.1 mostra que, de fato,* $\overline{\psi}^*(H_m) \subseteq H_{qm}$, *de modo que um função não constante*

em $\overline{\psi}^*(H_m)$ *tem um polo somente em* $\overline{P}$. *Sejam* $f = \sum_{i=1}^r w_i\overline{\psi}^*(s_i) \in H_\ell^{p^\mu}\overline{\psi}^*(H_m)$ *e*

$$\delta_\sigma(f) := \sum_{i=1}^r w_i s_i \in H_\ell^{p^\mu} H_m.$$

Se existe $f \in H_\ell^{p^\mu}\overline{\psi}^*(H_m) \setminus \{0\}$ *tal que* $\delta_\sigma(f) = 0$, *então* f *se anula em todos os pontos* $\overline{Q} \in \mathcal{N}_1(X/Y,\sigma) \setminus \{\overline{P}\}$. *De fato,* $w_i, \overline{\psi}^*(s_i) \in \mathcal{O}_{\overline{Q}}$, *para todo* $\overline{Q} \in \mathcal{N}_1(X/Y,\sigma) \setminus \{\overline{P}\}$ *e todo* $i = 1, \ldots, r$. *Pela definição do elemento de Frobenius,* $\overline{\psi}^*(s_i) \equiv s_i \mathrm{mod}\mathcal{M}_{\overline{Q}}$.

Como $\deg \overline{P} = 1$, H_m *possui uma base* $\{s_1, \ldots, s_r\}$ *tal que*

$$\mathrm{ord}_{\overline{P}}(s_i) \geqslant \mathrm{ord}_{\overline{P}}(s_{i-1}) + 1, \forall i = 2, \ldots, r.$$

Uma vez que $\overline{\psi}^*$ *é uma bijeção de* $\overline{k}-$*álgebras, é fácil ver que* $\{\overline{\psi}^*(s_1), \ldots, \overline{\psi}^*(s_r)\}$ *é uma base para* $\overline{\psi}^*(H_m)$. *Procedendo como na prova do teorema 8.5.1 podemos mostrar:*

$$\delta_\sigma : H_\ell^{p^\mu}\overline{\psi}^*(H_m) \longrightarrow H_\ell^{p^\mu} H_m$$

está bem definida e é um homomorfismo de $\overline{k}-$*espaços vetoriais. E ainda, que existem inteiros* ℓ, m, μ *tais que* $\ker(\delta_\sigma) \neq \{0\}$. *E isso conclui a prova do teorema.* ■

Usaremos agora o teorema 8.5.2 para provar a existência de cota inferior para $N_1 = |X(\mathbb{F}_q)|$. Seja $X/\mathbb{F}_q$ uma curva. Escolha um morfismo separável $X \to \mathbb{P}^1$ (como no corolário 8.1.2). É claro que para provar a afirmação 8.3 $X/\mathbb{F}_q$, é suficiente basta prová-lo para $X_{\mathbb{F}_{q^e}}/\mathbb{F}_{q^e}$ para algum $e \geqslant 1$. Tendo em vista esta observação, podemos assumir, depois de tomar uma extensão do corpo de base se necessário, que existem uma cobertura de Galois $\pi : Z \to X$ de curvas completas não singulares sobre $\mathbb{F}_q$ e um morfismo separável $v : X \to \mathbb{P}^1$ sobre $\mathbb{F}_q$, tais que $v \circ \pi$ é uma cobertura de Galois de $\mathbb{P}^1$ e $\mathbb{F}_q(Z)$ é o fecho de Galois de $\mathbb{F}_q(X)$ em $\overline{\mathbb{F}_q(\mathbb{P}^1)}$ (como em 8.4.1). Sejam $G := \mathrm{Gal}(\mathbb{F}_q(Z)|\mathbb{F}_q(\mathbb{P}^1))$ e $H := \mathrm{Gal}(\mathbb{F}_q(Z)|\mathbb{F}_q(X))$. Podemos assumir também, depois de mais uma possível extensão de corpos, que q é um quadrado e $q > (g+1)^4$.

Aplicando o lema 8.4.1 para a cobertura de Galois $Z \to \mathbb{P}^1$, obtemos

$$\left| \sum_{\sigma \in G} N_1(Z/\mathbb{P}^1, \sigma) - |G||\mathbb{P}^1(\mathbb{F}_q)| \right| \leqslant C(Z/\mathbb{P}^1). \tag{8.7}$$

Aplicando o teorema 8.5.2 para a cobertura de Galois $Z \to \mathbb{P}^1$,

$$N_1(Z/\mathbb{P}^1, \sigma) \leqslant q + 1 + (2g(Z) + 1)\sqrt{q}. \tag{8.8}$$

Segue de 8.7 que

$$N_1(Z/\mathbb{P}^1,\sigma)-(q+1)+\sum_{\tau\neq\sigma}[N_1(Z/\mathbb{P}^1,\tau)-(q+1)]\geqslant -C(Z/\mathbb{P}^1). \tag{8.9}$$

Concluímos de 8.8 e 8.9 que

$$\begin{array}{rcc} |N_1(Z/\mathbb{P}^1,\sigma)-(q+1)| & \geqslant & -C(Z/\mathbb{P}^1)-(|G|-1)(2g(Z)+1)\sqrt{q} \\ & = & C_1+C_2\sqrt{q}, \end{array} \tag{8.10}$$

onde C_1 e C_2 são constantes que não dependem do corpo de base. Aplicado a cobertura de Galois $Z\to X$, o lema 8.4.1 mostra que

$$\left|\sum_{\sigma\in H}N_1(Z/X,\sigma)-|H||X(\mathbb{F}_q)|\right|\leqslant C(Z/X). \tag{8.11}$$

Lema 8.5.4 *Seja $\sigma\in H$. Então $\mathcal{N}_1(Z/\mathbb{P}^1,\sigma)\subseteq\mathcal{N}_1(Z/X,\sigma)$.*
Demonstração: *Sejam $\overline{P}\in\mathcal{N}_1(Z/\mathbb{P}^1,\sigma)$ e P o correspondente em Z. Por definição, P é não ramificado sobre $\mathbb{P}^1$ e assim, não ramificado sobre X. O automorfismo σ é o elemento de Frobenius em P para o morfismo $\sqsubseteq\circ\pi: Z\to\mathbb{P}^1$ de modo que, o grupo de decomposição $D(P)$ do morfismo $\sqsubseteq\circ\pi$ é gerado por σ. Uma vez que $D(P)\subseteq H$, é fácil ver que $D(P)$ é também o grupo de decomposição em P para a cobertura de Galois Z/X. Por construção,*

$$k(\mathbb{P}^1)\subseteq k(Z)^H=k(X)\subseteq k(Z)^{D(P)}\subseteq k(Z).$$

Sejam $Q:=(\sqsubseteq\circ\pi)(P)$ e $Q'=\pi(P)$. Como $k(X)\subseteq k(Z)^{D(P)}$, $f_{Q'/Q}=1=e_{Q'/Q}$ (2.6.2). Uma vez que Q é um $\mathbb{F}_q-$ponto racional (isto é, $\mathcal{O}_Q/\mathcal{M}_Q=\mathbb{F}_q$) e $f_{Q'/Q}=1$, concluímos que Q' é um $\mathbb{F}_q-$ponto racional de X. ■

Segue do lema 8.5.4, 8.10 e 8.11 que

$$|X(\mathbb{F}_q)|\geqslant -C(Z/X)/|H|+\sum_{\sigma\in H}N_1(Z/X,\sigma)/|H|\geqslant (q+1)+C_3+C_4\sqrt{q}.$$

Assim, uma vez que as constantes C_3 e C_4 são independentes do corpo de definição de $\pi_{\overline{\mathbb{F}}_q}$, concluímos, para todo $n\in\mathbb{N}$,

$$N_n-(q^n+1)\geqslant C_3+C_4\sqrt{q^n}. \tag{8.12}$$

Finalmente, o teorema 8.5.1 combinado com 8.12, implicam que as hipóteses do lema 8.5.3 são sempre válidas. Portanto, a hipótese de Riemann (8.1) vale.

Referências Bibliográficas

[1] Lang S.; **Algebra** (terceira edição revisada). Springer, 2002.

[2] Lang S.; **Algebraic Number Theory**. Springer-Verlag, 1986.

[3] Marcus D. A.; **Number Fields**. Springer-Verlag, New York, 1977.

[4] Anderson D.; Dobbs D.; **Zero-dimensional commutative rings**. Marcel Dekker, 1995.

[5] Hefez A.; **Introdução a Geometria Projetiva**, X Escola de Álgebra. IMPA, 1990.

[6] Lorenzini, D.; **An Invitation to Arithmetic Geometry**, Graduate Texts in Mathematics, Vol. 9, American Mathematical Society (1996).

[7] Ribenboim, P.; **Algebraic numbes**, Wiley-Interscience, 1972.

[8] Morandi, P.; **Field and Galois Theory**, Graduate Texts in Mathematics, Springer 1996.

[9] Samuel, P.; **Algebraic Theory of Numbers**, Publishers in Arts and Science, Paris, France 1967.

[10] Zariski, O.; Samuel P.; **Comutative Algebra**, vol I, Springer, Verlag, 1975.

[11] Atiyah, M. F; Macdonald L. G.; **Introduction to Commutative Algebra**, Addison-Wesley Publishing Company, 1969.

[12] Eisenbud, D; **Commutative Algebra with a View Toward Algebraic Geometry**, Springer, 1995.

Índice Remissivo