UNIVERSIDADE FEDERAL DE PERNAMBUCO

Centro de Ciências Exatas e da Natureza

Departamento de Matemática

Mestrado em Matemática

ARITMÉTICA DAS CURVAS ALGÉBRICAS

Rodrigo José Gondim Neves

DISSERTAÇÃO DE MESTRADO

Recife

15 de Fevereiro de 2006

UNIVERSIDADE FEDERAL DE PERNAMBUCO
Centro de Ciências Exatas e da Natureza
Departamento de Matemática

Rodrigo José Gondim Neves

ARITMÉTICA DAS CURVAS ALGÉBRICAS

Trabalho apresentado ao Programa de Mestrado em Matemática do Departamento de Matemática da UNIVERSIDADE FEDERAL DE PERNAMBUCO como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: *Prof. Francesco Russo*

Recife
15 de Fevereiro de 2006

Catalogação na fonte
Bibliotecária Jane Souto Maior, CRB4-571

Gondim, Rodrigo
Aritmética das curvas algébricas / Rodrigo Gondim - Recife: O Autor, 2006.
xiii, 95 p.

Orientador: Francesco Russo.
Dissertação (mestrado) - Universidade Federal de Pernambuco. CCEN, Matemática, 2006.

Inclui bibliografia.

1. Álgebra. 2. Geometria algébrica. 3. Geometria aritmética. I. Russo, Francesco (orientador). II. Título.

512 CDD (22. ed.) MEI2011 – 140

Tese submetida ao Corpo Docente do Programa de Pós-graduação do Departamento de Matemática da Universidade Federal de Pernambuco como parte dos requisitos necessários para a obtenção do Grau de Mestrado em Ciências.

Aprovado: _____

Francesco Russo, DMAT-UFPE
Orientador

_____

Aron Simis , DMAT-UFPE

_____

Amílcar Pacheco, IM -UFRJ

ARITMÉTICA DAS CURVAS ALGÉBRICAS

Por
Rodrigo José Gondim Neves

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
DEPARTAMENTO DE MATEMÁTICA
Cidade Universitária – Tels. (081) 2126 - 8414 – Fax: (081) 2126 - 8410
RECIFE – BRASIL

Fevereiro - 2006

À minha família, namorada, mestres e amigos.

AGRADECIMENTOS

À minha família, Ijefisson (Pai), Maria de Fátima (Mãe), Ciro e Ana Lídia (irmãos).
À minha namorada, Giovana.
À meus familiares em geral.
À meus mestres e incentivadores, Tia Jaqueline (primário), Marcos Miguel (ginásio), Aécio, Consulim, Efraim, Folhadela, Herbetes, Jorge, Luiz Antônio, Luiz Carlos, Marcelo, Malba e Mirta (segundo grau) Tânia, Faleiros (ITA), Airton Castro, Antônio Carlos, Aron Simis, César Castilho, Claudio Cuevas, Caudio Vidal, Cleide Martins, Eduardo Leandro, Francesco Russo(Orientador), Francisco Brito, Henrique, Hidelberto Cabral, Manoel Lemos, Marcus Vinícius, Maria Luiza, Pablo B.Silva, Paulo Santiago, Pedro Ontaneda, Ramon Mendoza, Sérgio Santa Cruz, Sílvio Melo, Sóstenes Lins(UFPE).
À meus amigos, Bilife, Gop, Suva, Tite(Infância), David, Juliana, Karen, Marcelo (Macedônia), Carol, Esdras, Fábio, Gildrei, Marcelo, Maria Clara, Marquinhos, Morgana, Patrícia, Rodrigo, Tulia, Thiago, todos os amigos do (IPSEP), Daniel, Marcio, Tiago, Rodrigos, Luana, Sílvia, Patrícia, Ivan, Paula, Severo, Kessie, Julili, Kolontai, a todos os amigos da (ETFPE), Audir, Érico, Gabriel, Guedes, Kohwalter, Laurent, Macarrão, Márcio, Mariana, Milton, Natália, Pipoca, Rei, Simas, Thaís, Violeta, Yuri, todos os amigos do (ITA), Adrianos, Alberto, Ana Cristina, Anete, Antônio, Audi, Bebê, Carla, Claudio, Cleto, Darlan, Éder, Eudes, Evaneide, Fábio, Felipe, Flávio, Formiga, Fred, Gabriel, Gersonilo, Giovana, Hélio, Henrique, Hugo, Humberto, Kalasas, Letícia, Lúcia, Mardônio, Marta, Mulambo, Naldson, Paulo, Rafael, Renato, Ricardo, Severo, Simas, Tiago, Vovô, Walison, a todos os amigos da (UFPE) Catherina, Cleber, DJ, Edson(Babau), Fábio(Piauí), Jaime, Roberto Cahu, Lira, a todos os amigos de (Boa Viagem)
À tia Geruza, pela preciosa revisão ortográfica.
À meus alunos.
À todos que esqueci de mencionar nome, desculpem-me.
Ao CNPQ.

Esqueci de falar,
de viver e sonhar
todas as palavras de amor
que eu não conheceria.

Até tentei sabotar,
destruir e extirpar
as muitas formas anarquistas de governo
que não existiam.

Não lembrei de explorar,
entender, decifrar
os infinitos mistérios do universo
que já se sabiam.

Preferi aceitar,
e assim assimilar
mitos e superstições
que não me interferiam.

—AUTOR DESCONHECIDO (Somente estas)

RESUMO

Esta dissertação tem como principal objetivo expor o bem sucedido projeto de entender a aritmética das curvas algébricas a partir de sua geometria. Estaremos interessados em características qualitativas do conjunto dos pontos K-racionais (K corpo de números) da curva tais como existência, finitude e estrutura algébrica.
Para curvas de gênero zero, mostramos o principio local-global (para quádricas) que garante a existência de um ponto em K baseado na existência de pontos em todos os completamentos de K.
Para curvas de gênero um que possuem um ponto K-racional, o método da tangente e da secante fornece ao conjunto dos pontos K-racionais da curva uma estrutura algébrico-geométrica de grupo abeliano, o principal resultado é o teorema de Mordell-Weil que garante que tal grupo é finitamente gerado, mostraremos mais geralmente o teorema de Mordell-Weil para variedades abelianas.
A última classe de curvas que iremos considerar são as curvas de gênero maior ou igual a dois, para tais curvas o conjunto dos pontos K-racionais é sempre finito. Este é o teorema de Faltings (que não daremos uma demonstração completa).

palavras-chave: Equações Diofantinas, Geometria Aritmética, Princípio local-global, Teorema de Mordel-Weil, Teorema de Faltings.

ABSTRACT

The main goal of this dissertation show the well done project of understand the arithmetic of algebraic curves from its geometry, "Geometry determines Arithmetic". We will be interested in qualitative characteristics of the set of K-rational points of the curve (K denotes a number field). The most important of this characteristics is the emptiness, the finitude and the algebraic structure if there is.
For curves of genus zero we will show the local-global principle (in general for quadrics) witch guarantee the existence ok a K-rational point if there exists points in all the local fields, completations of K.
For curves of genus one witch posses one K-rational point, the tangent and secant argument of Fermat provides to the set of K-rational points an algebraic and geometric structure of abelian group, the most important result in this setting is the Theorem of Mordell-Weil proving that this group is finitely generated, in general we will proof the Mrdell-Weil theorem to abelian varieties.
The last class of curves considered was the curves of genus grater than or equal to two, for this class the set of K-rational point is finite. This is Faltings Theorem (witch we will not proof completely).

keywords: Diophantine Equations , Arithmetic Geometry, Local-global principle, Mordel-Weil Theorem, Faltings Theorem.

SUMÁRIO

INTRODUÇÃO

Chamamos equação diofantina uma equação (ou sistema de equações) polinomial em mais de uma variável a coeficientes inteiros ou racionais na qual se buscam soluções inteiras e/ou racionais. A história das equações diofantinas é milenar e seu nome é uma homenagem ao matemático grego Diofanto, que resolveu alguns problemas desse tipo no tratado *Aritmetica*. É natural, entretanto, tentar generalizar esse estudo para corpos de números, isto é, extenções finitas dos racionais. Existe uma semelhança entre tais corpos, mas também uma dificuldade técnica adicional devida ao fato de que, em geral, o anel de inteiros de corpos de números não é domínio de fatorização única .

Vamos, durante toda a dissertação, interpretar o conjunto-solução de uma equação, ou de um sistema, como uma variedade algébrica. As principais questões a serem respondidas sobre problemas diofantinos são de origem qualitativa, uma vez que, em geral, não é possível encontrar explicitamente o conjunto-solução de modo efetivo. Vamos enunciar, agora, as principais questões a serem respondidas:

(i) Existência de pontos K-racionais, isto é, soluções em K da equação (ou sistema);

(ii) Finitude do conjunto dos pontos K-racionais;

(iii) Estrutura do conjunto dos pontos K-racionais.

As perguntas correspondentes para pontos inteiros (no caso afim) usam, em geral, técnicas de aproximação diofantina e da teoria de classes e não serão expostas. Vamos tratar, principalmente, de curvas.

As primeiras equações diofantinas a serem consideradas são as de graus um e grau dois, em duas variáveis. Essas equações foram resolvidas (parcialmente) pelo próprio Diofanto. Na linguagem geométrica, tais equações representam curvas de

gênero zero. Uma curva lisa projetiva sobre um corpo perfeito K e de gênero zero é K-isomorfa a uma curva plana, dada por uma equação de grau doi, com coeficientes em K, i.e. a uma cônica. Portanto, uma tal curva é isomorfa a $\mathbb{P}^1_K$ se e somente se tem um ponto K-racional. No capítulo intitulado O Princípio Local-Global para quádricas, damos uma caracterização para a existência de pontos K-racionais para quádricas de $\mathbb{P}^n_K$, $n \geq 2$ em que K é um corpo de números. O teorema principal, devido a Hasse-Minkowski, teorema 2.5.4, garante a existência de um ponto em K (global), baseado na hipótese da existência de pontos em todos os completamentos (locais) de K, com respeito a todos os possíveis valores absolutos em K. As técnicas utilizadas para a demonstração desse resultado são, essecialmente, aritméticas e introduzidas na primeira parte do capítulo.

Seguindo a ordem de dificuldade natural, o passo seguinte é considerar as curvas lisas e projetivas sobre um corpo perfeito K, de gênero 1. Se tais curvas admitem um ponto K-racional, podem ser naturalmente identificadas com cúbicas planas dadas por particulares equações (de grau 3) com coeficientes em K. As curvas lisas e projetivas sobre K de gênero 1, que admitem um ponto K-racional, se dizem curvas elípticas. Para as cúbicas planas, o método da secante e da tangente, um antigo procedimento para encontrar novos pontos racionais, a partir de pontos conhecidos, fora exaustivamente utilizado por Fermat e deu origem à consagrada lei de grupo geométrica nas curvas elípticas. Dedicamos um capítulo às curvas de gênero um, no qual damos ainda um critério para a existência de pontos K-racionais. Os pontos K-racionais de uma curva elíptica, definida sobre um corpo de números K, têm uma estrutura de grupo abeliano finitamente gerado. Tal resultado será demonstrado em toda sua generalidade no capítulo intitulado Teorema de Mordell-Weil, em que mostraremos o resultado para variedades abelianas definidas sobre um corpo de números. Os capítulos Variedades Abelianas e Teoria das Alturas são técnicos e têm como principal objetivo fornecer os pré-requisitos (geométricos e aritméticos) necessários para a demonstração do teorema de Mordell-Weil. O teorema de Mordell-Weil, 6.3.1, nos dá uma estrutura para o conjunto dos pontos K-racionais e leva a questão de finitude ao estudo do posto de um grupo abeliano finitamente gerado. O problema do posto, entretanto, está em aberto e é conhecido como Conjectura de Birch e Swinnerton–Dyer.

Se levarmos em conta a classificação geométrica das curvas, seria natural, agora, considerar o problema para curvas de gênero maior ou igual a dois. Do ponto de vista aritmético, a curva geral de gênero $g \geq 2$, sobre um corpo de números K,

representa uma equação diofantina extremamente complicada, de modo que os resultados gerais sobre tais curvas são complexos raros e pouco conhecidos. É suficiente observar que o Último Teorema de Fermat, demonstrado recentemente por Wiles, [Wi], garante que as curvas projetivas planas e lisas de equações $X^n + Y^n = Z^n$, $n \geq 3$, de gênero $\frac{1}{2}(n-1)(n-2) \geq 1$ têm somente soluções racionais (ou equivalentemente inteiras) triviais, i.e., com uma das coordenadas nula. Em 1922, Mordell conjecturou em [Mor] que curvas lisas, projetivas sobre um corpo de numeros K e de gênero, $g \geq 2$, têm somente um número finito de pontos K-racionais. Esse resultado foi provado em 1982, por Faltings, em [Fa], e se destaca como uma das maiores conquistas da Matemática do século passado. Infelizmente, devido às dificuldades técnicas e à insuficiênca de espaço, não será possível dar uma demonstração completa do Teorema de Faltings, 7.0.2. Vamos dar uma idéia sobre duas das principais técnicas utilizadas para demonstrar este resultado. Existem várias conjecturas e teoremas importantes que de alguma forma, se relacionam com o teorema de Faltings, como descreveremos na última seção deste trabalho.

CAPÍTULO 1

DEFINIÇÕES E PRELIMINARES

O objetivo desta dissertação é explicar alguns entre os principais resultados sobre a aritmética das curvas algébricas. Neste capítulo, vamos estabelecer notações, introduzir varias definições e lembrar varias noções básicas de geometria das curvas algébricas e de teoria algebrica dos numeros, utilizados em seguida. Todos os corpos considerados são assumidos perfeitos.

1.1 CURVAS

1.1.1 Pontos K-racionais e modelos

Definição 1.1.1 *Sejam K um corpo, X um K-esquema e R uma K-algebra. O conjunto dos pontos R-racionais de X é o conjunto* $\mathrm{Mor}_K(\mathrm{Spec}(R), X)$*, que será denotado por $X(R)$. A extensão de base de X por R é o R-esquema $X \times_{\mathrm{Spec}(K)}$* $\mathrm{Spec}(R)$*, que será denotado por X_R.*

Devido a nossas aplicações, estaremos interessados exclusivamente em esquemas de tipo finito sobre K. Neste caso, quando $R = L$ é um corpo, existe uma identificação natural entre $X(L)$ e o conjunto dos pontos fechados $P \in X$ tais que $K(P) \subseteq L$, que numa vizinhança afim correspondem com soluções em K da equação (ou sistema) que gera o ideal.

Definição 1.1.2 *Uma variedade X sobre um corpo K é um K-esquema de tipo finito, integral, separado e tal que K seja algebricamente fechado em $K(X)$. Nestas condições, $X_{\bar{K}}$ é uma variedade sobre $\bar{K}$. Uma curva é uma variedade de dimensão 1, definida sobre um corpo K fixado.*

Toda curva $\mathcal{C}$ é birracionalmente equivalente a uma curva não-singular $\tilde{\mathcal{C}}$, chamada normalização de $\mathcal{C}$. Quando estamos interesados em problemas aritméticos,

vamos estar sempre tratando de curvas não-singulares, uma vez que as principais questões aritméticas qualitativas são invariantes na classe de equivalência birracional. Vamos considerar nossas curvas não-singulares e projetivas sobre o corpo K em questão. Sobre o problema de existência de pontos K-racionais, fixada uma classe de equivalência birracional, temos que a existência de pontos no caso liso implica a existência de pontos no caso geral, pelo seguinte:

Teorema 1.1.3 *Uma aplicação racional de uma curva lisa numa variedade projetiva se extende a um morfismo definido na curva.*

Demonstração: [Hin-Sil, pag.69]. □

Corolário 1.1.4 *Uma aplicação birracional entre curvas projetivas lisas é um isomorfismo.*

A normalização de uma curva é única, a menos de isomorfismo, pelo corolário acima.

1.1.2 Mergulhos no espaço projetivo

Quando estivermos tratando de curvas (variedades) projetivas lisas, vamos identificar divisores e fibrados lineares, uma vez que a correspondência $D \mapsto \mathfrak{L}(D)$, que a cada divisor de Weil faz corresponder um fibrado linear, fornece um isomorfismo entre o grupo dos divisores, módulo equivalência linear, e o grupo dos fibrados lineares, módulo isomorfismo.

Definição 1.1.5 *Um divisor D sobre uma curva $\mathcal{C}$ é um elemento do grupo livre gerado pelos pontos fecahdos de $\mathcal{C}$, i.e.*

$$D = \sum_{i=1}^{l} n_i P_i,$$

com $n_i \in \mathbb{Z}$ e $l \in \mathbb{Z}$.

Um divisor se diz efetivo se $n_i \geq 0$ para todo $i = 1, \ldots, l$.

Se a curva esta definida sobre um corpo K, definimos o grau de $D = \sum_{i=1}^{l} n_i P_i$ sobre K como sendo

$$\deg_K(D) = \sum_{i=1}^{l} n_i [K(P_i) : K] \in \mathbb{Z}.$$

Pelo fato de $\mathcal{C}$ ser de tipo finito sobre K, temos $[K(P) : K] < \infty$ para cada ponto fechado $P \in \mathcal{C}$.

Definição 1.1.6 *Seja D um divisor numa curva $\mathcal{C}$ sobre um corpo K. Definimos $L(D) = \Gamma(X, \mathfrak{L}(D))$ e $l(D) = \dim_K(L(D))$.*

Definição 1.1.7 *O feixe de diferenciais de uma curva lisa $\mathcal{C}$ sobre um corpo K será denotado por $\omega_{\mathcal{C}/K}$. Chamaremos divisor canônico qualquer divisor $K_{\mathcal{C}}$ de $\mathcal{C}$ tal que $\mathfrak{L}(K_{\mathcal{C}}) \simeq \omega_{\mathcal{C}/K}$. O divisor canônico só está bem definido, módulo equivalência linear.*

Definição 1.1.8 *O gênero de uma curva $\mathcal{C}$ projetiva, lisa sobre K é definido por:*

$$g(\mathcal{C}) = \dim_K(\Gamma(\mathcal{C}, \omega_{\mathcal{C}/k})) = l(K_{\mathcal{C}}).$$

Proposição 1.1.9 *Sejam $\mathcal{C}$ uma curva projetiva, lisa sobre um corpo K e D um divisor em $\mathcal{C}$. Então, se $L|K$ é uma extensão de corpos:*

(i) *O grau de D é invariante pela mudança de base, i.e. $\deg_K(D) = \deg_L(D_L)$, onde D_L é o divisor induzido sobre X_L pela mudança de base $\mathrm{Spec}(L) \to \mathrm{Spec}(K)$;*

(ii) *A dimensão $l(D)$ é invariante pela mudança de base;*

(iii) *O gênero de $\mathcal{C}$ é invariante pela mudança de base.*

Demonstração: (i) [Liu, pag.276]. (ii) e (iii) são consequência do fato que a dimensão de um espaço vetorial é invariante por tensorização e no terceiro caso que o feixe dos diferencial comuta com a mudança de base, i.e. $\omega_{X_L/L} \simeq \omega_{X/K} \otimes_K L$. □

Teorema 1.1.10 (**Riemann-Roch**) *Sejam $\mathcal{C}$ uma curva projetiva, lisa sobre um corpo K e D um divisor em $\mathcal{C}$. Então:*

$$l(D) - l(K_{\mathcal{C}} - D) = \deg(D) + 1 - g(\mathcal{C}).$$

Demonstração: [Liu, pag.281]. □

Corolário 1.1.11 *Sejam $\mathcal{C}$ uma curva e $K_{\mathcal{C}}$ um divisor canônico. Então:*

$$\deg(K_{\mathcal{C}}) = 2g(\mathcal{C}) - 2.$$

Demonstração: [Liu, pag.282]. □

Definição 1.1.12 *Sejam X uma variedade sobre K e D um divisor. Dizemos que D é sem ponto base (respectivamente amplo, respectivamente muito amplo) se o feixe $\mathfrak{L}(\mathcal{C})$ for gerado por seções globais (respectivamente amplo, respectivamente muito amplo).*

Seja X uma variedade projetiva, lisa definida sobre K. A maneira natural de definir aplicações de X no espaço projetivo $\mathbb{P}^n_K$ é a partir dos divisores (ou equivalentemente dos fibrados lineares ou feixes inversíveis) de X. Lembramos que se X é uma variedade sobre um corpo K e $\{s_0, ..., s_n\} \in \Gamma(X, \mathfrak{L})$ são linearmente independentes, podemos definir uma aplicação racional:

$$\Phi : X \dashrightarrow \mathbb{P}^n_K.$$

Temos o seguinte:

Teorema 1.1.13 *Seja X uma variedade projetiva, lisa sobre K e seja $\mathcal{O}(1)$ o feixe inversivel de $\mathbb{P}^n_K$ associado a um hiperplano.*

(i) *Se $\Phi : X \to \mathbb{P}^n_K$ é um morfismo, então $\Phi^*(\mathcal{O}(1))$ é um feixe inversível, gerado pelas seções globais $s_i = \Phi^*(x_i)$.*

(ii) *Reciprocamente, se $\mathfrak{L}$ é um feixe inversível em X, e se $\{s_0, ..., s_n\} \subseteq \Gamma(X, \mathfrak{L})$ são seções globais que geram $\mathfrak{L}$, então existe um único morfismo $\Phi : X \to \mathbb{P}^n_K$ tal que $\mathfrak{L} \simeq \Phi^*(\mathcal{O}(1))$ e tal que $s_i = \Phi^*(x_i)$ via esse isomorfismo.*

Demonstração: [Har, 150]. □

Corolário 1.1.14 *Seja $\mathcal{C}$ uma curva sobre um corpo K, projetiva e lisa de gênero g e seja D um divisor em $\mathcal{C}$. Então:*

(i) *se $\deg(D) \geq 2g$, então $\mathfrak{L}(D)$ é gerado por seções globais;*

(ii) *se $\deg(D) \geq 2g+1$, então $\mathfrak{L}(D)$ é muito amplo.*

Demonstração: [Liu, pag.286]. □

Definição 1.1.15 *Seja $\mathcal{C}$ uma curva sobre K, projetiva e lisa de gênero $g \geq 1$, dizemos que $\mathcal{C}$ é hiperelíptica se existe um morfismo finito e separável de grau dois:*

$$\Phi : \mathcal{C} \to \mathbb{P}^1_K.$$

Tal condição é equivalente a existência de um divisor D tal que $l(D) = \deg(D) = 2$ como descrito em [Liu, pag.287].

Proposição 1.1.16 *Toda curva $\mathcal{C}$ de gênero dois é hiperellíptica.*

Demonstração: O divisor canônico $K_{\mathcal{C}}$ tem grau $2g(\mathcal{C}) - 2 = 2$ e $l(K_{\mathcal{C}}) = g(\mathcal{C})$. Portanto se $g(\mathcal{C}) = 2$, tal curva é hipereliptica. □

Teorema 1.1.17 *Seja $\mathcal{C}$ uma curva sobre um corpo K, projetiva e lisa, de gênero g. Então:*

(i) *se $g = 0$, então $-K_{\mathcal{C}}$ é muito amplo;*

(ii) *se $g = 1$, então $K_{\mathcal{C}} = 0$;*

(iii) *se $g \geq 2$, então $K_{\mathcal{C}}$ é amplo. Numa curva $\mathcal{C}$ de genero $g \geq 3$, o divisor $K_{\mathcal{C}}$ é muito amplo se e somente se $\mathcal{C}$ não é hipereliptica.*

Demonstração: [Hin-Sil, pag.68] ou [Liu, pag. ??]. □

Proposição 1.1.18 *Seja $\mathcal{C}$ uma curva sobre um corpo K, projetiva, lisa e de gênero zero. Então:*

(i) *O divisor anticanônico $-K_{\mathcal{C}}$ define um mergulho $\mathcal{C} \hookrightarrow \mathbb{P}^2_K$ da curva $\mathcal{C}$ numa cônica plana lisa;*

(ii) *$\mathcal{C}(K) \neq \emptyset$ se e somente $\mathcal{C}$ é K-isomorfo a $\mathbb{P}^1_K$.*

Demonstração: (i) Como $-K_{\mathcal{C}}$ é muito amplo, basta notar que $\deg(-K_{\mathcal{C}}) = 2$ e $l(-K_{\mathcal{C}}) = 3$.
(ii) Se $P \in \mathcal{C}(K)$, temos que $D = P$ tem grau 1 e portanto é muito amplo pelo corolario 1.1.14. Pelo teorema de Riemann-Roch temos $l(P) = 2$ e portando o morfismo associado a P identifica $\mathcal{C}$ com $\mathbb{P}^1_K$. A outra implicação é trivial. □

Proposição 1.1.19 *Seja $\mathcal{C}$ uma curva sobre um corpo K que seja projetiva, lisa e de gênero um tal que $\mathcal{C}(K) \neq \emptyset$. Então existe um mergulho definido sobre K:*

$$\phi : \mathcal{C} \hookrightarrow \mathbb{P}^2_K$$

da curva $\mathcal{C}$ núma cúbica plana lisa.

Demonstração: Basta notar que se $P \in \mathcal{C}(K)$, então $\deg(\mathcal{L}(3(P))) = 3 = 2g(C) + 1$. Assim $\mathcal{L}(3(P))$ é muito amplo pelo corolario 1.1.14, $l((3P)) = 3$, pelo teorema de Riemann-Roch e portanto $\mathcal{L}(3(P))$ induz um mergulho definido sobre K de $\mathcal{C}$ em $\mathbb{P}^2_K$. A imagem é uma cúbica plana por construção. □

Para entender a aritmética das curvas de gênero maior ou igual a dois faz-se necessário introduzir o conceito de jacobiana e assim reduzir o problema ao estudo de variedades abelianas, como ilustraremos no último capítulo.

1.2 ARITMÉTICA

1.2.1 Corpos de números

Definição 1.2.1 *Um corpo de números $K|\mathbb{Q}$ é uma extensão finita dos racionais. Dado K um corpo de números, chamamos anel de inteiros de K, denotado $\mathcal{O}_K$, ao fecho integral de $\mathbb{Z}$ em K.*

A partir de nossa definição, é claro que $\mathcal{O}_K$ é integralmente fechado. Além disso, notamos também que $\mathcal{O}_K$ é $\mathbb{Z}$-módulo livre de posto $[K : \mathbb{Q}]$.

Temos $K \simeq \mathbb{Q}[X]/f(X)$, em que $f(X)$ é um polinômio irredutível sobre $\mathbb{Q}$ de grau $n = \deg(f) = [K : \mathbb{Q}]$. Sejam $\{\alpha_1, ..., \alpha_r\}$ as raíze reais de f e $\{\beta_1, \bar{\beta}_1, ..., \beta_s, \bar{\beta}_s\}$ as raízes complexas conjugadas. Claramente $r + 2s = n$.

Cada raiz real induz um mergulho real de K, $\iota_{\alpha_i} : K \hookrightarrow \mathbb{R}$, via o isomorfismo $K \simeq \mathbb{Q}(\alpha_i) \subset \mathbb{R}$. Cada par de raízes complexas conjugadas de f induz um mergulho complexo de K, $\iota_{\beta_j} : K \hookrightarrow \mathbb{C}$, via o isomorfismo $K \simeq \mathbb{Q}(\beta_j) \subset \mathbb{C}$.

Definição 1.2.2 *Sejam $L|K$ uma extensão finita de corpos e $x \in L$. Consideremos o endomorfismo:*

$$\begin{array}{rccc} T_x : & L & \to & L \\ & \alpha & \mapsto & x\alpha \end{array}$$

Definimos a norma de x por $N_{L|K}(x) = \det(T_x)$ e o traço de x por $Tr_{L|K} = Tr(T_x)$

Proposição 1.2.3 *Seja $L|K$ uma extensão separável e $\sigma : L \to \bar{K}$ variando entre todos os possíveis K-mergulhos de L em $\bar{K}$ (que correspondem ao grupo de Galois, no caso Galoisiano). Então:*

(i) *o polinômio característico de x é $f_x(t) = \prod_{\sigma}(t - \sigma(x))$;*

(ii) $Tr_{L|K}(x) = \sum_{\sigma} \sigma(x)$;

(iii) $N_{L|K}(x) = \prod_{\sigma} \sigma(x)$.

Demonstração: [Neu 1, pag.9]. □

Definição 1.2.4 *Seja K um corpo de números, $\mathcal{O}_K$ o anel de inteiros de K. Se $\beta = \{\omega_1, ..., \omega_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_K$, o discriminante de K é dado por:*

$$d_K = (\det([\sigma_i(\alpha_j)]))^2.$$

O discriminante é independente da base base β ([Neu 1, pag.15]).

Teorema 1.2.5 *Sejam K um corpo de números e $\mathcal{O}_K$ seu anel de inteiros. O anel $\mathcal{O}_K$ é um domínio de Dedekind, ou seja, é noetheriano, integralmente fechado e de dimensão 1. Logo, todo ideal primo $\mathfrak{p} \in Spec(\mathcal{O}_K) \setminus \{0\}$ é ideal maximal. Como $\mathcal{O}_K$ é Dedekind, todo ideal I diferente de (0) e (1), admite uma fatoração:*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_l$$

em ideais primos, não nulos de $\mathcal{O}_K$. Tal fatoração é única, a menos da ordem dos fatores.

Demonstração: [Neu 1, pag. 17–18]. □

Definição 1.2.6 *Sejam K um corpo de números e $\mathcal{O}_K$ seu anel de inteiros. O grupo multiplicativo dos ideais de $\mathcal{O}_K$ será denotado J_K. Os ideais principais formam um subgrupo denotado P_K. O grupo de classes de ideais de K é o grupo quociente*

$$\mathrm{Cl}_K = J_K / P_K.$$

Temos a seqüência exata de grupos abelianos:

$$1 \to \mathcal{O}_K^* \to K^* \to J_K \to \mathrm{Cl}_K \to 1.$$

Definição 1.2.7 *Sejam K um corpo de números e $\mathcal{O}_K$ seu anel de inteiros. Se $I \subset \mathcal{O}_K$ é um ideal não nulo, definimos a norma de I por:*

$$\mathfrak{N}(I) = [\mathcal{O}_K : I]$$

A norma é sempre finita e multiplicativa, ([Neu 1, pag.35]).

Teorema 1.2.8 (**Finitude do número de classes**) *Seja K um corpo de números. Então o grupo de classes de ideais Cl_K é finito e sua ordem é chamada número de classes de K.*

Demonstração: [Neu 1, pag.36]. □

Teorema 1.2.9 (**das unidades de Dirichlet**) *Seja K um corpo de números. O grupo das unidades de K, $\mathcal{O}_K^*$, é um grupo abeliano finitamente gerado de posto $r+s-1$, em que r e s são respectivamente o números de mergulhos reais e complexos de K.*

Demonstração: [Neu 1, pag.42]. □

Definição 1.2.10 *Sejam $L|K$ uma extensão finita de corpos de números, $\mathcal{O}_K$ e $\mathcal{O}_L$ o anel de inteiros de K e L respectivamente. Então, dado $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) \setminus \{0\}$, como $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$, temos pela fatoração única de ideais em $\mathcal{O}_L$:*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_l^{e_l}.$$

Os expoentes $\mathrm{e_i}$ são chamados índices de ramificação. Dizemos que $\mathfrak{p}$ não se ramifica se todos os índices de ramificação forem iguais a 1. O grau da extensão dos corpos residuais é chamado grau de inércia de $\mathfrak{P}_i$ sobre $\mathfrak{p}$ e é denotado por f_i, i.e.

$$f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}].$$

Os ideais, descritos na fatoração anterior, são os primos de $\mathcal{O}_L$ cuja restrição a $\mathcal{O}_K$ coincidem com $\mathfrak{p}$. Vamos denota-los $\mathfrak{P} \mid \mathfrak{p}$.

Teorema 1.2.11 (**Fórmula do grau**) *Seja $K|L$ uma extensão de corpos de números de grau $n = [L : K]$. Então:*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Demonstração: [Neu 1, pag.46]. □

Teorema 1.2.12 *Seja $L|K$ uma extensão finita de corpos de números, então é finito o número de primos de $\mathcal{O}_K$ que se ramificam em $\mathcal{O}_L$*

Demonstração: [Neu 1, pag.49]. □

Proposição 1.2.13 *Sejam $L|K$ uma extensão galoisiana de corpos de números, $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ e $S = \{\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L) \mid \mathfrak{P} \parallel \mathfrak{p}\}$. Então o grupo de Galois $\mathrm{Gal}\, L|K$ age transitivamente em S.*

Demonstração: [Neu 1, pag.54]. □

1.2.2 Valorizações e completamentos

Definição 1.2.14 *Uma valor absoluto de um corpo K é uma função:*

$$|\ | : K \to \mathbb{R},$$

satisfazendo as propriedades:

(i) $|x| \geq 0,\ \forall x \in K$ e $|x| = 0 \Leftrightarrow x = 0$;

(ii) $|x \cdot y| = |x| \cdot |y|$;

(iii) $|x + y| \leq |x| + |y|$.

De agora em diante, excluiremos o valor absoluto trivial. Definindo a distancia entre dois pontos por $d(x, y) = |x - y|$, K torna-se um espaço métrico. A dupla $(K, |\ |)$ se diz um corpo metrico.

Definição 1.2.15 *Dois valores absolutos de K são equivalentes se definem a mesma topologia.*

Teorema 1.2.16 (**Aproximação fraca**) *Sejam* $|\ |_1, ..., |\ |_n$ *um conjunto de valores absolutos de um corpo* K*, duas a duas não equivalentes. Dados* $\{a_1, ..., a_n\} \subset K$ *e* $\varepsilon > 0$*, existe um elemento* $x \in K$ *tal que:*

$$|x - a_i|_i < \varepsilon$$

para cada $i = 1, ..., n$*.*

Demonstração: [Neu 1, pag.117]. □

Definição 1.2.17 *Um valor absoluto de um corpo* K *é não arquimediano se a sequência* $\{|n|\}_{n\in\mathbb{N}}$ *é limitada ou, equivalentemente, vale a desigualdade ultramétrica:*

$$|x + y| \leq \max\{|x|, |y|\},\ \forall\ x, y \in K.$$

Em caso contrário dizemos que o valor absoluto é arquimediano.

Definição 1.2.18 *Seja* $(K, |\ |)$ *um corpo métrico. Dizemos que* K *é completo (com respeito a* $|\ |$*) se toda sequência de Cauchy converge.*

Definição 1.2.19 *Seja* $(K, |\ |)$ *um corpo métrico, existe um único (a menos de isomorfismo homeomórfico) corpo métrico completo* $(\hat{K}, |\ |)$ *tal que:*

(i) $K \hookrightarrow \hat{K}$*;*

(ii) *a métrica de* $\hat{K}$ *estende a métrica de* K*;*

(iii) *(a imagem de)* K *é denso(a) em* $\hat{K}$*.*

Tal corpo é chamado o completamento de K *com respeito a* $|\ |$*.*

Se K é um corpo de números e $\mathcal{O}_K$ seu anel de inteiros, para cada $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_k) \setminus \{0\}$, a localização $\mathcal{O}_\mathfrak{p}$ é um anel local de dimensão 1 e portanto um anel de valorização discreta. Vamos denotar a valorização (normalizada) por $v_\mathfrak{p}$. A função:

$$\begin{array}{rccc} |\ |_\mathfrak{p}: & K & \to & \mathbb{R} \\ & x & \mapsto & N_{K|\mathbb{Q}}(x)^{-v_\mathfrak{p}} \end{array}$$

é um valor absoluto não arquimediano de K, chamado valor absoluto $\mathfrak{p}$-ádico de K.

Seja K um corpo de números e considere um mergulho $\iota : K \hookrightarrow \mathbb{R}$. Temos em K um valor absoluto arquimediano dado por $|x|_K = |\iota(x)|$. Analogamente, se $\iota : K \hookrightarrow \mathbb{C}$, $|x|_K = |\iota(x)|^2$ é um valor absoluto arquimediano.

Definição 1.2.20 *Seja K um corpo de números. Então o conjunto das classes de equivalência dos valores absolutos de K será denotado M_K. As classes de valores absolutos arquimedianos serão denotados com M_K^∞ e as classes de não arquimedianos com M_K^0.*

Uma classe de equivalência de valores absolutos será chamada um Place e será denotada por v. Se $v \in M_K^\infty$, v é chamado um Place infinito ou arquimediano *e se $v \in M_K^0$, o Place é chamado* Place finito ou não arquimediano.

Teorema 1.2.21 *Seja K um corpo de números. Os Places finitos de K correspondem aos primos não nulos de $\mathcal{O}_K$ e os Places infinitos aos mergulhos em $\mathbb{R}$ ou $\mathbb{C}$.*

Demonstração: [Neu 1, pag.124]. □

Definição 1.2.22 *Sejam K um corpo de números, $v \in M_K^0$ um Place finito e $\mathfrak{p}$ o primo correspondente a v. Denotamos por $(\mathcal{O}_K)_v$ o completamento de $(\mathcal{O}_K)_\mathfrak{p}$ com respeito ao valor absoluto induzido por v. Denotamos por K_v o corpo de frações de $(\mathcal{O}_K)_\mathfrak{p}$.*

Os corpos locais definidos acima são extensões finitas dos corpos p-ádicos. Se $v \in M_K^\infty$ definimos K_v como sendo $\mathbb{R}$ ou $\mathbb{C}$ de acordo com o mergulho associado a v ser real ou complexo.

Algebricamente definimos $(\mathcal{O}_K)_v = \varprojlim \mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K$.

Lema 1.2.23 (**Hensel**) *Sejam K um corpo de números, $v \in M_K^0$ um Place finito associado a um primo $\mathfrak{p}$. Dado $f \in (\mathcal{O}_K)_v[X]$, suponha que existe $a \in (\mathcal{O}_K)_v$ tal $\bar{a} \in (\mathcal{O}_K)_v/\mathfrak{p}(\mathcal{O}_K)_v$ seja uma raiz simples de $\bar{f} \in (\mathcal{O}_K)_v/\mathfrak{p}(\mathcal{O}_K)_v[X]$. Então f tem uma raiz em K_v.*

Este importante lema está entre as principais propriedades dos números p-ádicos. O lema de Hensel segue como corolário do seguinte:

Lema 1.2.24 (**Newton**) *Sejam K um corpo de números, $v \in M_K^0$ um Place finito associado a um primo $\mathfrak{p}$ e $f \in (\mathcal{O}_K)_v[X]$. Suponha que exista $a \in (\mathcal{O}_K)_v$ tal que*

$$v_{\mathfrak{p}}(f(a)) > 2v_{\mathfrak{p}}(f'(a)).$$

Então f tem uma raiz em K_v.

Demonstração: [Pr, pag.22]. □

Teorema 1.2.25 *Sejam $L|K$ uma extensão de corpos de números e $v \in M_K^0$ um Place finito de K. Então:*

(i) *toda extensão $\Upsilon \in M_L$ de v é proveniente de um mergulho $L \hookrightarrow \bar{K}_v$;*

(ii) *duas extensões representam o mesmo Place se e somente se os mergulhos são conjugados sobre K_v;*

(iii) *se o primo associado a v é da forma $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_s$, os Places de L extendendo v são aqueles associados a $\mathfrak{P}_i$.*

Demonstração: [Neu 1, pag.162]. □

Proposição 1.2.26 *Sejam $L|K$ uma extensão de corpos de números e $v \in M_K^0$ um Place finito. Então:*

(i) $\displaystyle\sum_{\Upsilon|v} [L_\Upsilon : K_v] = [L : K]$;

(ii) $\displaystyle\sum_{\Upsilon|v} e_\Upsilon f_\Upsilon = [L : K]$,

onde $e_\Upsilon = (\Upsilon(L^*) : v(K^*))$ e $f_\Upsilon = [\kappa_\Upsilon : \kappa_v]$.

Demonstração: [Neu 1, pag. 164–165]. □

CAPÍTULO 2

O PRINCÍPIO LOCAL-GLOBAL PARA QUÁDRICAS

As primeiras classes de equações diofantinas a serem estudadas foram as equações de retas e cônicas no plano (que vamos considerar projetivas sobre um corpo de números K). Tais curvas têm gênero zero, logo, a existência de um ponto K-racional fornece um K-isomorfismo em $\mathbb{P}^1$, como descrito na proposição, 1.1.18. Portanto, para entender a aritmética de tais curvas, é suficiente decidir quando seu conjunto de pontos K-racionais é ou não vazio. Legendre foi o primeiro a resolver este problema sobre os racionais, entretanto, sua demonstração não se generaliza para corpos de números. Neste capítulo, vamos desenvolver o ferramental necessário para dar uma condição necessária e suficiente para a existência de um ponto K-racional em hipersuperfícies quádricas de $\mathbb{P}^n_K$, $n \geq 2$. O *princípio local-global* diz que uma condição necessária e suficiente para a existência de um ponto K-racional, numa varidade projetiva lisa sobre um corpo de números K é a existência de pontos em K_v para cada $v \in M_K$. Esse resultado, em geral é falso, como mostraremos no final do próximo capítulo, mas vale para hipersuperfícies quádricas lisas, Teorema de Hasse–Minkowski.

2.1 COHOMOLOGIA DE GRUPOS

Nesta seção, vamos introduzir os conceitos básicos sobre cohomologia de gupos que serão usados em seções posteriores para a demonstração do princípio local-global.

Definição 2.1.1 *Seja G um grupo com identidade* 1. *Um G-módulo é um grupo abeliano A (notação aditiva) sobre o qual G age e tal que:*

(i) $1a = a$, $\forall a \in A$;

(ii) $\sigma(a + b) = \sigma a + \sigma b$, $\forall \sigma \in G$ *e* $\forall a, b \in A$;

(iii) $(\sigma\tau)a = \sigma(\tau a)$, $\forall \sigma, \tau \in G$ *e* $\forall a \in A$.

O submódulo fixo de um G-módulo A é o subgrupo

$$A^G = \{a \in A | \sigma a = a \ \forall \sigma \in G\}$$

Definição 2.1.2 *Se G é um grupo finito, então, cada G-módulo A contém (como subgrupo) o subgrupo das normas:*

$$N_G A = \{N_G(a) = \sum_{\sigma \in G} \sigma a \mid a \in A\}$$

Claramente, $\tau N_G(a) = \sum_{\sigma \in G} \tau\sigma a = \sum_{\tau\sigma \in G} \tau\sigma a = N_G(a)$. Logo, $N_G A < A^G$.

Definição 2.1.3 *O grupo residual de normas é o grupo quociente:*

$$H^0(G, A) = A^G / N_G A.$$

Definição 2.1.4 *Um 1-cociclo de G em A é uma função $f : G \to A$ tal que:*

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau).$$

Os 1-cociclos formam um grupo abeliano denotado $Z^1(G, A)$.
Para cada $a \in A$, temos um 1-cobordo

$$f_a : G \to A, \ f_a(\sigma) = \sigma a - a,$$

que é claramente um 1-cociclo, pois

$$f_a(\sigma\tau) = (\sigma\tau)a - a = \sigma(\tau a - a) + \sigma a - a = f_a(\sigma) + \sigma f_a(\tau).$$

Os 1-cobordos formam um subgrupo dos 1-cociclos que denotamos $B^1(G, A)$.
Definimos o primeiro grupo de cohomologia como:

$$H^1(G, A) = Z^1(G, A)/B^1(G, A)$$

Proposição 2.1.5 *Considere a seqüência exata curta de G módulos:*

$$0 \to A \to B \to C \to 0$$

Então, temos induzida a seqüência exata:

$$0 \to A^G \to B^G \to C^G \to H^1(G, A)$$

Demonstração: [Neu 2, pag.9]. □

Definição 2.1.6 *Sejam G um grupo, $H < G$ um subgrupo, e B um H-módulo. O G-módulo induzido por B, denotado por $M_G^H(B)$ é o grupo abeliano*

$$M_G^H(B) = \{f : G \to B \ : \ f(\tau x) = \tau f(x) \ \ \forall \tau \in H\}.$$

A ação de G em $M_G^H(B)$ é dada por:

$$(\sigma f)(x) = f(x\sigma)$$

Temos, assim, um H homomorfismo canônico:

$$\begin{array}{rccc} \pi : & M_G^H(B) & \to & B \\ & f & \to & f(1) \end{array}$$

Proposição 2.1.7 *Sejam G um grupo finito, $H < G$ um subgrupo e B um H-módulo. Para $i = 0, 1$ temos um isomorfismo natural*

$$H^i(G, M_G^H(B)) \simeq H^i(H, B).$$

Demonstração: [Neu 2, pag.11]. □

Definição 2.1.8 *Sejam $G =< \sigma >$ um grupo finito e cíclico e A um G-módulo. Definimos os G-submódulos de A:*

$${}_{N_G}A = \{a \in A | N_G(a) = 0\}$$

$$I_G A = \{\sigma a - a | a \in A\}.$$

Claramente $I_G A <_{N_G} A$ e podemos definir:

$$H^{-1}(G, A) =_{N_G} A/I_G A.$$

Proposição 2.1.9 (**Periodicidade**) *Sejam G um grupo cíclico finito e A um G–módulo. Então:*

$$H^1(G, A) \simeq H^{-1}(G, A).$$

Demonstração: [Neu 2, pag.12] □

Proposição 2.1.10 (**Seqüência Exata Longa**) *Consideremos a seqüência exata curta de G–módulos:*

$$0 \to A \to B \to C \to 0.$$

Então, temos a seguinte seqüência exata induzida:

$$H^{-1}(G,A) \to H^{-1}(G,B) \to H^{-1}(G,C) \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \to H^1(G,A)$$

Demonstração: [Neu 2, pag.14]. □

Definição 2.1.11 *Sejam G um grupo finito cíclico e A um G–módulo. Quando ambas as cardinalidades são finitas, definimos o qüociente de Herbrand como sendo:*

$$h(G,A) = \frac{\sharp H^0(G,A)}{\sharp H^{-1}(G,A)}.$$

Proposição 2.1.12 *Consideremos uma sequência exata curta de G módulos, com G um grupo finito cíclico.:*

$$0 \to A \to B \to C \to 0$$

Então quando dois quocientes de Herbrand são finitos, o terceiro também o é, e vale a igualdade:

$$h(G,B) = h(G,A) \cdot h(G,C).$$

Além disso, se A é finito, então, $h(G,A) = 1$

Demonstração: [Neu 2, pag.13]. □

2.2 COHOMOLOGIA DE GALOIS

Teorema 2.2.1 (**90 de Hilbert**) *Seja $L|K$ uma extensão de corpos finita e Galoisiana e seja $G = \mathrm{Gal}(L|K)$. Assim, o grupo multiplicativo L^* é um G–módulo e temos*

$$H^1(G,L^*) = 1.$$

Em particular, se $G =< \sigma >$ *é cíclico, então, todo elemento* $a \in L^*$ *cuja norma* $N_{L|K}(a) = 1$, *é da forma:*

$$a = \frac{\sigma b}{b} \ , \ b \in L^*$$

Demonstração: Consideremos um 1-cociclo $f : G \to L^*$. Seja $c \in L^*$ tal que $\alpha := \sum_{\sigma \in G} f(\sigma)\sigma c \neq 0$ (isso é sempre possível pela independencia linear dos $\sigma \in G$). Para cada $\tau \in G$, obtemos assim:

$$\tau\alpha = \sum_{\sigma \in G} \tau f(\sigma)(\sigma c) = \sum_{\tau\sigma \in G} f(\tau)^{-1} f(\tau\sigma)(\tau\sigma c) = f(\tau)^{-1}\alpha,$$

isto é, $f(\tau) = \frac{\tau\alpha^{-1}}{\alpha^{-1}}$ e, portanto, f é um 1-cobordo. Se $G =< \sigma >$ é ciclico, então pela proposição 2.1.9, $H^1(G, L^*) = H^{-1}(G, L^*) = 1$ e ${}_{N_G}L^* = I_G L^*$, que é o resultado requerido. □

Teorema 2.2.2 *Seja* $L|K$ *uma extensão cíclica finita de corpos* $\mathfrak{p}$*-ádicos, então:*

$$\sharp H^0(\mathrm{Gal}(G|L), L^*) = [L : K]$$

Demonstração: Seja $G = \mathrm{Gal}(L|K)$, pelo teorema 90 de Hilbert, 2.2.1, temos $H^1(G, L^*) = H^{-1}(G, L^*) = 1$ e, portanto, o quociente de Herbrand $h(G, L^*) = H^0(G, L^*)$. Consideremos a seqüência exata de valorização $\mathfrak{p}$-ádica:

$$1 \to U_L \to L^* \to \mathbb{Z} \to 0$$

na qual $\mathbb{Z}$ é considerado um G–módulo trivial. Pela multiplicatividade do quociente de Herbrand, proposição 2.1.12, temos:

$$h(G, L^*) = h(G, \mathbb{Z}) \cdot h(G, U_L) = [L : K] \cdot h(G, U_L)$$

Desse modo, para mostrar nosso resultado, devemos mostrar que $h(G, U_L) = 1$. Detalhes em [Neu 2, pag.40]. □

Proposição 2.2.3 *Sejam* $L|K$ *uma extensão finita e não ramificada de corpos* $\mathfrak{p}$*-ádicos e seja* $U_L = \mathcal{O}_L^*$. *Então, para* $i = 0, 1$ *temos:*

$$H^i(\mathrm{Gal}(L|K), U_L) = 1.$$

Demonstração: Sejam $G = \mathrm{Gal}(L|K)$, $n = [L : K]$ e considere $\mathbb{Z}$ como um G–módulo trivial. Temos

$$H^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} \ , \ \ H^{-1}(G, \mathbb{Z}) = 0.$$

A sequência exata curta de valorização $\mathfrak{p}$-ádica:

$$1 \to U_L \to L^* \to \mathbb{Z} \to 0$$

e a proposição 2.1.10 fornecem a seqüência exata:

$$1 \to H^0(G, U_L) \to H^0(G, L^*) \to H^0(G, \mathbb{Z}) \to H^1(G, U_L) \to 1$$

uma vez que $H^{-1}(G, \mathbb{Z}) = 0$ e que, pelo teorema 90 de Hilbert 2.2.1, $H^1(G, L^*) = 1$. Seja π_K um fator uniformizante de $\mathcal{O}_K$. Como a extensão é não ramificada,

$$v_L(\pi_K) = v_K(\pi_K) = 1$$

e, portanto, o homomorfismo $v_L^* : H^0(G, L^*) \to H^0(G, \mathbb{Z})$ é sobrejetivo. Por outro lado, o teorema 2.2.2, nos diz que $\sharp H^0(G, L^*) = n$, logo v_L^* é, de fato, um isomorfismo e o nosso resultado segue. □

2.3 ADELES, IDELES E CLASSES DE IDELES

Definição 2.3.1 *Seja K um corpo de números, um adele α de K é uma família $\alpha = (\alpha_\upsilon)_{\upsilon \in M_K}$ de elementos $\alpha_\upsilon \in K_\upsilon$, em que, para quase todos $\upsilon \in M_K$, temos: $\alpha_\upsilon \in \mathcal{O}_K$.*

Os adeles formam um anel denotado $\mathbb{A}_K$. Nesse anel, adição e multiplicação são definidas componente a componente.

Um idele é uma unidade no anel dos adeles, ou seja, uma família $\alpha = (\alpha_\upsilon)$ de elementos $\alpha_\upsilon \in K_\upsilon^*$, em que para quase todo $\upsilon \in M_K$, $\alpha_\upsilon \in U_\upsilon$ é uma unidade em $\mathcal{O}_{K_\upsilon}$.

Os ideles, assim, formam um grupo abeliano que denotaremos I_K.

Para cada $x \in K^*$, estaremos considerando $(x) \in I_K$ como o idele cuja componente υ é $x \in K_\upsilon$, notando que, para quase todo $\upsilon \in M_K$, x é uma unidade em $\mathcal{O}_{K_\upsilon}$.

O grupo quociente:

$$C_K = I_K/K^*$$

é chamado o grupo de classes de ideles.

Temos, assim, a importante seqüência exata:

$$1 \to K^* \to I_K \to C_K \to 1.$$

Proposição 2.3.2 *Seja $L|K$ uma extensão Galoisiana de corpos de números, $\upsilon \in M_K$ um Place e $\Upsilon \in M_L$ um Place. Se Υ estende υ, escrevemos $\Upsilon|\upsilon$. Então:*

(i) *Existe uma injeção natural*

$$I_K \hookrightarrow I_L.$$

(ii) *Cada $\sigma \in \mathrm{Gal}(L|K)$ induz um automorfismo $\sigma : I_L \to I_L$ de modo que I_L torna-se um G–módulo tal que $I_L^G = I_K$.*

(iii) *A função norma $N_{L|K} : I_L \to I_K$ é dada por:*

$$N_{L|K}(\alpha) = \prod_{\sigma \in Gal(L|K)} \sigma\alpha = (\prod_{\Upsilon|\upsilon} N_{L_\Upsilon|K_\upsilon}(\alpha_\Upsilon))_\upsilon,$$

isto é, a componente υ do idele $N_{L|K}(\alpha)$ é $\prod_{\Upsilon|\upsilon} N_{L_\Upsilon|K_\upsilon}(\alpha_\Upsilon)$.

Demonstração: [Neu 2, pag.82]. □

Proposição 2.3.3 *Seja $L|K$ uma extensão Galoisiana de corpos de números com grupo de Galois G, seja*

$$I_L^\upsilon = \prod_{\Upsilon|\upsilon} L_\Upsilon^*,$$

seja

$$U_L^\upsilon = \prod_{\Upsilon|\upsilon} U_\Upsilon^*$$

e seja

$$I_L^S = \prod_{\upsilon \in S} I_L^\upsilon \times \prod_{\upsilon \notin S} U_L^\upsilon$$

com $S \subset M_K$ finito. Então:

(i) $I_L^v = M_G^{G_\Upsilon}(L_\Upsilon^*)$ *e* $U_L^v = M_G^{G_\Upsilon}(U_\Upsilon^*)$.

(ii) $I_L = \varinjlim_S I_L^S$.

(iii) *Se* S *contém os lugares infinitos e os primos que se ramificam, temos, para* $i = 0, 1$*:*

$$H^i(G, I_L^S) \simeq \bigoplus_{v \in S} H^i(G_\Upsilon, L_\Upsilon^*)$$

e

$$H^i(G, I_L) \simeq \bigoplus_{v \in M_K} H^i(G_\Upsilon, L_\Upsilon^*).$$

Demonstração: (i) Consideremos um $\Upsilon|v$ fixado e um conjunto de representantes de $G/G_\Upsilon = \mathrm{Gal}(L|K)/\mathrm{Gal}(L_\Upsilon|K_v)$, então:

$$I_L^v = \prod_\sigma L_{\sigma\Upsilon}^* = \prod_\sigma \sigma(L_\Upsilon^*) \ , \ U_L^v = \prod_\sigma U_{\sigma\Upsilon} = \prod_\sigma \sigma(U_\Upsilon)$$

Daí segue nosso resultado. A parte (ii) segue imediatamente da definição. A partir da decomposição $I_L^S = [\bigoplus_{v \in S} I_L^v] \oplus V$ em que $V = \prod_{v \notin S} U_L^v$ obtemos isomorfismos para $i = 0, 1$:

$$H^i(G, I_L^S) = [\bigoplus_{v \in S} H^i(G, I_L^v)] \oplus H^i(G, V)$$

Por outro lado, temos, da letra (i) e da proposição 2.1.7, os isomorfismos:

$$H^i(G, I_L^v) \simeq H^i(G, M_G^{G_\Upsilon}(L_\Upsilon^*)) \simeq H^i(G_\Upsilon, L_\Upsilon^*).$$

Temos ainda uma injeção natural:

$$H^i(G, V) \hookrightarrow \prod_{v \notin S} H^i(G, U_L^v)$$

e, pela proposição 2.2.3, temos, para todo primo que não se ramifica, $H^i(G_\Upsilon, U_\Upsilon) = 1$. Isso conclui a demonstração do primeiro isomorfismo. O segundo isomorfismo segue de (ii) e das propriedades de comutatividade de somas diretas e limites diretos, provando também (iii). □

2.4 TEOREMA DA NORMA DE HASSE

Lema 2.4.1 *Sejam $L|K$ uma extensão cíclica de corpos de números. Então:*

$$H^1(\mathrm{Gal}(L|K), C_L) = H^{-1}(\mathrm{Gal}(L|K), C_L) = 0.$$

Demonstração: [Neu 2, pag.89]. □

Teorema 2.4.2 (**Hasse**) *Seja $L|K$ uma extensão cíclica de corpos de números. A propriedade de um elemento $x \in K^*$ ser norma de um elemento de L é local, ou seja, é equivalente à propriedade de ser uma norma em qualquer completamento $L_{\mathfrak{P}}|K_{\mathfrak{p}}$.*

Demonstração: Considere a sequência exata de $Gal(L|K)$ módulos:

$$1 \to L^* \to I_L \to C_L \to 1.$$

Tal seqüência induz uma seqüência exata nas cohomologias, pela proposição 2.1.10:

$$H^{-1}(\mathrm{Gal}(L|K), C_L) \to H^0(\mathrm{Gal}(L|K), L^*) \to H^0(\mathrm{Gal}(L|K), I_L).$$

Temos visto que, pelo lema 2.4.1, $H^{-1}(\mathrm{Gal}(L|K), C_L) = 1$. Da definição segue $H^0(\mathrm{Gal}(L|K), L^*) \simeq K^*/N_{L|K}L^*$ e, pela proposição 2.3.3,

$$H^0(\mathrm{Gal}(L|K), I_L) \simeq \bigoplus_{\mathfrak{p} \in M_K} K_{\mathfrak{p}}^*/N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}L_{\mathfrak{P}}^*.$$

Portanto, nossa seqüência exata se traduz em uma injeção:

$$K^*/N_{L|K}L^* \hookrightarrow \bigoplus_{\mathfrak{p} \in M_K} K_{\mathfrak{p}}^*/N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}L_{\mathfrak{P}}^*,$$

que é o resultado desejado. □

2.5 PRINCÍPIO LOCAL-GLOBAL PARA QUADRICAS

Nesta seção, vamos mostrar o principal resultado deste capítulo, o princípio local-global para hipersuperfícies quádricas lisas. Para facilitar o entendimento, vamos destacar alguns lemas técnicos que serão úteis durante a demonstração do teorema.

Lema 2.5.1 *Sejam K um corpo, $K(\sqrt{a})|K$ e $K(\sqrt{b})|K$ extensões quadráticas de K e $c \in K^*$. Então, c é produto de uma norma de $K(\sqrt{a})|K$ por uma norma de $K(\sqrt{b})|K$ se e somente se c visto como elemento de $K(\sqrt{ab})$ for uma norma da extensão $K(\sqrt{a},\sqrt{b})|K(\sqrt{ab})$.*

Demonstração: Seja γ um elemento da extensão $K(\sqrt{a},\sqrt{b})|K(\sqrt{ab})$ então $\gamma = u + v\sqrt{a}$ em que $u, v \in K(\sqrt{ab})$. Desta feita, se $c = N_{K(\sqrt{a},\sqrt{b})|K(\sqrt{ab})}(\gamma)$, então, $\gamma = u + v\sqrt{a}$. Escrevendo $u = x + y\sqrt{ab}$ e $v = z + t\sqrt{ab}$, com $x, y, z, t \in K$, obtemos:

$$c = x^2 + y^2ab - az^2 - a^2t^2b + (2xy - 2azt)\sqrt{ab}.$$

Como $c \in K^*$ por hipótese, temos que $xy = azt$. Os elementos x, y, z, t não podem ser todos nulos. Podemos supor, sem perda de generalidade, $y \neq 0$. Assim $x = \frac{azt}{y}$ e

$$c = (\frac{azt}{y})^2 - a^2t^2b + y^2ab - az^2$$

$$c = (z^2 - y^2b)(\frac{a^2t^2 - ay^2}{y^2})$$

$$c = N_{K(\sqrt{a})|K}(z + y\sqrt{b})N_{K(\sqrt{b})|K}(\frac{at}{y} + y\sqrt{a}).$$

A recíproca é imediata, revertendo os cálculos. □

Lema 2.5.2 (**Aproximação fraca**) *Sejam K um corpo de números e $S = \{v_1, ..., v_l\} \in M_K$ um conjunto finito de Places. Então, (a imagem de) K é denso(a) em $\prod_{v \in S} K_v$.*

Demonstração: Tal afirmação é equivalente a de que dados $\varepsilon > 0$ e $x_i \in K_{v_i}$, $i = 1, ..., l$, existe $x = x(\varepsilon) \in K$ tal que $\| x - x_i \|_{v_i} < \varepsilon$ que é o conteúdo do teorema, 1.2.16 □

Lema 2.5.3 *Sejam K um corpo de números e $v \in M_K^0$ um Place finito. Então K_v^{*2} é aberto em K_v^**

Demonstração: [O'Me, pag.159]. □

Teorema 2.5.4 (**Hasse-Minkowski**) *Seja $X \subset \mathbb{P}^n_K$, $n \geq 2$, uma quádrica lisa definida sobre um corpo de números K, i.e. X é dada por uma forma quadrática não degenerada em $n+1$ variáveis com coeficientes em K. Uma condição necessária e suficiente para a existência de um ponto K-racional é existir, localmente, pontos em K_v para cada Place $v \in M_K$.*

Demonstração: A necessidade é clara, vamos mostrar a suficiência. Seja Q a forma quadrática associada a X. Diremos que Q representa 0 em K se X tiver um ponto K racional. Lembramos que, se uma forma quadrática não degenerada representa 0 em K, então ela representa todo K. Isso porque $Q(tv+w) = t^2Q(v) + tB(v,w) + Q(w)$, em que B é a forma bilinear associada e, se $Q(v) = 0$, $v \neq 0$, existe w tal que $B(v,w) \neq 0$, pois Q é não degenerada.

Vamos considerar primeiramente o caso $n = 2$, i.e. de três variáveis X, Y, Z. A menos de uma projetividade, podemos supor $Q = X^2 - aY^2 - bZ^2$. A condição de Q representar 0 em K é, portanto, equivalente a b ser uma norma de um elemento da extensão $K(\sqrt{a})|K$, de fato, $b = N_{K[(\sqrt{a})|K}(x + y\sqrt{a})$. Como a extensão $K(\sqrt{a})|K$ é cíclica, pelo teorema da norma de Hasse, 2.4.2, sabemos que tal propriedade é local e portanto, o resultado vale nesse caso.

Vamos agora tratar o caso em que Q tem quatro variáveis, i.e. $n = 3$. A menos de uma projetividade, podemos supor $Q = X^2 - bY^2 - cZ^2 + adT^2$. Nesse caso, a propriedade de Q representar 0 em K é equivalente a c ser o produto de uma norma de um elemento de $K(\sqrt{a})|K$ por uma norma de um elemento da extensão $K(\sqrt{b})|K$. De fato, $c = N_{K[(\sqrt{b})|K}(x + y\sqrt{b})N_{K[(\sqrt{a})|K}(z + t\sqrt{a})^{-1}$ e isso é equivalente a ser uma norma de um elemento da extensão $K(\sqrt{a}, \sqrt{b})|K(\sqrt{ab})$ pelo lema 2.5.1. Como tal extensão é cíclica, podemos usar o teorema da norma de Hasse, 2.4.2, para concluir o resultado também nesse caso.

Para o caso em que o número de variáveis de Q é maior ou igual a 5, i.e. $n \geq 4$, vamos proceder por indução. Escrevendo $Q = aX_1^2 + bX_2^2 - \tilde{Q}$, o fato da injeção:

$$K^*/N_{L|K}L^* \hookrightarrow \bigoplus_{\mathfrak{p} \in M_K} K^*_{\mathfrak{p}}/N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}L^*_{\mathfrak{P}},$$

obtida no teorema da norma de Hasse, ser numa soma direta implica que há, no maximo, um número finito de *Places* S, em que $\tilde{Q}$ não representa 0 em K_v. Nossa hipótese é de Q representar 0 em K_v para cada $v \in M_K$, portanto, para cada $v \in M_K$, existe um $c_v \in K_v^*$ tal que $aX_1^2 + bX_2^2$ e $\tilde{Q}$ o representam em K_v. Vamos

chamar tais coordenadas $x_i(v)$. Variando x_1 e x_2, $aX_1^2 + bX_2^2$ reppresenta todo K. Pelo lema de aproximação fraca, 1.2.16, a imagem de K em $\prod_{v\in S} K_v$ é densa, portanto, existem x_1 e x_2 em K tais que $c/c_v \in K_v^{*2}$, $\forall v \in S$, uma vez que, pelo lema 2.5.3, K_v^{*2} é aberto em K_v^*. Considere agora a forma quadrática $\bar{Q} := cY^2 - \tilde{Q}$. Ela representa 0 em K_v $\forall v \notin S$, pois $\tilde{Q}$ representa 0 nesses corpos, por hipótese.

Por outro lado, nossa construção nos mostra que a forma quadrática $\tilde{Q}$ também representa 0 em K_v $\forall v \in S$, pois, nesse caso, $c = c_v d_v^2$ e é suficiente tomar $Y = \frac{1}{d_v}$ e as coordenadas em $\tilde{Q}$, que a fazem representar c_v. Pela hipótese indutiva, temos que a forma quadrática $\bar{Q}$ representa 0 em K. Se, nesse caso, tivermos $y = 0$, então $\tilde{Q}$ representa 0 em K e, assim, Q também. Se ocorrer $y \neq 0$, então, dividindo por y, percebemos que $\tilde{Q}$ e $aX_1^2 + bX_2^2$ representam o mesmo c em K e, portanto, sua diferença, Q, representa 0 em K. □

CAPÍTULO 3

CURVAS ELÌPTICAS

3.1 CÚBICAS PLANAS

Depois das equações diofantinas de segundo grau, é natural tratar o caso de equações cúbicas. Nós nos limitaremos ao caso de duas variáveis, estudando as cúbicas planas. Quando estamos interessados em entender o conjunto dos pontos K–racionais, é razoável considerarmos cúbicas projetivas $\mathcal{C} \subset \mathbb{P}^2_K$ dadas por equações da forma:

$$P(X_0 : X_1 : X_2) = 0$$

em que P é um polinômio homogêneo, irredutível, de grau três.

Quando a curva associada é singular, existe apenas um ponto singular sobre $\overline{K}$ (se sobre $\overline{K}$ houvesse mais de um, a reta, ligando dois desses pontos, intersectaria a cúbica $\mathcal{C}$ em, no mínimo, quatro pontos contados com multiplicidade, contradizendo o Teorema de Bèzout). O ponto singular é, portanto, definido sobre K e pode ser uma cúspide ou um nó. Em qualquer dos casos, a curva é racional.

Vamos agora nos preocupar com o caso não-singular. Assim sendo, a curva $\mathcal{C}$ tem gênero 1 (pela formula do gênero de curvas planas projetivas não-singulares de grau n: $g = \frac{(n-1)(n-2)}{2}$). Existe uma mudança de coordenadas (por projetividades) quando a característica do corpo é diferente de 2 e 3, tal que $\mathcal{C}$ admite uma forma canônica, conhecida como forma de *Weierstrass*:

$$Y^2Z = X^3 + AXZ^2 + BZ^3.$$

Escrevendo a equação no aberto afim $\mathcal{U}_Z$ dos pontos de $\mathbb{P}^2_K$ com $Z \neq 0$, obtemos:

$$Y^2 = X^3 + AX + B.$$

Seja $\Delta = -16(4A^3 + 27B^2)$ o disccriminante de $f(X) = X^3 + AX + B$. Define-se o j-invariante de $\mathcal{C}$ por:

$$j = \frac{1728(4A)^3}{\Delta}.$$

Claramente a não singularidade de $\mathcal{C}$ é equivalente a $\Delta \neq 0$.

Proposição 3.1.1 *Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ duas cúbicas planas não singulares dadas por equações na forma de Weierstrass. Então, uma condição necessária e suficiente para que as curvas sejam isomorfas é que tenham o mesmo j-invariante.*

Demonstração: [Sil, pag.50]. □

Proposição 3.1.2 *Seja $\mathcal{C}$ uma cúbica plana, afim, não singular dada por uma equação na forma de Weierstrass. Considere o diferencial:*

$$\omega = \frac{dY}{3X^2 + A} = \frac{dX}{2Y}.$$

Então ω é regular e não se anula em $\mathcal{C}$, isto é, $\mathrm{div}(\omega) = 0$. *Em particular, concluímos que o gênero de $\mathcal{C}$ é 1.*

Demonstração: [Sil, pag.52]. □

3.2 A LEI DE GRUPO GEOMÉTRICA

Sejam $\mathcal{C}$ uma cúbica plana definida sobre um corpo K e $\epsilon \in \mathcal{C}(K)$ um ponto K-racional. Vamos definir, de maneira completamente geométrica, uma estrutura de grupo abeliano em $\mathcal{C}(K)$.
Sejam P e Q pontos (não necessariamente distintos) de $\mathcal{C}(K)$. A reta, unindo esses dois pontos, é claramente definida sobre K e intersecta $\mathcal{C}$, contando com multiplicidade, em um terceiro ponto (não necessáriamente distinto de P ou Q), que vamos denotar R. Se $P = Q$, a reta que os une, por convenção, é a reta tangente a C por P.
Seja S o terceiro ponto na intersecção da reta ligando R a ϵ. Defnimos a operação de grupo de seguinte forma:

$$P \oplus Q := S$$

De nossa definição segue :

$$P \oplus Q = Q \oplus P \ , \ \forall P, Q \in \mathcal{C}(K)$$

$$\epsilon + P = P \ , \ \forall P \in \mathcal{C}(K).$$

Definimos o inverso da seguinte maneira: seja $P \in \mathcal{C}(K)$ e consideremos a reta $T_\epsilon C$ tangente a $\mathcal{C}$ no ponto ϵ. Tal reta intersecta $\mathcal{C}$ num terceiro ponto, que vamos chamar T.
Definimos $-P$ como o terceiro ponto de intersecção da reta que une P a T. Segue diretamente da definição da nossa operação que:

$$P \oplus (-P) = (-P) \oplus P = \epsilon$$

Para mostrar a asociatividade, consideremos dados os pontos: $P_0 = \epsilon$ origem, P_1, P_2 e P_3. Denotamos P_4 o terceiro ponto da interceção da reta l_{124} que liga P_1 a P_2 com $\mathcal{C}$ e $P_5 = P_1 \oplus P_2$. Chamaremos l_{045} a reta que passa por P_0, P_4 e P_5. Denotamos P_6 o terceiro ponto da interceção da reta l_{236} que liga P_2 a P_3 com $\mathcal{C}$ e $P_7 = P_2 \oplus P_3$. Chamaremos l_{067} a reta que passa por P_0, P_6 e P_7. Seja ainda P_8 o terceiro ponto de interceção da reta ligando P_3 a P_5, l_{358} a reta passando por P_3, P_5 e P_8. Finalmente seja P_9 o terceiro ponto de interceção da reta ligando P_1 a P_7, que denotaremos l_{179}. Se mostrarmos que $P_8 = P_9$, a associatividade segue. Para mostrar que $P_8 = P_9$, consideremos o divisor da função racional:

$$f = \frac{l_{124} l_{358} l_{067}}{l_{179} l_{236} l_{045}}$$

Temos que $(f) = (P_8) - (P_9)$ e portanto $P_8 = P_9$, uma vez que $\mathcal{C}$ tem gênero 1.

Teorema 3.2.1 *Sejam $(\mathcal{C}, \epsilon)$ uma cúbica plana definida sobre um corpo K ($car(K) \neq 2$ ou 3) que suporemos na forma de Weierstrass, e seja $\mathrm{Pic}^0_K(\mathcal{C})$ o grupo dos divisores (definidos sobre K) de grau zero, módulo equivalência linear. A aplicação:*

$$\iota : \mathcal{C}(K) \to Pic^0_K(\mathcal{C}) \ , \ P \mapsto (P) - (\epsilon)$$

é um isomorfismo de grupos.

Demonstração: A injetividade é clara, pois, se $\iota(P_1) = \iota(P_2)$, então $(P_1) \sim (P_2)$ e portanto $P_1 = P_2$.
A sobrejetividade pode ser mostrada a partir do teorema de Riemann-Roch. Seja $D \in \mathrm{Pic}^0(\mathcal{C})$ então:

$$\dim(L(D + (\epsilon))) = 1$$

Seja $f \in \bar{K}(\mathcal{C})$ um gerador de $L(D+(\epsilon))$. Como $\mathrm{div}(f) \geq -D-(\epsilon)$, e $\deg(\mathrm{div}(f)) = 0$, existe P tal que:

$$\mathrm{div}(f) = -D - (\epsilon) + (P),$$

isso é equivalente a dizer que:

$$D \sim (P) - (\epsilon).$$

Para mostrar que ι é um homomorfismo, notamos que a curva na forma de Weierstrass tem $\epsilon = (0 : 1 : 0)$, que é um ponto de inflexão. Portanto a colinearidade de três pontos P, Q *e* R é equivalente a $(P) + (Q) + (R) = (3\epsilon)$. Assim temos:

$$(P \oplus Q) \oplus R = \epsilon \Leftrightarrow \iota(P) + \iota(Q) + \iota(R) = 0$$

e, daí, segue nosso resultado. □

Proposição 3.2.2 *Seja $\mathcal{C}$ uma cúbica projetiva lisa na forma de Weierstrass. Então:*

(i) *A lei de grupo em $\mathcal{C}$ é algébrica, isto é, as aplicações de adição e inverso são morfismos entre variedades projetivas.*

(ii) *Se escolhermos outro ponto para elemento identidade por translação, a nova estrutura de grupo é naturalmente isomorfa à antiga.*

(iii) *Se escolhermos para elemento identidade um dos pontos de inflexão da cúbica, a lei de grupo pode ser facilmente descrita da seguinte forma:*

$$P \oplus Q \oplus R = \epsilon \Leftrightarrow P, Q \text{ e } R \text{ sao colineares.}$$

Demonstração: A primeira afirmação depende de um cálculo explícito e pode ser encontada em [Sil, pag.58, 68], enquanto a segunda e a terceira afirmações são claras. □

3.3 CURVAS DE GÊNERO 1

Seja $\mathcal{C}$ uma curva de gênero 1 sobre um corpo K e seja $K_{\mathcal{C}}$ um divisor canônico. Um corolário imediato do Teorema de Riemann-Roch nos diz que $\deg(K_{\mathcal{C}}) = 0$ e $l(K_{\mathcal{C}}) = 1$. Portanto, existe um divisor canônico efetivo cujo grau é 0 e $K_{\mathcal{C}} = 0$.
Seja D um divisor efetivo e não nulo em $\mathcal{C}$. Do teorema de Riemann-Roch, temos:

$$l(D) - l(K_{\mathcal{C}} - D) = \deg(D) - g + 1,$$

$$l(D) - l(-D) = \deg(D).$$

Como $l(-D) = 0$, temos que $l(D) = \deg(D)$.

Teorema 3.3.1 *Seja $\mathcal{C}$ uma curva projetiva lisa de gênero 1 sobre um corpo K e seja $P \in \mathcal{C}(K)$. Então $\mathcal{C}$ é K–isomorfa a uma cúbica plana lisa. Se a característica de K for diferente de 2 e 3, então tal cúbica pode ser tomada na forma de Weierstrass:*

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

e o ponto P é levado por esse isomorfismo no ponto de inflexão (0:1:0).

Demonstração: Considere para cada $n \in \mathbb{N}$ os espaços vetoriais $L(n(P)) = \Gamma(\mathcal{C}, \mathfrak{L}(n(P)))$ cuja dimensão é n. Como $\deg(L(3(P))) \geq 2g+1 = 3$, $L(3(P))$ é muito amplo e portanto induz um mergulho de $\mathcal{C}$ em $\mathbb{P}^2$ como cúbica plana. Explicitamente, existem duas funções x e y em $K(\mathcal{C})$ tais que:

$$L((P)) \simeq K \ , \ L(2(P)) \simeq K \oplus Kx \text{ e } L(3(P)) \simeq K \oplus Kx \oplus Ky.$$

As funções $1, x, x^2, x^3, y, xy, y^2 \in L(6(P))$, que é um espaço vetorial cuja dimensão é 6. Logo, tais funções são linearmente dependentes e, portanto, existe um polinômio do terceiro grau f tal que $f(x, y) = 0$ (o mergulho acima descrito é dado por $(x : y : 1)$ e, portanto, $\deg(f) = 3$). Os monômios x^2 e y^3 devem aparecer em f porque tais funções são as unicas que têm um pólo de ordem 6. □

Definição 3.3.2 *Uma Curva Elíptica é um par $(\mathcal{C}, \epsilon)$ onde $\mathcal{C}$ é uma curva projetiva lisa de gênero 1 e ϵ um ponto distinguido de $\mathcal{C}$. Dizemos que a curva elíptica é definida sobre K, se $\mathcal{C}$ é definida sobre K e $\epsilon \in \mathcal{C}(K)$.*

Teorema 3.3.3 *Seja $\mathcal{C}$ uma curva projetiva lisa de gênero 1, então existe uma única (a menos de K-isomorfismo) curva elíptica definida sobre K, chamada jacobiana de $\mathcal{C}$ e denotada* $\mathrm{Jac}(\mathcal{C})$ *e um $\bar{K}$-isomorfismo:*

$$\iota : \mathcal{C} \to \mathrm{Jac}(\mathcal{C})$$

(ι em geral não pode ser escolhido K-isomorfismo).
A curva $\mathrm{Jac}(\mathcal{C})$ *age de maneira simples, transitiva e algébrica sobre $\mathcal{C}$.*

Demonstração: Seja $P \in \mathcal{C}(\bar{K})$ e considere então a curva elíptica com origem em P, que vamos chamar $\mathcal{C}^*$ (definida sobre $\bar{K}$ a priori). Então, obtemos um $\bar{K}$-isomorfismo natural: $\Phi : \mathcal{C} \to \mathcal{C}^*$. Fazendo agir o grupo de Galois, obtemos: $\sigma(\Phi) : \mathcal{C} \to \sigma(\mathcal{C}^*)$ (observamos que $\mathcal{C}$ é definida sobre K). Por outro lado, como $\mathcal{C}^*$ e $\sigma(\mathcal{C}^*)$ são $\bar{K}$-isomorfas, temos:

$$\sigma(j(\mathcal{C}^*)) = j(\sigma(\mathcal{C}^*)) = j(\mathcal{C}^*)$$

daí $j(\mathcal{C}^*) \in K^*$ e, portanto, a menos de mudança de variáveis, podemos supor, sem perda de generalidade, que $\mathcal{C}^*$ seja definida sobre K.

Para mostrar que existe uma tal $\mathcal{C}^*$ que age em $\mathcal{C}$ e que a ação satisfaz as propriedades requeridas, pode-se fazer diretamente usando certas mudanças de coordenadas como é feito em [Ca, pag.106], ou usar cohomologia de grupos. □

3.4 EXISTÊNCIA DE PONTOS K-RACIONAIS

Para entender a aritmética de uma curva de gênero um, definida sobre um corpo K, é interessante nos utilizarmos da estrutura de grupo abeliano e, assim, considerar a curva elíptica associada. Entretanto, toda construção foi baseada na hipótese da existência de um ponto K-racional $\epsilon \in \mathcal{C}(K)$. Para nossa descrição ser completa, vamos dar um critério para existência de um tal ponto.

Definição 3.4.1 *Seja $\mathcal{C}$ uma curva projetiva lisa, definida sobre um corpo K. Um twist de $\mathcal{C}$ é uma curva $\tilde{\mathcal{C}}$, definida sobre K, que é $\bar{K}$ isomorfa a $\mathcal{C}$. Denotaremos* $\mathrm{Twist}_K(\mathcal{C})$ *o conjunto dos twists de $\mathcal{C}$ módulo K-isomorfismos,* $\mathrm{Isom}(\mathcal{C})$ *o grupo (não necessariamente abeliano) dos $\bar{K}$-isomorfismos entre $\mathcal{C}$ com ela mesma e* $\mathrm{Isom}_K(\mathcal{C})$ *o grupo dos K-isomorfismos.*

Teorema 3.4.2 *Seja $\mathcal{C}$ uma curva projetiva lisa definida sobre K. Para cada twist $\tilde{\mathcal{C}}$ de $\mathcal{C}$, considere um $\bar{K}$-isomorfismo $\Phi : \tilde{\mathcal{C}} \to \mathcal{C}$.*
Definindo:

$$\xi : \mathrm{Gal}(\bar{K}|K) \to \mathrm{Isom}(C) \ , \ \sigma \mapsto \xi_\sigma := \sigma(\Phi) \circ \Phi^{-1}$$

temos:

(i) *ξ é um 1-cociclo.*

(ii) *A classe de cohomologia de ξ é determinada por pela classe de K-isomorfismos de $\tilde{\mathcal{C}}$ e, portanto, obtemos uma aplicação natural:*

$$\mathrm{Twist}_K(\mathcal{C}) \to H^1(\mathrm{Gal}(\bar{K}|K), \mathrm{Isom}(\mathcal{C})).$$

(iii) *A aplicação dada em (ii) é uma bijeção.*

Demonstração: (i) $\xi_{\sigma\tau} := \sigma\tau(\Phi) \circ \Phi^{-1} = \tau(\sigma(\Phi) \circ \Phi^{-1}) \circ (\tau(\Phi) \circ \Phi^{-1}) = \tau(\xi_\sigma)\xi_\tau$
(ii) Sejam $\tilde{\mathcal{C}}_1$ e $\tilde{\mathcal{C}}_2$ dois *twists* de $\mathcal{C}$ que sejam K-isomorfos. Consideremos agora $\Phi_i : \tilde{\mathcal{C}}_i \to \mathcal{C}$, $i = 1, 2$ $\bar{K}$-isomorfismos e um K-isomorfismo $\theta : \tilde{\mathcal{C}}_2 \to \tilde{\mathcal{C}}_1$. Devemos mostrar que os cociclos $\sigma(\Phi_1) \circ \Phi_1^{-1}$ e $\sigma(\Phi_2) \circ \Phi_2^{-1}$ são cohomólogos. Ora, o elemento $\alpha = \Phi_1 \circ \theta \circ \Phi_2^{-1} \in \mathrm{Isom}\,\mathcal{C}$, daí vê-se que:

$$\sigma(\alpha) \circ (\sigma(\Phi_2) \circ \Phi_2^{-1}) = (\sigma(\Phi_1) \circ \Phi_1^{-1}) \circ \alpha.$$

(iii) [Sil, pag.285]. □

Definição 3.4.3 *Seja $(\mathcal{C}, \epsilon)$ um curva elíptica definida sobre K. Um espaço homogêneo (principal) para $\mathcal{C}$ é uma curva lisa $\tilde{\mathcal{C}}$ sobre a qual $\mathcal{C}$ age de maneira simples, transitiva e algébrica, isto é, existe um morfismo definido sobre K:*

$$\mu : \mathcal{C} \times_K \tilde{\mathcal{C}} \to \tilde{\mathcal{C}}$$

satisfazendo as propriedades:

(i) $\mu(p, \epsilon) = p$.

(ii) $\mu(\mu(p, P), Q) = \mu(p, P \oplus Q)$.

(iii) *Dados $p, q \in \tilde{\mathcal{C}}$, existe um único $P \in \mathcal{C}$ tal que $\mu(p, P) = Q$.*

A partir da definição acima vemos que existe uma aplicação:

$$\nu : \tilde{\mathcal{C}} \times \tilde{\mathcal{C}} \to \mathcal{C}$$

dada por $\nu(p, q) = P$ em que P é o único ponto tal que $\mu(p, P) = q$

Proposição 3.4.4 *Sejam $\mathcal{C}$ uma curva elíptica sobre K e $\tilde{\mathcal{C}}$ um espaço homogêneo para $\mathcal{C}$. Definindo (fixando $p_0 \in \tilde{\mathcal{C}}$):*

$$\theta : \mathcal{C} \to \tilde{\mathcal{C}} \ , \ P \mapsto \mu(p_0, P)$$

obtemos que:

(i) *θ é um isomorfismo definido sobre $K(p_0)$. Em particular $\tilde{\mathcal{C}}$ é um twist de $\mathcal{C}$.*

(ii) *Se $p \in \tilde{\mathcal{C}}$ e $P \in \mathcal{C}$ então:*

$$\mu(p, P) = \theta(\theta^{-1}(p) \oplus P).$$

(iii) *Se $p, q \in \tilde{\mathcal{C}}$, então:*

$$\nu(q, p) = \theta^{-1}(q) \oplus (-\theta^{-1}(p)).$$

(iv) *A aplicação ν é um K-morfismo.*

Demonstração: (i) É claro que θ é um $K(p_0)$-morfismo, por outro lado como a ação de $\mathcal{C}$ é simples, transitiva, θ tem grau 1 e, por isso, é um isomorfismo.
(ii) $\theta(\theta^{-1}(p) \oplus P) = \mu(p_0, \theta^{-1}(p) \oplus P) = \mu(p, P)$.
(iii) $\theta^{-1}(q) \oplus (-\theta^{-1}(p)) = \nu(\mu(p_0, \theta^{-1}(q)), \mu(p_0, \theta^{-1}(p))) = \nu(q, p)$.
(iv) O fato de ν ser um morfismo segue de (iii), para mostrar que é definido sobre K, devemos mostrar que é $\mathrm{Gal}(\bar{K}|K)$ invariante. De fato:

$$\sigma(\nu(q, p)) = \sigma(\theta^{-1}(q) - \theta^{-1}(p)) = \sigma(\theta^{-1}(q)) - \sigma(\theta^{-1}(p))$$

$$= \nu\{\sigma[\mu(p_0, \theta^{-1}(q))], \sigma[\mu(p_0, \theta^{-1}(p))]\} = \nu(\sigma(q), \sigma(p)).$$

□

Definição 3.4.5 *Sejam $\mathcal{C}$ uma curva elíptica e $\tilde{\mathcal{C}}_1$ e $\tilde{\mathcal{C}}_2$, dois espaços homogêneos para $\mathcal{C}$. Dizemos que $\tilde{\mathcal{C}}_1$ e $\tilde{\mathcal{C}}_2$ são equivalentes se existir um K-isomorfismo $\theta : \tilde{\mathcal{C}}_2 \to \tilde{\mathcal{C}}_1$ que seja compatível com a ação de $\mathcal{C}$.*
A classe de equivalência contendo $\mathcal{C}$, agindo em si própria por translações, é chamada classe trivial.

Proposição 3.4.6 *Sejam $\mathcal{C}$ uma curva elíptica sobre K e $\tilde{\mathcal{C}}$ um espaço homogêneo para $\mathcal{C}$. Uma condição necessária e suficiente para que $\tilde{\mathcal{C}}$ esteja na classe trivial é que $\tilde{\mathcal{C}}(K) \neq \emptyset$*

Demonstração: Se $\tilde{\mathcal{C}}$ está na classe trivial, então existe um K-isomorfismo $\theta : \mathcal{C} \to \tilde{\mathcal{C}}$ e portanto $\theta(\epsilon) \in \tilde{\mathcal{C}}(K)$. Reciprocamentre, seja $p_0 \in \tilde{\mathcal{C}}(K)$, então, pela proposição anterior, a aplicação $\theta : \mathcal{C} \to \tilde{\mathcal{C}}$ dada por $\theta(P) = \mu(p_0, P)$ é um isomorfismo definido sobre $K(p_0) = K$ e claramente compatível. □

Vamos denotar por $\mathrm{WC}_K(\mathcal{C})$ o conjunto das classes de equivalência de espaços homogêneos para $\mathcal{C}$ e a partir da próxima proposição vamos dar-lhe uma estrutura de grupo. Ele é chamado grupo de Weil-Châtelet.

Proposição 3.4.7 *Seja $\mathcal{C}$ uma curva elíptica sobre um corpo K. Então existe uma bijeção natural:*

$$\mathrm{WC}_K(\mathcal{C}) \to H^1(\mathrm{Gal}(\bar{K}|K), \mathcal{C}),$$

definida da seguinte forma, se $\tilde{\mathcal{C}}$ é um espaço homogêneo para $\mathcal{C}$, e $p_0 \in \tilde{\mathcal{C}}$, então:

$$[\tilde{\mathcal{C}}] \mapsto [\sigma \mapsto \sigma(p_0) - p_0].$$

Demonstração: [Sil, pag.291]. □

Teorema 3.4.8 *Sejam $\tilde{\mathcal{C}}$ um espaço homogêneo para uma curva elíptica $\mathcal{C}$ definida sobre um corpo K e $p_0 \in \tilde{\mathcal{C}}$ um ponto. Consideremos a aplicação:*

$$\begin{array}{rccc} \mathrm{sum}: & \mathrm{Div}^0(\tilde{\mathcal{C}}) & \to & \mathcal{C} \\ & \sum n_i(p_i) & \mapsto & \sum [n_i](p_i - p_0) \end{array}$$

então temos:

(i) *uma sequência exata:*

$$1 \to \bar{K}^* \to \bar{K}(\tilde{\mathcal{C}})^* \to \mathrm{Div}^0(\tilde{\mathcal{C}}) \to \mathcal{C} \to 0.$$

(ii) sum *independe de p_0 e comuta com a ação de* $\mathrm{Gal}(\bar{K}|K)$ *em* $\mathrm{Div}^0(\mathcal{C}^*)$

(iii) *do teorema do isomorfismo:*

$$\mathrm{sum} : \mathrm{Pic}^0(\mathcal{C}^*) \simeq \mathcal{C}$$

e em particular:

$$\mathrm{Pic}^0_K(\mathcal{C}^*) \simeq \mathcal{C}(K).$$

3.5 ISOGENIAS E O ANEL DE ENDOMORFISMOS

Definição 3.5.1 *Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ curvas elípticas. Uma isogenia entre $\mathcal{C}_1$ e $\mathcal{C}_2$ é um morfismo:*

$$\Phi : \mathcal{C}_1 \to \mathcal{C}_2$$

satisfazendo $\Phi(\epsilon_1) = \epsilon_2$

Estamos admitindo $\Phi = [0]$, o morfismo nulo, como isogenia em favor de uma estrutura de anel, a posteriori, na definição clássica, tal morfismo não seria considerado isogenia. No capítulo sobre variedades abelianas, voltaremos a falar sobre isogenias. Notemos também que os morfismos de multiplicação por n são isogenias de grau n^2.

Proposição 3.5.2 *Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ curvas elípticas e consideremos uma isogenia não nula entre $\mathcal{C}_1$ e $\mathcal{C}_2$:*

$$\Phi : \mathcal{C}_1 \to \mathcal{C}_2.$$

Então:

(i) Φ *é um morfismo sobrejetivo que é de fato um homomorfismo cujo núcleo é finito.*

(ii) $\sharp \ker \Phi = \deg(\Phi)$.

(iii) *Existe uma única isogenia:*

$$\hat{\Phi} : \mathcal{C}_2 \to \mathcal{C}_1$$

satisfazendo:

$$\hat{\Phi} \circ \Phi = [m] \ e \ \ \Phi \circ \hat{\Phi} = [m],$$

em que $m = \deg(\Phi)$. *Tal isogenia é chamada isogenia dual.*

Demonstração: [Sil, pag.71]. □

A partir dessa proposição, faz sentido considerar o grupo

$$\mathrm{Hom}(\mathcal{C}_1, \mathcal{C}_2) := \{isogenias \ \Phi : \mathcal{C}_1 \to \mathcal{C}_2\}$$

$$\mathrm{End}(\mathcal{C}) := \mathrm{Hom}(\mathcal{C}, \mathcal{C})$$

Por outro lado, a $\mathrm{End}(\mathcal{C})$ podemos dar uma estrutura natural de anel fazendo a composição como multiplicação. Nesse anel definimos:

$$\mathrm{Aut}(\mathcal{C}) := \mathrm{End}(\mathcal{C})^*.$$

Proposição 3.5.3 *Sejam $\mathcal{C}_1$, $\mathcal{C}_2$ e $\mathcal{C}_3$ curvas elípticas, e $\phi : \mathcal{C}_1 \to \mathcal{C}_2$, $\lambda : \mathcal{C}_2 \to \mathcal{C}_3$ e $\psi : \mathcal{C}_1 \to \mathcal{C}_2$ isogenias. Então a isogenia dual satisfaz:*

$$\widehat{(\lambda \circ \phi)} = \hat{\phi} \circ \hat{\lambda}$$

$$\widehat{(\phi + \psi)} = \hat{\phi} + \hat{\psi}$$

$$\widehat{(\hat{\phi})} = \phi$$

Demonstração: [Sil, pag.86]. □

Proposição 3.5.4 *Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ curvas elípticas. A aplicação grau:*

$$\deg : \mathrm{Hom}(\mathcal{C}_1, \mathcal{C}_2) \to \mathbb{Z}$$

é uma forma quadrática, definida positiva.

Demonstração: *Quanto a ser definida positiva, é claro, para mostar que é uma forma quadrática, devemos apenas mostrar ser bilinear a aplicação:*

$$\begin{array}{rccc} < , >: & \mathrm{Hom}(\mathcal{C}_1, \mathcal{C}_2) \times \mathrm{Hom}(\mathcal{C}_1, \mathcal{C}_2) & \to & \mathbb{Z} \\ & (\phi, \psi) & \mapsto & \deg(\phi + \psi) - \deg(\phi) - \deg(\psi) \end{array}$$

mas usando a injeção natural:

$$[\ ] : \mathbb{Z} \hookrightarrow \mathrm{End}(\mathcal{C}_1)$$

temos:

$$\begin{aligned} [< \phi, \psi >] &= [\deg(\phi + \psi)] - [\deg(\phi)] - [\deg(\psi)] \\ &= (\phi \hat{+} \psi) \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ &= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi \end{aligned}$$

e, portanto, a bilinearidade segue da proposição anterior. □

3.6 CURVAS ELÍPTICAS SOBRE CORPOS FINITOS

Seja $\mathbb{F}_q$ um corpo finito de característica p, $q = p^e$. Consideremos uma curva elíptica $\mathcal{C}$ definida sobre $\mathbb{F}_q$. Podemos garantir a existência de um modelo na forma de Weierstrass só se considerarmos $p \neq 2$ ou 3. No caso geral, entretanto, é sempre possível encontrar um mergulho em $\mathbb{P}^2$ que seja uma cúbica da forma:

$$ZY^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2ZX^2 + a_4XZ^2 + a_6Z^3.$$

Nosso objetivo nessa seção é dar a estimativa de Hasse para o número de pontos $\mathbb{F}_q$-racionais e mostrar que $\mathcal{C}(\mathbb{F}_q) \neq \emptyset$ para qualquer curva lisa de gênero um, assim sendo, qualquer curva de gênero um sobre um corpo finito é uma curva elíptica.

Definição 3.6.1 *O morfismo de Frobenius é definido por:*

$$\Phi : \mathcal{C} \to \mathcal{C}$$

onde $(x, y) \mapsto (x^q, y^q)$.

Lema 3.6.2 *Seja* $\Phi : \mathcal{C} \to \mathcal{C}$ *o morfismo de Frobenius entre curvas elípticas sobre* $\mathbb{F}_q$. *Então:*

(i) Φ *é puramente inseparável de grau* q.

(ii) $1 - \Phi$ *é separável.*

Demonstração: [Sil, pag.30,83]. □

Teorema 3.6.3 *Seja* $\mathcal{C}$ *uma curva de gênero 1 definida sobre* $\mathbb{F}_q$. *Então* $\mathcal{C}$ *possui um ponto* $\mathbb{F}_q$*-racional.*

Demonstração: Considere $\mathrm{Jac}(\mathcal{C})$ a jacobiana de $\mathcal{C}$. A curva $\mathcal{C}$ é um espaço homogêneo para $\mathrm{Jac}(\mathcal{C})$, pela proposição 3.3.3. Se mostrarmos que:

$$H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q \,|\, \mathbb{F}_q), \mathrm{Jac}(\mathcal{C})) = 0,$$

então, pela proposição 3.4.6, concluiremos que $\mathcal{C}(\mathbb{F}_q) \neq \emptyset$.

Lembramos que o grupo $\mathrm{Gal}(\bar{\mathbb{F}}_q \,|\, \mathbb{F}_q)$ é topologicamente gerado pelo automorfismo de Frobênius. Vamos mostrar que qualquer cociclo $\{a_0\}$ é trivial e, para isso, devemos encontrar $b \in \mathrm{Jac}(\mathcal{C})$ tal que $a_\sigma = \sigma(b) - b$. Mas, quando σ é o Frobênius, temos que $\sigma(b) - b = (1 - \Phi)b$, em que Φ é o Frobênius geométrico. Como $1 - \Phi$ é sobrejetiva (pois não é constante), nosso resultado segue imediatamente. □

Lema 3.6.4 *Sejam A um grupo abeliano e:*

$$d : A \to \mathbb{Z}$$

uma forma quadrática positiva definida. Então para todos $\psi, \phi \in A$ temos:

$$|d(\psi - \phi) - d(\psi) - d(\phi)| \leq 2\sqrt{d(\psi)d(\phi)}.$$

Demonstração: Seja $B(\psi, \phi) = d(\psi - \phi) - d(\psi) - d(\phi)$, que é uma forma bilinear pela definição de d ser uma forma quadrática. Como d é positiva definida, temos para cada $m, n \in \mathbb{Z}$:

$$0 \leq d(m\psi - n\phi) = m^2 d(\psi) + mnB(\psi, \phi) + n^2 d(\phi).$$

Em particular, tomando $m = -B(\psi, \phi)$ e $n = 2d(\psi)$, temos:

$$0 \leq d(\psi)[4d(\psi)d(\phi) - B(\psi, \phi)^2].$$

Claramente se $\psi = 0$, a desigualdade é trivial; caso contrário, como d é positiva definida, segue nosso resultado. □

Teorema 3.6.5 (**Estimativa de Hasse**) *Seja $\mathcal{C}$ uma curva elíptica definida sobre $\mathbb{F}_q$. Então:*

$$|\sharp\mathcal{C}(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Demonstração: Lembrando que o grupo de Galois $\mathrm{Gal}(\bar{\mathbb{F}}_q|\mathbb{F}_q)$ é topologicamente gerado por Φ, "o Frobenius da extensão", temos:

$$P \in \mathcal{C}(\mathbb{F}_q) \Leftrightarrow \Phi(P) = P.$$

Então:

$$\mathcal{C}(\mathbb{F}_q) = \ker(1 - \Phi)$$

e, portanto,

$$\sharp\mathcal{C}(\mathbb{F}_q) = \sharp\ker(1-\Phi) = \deg(1-\Phi),$$

pois $1-\Phi$ é separável pelo lema 3.6.2. Por outro lado, sabemos que a aplicação $\deg : \mathrm{End}(\mathcal{C}) \to \mathbb{Z}$ é uma forma quadrática definida positiva pela proposição 3.5.4, e $\deg(\Phi) = q$ pelo lema 3.6.2. Nosso resultado segue imediatamente do lema 3.6.4. □

3.7 CURVAS ELÍPTICAS SOBRE CORPOS DE NÚMEROS

A motivação aritmética histórica dos estudos de curvas elípticas reside na busca de soluções inteiras e racionais de cúbicas planas. O principal resultado sobre o conjunto dos pontos $\mathbb{Q}$-racionais de tais curvas é o teorema de Mordell garantindo que tal conjunto é um grupo abeliano finitamente gerado.
De fato, temos a seguinte generalização do teorema de Mordell, devida a Weil, mas relacionada à demonstração original.

Teorema 3.7.1 (**Mordell-Weil**) *Sejam K um corpo de números e $\mathcal{C}$ uma curva elíptica sobre K. Então, o grupo abeliano dos pontos K-racionais de $\mathcal{C}$, $\mathcal{C}(K)$ é finitamente gerado.*

Demonstração: Esse teorema é um caso particular do teorema de Mordell-Weil, demonstrado por Weil, que iremos mostrar na seção intitulada O teorema de Mordell-Weil, 6.3.1. A demonstração será dividida em três partes completamente independentes uma das quais, chamada teorema fraco de Mordell-Weil □

Agora vamos dar uma demonstração explícita, no caso de curvas elípticas sobre os raconais, do teorema fraco de Mordell, para isso vamos fazer uma hipótese adicional de que a curva na forma de Weierstrass seja da forma $Y^2 = f(X)$, em que $f(X)$ seja irredutível

Teorema 3.7.2 (**Mordell**) *Seja $\mathcal{C}$ uma curva elíptica definida sobre $\mathbb{Q}$ dada por uma equação na forma de Weierstrass:*

$$Y^2 = f(X) = X^3 + AX + B$$

em que suporemos $f(X) \in \mathbb{Q}[X]$ irredutível. Então $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ é um grupo finito.

Demonstração: Sejam $\mathbb{Q}(\theta) = \mathbb{Q}[X]/(f(X))$, $\mathfrak{G} := \mathcal{C}(\mathbb{Q})$ e $\mathfrak{H} < \mathbb{Q}(\theta)^*/(\mathbb{Q}(\theta)^*)^2$ o subgrupo dos elementos de norma quadrada. Vamos definir um homomorfismo:

$$\mu : \mathfrak{G} \to \mathfrak{H}$$

da seguinte maneira. Se $P = (a, b)$ (afim), $\mu(P) = (a-\theta)(\mathbb{Q}(\theta)^*)^2$. Para mostrar que μ é um homomorfismo de grupos, sejam P_1, P_2 *e* P_3 pontos colineares, pertencentes a reta $Y = lX + m$. Então: $P_1 \oplus P_2 \oplus P_3 = \epsilon$, fazendo $P_j = (a_j, b_j)$, temos:

$$(a_1 - \theta)(a_2 - \theta)(a_3 - \theta) = (l\theta + m)^2$$

Daí, é fácil ver que:

$$N_{\mathbb{Q}(\theta)|\mathbb{Q}}(a_j - \theta) = f(a_j) = b_j^2$$

e temos assim:

$$\mu(P_1)\mu(P_2)\mu(P_3) = (a_1 - \theta)(a_2 - \theta)(a_3 - \theta) \mod (\mathbb{Q}(\theta)^*)^2$$

Desta feita, mostramos que:

$$\mu(P_1)\mu(P_2)\mu(P_3) = 1$$

Agora vamos mostrar que $\ker(\mu) = 2\mathfrak{G}$. De fato, $\mu(2P) = (\mu(P))^2 = 1$, logo $2\mathfrak{G} \subset \ker(\mu)$. Reciprocamente, seja $P = (a, b) \in \ker(\mu)$, então:

$$a - \theta = (p_2\theta^2 + p_1\theta + p_0)^2.$$

Da invertibilidade de $a - \theta$, temos:

$$(s_0 - \theta)(p_2\theta^2 + p_1\theta + p_0) = (r_1\theta + r_0)$$

$$(s_0 - \theta)^2(a - \theta) = (r_1\theta + r_0)^2.$$

Considere o polinômio:

$$(r_1X + r_0)^2 - (s_0 - X)^2(a - X) = f(X).$$

Temos que a reta $Y = r_1X + r_0$ intersecta nossa curva em $(a, \pm b)$ e em (s_0, t) com multiplicidade dois para algum t. Logo $(a, b) \in 2\mathfrak{G}$.

Se mostrarmos que $\mathfrak{G}/2\mathfrak{G} \simeq \mathrm{Im}(\mu)$ é finito, o resultado segue. Podemos supor que $A, B \in \mathbb{Z}$. Seja $P = (a, b) \in \mathfrak{G}$, sejam $\varepsilon_1, \varepsilon_2, \varepsilon_3$ as três raízes distintas de f e $a = \frac{r}{t^2}$ e $b = \frac{s}{t^3}$. Como

$$s^2 = (r - \varepsilon_1 t^2)(r - \varepsilon_2 t^2)(r - \varepsilon_3 t^2)$$

em $\mathcal{O}_{\mathbb{Q}(\varepsilon_1,\varepsilon_2,\varepsilon_3)}$ temos pela fatoraçõa única de ideais:

$$< s^2 >=< r-\varepsilon_1 t^2 >< r-\varepsilon_2 t^2 >< r-\varepsilon_3 t^2 > .$$

Claramente:

$$< r-\varepsilon_i t^2, r-\varepsilon_j t^2 > | < r-\varepsilon_i t^2 > \ e \ < r-\varepsilon_j t^2 > .$$

Então:

$$< r-\varepsilon_i t^2, r-\varepsilon_j t^2 > | < \varepsilon_i - \varepsilon_j >$$

fazendo $< r-\varepsilon_j t^2 >= I_j J_j^2$, temos que:

$$I_j | < \varepsilon_1 - \varepsilon_2 >< \varepsilon_1 - \varepsilon_3 >< \varepsilon_2 - \varepsilon_3 >$$

e $I_1 I_2 I_3$ é quadrado. Pela finitude do número de classes de ideais, segue nosso resultado. □

Lembramos que se A é um DIP (Domínio de Ideais Principais), todo A-módulo livre de torção é livre e, portanto, todo grupo abeliano finitamente gerado G pode ser (abstratamente) descrito da forma:

$$G \simeq G_{\text{tor}} \bigoplus \mathbb{Z}^{\oplus r},$$

em que G_{tor} é a parte de torção de G, necessariamente finita e $r = \text{rk}(G)$ é o posto de G. No caso de uma curva elíptica sobre $\mathbb{Q}$, a torção é completamente conhecida. Quanto ao posto, faz parte de uma importante conjectura de Birch e Swinnerton-Dyer, sobre a qual não falaremos.

3.8 EXEMPLO DE SELMER

Foi visto que, para curvas de gênero 0 sobre um corpo de números K, vale um princípio para a existência de pontos K racionais, denominado princípio local-global, assegurando a existência de tais pontos, quando estas curvas admitem pontos em todos os completamentos de K (com respeito aos *Places* de K). Para curvas de gênero positivo, o princípio não vale em geral. O primeiro contra-exemplo do princípio foi obtido por Selmer,em [Sel], e é a cúbica plana não singular de equação(homogênea):

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

Vamos mostrar primeiramente que essa curva não possui ponto $\mathbb{Q}$–racional e, posteriormente mostraremos a existência de pontos localmente em $\mathbb{Q}_p$ para cada primo p. Claramente existem pontos reais.

Lema 3.8.1 *Sejam $a, b, c \in \mathbb{Z}$ números inteiros maiores que 1, tais que $d := abc$ é livre de cubos. Consideremos as cúbicas projetivas dadas pelas equações:*

$$C_1 : \ aX^3 + bY^3 + cZ^3 = 0$$

$$C_2 : \ X^3 + Y^3 + dZ^3 = 0.$$

Se $C_1(\mathbb{Q}) \neq \emptyset$ temos que $C_2(\mathbb{Q}) \cap \mathcal{U}_Z \neq \emptyset$, em que $\mathcal{U}_Z$ é o aberto principal dos pontos tais que: $z \neq 0$

Demonstração: Sejam ω uma raiz cúbica primitiva da unidade e $(u : v : w) \in C_1(\mathbb{Q})$. Sem perda de generalidade, vamos supor $u, v, w \in \mathbb{Z}$. Defina:

$$\xi := au^3 + \omega bv^3 + \omega^2 cw^3$$

$$\eta := au^3 + \omega^2 bv^3 + \omega cw^3.$$

Então:

$$\xi + \eta = 3au^3,$$
$$\omega\xi + \omega^2\eta = 3cw^3,$$
$$\omega^2\xi + \omega\eta = 3bv^3.$$

Portanto, fazendo $\mu = -3uvw \in \mathbb{Z}$ obtemos:

$$\xi^3 + \eta^3 + d\mu^3 = 0.$$

Logo, os pontos $P_1 = (\xi : \omega\eta : \mu)$ e $P_2 = (\eta : \omega\xi : \mu)$ são pontos $\mathbb{Q}(\omega)$ racionais, isto é, pertencem a $C_2(\mathbb{Q}(\omega))$ e são conjugados sobre $\mathbb{Q}$. Se considerarmos a reta que liga P_1 a P_2, dada por $Z - \mu = 0$, sabemos que ela deve encontrar C_2 em outro ponto P_3. Como P_1 e P_2 são conjugados, o automorfismo não trivial de $\mathrm{Gal}(\mathbb{Q}(\omega)|\mathbb{Q}))$ deixa P_3 invariante (pois permuta apenas P_1 e P_2) e podemos concluir que $P_3 \in C_2(\mathbb{Q}) \cap \mathcal{U}_Z$.

□

Lema 3.8.2 *Seja $a \geq 3$ um inteiro livre de cubos e considere a curva elíptica dada pela equação:*

$$\mathcal{C} : X^3 + Y^3 - aZ^3 = 0$$

e com origem em $(1 : -1 : 0)$. Então, não existe ponto de torção $\mathbb{Q}$-racional de $\mathcal{C}$.

Demonstração: Seja $P_0 = (x_0 : y_0 : z_0)$ um ponto $\mathbb{Q}$-racional de $\mathcal{C}$, sem perda de generalidade, podemos supor $x_0, y_0, z_0 \in \mathbb{Z}$ e que $\mathrm{m.\,d.\,c.}(x_0, y_0, z_0) = 1$. Pela equação de $\mathcal{C}$ observa-se que tal condição implica que x_0, y_0, z_0 são dois a dois coprimos.
Consideremos $P_1 = (x_1 : y_1 : z_1)$ como sendo o terceiro ponto da intersecção da reta tangente a $\mathcal{C}$ em P_0. Sem perda de generalidade vamos supor que $x_1, y_1, z_1 \in \mathbb{Z}$ e que $\mathrm{m.\,d.\,c.}(x_1, y_1, z_1) = 1$. Notamos que:

$$P_1 = (x_0(x_0^3 + 2y_0^3) : -y_0(2x_0^3 + y_0^3) : z_0(x_0^3 - y_0^3)).$$

Seja $d = \mathrm{m.\,d.\,c.}(x_0(x_0^3 + 2y_0^3), -y_0(2x_0^3 + y_0^3), z_0(x_0^3 - y_0^3))$. Se $d = 1$, então $z_1 = \pm z_0(x_0^3 - y_0^3)$ daí $|z_1| > |z_0|$. Se $d \neq 1$, seja $p \,|\, d$ um fator primo de d. Se $p \,|\, x_0$, então $p \,|\, y_0$ que é um absurdo. Portanto $d \,|\, (x_0^3 + 2y_0^3)$ e $d \,|\, (2x_0^3 + y_0^3)$ e daí $d \,|\, 3x_0^3$ e $d \,|\, 3y_0^3$. Conclusão: $d = 3$ assim $z_1 = \pm z_0(x_0^3 - y_0^3)/3$ e novamente $|z_1| > |z_0|$.
Indutivamente podemos, assim, construir, pelo processo da tangente, uma sequência de pontos $P_0, P_1, ...$ todos distintos, em que $P_{i+1} = -2P_i$ e, portanto, P_0 não é de torção. □

Lema 3.8.3 *Consideremos a curva elíptica $\mathcal{C}$ dada por:*

$$X^3 + Y^3 + 60Z^3 = 0$$

que é birracionalmente equivalente à curva elíptica dada por:

$$Y^2 = X^3 - 3^3(30)^2.$$

Então, o grupo $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ é trivial.

Demonstração: Vamos considerar $\delta^3 = 30$ e $\rho^3 = 1$. Em $\mathbb{Q}(\delta)$, o número de classes de ideais é 3 e uma unidade fundamental é $\eta = 1 + 9\delta - 3\delta^2$. As raízes de $f(X) = X^3 - 3^3(30)^2$ são $3\delta^2$, $3\rho\delta^2$ e $3\rho\delta^2$. Seja $P = (\frac{r}{t^2}, \frac{s}{t^3}) \in \mathcal{C}(\mathbb{Q})$, qualquer ideal primo dividindo dois dos ideais: $< r - 3\delta^2 t^2 >$, $< r - 3\rho\delta^2 t^2 >$ e $< r - 3\rho^2\delta^2 t^2 >$ deve

dividir $2 \cdot 3 \cdot 5$ e, portanto, uma vez que 2, 3 e 5 ramificam, temos que $< r - 3\delta^2 t^2 >$ deve ser um ideal quadrado perfeito. Existem agora apenas duas possibilidades: $r - 3\delta^2 t^2 = \alpha^2$, que é o resultado desejado ou $r - 3\delta^2 t^2 = \eta\alpha^2$ que é descartada, equacionando os coeficientes, após fazer $\alpha = u + v\delta + w\delta^2$ e perceber que a igualdade é impossível em $\mathbb{Q}_2$. Detalhes em [Ca, pag.72] □

Proposição 3.8.4 *Considere a curva elíptica $\mathcal{C}$ definida sobre $\mathbb{Q}$ e dada por $3X^3 + 4Y^3 + 5Z^3 = 0$. Então, $\mathcal{C}$ não possui ponto $\mathbb{Q}$-racional, isto é, $\mathcal{C}(\mathbb{Q}) = \emptyset$*

Demonstração: Suponhamos que $\mathcal{C}(\mathbb{Q}) \neq \emptyset$, então, pelo lema 3.8.1, deveríamos ter um ponto $\mathbb{Q}$-racional em $\mathcal{C}_2$, dada por: $X^3 + Y^3 + 60z^3 = 0$ com $Y \neq 0$. Pelos lemas 3.8.2 e 3.8.3, sabemos que o grupo $\mathcal{C}_2(\mathbb{Q})$ é livre e como $\mathcal{C}_2(\mathbb{Q})/2\mathcal{C}_2(\mathbb{Q})$ é trivial, $\mathrm{rk}(\mathcal{C}_2(\mathbb{Q})) = 0$ daí $\mathcal{C}_2(\mathbb{Q}) = 0$ e, portanto, o único ponto $\mathbb{Q}$-racional de $\mathcal{C}_2$ é $(1 : -1 : 0)$ que é uma contradição. □

Vamos agora mostrar a existência de pontos $\mathbb{Q}_p$-racionais para cada primo p.

Proposição 3.8.5 *Seja $p \neq 2, 3$ ou 5 um primo, então existem pontos $\mathbb{Q}_p$ racionais em $\mathcal{C}$.*

Demonstração: Consideremos o morfismo $\pi : \mathcal{C} \to \bar{\mathcal{C}}$ que é o morfismo de redução módulo p. Como p não divide Δ, $\bar{\mathcal{C}}$ é uma curva elíptica, $\bar{\Delta} \neq \bar{0}$, definida sobre um corpo finito. Pelo teorema 3.6.3, existe ponto $\mathbb{F}_p$-racional e pelo lema de Hensel, esses pontos podem ser levantados a pontos em $\mathbb{Q}_p$. □

Falta mostrar a existência de pontos em $\mathbb{Q}_p$ para $p = 2, 3$ ou 5.

(i) Primeiro caso: $p = 2$. Neste caso, notamos que o ponto $\bar{P} = (\bar{1} : \bar{0} : \bar{1}) \in \mathcal{C}_{ns}(\mathbb{F}_2)$ é um ponto não singular e portanto, pelo lema de Hensel, teorem 1.2.23, levanta-se a um ponto de $\mathbb{Q}_2$.

(ii) Segundo caso: $p = 3$. Este é o caso mais difícil, uma vez que se $f = 3X^3 + 4Y^3 + 5Z^3$, reduzindo módulo 3, obtemos, $\bar{f} = Y^3 + 2Z^3 = (Y + 2Z)^3$ e portanto não podemos encontrar pontos não singulares em $\mathbb{F}_3$. Contudo, podemos encontrar um ponto em $\mathcal{C}(\mathbb{Q}_3)$, desomogeneizando em Z e fazendo $X = 0, Y = t/4$.

De fato, nestas condições obtemos (clareando denominadores) o polinômio $g(t) = t^3 + 80$ que pelo lema de Newton, teorema 1.2.24, têm solução em $\mathbb{Q}_3$ uma vez que $g(3^\alpha + 1) = 3^{3\alpha} + 3^{2\alpha+1} + 3^{\alpha+1} + 81$ daí $v_3(g(3^{\alpha+1})) = 4$ se $\alpha > 1$ e $v_3(g'(3^\alpha + 1)) = 1$.

(iii) Terceiro caso: $p = 5$. Neste caso, nortamos que o ponto $\bar{P} = (\bar{1} : \bar{2} : \bar{0}) \in \mathcal{C}_{ns}(\mathbb{F}_5)$ é um ponto não singular e, portanto, pelo lema de Hensel, *loc. cit.*, levanta-se a um ponto de $\mathbb{Q}_5$.

CAPÍTULO 4

VARIEDADES ABELIANAS

4.1 O CASO CLÁSSICO

Nesta seção, vamos enunciar certas propriedades das variedades abelianas que serviram históricamente como um guia para se estudar o caso geral. Os detalhes e as demonstrações podem ser encontrados em [Mum 1].

Teorema 4.1.1 *Sejam X um grupo de Lie complexo, compacto e conexo de dimensão g e seja $V = T_0(X)$ o espaço tangente na origem. Então:*

(i) *X é um grupo comutativo.*

(ii) *A aplicação exponencial $exp : V \to X$ é um homomorfismo sobrejetivo entre grupos de Lie complexos cujo núcleo é um reticulado Γ em V e, portanto, induz um isomorfismo de grupos de Lie $V/\Gamma \simeq X$, isto é, X é um toro complexo.*

(iii) *X é um grupo divisível, isto é, o homomorfismo de multiplicação por n é sobrejetivo para cada $n \neq 0$ e, além disso, seu núcleo X_n é isomorfo a $X_n \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$.*

(iv) *Uma condição necessária e suficiente para que X seja algébrica é que exista uma forma Hermitiana definida positiva H em V, tal que $Im(H)$ assuma valores inteiros em $\Gamma \times \Gamma$. Nesse caso, chamamos X variedade abeliana.*

4.2 PROPRIEDADES FUNDAMENTAIS

Definição 4.2.1 *Uma variedade abeliana sobre um corpo k é uma variedade projetiva X sobre k dotada de dois morfismos:*

$$m : X \times X \to X$$

$$\text{inv} : X \to X$$

(multiplicação e inverso)e um elemento $\epsilon \in X(k)$ *tal que a estrutura definida em* $X(\bar{k})$*, seja de grupo com identidade* ϵ*.*

Observação 4.2.2 Para cada k álgebra R, $X(R)$ adquire, assim, uma estrutura de grupo que depende funtorialmente de R.

Observação 4.2.3 De fato, classicamente, define-se variedade abeliana como uma variedade completa e mostra-se que, dado qualquer divisor efetivo, seu triplo é muito amplo e, portanto, tal variedade é realmente projetiva.

Observação 4.2.4 Toda variedade abeliana é não singular, pois seu aberto não singular por translação cobre toda variedade.

Lema 4.2.5 (**Lema de Rigidez**) *Sejam* X *uma variedade projetiva,* Y *e* Z *variedades e* $\Phi : X \times Y \to Z$ *um morfismo. Se existe* $y_0 \in Y$ *tal que* Φ *é constante em* $X \times \{y_0\}$*, então* Φ *é constante em* $X \times \{y\}$ *para cada* $y \in Y$*. Além disso, se* Φ *for também constante em* $\{x_0\} \times Y$ *para algum* $x_0 \in X$*, então,* Φ *é constante.*

Demonstração: Considere a projeção $\pi_2 : X \times Y \to Y$. Como X é própria, π_2 é um morfismo fechado. Portanto, se $\mathcal{U}$ é uma vizinhança afim de $z_0 = \Phi(x, y_0)$, então, $W = \pi_2(\Phi^{-1}(Z \setminus \mathcal{U})) \subset Y$ é fechado. Por hipótese, $y_0 \notin W$, daí, $Y \setminus W$ é um aberto denso de Y. Dado $y \notin W$, temos que a variedade projetiva $\Phi(X \times \{y\})$ está contida no aberto afim $\mathcal{U}$ e portanto é reduzida a um ponto. Concluímos, então, que Φ é constante em $X \times \{y\}$ para cada $y \in Y \setminus W$ e como $Y \setminus W$ é denso, segue nosso resultado. □

Corolário 4.2.6 *Sejam* X *e* Y *variedades abelianas e* $\Phi : X \to Y$ *um morfismo. Então,* Φ *é a composição de um homomorfismo e uma translação.*

Demonstração: Vamos supor, sem perda de generalidade, que $\Phi(0) = 0$ e mostrar que Φ é um homomorfismo. Definimos $\Psi : X \times X \to Y$ por $\Psi = \Phi \circ m_X - m_Y \circ (\Phi \times \Phi)$; mostrar que Φ é um homomorfismo é o mesmo que mostrar que Ψ é a aplicação nula. Pelo lema anterior, como $\Psi(X \times \{0\}) = \Psi(\{0\} \times X) = 0$ temos que $\Psi = 0$. □

Corolário 4.2.7 *A lei de grupo numa variedade abeliana é comutativa.*

Demonstração: Basta notar que inv : $X \to X$ é um homomorfismo, pelo corolário anterior. Esta é a condição necessária e suficiente para que um grupo seja comutativo. □

A partir de agora, vamos adotar a notação aditiva para a lei de grupo numa variedade abeliana.

Proposição 4.2.8 *Uma aplicação racional $\Phi : X \dashrightarrow Y$, de uma variedade não singular X, em uma variedade abeliana Y estende-se a um morfismo.*

Demonstração: [Hin-Sil, pag.120]. □

Proposição 4.2.9 *Sejam X uma variedade abeliana e $\Phi : X \to Y$ um morfismo. Então, existe uma subvariedade abeliana $Z \subset X$ tal que, para cada $x \in X$, a componente conexa de $\Phi^{-1}(\Phi(x))$ contendo x é $Z + x$*

Demonstração: [Hin-Sil, pag.120]. □

4.3 TEOREMA DO CUBO

Teorema 4.3.1 (**Princípio SeeSaw**) *Sejam X e Y variedades, X completa e $\mathfrak{L}$ um fibrado linear em $X \times Y$, então, o conjunto:*

$$Y_1 = \{y \in Y \mid \mathfrak{L}|_{X\times\{y\}}\} \simeq \mathcal{O}_{X\times\{y\}}$$

é fechado em Y.

Demonstração: [Mum 1, pag.54]

Teorema 4.3.2 (**Teorema do cubo**) *Sejam X e Y variedades completas, Z um esquema conexo, e $\mathfrak{L}$ um fibrado linear em $X \times Y \times Z$ cujas restrições a $\{x_0\} \times Y \times Z$, $X \times \{y_0\} \times Z$ e $X \times Y \times \{z_0\}$ são triviais para algum $x_0 \in X$, $y_0 \in Y$ e $z_0 \in Z$. Então, $\mathfrak{L}$ é trivial.*

Demonstração: Seja $Z^{'}$ o subesquema fechado maximal de Z sobre o qual $\mathfrak{L}$ é trivial, notemos que $Z^{'} \neq \emptyset$ pois $z_0 \in Z^{'}$ e também que $Z^{'}$ é fechado de acordo com o teorema Seesaw. Devemos mostrar que $Z^{'} = Z$, mas, como Z é conexo, e $Z^{'}$ fechado, basta mostrar que $Z^{'}$ é aberto, vamos mostrar que dado $z \in Z^{'}$ existe um aberto de $Z^{'}$ que o contém. Denotando por z_0 esse ponto, $\mathfrak{m} \subset \mathcal{O}_{Z,z_0}$ o ideal maximal e I o ideal definindo $Z^{'}$ em z_0, e observando que I é obtido como limite nas vizinhanças afins de z_0, devemos mostrar que $I = 0$, $I \subset \mathfrak{m}$. Suponhamos que $I \neq 0$, como, pelo teorema de Krull, $\bigcap_{n\geq 0} \mathfrak{m}^n = 0$, existe $n > 0$ tal que $I \subset \mathfrak{m}^n eI \nsubseteq \mathfrak{m}^n + 1$,de modo que o $k = \mathcal{O}_{Z,z_0}/\mathfrak{m}$ espaço vetorial $\mathfrak{m}^{n+1} + I/\mathfrak{m}^{n+1} \subset \mathfrak{m}^n/\mathfrak{m}^{n+1}$ seja não nulo. Sejam agora: $I_0 = \mathfrak{m}$, $I_1 = \mathfrak{m}^{n+1} + I$ e I_2 um ideal tal que $\mathfrak{m}^{n+1} \subset I_2 \subset I_1$ e $dim_k I_1/I_2 = 1$ desta feita, temos $I_1 = I_2 + k.a$ para algum $a \in I_1$ note ainda que $I \subset I_1 eI \nsubseteq I_2$. Seja agora Z_i o subesquema fechado de Z constituído de um ponto, z_0, e com feixe estrutural : $\mathcal{O}_{Z,z_0}/I_i$, de modo que temos inclusões naturais $Z_0 \subset Z_1 \subset Z_2 \subset Z^{'}$ e $Z_2 \nsubseteq Z^{'}$. Consideremos agora $\underline{\mathfrak{L}_i}$ (i=0,1,2) as restrições a $X \times Y \times Z_i$ do feixe $\underline{\mathfrak{L}}$ de seções de $\mathfrak{L}$, note que $\underline{\mathfrak{L}_i}$ (i=0, 1)são triviais em $X \times Y \times Z_i$ (i=0, 1) respectivamente uma vez que $Z_0 \subset Z^{'} eZ_1 \subset Z^{'}$, desta feita, obtemos isomorfismos $\underline{\mathfrak{L}_i} \cong \mathcal{O}_{X\times Y\times Z_i}$ $(i = 0, 1)$ e, além disso, a seqüência exata

$$\begin{array}{ccccccccc} 0 & \to & \mathcal{O}_{Z,z_0}/I_0 & \to & \mathcal{O}_{Z,z_0}/I_2 & \to & \mathcal{O}_{Z,z_0}/I_1 & \to & 0 \\ & & f + I_0 & \mapsto & af + aI_0 = af + I_2 & \mapsto & af + I_1 = 0 + I_1 & & \end{array}$$

induz a seqüência exata de feixes em Z_0 :

$$0 \to \mathcal{O}_{Z_0} \to \iota_2^* \mathcal{O}_{Z_2} \to \iota_1^* \mathcal{O}_{Z_1} \to 0$$

a qual, por sua vez, induz a seqüência exata de feixes em $X \times Y \times Z_0$:

$$0 \to \mathcal{O}_{X\times Y\times Z_0} \to \iota_2^* \mathcal{O}_{X\times Y\times Z_2} \to \iota_1^* \mathcal{O}_{X\times Y\times Z_1} \to 0$$

Ora, essa seqüência fornece, por tensorização (por um feixe localmente livre), a seginte sequência exata:

$$0 \to \underline{\mathfrak{L}}_0 \to \iota_2^* \underline{\mathfrak{L}}_2 \to \iota_1^* \underline{\mathfrak{L}}_1 \to 0.$$

Consideremos agora a seção $s \in \Gamma(X \times Y \times Z_1, \mathfrak{L}_1)$ que corresponde à imagem de $1 \in \mathcal{O}_{X\times Y\times Z_1}$ via o isomorfismo descrito. A condição necessária e suficiente para que $\mathfrak{L}_2$ seja trivial é que s possa ser levantado a uma seção $s' \in \mathfrak{L}_2$ pois isso induziria um homomorfismo(não nulo) $\mathcal{O}_{X\times Y\times Z_2} \to \underline{\mathfrak{L}}_2$, o qual é isomorfismo em cada talo, uma vez que $\underline{\mathfrak{L}_2}$ é localmente livre de posto 1. Desta feita, concluiríamos

que $\mathfrak{L}_2$ é trivial, a recíproca é clara. Para mostrar que s pode ser levantada, vamos fixar um isomorfismo $\underline{\mathfrak{L}_0} \cong \mathcal{O}_{X\times Y}$ e construindo a seqüência longa nas cohomologias provenientes da seqüência exata curta:

$$0 \to \underline{\mathfrak{L}_0} \to \iota_2^*\underline{\mathfrak{L}_2} \to \iota_1^*\underline{\mathfrak{L}_1} \to 0$$

temos :

$$0 \to \Gamma(\underline{\mathfrak{L}_0}) \to \Gamma(\iota_2^*\underline{\mathfrak{L}_2}) \to \Gamma(\iota_1^*\underline{\mathfrak{L}_1}) \to H^1(X\times Y, \mathcal{O}_{X\times Y}) \to ...$$

portanto, concluímos que s poderá ser levantada se e somente se:
$\partial(s) = 0 \in H^1(X\times Y, \mathcal{O}_{X\times Y})$.Por outro lado, sabemos que as restrições de $\mathfrak{L}_0$ a $X\times y_0\times Z$, a $x_0\times Y\times Z, X\times y_0\times Z_2$ e a $x_0\times Y\times Z_2$ são triviais, o que implica que as imagens de $\partial(s)$ pelas aplicações $H^1(X\times Y, \mathcal{O}_{X\times Y}) \to H^1(X, \mathcal{O}_X)$ induzida por $x \mapsto (x, y_0)$ e $H^1(X\times Y, \mathcal{O}_{X\times Y}) \to H^1(Y, \mathcal{O}_Y)$ induzida por $y \mapsto (x_0, y)$, são nulas e da fórmula de Kuneth:

$$H^1(X\times Y, \mathcal{O}_{X\times Y}) \cong H^1(X, \mathcal{O}_X) \bigoplus H^1(Y, \mathcal{O}_Y)$$

concluimos que $\partial(s) = 0$ e, portanto, s pode ser levantada, o que nos leva a concluir que $\underline{\mathfrak{L}_1}$ é trivial; que é uma contradição e o resultado então segue. □

Corolário 4.3.3 (**Teorema do cubo para Variedades Abelianas**) *Sejam X uma variedade abeliana, $\mathfrak{L}$ um fibrado linear em X e, para cada $I \subset \{1,2,3\}$,*

$$s_I : X\times X\times X \to X,$$

onde $s_I(x_1,x_2,x_3) = \sum_{i\in I} x_i$. Então, em Pic$(X)$ *temos:*

$$s_{123}^*(\mathfrak{L}) \otimes s_{12}^*(\mathfrak{L})^{-1} \otimes s_{13}^*(\mathfrak{L})^{-1} \otimes s_{23}^*(\mathfrak{L})^{-1} \otimes s_1^*(\mathfrak{L}) \otimes s_2^*(\mathfrak{L}) \otimes s_3^*(\mathfrak{L}) = 0.$$

Demonstração: A partir da conclusão do teorema do cubo, basta mostrar que a restrição de $s_{123}^*(\mathfrak{L}) \otimes s_{12}^*(\mathfrak{L})^{-1} \otimes s_{13}^*(\mathfrak{L})^{-1} \otimes s_{23}^*(\mathfrak{L})^{-1} \otimes s_1^*(\mathfrak{L}) \otimes s_2^*(\mathfrak{L}) \otimes s_3^*(\mathfrak{L})$ a $X\times X\times 0$ é trivial, uma vez que o problema é completamente simétrico. Por outro lado, percebe-se facilmente que tal restrição é (isomorfa a)

$$s_{12}^*(\mathfrak{L}) \otimes s_{12}^*(\mathfrak{L})^{-1} \otimes s_1^*(\mathfrak{L})^{-1} \otimes s_2^*(\mathfrak{L})^{-1} \otimes s_1^*(\mathfrak{L}) \otimes s_2^*(\mathfrak{L}) = 0 \in \text{Pic}(X).$$

□

Corolário 4.3.4 *Sejam X uma variedade abeliana, Y uma variedade qualquer e $f, g, h : Y \to X$ três morfismos. Então, vale a seguinte relação para qualquer fibrado linear $\mathfrak{L}$ em X:*

$$(f+g+h)^*(\mathfrak{L})\otimes(f+g)^*(\mathfrak{L})^{-1}\otimes(f+h)^*(\mathfrak{L})^{-1}\otimes(g+h)^*(\mathfrak{L})^{-1}\otimes f^*(\mathfrak{L})\otimes g^*(\mathfrak{L})\otimes h^*(\mathfrak{L}) \simeq \mathcal{O}_Y.$$

Demonstração: Basta notar que tal fibrado é o pullback via o morfismo $(f, g, h) : Y \times Y \times Y \to X \times X \times X$ do fibrado linear $s_{123}^*(\mathfrak{L}) \otimes s_{12}^*(\mathfrak{L})^{-1} \otimes s_{13}^*(\mathfrak{L})^{-1} \otimes s_{23}^*(\mathfrak{L})^{-1} \otimes s_1^*(\mathfrak{L}) \otimes s_2^*(\mathfrak{L}) \otimes s_3^*(\mathfrak{L})$ que é trivial. □

Corolário 4.3.5 (**Fórmula de Mumford**) *Sejam X uma variedade abeliana, $\mathfrak{L}$ um fibrado linear em X e $[n] : X \to X$ o morfismo de multiplicação por n. Então:*

$$[n]^*(\mathfrak{L}) \simeq \mathfrak{L}^{\frac{n^2+n}{2}} \otimes ([-1]^*(\mathfrak{L}))^{\frac{n^2-n}{2}}$$

Em particular,

(i) *se $\mathfrak{L}$ é simétrico, isto é, $[-1]^*(\mathfrak{L}) \simeq \mathfrak{L}$, então:*

$$[n]^*(\mathfrak{L}) \simeq \mathfrak{L}^{n^2}.$$

(ii) *se $\mathfrak{L}$ é anti-simétrico, isto é, $[-1]^*(\mathfrak{L}) \simeq \mathfrak{L}^{-1}$, então:*

$$[n]^*(\mathfrak{L}) \simeq \mathfrak{L}^{n}.$$

Demonstração: Aplicando o corolário anterior com $f = [n]$, $g = [1]$ e $h = [-1]$ obtemos

$$[n+1]^*(\mathfrak{L}) \otimes [n-1]^*(\mathfrak{L}) \otimes [2n]^*(\mathfrak{L})^{-1} \simeq \mathfrak{L} \otimes [-1]^*(\mathfrak{L}).$$

O resultado agora segue por indução. □

Corolário 4.3.6 (**Teorema do quadrado**) *Seja X uma variedade abeliana e para cada $a \in X$ consideremos o morfismo de translação por a; $t_a : X \to X$, dado por $t_a(x) = x + a$. Então:*

$$t_{a+b}^*(\mathfrak{L}) \otimes \mathfrak{L} \simeq t_a^*(\mathfrak{L}) \otimes t_b^*(\mathfrak{L})$$

E, portanto, para cada fibrado linear, a aplicação

$$\Phi_{\mathfrak{L}} : X \to Pic(X) \ , \ \textit{dada por} \ \ \Phi_{\mathfrak{L}}(a) = t_a^*(\mathfrak{L}) \otimes \mathfrak{L}^{-1}$$

é um homomrfismo de grupos.

Demonstração: Segue do corolário 4.3.4, fazendo $f = id, g = a$ e $h = b$ (g e h constantes). □

4.4 ISOGENIAS

Definição 4.4.1 *Seja $\Phi : X \to Y$ um homomorfismo entre variedades abelianas. Dizemos que Φ é uma isogenia se for sobrejetivo e tiver núcleo finito.*

Proposição 4.4.2 *Seja $\Phi : X \to Y$ um homomorfismo entre variedades abelianas. Então são equivalentes:*

(i) *Φ é uma isogenia.*

(ii) *$\dim(X) = \dim(Y)$ e Φ é sobrejetiva.*

(iii) *$\dim(X) = \dim(Y)$ e ker(Φ) é finito.*

(iv) *Φ é finito, plano e sobrejetivo.*

Demonstração: [Cor-Sil, pag.115]. □

Notemos que, quando Φ é isogenia, (via Φ^*) $k(X)$ é uma extensão finita de $k(Y)$ e, assim, definimos o grau de Φ, o grau de separabilidade de Φ e o grau de inseparabilidade de Φ, como sendo tais graus da extensão de corpos. Notamos ainda que como $\sharp \ker[n] = \sharp \Phi^{-1}(y)$ para todo $y \in Y$, desta feita, $\sharp \ker[n] = \deg_s \Phi$.

Teorema 4.4.3 *Seja X uma variedade abeliana de dimensão g e $n > 0$ um inteiro. Então:*

(i) *O morfismo de multiplicação por n, $[n] : X \to X$ é uma isogenia de grau n^{2g}.*

(ii) *Se a característica de k não divide n, então, $[n]$ é ètale e:*

$$X_n := \ker[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

(iii) *Se a característica de k é $p > 0$ e $p|n$, então, $[n]$ não é separável e:*

$$X_{p^r} \simeq (\mathbb{Z}/p^r\mathbb{Z})^t$$

para algum t, $0 \leq t \leq g$.

Demonstração: (i) Escolhendo um fibrado linear $\mathfrak{L}$ simétrico e amplo em X, notamos que, como $[n]^*\mathfrak{L} \simeq \mathfrak{L}^{n^2}$, a restrição de $[n]^*\mathfrak{L}$ a $\ker([n])$ é amplo, (restrição de um feixe amplo a um subesquema fechado) e trivial (pois em $\ker([n])$, $[n] = 0$) isso é impossível, a menos que $\dim(\ker([n])) = 0$. Portanto, do nosso critério de caracterização de isogenias, $[n]$ é isogenia.
Consideremos o divisor D associado a $\mathfrak{L}$. Temos das propriedades do número de interseção que

$$\deg([n])D^g = ([n]^*D)^g = (n^2D)^g = n^{2g}D^g.$$

(ii) Como a característica de k não divide o grau de $[n]$, ele deve ser separável e claramente não ramificado. Quanto à estrutura do grupo $A = \ker[n]$, basta notarmos que, para cada $d \,|\, n^{2g}$, a d–torção A_d tem ordem d^{2g}. De um lema de grupos em [Hin-Sil, pag. 125], segue nosso resultado.
(iii) Isso é conseqüência do fato de que a derivada (na origem) do morfismo de multiplicação por n é nula. Detalhes em [Mum 1, pag.63]. □

CAPÍTULO 5

TEORIA DAS ALTURAS

5.1 ALTURAS NO ESPAÇO PROJETIVO

Intuitivamente, podemos pensar numa função altura como sendo uma função que, de alguma forma, possa medir a complexidade aritmética de um ponto, de modo que se cumpra o objetivo de haver apenas um número finito de pontos racionais com altura limitada. Uma maneira simples de medir a altura de um ponto $P \in \mathbb{P}^n(\mathbb{Q})$ é, escolhendo coordenadas inteiras coprimos, assim definir $\mathrm{H}(P) = \max_i \mid x_i \mid$ em que $P = (x_0 : x_1 : ... : x_n)$. Uma maneira mais coveniente (por independer de coordenadas homogêneas) de definir tal altura seria:

$$\mathrm{H}(P) = \prod_{v \in M_{\mathbb{Q}}} \max_i \mid x_i \mid_v .$$

Notamos que as duas definições coicidem e, portanto, o conjunto dos pontos, cuja altura é limitada por alguma constante real, é finito.
Seria, portanto, natural tentar generalizar tal definição para qualquer corpo de números K fazendo para $P \in \mathbb{P}^n(K)$:

$$\mathrm{H}_K(P) = \prod_{v \in M_K} \max_i \parallel x_i \parallel_v .$$

Proposição 5.1.1 *Seja K um corpo de números e $P \in \mathbb{P}^n(K)$ um ponto. Então:*

(i) $\mathrm{H}_K(P)$ *está bem definida, isto é, independe das coordenadas homogêneqas escolhidas para P.*

(ii) $\mathrm{H}_K(P) \geq 1, \forall P \in \mathbb{P}^n(K)$.

(iii) *Se $L \mid K$ é uma extensão finita de K, então:*

$$\mathrm{H}_L(P) = \mathrm{H}_K(P)^{[L\,:\,K]}.$$

Demonstração: (i)Se $P = (\lambda x_0 : \lambda x_1 : ... : \lambda x_n)$ com $\lambda \in K^*$,

$$\prod_{v \in M_K} \max_i \| \lambda x_i \|_v = (\prod_{v \in M_K} \| \lambda \|_v)(\prod_{v \in M_K} \max_i \| x_i \|_v) = \prod_{v \in M_K} \max_i \| \lambda x_i \|_v,$$

pois pela fórmula do produto $\prod_{v \in M_K} \| \lambda \|_v = 1$.
(ii) Basta notar que podemos escolher coordenadas homogêneas tais que uma das coordenadas seja 1.
(iii) Basta lembrar que para cada $w \in M_L$, e $v|w$, $v \in M_L$, temos

$$n_w = [L_w : \mathbb{Q}_w] = [L_w : K_v] \cdot n_v$$

e a fórmula do grau:

$$\sum_{w \in M_L, w|v} [L_w : K_v] = [L : K]$$

e aplicar a definição:

$$\mathrm{H}_L(P) = \prod_{w \in M_L} \max_i \| x_i \|_w = \prod_{v \in M_K} \prod_{w \in M_L, w|v} \max_i \| x_i \|_w = \prod_{v \in M_K} \prod_{w \in M_L, w|v} \max_i | x_i |_v^{n_w} =$$

$$= \prod_{v \in M_K} \prod_{w \in M_L, w|v} \max_i \| x_i \|_v^{[L_w : K_v]} = \prod_{w \in M_L} \max_i \| x_i \|_v^{[L:K]} = \mathrm{H}_K(P)^{[L:K]}.$$

□

Definição 5.1.2 *A altura (multiplicativa) absoluta em $\mathbb{P}^n(\overline{\mathbb{Q}})$ é a função*

$$\mathrm{H} : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [1, \infty)$$

dada por $\mathrm{H}(P) = \mathrm{H}_K(P)^{\frac{1}{[K:(Q)]}}$, onde K é qualquer corpo tal que $P \in \mathbb{P}^n(K)$.
A altura (logarítmica) absoluta em $\mathbb{P}^n(\overline{\mathbb{Q}})$ é a função

$$\mathrm{h} : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [0, \infty)$$

dada por $\mathrm{h}(P) = \log \mathrm{H}(P) = \frac{1}{[K:\mathbb{Q}]}$.

Observe que a proposição anterior nos garante a independencia do corpo K. Chamamos corpo de definição de P, o corpo $\mathbb{Q}(P) := \mathbb{Q}(x_0/x_j, x_1/x_j, ..., x_n/x_j)$.

Proposição 5.1.3 *A função altura definida é invariante pela ação do grupo de Galois absoluto dos racionais, isto é, se* $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ *e* $\sigma \in G_{\mathbb{Q}}$, *então* $\mathrm{H}(\sigma(P)) = \mathrm{H}(P)$.

Demonstração: Basta escolher uma extensão finita dos racionais tal que $P \in \mathbb{P}^n(K)$ e notar que σ induz um isomorfismo $K \cong \sigma(K)$ que identifica de maneira natural o conjunto de valores absolutos de K e $\sigma(K)$. Como a definição da altura depende apenas de M_K, segue a invariância. □

Teorema 5.1.4 (**Northcott**) *Sejam* $B, D \in (0, \infty)$. *O conjunto*

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid \mathrm{H}(P) \leq B \text{ e } [\mathbb{Q}(P) : \mathbb{Q}] \leq D\}$$

é finito. Em particular, para cada corpo de números fixado, temos que o conjunto

$$\{P \in \mathbb{P}^n(K) | \, \mathrm{H}_K(P) \leq B\}$$

é finito.

Demonstração: Escolhendo coordenadas homogêneas para P tais que alguma das coordenadas seja 1, notamos que $\mathrm{H}(x_i) := \mathrm{H}(x_i : 1) \leq \mathrm{H}(P)$ e $\mathbb{Q}(x_i) \subset \mathbb{Q}(P)$. Portanto podemos nos reduzir a mostrar que o conjunto

$$\{x \in \overline{\mathbb{Q}} \mid \mathrm{H}(x) \leq B \text{ e } [\mathbb{Q}(x) : \mathbb{Q}] = d\}$$

é finito. Seja $x \in \overline{\mathbb{Q}}$ um elemento de grau d sobre os racionais e sejam $x = x_1, ..., x_d$ os conjugados de x sobre $\mathbb{Q}$. O polinômio mínimo de x é :

$$p_x(T) = \prod_{j=1}^{d}(T - x_j) = \sum_{r=0}^{d}(-1)^r s_r(x) T^{d-r},$$

em que os s_r são os polinõmios simétricos em $x_1, ..., x_d$. Como os x_i são conjugados, pela proposição anterior temos que $\mathrm{H}(x_i) = \mathrm{H}(x)$ e, portanto, da desigualdade triangular, segue que $\mathrm{H}(s_j) \leq c_j \, \mathrm{H}(x)^j$ para certas constantes que independem de x. concluimos que $\mathrm{H}(s_0(x) : s_1(x) : ... : s_d(x))$ é também limitado, logo x é uma das raízes de um polinômio com coeficientes racionais de altura (dos coeficientes vistos como pontos de $\mathbb{P}^d$) limitada. Como o conjunto dos coeficientes é limitado, existe apenas um número finito de posibilidades para o polinômio mínimo de x e consequentemente um número finito de possibilidades para x. □

Proposição 5.1.5 (i) *Seja* $S_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N$ *o mergulho de Segre. Então:*

$$\mathrm{h}(S_{n,m}(x,y)) = \mathrm{h}(x) + \mathrm{h}(y).$$

(ii) *Seja* $\nu_d : \mathbb{P}^n \to \mathbb{P}^N$ *o mergulho de Veronese. Então:*

$$\mathrm{h}(\nu_d(x)) = d \cdot \mathrm{h}(x).$$

(iii) *Seja* $\Phi : \mathbb{P}^n \dashrightarrow \mathbb{P}^m$ *uma aplicação racional de grau* d *sobre* $\overline{\mathbb{Q}}$ *e seja* $\mathcal{U}$ *o aberto maximal de definição de* Φ*. Então em* $\mathcal{U}$*, temos:*

$$\mathrm{h}(\Phi(P)) \leq d \cdot \mathrm{h}(P) + O(1).$$

Além disso , se $X \subset \mathcal{U}$ *é uma subvariedade fechada, então, em* $X(\mathbb{Q})$ *temos:*

$$\mathrm{h}(\Phi(P)) = d \cdot \mathrm{h}(P) + O(1).$$

Demonstração: [Hin-Sil, pag.179]. □

5.2 ALTURAS EM VARIEDADES PROJETIVAS

Nesta seção, estaremos considerando variedades projetivas lisas, definidas sobre $\overline{\mathbb{Q}}$, bem como morfismos, fibrados, etc, etc. Vamos também usar X para denotar $X(\overline{\mathbb{Q}})$.

Definição 5.2.1 *Seja* $\Phi : X \to \mathbb{P}^n$ *um morfismo. A altura (logarítmica absoluta) em* X *relativa a* Φ *é a função*

$$\mathrm{h}_\Phi : X \to \mathbb{R}$$

$$\mathrm{h}_\Phi(P) = \mathrm{h}(\Phi(P)),$$

onde $\mathrm{h} : \mathbb{P}^n \to \mathbb{R}$ *é a função altura no espaço projetivo definida anteriormente.*

Sabemos que, a cada morfismo $\Phi : X \to \mathbb{P}^n$ podemos associar um fibrado linear em X gerado por seções globais, o pullback do feixe de Serre $\mathcal{O}_{\mathbb{P}^n}(1)$. É fundamental entender a conseqüência de isomorfismos entre esses feixes. Reciprocamente, a cada fibrado linear em X, podemos associar uma aplicação racional.

Proposição 5.2.2 *Sejam X uma variedade projetiva lisa, $\Phi : X \to \mathbb{P}^n$ e $\Psi : X \to \mathbb{P}^m$ morfismos. Suponha que $\Phi^*(\mathcal{O}_{\mathbb{P}^n}(1)) \simeq \Psi^*(\mathcal{O}_{\mathbb{P}^n}(1))$. Então:*

$$\mathrm{h}_\Phi = \mathrm{h}_\Psi + O(1).$$

Demonstração: Sabemos que os morfismos Φ e Ψ se fatoram via certas aplicações lineares $A : \mathbb{P}^N \to \mathbb{P}^n$ e $B : \mathbb{P}^N \to \mathbb{P}^m$ e φ em que $\varphi : X \to \mathbb{P}^N$. Portanto, $\mathrm{h}(A(Q)) = \mathrm{h}(Q) + O(1)$ e $\mathrm{h}(B(Q)) = \mathrm{h}(Q) + O(1)$ para cada $Q \in \varphi(\overline{\mathbb{Q}})$. Fazendo $Q = \varphi(P)$ obtemos:

$$\mathrm{h}(\Phi(P)) = \mathrm{h}(A(\varphi(P))) = \mathrm{h}(\varphi(P)) + O(1) = \mathrm{h}(B(\varphi(P))) + O(1) = \mathrm{h}(\Psi(P)) + O(1).$$

□

Definição 5.2.3 *Vamos denotar $\mathcal{H}(X)$ o grupo de funções reais $\mathrm{h} : X \to \mathbb{R}$ modulo funções limitadas em X*

Notamos que a proposição anterior nos permite definir alturas (módulo $O(1)$) associadas à classe de isomorfismo de fibrados lineares sem pontos base em $\mathrm{Pic}(X)$.

Definição 5.2.4 *Seja $\mathfrak{L}$ a classe de um fibrado linear sem pontos base em X. A "função"altura associada a $\mathfrak{L}$ é a classe de funções $\mathrm{h}_\mathfrak{L} \in \mathcal{H}(X)$ obtida a partir de qualquer morfismo associado a qualquer fibrado na classe.*

Proposição 5.2.5 (**Aditividade**) *Sejam $\mathfrak{L}_1$ e $\mathfrak{L}_2$ fibrados lineares sem pontos base em X. Então:*

$$\mathrm{h}_{\mathfrak{L}_1 \otimes \mathfrak{L}_2} = \mathrm{h}_{\mathfrak{L}_1} + \mathrm{h}_{\mathfrak{L}_2} \in \mathcal{H}(X).$$

Demonstração: Considere morfismos $\Phi_i : X \to \mathbb{P}^{n_i}$ associados a $\mathfrak{L}_i$; associado a $\mathfrak{L}_1 \otimes \mathfrak{L}_2$ temos o morfismo $\Phi_1 \otimes \Phi_2$ dado por $\Phi_1 \otimes \Phi_2(P) = S_{n_1,n_2}(\Phi_1(P), \Phi_2(P))$ onde S_{n_1,n_2} é o mergulho de Segre. Logo, temos:

$$\mathrm{h}_{\mathfrak{L}_1 \otimes \mathfrak{L}_2}(P) = \mathrm{h}(\Phi_1 \otimes \Phi_2(P)) + O(1)$$

$$= \mathrm{h}(S_{n_1,n_2}(\Phi_1(P), \Phi_2(P))) + O(1) = \mathrm{h}_{\mathfrak{L}_1}(P) + \mathrm{h}_{\mathfrak{L}_2}(P) + O(1).$$

□

Definição 5.2.6 *Seja $\mathfrak{L}$ um fibrado linear em X e sejam $\mathfrak{L}_1$ e $\mathfrak{L}_2$ fibrados lineares sem pontos base tais que $\mathfrak{L} \simeq \mathfrak{L}_1 \otimes \mathfrak{L}_2^{-1}$. Definimos a função altura associada a $\mathfrak{L}$ como sendo a função*

$$\mathrm{h}_{\mathfrak{L}} := \mathrm{h}_{\mathfrak{L}_1} - \mathrm{h}_{\mathfrak{L}_2} \in \mathcal{H}(X).$$

Pela proposição anterior, tal definição não depende da escolha de $\mathfrak{L}_1$ e $\mathfrak{L}_2$.

Teorema 5.2.7 (**Propriedades de alturas de Weil**) *Seja X uma variedade lisa sobre $\overline{\mathbb{Q}}$. Então, existe um único homomorfismo:*

$$\mathrm{Pic}(X) \to \mathcal{H}(X)$$

$$\mathfrak{L} \mapsto \mathrm{h}_{\mathfrak{L}}$$

com as seguintes propriedades:

(i) (Normalização) *Se $\mathfrak{L}$ é um fibrado linear, sem pontos base e $\Phi : X \to \mathbb{P}^n$ um morfismo asociado a $\mathfrak{L}$, então:*

$$\mathrm{h}_{\mathfrak{L}} = \mathrm{h}_{\Phi} \in \mathcal{H}(X).$$

Em particular, se $X = \mathbb{P}^n$ e $\mathfrak{L} = \mathcal{O}_{\mathbb{P}^n}(1)$, temos:

$$\mathrm{h}_{\mathcal{O}_{\mathbb{P}^n}(1)} = \mathrm{h} \in \mathcal{H}(X).$$

(ii) (Funtorialidade) *Seja $\Phi : X \to Y$ um morfismo e seja $\mathfrak{L} \in \mathrm{Pic}(Y)$. Então:*

$$\mathrm{h}_{X,\Phi^*(\mathfrak{L})} = \mathrm{h}_{Y,\mathfrak{L}} \in \mathcal{H}(X).$$

(iii) (Positividade) *Seja $\mathfrak{L}$ um fibrado linear efetivo e B o suporte de uma seção global de $\mathfrak{L}$. Então:*

$$\mathrm{h}_{\mathfrak{L}} \geq 0 \in \mathcal{H}(X \setminus B).$$

(iv) (Finitude) *Seja $\mathfrak{L}$ um fibrado linear amplo. Então o conjunto:*

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \ \mid \ \mathrm{h}_{\mathfrak{L}}(P) \leq C \text{ e } [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}$$

é finito para quaisquer constantes B e d.

Demonstração: A unicidade é clara, quanto à existência, é conseqüência da construção que estamos fazendo que de fato já nos forneceu a aplicação (bem definida) e mostrou-nos ser um homomorfismo de grupos pela aditividade, a propriedade (i) é bastante clara da nossa construção e a finitude é devida ao teorema de Northcott. De fato, escolhendo uma potência do nosso fibrado(amplo) que seja muito amplo, podemos supor $X \hookrightarrow \mathbb{P}^N$ isso implica a finitude. Funtorialidade, num caso particular, segue da nossa construção, positividade e funtorialidade, no caso geral, são feitas em detalhes em [Hin-Sil, pag.185]. □

5.3 ALTURAS EM VARIEDADES ABELIANAS

Teorema 5.3.1 *Sejam X uma variedade abeliana sobre $\overline{\mathbb{Q}}$ e seja $\mathfrak{L}$ um feixe inversível em X. Então, para quaisquer $P, Q, R \in X$, temos:*

$$\mathrm{h}_{\mathfrak{L}}(P+Q+R)-\mathrm{h}_{\mathfrak{L}}(P+Q)-\mathrm{h}_{\mathfrak{L}}(P+R)-\mathrm{h}_{\mathfrak{L}}(Q+R)+\mathrm{h}_{\mathfrak{L}}(P)+\mathrm{h}_{\mathfrak{L}}(Q)+\mathrm{h}_{\mathfrak{L}}(R) = O(1).$$

Demonstração: Ora, este resultado é a tradução, na linguagem de alturas, do teorema do cubo para variedades abelianas 4.3.3. De fato, aplicando as propriedades de alturas de Weil temos à relação

$$s_{123}^*(\mathfrak{L}) \otimes s_{12}^*(\mathfrak{L})^{-1} \otimes s_{13}^*(\mathfrak{L})^{-1} \otimes s_{23}^*(\mathfrak{L})^{-1} \otimes s_1^*(\mathfrak{L}) \otimes s_2^*(\mathfrak{L}) \otimes s_3^*(\mathfrak{L}) = 0,$$

obtendo o resultado desejado. □

Corolário 5.3.2 *Sejam X uma variedade abeliana $n \in \mathbb{Z}$ e $[n] : X \to X$, o morfismo de multiplicação por n. Então:*

$$\mathrm{h}_{\mathfrak{L}} \circ [n] = \frac{n^2+n}{2}\,\mathrm{h}_{\mathfrak{L}} + \frac{n^2-n}{2}\,\mathrm{h}_{\mathfrak{L}} \circ [-1] \in \mathcal{H}(X).$$

Em particular,

(i) *Se $\mathfrak{L}$ é par, (isto é, $[-1]^*\mathfrak{L} \simeq \mathfrak{L}$), então:*

$$\mathrm{h}_{\mathfrak{L}} \circ [n] = n^2\,\mathrm{h}_{\mathfrak{L}} \in \mathcal{H}(X)$$

e

$$\mathrm{h}_{\mathfrak{L}}(P+Q) + \mathrm{h}_{\mathfrak{L}}(P-Q) = 2\,\mathrm{h}_{\mathfrak{L}}(P) + 2\,\mathrm{h}_{\mathfrak{L}}(Q) \in \mathcal{H}(X).$$

(ii) *Se $\mathfrak{L}$ é ímpar, (isto é, $[-1]^*\mathfrak{L} \simeq \mathfrak{L}^{-1}$), então:*

$$\mathrm{h}_{\mathfrak{L}} \circ [n] = n\,\mathrm{h}_{\mathfrak{L}} \in \mathcal{H}(X)$$

e

$$\mathrm{h}_{\mathfrak{L}}(P+Q) = \mathrm{h}_{\mathfrak{L}}(P) + \mathrm{h}_{\mathfrak{L}}(Q) \in \mathcal{H}(X).$$

Demonstração: A relação estabelecida pelo teorema anterior, fazendo $Q = [n]P$ e $r = [-1]P$ é:

$$\mathrm{h}_{\mathfrak{L}}([n+1]P) + \mathrm{h}_{\mathfrak{L}}([n-1]P) = 2\,\mathrm{h}_{\mathfrak{L}}([n]P) + \mathrm{h}_{\mathfrak{L}}(P) + O(1).$$

O resultado agora segue por indução. Notamos que este resultado é a tradução da fórmula de Munford 4.3.5 via as propriedades das alturas mostradas no teorema 5.2.7, e poderia, assim, ser deduzido diretamente. □

5.4 ALTURAS CANÔNICAS EM VARIEDADES ABELIANAS

Teorema 5.4.1 (**Néron, Tate**) *Sejam X uma variedade projetiva lisa definida sobre um corpo de números, $\mathfrak{L}$ um fibrado linear em X, e $\Phi : X \to X$ um morfismo. Suponhamos que, em* $\mathrm{Pic}(X) \otimes \mathbb{R}$*, vale:*

$$\Phi^*(\mathfrak{L}) = \mathfrak{L}^{\alpha}$$

para algum número real $\alpha > 1$. Então, existe uma única função, chamada a altura canônica em X relativa a Φ e $\mathfrak{L}$,

$$\widehat{\mathrm{h}}_{X,\Phi,\mathfrak{L}} : X \to \mathbb{R}$$

com as seguintes propriedades:

(i) $\widehat{\mathrm{h}}_{X,\Phi,\mathfrak{L}} = \mathrm{h}_{X,\mathfrak{L}} \in \mathcal{H}(X)$.

(ii) $\widehat{\mathrm{h}}_{X,\Phi,\mathfrak{L}} \circ \Phi = \alpha \widehat{\mathrm{h}}_{X,\Phi,\mathfrak{L}}$.

Além disso, a altura canônica pode ser calculada como o limite:

$$\widehat{\mathrm{h}}_{X,\Phi,\mathfrak{L}}(P) = \lim_{n\to\infty} \frac{1}{\alpha^n}\,\mathrm{h}_{X,\mathfrak{L}}(\Phi^n(P)).$$

Demonstração: Um cálculo simples nos mostra que a função assim definida satisfaz a propriedade (ii). Para mostrar que tal função é bem definida, devemos mostrar que a sequência $\{\frac{1}{\alpha^n}\,\mathrm{h}_{X,\mathfrak{L}}(\Phi^n(P))\}_n$ é convergente para cada $P \in X$. Aplicando a máquina de alturas de Weil à relação $\Phi^*(\mathfrak{L}) = \mathfrak{L}^\alpha$, obtemos que existe uma constante C tal que $|\,\mathrm{h}_{X,\mathfrak{L}}(\Phi(P)) - \alpha\,\mathrm{h}_{X,\mathfrak{L}}(P)| \leq C\ ,\ \forall P \in X$. A partir dessa relação, mostraremos que a sequência é de Cauchy, de fato,

$$|\alpha^{-n}\,\mathrm{h}_{X,\mathfrak{L}}(\Phi^n(P)) - \alpha^{-m}\,\mathrm{h}_{X,\mathfrak{L}}(\Phi^m(P))|$$

$$= |\sum_{i=m+1}^{n} \alpha^{-i}(\mathrm{h}_{X,\mathfrak{L}}(\Phi^i(P)) - \alpha\,\mathrm{h}_{X,\mathfrak{L}}(\Phi^{i-1}(P)))|$$

$$\leq \sum_{i=m+1}^{n} \alpha^{-i}|\,\mathrm{h}_{X,\mathfrak{L}}(\Phi^i(P)) - \alpha\,\mathrm{h}_{X,\mathfrak{L}}(\Phi^{i-1}(P))|$$

$$\leq \sum_{i=m+1}^{n} \alpha^{-i}C = (\frac{\alpha^{-m} - \alpha{-n}}{\alpha - 1})C.$$

Para verificar a propriedade (i), basta aplicar a desigualdade anterior com $m = 0$ e então fazer $n \to \infty$ para obter:

$$|\widehat{\mathrm{h}}_{X,\Phi,\mathfrak{L}}(P) - \mathrm{h}_{X,\mathfrak{L}}(P)| \leq \frac{C}{\alpha - 1}.$$

□

Teorema 5.4.2 (**Néron, Tate**) *Sejam X uma variedade abeliana sobre um corpo de números e $\mathfrak{L}$ um fibrado linear em X que seja simétrico. Então, existe uma única função*

$$\widehat{\mathrm{h}}_{X,\mathfrak{L}} : X \to \mathbb{R}$$

chamada a altura canônica em X relativa a $\mathfrak{L}$, com as seguintes propriedades:

(i)
$$\widehat{\mathrm{h}}_{X,\mathfrak{L}} = \mathrm{h}_{X,\mathfrak{L}}\ \in \mathcal{H}(X).$$

(ii) *Para qualquer inteiro m, temos:*

$$\widehat{\mathrm{h}}_{X,\mathfrak{L}} \circ [m] = m^2\,\mathrm{h}_{X,\mathfrak{L}}\,.$$

(iii) (Regra do Paralelogramo)

$$\widehat{\mathrm{h}}_{X,\mathfrak{L}}(P+Q)+\widehat{\mathrm{h}}_{X,\mathfrak{L}}(P-Q)=2\widehat{\mathrm{h}}_{X,\mathfrak{L}}(P)+2\widehat{\mathrm{h}}_{X,\mathfrak{L}}(Q).$$

(iv) *A altura canônica é uma forma quadrática, a qual podemos associar uma forma bilinear:*

$$\langle\ .\ ,\ .\ \rangle_{\mathfrak{L}} : X\times X\to\mathbb{R}$$

definida por:

$$\langle P,Q\rangle_{\mathfrak{L}} := \frac{\widehat{\mathrm{h}}_{X,\mathfrak{L}}(P+Q)-\widehat{\mathrm{h}}_{X,\mathfrak{L}}(P)-\widehat{\mathrm{h}}_{X,\mathfrak{L}}(Q)}{2}.$$

Demonstração: Consideremos a altura canônica com respeito ao morfismo $\Phi = [2]$. Notamos que, pela fórmula de Munford, corolário 4.3.5, $[2]^*(\mathfrak{L}) = \mathfrak{L}^4 \in \mathrm{Pic}(X)$. Portanto, podemos aplicar o teorema de Néron-Tate 5.4.1 e definir:

$$\widehat{\mathrm{h}}_{X,\mathfrak{L}}(P)=\lim_{n\to\infty}\frac{1}{4^n}\,\mathrm{h}_{X,\mathfrak{L}}([2^n](P)).$$

Para mostrar que tal função satisfaz às propriedades requeridas, basta notar que, pelo teorema 5.3.1 e seu corolário 5.3.2, tais propriedades já são satisfeitas módulo $O(1)$. Para eliminar as funções $O(1)$, basta substituir cada ponto P por $[2^n]P$ e, em seguida, dividir a relação encontrada por 4^n. Além disso, mostra-se que num grupo abeliano, se uma função satisfaz a regra do paralelogramo, então, esta função é uma forma quadrática. Detalhes [Hin-Sil, pag.200,201]. □

Proposição 5.4.3 *Sejam X uma variedade abeliana sobre um corpo de números e $\mathfrak{L}$ um fibrado linear simétrico e amplo. Então, a altura canônica associada a $\mathfrak{L}$ é tal que:*

(i) *Para cada $P \in X(\bar{K})$, $\hat{\mathrm{h}}_{X,\mathfrak{K}}(P) \geq 0$ com igualdade se e somente se P é ponto de torção.*

(ii) *Ambas a forma quadrática $\hat{\mathrm{h}}_{X,\mathfrak{K}}$ e a forma bilinear associada se estendem linearmente a uma forma quadrática definida positiva e a um produto interno euclidiano em $X(\bar{K}\otimes\mathbb{R})$*

Demonstração: [Hin-Sil, pag.201]. □

CAPÍTULO 6

TEOREMA DE MORDELL-WEIL

6.1 TEOREMA DE MORDELL-WEIL FRACO

Nosso objetivo nesta seção será demonstrar o seguinte:

Teorema 6.1.1 (**Mordell-Weil**(**fraco**)) *Sejam X uma variedade abeliana sobre um corpo de números K, $X(K)$ o grupo de pontos K racionais de X e seja $m \geq 2$ um inteiro. Então o grupo $X(K)/mX(K)$ é finito.*

Para cumprir nosso objetivo, vamos proceder em duas partes e supor, sem perda de generalidade, que $X_m \subset X(K)$, pois podemos fazer uma extensõa finita de K onde esta propriedade se cumpra e se o teorema de Mordell-Weil(fraco) vale na extensão, vale também em K.

Lema 6.1.2 *Seja $L|K$ uma extenção galoisiana finita, X uma variedade abeliana sobre K. Se $X(L)/mX(L)$ é finito, então $X(K)/mX(K)$ é finito.*

Demonstração: [Sil, pag.190]. □

Proposição 6.1.3 (**Kummer pairing**) *Existe uma função bilinear*

$$t : \mathrm{Gal}(\bar{K}|K) \times X(K) \to X_m$$

com as seguintes propriedades:

(i) *o núcleo à esquerda é $\mathrm{Gal}(\bar{K}|L)$, em que $L = K(m^{-1}X(K))$ é o compositum de todos os corpos da forma $K(y)$ nos quais $[m]y \in X(K)$;*

(ii) *o núcleo à direita é $mX(K)$.*

Portanto, t induz uma função bilinear não degenerada

$$t : \mathrm{Gal}(L|K) \times X(K)/mX(K) \to X_m,$$

que por sua vez induz uma injeção

$$X(K)/mX(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L|K), X_m).$$

Demonstração: Para cada $x \in X(K)$ seja $y \in X(\bar{K})$ tal que $[m]y = x$, isso é sempre possível pois $X(\bar{K})$ é um grupo divisível pelo teorema 4.4.3. Seja agora $\sigma \in \mathrm{Gal}(\bar{K}|K)$. Definimos $t(\sigma, x); = \sigma(y) - y$. Vamos verificar primeiramente que $t(\sigma, x) \in X_m$. De fato,

$$[m](t(\sigma, x)) = [m](\sigma(y) - y) = \sigma([m]y) - [m]y = \sigma(x) - x = 0.$$

Vamos verificar agora que t não depende da escolha de y. De fato, suponha que $[m]y = [m]y' = x$. Então $y' - y \in X_m \subset X(K)$. Desta feita

$$(\sigma(y) - y) - (\sigma(y') - y') = \sigma(y - y') - (y - y') = 0.$$

A verificação da bilinearidade é também bem simples e segue da definição:

$$t(\sigma\sigma', x) = \sigma\sigma'(y) - y = \sigma\sigma'(y) - \sigma(y) + \sigma(y) - y =$$

$$= \sigma(\sigma'(y) - y) + \sigma(y) - y = \sigma(t(\sigma', x)) + t(\sigma, x) = t(\sigma, x) + t(\sigma', x),$$

pois $t(\sigma', x) \in X_m \subset X(K)$.

$$t(\sigma, x + x') = \sigma(y + y') - (y + y') = (\sigma(y) - y) + (\sigma(y') - y') = t(\sigma, x) + t(\sigma, x').$$

(i) Notamos que σ está no núcleo à esquerda de t se e somente se $\sigma(y) = y$ para todo $y \in X(\bar{(}K))$ tal que $[m]y \in X(K)$. Isto é justamente dizer que L é o corpo fixo de tal núcleo e portanto este núcleo é exatamente $\mathrm{Gal}(\bar{k}|L)$.
(ii) Claramente X_m é subconjunto do núcleo á direita de t pois tal grupo tém expoente m. Para mostrar a igualdade, seja x um elemento do núcleo á direita. Temos então que $\sigma(y) = y$ para todo $\sigma \in \mathrm{Gal}(\bar{K}|K)$ e portanto $y \in X(K)$. Daí $x = [m]y \in mX(K)$.
Segue da propriedade universal que, passando ao quociente, obtemos uma aplicação bilinear não degenerada $t : \mathrm{Gal}(L|k) \times X(K)/mX(K) \to X_m$. A inclusão

$$X(k)/mX(k) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L|k), X_m)$$

que desejamos é dada por $x \mapsto t(.,x) \in \hom(\mathrm{Gal}(L|k), X_m)$, cuja injetividade segue diretamente do fato da nossa aplicação bilinear ser não degenerada. □

A partir da proposição acima, para mostrar que $X(K)/mX(K)$ é finito, basta mostrar que o grupo $\mathrm{Hom}(\mathrm{Gal}(L|K), X_m)$ é finito. Como já sabemos que X_m é finito, será bastante mostrar que $\mathrm{Gal}(L|K)$ é finito, que é equivalente a mostrar que a extensão de corpos $L|K$ é finita. Para isso vamos usar um teorema de Hermite, a partir do qual deduziremos um teorema de Chevalley-Weil que irá implicar nosso resultado facilmente.

Teorema 6.1.4 (**Hermite**) *O conjunto dos corpos de números (vistos como subcorpos de $\mathbb{C}$) com dado discriminante é finito.*

Demonstração: [Hin-Sil, pag.273]. □

Teorema 6.1.5 (**Chevalley-Weil**) *Seja $\Phi : X \to Y$ um recobrimento não ramificado entre variedades projetivas normais sobre um corpo de números K. Então existe uma extensão finita $L|K$ tal que:*

$$\Phi^{-1}(Y(K)) \subset X(L).$$

Demonstração: Primeiramente vamos considerar o caso afim, $X = \mathrm{Spec}(B)$ e $Y = \mathrm{Spec}(A)$, onde $A = K[f_1, f_2, \ldots, f_m]$ e B são K domínios de tipo finito. Temos que B é um A–módulo livre de posto n (condição de recobrimento) e além disso existe uma base $\{g_1, g_2, \ldots, g_n\}$ de B sobre A tal que o discriminante $\Delta_A^B(g_1, g_2, \ldots, g_n) \in A^*$ (condição de não ramificação). Ora, seja, para cada $v \in M_k$,

$$\mathcal{U}_v = \{x \in X(K) \mid v(f_i(x)) \geq 0 \ \forall\ 1 \leq i \leq m\}$$

(que depende também dos f_i). Temos que dado $f \in A^* = (K[f_1, f_2, ..., f_m])^*$, clariando o denominador obtemos $af \in \mathcal{O}_K[f_1, f_2, ..., f_m]$ para algum $a \in \mathcal{O}_K$. Analogamente para o inverso de f, existe $b \in \mathcal{O}_K$ tal que $bf^{-1} \in \mathcal{O}_K[f_1, f_2, ..., f_m]$. Assim temos para $\forall x \in \mathcal{U}_v$ e, $\forall v \in M_k$ associado a um primo que não divide a nem divide b, $|af(x)|_v \leq 1$ e $|bf^{-1}(x)|_v \leq 1$. Isso implica $|ab|_v \leq 1$ e mais precisamente $|ab|_v = 1$, pois a e b são K-inteiros . Logo $|f(x)|_v = 1$. Sendo assim para quase todo $v \in M_k$, temos $|\Delta(K(\Phi^{-1}(x))|K)|_v = 1$.

Como A e B são normais, seu anel de inteiros é a interseção das localizações nos primos de altura um. Portanto, denotando $\mathcal{U}((O)_k) = \bigcap_{v \in M_k} \mathcal{U}_v$, temos que existe uma constante c_1 tal que $|\Delta(K(\Phi^{-1}(x))|K)|_v \leq c_1 \ \forall \ x \in \mathcal{U}(\mathcal{O}_K)$ (tal constante pode ser tomada como sendo o máximo (em um número finito) entre os valores absolutos não unitários e 1). Pelo teorema de Hermite,6.1.4, temos que existem apenas um número finito de corpos $K(\Phi^{-1}(x))$ e portanto, tomando seu compositum, encontramos uma extensão finita $L|K$ de K tal que $\Phi^{-1}(\mathcal{U}(\mathcal{O}_K)) \subset X(L)$.

Agora para deduzir nosso resultado podemos considerar X e Y mergulhadas em algum espaço projetivo e lembrando que para qualquer corpo de números $\mathbb{P}^n_K = \mathbb{P}^n_{\mathcal{O}_K}$, deduzimos que para todo $x \in X(K)$ o discriminante $|\Delta(K(\Phi^{-1}(x))|K)|_v$ é limitado, aplicando o caso afim (basta cobrir X com um número finito de abertos afins suficientemente pequenos para estarem contidos nos abertos principais do espaço projetivo). Assim, tomando o compositum das extensões finitas obtidas do caso afim, obtemos uma extensão finita L de K tal que $\Phi^{-1}(Y(K)) \subset X(L)$. □

Corolário 6.1.6 *Seja X uma variedade abeliana sobre um corpo de números K e seja $L = K([m]^{-1}X(K))$ o compositum de todos os corpos da forma $K(y)$, em que $[m]y \in X(K)$. Então, $L|K$ é uma extenção finita.*

Demonstração: Basta notar que o morfismo de multiplicação por m é um recobrimento não ramificado. Assim, como consequência do teorema de Chevalley-Weil, 6.1.5, temos que existe uma extensão finita $E|K$ tal que $L = K([m]^{-1}X(K)) \subset E(X(K)) = E$ e, portanto, $L|K$ é uma extensão finita. □

Da nossa discusão anterior segue o teorema de Mordell-Weil (fraco).

6.2 LEMA DA DESCIDA

O termo descida (infinite descent) é referente ao argumento de Fermat, utilizado ora para mostrar que dada equação difantina não tinha solução, ora para mostrar que uma equação diofantina possuía infinitas soluções(racionais ou inteiras).

Esse argumento foi usado por Fermat por exemplo para mostrar que a equação:

$$x^4 + y^4 = z^2$$

não possuía soluções não triviais em $\mathbb{Z}$, implicando assim que a equação:

$$x^4 + y^4 = z^4$$

não possui soluções não triviais em $\mathbb{Z}$. A idéia era supor a existência de solução não trivial e escolher dentre todas, aquela de menor coordenada positiva x (por exemplo), e a partir desta, construir uma outra com coordenada positiva x menor. Outra aplicação desse raciocínio pode ser vista nas equações de Fermat-Pell

$$x^2 - dy^2 = 1$$

com d livre de quadrados. Elas possuem uma infinidade de soluções em $\mathbb{Z}$ e tais soluções são , de fato, geradas por uma solução fundamental. Novamente o raciocínio é simples: a partir de cada solução, podemos construir outra com coordenada x (por exemplo) estritamente maior que a anterior. Um aspecto fundamental no raciocínio de Fermat reside em saber, de alguma forma, mensurar o "tamanho"de uma solução. No nosso caso, temos uma maneira natural de medir o "tamanho"de uma solução, usando as alturas. Portanto para concluir a demonstração do teorema de Mordell-Weil, vamos mostrar o seguinte:

Lema 6.2.1 (**Lema da descida**) *Seja G um grupo abeliano equipado com uma forma quadrática $q : G \to \mathbb{R}$ satisfazendo as condições:*

(i) *Para cada $B \in \mathbb{R}_+$, o conjunto:*

$$\{x \in G \mid q(x) \leq B\}$$

é finito;

(i) *existe algum inteiro $m \geq 2$ tal que o quociente G/mG é finito.*

Então, G é finitamente gerado.

Mais precisamente, dado um sistema de representantes $\{g_1, g_2, \ldots, g_s\}$ para G/mG, seja $\tilde{B} := \max_i q(g_i)$. Então, G é gerado pelo congunto finito

$$\{x \in G \mid q(x) \leq \tilde{B}\}.$$

Demonstração: Primeiramente, notamos que os pontos de torção tem $q(x) = 0$, pois claramente $q(0) = 0$ e se $m \cdot x = 0$, então $m^2 q(x) = 0$. Mostramos agora que $\forall x \in G,\ q(x) \geq 0$. Se G for de torção é finito pela condição (i) e não há nada para mostarar. Em caso contrário, escolhendo $x \in G$ de período infinito, se $q(x) < 0$ teremos $q(mx) = m^2 q(x) < 0$ para cada $m \in \mathbb{Z}$ e portanto existiriam infinitos elementos no conjunto $\{x \in G \mid q(x) \leq 0\}$, contradizendo a condição (i). Podemos definir $|x| := \sqrt{q(x)}$, $b := \max_i |g_i|$ e considerar o conjunto finito $S = \{x \in G \mid |x| \leq b\}$.
Queremos mostrar que $G =< S >$. Seja agora $x_0 \in G$. Se $x_0 \in S$ nada há para fazer. Em caso contrário, $|x_0| > b$. Reduzindo módulo mG, $x_0 = g_i + m.x_1$ para algum $x_1 \in G$. Usando a desiguldade triangular obtemos:

$$m|x_1| = |x_0 - g_i| \leq |x_0| + |g_i|.$$

Como $|g_i| \leq b < |x_0|$, $m|x_1| < 2|x_0|$ e como $m \geq 2$ obtemos que $|x_1| < |x_0|$. Se $x_1 \in S$, então $x_0 = x_1 + m \cdot g_i \in < S >$. Em caso contrário,$|x_1| > b$. Reduzindo módulo mG, $x_1 = g_j + m \cdot x_2$ para algum $x_2 \in G$. Uma verificação análoga nos mostra que $|x_2| < |x_1|$. Raciocinando indutivamente, construímos uma sequência de elementos de G, tal que $|x_0| > |x_1| > |x_2| > \ldots$. Pela propriedade (i) de nosso enunciado, tal sequência deve estacionar e, de fato, isso deve ocorrer em um elemento de S. Como x_k é combinação linear dos $x_i,\ i \geq k+1$ e elementos de S, por indução decrescente mostra-se que x_0 é combinação linear de elementos de S. □

6.3 TEOREMA DE MORDELL-WEIL

Teorema 6.3.1 (**Mordell-Weil**) *Seja X uma variedade abeliana sobre um corpo de números K. Então o grupo dos pontos K-racionais, $X(K)$, é um grupo abeliano finitamente gerado.*

Demonstração: A demonstração do teorema de Mordell-Weil foi dividida em três partes:

i) (Forma Quadrática) Existe uma forma forma quadrática em $X(K)$:

$$\widehat{\mathrm{h}}_{X,\mathfrak{L}} : X(K) \to \mathbb{R},$$

chamada a altura canônica em X relativa a $\mathfrak{L}$ (fibrado linear) tal que para cada $B \in \mathbb{R}$, o conjunto:

$$\{x \in X(K) \mid \widehat{h}_{X,\mathfrak{L}}(x) \leq B\}$$

é finito. Isto foi mostrado na seção de alturas bastando escolher $\mathfrak{L}$ simétrico, para usarmos o teorema de Neron-Tate 5.4.2 e amplo para garantir a finitude do conjunto dos pontos de altura limitada, pelo teorema das propriedades das alturas de Weil 5.2.7.

ii) (Mordell-Weil(fraco)) Para cada $m \geq 2$ o grupo $X(K)/mX(K)$ é finito. Isto foi mostrado numa seção anterior como consequência do teorema 6.1.6.

iii) (Lema da descida) Seja G um grupo abeliano equipado com uma forma quadrática $q : G \to \mathbb{R}$ satisfazendo as condições:

(i) Para cada $B \in \mathbb{R}_+$, o conjunto:

$$\{x \in G \mid q(x) \leq B\}$$

é finito;

(i) existe algum inteiro $m \geq 2$ tal que o quociente G/mG é finito.

Então G é finitamente gerado. Isto foi mostrado na seção anterior como sendo o *Lema da descida*, 6.2.1.

O teorema de Mordell-Weil está, portanto, completamente demonstrado. □

Lembramos que novamente que todo grupo abeliano finitamente gerado G pode ser (abstratamente) descrito da forma:

$$G \simeq G_{\text{tor}} \bigoplus \mathbb{Z}^{\oplus r},$$

onde G_{tor} é a parte de torção de G, necessariamente finita, e $r = \text{rk}(G)$ é o posto de G.

Portanto para variedades abelianas sobre um corpo de números K, podemos definir a noção de *posto* de uma tal variedade, como o posto do grupo abeliano

finitamente gerado dos seus pontos K-racionais. O problema do calculo do posto faz parte de uma importante Conjectura de Birch e Swinnerton-Dyer sobre a qual não falaremos, Este problema é ainda aberto para curvas elipticas definidas sobre $\mathbb{Q}$. Em particular não é conhecida a existencia de tais curvas elipticas de posto arbitrariamente grande e nem se (e por qual razão) o posto das curvas elipticas sobre $\mathbb{Q}$ seja universalmente limitado.

CAPÍTULO 7

TEOREMA DE FALTINGS

Neste capítulo, nosso objetivo é dar uma idéia de como a conjectura de Mordell (Teorema de Faltings) se relaciona com outras conjecturas e outros teoremas, dando uma linha de raciocínio de como completar a demonstração sem fornecer todos os detalhes. As dificuldades técnicas serão completamente escondidas de modo que a impresão de facilidade é falsa.

Na primeira seção, vamos introduzir o importante conceito da jacobiana de uma curva, uma variedade abeliana relacionada com a curva que retém propriedades geométricas da mesma. Na segunda seção mostraremos como a desigualdade de Vojta implica o teorema de Faltings. A desigualdade de Vojta é um profundo resultado sobre aproximação diofantina que vamos assumir sem maiores referências. As outras seções se dedicam a ilustrar o caminho seguido pelo próprio Faltings na demonstração original.

Teorema 7.0.2 (**Conjectura de Mordell-Teorema de Faltings**) *Sejam K um corpo de números e seja $\mathcal{C}$ uma curva lisa sobre K, cujo gênero é maior ou igual a dois. Então $\mathcal{C}(K)$ consiste de um conjunto finito.*

7.1 VARIEDADE JACOBIANA

Em primeiro lugar, consideremos uma superfície de Riemann X de gênero $g \geq 1$ e um ponto P_0. A integração por caminhos partindo de P_0 é bem definida módulo Γ, o reticulado dos períodos (base da homologia), e fornece uma injeção:

$$\begin{array}{rccll} \iota: & X & \hookrightarrow & \mathrm{Jac}(X) := \mathbb{C}^g/\Gamma & \\ & P & \mapsto & (\int_{P_0}^{P} \omega_1, \ldots, \int_{P_0}^{P} \omega_g) & \mod\ (\Gamma). \end{array}$$

Mostra-se que a variedade $\mathrm{Jac}(X)$, que é um toro complexo de dimensão g, é uma variedade abeliana chamada *variedade jacobiana de X*. Weil generalizou a definição de variedade jacobiana para curvas lisas definidas sobre um corpo qualquer. Sua

construção utiliza as potências simétricas da curva e pode ser encontrada com detalhes em [Hin-Sil, pag.134]. A descrição que nos interessa pode ser sumarizada no seguinte:

Teorema 7.1.1 (**Construção da jacobiana**) *Seja $\mathcal{C}$ uma curva lisa de gênero $g \geq 1$, projetiva sobre um corpo K. Existe uma variedade abeliana sobre K de dimensão g,* $\mathrm{Jac}(\mathcal{C})$*, chamada jacobiana de $\mathcal{C}$, e um mergulho:*

$$\iota : \mathcal{C} \hookrightarrow \mathrm{Jac}(\mathcal{C}),$$

que pode ser escolhido um K-mergulho se $\mathcal{C}(K) \neq \emptyset$. O morfismo ι satisfaz as seguintes propriedades:

(i) *Estendendo ι linearmente a* $\mathrm{Div}(\mathcal{C})$*, ι induz um isomorfismo de grupos*

$$\mathrm{Pic}^0(\mathcal{C}(L)) \simeq \mathrm{Jac}(\mathcal{C})(L)$$

desde que na extensão $L|K$, $\mathcal{C}(L) \neq \emptyset$ (ι é L-morfismo)

(ii) *Para cada $r \geq 0$ definimos $W_r \in$* $\mathrm{Jac}(\mathcal{C})$*:*

$$W_r = \iota(\mathcal{C}) + ... + \iota(\mathcal{C}) = \sum_{i=1}^{r} \iota(C).$$

Então, $\dim(W_r) = \min(r, g)$ *e* $W_g = \mathrm{Jac}(\mathcal{C})$.

(iii) *Se $\Theta = W_{g-1}$, então, Θ é um divisor irredutível e amplo em* $\mathrm{Jac}(\mathcal{C})$*, chamado divisor Theta.*

7.2 A DESIGUALDADE DE VOJTA

Durante toda a seção, sejam K um corpo de números, $\mathcal{C}$ uma curva projetiva e lisa sobre K de gênero maior ou igual a dois. Vamos supor $\mathcal{C}(K) \neq \emptyset$, e considerar o K-mergulho $\iota : \mathcal{C} \hookrightarrow \mathrm{Jac}(\mathcal{C})$. Sejam ainda $\Theta \in \mathrm{Pic}(\mathrm{Jac}(\mathcal{C}))$ o divisor theta, $|\ .\ |$ a norma em $\mathrm{Jac}(\mathcal{C})(\bar{K})$ associada à altura canônica relativa a Θ e $<\ .\ ,\ .\ >$ a forma bilinear associada em $\mathrm{Jac}(\mathcal{C}(\bar{K}))$. Lembramos que a norma $|\ .\ |$ se estende linearmente a uma forma quadrática definida positiva em $\mathrm{Jac}(\mathcal{C}(\bar{K})) \otimes \mathbb{R}$ e que a forma bilinear se estende linearmente a um produto interno euclidiano.

Teorema 7.2.1 (**Desigualdade de Vojta**) *Seja $\mathcal{C}$ uma curva lisa e projetiva sobre um corpo de números K de gênero $g = g(C) \geq 2$. Existem constantes $\kappa_1 = \kappa_1(C)$ e $\kappa_2 = \kappa_2(g)$ tais que, se $z, w \in \mathcal{C}(\bar{K})$ satisfazem $|z| \geq \kappa_1$ e $|w| \geq \kappa_2|z|$, então*

$$< z, w > \leq \frac{3}{4}|z||w|.$$

Demonstração: [Hin-Sil, pag.379-425]. □

Teorema 7.2.2 *Seja $\mathcal{C}$ uma curva lisa e projetiva sobre um corpo de números K, cujo gênero seja maior ou igual a dois. A desigualdade de Vojta, teorema 7.2.1, implica o teorema de Faltings 7.0.2, i.e. $\mathcal{C}(K)$ é finito.*

Demonstração: Denotemos $J = \mathrm{Jac}(\mathcal{C})$. Em primeiro lugar notemos que o núcleo do homomorfismo:

$$J(K) \to J(K) \otimes \mathbb{R}$$

é exatamente o subgrupo de torção $J(K)_{\mathrm{tor}}$, que é finito pelo teorema de Mordell-Weil. Portanto para mostrar que $\mathcal{C}(K)$ é finito, é suficiente mostrar que a imagem de $\mathcal{C}$ em $J(K) \otimes \mathbb{R}$ é finita. Vamos denotar tal imagem $C(K)$. A forma bilinear $< \ . \ , \ . \ >$ dá a $J(K) \otimes \mathbb{R}$ uma estrutura de espaço euclidiano de dimensão finita, de modo que podemos definir o ângulo entre dois pontos da maneira usual:

$$\cos(\theta(x, y)) = \frac{< x, y >}{|x||y|}.$$

Sejam x_0 um ponto de $J(K) \otimes \mathbb{R}$ e θ_0 um ângulo. Vamos denotar por Γ_{x_0,θ_0} o cone de direção x_0 e ângulo central $2\theta_0$.

$$\Gamma_{x_0,\theta_0} = \{x \in J(K) \otimes \mathbb{R} \mid \theta(x, x_0) < \theta_0\}.$$

A desigualdade de Vojta será usada agora para mostrar que se θ_0 é suficientemente pequeno, então a interseção

$$\Gamma_{x_0,\theta_0} \cap \mathcal{C}(K)$$

é finita. Vamos supor que tal interseção seja finita. Como em $J(K)$ (e por conseguinte $\mathcal{C}(K)$) é finito o número de pontos de norma limitada, existe $z \in \Gamma_{x_0,\theta_0} \cap \mathcal{C}(K)$ tal que $|z| \geq \kappa_1$. Portanto podemos encontrar $w \in \Gamma_{x_0,\theta_0} \cap \mathcal{C}(K)$ tal que $|w| \geq \kappa_2|z|$. Pela desigualdade de Vojta, teorema 7.2.1, temos que:

$$< z, w > \leq \frac{3}{4}|z||w|,$$

ou equivalentemente:

$$\cos\theta(z,w) \leq \frac{3}{4}.$$

Deduzimos que

$$\theta(z,w) \geq \arccos(\frac{3}{4}) \Rightarrow 2\theta_0 \geq \arccos(\frac{3}{4}).$$

Logo, escolhendo θ_0 menor que $\frac{1}{2}\arccos(\frac{3}{4})$, temos que a interseção

$$\Gamma_{x_0,\theta_0} \cap \mathcal{C}(K)$$

é finita.

Para concluir nossa demonstração, vamos mostrar que $J(K) \otimes \mathbb{R}$ pode ser coberto por um número finito de cones com ângulo pequeno. De fato, considere a esfera unitária:

$$S = \{x \in J(K) \otimes \mathbb{R} |\ |x| = 1\}$$

e seja θ_0 um ângulo pequeno. Temos que

$$S = \bigcup_{x \in S} (\Gamma_{x,\theta_0} \cap S).$$

Claramente $\Gamma_{x,\theta_0} \cap S$ é um aberto em S. Como S é compacto, de nossa cobertura podemos extrair uma subcobertura finita. Os cones dessa subcobertura certamente cobrem $J(K) \otimes \mathbb{R}$, concluindo a demonstração. □

7.3 VARIEDADE ABELIANA DUAL E POLARIZAÇÕES

Definição 7.3.1 *Seja X uma variedade abeliana.* $\mathrm{Pic}^0(X)$ *é o grupo das classes de isomorfismo de fibrados lineares que são invariantes por translação, $t_P : X \to X$, i.e.*

$$\mathrm{Pic}^0(X) = \{\mathfrak{L} \in \mathrm{Pic}(X) \mid t_P^*\mathfrak{L} \simeq \mathfrak{L}\ \forall P \in X(\bar{K})\}.$$

Teorema 7.3.2 *Sejam X uma variedade abeliana e $\mathfrak{L}$ um fibrado linear em X. Consideremos o homomorfismo dado pelo teorema do quadrado:*

$$\begin{array}{rccc} \Phi_{\mathfrak{L}}: & X & \to & \mathrm{Pic}(X) \\ & P & \mapsto & t_P^*\mathfrak{L} \otimes \mathfrak{L}^{-1}. \end{array}$$

então:

(i) $\mathrm{Im}(\Phi_{\mathfrak{L}}) \subset \mathrm{Pic}^0(X)$;

(ii) *se* $\mathfrak{L}^n \in \mathrm{Pic}^0(X)$, $n \neq 0$, *então* $\mathfrak{L} \in \mathrm{Pic}^0(X)$;

(iii) *se* $\mathfrak{L}$ *é amplo, então:*

$$\Phi_{\mathfrak{L}} : X \to \mathrm{Pic}^0(X)$$

é sobrejetiva e tem núcleo finito.

Demonstração: [Hin-Sil, pag.128]. □

Definição 7.3.3 *Seja X uma variedade abeliana. O grupo de Néron-Severi de X é o grupo quociente:*

$$\mathrm{NS}(X) = \mathrm{Pic}(X)/\,\mathrm{Pic}^0(X).$$

Existe uma injeção natural:

$$\mathrm{NS}(X) \hookrightarrow \mathrm{Hom}(X, \mathrm{Pic}^0(X)),$$

associando a $[\mathfrak{L}]$ o morfismo $\Phi_{\mathfrak{L}}$, que não depende da escolha do representante na classe de equivalência.

Definição 7.3.4 *Seja X uma variedade abeliana. Uma variedade abeliana $\hat{X}$ é chamada variedade abeliana dual de X, se existir um fibrado linear $\mathcal{P}$ em $X \times \hat{X}$, chamado feixe de Poicaré, tal que, definindo $\mathrm{i}_P(\widehat{P}) = (P, \widehat{P})$ e $\mathrm{i}_{\widehat{P}}(P) = (P, \widehat{P})$, as aplicações:*

$$\hat{X} \to \mathrm{Pic}^0(X)\ ,\ \widehat{P} \mapsto \mathrm{i}_{\widehat{P}}^*(\mathcal{P}),$$

$$X \to \mathrm{Pic}^0(\hat{X})\ ,\ P \mapsto \mathrm{i}_P^*(\mathcal{P})$$

sejam bijeções.

Se existe $\hat{X}$, $\mathrm{Pic}^0(X)$ tem uma estrutura de variedade abeliana e quando $\mathfrak{L}$ é amplo, a aplicação:

$$\Phi_{\mathfrak{L}} : X \to \hat{X}$$

é uma isogenia.

Teorema 7.3.5 *Seja X uma variedade abeliana. Então a variedade abeliana dual existe e o par $(\hat{X}, \mathcal{P})$ é único a menos de isomorfismo.*

Demonstração: [Cor-Sil, pag.119]. □

Definição 7.3.6 *Seja X uma variedade abeliana e $\mathfrak{L}$ um fibrado linear amplo em X, cuja classe em $\mathrm{NS}(X)$ denotaremos ainda por $\mathfrak{L}$. A isogenia $\Phi_{\mathfrak{L}} : X \to \hat{X}$ é chamada uma polarização de X. O grau de uma polarização é o grau da isogenia. A isogenia $\Phi_{\mathfrak{L}}$ chama-se polarização principal quando seu grau for um. Nesse caso $\Phi_{\mathfrak{L}}$ é um isomorfismo. Vamos denotar por $(X, \mathfrak{L})$ uma variedade abeliana polarizada. Um morfismo entre variedades abelianas polarizadas $(X_i, \mathfrak{L}_i)$, $i = 1, 2$, é um morfismo entre as variedades abelianas:*

$$\Phi : X_1 \to X_2$$

tal que:

$$\Phi^*(\mathfrak{L}_2) = \mathfrak{L}_1 \in \mathrm{NS}(X_1).$$

Teorema 7.3.7 *Sejam $\mathcal{C}$ uma curva definida sobre K, $\mathrm{Jac}(\mathcal{C})$ sua variedade jacobiana, $\iota : \mathcal{C} \hookrightarrow \mathrm{Jac}(\mathcal{C})$ o mergulho jacobiano e $\theta \in \mathrm{NS}(\mathrm{Jac}(\mathcal{C}))$ a classe do divisor Θ, então o par $(\mathrm{Jac}(\mathcal{C}), \theta)$ determina uma polarização principal.*

Demonstração: [Cor-Sil, pag. 136] □

Teorema 7.3.8 *Seja X uma variedade abeliana sobre um corpo algebricamente fechado K. É finito o número de classes de isomorfismos de variedades abelianas polarizadas $(X, \mathfrak{L})$ com grau fixado de polarização. Em particular é finito o número de classes de isomorfismo de variedades abelianas principalmente polatizadas $(X, \mathfrak{L})$*

Demonstração: [Cor-Sil, pag.140]. □

7.4 TEOREMA DE TORELLI

Todo isomorfismo entre curvas induz de maneira natural um isomorfismo entre suas jacobianas principalmente polarizadas, isto é, se $\alpha : \mathcal{C}_1 \to \mathcal{C}_2$ é um isomorfismo, então existe um isomorfismo:

$$\beta : (\mathrm{Jac}(\mathcal{C}_1), \theta_1) \to (\mathrm{Jac}(\mathcal{C}_2), \theta_2).$$

Não é verdade em geral que um isomorfismo entre as jacobianas induza um isomorifsmo, entre as curvas. Isto é verdade se o isomorfismo for de variedades abelianas polarizadas pelo seguinte:

Teorema 7.4.1 (**Torelli**) *Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ curvas lisas e projetivas sobre um corpo algebricamente fechado K. Considere os respectivos mergulhos jacobianos: $\iota_i : \mathcal{C}_i \hookrightarrow \mathrm{Jac}(\mathcal{C}_i)$, $i = 1, 2$. Se $\beta : (\mathrm{Jac}(\mathcal{C}_1), \theta_1) \to (\mathrm{Jac}(\mathcal{C}_2), \theta_2)$ é um isomorfismo de variedades abelianas polarizadas, então existe um isomorfismo:*

$$\alpha : \mathcal{C}_1 \to \mathcal{C}_2$$

tal que

$$\iota_2 \circ \alpha = \pm\beta \circ \iota_1 + c$$

para algum $c \in \mathrm{Jac}(\mathcal{C}_2)(K)$.

Demonstração: [Cor-Sil, pag.202]. □

O teorema de Torelli é clássico, entretanto, no âmbito da geometria aritmética, fez-se necessária a seguinte generalização:

Corolário 7.4.2 *Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ curvas lisas e projetivas sobre um corpo K e de gênero $g \geq 2$. Se as jacobianas principalmente polarizadas de $\mathcal{C}_1$ e $\mathcal{C}_2$ são K-isomorfas, então $\mathcal{C}_1$ e $\mathcal{C}_2$ são também K-isomorfas.*

Demonstração: [Cor-Sil, pag.203]. □

Teorema 7.4.3 *Seja X uma variedade abeliana sobre um corpo K. É finito o número de classes de isomorfismos de curvas $\mathcal{C}$ sobre K, mergulhadas sobre K em suas jacobianas $\mathrm{Jac}(\mathcal{C})$ e tais que:*

$$\mathrm{Jac}(\mathcal{C}) \simeq X,$$

isto é, de maneira que suas jacobianas sejam K-isomorfas a X.

Demonstração: [Cor-Sil, pag.202]. □

7.5 CONJECTURA DE SHAFAREVICH

Definição 7.5.1 *Sejam (R, m) um anel de valorização discreta e F seu corpo de frações. Consideremos uma curva lisa e projetiva $\mathcal{C}$ definida sobre F. Dado $y \in \mathrm{Spec}(R)$, dizemos que $\mathcal{C}$ tem boa redução em y, se existir um R-esquema X próprio e liso, tal que $X_F = \mathcal{C}$. Nesse caso, se $k = R/\mathfrak{m}$ é o corpo residual, então a fibra X_k é uma curva não singular sobre k, tendo o mesmo gênero de $\mathcal{C}$.*

Definição 7.5.2 *Seja K um corpo de números. Dados $\mathcal{C}$ uma curva sobre K e $y \in Y = \mathrm{Spec}(\mathcal{O}_K)$, dizemos que $\mathcal{C}$ tem boa redução em y se $\mathcal{C}_{\mathcal{O}_{y,Y}}$ tem boa redução em y no sentido previamente exposto.*

Conjectura 7.5.3 (**Shafarevich**) *Sejam K um corpo de números e $S \subset M_K$ um conjunto finito de Places. É finito o número de curvas lisas e projetivas sobre K de gênero g, modulo K-isomorfismo, que tem boa redução em todos os Places exceto os de S.*

Lema 7.5.4 *Sejam K um corpo de números, $\mathcal{C}$ uma curva projetiva lisa sobre K de gênero $g \geq 1$ e $S \subset M_K$ um conjunto finito de Places. Suponha que $\mathcal{C}$ tem boa redução fora de S. Então existe uma extensão finita $L|K$ e um conjunto finito de Places $\tilde{S} \subset M_L$ (contendo os Places referentes aos primos que dividem 2) tal que: para cada ponto racional $P \in \mathcal{C}(K)$, existe um recobrimento $\pi_P : \mathcal{C}_P \to \mathcal{C}_L$ com boa redução fora de $\tilde{S}$, de grau $\deg(\pi_P) \leq 2 \cdot 2^{2g}$, com índice de ramificação menor ou igual a dois em P e não ramificada en todos os pontos de $\mathcal{C}_L$. Em particular o gênero de $\mathcal{C}_P$ é limitado, como conseqüencia da fórmula de Hurwitz.*

Demonstração: [Cor-Sil, pag.197,198] ou [La 2, pag.105]. □

O ponto essencial onde se usa a hipotese do gênero de $\mathcal{C}$ é maior ou igual a dois é descrito no seguinte:

Teorema 7.5.5 (**de–Franchis**) *Sejam X uma variedade sobre um corpo K e $\mathcal{C}$ uma curva de gênero $g \geq 2$ sobre K. Então é finito o número de aplicações racionais genericamente sobrejetivas de X em $\mathcal{C}$.*

Demonstração: [La 1, pag223]. □

Teorema 7.5.6 *A conjectura de Shafarevich implica a conjectura de Mordell.*

Demonstração: Seja $\mathcal{C}$ uma curva projetiva, lisa e de gênero $g \geq 2$ sobre K. Suponha ainda que $\mathcal{C}$ têm boa redução fora um conjunto de *Places* de K. Para cada ponto $P \in \mathcal{C}(K)$ existe pelo lema 7.5.4, um recobrimento $\pi_P : \mathcal{C}_P \to \mathcal{C}$ em que o gênero de $\mathcal{C}_P$ é limitado e $\mathcal{C}_P$ tem boa redução fora de S. Suponha (por absurdo) que o conjunto $\mathcal{C}(K)$ dos pontos K-racionais de $\mathcal{C}$ seja infinito. Como o conjunto das classes de isomorfismo das curvas $\mathcal{C}_P$ é finito pela conjectura de Shafarevich, 7.5.3, devemos ter uma infinidade de curvas isomorfas a uma dada $\mathcal{C}_{P_0}$. Desta forma obteríamos infinitos morfismos sobrejetivos de $\mathcal{C}_{P_0}$ em $\mathcal{C}$ que é um absurdo pelo teorema de de Franchis, 7.5.5. Portanto o conjunto $\mathcal{C}(K)$ é finito. □

A partir da conseqüência do teorema de Torelli dada pelo teorema 7.3.8, podemos reduzir a conjectura de Shafarevich para curvas na seguinte:

Conjectura 7.5.7 (**Shafarevich para Variedades Abelianas**) *Sejam K um corpo de números, $S \subset M_K$ um conjunto finito de Places. O número de classes de isomorfismo de variedades abelianas X sobre K, que tem boa redução fora de S, é finito.*

7.6 TEOREMAS DE FINITUDE DE FALTINGS

Como a conjectura de Mordell pode ser reduzida a conjectura de Shafarevich para variedades abelianas, para demonstrá-la é suficiente mostrarmos os seguintes teoremas de finitude para variedades abelianas devidos a Faltings.

Teorema 7.6.1 (**Faltings I**) *Seja X uma variedade abeliana definida sobre um corpo de números K. É finito o numero de classes de isomorfismos de variedades abelianas que são K-isógenas a X.*

Teorema 7.6.2 (**Faltings II**) *Sejam K um corpo de números e $S \in M_K$ um conjunto finito de Places. Então é finito o número de classes de K-isogenias de variedades abelianas de dimensão fixada, que tenham boa redução fora de S.*

Nas duas seções subseqüentes explicaremos que o teorema 7.6.1, (Faltings I) implica o teorema 7.6.2, (Faltings II). Na última seção vamos mostrar um dos pontos de vista que podem ser usados na demonstração do teorema 7.6.1, (Faltings I).

Tal ponto de vista está diretamente relacionado com a demonstração original de Faltings e em última instância consiste em definir uma altura de variedades abelianas que tenha uma propriedade de finitude sensível a isogenias. A conclusão da técnica pode ser sumarizada pelo seguinte:

Teorema 7.6.3 *Sejam K um corpo de números e X uma variedade abeliana sobre K. O conjunto das alturas de Faltings das variedades abelianas K-isógenas a X é finito.*

Há um segundo ponto de vista, devido a Masser-Wüstholz, e não abordado, que consiste em resolver o problema geral descrito no seginte:

Teorema 7.6.4 *Sejam d, m e n inteiros positivos. Então existem constantes $c = c(m,n,d)$ e r=r(n) tendo a seguinte propriedade: se X e Y são variedades abelianas de dimensão n sobre um corpo de números K de grau d, tendo polarizações de gau no máximo m, e se X e Y são K-isógenas, então existe uma K-isogenia de grau limitado em termos de X por:*

$$c \cdot \max(1, \mathrm{h}_{\mathrm{Fal}}^{\mathrm{st}}(X))^r,$$

onde $\mathrm{h}_{\mathrm{Fal}}^{\mathrm{st}}(X)$ é a áltura estavel de Faltings de X que definiremos em seguida.

É claro que ambos teoremas implicam o teorema Faltings I.

7.7 REPRESENTAÇÕES E BOA REDUÇÃO

Definição 7.7.1 *Sejam G um grupo e V um espaço vetorial sobre um corpo K. Uma representação de G em V um homomorfismo (contínuo):*

$$\rho : G \to \mathrm{Aut}(V)$$

Nestas condições $\mathrm{Aut}(V)$ adquire uma estrutura de $\mathbb{Z}(G)$-módulo. Dizemos que a representação é semisimples se a estrutura de $\mathbb{Z}(G)$-módulo de $\mathrm{Aut}(V)$ for semisimples.

As representações semisimples são de primordial importância pela seguinte:

Proposição 7.7.2 *Sejam G um grupo, $\rho : G \to \mathrm{Aut}(V)$ e $\tilde{\rho} : G \to \mathrm{Aut}(V)$ duas representações de G num espaço vetorial de dimensão finita sobre um corpo de característoca zero. Então ρ e $\tilde{\rho}$ são isomorfas se e somente se:*

$$\mathrm{Tr}(\rho(g)) = \mathrm{Tr}(\tilde{\rho(g)}) \ , \ \forall g \in G.$$

Demonstração: [Hu, pag.277]. □

Definição 7.7.3 *Uma representação l-ádica do grupo de Galois $\mathrm{Gal}(\bar{K}|K)$ de um corpo K é um homomorfismo contínuo:*

$$\rho : \mathrm{Gal}(\bar{K}|K) \to \mathrm{Gl}(V) = \mathrm{Gl}_n(\mathbb{Q}_l)$$

em que V é um espaço vetorial $\mathbb{Q}_l$-ádico de dimensão n.

Definição 7.7.4 *Seja X uma variedade abeliana definida sobre um corpo K e considere um primo l diferente da característica de K. A multiplicação por l fornece uma aplicação natural nos subgrupos de l^n-torção :*

$$X[l^n] \to X[l^{n+1}].$$

Tais aplicações comutam com os isomorfismos $X[l^n] \simeq (\mathbb{Z}/l^n\mathbb{Z})^{2d}$, onde $d = \dim(X)$. Desta feita, podemos tomar o limite projetivo e assim definir o módulo de Tate:

$$T_l(X) := \lim_{\leftarrow} X[l^n].$$

Da nossa discussão anterior é fácil ver que que o módulo de Tate tem assim uma estrutura natural de $\mathbb{Z}_l$-módulo livre com posto $2d$. Definimos também os $\mathbb{Q}_l$ espaços vetoriais $V_l(X) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(X)$.

A definição do módulo de Tate tem propriedades funtoriais de modo que se temos um homomorfismo de variedades abelianas

$$\Phi : X \to Y,$$

ele induz de maneira natural um homomorfismo nos módulos e espaços vetoriais de Tate:

$$T_l(\Phi) : T_l(X) \to T_l(Y),$$

$$V_l(\Phi) : V_l(X) \to V_l(Y).$$

Após escolhermos uma base obtemos representações de $\mathrm{Gal}(\bar{K}|K)$ em $\mathrm{Gl}_{2d}(\mathbb{Z}_l)$ e em $\mathrm{Gl}_{2d}(\mathbb{Q}_l)$, induzidas pela açã natural do grupo de Galois $\mathrm{Gal}(\bar{K}|K)$ no módulo de Tate. Essas são as principais representações l-ádicas.

Para nossas aplicações considere K um corpo de números, $\upsilon \in M_K^0$ um *Place* finito, $\mathcal{O}_\upsilon$ o anel de valorização discreta que é o completamento de $\mathcal{O}_K$ com respeito a υ e F o corpo de frações de $\mathcal{O}_\upsilon$. Seja Υ um Place de $\bar{F}$ tal que $\Upsilon|\upsilon$.

Definição 7.7.5 *O grupo de decomposição de* Υ*,* G_Υ *é o subgrupo de* $\mathrm{Gal}(\bar{F}|F)$ *consistindo de todos os elementos que fixam* Υ*, isto é:*

$$G_\Upsilon = \{\sigma \in \mathrm{Gal}(\bar{F}|F) \mid \sigma(\Upsilon) = \Upsilon\}.$$

A partir de nossa definição, podemos identificar G_Υ com o grupo de Galois do completamento:

$$G_\Upsilon = \mathrm{Gal}(\bar{F}_\Upsilon|F_\upsilon).$$

Se $\Upsilon|\upsilon$ e $\tilde{\Upsilon}|\upsilon$ então G_Υ e $G_{\tilde{\Upsilon}}$ são conjugados.

Cada elemento de G_Υ induz um automorfismo do corpo residual k_Υ sobre k_υ e, portanto, existe um homomorfismo sobrejetivo natural:

$$\Phi_\Upsilon : G_\Upsilon \to \mathrm{Gal}(k_\Upsilon|k_\upsilon).$$

Definição 7.7.6 *O núcleo do homomorfismo* Φ_Υ *é chamado o grupo de inércia e denotado* I_Υ*.*

É fácil mostrar que os grupos de inércia são conjugados no caso em que $\Upsilon|\upsilon$ e $\tilde{\Upsilon}|\upsilon$. O anulamento do grupo de inércia fornece um critério de não ramificação, daí, dada uma representação:

$$\rho : \mathrm{Gal}(\bar{F}|F) \to \mathrm{Aut}(V)$$

dizemos que ρ é não ramificada em υ se seu núcleo contém o grupo de inércia.

Com as mesmas notações anteriores, consideremos k_v o corpo residual de $\mathcal{O}_v$ e k_Υ o corpo residual de $\mathcal{O}_\Upsilon$. Se k_Υ é um corpo finito com q elementos, existe um único elemento $\sigma \in \mathrm{Gal}(k_\Upsilon|k_v)$ tal que:

$$\sigma(x) = x^q \ , \ \forall x \in k_\Upsilon.$$

Tal elemento é chamado o automorfismo de Frobenius. Portanto, existe um único elemento $\mathrm{Fr}_\Upsilon \in G_\Upsilon/I_\Upsilon$ que induz o automorfismo de Frobenius em k_Υ. Outra vez, temos que, dois tais elementos são conjugados.

Se $\mathrm{Fr} \in G_\Upsilon$ é o elemento de Frobenius, então, considerando a representação $V_l(\mathrm{Fr})$ em $V_l(X)$. Podemos dterminar as raízes do polinômio característico de $V_l(\mathrm{Fr})$ e temos assim o seguinte:

Teorema 7.7.7 *As raízes do polinômio característico do elemento de Frobenius $V_l(\mathrm{Fr})$ são algébricos e tem valor absoluto $q^{1/2}$. O polinômio característico tem coeficientes inteiros. Em particular o traço do elemento de Frobenius é inteiro e satisfaz:*

$$|\operatorname{Tr}(\rho_l(Fr))| \leq 2dq^{1/2}.$$

Demonstração: [La 2, pag.85]. □

Definição 7.7.8 *Seja X uma variedade não singular sobre um corpo F que é o corpo de frações de um domínio de valorização discreta $\mathcal{O}_v$. Dizemos que X tem boa redução em v se existir um modelo, isto é, um esquema liso e próprio sobre $S = \mathrm{Spec}(\mathcal{O}_v)$:*

$$\tilde{X} \to S$$

tal que a fibra genérica desse esquema seja (isomorfa a) X.

Definição 7.7.9 *Se X_F é uma variedade abeliana, um modelo de Néron para X_F é esquema em grupos liso sobre $S = \mathrm{Spec}(\mathcal{O}_v)$:*

$$N(X_F) \to S$$

tal que a fibra genérica seja X_F e tal que para cada morfismo liso $Y \to S$, o homomorfismo natural:

$$\mathrm{Mor}_S(Y, N(X)) \to \mathrm{Mor}_F(Y_F, X_F)$$

seja um isomorfismo.

Teorema 7.7.10 (**Néron(local)**) *Seja X uma variedade abeliana sobre um corpo F que é o corpo de frações de um anel de valorização discreta R. O modelo de Néron existe, é de tipo finito sobre S e é único a menos de $S = Spec(R)$-isomorfismos.*

Demonstração: [Cor-Sil, pag.214]. □

Teorema 7.7.11 (**Néron-Ogg**) *Seja X uma variedade abeliana sobre um corpo F, corpo de frações de um anel de valorização discreta. Seja l um primo diferente da característica do corpo residual. Então, X tem boa redução se e somente se a representação de $\mathrm{Gal}(\bar{F}|F)$ em $V_l(X)$ for não ramificada.*

Demonstração: [La 2, pg. 113]. □

Corolário 7.7.12 (**Koizumi-Shimura**) *Sejam X e Y variedades abelianas sobre um corpo F, corpo de frações de um anel de valorização discreta. Se Y é isógena a X sobre F e se X tem boa redução, então Y tem boa redução.*

Demonstração: [La 2, pag.113]. □

No caso global temos uma construção similar:

Definição 7.7.13 *Seja R um domínio de Dedekind, com anel de frações K, Se X é uma variedade abeliana sobre K, então um modelo de Néron $N(X)$ para X é um esquema em grupos sobre $Spec(R)$ cuja fibra genérica seja X e que satisfaz a seguinte propriedade universal:*
Se Y é um R-esquema liso (sobre R) e se $\Phi : Y \dashrightarrow N(X)$ é uma aplicação racional, então Φ se estende a um R-morfismo.

Teorema 7.7.14 (**Néron(global)**) *Seja X uma variedade abeliana sobre um corpo K, corpo de frações de um domínio de Dedekind R. O modelo de Néron existe, é de tipo finito sobre $S = Spec(R)$ e é único a menos de R-morfismos.*

Demonstração: [Cor-Sil, pag.214]. □

7.8 REDUÇÃO DE LANG

Nesta seção, nosso objetivo é mostrar que o teorema Faltings I, teorema 7.6.1, implica o teorema Faltings II, teorema 7.6.2. Dessa maneira, para demonstrar a conjectura de Mordell, teorema 7.0.2, é necessário apenas demonstrar o teorema 7.6.1. Tal redução é descrita por Serge Lang, no livro *Survey of Diofantine Geometry*,[La 2], onde todos os detalhes podem ser encontrados.

Teorema 7.8.1 *O teorema Faltings I implica que:*

(i) *a representação de* $G_K := \mathrm{Gal}(\bar{K}|K)$ *em* $V_l(X)$ *é semisimples;*

(ii) *as aplicações naturais:*

$$\mathbb{Z}_l \otimes \mathrm{End}_K(X) \to \mathrm{End}_{G_K}(T_l(X))$$

e

$$\mathbb{Q}_l \otimes \mathrm{End}_K(X) \to \mathrm{End}_{G_K}(V_l(X))$$

são isomorfismos.

Demonstração: Seja l um primo. Vamos chamar (l, K)-isogenia qualquer K-isogenia cujo grau seja uma potência de l. Como a classe de (l, K)-isogenias de X contém só um número finito de classes de isomorfismos, então para cada submódulo $W \subset V_l(X)$, existe $u \in \mathbb{Q}_l \otimes \mathrm{End}_K(X)$ tal que $u(V_l(X)) = W$.

De fato, fazendo $W^0 = W \cap T_l(X)$ e $W_n^0 = W^0 + l^n T_l(X) \subset T_l(X)$, definimos $W_n = \gamma_n(W_n^0)$, onde $\gamma_n : T_l(X) \to T_l(X)/l^n T_l(X)$. Identificando W_n com um subgrupo de $X(l^n)$, consideremos as isogenias:

$$\alpha_n : X \to X/W_n = Y_n$$

e

$$\beta_n : Y_n \to X,$$

onde β_n é a isogenia dual de α_n, e $\beta_n \circ \alpha_n = [l^n]_X$.

A construção anterior implica que $\beta_n(T_l(Y_n)) = W_n^0$ e por um argumento de compacticidade segue nossa afirmação.

(i) Tal propriedade segue da semisimplicidade de $\mathbb{Q}_l \otimes \mathrm{End}_K(X)$ como $\mathbb{Q}_l$-algebra, da nossa afirmação anterior, isto é, para cada submódulo $W \subset V_l(X)$ existe $u \in \mathbb{Q}_l \otimes \mathrm{End}_K(X)$ tal que $u(V_l(X)) = W$. De fato isto implica que o ideal a direita $u(\mathbb{Q}_l \otimes End_K(X))$ é gerado por um elemento idempotente ϵ tal que $\epsilon V_l(X) = W$. O fato que os elementos de G_K comutam com os elementos de $End_K(X)$ conclui a demonstração da primeira parte.

(ii) Em primeiro lugar, notamos que a imagem E de $\mathbb{Q}_l[G_K]$ em $\mathrm{End}(V_l(X))$ é o comutador C de $\mathbb{Q}_l \otimes \mathrm{End}_K(X)$ em $\mathrm{End}(V_l(X))$ e em seguida, conclui-se a partir da teoria das algebras semisimples como descrito em [La 2, pag.111]. □

Corolário 7.8.2 *Sejam X e Y variedades abelianas sobre um corpo K que satisfazem:*

(i) *a representação de $G_K := \mathrm{Gal}(\bar{K}|K)$ em $V_l(X)$ é semisimples;*

(ii) *as aplicações naturais:*

$$\mathbb{Z}_l \otimes \mathrm{End}_K(X) \to \mathrm{End}_{G_K}(T_l(X))$$

e

$$\mathbb{Q}_l \otimes \mathrm{End}_K(X) \to \mathrm{End}_{G_K}(V_l(X))$$

são isomorfismos.

Então as aplicações naturais:

$$\mathbb{Z}_l \otimes \mathrm{Hom}_K(X, Y) \to \mathrm{Hom}_{G_K}(T_l(X), T_l(Y))$$

e

$$\mathbb{Q}_l \otimes \mathrm{Hom}_K(X, Y) \to \mathrm{Hom}_{G_K}(V_l(X), V_l(Y))$$

são isomorfismos.

Demonstração: [La 2, pag.108]. □

Teorema 7.8.3 *Sejam X e Y variedades abelianas sobre um corpo K que satisfazem:*

(i) *a representação de* $G_K := \mathrm{Gal}(\bar{K}|K)$ *em* $V_l(X)$ *é semisimples;*

(ii) *as aplicações naturais:*

$$\mathbb{Z}_l \otimes \mathrm{End}_K(X) \to \mathrm{End}_{G_K}(T_l(X))$$

e

$$\mathbb{Q}_l \otimes \mathrm{End}_K(X) \to \mathrm{End}_{G_K}(V_l(X))$$

são isomorfismos.

Então, um $\mathrm{Gal}(\bar{K}|K)$*-isomorfismo* $V_l(X) \simeq V_l(Y)$*, fornece uma* K*-isogenia entre* X *e* Y*.*

Demonstração: Seja

$$\Phi : V_l(X) \to V_l(Y)$$

um $\mathrm{Gal}(\bar{K}|K)$-isomorfismo. Multiplicando por um inteiro l-ádico no anel de endomorfismos, Φ induz um homomorfismo, que denotaremos novamente por Φ

$$\Phi : T_l(X) \to T_l(Y)$$

cujo co-núcleo é finito. Pelo corolário anterior, se $\{\alpha_1, \ldots, \alpha_r\}$ é uma base de $\mathrm{Hom}_K(X, Y)$, sobre $\mathbb{Z}$, podemos escrever:

$$\Phi = \sum_{i=1}^{r} z_i \alpha_i \ , \ z_i \in \mathbb{Z}_l.$$

Sejam agora $n_i \in \mathbb{Z}$ inteiros arbitrariamente próximos de z_i. O morfismo $\displaystyle\sum_{i=1}^{r} n_i \alpha_i$ tem núcleo finito em X_{l^∞} e portanto induz uma isogenia. □

Lema 7.8.4 *Seja* K *um corpo de números e* $S \in M_K$ *é um conjunto finito de Places. Existe um conjunto finito de Places* $\tilde{S} \in M_k$*, disjunto de* S *e dos Places dividindo* l*, tal que se* ρ *e* $\tilde{\rho}$ *são duas representações* l*-ádicas semisimples de dimensão* d *de* $\mathrm{Gal}(\bar{K}|K)$ *não ramificadas fora de* S *e se*

$$\mathrm{Tr}(\rho(\mathrm{Fr}_v)) = \mathrm{Tr}(\tilde{\rho}(\mathrm{Fr}_v)) \ , \ \forall v \in \tilde{S},$$

então, ρ *é* $\mathrm{Gal}(\bar{K}|K)$ *isomorfa a* $\tilde{\rho}$*.*

Demonstração: Como $\mathrm{Gal}(\bar{K}|K)$ é compacto, existem nos espaços l-ádicos V e $\tilde{V}$ reticulados l-ádicos $T \in V$ e $\tilde{T} \in \tilde{V}$ que são $\mathrm{Gal}(\bar{K}|K)$ estáveis, vide-se por exemplo [Hu, pg. 275]. Seja R a $\mathbb{Z}_l$-álgebra gerada pela imagem de $\mathrm{Gal}(\bar{K}|K)$ em

$$\mathrm{End}_{\mathbb{Z}_l}(T) \times \mathrm{End}_{\mathbb{Z}_l}(\tilde{T}).$$

Então temos que:

$$\dim_{\mathbb{Z}_l}(R) \leq 8d^2 = \dim_{\mathbb{Z}_l}(\mathrm{End}_{\mathbb{Z}_l}(T) \times \mathrm{End}_{\mathbb{Z}_l}(\tilde{T})).$$

Desta feita, como $\sharp(R/lR) \leq l^{\dim(R)}$, R é finitamente gerado sobre $\mathbb{Z}_l$, uma vez que pelo lema de Nakayama representantes de R/lR geram R como $\mathbb{Z}_l$-módulo.

Considerando o homomorfismo natural (representação):

$$\varrho : \mathrm{Gal}(\bar{K}|K) \to (R/lR)^*,$$

mostra-se que a representação de $\mathrm{Gal}(\bar{K}|K)$ no grupo finito $(R/lR)^*$ é não ramificada fora de S. Por um teorema de Hermite, teorema 6.1.4, existe apenas um número finito de extenções de corpos de números de grau fixado que são não ramificadas fora de S. Do exposto, existe um subgrupo fechado $H < \mathrm{Gal}(\bar{K}|K)$ de índice finito em $\mathrm{Gal}\,\bar{K}|K$ tal que para todas as representações como as de nossa hipótese, seu núcleo contém H. Podemos assim considerar a representação do grupo finito $\mathrm{Gal}(\bar{K}|K)/H$:

$$\varrho : \mathrm{Gal}(\bar{K}|K)/H \to (R/lR)^*$$

e então concluir a existência de um conjunto finito $\tilde{S} \subset M_K^0$ tal que os elementos de Frobenius Fr_υ com $\upsilon \in \tilde{S}$ tenham imagens que cobrem a imagem de $\mathrm{Gal}(\bar{K}|K)$ em $(R/lR)^*$. Se

$$\mathrm{Tr}(\rho(\mathrm{Fr}_\upsilon)) = \mathrm{Tr}(\tilde{\rho}(\mathrm{Fr}_\upsilon)) \ , \ \forall \upsilon \in \tilde{S},$$

obtemos que

$$\mathrm{Tr}(\rho(\alpha)) = \mathrm{Tr}(\tilde{\rho}(\alpha)) \ , \ \forall \alpha \in R.$$

Disto concluimos que as representações são $\mathrm{Gal}(\bar{K}|K)$-isomorfas, pois pela hipótese de semisimplicidade podemos aplicar a proposição, 7.7.2. □

Teorema 7.8.5 (**Lema de Faltings**) *Sejam K um corpo de números, d um inteiro positivo, $S \in M_K$ um conjunto finito de Places e para cada $\upsilon \notin S$ seja $Z_\upsilon \subset \mathbb{Q}_l$ um conjunto finito. Então, o número de classes de isomorfismos de representações semisimples de $\mathrm{Gal}\,\bar{K}|K$, cuja dimensão é d sobre $\mathbb{Q}_l$, que são não ramificadas fora de S e tais que, para cada $\upsilon \notin S$ os traços dos Frobenius, $\mathrm{Tr}(\rho(\mathrm{Fr}_\upsilon))$ estão em Z_υ é finito.*

Demonstração: Corolário imediato do lema anterior. □

Teorema 7.8.6 (**Redução de Lang**) *O teorema 7.6.1, Faltings I, implica o teorema 7.6.2, Faltings II.*

Demonstração: Em primeiro lugar, pelo teorema 7.8.1, o teorema Faltings I implica as propriedades:

(i) a representação de $G_K := \mathrm{Gal}(\bar{K}|K)$ em $V_l(X)$ é semisimples;

(ii) as aplicações naturais:

$$\mathbb{Z}_l \otimes \mathrm{End}_K(X) \to \mathrm{End}_{G_K}(T_l(X))$$

e

$$\mathbb{Q}_l \otimes \mathrm{End}_K(X) \to \mathrm{End}_{G_K}(V_l(X))$$

são isomorfismos.

Posteriormente, mostramos que as propriedades supracitadas implicam o teorema da isogenia, teorema 7.8.3. Portanto, as classes de K-isogenias de uma variedade abeliana podem ser descritas a partir das classes de $\mathrm{Gal}(\bar{K}|K)$-isomorfismos de $V_l(X)$.

O critério de boa redução de Néron-Ogg, teorema 7.7.11, nos garante que o conjunto das classes de isogenias de X tendo boa redução fora um conjunto finito S de Places se injeta no conjunto das classes de isomorfismos de representações de $\mathrm{Gal}(\bar{K}|K)$ em $V_l(X)$, não ramificadas fora de S.

O teorema de Weil, 7.7.7, nos garante que o traço das imagens, pela nossa representação, dos elementos de Frobenius está em um conjunto finito e portanto podemos aplicar o lema de Faltings, 7.8.5, para concluir a finitude do conjunto das classes de isomorfismos de representações de $\mathrm{Gal}(\bar{K}|K)$ em $V_l(X)$, não ramificadas fora de S. Assim asseguramos a finitude do conjunto das classes de isogenias de X tendo boa redução fora um conjunto finito de Places $S \in M_K$. □

7.9 FIBRADOS LINEARES METRIZADOS E ALTURA DE FALTINGS

Definição 7.9.1 *Sejam K um corpo de números e $\mathcal{O}_K$ seu anel de inteiros. Um fibrado linear metrizado em $\mathrm{Spec}(\mathcal{O}_K)$ consiste de um $\mathcal{O}_K$-módulo projetivo P munido de normas $\| \ \|_v$ em $P \otimes_{\mathcal{O}_K} K_v$ para cada Place infinito $v \in M_K^\infty$. O grau do fibrado linear metrizado é defnido por:*

$$\deg(P, \| \ \|) = \log[\sharp(P/p\mathcal{O}_K)] - \sum_{v \in M_K^\infty} \varepsilon_v \log \|p\|,$$

em que $\varepsilon_v = 1$ ou 2 de acordo com v induzir um mergulho real ou complexo. Note que nossa definição fez uso da escolha de um elemento não nulo $p \in P$, entretanto o lado direito é independente de p.

Definição 7.9.2 *Sejam K um corpo de números, $\mathcal{O}_K$ su anel de inteiros, X uma variedade abeliana sobre K, $N(X)$ o modelo de Néron de X sobre $S = \mathrm{Spec}(\mathcal{O}_K)$, $\eta : S \to N(X)$ a seção nula, $\Omega^1_{N(X)/S}$ o feixe de diferenciais. O determinante co-Lie é definido por:*

$$\mathfrak{L}(N(X)) = \eta^*(\det(\Omega^1_{N(X)/S})).$$

Note que $\mathfrak{L}(N(X))$ é um fibrado linear em $S = \mathrm{Spec}(\mathcal{O}_K)$.

Para aplicar o conceito de grau de fibrado linear metrizado ao determinante co-Lie, vamos considerar uma estrutura Hermitiana dada por:

$$< \omega, \omega >= \frac{1}{(2\pi)^d} \int_{X(\mathbb{C})} |\omega \wedge \bar{\omega}| \ , \ \omega \in \mathfrak{L}(N(X)) \ d = \dim(X).$$

Definição 7.9.3 *Seja X uma variedade abeliana sobre um corpo de números K. A altura de Faltings é definida por:*

$$\mathrm{h}_{\mathrm{Fal}}(X) = \frac{1}{[K : \mathbb{Q}]} \deg(\mathfrak{L}(N(X))).$$

Teorema 7.9.4 *Sejam K um corpo de números e n, d, h_0 inteiros. Então o número de classes de isomorfismos de variedades abelianas polarizadas $(X, \mathfrak{L})$ sobre K em que $\dim(X) = d$, $\deg(\Phi_{\mathfrak{L}}) = n$ e $\mathrm{h}_{\mathrm{Fal}}(X) \leq h_0$ é finito.*

Proposição 7.9.5 *Sejam K um corpo de números e X uma variedade abeliana sobre K com redução semiestável. Então, se $L|K$ é uma extensão finita:*

$$\mathrm{h}_{\mathrm{Fal}}(X_L) = \mathrm{h}_{\mathrm{Fal}}(X).$$

Definição 7.9.6 *Seja K um corpo de números e X uma variedade abeliana sobre K. Escolhendo qualquer extensão finita $L|K$ tal que X_L seja semiestável, definimos a altura estável de Faltings por:*

$$\mathrm{h}^{\mathrm{st}}_{\mathrm{Fal}}(X) = \mathrm{h}_{\mathrm{Fal}}(X_L).$$

Pela proposição anterior, tal altura não depende do corpo de definição.

Definição 7.9.7 *Seja X uma variedade abeliana de dimensão d. Uma estrutura de nível N de X é um isomorfismo:*

$$\varepsilon : (\mathbb{Z}/N\mathbb{Z})^{2d} \to X[N].$$

Teorema 7.9.8 (**Construção do espaço de moduli**)*Sejam d e N inteiros positivos de modo que N seja divisível por pelo menos dois primos $p \geq 3$. Então, existem*

(i) *uma união disjunta finita de variedades projetivas $\bar{M}_{d,N}$, definida sobre $\mathbb{Q}$, tal que todas as componentes tem a mesma dimensão $\frac{d(d+1)}{2}$;*

(ii) *um aberto denso $M_{d,N} \subset \bar{M}_{d,N}$ não singular sobre $\mathbb{Q}$, cujo complemento tem codimensão d;*

(iii) *um $\mathbb{Q}$-morfismo próprio e liso,*

$$\Phi : X \to M_{d,N},$$

que é um esquema abeliano de dimensão relativa d;

(iv) *uma estrutura de nível N:*

$$\varepsilon : (\mathbb{Z}/N\mathbb{Z})^{2d} \to X[N];$$

(iv) *uma classe de equivalência algébrica:*

$$\mathfrak{L} \in \mathrm{NS}(X),$$

tais que para cada extensão $K|\mathbb{Q}$ *a associação:*

$$x \mapsto (X_x, \mathfrak{L}_x, \varepsilon_x) = \Phi^{-1}(x)\ ,\ x \in M_{d,N}(K)$$

fornece uma bijeção entre o conjunto $M_{d,N}(K)$ *dos pontos* K*-racionais de* $M_{d,N}$ *e o conjunto das classes de isomorfismo de tais triplas sobre* K*.*

Demonstração: [FC, V, Theorem 2.5]. □

Pode-se definir o determinante co-Lie em $\bar{M}_{d,N}$ correspondendo a uma classe de divisores amplo $\lambda \in \mathrm{Pic}(\bar{M}_{d,N})$. Pelo exposto, podemos associar a λ uma função altura módulo $O(1)$:

$$\mathrm{h}_\lambda : \bar{M}_{d,N} :\to \mathbb{R}.$$

Tal altura é chamada altura de Lie. A relação fundamental entre a altura de Lie e a altura de Faltings é o conteúdo do seguinte:

Teorema 7.9.9 *Para cada tripla* $(X, \mathfrak{L}, \varepsilon)$ *sobre um corpo de números, seja* $m(X, \mathfrak{L}, \varepsilon)$ *o respectivo ponto no espaço de moduli. Então:*

$$\mathrm{h}^{\mathrm{st}}_{\mathrm{Fal}}(X) = \mathrm{h}_\lambda(m(X, \mathfrak{L}, \varepsilon)) + O(\log(\mathrm{h}_\lambda\, m(X, \mathfrak{L}, \varepsilon))).$$

Demonstração: [La 2, pa.119]. □

Teorema 7.9.10 *Sejam* K *um corpo de números e* X *uma variedade abeliana sobre* K*. O conjunto das alturas de Faltings das variedades abelianas* K*-isógenas a* X *é finito.*

Demonstração: [Fa]. □

REFERÊNCIAS BIBLIOGRÁFICAS

[Ca] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. 24, 1991.

[Cor-Sil] G. Cornell, J. Silverman (Editors), *Aritmetic Geometry*, Springer-Verlag, 1986.

[Fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[FC] G. Faltings, C. L. Chai, *Degenerations of Abelian Varieties*, Springer–Verlag, 1990.

[Har] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.

[Hin-Sil] M. Hindry, J. Silverman, *Diophantine Geometry: an Introduction*, Springer-Verlag, 2000.

[Hu] D. Husemöller, *Elliptic Curves*, Springer-Verlag, 1986.

[La 1] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, 1983.

[La 2] S. Lang, *Survey of Diophantine Geometry*, Springer-Verlag, 1997.

[La 3] S. Lang, *Algebra*, Springer-Verlag, 1984.

[Liu] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Science Publications, 2002.

[Mat] H. Matsumura, *Comutative Ring Theory*, Cambridge University Press, 1989

[Mor] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Camb. Phil. Soc. 21 (1922), 179–192.

[Mum 1] D. Mumford, *Abelian Varieties*, Oxford University Press, 1974.

[Mum 2] D. Mumford, *Curves and their jacobians*, Michigan University Press, 1976.

[Neu 1] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999.

[Neu 2] J. Neukirch, *Class Field Theory*, Springer-Verlag, 1978.

[O'Me] O. T. O' Meara, *Introduction to Quadratic Forms*, Springer-Verlag, 1963.

[Pr] A. Prestel, *Lectures on formally p-ádic fields*, IMPA, 1983.

[Sel] E. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. 85 (1951), 203–362 e 92 (1954), 191–197.

[Sil] J. Silverman, *The Aritmethic of Elliptic Curves*, Springer-Verlag, 1986.

[Sil-Ta] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.

[Wi] A. Wiles, *Elliptic curves, modular forms and Fermat's Last Theorem*, Annals of Math. 141 (1995), 443–551.