Formas Quadráticas Binárias Integrais e Racionais

Marcio Masaki Onodera

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para obtenção do título de Mestre
em
Matemática.

Orientador : Prof. Dr. Paulo Agozzini Martin

Este trabalho contou com o apoio financeiro do CNPq.

Este exemplar corresponde à redação
final da dissertação devidamente
corrigida e defendida por
Marcio Masaki Onodera
e aprovada pela comissão julgadora.

São Paulo, agosto de 2005.

Banca examinadora:

- Prof. Dr. Paulo Agozzini Martin (Orientador) - IME-USP
- Prof. Dr. Daniel Levcovitz - ICMC-USP
- Prof. Dr. Vyacheslav Futorny - IME-USP

Dedicatória

O presente trabalho é dedicado a todas as pessoas que, assim como o autor, acreditam que um sonho somente pode ser concretizado quando a força de vontade é maior que os obstáculos impostos pela vida. Em especial, dedico este sonho realizado ao amigo e orientador Paulo A. Martin, à minha família, à Camila K. Kasai e em memória de meus queridos avós Maçato Sigaki, Massaru Onodera e Yukiko Onodera.

Agradecimentos

Agradeço imensamente a todas as pessoas que contribuiram na concretização deste trabalho. Particularmente, agradeço ao meu amigo e orientador Paulo A. Martin, ao CNPq, à minha família, à Camila K. Kasai e sua família, ao professor e amigo Geraldo Itsuro Haramura, à amiga Elza Nakayama, aos amigos de infância : Marcio H. Kikuti, Ivan M. Carlos, Emilson P. Leite e Marcos Kikuti, a todos os amigos do Colégio Lantagi e aos amigos do IME-USP : Tatyana M. Okano, Carlos H. Griese, Paulo T. Taneda, Ednei F. Reis, Débora C. Brandt, João R. Sato e André Fujita.

Abstract

In this work we will study two important topics : integral and rational binary quadratic forms. As regards to integral forms, the classical problem of integer representation by these forms leads to a classification of forms by some natural equivalence relation (introduced by Gauss). We expose here Gauss' work.

Concerning rational forms we make a study that culminates in the Hasse-Minkowski theorem for binary forms. For this goal we have to face p-adics numbers, Hilbert symbol and some other preliminary general results about n-ary forms over fields.

Resumo

Neste trabalho, estudaremos dois tópicos importantes : formas quadráticas binárias integrais (com coeficientes em $\mathbb{Z}$) e racionais (com coeficientes em $\mathbb{Q}$). No que concerne às formas integrais, o problema clássico da representabilidade de inteiros por tais formas conduz ao estudo da classificação dessas formas por uma relação de equivalência introduzida por Gauss. Fazemos aqui uma exposição do trabalho de Gauss. No que toca às formas racionais, fazemos um estudo que culmina no teorema de Hasse-Minkowski para formas binárias. Com tal objetivo em mira, estudaremos os corpos p-ádicos, o Símbolo de Hilbert e alguns resultados gerais de formas sobre corpos.

Sumário

Introdução

Representação de Inteiros por Formas Quadráticas

Em teoria dos números, estuda-se o seguinte teorema de Fermat : "Se p é um inteiro primo, então

$$x^2 + y^2 = p$$

admite soluções inteiras se e somente se $p = 2$ ou $p \equiv 1 \ (mod\ 4)$". Pode-se generalizar este resultado para : "A equação $x^2 + y^2 = n$, com $n \in \mathbb{Z}$, admite soluções inteiras se e somente se n se fatorar como

$$n = 2^{\alpha} p_1^{\alpha_1} ... p_r^{\alpha_r} q_1^{\beta_1} ... q_s^{\beta_s},$$

onde para todo i, j, β_j é par e p_i, q_j são primos tais que $p_i \equiv 1 \ (mod\ 4)$ e $q_j \equiv 3 \ (mod\ 4)$". Por meio desse resultado, podemos identificar todos os inteiros que podem ser expressos como soma de dois quadrados de inteiros. Um outro modo de entendermos esse teorema é usando o conceito de representação de inteiros por formas quadráticas integrais. Assim, $f(x, y) = x^2 + y^2$ representa todo número inteiro da forma citada acima. Isso motiva o estudo das formas $ax^2 + bxy + cy^2$, com $a, b, c \in \mathbb{Z}$. Por razões técnicas, estudaremos formas do tipo :

$$f(x, y) = ax^2 + 2bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \ a, b, c \in \mathbb{Z}$$

que foram estudadas por Carl Friedrich Gauss no seu "Disquisitiones Arithmeticae" [GAU].

Uma pergunta que surge naturalmente é : quais são todos os inteiros representados por uma dada forma, como por exemplo, $g(z, t) = 2z^2 + 2zt + t^2$? Suponhamos que $a_1^2 + a_2^2 = n$, com $a_1, a_2 \in \mathbb{Z}$. Então $g(a_1, a_2 - a_1) = a_1^2 + a_2^2 = n$ e, portanto, g representa n. Agora, se g representa um inteiro m, ou seja, $g(b_1, b_2) = 2b_1^2 + 2b_1 b_2 + b_2^2 = m$ com $b_1, b_2 \in \mathbb{Z}$, temos que $f(b_1, b_1 + b_2) = m$. Então, todo inteiro representado por g também é representado por f. Tal fato deve-se à existência de uma mudança de variáveis, não singular, que transforma uma forma na outra. Isso motiva definirmos que duas formas quadráticas binárias integrais f e g, com matrizes $[f]$ e $[g]$ são equivalentes se existir uma matriz $M \in GL_2(\mathbb{Z}) = \{M \in M_2(\mathbb{Z}) : det\ M = \pm 1\}$ tal que $[f] = M^t [g] M$. Se $det\ M = 1$, dizemos que a equivalência é própria e, caso contrário, que a equivalência é imprópria.

As formas quadráticas integrais foram primeiramente estudadas por Gauss em seu

"Disquisitiones Arithmeticae". Ele classificou as formas quadráticas binárias integrais usando a equivalência própria. Veremos adiante que resultados análogos podem ser obtidos usando a outra equivalência.

Observe-se que o determinante d é um invariante pela equivalência. Assim sendo, iniciaremos a classificação das formas pelo determinante.

Formas Quadráticas Binárias Integrais

Os casos a serem estudados são : $d > 0$ e $d < 0$. Como o discriminante Δ de $f(x, y)$ é dado por $\Delta = (2b)^2 - 4ac = -4d$, definimos os seguintes casos : formas positivas ($\Delta < 0$ e $a > 0$), formas negativas ($\Delta < 0$ e $a < 0$) e formas indefinidas ($\Delta > 0$). Observe-se que dessa definição segue que : $f(x, y) > 0$, $f(x, y) < 0$ e $f(x, y)$ assume valores positivos, negativos ou nulos, respectivamente.

Gauss provou que toda forma positiva é propriamente equivalente a uma única forma $ax^2 + 2bxy + cy^2$, onde $-a < 2b \leq a \leq c$; com $b \geq 0$, se $a = c$ (forma positiva reduzida). Desse resultado segue que existe um número finito de classes de equivalência própria, onde todas as formas de uma dada classe são propriamente equivalentes a uma única forma positiva reduzida.

Para decidirmos se duas dadas formas positivas de uma mesmo determinante são propriamente equivalentes, existe um algoritmo que encontra, num número finito de passos, as formas positivas reduzidas correspondentes. Considerando, por exemplo, as formas $2x^2 - 2xy + 3y^2$ e $x^2 + 4xy + 9y^2$ e aplicando o algoritmo, obtemos as seguintes seqüências de formas :

$$\begin{pmatrix} 2 & -1 \\ -1 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 2 & 9 \end{pmatrix}, \begin{pmatrix} 9 & -2 \\ -2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

Como as últimas formas de cada seqüência são reduzidas e diferentes, as primeiras formas das seqüências não podem ser propriamente equivalentes.

No caso das formas indefinidas, quando $-d$ é um quadrado, valem os mesmo resultados anteriores, com a ressalva de usarmos outra definição de forma reduzida. Já no outro caso, se $-d$ não for um quadrado, só não conseguimos garantir a unicidade em cada classe de equivalência própria. Isto é contornado ao provarmos a unicidade de uma sequência periódica de formas reduzidas (definição diferente das anteriores) em cada classe de equivalência própria. Pode-se construir um algoritmo semelhante ao dos casos anteriores para as formas indefinidas. Aplicando este algoritmo nas formas $2x^2 + 6xy + 3y^2$ e $x^2 + 10xy + 23y^2$, temos as seqüências :

$$\begin{pmatrix} 2 & 3 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 2 \end{pmatrix}, \ldots$$

$$\begin{pmatrix} 1 & 5 \\ 5 & 23 \end{pmatrix}, \begin{pmatrix} 23 & -5 \\ -5 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} -2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix}, \ldots$$

cujos períodos de formas reduzidas são diferentes. Portanto, aquelas formas não podem ser propriamente equivalentes.

Formas Quadráticas Binárias Racionais

Uma forma quadrática binária racional, $f(x,y) = ax^2 + 2bxy + cy^2$ com $a,b,c \in \mathbb{Q}$ é singular quando $det\ [f] = 0$ e é não singular quando $det\ [f] \neq 0$. A equivalência entre formas racionais é análoga a definida acima, mas não possui a propriedade de manter invariante o determinante. Os determinantes de duas formas racionais equivalentes diferem por um fator que é um quadrado em $\mathbb{Q}$. Contudo, toda forma quadrática sobre um corpo com característica diferente de 2 é equivalente a uma forma diagonal do tipo : $a_1x_1^2 + a_2x_2^2$, com $a_1, a_2 \in K$, reduzindo a questão de equivalência em K para formas diagonais. Em particular, se $K = \mathbb{R}$, pelo Teorema de Sylvester, fazendo a mudança de variável $x_i = \pm y_i/\sqrt{|a_i|}$ (+ se $a_i > 0$ e - se $a_i < 0$), esta forma diagonal é somente composta pelos elementos : 1 ou -1. Porém, quando $K = \mathbb{Q}$, tal resultado não é possível, pois nem todos os racionais positivos são quadrados em $\mathbb{Q}$. É claro que formas equivalentes sobre $\mathbb{Q}$ são também equivalentes sobre $\mathbb{R}$. As formas racionais $x^2 + y^2$ e $z^2 + 2t^2$, cujos determinantes não diferem por um fator que é um quadrado em $\mathbb{Q}$, mostram que a recíproca do fato acima não é verdadeira. Desta forma, nada mais natural que estudarmos essa equivalência nos outros completamentos de $\mathbb{Q}$. O Teorema de Ostrowski garante que os únicos completamentos de $\mathbb{Q}$ são os reais e os corpos p-ádicos ($\mathbb{Q}_p$), onde p é um primo. Contudo, antes de estudarmos a equivalência nos p-ádicos, faz-se necessário conhecermos melhor os quadrados de $\mathbb{Q}_p$. Veremos que $[\mathbb{Q}_2^* : (\mathbb{Q}_2^*)^2] = 8$ e $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2] = 4, p \neq 2$ (*). Como toda forma binária pode ser posta na forma $x^2 - \alpha y^2, \alpha \neq 0, \alpha \in \mathbb{Q}_p$, estudaremos o grupo multiplicativo H_α :=todos os elementos de $\mathbb{Q}_p$ representados por $x^2 - \alpha y^2, \alpha \neq 0, \alpha \in \mathbb{Q}_p$. Usando (*), provamos que $[\mathbb{Q}_p^*, H_\alpha]$ é 1 se α é um quadrado e 2 no caso contrário. Assim, existe um homomorfismo sobrejetor $\varphi_\alpha : \mathbb{Q}_p^* \to \{+1, -1\}$ que será definido como o Símbolo de Hilbert :

$$(\alpha, \beta) = \varphi_\alpha(\beta) := \begin{cases} +1, & \text{se } \beta \in H_\alpha \\ -1, & \text{caso contrário} \end{cases}$$

Utilizando o Símbolo de Hilbert, provaremos que duas formas binárias p-ádicas, não singulares são equivalentes sobre $\mathbb{Q}_p$ se e somente se seus determinantes diferirem por um quadrado de $\mathbb{Q}_p$ e $(\alpha, -det\ [f]) = (\alpha, -det\ [g])$, onde $\alpha \in \mathbb{Q}_p$ é representado por f e g. Este resultado é usado para provarmos o Teorema de Hasse-Minkowski : Uma forma quadrática binária racional representa 0 em $\mathbb{Q}$ se e somente se representa 0 em todos os corpos p-ádicos e nos reais. Como corolário, segue que duas formas quadráticas binárias racionais são equivalentes sobre $\mathbb{Q}$ se e somente se forem equivalentes sobre todos os p-ádicos e nos reais.

Preliminares

0.1 Formas Quadráticas Binárias Integrais

Definição 0.1.1 *Um polinônio com coeficientes num corpo K do tipo :*

$$f(x,y) = ax^2 + 2bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = v^t[f]v$$

é chamado de ***forma quadrática binária com matriz associada [f] e determinante*** $d = ac - b^2$. *Denotaremos a matriz* $[f]$ *por* (a,b,c) *também.*

A definição acima é devida a Gauss. Vale a pena notar que, na obra de Gauss, o seu determinante é o oposto do nosso, talvez para manter o mesmo sinal que o discriminante $\Delta = 4(b^2 - ac)$ do polinômio $f(x,1)$.

Definição 0.1.2 *Uma forma quadrática binária f é chamada de* ***integral*** *se e somente se os coeficientes da matriz associada a f forem inteiros.*

Definição 0.1.3 *Dizemos que um forma integral* ***representa um inteiro n*** *se e somente se a equação $f(x,y) = n$ admite solução em $\mathbb{Z}^2$.*

Consideremos as formas $f(x,y) = x^2 + y^2$ e $g(z,t) = 2z^2 + 2zt + t^2$. Sabemos, [SAN], que se n tiver a fatoração da $2^{\alpha}p_1^{\alpha_1}...p_r^{\alpha_r}q_1^{\beta_1}...q_s^{\beta_s}$, onde para todo i,j, β_j é par e p_i, q_j são primos tais que $p_i \equiv 1 \ (mod\ 4)$ e $q_j \equiv 3 \ (mod\ 4)$, então existem $a_1, a_2 \in \mathbb{Z}$, tais que $a_1^2 + a_2^2 = n$. Como $g(a_1, a_2 - a_1) = a_1^2 + a_2^2 = n$, temos que g representa este produto. Agora, suponhamos que para um dado inteiro m, existam $b_1, b_2 \in \mathbb{Z}$ tais que $g(b_1,b_2) = m$. Então, $f(b_1, b_1 + b_2) = m$ e f representa m. Portanto, f e g representam os mesmo inteiros. Nesse caso, o fato é justificado pela existência de uma mudança de variáveis linear e não singular, $z = x, t = y - x$, que transforma uma forma na outra. Assim, motivamos a :

Definição 0.1.4 *Dizemos que duas formas integrais f e g, com matrizes A e B respectivamente, são* ***integralmente equivalentes****, ou que pertencem a mesma classe, se existir uma matriz $M \in GL_2(\mathbb{Z})$ tal que $B = M^tAM$. No caso de $\det M = 1$, dizemos que a equivalência é* ***própria*** *e, caso contrário, dizemos que a equivalência é* ***imprópria****.*

Notação *: Usaremos $\sim$ para a equivalência própria.*

Não é difícil ver que a equivalência integral, acima definida, é uma relação de equivalência.

Proposição 0.1.1 *Formas integralmente equivalentes representam os mesmos inteiros.*

Prova : Sejam A e B as matrizes associadas a $f(x,y) = ax^2 + 2bxy + cy^2$ e a $g(z,t) = a'z^2 + 2b'zt + c't^2$ respectivamente. Como f e g são integralmente equivalentes, existe $M \in GL_2(\mathbb{Z})$ tal que $B = M^tAM$. Se $f(x,y) = n$ para algum $(x,y) \in \mathbb{Z}^2$, tomando $v_2 = M^{-1}v_1$, com $v_1 = (x,y), v_2 = (z,t)$, temos:

$$\begin{aligned} g(z,t) &= v_2^tBv_2 = v_2^t(M^tAM)v_2 = (M^{-1}v_1)^t(M^tAM)M^{-1}v_1 = \\ &= v_1^t(M^t)^{-1}M^tAMM^{-1}v_1 = v_1^tAv_1 = f(x,y) = n \end{aligned}$$

Então, g representa os mesmos inteiros que f. Para verificarmos que f representa os mesmos inteiros que g, suponhamos que g representa um inteiro m e definamos $v_1 = Mv_2$. Logo, f e g representam os mesmos inteiros. ■

Observação : As formas $f(x,y) = 2x^2+2xy+2y^2 = 2(x^2+xy+y^2)$ e $g(z,t) = 2z^2+6t^2 = 2(z^2+3t^2)$ representam os mesmo inteiros, porém não são propriamente equivalentes. De fato, se $g(z_0,t_0) = m$, fazendo

$$(*)\begin{cases} x_0 = z_0 - t_0 \\ y_0 = 2t_0 \end{cases}$$

obtemos

$$\begin{aligned} f(x_0,y_0) &= 2(z_0-t_0)^2 + 2(z_0-t_0)2t_0 + 2(2t_0)^2 \\ &= 2z_0^2 - 4z_0t_0 + 2t_0^2 + 4z_0t_0 - 4t_0^2 + 8t_0^2 \\ &= 2z_0^2 + 6t_0^2 \\ &= g(z_0,t_0) \\ &= m \end{aligned}$$

ou seja, se g representa m, f também representa m. Note-se que a inversão de (*) produz

$$(**)\begin{cases} z = x + y/2 \\ t = y/2 \end{cases}$$

e não podemos aplicar diretamente essa mudança de variáveis, pois y pode não ser par.

Suponhamos que $f(x_0,y_0) = n$ com y_0 ímpar (se y_0 for par não há o que fazer). Se x_0 for par, tomamos

$$\begin{cases} z_0 = x_0 + x_0/2 \\ t_0 = x_0/2 \end{cases}$$

e, como $f(x,y)$ é simétrica em x e y, temos $f(x_0,y_0) = f(y_0,x_0) = n$ e $g(y_0,x_0) = n$. Podemos então supor que x_0 e y_0 são ambos ímpares. Vamos mostrar que existe k ímpar tal que

$$2x_0^2 + 2x_0(y_0+k) + 2(y_0+k)^2 = n$$

e que, portanto $f(x_0, y_0) = f(x_0, y_0+k) = n$ com y_0+k par. Isso acarreta $g(x_0, y_0+k) = n$ via $(**)$.

$$\begin{aligned} 2x_0^2 + 2x_0(y_0+k) + 2(y_0+k)^2 &= 2x_0^2 + 2x_0y_0 + 2kx_0 + 2y_0^2 + 4y_0k + 2k^2 \\ &= n + 2kx_0 + 4y_0k + 2k^2 \\ &= n + 2k(x_0 + 2y_0 + k) \end{aligned}$$

Tomamos $k = -x_0 - 2y_0$ de modo que k seja ímpar e $f(x_0, y_0 = k) = n$. Isso mostra que f e g representam os mesmos inteiros. As matrizes associadas à f e à g são :

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$$

de modo que $det\ f \neq det\ g$ e, com o lema abaixo, vemos que f e g não podem ser propriamente equivalentes.

Proposição 0.1.2 *Sejam f, g formas integrais integralmente equivalentes com matrizes associadas A e B, respectivamente. Então $det\ A = det\ B$, isto é, $det\ A$ é um invariante pela equivalência integral.*

Prova : Suponhamos que f, g sejam integralmente equivalentes. Então, existe $M \in GL_2(\mathbb{Z})$ tal que $B = M^tAM$ e segue :

$$det\ B = det\ (M^tAM) \Longrightarrow det\ B = (det\ M^t)(det\ A)(det\ M) \Longrightarrow det\ B = (det\ M)^2(det\ A)$$

Como $M \in GL_2(\mathbb{Z})$, temos $det\ M = det\ M^t = \pm 1$. Então :

$$det\ B = (\pm 1)^2(det\ A) \Longrightarrow det\ B = det\ A$$

e $det\ A$ é um invariante pela equivalência integral. ■

Para verificar que a recíproca da proposição acima não é verdadeira, basta considerar as formas $x^2 + 3y^2$ e $-x^2 - 3y^2$ de mesmo determinante. Como a primeira não representa nenhum inteiro negativo representado pela segunda, temos que elas não podem ser integralmente equivalentes. Observe também que pela proposição acima, as formas $f(x, y) = x^2 + y^2$ e $g(x, y) = 2x^2 + 2y^2$ não são integralmente equivalentes, pois os determinantes são diferentes.

Um outro conceito importante que usaremos é :

Definição 0.1.5 *Duas formas integrais (a, b, c) e (a', b', c') com o mesmo determinante são **adjacentes** se e somente se $c = a'$ e $b+b' \equiv 0\ (mod\ c)$ ou $a = c'$ e $b+b' \equiv 0\ (mod\ c')$.*

As formas $(2, 3, 5), (5, 2, 1)$ são adjacentes, enquanto que as formas $(3, 4, 2), (9, 1, -1)$ não o são.

Proposição 0.1.3 *Formas adjacentes são propriamente equivalentes.*

Prova : Suponhamos que (a', b', c') seja adjacente a (a, b, c) e $c = a'$. Então, existe $k \in \mathbb{Z}$ tal que $(b + b')/c = (b + b')/a' = k$. Desta forma :

$$\begin{pmatrix} 0 & 1 \\ -1 & k \end{pmatrix}\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} = \begin{pmatrix} c & ck - b \\ ck - b & ck^2 - 2bk + a \end{pmatrix} = \begin{pmatrix} a' & b' \\ b' & ck^2 - 2bk + a \end{pmatrix}$$

Como $d = a'c' - b'^2$, temos que :

$$c' = \frac{b'^2 + d}{a'} = \frac{(ck - b)^2 + (ac - b)^2}{c} = ck^2 - 2bk + a$$

Então $(a', b', c') \sim (a, b, c)$. Se (a', b', c') for adjacente a (a, b, c) e $c' = a$, procedendo de maneira análoga ao caso anterior, obtemos que $(a', b', c') \sim (a, b, c)$. ■

0.2 Os Números p-Ádicos $\mathbb{Q}_p$

Os números p-ádicos foram introduzidos por K. Hensel, possivelmente através de uma analogia entre $\mathbb{Q}$ e o corpo de funções racionais $\mathbb{C}(X)$ [GOU]. A norma $|.|_p$ é um valor absoluto não arquimediano definido para qualquer $x \in \mathbb{Q}$ por :

$$|x|_p = p^{-v_p(x)}, x \neq 0 \ e \ |0|_p = 0$$

onde p é um primo e $v_p(x)$ é tal que

$$x = p^{v_p(x)}\frac{a}{b} \ , \ p \nmid ab$$

O corpo $\mathbb{Q}_p$ é definido por C/N, onde C é o conjunto de todas as sequências de Cauchy em relação a $|.|_p$ e N é o conjunto de todas as sequências que convergem para 0 em relação a $|.|_p$. Como $\mathbb{Q} \subset \mathbb{Q}_p$ e a norma $|.|_p$ pode ser estendida a uma norma em $\mathbb{Q}_p$ [GOU], prova-se que o corpo dos números p-ádicos é completo segundo esta norma. Definimos os inteiros p-ádicos por $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. A seguir listaremos algumas propriedades dos números p-ádicos que podem ser consultados em [GOU] ou [SHA].

1. Dado $x \in \mathbb{Z}_p$, existem $a_n \in \mathbb{Z}$ tais que :

$$a_n \equiv x \ (mod \ p^n) \ , \ a_{n+1} \equiv a_n \ (mod \ p^n) \ , \ 0 \leq a_n \leq p^n - 1$$

2. Todo $x \in \mathbb{Z}_p$ se escreve de forma única como :

$$x = b_0 + b_1 p + ... + b_n p^n + ... \ , \ 0 \leq b_i \leq p - 1$$

3. Todo $x \in \mathbb{Q}_p$ se escreve de forma única como :

$$x = b_{-n_0}p^{-n_0} + ... + b_0 + b_1 p + ... + b_n p^n + ... \ , \ 0 \leq b_i \leq p - 1, \ -n_o = v_p(x)$$

4. O conjunto dos elementos invertíveis de $\mathbb{Z}_p$ será denotado por $\mathbb{Z}_p^\times$. Então :

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\} \ , \ \mathbb{Z}_p^\times \cap \mathbb{Q} = \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid ab\right\}$$

5. Um inteiro p-ádico $x = b_0 + b_1 p + ... + b_n p^n + ... \in \mathbb{Z}_p$ é invertível se e somente se $b_0 \not\equiv 0 \ (mod\ p)$

6. Qualquer $x \in \mathbb{Q}_p$, não nulo, pode ser representado de modo único na forma $p^m u$, onde $m \in \mathbb{Z}$ e $u \in \mathbb{Z}_p^\times$.

7. **Teorema de Ostrowski** - Todo valor absoluto não-trivial em $\mathbb{Q}$ é equivalente a um dos valores absolutos p-ádicos $|.|_p$ ou ao valor absoluto real $|.|$.

O Lema de Hensel e seus corolários serão muito úteis posteriormente. [SHA]

Lema 0.2.1 ***(Lema de Hensel)*** *Sejam $F(x_1, ..., x_n)$ um polinômio com coeficientes em $\mathbb{Z}_p$ e $a_1, ..., a_n \in \mathbb{Z}_p$ tais que para algum i $(1 \leq i \leq n)$ e $r \in \mathbb{N}$, temos :*

$$F(a_1, ..., a_n) \equiv 0 \ (mod\ p^{2r+1})$$

$$\frac{\partial F}{\partial x_i}(a_1, ..., a_n) \equiv 0 \ (mod\ p^r)$$

$$\frac{\partial F}{\partial x_i}(a_1, ..., a_n) \not\equiv 0 \ (mod\ p^{r+1})$$

Então, existem $b_1, ..., b_n \in \mathbb{Z}_p$ tais que

$$F(b_1, ...b_n) = 0 \ , \ b_i \equiv a_i \ (mod\ p^{r+1}) \ , \ \forall i$$

Corolário 0.2.1 *Sejam $F(x_1, ..., x_n)$ um polinômio com coeficientes em $\mathbb{Z}_p$ e $a_1, ..., a_n \in \mathbb{Z}_p$ tais que para algum i $(1 \leq i \leq n)$, temos :*

$$F(a_1, ..., a_n) \equiv 0 \ (mod\ p)$$

$$\frac{\partial F}{\partial x_i}(a_1, ..., a_n) \not\equiv 0 \ (mod\ p)$$

Então, existem $b_1, ..., b_n \in \mathbb{Z}_p$ tais que

$$F(b_1, ...b_n) = 0 \ , \ b_i \equiv a_i \ (mod\ p) \ , \ \forall i$$

Corolário 0.2.2 ***(Teorema de Chevalley)*** *Se $F(x_1, ..., x_n)$ é um polinômio com coeficientes inteiros de grau menor ou igual a n, então a congruência $F(x_1, ..., x_n) \equiv 0 \ (mod\ p)$ tem uma solução não trivial.*

O seguinte teorema segue do Teorema de Chevalley.

Teorema 0.2.1 *Se $f(x_1, ..., x_n)$ é uma forma quadrática integral, com $n \geq 3$, então a congruência $f(x_1, ..., x_n) \equiv 0 \ (mod\ p)$ tem uma solução não nula.*

Veremos no capítulo 2 que os determinantes de duas formas quadráticas equivalentes sobre um corpo diferem por um fator que é um quadrado nesse corpo. Assim, a fim de entendermos melhor esta equivalência, faz-se necessário o estudo dos quadrados de $\mathbb{Q}_p$.

Suponhamos que um p-ádico $x = p^m u$, com $u \in \mathbb{Z}_p^\times$ seja um quadrado em $\mathbb{Q}_p$. Então existe um p-ádico $y = p^n v$, com $v \in \mathbb{Z}_p^\times$ tal que $x = y^2$. Segue :

$$x = y^2 \Longleftrightarrow p^m u = p^{2n} v^2 \Longleftrightarrow p^m = p^{2n} \ , \ u = v^2$$

Portanto, para determinarmos os quadrados em $\mathbb{Q}_p$, devemos achar os quadrados em $\mathbb{Z}_p^\times$

Definição 0.2.1 *Sejam a e m inteiros primos entre si. Dizemos que a é um* ***Resíduo quadrático módulo m*** *se e somente se a congruência $x^2 \equiv a \ (mod\ m)$ possuir solução. Caso esta congruência não tenha solução, dizemos que a não é um resíduo quadrático módulo m.*

Teorema 0.2.2 *Sejam $p \neq 2$ e $u = c_0 + c_1 p + c_2 p^2 + ... \in \mathbb{Z}_p$ um inteiro p-ádico, com $0 \leq c_i \leq p-1$ e $c_0 \neq 0$. Então, u é um quadrado em $\mathbb{Q}_p$ se e somente se c_0 é um resíduo quadrático módulo p.*

Prova : Se $u = v^2$ e $v \equiv b \ (mod\ p)$, com $b \in \mathbb{Z}$, então :

$$\begin{cases} u = v^2 \\ v^2 \equiv b^2 \ (mod\ p) \end{cases} \Longrightarrow u \equiv b^2 \ (mod\, p) \Longrightarrow c_0 + c_1 p + ... \equiv b^2 \ (mod\, p) \Longrightarrow c_0 \equiv b^2 \ (mod\, p)$$

e, portanto, c_0 é um resíduo quadrático módulo p.

Para a recíproca, suponhamos que $c_0 \equiv b^2 \ (mod\ p)$ e consideremos $F(x) = x^2 - u$. Desta forma, temos que $F(b) = b^2 - u \equiv b^2 - c_0 \equiv 0 \ (mod\ p)$ e $F'(b) = 2b \not\equiv 0 \ (mod\ p)$. Note-se que $F'(b) \equiv 0 \ (mod\ p)$, então $b \equiv 0 \ (mod\ p)$ (pois $p \neq 2$) e portanto $c_0 = 0$, contrariado a hipótese. Pelo corolário 0.2.1, existe $v \in \mathbb{Z}_p$ tal que $F(v) = 0$ e $u \equiv b^2 \ (mod\ p)$. Logo, $v^2 = u$. ■

Corolário 0.2.3 *Se $p \neq 2$ e $u \in \mathbb{Z}_p^\times$ verifica $u \equiv 1 \ (mod\ p)$, então u é um quadrado em $\mathbb{Q}_p$.*

Prova : Basta observar que $u \equiv 1^2 \ (mod\ p)$ e aplicar o teorema. ■

Corolário 0.2.4 *Se $p \neq 2$, então o índice $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2]$ (número de classes) do subgrupo de quadrados $(\mathbb{Q}_p{}^*)^2$ no grupo multiplicativo $\mathbb{Q}_p^*$ é igual a 4.*

Prova : Sejam $x = p^n\beta$ e u um inteiro p-ádico que não é um resíduo quadrático módulo p. Então $\beta \equiv a^2 \ (mod\ p)$ ou $\beta \equiv ua^2 \ (mod\ p)$ para algum inteiro a. Assim, $a^{-2}\beta \equiv 1 \ (mod\ p)$ ou $u^{-1}a^{-2}\beta \equiv 1 \ (mod\ p)$. Pelo corolário anterior, temos que $a^{-2}\beta$ e $u^{-1}a^{-2}\beta$ são quadrados em $\mathbb{Z}_p$ e, portanto :

$$\beta = 1a^2k^2 \text{ ou } \beta = ua^2l^2 \text{ para algum k e l}$$

Portanto, temos os seguintes casos : I) p^n não é um quadrado e β é um quadrado.

$$x = p^n\beta = p(p^{n-1}\beta)$$

II) p^n é um quadrado e u não é um quadrado.

$$x = p^n\beta = u(a^2l^2p^n)$$

III) p^n não é um quadrado e u não é um quadrado.

$$x = p^n\beta = pu(a^2l^2p^{n-1})$$

Logo $\{1, p, u, pu\}$, onde u não é um resíduo quadrático módulo p é um conjunto de representantes para $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)$ e $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2] = 4$. ■

Teorema 0.2.3 *O número $u \in \mathbb{Z}_2^\times$ é um quadrado em $\mathbb{Q}_2$ se e somente se $u \equiv 1 \ (mod\ 8)$.*

Prova : Seja $u = v^2 = (a_0 + a_1 2 + a_2 2^2 + ...)^2$, com $a_i = 0, 1$. Como u é inversível, $2 \nmid {a_0}^2$ e portanto $a_0 = 1$.

$$\begin{aligned} u &= (1 + a_1 2 + a_2 2^2 + ...)(1 + a_1 2 + a_2 2^2 + ...) \\ &= (1 + a_1 2 + a_2 2^2 + ...) + (a_1 2 + {a_1}^2 2^2 + a_1 a_2 2^3 + ...) + (a_2 2^2 + a_1 a_2 2^3 + ...) + ... \\ &= 1 + (a_1 + a_1)2 + (a_2 + {a_1}^2 + a_2)2^2 + (a_3 + a_1 a_2 + a_1 a_2 + a_3)2^3 + ... \end{aligned}$$

Se $a_1 = 0$, então $u = 1 + a_2 2^3 + ... \equiv 1 \ (mod\ 8)$. Se $a_1 = 1$, então :

$$\begin{aligned} u &= 1 + (1 + 1)2 + (1 + 2a_2)2^2 + (a_3 + a_2 2 + a_3)2^3 = ... \\ &= 1 + 2^2 + (1 + 2a_2)2^2 + (a_3 + 2a_2 + a_3)2^3 = ... \\ &= 1 + (2 + 2a_2)2^2 + (a_3 + 2a_2 + a_3)2^3 + ... \\ &= 1 + (1 + a_2 + a_3 + 2a_2 + a_3)2^3 + ... \\ &= 1 + (1 + 2a_2 + 2a_3)2^3 + ... \\ &= 1 + 2^3 + (a_2 + a_3)2^4 + ... \end{aligned}$$

e, portanto, $u \equiv 1 \ (mod\ 8)$.

Para provarmos a recíproca do teorema, consideremos $F(x) = x^2 - u$. Como $F(1) = 1 - u \equiv 0 \ (mod\ 2^3)$ e $F'(1) = 2 \not\equiv 0 \ (mod\ 2^2)$, pelo Lema de Hensel, temos que existe $v \in \mathbb{Z}_2$ tal que $F(v) = 0$. Logo $u = v^2$. ■

Corolário 0.2.5 *O grupo quociente* $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ *possui exatamente* 8 *elementos, ou seja,* $[\mathbb{Q}_2^* : (\mathbb{Q}_2^*)^2] = 8$.

Prova : Vimos acima que $u \in \mathbb{Z}_2^\times$ é um quadrado em $\mathbb{Q}_2^*$ se e somente se $u \equiv 1 \ (mod\ 8)$. Como todo elemento x de $\mathbb{Q}_2^*$ se escreve de modo único como $x = 2^n u$ com $n \in \mathbb{Z}$ e $u \in \mathbb{Z}_2^\times$, temos : x é um quadrado se e somente se n é par e $u \equiv 1 \ (mod\ 8)$. Assim, os elementos $\{1, 3, 5, 7, 2.1, 2.3, 2.5, 2.7\}$ são dois a dois não equivalentes, ou seja, geram classes distintas em $\mathbb{Q}_2^*$. Se x for um quadrado, então $x = 1.x$ e 1 é um representante. Se $x = 2^n u$ não for um quadrado, então :
I) n é ímpar e $u \equiv 1 \ (mod\ 8)$.

$$x = 2^n.u = 2.2^{n-1}u = 2.1.2^{n-1}$$

II) n é par e $u \not\equiv 1 \ (mod\ 8)$, ou seja, $u \in \{3, 5, 7\}$.

$$x = 2^n.u = u.2^n$$

III) n é ímpar e $u \not\equiv 1 \ (mod\ 8)$, ou seja, $u \in \{3, 5, 7\}$.

$$x = p^n.u = 2.u.2^{n-1}$$

Desta forma, terminamos a prova. ■

Antes de definirmos o Símbolo de Legendre para os inteiros p-ádicos, recordaremos este Símbolo para os inteiros.

Definição 0.2.2 *Sejam* p *um primo ímpar e* a *um inteiro não divisível por* p. *Definimos o* ***Símbolo de Legendre*** $\left(\frac{a}{p}\right)$ *por :*

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \textit{se } a \textit{ é um resíduo quadrático módulo } p \\ -1, & \textit{caso contrário} \end{cases}$$

As seguintes propriedades do Símbolo de Legendre podem ser consultadas em [SAN] ou [FLA].

- Se a e b são inteiros não divisíveis por um primo ímpar p, então :

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

- Se p é um primo ímpar, temos :

$$\left(\frac{-1}{p}\right) = \begin{cases} +1, & \text{se } p \equiv 1 \ (mod\ 4) \\ -1, & \text{se } p \equiv -1 \ (mod\ 4) \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & \text{se } p \equiv \pm 1 \ (mod\ 8) \\ -1, & \text{se } p \equiv \pm 3 \ (mod\ 8) \end{cases}$$

Definição 0.2.3 *Sejam p um primo ímpar e $u = c_0 + c_1 p + c_2 p^2 + ... \in \mathbb{Z}_p$, com $0 \leq c_i < p$, $c_0 \neq 0$, ou seja, $u \in \mathbb{Z}_p^\times$. Definimos o* ***Símbolo de Legendre*** $\left(\frac{u}{p}\right)$ *por :*

$$\left(\frac{u}{p}\right) = \begin{cases} +1, & \text{se } u \text{ é um quadrado em } \mathbb{Z}_p \\ -1, & \text{caso contrário} \end{cases}$$

Se o inteiro p-ádico u for inteiro racional, então o Símbolo de Legendre coincide com Símbolo de Legendre usual. Caso contrário, o teorema 0.2.1 afirma que u é um quadrado se e somente se c_0 é um resíduo quadrático módulo p e portanto $\left(\frac{u}{p}\right) = \left(\frac{c_0}{p}\right)$.

Além disso, se $u = c_0 + c_1 p + ...$ e $v = d_0 + d_1 p + ...$ em $\mathbb{Z}_p^\times$, então :

$$\left(\frac{uv}{p}\right) = \left(\frac{c_0 d_0}{p}\right) = \left(\frac{c_0}{p}\right)\left(\frac{d_0}{p}\right) = \left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$$

Capítulo 1

Formas Quadráticas Integrais

Este capítulo trata da classificação de formas quadráticas binárias integrais desenvolvida por Gauss, que pode ser vista em [GAU],[EDW],[MAT],[FLA]. Uma vez que o determinante é um invariante por equivalência integral, é natural dividirmos nosso estudo nos seguintes casos :
I) $d > 0$. Então o discriminante $\Delta = 4(b^2 - ac) = -4d$ da parábola

$$f(\frac{y}{x}) = a + 2b\Big(\frac{y}{x}\Big) + c\Big(\frac{y}{x}\Big)^2$$

é negativo e temos duas possibilidades para c : $c > 0$ e $c < 0$. Note-se que no primeiro caso $f(y/x) > 0$, enquanto que no segundo caso, $f(y/x) < 0$. Por isso, essas formas são chamadas de positivas e negativas, respectivamente.
II) $d < 0$. Neste caso, o discriminante da parábola

$$f(\frac{y}{x}) = a + 2b\Big(\frac{y}{x}\Big) + c\Big(\frac{y}{x}\Big)^2$$

é positivo. Assim, $f(y/x)$ pode assumir valores positivos e negativos. Neste caso, chamaremos esta forma de indefinida.

A classificação das formas quadráticas binárias integrais foi feita por Gauss, usando a equivalência própria. A equivalência integral pode ser vista em termos de ações de grupos assim : seja $Sim(2,\mathbb{Z})$ o conjunto das matrizes simétricas com entradas inteiras. Então, o grupo $GL_2(\mathbb{Z})$ age em $Sim(2,\mathbb{Z})$ do seguinte modo :

$$GL_2(\mathbb{Z}) \times Sim(2,\mathbb{Z}) \longrightarrow Sim(2,\mathbb{Z})$$

$$(M, A) \longmapsto M^t A M$$

A equivalência própria pode ser vista como a ação do subgrupo $SL_2(\mathbb{Z})$ de $GL_2(\mathbb{Z})$ em $Sim(2,\mathbb{Z})$. Veremos adiante que as órbitas da ação de $SL_2(\mathbb{Z})$ em $Sim(2,\mathbb{Z})$ são em número finito. É claro que isso acarreta a finitude das órbitas da ação do grupo maior

$GL_2(\mathbb{Z})$. Como $SL_2(\mathbb{Z})$ é um subgrupo normal de índice 2 em $GL_2(\mathbb{Z})$, existe $\sigma \in GL_2(\mathbb{Z})$ tal que

$$GL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) \dot{\cup} \sigma SL_2(\mathbb{Z})$$

e se $A \in Sim(2, \mathbb{Z})$, podemos fazer $SL_2(\mathbb{Z})$ agir na órbita $O(A)$ de $GL_2(\mathbb{Z})$.

Em princípio poderia acontecer da órbita $O(A)$ também ser uma órbita de $SL_2(\mathbb{Z})$. Suponhamos que $O(A)$ se parta em pelo menos duas órbitas sob a ação de $SL_2(\mathbb{Z})$: nesse caso, $\sigma.A \neq g.A$ para todo $g \in SL_2(\mathbb{Z})$ e

$$O(A) = \{g_i.A : g_i \in SL_2(\mathbb{Z}\} \dot{\cup} \{\sigma g_i.A : g_i \in SL_2(\mathbb{Z})\}$$

Se houvesse algum outro elemento fora dos listados acima, necessariamente ele seria do tipo

$$\sigma g.A$$

para algum $g \in SL_2(\mathbb{Z})$. Como $g.A = g_i.A$ para algum i, temos que $\sigma g.A = \sigma g_i.A$. Assim, cada órbita $O(A)$ de $GL_2(\mathbb{Z})$ se parte no máximo em duas órbitas da ação de $SL_2(\mathbb{Z})$ em $O(A)$. A condição para a existência de uma única órbita é :

$$\sigma.A = g.A$$

para algum $g \in SL_2(\mathbb{Z})$. Ou seja, $g^{-1}\sigma.A = A$. Em termos concretos, se existir uma matriz $M \in GL_2(\mathbb{Z})$ com determinante -1 tal que

$$M^t A M = A,$$

então $O(A)$, órbita de $GL_2(\mathbb{Z})$, também será uma órbita de $SL_2(\mathbb{Z})$.

Exemplo 1 : Se $A = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$, ou seja, a forma associada é $f(x, y) = 2x^2 - 2xy + y^2$, então

$$M = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$$

verifica $M^t A M = A$. Logo, a órbita de A sob $GL_2(\mathbb{Z})$ coincide com a órbita de A sob $SL_2(\mathbb{Z})$.

Exemplo 2 : Se $A = \begin{pmatrix} 3 & 5 \\ 5 & 1 \end{pmatrix}$, então as únicas soluções da equação matricial $M^t A M = A$, com $M = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ são :

$$M_1 = \begin{pmatrix} 0 & -1/\sqrt{3} \\ -\sqrt{3} & 0 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & \sqrt{3} \\ 1/\sqrt{3} & 0 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} -1/\sqrt{26} & -5/\sqrt{26} \\ -5/\sqrt{26} & 1/\sqrt{26} \end{pmatrix}, M_4 = M_3^t$$

Logo, $O(A)$ se parte em duas.

1.1 Formas Binárias Positivas e Negativas

Definição 1.1.1 *Uma forma integral com matriz associada $A = (a, b, c)$ é* ***positiva*** *se e somente se det $A > 0$, $c > 0$,e* ***negativa,*** *se e somente se det $A > 0$, $c < 0$.*

Segue imediatamente da definição que numa forma positiva $a > 0$, e que numa forma negativa, $a < 0$. Como a classificação das formas negativas é análoga à das formas positivas, faremos somente este caso.

Proposição 1.1.1 *Se (a, b, c) é uma forma positiva propriamente equivalente à forma (a', b', c'), então (a', b', c') é positiva.*

Prova : Se $(a, b, c) \sim (a', b', c')$, segue da proposição 0.1.2 que o determinante de (a',b',c') é positivo. Seja $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ a matriz tal que

$$\begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \Longrightarrow a' = \alpha^2 a + 2\alpha\gamma b + \gamma^2 c$$

Como $\alpha\delta - \beta\gamma = 1$, temos que $\alpha = \gamma = 0$ não pode ocorrer. Desta forma, podemos supor, sem perda de generalidade, que $\gamma \neq 0$. Pela positividade de (a, b, c), temos que o discriminante $\Delta = -4(ac - b^2)$ de (a', b', c') é negativo e, portanto

$$\alpha^2 a + 2\alpha x b + x^2 c > 0$$

Em particular,

$$\gamma^2 a' = a(\alpha/\gamma)^2 + 2b(\alpha/\gamma) + c > 0$$

e segue que (a', b', c') é positiva. ■

Definição 1.1.2 *Sejam m um inteiro positivo e b um inteiro. Chamaremos de* ***menores resíduos de b módulo m*** *quaisquer números inteiros entre $-(m-1)$ e $m-1$, inclusive.*

Consideremos $b \equiv r \ (mod\ m)$. A menos que $r = 0$, sempre teremos dois menores resíduos r_1, r_2 com sinais opostos, tais que $|r_1| + |r_2| = m$. Se $|r_1| = |r_2|$, então $|r_1| = |r_2| = m/2$. Caso contrário, $2min\{|r_1|, |r_2|\} < m$ e portanto $min\{|r_1|, |r_2|\} < m/2$. Logo, todo número possui um menor resíduo, cujo módulo não é maior que a sua metade.

Exemplo : Tomando $m = 5$ no parágrafo anterior, os menores resíduos de b módulo 5 são :

$$-4, -3, -2, -1, 0, 1, 2, 3, 4$$

Pondo $b = 27$, temos que a congruência $27 \equiv r \ (mod\ 5)$ possui dois menores resíduos, 3 e -2, tais que a soma dos módulos é igual a 5.

Definição 1.1.3 *Chamaremos esse número, cuja existência é garantida acima, de* ***menor resíduo absoluto de b módulo m.***

Teorema 1.1.1 *Toda forma definida positiva de determinante d é propriamente equivalente à uma forma* (A, B, C), *com* $A \leq \sqrt{4d/3}$ *e* $|2B| \leq A \leq C$.

Prova : A fim de demonstrarmos este resultado, iremos construir uma sequência de formas positivas :

$$(a, b, a_1), (a_1, b_1, a_2), ..., (a_n, b_n, a_{n+1})$$

Assim, suponhamos que a forma integral positiva (a, b, a_1) não satisfaça as duas condições acima. Pela proposição 1.1.1 podemos supor que todos os a_i's são positivos. Vamos provar que existe $m \in \mathbb{Z}$ tal que $a_m \leq a_{m+1}$. Seja b_1 o menor resíduo absoluto de $-b \equiv b_1 \ (mod\ a_1)$ (ou seja, $b + b_1 \equiv 0 \ (mod\ a_1)$). Desta forma,

$$b_1{}^2 \equiv b^2 \ (mod\ a_1) \Longrightarrow b_1{}^2 + d \equiv b^2 + d \ (mod\ a_1)$$

Por $b^2 + d \equiv 0 \ (mod\ a_1)$, temos que $b_1{}^2 + d \equiv 0 \ (mod\ a_1)$. Definamos $a_2 = (b_1{}^2 + d)/a_1 \in \mathbb{Z}$. Se $a_1 > a_2$, consideremos b_2 o menor resíduo absoluto de $b_1 + b_2 \equiv 0 \ (mod\ a_2)$ e $a_3 = (b_2{}^2 + d)/a_2 \in \mathbb{Z}$. Se este processo continuasse infinitamente, teríamos a sequência de inteiros positivos $a, a_1, a_2, a_3, ...$ estritamente decrescente e infinita. Então o processo deve parar, ou seja, existe m tal que $a_m \leq a_{m+1}$.

Vamos verificar que $(A, B, C) = (a_m, b_m, a_{m+1})$, onde $a_m \leq a_{m+1}$, b_m é o menor resíduo absoluto de $b_{m-1} + b_m \equiv 0 \ (mod\ a_m)$ e $a_{m+1} = (b_m{}^2 + d)/a_m \in \mathbb{Z}$ satisfaz as condições requeridas.

(i) Como a sequência é formada somente por formas adjacentes e $\sim$ é uma relação de equivalência, pela proposição 0.1.3, temos que $(A, B, C) \sim (a, b, a_1)$.

(ii) Como b_m é o menor resíduo absoluto de $b_{m-1} + b_m \equiv 0 \ (mod\ a_m)$, temos que $|b_m| \leq a_m/2$ e portanto $|2B| \leq A$.

(iii) Como $a_m a_{m+1} = b_m{}^2 + d$ e $a_m \leq a_{m+1}$, concluímos que $a_m{}^2 \leq b_m{}^2 + d$. Pelo item anterior, $2b_m \leq |2b_m| \leq a_m$. Disto segue :

$$a_m{}^2 \leq \left(\frac{a_m}{2}\right)^2 + d \Longrightarrow \frac{3a_m{}^2}{4} \leq d \Longrightarrow a_m{}^2 \leq \frac{4d}{3}$$

Logo $A = a_m \leq \sqrt{4d/3}$, pois $a_m > 0$. ■

Corolário 1.1.1 *Todas as formas positivas de determinante* $d = 1$ *são propriamente equivalentes.*

Prova : Pelo teorema anterior, temos que toda forma é propriamente equivalente a uma forma (a, b, c) onde $|2b| \leq a \leq c$ e $a \leq \sqrt{4d/3}$. Fazendo $d = 1$, temos que $a \leq \sqrt{4/3}$ e portanto $a = 1$. Por $|2b| \leq 1 \leq c$, segue que $b = 0$. De $ac - b^2 = 1$, temos que $c = 1$. Logo, toda forma positiva de determinante 1 é propriamente equivalente à forma $(1, 0, 1)$. ■

Corolário 1.1.2 *Toda forma positiva é propriamente equivalente a uma forma* (a, b, c), *onde* $-a < 2b \leq a \leq c$, *com* $b \geq 0$ *se* $a = c$.

Prova : Pelo teorema anterior, toda forma integral positiva é propriamente equivalente a uma forma $f(x) = ax_1{}^2 + 2bx_1x_2 + cx_2{}^2$, com $|2b| \leq a \leq c$. Se $2b = a$, façamos :

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & -a/2 \\ -a/2 & c \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a/2 \\ a/2 & c \end{pmatrix}$$

Como $-a_1 = -a < 2b_1 = a \leq c = c_1$, temos que $(a, -a/2, c) \sim (a, a/2, c)$. Se $a = c$ e $b < 0$, façamos :

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ b & a \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & -b \\ -b & a \end{pmatrix}$$

De $a_1 = c_1$ e $b_1 - b > 0$, temos que $(a, b, a) \sim (a, -b, a)$. ■

Definição 1.1.4 *Uma forma positiva* (a, b, c) *é chamada de* ***reduzida*** *se e somente se* $-a < 2b \leq a \leq c$, *com* $b \geq 0$ *se* $a = c$.

Teorema 1.1.2 *Existe uma única forma reduzida em toda classe de equivalência própria de formas positivas.*

Prova : Primeiramente resolvamos a seguinte inequação : $0 < f(x) = ax_1{}^2 + 2bx_1x_2 + cx_2{}^2 \leq a$, onde $-a < 2b \leq a \leq c$, com $b \geq 0$ se $a = c$.

$$ax_1{}^2 + 2bx_1x_2 + cx_2{}^2 = a\Big(x_1 + \frac{b}{a}x_2\Big)^2 + \Big(\frac{|4d|}{4a}\Big)x_2{}^2 \leq a \Longrightarrow$$

$$\Longrightarrow \Big(\frac{|d|}{a}\Big)x_2{}^2 \leq a \Longrightarrow x_2{}^2 \leq \frac{a^2}{|d|} = \frac{a^2}{d}$$

Pelo teorema 1.1.1 :

$$x_2{}^2 \leq \frac{a^2}{d} \leq \frac{1}{d}\frac{4d}{3} = \frac{4}{3} \Longrightarrow x_2 = \pm 1, 0$$

Se $x_2 = 0$, então $x_1 = \pm 1$ e $f(x) = a$. Se $x_2 = \pm 1$, temos que resolver $ax_1{}^2 \pm 2bx_1 + c \leq a$. Como $|2b| \leq a$, temos que $ax_1 \pm 2b \geq 0$ se $x_1 < 0$ e $ax_1 \pm 2b \geq 0$ se $x_1 \geq 0$. Em ambos os casos :

$$ax_1{}^2 \pm 2bx_1 = x_1(ax_1 \pm 2b) \geq 0$$

Como $a \leq c$, $ax_1{}^2 \pm 2bx_1 \geq 0$ e $ax_1{}^2 \pm 2bx_1 \leq a - c$, segue que $ax_1{}^2 \pm 2bx_1 = 0$ e $a = c$. Portanto, $x = 0$ ou $ax \pm 2b = 0$. Mas, $x \in \mathbb{Z}$ e $|2b| \leq a$, o que implica em $|2b| = a$ e $x = \pm 1$.

Desta forma, temos que ter $f(x) = a$ e as 3 soluções são : (I) $x = (\pm 1, 0)$, onde $a < c$, (II) $x = (0, \pm 1)$, onde $a = c$ e (III) $x = (\pm 1, \mp 1)$, onde $a = c = |2b|$. Então, a é o menor

inteiro que pode ser representado pela forma reduzida $f(x)$.

Considere as formas reduzidas $f(x) = ax_1{}^2 + 2bx_1x_2 + cx_2{}^2$ e $f'(x) = a'x_1{}^2 + 2b'x_1x_2 + c'x_2{}^2$ propriamente equivalentes.

Pelo que foi feito acima, podemos escrever $f(x) = a$ e $f'(x) = a'$. Como $f(x) \sim f'(x)$, pela proposição 0.1.1, $f(x)$ e $f'(x)$ representam os mesmos inteiros. Então, $a = a'$.

Seja $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$ tal que $A' = MAM^t$.

$$\begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} r & t \\ s & u \end{pmatrix} =$$

$$= \begin{pmatrix} r^2a + 2rsb + s^2c & rta + rub + stb + suc \\ rta + rub + stb + suc & t^2a + 2tub + u^2c \end{pmatrix}$$

Se $a < c$, então a única solução para $f(x_1, x_2) = a$ é $(\pm 1, 0)$. Como $a = a' = r^2a + 2rsb + s^2c$, devemos ter $r = \pm 1$ e $s = 0$. De $det\ M = 1$, segue que $u = \pm 1$. Então :

$$b' = rta + rub + stb + suc = b \pm ta \Longrightarrow b' - b = \pm ta$$

Mas $-a/2 < b, b' \leq a/2$ implica em $-a < b' - b < a$ e, portanto, $b = b'$. Como os determinantes são iguais, segue que $c = c'$ e $f = f'$.

Suponhamos que $a = c$. Vamos mostrar que $a' < c'$ não pode ocorrer. Usando (I),(II) e (III), temos que $a = a'$ e $c' = t^2a + 2tub + u^2c = t^2a + 2tub + u^2a = a$. Logo, $a' = a = c = c'$. Como os determinantes são iguais, temos que $b^2 = b'^2$ e $b = \pm b'$. Porém, como as formas são reduzidas e $a = c = a' = c'$, temos que $b, b' \geq 0$ e portanto $b = b'$. ■

O teorema 1.1.1 garante que dado um determinante positivo d, existe um número finito de classes de equivalência própria de formas de determinante d. Além disso, pelo teorema 1.1.2, cada uma dessas classes possui uma única forma reduzida. Na tabela a seguir, para um dado determinante d, listamos ao lado todas as formas reduzidas com esse determinante.[CON]

d	*Formas Reduzidas*
1	(1,0,1)
2	(1,0,2)
3	(1,0,3),(2,1,2)
4	(1,0,4),(2,0,2)
5	(1,0,5),(2,1,3)
6	(1.0.6),(2,0,3)
7	(1,0,7),(2,1,4)
8	(1,0,8),(2,0,4),(3.1,3)
9	(1,0,9),(3,0,3),(2,1,5)
10	(1,0,10),(2,0,5)

d	*Formas Reduzidas*
11	(1,0,11),(2,1,6),(3,1,4),(3,-1,4)
12	(1,0,12),(2,0,6),(3,0,4),(4,2,4)
13	(1,0,13),(2,1,7)
14	(1,0,14),(2,0,7),(3,1,5),(3,-1,5)
15	(1,0,15),(3,0,5),(2,1,8),(4,1,4)
16	(1,0,16),(2,0,8),(4,0,4),(4,2,5)
17	(1,0,17),(2,1,9),(3,1,6),(3,-1,6)
18	(1,0,18),(2,0,9),(3,0,6)
19	(1,0,19),(2,1,10),(4,1,5),(4,-1,5)
20	(1,0,20),(3,0,7),(4,0,5),(3,1,7),(3,-1,7),(4,2,6)
21	(1,0,21),(3,0,7),(2,1,11),(5,2,5)
22	(1,0,22),(2,0,11)
23	(1,0,23),(2,1,12),(3,1,8),(3,-1,8),(4,1,6),(4,-1,6)
24	(1,2,24),(2,0,12),(3,0,8),(4,0,6),(5,1,5),(4,2,7)
25	(1,0,25),(5,0,5),(2,1,13)
26	(1,0,26),(2,0,13),(3,1,9),(3,-1,9),(5,2,6),(5,-2,6)
27	(1,0,27),(3,0,9),(2,1,14),(4,1,7),(4,-1,7),(6,3,6)
28	(1,0,28),(2,0,14),(4,0,7),(4,2,8)
29	(1,0,29),(2,1,15),(3,1,10),(3,-1,10),(5,1,6),(5,-1,6)
30	(1,0,30),(2,0,15),(3,0,10),(5,0,6)
31	(1,0,31),(2,1,16),(4,1,8),(4,-1,8),(5,2,7),(5,-2,7)
32	(1,0,32),(2,0,16),(4,0,8),(3,1,11),(3-1,11),(4,2,9),(6,2,6)
33	(1,0,33),(3,0,11),(2,1,7),(6,3,7)
34	(1,0,34),(2,0,17),(5,1,7),(5,-1,7)
35	(1,0,35),(5,0,7),(2,1,18),(3,1,12),(3,-1,12),(4,1,9),(4,-1,9),(6,1,6)
36	(1,0,36),(2,0,18),(3,0,12),(4,0,9),(6,0,6),(4,2,10),(5,2,8),(5,-2,8)
37	(1,0,37),(2,1,19)
38	(1,0,38),(2,0,19),(3,1,13),(3,-1,13),(6,2,7),(6,-2,7)
39	(1,0,39),(3,0,13),(2,1,20),(4,1,10),(4,-1,10),(5,1,8),(5,-1,8),(6,3,8)
40	(1,0,40),(2,0,20),(4,0,10),(5,0,8),(4,2,11),(7,3,7)
41	(1,0,41),(2,1,21),(3,1,14),(3,-1,14),(6,1,7),(6,-1,7),(5,2,9),(5,-2,9)
42	(1,0,42),(2,0,21),(3,0,14),(6,0,7)
43	(1,0,43),(2,1,22),(4,1,11),(4,-1,11)
44	(1,0,44),(2,0,22),(4,0,11),(3,1,15),(3,-1,15),(5,1,9),(5,-1,9),(4,2,12),(6,2,8),(6,-2,8)
45	(1,0,45),(3,0,15),(5,0,9),(2,1,23),(7,2,7),(6,3,9)
46	(1,0,46),(2,0,23),(5,2,10),(5,-2,10)
47	(1,0,47),(2,1,24),(3,1,16),(3,-1,16),(4,1,12),(4,-1,12),(6,1,8),(6,-1,8),(7,3,8),(7,-3,8)
48	(1,0,48),(2,0,24),(3,0,16),(4,0,12),(6,0,8),(7,1,7),(4,2,13),(8,4,8)
49	(1,0,49),(7,0,7),(2,1,12),(5,1,10),(5,-1,10)
50	(1,0,50),(2,0,25),(5,0,10),(3,1,17),(3,-1,17),(6,2,9),(6,-2,9)

Dada uma forma positiva de matriz $A = (a, b, c)$, como achar a forma reduzida, a qual ela é propriamente equivalente ? E como decidir quando duas formas positivas são propriamente equivalentes ?

Poderíamos achar todas as classes de equivalência própria para o dado determinante e depois verificar a que classe ela pertence. Mas este processo pode ser muito demorado para determinantes grandes.

O corolário a seguir fornecerá um algoritmo mais rápido para respondermos a essas questões.

Corolário 1.1.3 *Seja* $\begin{pmatrix} a_0 & b_0 \\ b_0 & a_1 \end{pmatrix}$ *uma forma positiva de determinante* $d = a_0a_1 - {b_0}^2$. *Definimos a sequência :*

$$\begin{pmatrix} a_0 & b_0 \\ b_0 & a_1 \end{pmatrix}, \begin{pmatrix} a_1 & b_1 \\ b_1 & a_2 \end{pmatrix}, \ldots, \begin{pmatrix} a_i & b_i \\ b_i & a_{i+1} \end{pmatrix}, \ldots$$

de formas integrais de determinante d, pelas seguintes condições :

- *Seja* $S = \{x \in \mathbb{Z} : x + b_{i-1} \equiv 0 \ (mod\ a_i)\}$ *e considere* $m = min\{|x| : x \in S\}$. *Se* $m \in S$ *e* $-m \in S$ *ou* $-m \notin S$, *então* $b_i = m$. *Se* $m \notin S$, *então* $b_i = -m$.
- $a_{i+1} = ({b_i}^2 + d)/a_i$.

Então, cada forma positiva da sequência será propriamente equivalente à forma (a_0, b_0, a_1) *e essa sequência se torna periódica a partir de um certo i. O ciclo de formas que se repetem é chamado de ciclos de formas reduzidas. Além disso, duas formas positivas são propriamente equivalentes se e somente se elas têm o mesmo período.*

Prova : Como todas as formas da sequência são adjacentes (proposição 0.1.3), temos que cada forma é propriamente equivalente à antecessora e à sucessora. Pela transitividade, todas as formas serão propriamente equivalentes à primeira forma. Além disso, pela proposição 1.1.1, temos que todas as formas da sequência serão positivas. Então $a_i \leq a_{i+1}$ para algum $i \in \mathbb{N}$ ocorre infinitas vezes, pois caso contrário, teríamos uma sequência estritamente decrescente infinita de inteiros positivos. Desta forma, $a_i^2 \leq |a_ia_{i+1}| \leq b_i^2 + d$ e $|b_i| \leq |a_i|/2$. Portanto a_i, b_i e a_{i+1} para algum $i \in \mathbb{N}$ assumem finitos valores. Assim, alguma forma deve ocorrer pelo menos duas vezes. Como cada forma determina univocamente a sua sucessora na sequência, concluímos que a sequência é periódica.

Provaremos que todo período sempre contém uma única forma reduzida e ainda acharemos os períodos. Para tanto, aplicaremos o algoritmo dado acima na forma (a, b, c), onde $|2b| \leq a \leq c$.

I) Se $b = 0$ e $a \leq c$, temos :

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}, \begin{pmatrix} c & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}, \ldots$$

II) Se $-a < 2b \leq a < c$, então a forma (a, b, c) é reduzida e temos que estudar o período dos casos : $b \neq 0$, $b = a/2$.

Se $b = a/2$, então de $b_1 + a/2 \equiv 0 \ (mod\ c)$ e $m = min\{|a/2|, |c - a/2|\} = a/2$, segue que $b_1 = a/2$ e $a_2 = a$. Continuando o algoritmo :

$$\begin{pmatrix} a & a/2 \\ a/2 & c \end{pmatrix}, \begin{pmatrix} c & a/2 \\ a/2 & a \end{pmatrix}, \begin{pmatrix} a & a/2 \\ a/2 & c \end{pmatrix}, \ldots$$

Se $b > 0$, temos que $m = min\{|-b|, |b-c|\} = |-b|$ e portanto $b_1 = -b$ e $a_2 = a$. Aplicando novamente o algoritmo, obtemos : $b_2 = b$ e $a_3 = c$. Se $b < 0$, então por $m = min\{|-b|, |b+c|\} = |-b|$, temos : $b_1 = -b > 0$ e $a_2 = a$. E segue que $b_2 = -b$ e $a_3 = c$. Em ambos os casos temos a sequência :

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}, \begin{pmatrix} c & -b \\ -b & a \end{pmatrix}, \begin{pmatrix} a & b \\ b & c \end{pmatrix}, \ldots$$

III) Se $-a = 2b < a < c$, então de $b_1 - a/2 \equiv 0 \ (mod\ c)$ e $m = \{|a/2|, |a/2 - c|\}$, obtemos que $b_1 = a/2$ e $a_2 = a$. Continuando o algoritmo, obtemos a seguinte sequência de formas :

$$\begin{pmatrix} a & -a/2 \\ -a/2 & c \end{pmatrix}, \begin{pmatrix} c & a/2 \\ a/2 & a \end{pmatrix}, \begin{pmatrix} a & a/2 \\ a/2 & c \end{pmatrix}, \begin{pmatrix} c & -a/2 \\ -a/2 & a \end{pmatrix}, \begin{pmatrix} a & a/2 \\ a/2 & c \end{pmatrix}, \ldots$$

IV) Se $-a = 2b < a = c$, temos :

$$\begin{pmatrix} a & -a/2 \\ -a/2 & a \end{pmatrix}, \begin{pmatrix} a & a/2 \\ a/2 & a \end{pmatrix}, \begin{pmatrix} a & a/2 \\ a/2 & a \end{pmatrix}, \ldots$$

V) Se $-a < 2b < a = c$ e $b < 0$, então $b_1 + b \equiv 0 \ (mod\ a)$ e $m = min\{|-b|, |-(a+b)|\}$ implicam que $b_1 = -b$ e $a_2 = a$. Continuando o algoritmo, obtemos :

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}, \begin{pmatrix} a & -b \\ -b & a \end{pmatrix}, \begin{pmatrix} a & -b \\ -b & a \end{pmatrix}, \ldots$$

Pela unicidade da forma reduzida em cada classe de equivalência própria, segue que todo ciclo de formas reduzidas contém uma única forma reduzida.

Se duas formas são propriamente equivalentes, pela unicidade da forma reduzida, temos que ambas serão propriamente equivalentes à mesma forma reduzida. Como cada ciclo de formas reduzidas contém uma única forma reduzida e cada sucessora da sequência é univocamente determinada, segue que os ciclos de formas reduzidas são iguais. ■

Exemplo : Decidir se as formas $(2, 2, 5)$ e $(1, 1, 7)$ são propriamente equivalentes. Alpicando o algoritmo em cada uma delas, obtemos as sequências :

$$(2, 2, 5), (5, -2, 2), (2, 0, 3), \ldots$$

$$(1, 1, 7), (7, -1, 1), (1, 0, 6), \ldots$$

Como as formas reduzidas $(2, 0, 3)$ e $(1, 0, 6)$ são diferentes, as formas $(2, 2, 5)$ e $(1, 1, 7)$ não podem ser propriamente equivalentes.

1.2 Formas Binárias Indefinidas

Nesta seção, estamos interessados na classificação das formas tais que $d < 0$. Observe-se que $\Delta = -4(b^2 - ac) = -4d > 0$ e, portanto, a forma $f(x, y) = ax^2 + 2bxy + cy^2$ pode assumir valores positivos ou negativos.

Definição 1.2.1 *Uma forma integral com matriz associada $A = (a, b, c)$ é* ***indefinida*** *se e somente se det $A < 0$.*

Analogamente ao que foi feito para formas definidas positivas, temos o seguinte teorema de Gauss :

Teorema 1.2.1 *Toda forma indefinida com determinante d, tal que $-d$ não é um quadrado, é propriamente equivalente à forma (A, B, C) onde $0 < B < \sqrt{-d}$ e $\sqrt{-d} - B < |A| < \sqrt{-d} + B$.*

Prova : Suponhamos que uma dada forma indefinida (a, b, a_1), não satisfaça as duas condições do enunciado. Observe que por $-d$ não ser um quadrado, temos que $aa_1 \neq 0$ e portanto $a, a_1 \neq 0$.

Afirmamos que existe um único $b_1 \in Z$ tal que $b + b_1 \equiv 0 \ (mod\ a_1)$ e $\sqrt{-d} - |a_1| < b_1 < \sqrt{-d})$. Como $-d$ não é um quadrado, $\sqrt{-d}$ é irracional e portanto, $(\sqrt{-d} + b)/|a_1|$ não é inteiro. Então, existe um único $t \in \mathbb{Z}$ tal que :

$$\frac{\sqrt{-d} + b}{|a_1|} - 1 < t < \frac{\sqrt{-d} + b}{|a_1|}$$

pois, a distância entre os dois extremos é 1 e nenhum deles é inteiro. Disso, segue que:

$$\sqrt{-d} - |a_1| < t|a_1| - b < \sqrt{-d}$$

Definindo $b_1 = t|a_1| - b$, temos ainda que $b + b_1 \equiv 0 \ (mod\ a_1)$. Seja $a_2 = ({b_1}^2 + d)/a_1 \in \mathbb{Z}$. Se $|a_1| > |a_2|$, tomemos b_2 tal que $b_1 + b_2 \equiv 0 \ (mod\ a_2)$, $\sqrt{-d} - |a_2| < b_2 < \sqrt{-d}$ e defina $a_3 = ({b_2}^2 + d)/a_2$. Como a sequência $|a_1|, |a_2|, \ldots$ de inteiros positivos não pode decrescer estritamente e infinitamente, a sequência deve parar. Então existe $m \in \mathbb{Z}$ tal que $|a_m| \leq |a_{m+1}|$. Definamos $(A, B, C) = (a_m, b_m, a_{m+1})$, onde

$$b_{m-1} + b_m \equiv 0 \ (mod\ a_m)\ ,\ \sqrt{-d} - |a_m| < b_m < \sqrt{-d},$$

$$|a_m| \leq |a_{m+1}| \ \text{ e } \ a_{m+1} = ({b_m}^2 + d)/a_m$$

e provemos que esta é a forma que desejamos encontrar.

I) Como a sequência é formada somente por formas adjacentes e $\sim$ é uma relação de equivalência, pela proposição 0.1.3, temos que $(A, B, C) \sim (a, b, a_1)$.

II) Mostraremos que $\sqrt{-d} - |A| < B < \sqrt{-d}$ e $|A| \leq |C|$ implicam em $\sqrt{-d} - B < |A| < \sqrt{-d} + B$ e $0 < B < \sqrt{-d}$.

II) Como $\sqrt{-d} - |A| < B < \sqrt{-d}$, temos que $\sqrt{-d} - B < |A|$ e $\sqrt{-d} - B > 0$ e assim :

$$| - d - B^2| = |A||C| > (\sqrt{-d} - B)|C| = |\sqrt{-d} - B||C| \Longrightarrow |\sqrt{-d} - B| < |A|$$

Suponhamos, por absurdo que $B \leq 0$. Pela hipótese, $\sqrt{-d} - B > 0$. Usando a última desigualdade acima, temos que $\sqrt{-d} - B < |\sqrt{-d} + B|$, o que é um absurdo, uma vez que $B \leq 0$. Logo, $0 < B < \sqrt{-d}$ e portanto :

$$\sqrt{-d} - B < |A| \leq |C| < \sqrt{-d} + B$$

Isso termina a prova. ■

Esse teorema sugere uma divisão das formas indefinidas em formas tais que $-d$ é ou não um quadrado.

Definição 1.2.2 *Uma forma indefinida (a, b, c) de determinante $-d$, tal que $-d$ não um quadrado, é chamada de* ***reduzida*** *se e somente se $\sqrt{-d} - b < |a| < \sqrt{-d} + b$ e $0 < b < \sqrt{-d}$.*

Note que da prova do teorema anterior segue que a e c têm sinais opostos, $|a| \leq |c|$ e $\sqrt{-d} - b < |c| < \sqrt{-d} + b$.

Corolário 1.2.1 *Se (a, b, c) é uma forma indefinida reduzida, então as formas reduzidas adjacentes a (a, b, c) são únicas.*

Prova : I) Existência das formas adjacentes reduzidas.

Consideremos $p = \sqrt{-d} + b - |c|$, $q = |c| - (\sqrt{-d} - b)$ e $r = \sqrt{-d} - b$. Da definição de forma reduzida, temos que $p, q, r > 0$. Por $\sqrt{-d} - |c| < b' < \sqrt{-d}$, segue que $q' = b' - (\sqrt{-d} - |c|)$ e $r' = \sqrt{-d} - b'$ também são positivos. Seja $b' = |/c|t - b$ para algum t inteiro. Como $p + q' = \sqrt{-d} + b - |c| + b' - (\sqrt{-d} - |c|) = b + b'$, $p + q' > 0$ e $b + b' = t|c|$, temos que $t > 0$. Além disso,

$$r + q' + t|c| = \sqrt{-d} - b + b' - (\sqrt{-d} - |c|) + t|c| = b' + b' + |c| = 2b' + |c|$$

e portanto $2b' = r + q' + (t - 1)|c|$. Disso segue que $2b', b' > 0$. Mas, $b' + r' = \sqrt{-d}$ e então $b' < \sqrt{-d}$. Como $r + (t - 1)|c| = \sqrt{-d} + b' - |c|$ e $r, t > 0$, temos que :

$$\sqrt{-d} + b' - |c| > 0 \Longrightarrow |c| < \sqrt{-d} + b'$$

Por outro lado, $|c| - (\sqrt{-d} - b') = q' > 0$ e segue que $\sqrt{-d} - b' < |c|$. Logo, $\sqrt{-d} - b' < |c| < \sqrt{-d} + b'$ e (A, B, C) é reduzida. Se $C = a$, procedendo analogamente ao caso anterior, temos que a forma (A, B, C) será reduzida e adjacente a (a, b, c).

II) Unicidade das formas adjacentes reduzidas.

Suponhamos que (c, b', c') e (c, b'', c'') sejam formas reduzidas e adjacentes a (a, b, c). Então $\sqrt{-d} - |c| < b', b'' < \sqrt{-d}$ e $0 < b', b''$. Mas, pela demonstração do teorema anterior, existe um único inteiro que satisfaz as condições acima. Desta forma $b' = b''$ e temos que as formas são iguais. Analogamente, se (a', b', a) e (a'', b'', a) são formas reduzidas e adjacentes a (a, b, c), então elas são iguais. ■

Observe-se que se (a, b, c) não for reduzida, não podemos garantir a unicidade da forma adjacente a (a, b, c). Basta considerar o seguinte exemplo : $(2, 1, 4)$ e $(2, -1, 4)$ são adjacentes a $(4, 1, 2)$.

Corolário 1.2.2 *Sejam* $('a,' b, a)$, (a, b, c) *e* (c, b', c') *formas indefinidas reduzidas adjacentes. Então :*

1. $(c', b', c), (c, b, a), (a,' b,' c)$
2. $(-'a,' b, -a), (-a, b, -c), (-c, b', -c')$
3. $(-c', b', -c), (-c, b, -a), (-a,' b, -'a)$

são adjacentes nesta ordem.

Prova : Segue diretamente da unicidade das formas adjacentes reduzidas. ■

Exemplo : Para $d = -79$, listamos todas as formas reduzidas :

$$(\pm 7, 3, \mp 10), (\pm 10, 3, \mp 7), (\pm 7, 4, \mp 9), (\pm 9, 4, \mp 7)$$

$$(\pm 6, 5, \mp 9), (\pm 9, 5, \mp 6), (\pm 2, 7, \mp 15), (\pm 3, 7, \mp 10)$$

$$(\pm 5, 7, \mp 6), (\pm 6, 7, \mp 5), (\pm 10, 7, \mp 3), (\pm 15, 7, \mp 2)$$

$$(\pm 1, 8, \mp 15), (\pm 3, 8, \mp 5), (\pm 5, 8, \mp 3), (\pm 15, 8, \mp 1)$$

Proposição 1.2.1 *Seja* $f_0, f_1, f_2, \ldots$ *uma sequência de formas indefinidas reduzidas adjacentes. Então, existe* $m \in \mathbb{Z}$ *tal que* $f_0 = f_m$.

Prova : Como a sequência é formada somente por formas adjacentes e $\sim$ é uma relação de equivalência, temos que $f_i \sim f_0, \forall i \geq 0$. Entretanto, pelo número de formas reduzidas de um dado determinante ser finito, existe m tal que $f_n = f_{n+m}$. Pela unicidade das formas indefinidas reduzidas, segue que $f_{n-1} = f_{n+m-1}, f_{n-2} = f_{n+m-2}, \ldots, f_0 = f_m$. ■

Isto motiva a seguinte definição :

Definição 1.2.3 *Chamaremos tal número* m *de* ***período de formas reduzidas*** *e a sequência* $f_0, f_1, \ldots, f_{m-1}$ *de* ***ciclo de formas reduzidas***.

Definição 1.2.4 *Seja $f = (a, b, c)$, uma forma indefinida com determinante d tal que $-d$ não é um quadrado. Definimos as* ***raízes*** *$\Omega(f)$ e $\omega(f)$* ***de f*** *por :*

$$\Omega(f) = \frac{b + \sqrt{-d}}{c} \text{ e } \omega(f) = \frac{b - \sqrt{-d}}{c}$$

Note-se que se f e g forem formas com mesmo determinante $d < 0$ tais que $\Omega(f) = \Omega(g)$, então $f = g$. Este fato segue de :

$$(z + \Omega(f))(z + \omega(f)) = 0 \Longleftrightarrow z^2 + \frac{2b}{c}z + \frac{a}{c} = 0 \Longleftrightarrow f(z) = cz^2 + 2bz + a = 0$$

onde $z = (x_2/x_1)$.

O resultado a seguir caracteriza uma forma indefinida, tal que $-d$ não é um quadrado, relacionando-a com suas raízes.

Lema 1.2.1 *Uma forma $f = (a, b, c)$ é reduzida se e somente se $\omega(f)\Omega(f) < 0$ e $|\omega(f)| < 1 < |\Omega(f)|$.*

Prova : Basta usar que f é reduzida se e somente se $\sqrt{-d} - b < |a| \leq |c| < \sqrt{-d} + b$ e $0 < b < \sqrt{-d}$. ■

Lema 1.2.2 *Se f é uma forma indefinida tal que $-d$ não é um quadrado e $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$, então :*

$$\Omega(\gamma f \gamma^t) = \frac{r\Omega(f) + s}{t\Omega(f) + u} \quad e \quad \omega(\gamma f \gamma^t) = \frac{r\omega(f) + s}{t\omega(f) + u}$$

Prova : Sejam $\Omega = \Omega(f)$, $\omega = \omega(f)$ e

$$\gamma f \gamma^t = \begin{pmatrix} A & B \\ C & D \end{pmatrix} := \begin{pmatrix} r^2a + 2rsb + s^2c & rta + stb + urb + usc \\ rta + stb + urb + usc & t^2a + 2tub + u^2c \end{pmatrix}$$

Mostraremos que :

$$\gamma f \gamma^t = C\left(z^2 + \frac{2B}{C}z + \frac{A}{C}\right) = C\left(z + \frac{r\Omega + s}{t\Omega + u}\right)\left(z + \frac{r\omega + s}{t\Omega + u}\right)$$

Como $\Omega\omega = 2b/c$ e $\Omega + \omega = a/c$, segue :

$$\begin{aligned}\left(z + \frac{r\Omega + s}{t\Omega + u}\right)\left(z + \frac{r\omega + s}{t\Omega + u}\right) &= z^2 + \left(\frac{r\Omega + s}{t\Omega + u} + \frac{r\omega + s}{t\omega + u}\right)z + \left(\frac{r\Omega + s}{t\Omega + u}\right)\left(\frac{r\omega + s}{t\omega + u}\right) = \\ &= z^2 + 2\left(\frac{rta + stb + urb + usc}{t^2a + 2tub + u^2c}\right)z + \frac{r^2a + 2rsb + s^2c}{t^2a + 2tub + u^2c} = \\ &= z^2 + \frac{2B}{C}z + \frac{A}{C}\end{aligned}$$

Portanto,

$$\Omega(\gamma f\gamma^t) = \frac{r\Omega(f)+s}{t\Omega(f)+u} \quad e \quad \omega(\gamma f\gamma^t) = \frac{r\omega(f)+s}{t\omega(f)+u}$$

o que encerra a prova. ■

Adiante, estudaremos algumas propriedades das matrizes com determinante igual a 1. A razão para tal estudo é a de compreendermos melhor a equivalência própria entre formas indefinidas.

Definição 1.2.5 *Dados $a_0, a_1, ..., a_n$ reais positivos, definimos a* ***fração contínua*** *(denotada por $(a_0, a_1, ..., a_n)$) pelas condições :*

$$(a_0) = a_0 \text{ e } (a_0, a_1, ..., a_n) = a_0 + \frac{1}{(a_1, ..., a_n)}$$

Dizemos que uma fração contínua $(a_0, a_1, ..., a_{n-1}, y)$ é ***quase simples*** *se e somente se $a_i \in \mathbb{N}^*$, $\forall i = 0, 1, ..., n-1$ e $y > 1$.*

Lema 1.2.3 *Se $x = (a_0, a_1, ..., a_{n-1}, y)$ é uma fração contínua e*

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}...\begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R}),$$

então $x = (ry+s)/(ty+u)$.

Prova : Se $n = 1$, então $r = a_0, s = t = 1, u = 0$ e $ru - st = -1$. Segue :

$$x = (a_0, y) = a_0 + \frac{1}{y} = \frac{a_0 y + 1}{y} = \frac{ry+s}{ty+u}$$

Suponhamos, por hipótese de indução, que :

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}...\begin{pmatrix} a_{n-2} & 1 \\ 1 & 0 \end{pmatrix}$$

$$x = (a_0, a_1, ..., a_{n-2}, y) = \frac{ry+s}{ty+u}$$

Vamos provar que $(a_0, ..., a_{n-1}, y') = (r'y + s')/(t'y + u')$, onde :

$$\begin{pmatrix} r' & s' \\ t' & u' \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}...\begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix}$$

Pela hipótese de indução, segue que :

$$\begin{pmatrix} r' & s' \\ t' & u' \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix}$$

e portanto $r' = ra_{n-1} + s, s' = r, u' = t$ e $t' = ta_{n-1} + u$. Como a fração contínua é definida por recorrência, temos que :

$$\frac{1}{y} = \frac{1}{a_{n-1} + 1/y'} \Longrightarrow y = a_{n-1} + \frac{1}{y'}$$

Disso segue :

$$(a_0, ..., a_{n-1}, y') = \frac{r(a_{n-1} + 1/y') + s}{t(a_{n-1} + 1/y') + u} = \frac{(ra_{n-1} + s)y' + r}{(ta_{n-1} + u)y' + t} = \frac{r'y' + s'}{t'y' + u'}$$

Logo, x é da forma que queríamos. ■

Observe-se que se $(a_0, a_1, ..., a_{n-1}, y)$ for quase simples, temos que $ru - ts = \pm 1$.

Proposição 1.2.2 *Se duas frações contínuas quase simples* $x = (a_0, ..., a_n)$ *e* $y = (b_0, ..., b_n)$ *são iguais, então* $a_i = b_i$, $\forall i = 0, 1, ..., n$.

Prova : Vamos provar por indução em n. O caso $n = 0$ é trivial. Suponhamos que se $(a_1, ..., a_n) = (b_1, ..., b_n)$, então $a_i = b_i$, $\forall i = 1, ..., n$.

Como $x = a_0 + 1/(a_1, ..., a_n)$ e $(a_1, ..., a_n) > 1$ (pois, x é quase simples), temos que $a_0 = [x]$. Analogamente, $b_0 = [y]$. Deste modo, se $x = y$, então $a_0 = b_0$ e portanto $(a_1, ..., a_n) = (b_1, ..., b_n)$. Usando a hipótese de indução, segue que $a_i = b_i$, $\forall i = 0, 1, ..., n$. ■

Proposição 1.2.3 *Se* $M = \begin{pmatrix} R & S \\ T & U \end{pmatrix} \in GL_2(\mathbb{Z})$, *onde* $R \geq S \geq U \geq 0$ *e* $R \geq T \geq U$, *então existem inteiros positivos* $n, a_0, ..., a_{n-1}$ *tais que :*

$$M = \begin{pmatrix} a_o & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} ... \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix}$$

Prova : Usaremos indução em T. Observe-se que $T = 0$ não pode ocorrer, pois U seria igual a 0, o que contradiz $RU - ST = \pm 1$. Se $T = 1$, então $U = 0$ ou $U = 1$. Como $RU - ST = \pm 1$, $S \geq 0$ e $R - S \geq 0$, temos que $S = 1$ ou $R = S + 1$. Desta forma :

$$M = \begin{pmatrix} R & 1 \\ 1 & 0 \end{pmatrix} \text{ ou } M = \begin{pmatrix} S+1 & S \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} S & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Suponhamos, por hipótese de indução, que $T > 1$ e existem inteiros positivos $n, a_0, ..., a_{n-2}$, tais que

$$\gamma = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} ... \begin{pmatrix} a_{n-2} & 1 \\ 1 & 0 \end{pmatrix}$$

Como $RU - ST = \pm 1$, temos que $R > T > U > 0$ e $T \nmid R$. Pois, se $T = U$ ou $R = T$ ou $T \mid R$, teremos que $T = 1$. Considere o inteiro positivo m, tal que $R/T - 1 < m < R/T$ e

$$\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} := \begin{pmatrix} m & 1 \\ 1 & 0 \end{pmatrix}^{-1} M = \begin{pmatrix} 0 & 1 \\ 1 & -m \end{pmatrix} \begin{pmatrix} R & S \\ T & U \end{pmatrix} = \begin{pmatrix} T & U \\ R - mT & S - mU \end{pmatrix}$$

Observe-se que $r = T > U = s > 0$. Pela escolha de m, temos que $0 < R - mT = t < T$. De $u = (st + det\ \gamma)/r$, segue que $u \geq 0$. Resta mostrarmos que $s \geq u$ e $t \geq u$. Se $s < u$, então $ru \geq (t+1)(s+1) = st + s + t + 1$ e portanto $ru - st \geq s + t + 1 > 1$ (contradição com $ru - st = \pm 1$). Analogamente, segue que não podemos ter $t < u$. Então :

$$M = \begin{pmatrix} m & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

e pela hipótese de indução :

$$M = \begin{pmatrix} m & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{n-2} & 1 \\ 1 & 0 \end{pmatrix}$$

onde $n, m, a_0, ..., a_{n-2}$ são inteiros positivos. ■

Lema 1.2.4 *Sejam* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$, $cx + d \neq 0$ *e* $cy + d \neq 0$, *onde* x *e* y *verificam as duas inequações :*

$$x > 1 \quad e \quad \frac{ax + b}{cx + d} > 1 \qquad (*)$$

$$-1 < y < 0 \quad e \quad -1 < \frac{ay + b}{cy + d} < 0 \qquad (**)$$

Então, exatamente uma das seguintes afirmativas é correta :

(A) $\gamma = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

(B) $\gamma = \pm \begin{pmatrix} r & s \\ t & u \end{pmatrix}$, *com* $r \geq s \geq u \geq 0$ *e* $r \geq t \geq u$

(C) $\gamma^{-1} = \pm \begin{pmatrix} r & s \\ t & u \end{pmatrix}$, *com* $r \geq s \geq u \geq 0$ *e* $r \geq t \geq u$

Prova : Vamos considerar os seguintes casos :

Caso 1 : $abcd \neq 0, c > 0, d > 0$

Como $ad = bc \pm 1$, temos que ad e bc são não nulos, consecutivos e têm o mesmo sinal. Então, a e b têm o mesmo sinal. De $(*)$, segue que $ax + b > cx + d > 0$ e portanto $(a - c)x > d - b$, $a > 0$ e $b > 0$. Desta forma, devemos ter $a > 0$ ou $b > d$. Pois, se $a \leq c$ e $b \leq d$, teríamos que $(a - c)x < 0$, $d - b > 0$ e portanto $(a - c)x < d - b$. Se $a > c$, então $b \geq d$. De fato, se $b < d$, então

$$ad \geq (b+1)(c+1) = bc + b + c + 1 \Longrightarrow ad - bc \geq b + c + 1 > 1\ ,$$

o que nos levaria a uma contradição. Analogamente, $b > d$ implica em $a \geq c$.

Se $ay + b < 0$, então por $-1 < y < 0$ e $y < -b/a$, temos $b/a < |y| < 1$. Mas, $a, b > 0$ e segue que $b < a$. Analogamente ao parágrafo anterior, $c \geq d$. Se $ay + b > 0$, então por

$(**)$, obtemos que $cy + d < 0$. Disto segue, $d/c < |y| < 1$ e portanto $c > d$. Logo, $a \geq b$ e acabamos de verificar (B).

Caso 2 : $abcd \neq 0$ e $c < 0, d < 0$.

Neste caso, verificamos (B), uma vez que $-\gamma$ pertence ao caso anterior.

Caso 3 : $abcd \neq 0$ e $c < 0, d > 0$.

Segue de $ad - bc = \pm 1$ que a e b têm sinais contrários. Como $cy + d > 0$, $(**)$ implica que $ay + d < 0$ e portanto $a > 0$.

Considere $\gamma^{-1} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in GL_2(\mathbb{Z})$, $x' = (ax + b)/(cx + d)$ e $y' = (ay + c)/(cy + d)$. Desta modo, temos duas inequações da forma de $(*), (**)$:

$$x' > 1 \; e \; \frac{dx' - b}{-cx' + a} > 1 \qquad (*')$$

$$-1 < y' < 0 \; e \; -1 < \frac{dy' - b}{-cy' + a} < 0 \qquad (**')$$

Usando as argumentações dos casos 1 e 2 na matriz γ^{-1}, verificamos (C).

Caso 4 : $abcd \neq 0, c > 0, d < 0$.

(C) é verificada, pois $-\gamma$ pertence ao caso anterior.

Caso 5 : $abcd = 0$.

As possíveis formas de γ são :

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} m & 1 \\ 1 & 0 \end{pmatrix} \; ou \; \pm \begin{pmatrix} 0 & 1 \\ 1 & -m \end{pmatrix} = \pm \begin{pmatrix} m & 1 \\ 1 & 0 \end{pmatrix}^{-1}$$

para algum inteiro m.

Estas formas verificam $(A), (B)$ ou (C). Como os casos são mutuamente exclusivos, segue a tese. ■

Seja $f = f_0$ uma forma indefinida reduzida tal que $-d$ não é um quadrado. Ao aplicarmos o algoritmo conseguimos uma sequência de formas reduzidas $f = f_0, f_1, f_2, ..., f_n, ...$ tais que cada duas formas reduzidas consecutivas são adjacentes.

Lema 1.2.5 *Se f e g são formas indefinidas reduzidas tais que o oposto de seus determinantes não são quadrados, então as seguintes afirmações são equivalentes :*

1. $f_n = g$
2. $sign(\Omega(g)) = (-1)^n sign(\Omega(f))$ *e existe uma fração contínua quase simples tal que* $|\Omega(f)| = (d_0, d_1, ..., d_{n-1}, |\Omega(g)|)$

Prova : Vamos provar, por indução em n, que (1) implica (2). Se $n = 1$, consideremos $f_1 = (a_1, b_1, a_2)$ adjacente a $f = (a, b, a_1)$. Como f é reduzida, temos que $a_1 a_2 < 0$ e

b, $b_1 > 0$. Portanto, $-1 = sign(a_1a_2) = sign(\Omega\Omega(f_1))$.

Seja $k \in \mathbb{Z}$ tal que $b + b_1 = k|a_1|$. Então :

$$\begin{aligned}\Omega &= \frac{b+\sqrt{-d}}{a_1} = \frac{k|a_1| - b_1 + \sqrt{-d}}{a_1} = \frac{k|a_1|}{a_1} + \frac{-b_1+\sqrt{-d}}{a_1} \\ &= k\ sign(a_1) - \frac{1}{\Omega(f_1)}\end{aligned}$$

Assim $|\Omega| = k + 1/\Omega(f_1) = (k, |\Omega(f_1)|)$. Como b e b_1 são positivos, temos que $k \geq 1$. Pelo lema 1.2.1, temos que $|\Omega(f_1)| > 1$.

Suponhamos, por hipótese de indução, que existam inteiros positivos $n, k_1, ..., k_n$ tais que $|\Omega(f_1)| = (k_1, ..., k_{n-1}, |\Omega(f_n)|)$ e $sign(\Omega(f_{n-1})) = (-1)^{n-1}sign(\Omega(f))$. Aplicando a mesma, obtemos

$$|\Omega| = (k, |\Omega(f_1)|) = (k, (k_1, ..., k_{n-1}, |\Omega(f_n)|) = (k, k_1, ..., k_{n-1}, |\Omega(f_n)|),$$

onde $k, k_1, ..., k_{n-1}$ são inteiros positivos e

$$sign(\Omega(f_n)) = -sign(\Omega(f_{n-1}) = (-1)(-1)^{n-1}sign(\Omega(f)) = (-1)^n sign(\Omega(f))$$

Pelo lema 1.2.1, temos que $|\Omega(g)| > 1$.

Vamos agora provar a recíproca. Por hipótese, existe uma fração contínua quase simples tal que $|\Omega(f)| = (k_0, k_1, ..., k_{n-1}, |\Omega(f_n)|)$, onde $sign(\Omega(f_n)) = (-1)^n sign(\Omega(f))$. Da mesma maneira, existe uma fração contínua quase simples tal que

$$|\Omega(f)| = (d_0, d_1, ..., d_{n-1}, |\Omega(g)|) \text{ e}$$

$$sign(\Omega(g)) = (-1)^n sign(\Omega(f))$$

Então, $sign(\Omega(g)) = sign(\Omega(f_n))$. Como

$$(k_0, k_1, ..., k_{n-1}, |\Omega(f_n)|) = (d_0, d_1, ..., d_{n-1}, |\Omega(g)|),$$

pela proposição 1.2.2, temos $|\Omega(f_n)| = |\Omega(g)|$. Deste modo, $\Omega(f_n) = \Omega(g)$ e portanto $f_n = g$. ■

Teorema 1.2.2 *Se f e g são formas indefinidas reduzidas propriamente equivalentes de mesmo determinante d tal que $-d$ não é um quadrado. então uma pertence ao ciclo de formas reduzidas da outra.*

Prova : Sejam f e g como na hipótese e $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$ tal que $f = MgM^t$. Denotaremos por Ω e ω as raízes de f e Ω' e ω' as raízes de g. Definamos :

$$\gamma = \begin{cases} \begin{pmatrix} r & s \\ t & u \end{pmatrix} = M & se\ \Omega, \Omega' > 0 \\ \begin{pmatrix} r & -s \\ -t & u \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} M \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} & se\ \Omega, \Omega' < 0 \\ \begin{pmatrix} -r & s \\ -t & u \end{pmatrix} = M \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} & se\ \Omega > 0, \Omega' < 0 \\ \begin{pmatrix} -r & -s \\ t & u \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} M & se\ \Omega < 0, \Omega' > 0 \end{cases}$$

Observe-se que $\gamma \in GL_2(\mathbb{Z})$ e $det\ \gamma = sign(\Omega\Omega')$. Se $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, então pelo lema 1.2.2, temos :

$$|\Omega| = \frac{a|\Omega'| + b}{c|\Omega'| + d} \quad e \quad -|\omega| = \frac{-a(|\omega'|) + b}{-c(|\omega'|) + d} \quad (I)$$

Como f, g são reduzidas e vale (I), pelo lema 1.2.1, segue que γ satisfaz as hipóteses do lema 1.2.4 com $x = |\Omega'|$ e $y = -|\omega'|$. Desta forma, somente umas das condições $(A), (B)$ ou (C) é satisfeita. Se γ satisfaz (A), então $\Omega = \Omega'$ e portanto $f = g$. Se γ satisfaz (B), então pela proposição 1.2.3, existem inteiros positivos $n, d_0, d_1, ..., d_{n-1}$ tais que :

$$\gamma = \pm \begin{pmatrix} d_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} d_{n-1} & 1 \\ 1 & 0 \end{pmatrix}$$

Pelo lema 1.2.3 e pelas equações (I), $|\Omega| = (r|\Omega'|+s)/(t|\Omega'|+u) = (d_0, d_1, ..., d_{n-1}, |\Omega'|)$. Observe-se que $(-1)^n = det\ \gamma = sign(\Omega\Omega')$. Desta forma, pelo lema anterior, concluímos que $f_n = g$.

Se γ satisfaz (C), então aplicando o mesmo processo usado no caso anterior em γ^{-1}, temos que existe um inteiro positivo n tal que $f = g_n$. Seja $N > 0$ tal que $g_N = g$. Então, $f_1 = g_{n+1}, f_2 = g_{n+2}, \cdots, f_{N-n} = g_{n+(N-n)} = g_n = g$. ■

Finalmente estamos pronto para provar o algoritmo para formas indefinidas tais que $-d$ não é um quadrado :

Corolário 1.2.3 *Seja* $\begin{pmatrix} a_0 & b_0 \\ b_0 & a_1 \end{pmatrix}$ *uma forma indefinida de determinante* $d = a_0a_1 - {b_0}^2$ *tal que* $-d$ *não é um quadrado. Definimos a sequência :*

$$\begin{pmatrix} a_0 & b_0 \\ b_0 & a_1 \end{pmatrix}, \begin{pmatrix} a_1 & b_1 \\ b_1 & a_2 \end{pmatrix}, \ldots, \begin{pmatrix} a_i & b_i \\ b_i & a_{i+1} \end{pmatrix}, \ldots$$

de formas integrais de determinante d pelas seguintes condições :

- *Se existe solução x que verifica* $x^2 + d < 0$ *e* $b_i + x \equiv 0\ (mod\ a_{i+1})$, *então* b_{i+1} *será a maior destas soluções e* $a_{i+2} = ({b_{i+1}}^2 + d)/a_{i+1}$.

- *Caso contrário, seja* $S = \{s \in \mathbb{Z} : x + b_{i-1} \equiv 0 \ (mod\ a_i)\}$ *e considere* $m = min\{|x| : x \in S\}$. *Se* $m \in S$ *e* $-m \in S$ *ou* $-m \notin S$, *então* $b_i = m$. *Se* $m \notin S$, *então* $b_i = -m$. *Em ambos os casos* $a_{i+1} = ({b_i}^2 + d)/a_i$.

Então, cada forma indefinida da sequência será propriamente equivalente a (a_0, b_0, a_1) *e essa sequência se torna periódica a partir de um certo* i. *O ciclo de formas que se repetem é chamado de ciclo de formas reduzidas. Além disso, duas formas indefinidas são propriamente equivalentes se e somente se têm o mesmo ciclo de formas reduzidas.*

Prova : Como todas as formas da sequência são adjacentes, todas serão propriamente equivalentes à primeira forma (a_0, b_0, a_1). Além disso, existe $n \in \mathbb{Z}$ tal que $|a_n| \leq |a_{n+1}|$ ocorre infinitas vezes, pois caso contrário, teríamos uma sequência estritamente decrescente e infinita de inteiros positivos. Assim, $|a_i| \leq |a_i a_{i+1}| \leq b_i^2 + |d|$ e $b_i^2 < -d$ ou $|b_i| \leq |a_i|/2$. Então $a_i^2 \leq 2|d|$ ou $a_i^2 \leq a_i^2/4 + |d|$, $|a_i| \leq 2\sqrt{|d|/3}$ e, portanto, a_i assume finitos valores. Logo, (a_n, b_n, b_{n+1}) assume finitos valores. Desta forma, alguma forma deve ocorrer pelo menos duas vezes. Como cada forma determina univocamente sua sucessora na sequência, concluímos que ela é periódica. Além disso, todo período sempre é formado somente por formas reduzidas. Caso contrário, não teríamos a unicidade das formas reduzidas.

É claro que se duas formas têm o mesmo ciclo de formas reduzidas, então elas são propriamente equivalentes.

Reciprocamente, se duas formas são propriamente equivalentes, então todas as formas do ciclo de formas reduzidas serão propriamente equivalentes às formas do outro ciclo de formas reduzidas. Pelo teorema acima, existem pelo menos duas formas reduzidas, uma de cada ciclo, as quais são iguais (ou seja, se duas formas reduzidas são propriamente equivalentes, então cada uma está contida no ciclo de formas reduzidas da outra). Pela unicidade das formas reduzidas adjacentes, concluímos que os ciclos são iguais. ■

A seguir, faremos alguns exemplos de todos os ciclos de formas reduzidas de um dado determinante d, tal que $-d$ não é quadrado. Usaremos as condições de redução e a da unicidade das formas adjacentes reduzidas.

1) Para $d = -2$, temos que o ciclo de formas reduzidas é :

- $(1, 1, -1), (-1, 1, 1), ...$

Portanto todas as formas de $d = -2$ são propriamente equivalentes.

2) Para $d = -3$, temos que os ciclos de formas reduzidas são :

- $(2, 1, -1), (-1, 1, 2), ...$
- $(1, 1, -2), (-2, 1, 1), ...$

3) Para $d = -5$, temos que os ciclos de formas reduzidas são :

- $(2, 1, -2), (-2, 1, 2), ...$

- $(1,2,-1),(-1,2,1),...$

4) Para $d=-6$, temos que os ciclos de formas reduzidas são :

- $(1,2,-2),(-2,2,1),...$
- $(-1,2,-2),(2,2,-1),...$

5) Para $d=-7$, temos que os ciclos de formas reduzidas são :

- $(2,1,-3),(-3,2,1),(1,2,-3),(-3,1,2),...$
- $(-2,1,3),(3,2,-1),(-1,2,3),(3,1,-2),...$

6) Para $d=-13$, temos que os ciclos de formas reduzidas são :

- $(-4,1,3),(3,2,-3),(-3,1,4),(4,3,-1),(-1,3,4),$
  $(4,1,-3),(-3,2,3),(3,1,-4),(-4,3,1),(1,3,-4),...$
- $(2,3,-2),(-2,3,2),...$

Abaixo, seguem exemplos da aplicação do algoritmo acima.

$$(2,3,3),(3,0,-1),(-1,1,2),(2,1,-1),(-1,1,2),...$$

$$(1,5,23),(23,-5,1),(1,1,-2),(-2,1,1),(1,1,-2),...$$

$$(1,3,7),(3,-3,1),(1,1,-1),(-1,1,1),(1,1,-1),...$$

$$(13,4,1),(1,1,-2),(-2,1,1),(1,1,-2),...$$

Agora, vamos classificar as formas indefinidas tais que $-d$ é um quadrado.

Teorema 1.2.3 *Toda forma indefinida (a,b,c) tal que $-d=h^2\neq 0$, onde h é a raiz positiva, é propriamente equivalente à forma $(A,h,0)$, com $0\leq A\leq 2h-1$.*

Prova : Vamos dividir em casos :
I) Se $a\neq 0$ e $b\neq -h$, por $h^2=-d=b^2-ac$ segue que :

$$h^2-b^2=-ac\Longrightarrow (h-b)(h+b)=-ac\Longrightarrow \frac{(h-b)}{a}=\frac{c}{-(h+b)}$$

Sejam $\beta,\delta\in\mathbb{Z}$, tais que $mdc(\beta,\delta)=1$ e β/δ seja igual a razão acima. Pelo teorema de Bézout, existem $\alpha,\gamma\in\mathbb{Z}$ tais que $\alpha\delta-\beta\gamma$. Deste modo :

$$\begin{aligned}\begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} &= \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\\ &= \begin{pmatrix} \alpha a+\gamma b & \alpha b+\gamma c \\ \beta a+\delta b & \beta b+\delta c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\\ &= \begin{pmatrix} \alpha^2 a+2\alpha\gamma b+\gamma^2 c & \alpha\beta a+b(\gamma\beta+\alpha\delta)+\gamma\delta c \\ \alpha\beta a+b(\gamma\beta+\alpha\delta)+\gamma\delta c & \beta^2 a+2\beta\delta b+\delta^2 c \end{pmatrix}\end{aligned}$$

Assim :

$$\begin{aligned} b' &= \alpha\beta a + b(\gamma\beta + \alpha\delta) + \gamma\delta c \\ &= (h-b)\alpha\delta + b\alpha\delta + b\beta\gamma - (h+b)\beta\gamma \\ &= h\alpha\delta - h\beta\gamma = h \end{aligned}$$

$$\begin{aligned} c' &= \beta^2 a + 2\beta\delta b + \delta^2 c \\ &= (h-b)\beta\delta + 2b\beta\delta - (h+b)\beta\delta \\ &= 2b\beta\delta - 2b\beta\delta = 0 \end{aligned}$$

Se, além disso, $0 < a' \leq 2h-1$, então (a', b', c') é a forma que procuramos. Caso contrário, ou seja, $a' \leq 0$ ou $a' > 2h-1$, considere A o menor inteiro positivo tal que $a' \equiv A \ (mod\ 2h)$. Então, $0 < A \leq 2h/2 = h \leq 2h-1$. Assim, existe $k \in \mathbb{Z}$ tal que $A = a' + 2hk$. Observe-se que :

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & h \\ h & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} = \begin{pmatrix} a'+2hk & h \\ h & 0 \end{pmatrix} = \begin{pmatrix} A & h \\ h & 0 \end{pmatrix}$$

e portanto $(a', b', c') \sim (A, h, 0)$. Por transitividade, temos que $(a, b, c) \sim (A, h, 0)$. Ou seja, (a, b, c) é tranformada em $(A, h, 0)$ pela matriz $\begin{pmatrix} \alpha+\beta k & \gamma+\delta k \\ \beta & \delta \end{pmatrix}$.

II) Se $a \neq 0$ e $b = -h$, então $c = 0$.

Considere β, δ inteiros tais que $mdc(\beta, \delta) = 1$ e $\beta/\delta = (h-b)/a = 2h/a$. Então, existem α, γ inteiros tais que $\alpha\delta - \beta\gamma = 1$. Temos :

$$\begin{aligned} c' &= \beta^2 a - 2h\beta\delta + \delta^2 c \\ &= 2h\delta\beta - 2h\beta\delta = 0 \end{aligned}$$

$$\begin{aligned} b' &= \alpha\beta a - h(\gamma\beta + \alpha\delta) + \gamma\delta c \\ &= a\alpha\beta - h\alpha\delta - h\beta\gamma \\ &= 2h\alpha\delta - h\alpha\delta - h\beta\gamma \\ &= h\alpha\delta - h\beta\gamma \\ &= h(\alpha\delta - \beta\gamma) = h \end{aligned}$$

Se $0 \leq a' \leq 2h-1$, então esta é a forma que procuramos. Caso contrário, tomemos A como sendo o menor inteiro positivo tal que $a' \equiv A \ (mod\ 2h)$. Analogamente ao caso anterior, temos que $(a, b, c) \sim (A, h, 0)$, com $0 < A \leq 2h-1$.

III) Se $a = 0$ e $b = -h$, então $(0, -h, c) \sim (c, h, 0)$. Caso c não satisfaça $0 \leq c \leq 2h-1$, então existe A tal que $(c, h, 0) \sim (A, h, 0)$, com $0 < A \leq 2h-1$.

IV) Se $a = 0$ e $b \neq -h$, então $b = h$.

Se $c = 0$, então não há o que provar. Caso contrário, considere δ, β inteiros tais que $mdc(\delta, \beta) = 1$ e $\delta/\beta = -(h+b)/c = -2h/c$. Então, existem α, γ inteiros tais que $\alpha\delta - \beta\gamma = 1$. Temos :

$$\begin{aligned} b' &= \alpha\beta a + h(\gamma\beta + \alpha\delta) + \gamma\delta c \\ &= h\beta\gamma + h\alpha\delta - 2h\beta\gamma \\ &= h\alpha\delta - h\beta\gamma \\ &= h(\alpha\delta - \beta\gamma) = h \end{aligned}$$

$$\begin{aligned} c' &= \beta^2 a + 2h\beta\delta + \delta^2 c = \\ &= 2h\delta\beta - 2h\beta\delta = 0 \end{aligned}$$

Se a' não satisfaz $0 \leq a' \leq 2h-1$, existe A tal que $(a', h, 0) \sim (A, h, 0)$, com $0 < A \leq 2h-1$. ■

Definição 1.2.6 *Dizemos que uma forma indefinida de determinante d, tal que* $0 \neq -d = h^2$, *é* ***reduzida*** *se ela é da forma* $(a, h, 0)$, *onde* $0 \leq a \leq 2h-1$.

Teorema 1.2.4 *As formas indefinidas* $(a, h, 0)$ *e* $(a', h, 0)$ *são propriamente equivalentes se e somente se* $a \equiv a' \ (mod\ 2h)$.

Prova : Se elas são propriamente equivalentes, então existe $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ tal que

$$\begin{pmatrix} a' & h \\ h & 0 \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a & h \\ h & 0 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha^2 a + 2\alpha\gamma h & \alpha\beta a + \beta\gamma h + \alpha\delta h \\ \alpha\beta a + \beta\gamma h + \alpha\delta h & \beta^2 a + 2\beta\delta h \end{pmatrix}$$

Disso segue o seguinte sistema de equações :

$$\begin{cases} \alpha^2 a + 2\alpha\gamma h = a' & (I) \\ \alpha\beta a + \beta\gamma h + \alpha\delta h = h & (II) \\ \beta^2 a + 2\beta\delta h = 0 & (III) \\ \alpha\delta - \beta\gamma = 1 & (IV) \end{cases}$$

Multiplicando (II) por β, obtemos $\beta h = \alpha\beta^2 a + h(\beta^2\gamma + \alpha\beta\gamma)$. De (III), segue que :

$$\beta h = \alpha(-2\beta\delta h) + h(\beta^2\gamma + \alpha\beta\delta) = h(\beta^2\gamma - \alpha\beta\delta) \Longrightarrow$$

$$\beta h = \beta h(\beta\gamma - \alpha\delta) \Longrightarrow \beta h = -\beta h \Longrightarrow \beta = 0$$

De (IV), temos $\alpha = \delta = \pm 1$. Então $a' = a \pm 2\gamma h$, ou seja, $a \equiv a' \ (mod\ 2h)$. Se $a \equiv a' \ (mod\ 2h)$, existe t inteiro tal que $a' = a + t2h$. Consideremos a matriz $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ e observemos que :

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & h \\ h & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \begin{pmatrix} a + t2h & h \\ h & 0 \end{pmatrix} = \begin{pmatrix} a' & h \\ h & 0 \end{pmatrix}$$

Logo, $(a, h, 0) \sim (a', h, 0)$. ■

Corolário 1.2.4 *As formas* ***reduzidas*** $(a, h, 0)$ *e* $(a', h, 0)$ *são propriamente equivalentes se e somente se são iguais.*

Prova : Se $a = a'$, então elas serão propriamente equivalentes pela matriz identidade. Se $(a, h, 0) \sim (a', h, 0)$, pelo teorema acima, temos que $a \equiv a' \ (mod\ 2h)$. Além disso, da demonstração do mesmo, obtemos que $a' = a \pm 2\gamma h$. Como as formas são reduzidas, temos que $|a' - a| \leq 2h - 1$. Então $\gamma = 0$. De

$$\begin{pmatrix} a' & h \\ h & 0 \end{pmatrix} = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \begin{pmatrix} a & h \\ h & 0 \end{pmatrix} \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \Longrightarrow \begin{pmatrix} a' & h \\ h & 0 \end{pmatrix} = \begin{pmatrix} a & h \\ h & 0 \end{pmatrix}$$

segue $a = a'$. ■

O teorema acima garante a existência e a unicidade de uma forma reduzida em cada classe de equivalência própria. Ou seja, duas formas reduzidas são propriamente equivalentes se e somente se elas forem iguais.

Com todos esses resultados, podemos dizer que dado um determinante $d \neq 0$, sempre conseguimos um número finito de classes de equivalência própria originadas pelas formas reduzidas únicas (no caso de positivas, negativas e indefinidas tais que $-d$ é um quadrado) ou pelas sequências únicas de formas reduzidas (no caso de formas indefinidas tais que $-d$ não é um quadrado).

Observe-se que o teorema 1.2.3 fornece um algoritmo para decidirmos se duas dadas formas indefinidas, tais que $-d$ não é um quadrado, são propriamente equivalentes. Para tanto, basta acharmos as correspondentes formas reduzidas e compará-las.

Capítulo 2

Formas Quadráticas Sobre um Corpo

Naturalmente, formas quadráticas binárias integralmente equivalentes, também são equivalentes sobre $\mathbb{Q}$. Mas, as formas $f(x,y) = x^2 + y^2$ e $g(z,t) = 2z^2 + 2t^2$ mostram que a recíproca de tal fato não é verdadeira. Fazendo a mudança de variáveis :

$$z = \frac{x+y}{2} \ , \ t = \frac{x-y}{2},$$

temos que essas formas são equivalentes sobre $\mathbb{Q}$. Por outro lado, elas não podem ser integralmente equivalentes, pois seus determinantes são diferentes.

Assim, nestes dois capítulos restantes, vamos estudar a equivalência de formas quadráticas binárias racionais. Começamos com alguns resultados básicos sobre formas quadráticas com coeficientes num corpo arbitrário K.

2.1 Formas Equivalentes

Definição 2.1.1 *Uma* ***forma quadrática n-ária sobre um corpo K*** *é um polinômio de grau 2 com coeficientes em K :*

$$f = f(x_1, ..., x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \ , \ a_{ij} = a_{ji}$$

A matriz $[f] = (a_{ij})$ é chamada de ***matriz da forma quadrática f.*** *Se o determinante da forma f for igual a zero, então f é* ***singular.*** *Caso contrátio, f é* ***não singular.***
Notação : $\sim$

Definição 2.1.2 *Dizemos que duas formas quadráticas n-árias sobre um corpo K são* ***equivalentes sobre o corpo*** *K se e somente se existir uma mudança de variáveis não singular que transforma uma forma na outra.*

Assim, as formas f e g são equivalentes se existir um matriz $M \in GL_n(K)$ tal que $[f] = M^t[g]M$. Se $f(x_1, ..., x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j = X^t[f]X$, com $X^t = (x_1, ..., x_n)$ e $M \in GL_n(K)$, então $[g] = Y^t M^t A M Y$, com $X = MY$.

Definição 2.1.3 *Dizemos que uma forma quadrática n-ária f sobre um corpo K* ***representa um elemento não nulo*** *$a \in K$ se e somente se existirem $a_1, ..., a_n \in K$ tais que $f(a_1, ..., a_n) = a$. Dizemos que f* ***representa zero em*** *K se e somente se existirem $a_1, ..., a_n \in K$ não todos nulos, tais que $f(a_1, ..., a_n) = 0$.*

Proposição 2.1.1 *Sejam f e g formas quadráticas n-árias equivalentes sobre um corpo K. Então :*

1. *Seus determinantes diferem por um fator quadrado ,não nulo, de K.*
2. *f e g representam os mesmo elementos de K.*

Prova : Seja $M \in GL_n(K)$ tal que $[f] = M^t[g]M$.
1) Segue de :

$$det\ [f] = det\ (M^t[g]M) \Longrightarrow det\ [f] = (det\ M)^2 det\ [g]$$

2) Se $n = f(X_0)$, então :

$$g(MX_0) = (MX_0)^t(M^t)^{-1}[f]M^{-1}(MX_0) = X_0^t[f]X_0 = f(X_0) = n$$

Se $m = g(Y_0)$, então $f((M^t)^{-1}Y_0) = m$. ■

Teorema 2.1.1 *Toda forma quadrática n-ária sobre um corpo K, de característica diferente de 2 é equivalente a uma forma diagonal :*

$$d(y_1, ..., y_r) = \sum_{i=1}^{n} b_i {y_i}^2 \ , \ b_i \in K \ , \ \forall\ i$$

Além disso, a matriz desta equivalência tem determinante igual a 1.

Prova : Seja $f(x_1, ..., x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ uma forma quadrática n-ária sobre K e consideremos os seguintes tipos de mudanças de variáveis :
Tipo I : $x_i = y_j, x_j = x_i$ e $x_k = y_k, k \neq i, j$

Esta operação troca as linhas i e j e depois as colunas i e j. Em termos da diagonal principal, troca-se os elementos a_{ii} e a_{jj}.
Tipo II : $x_i = y_i + ry_j$ e $x_k = y_k, k \neq i$

Esta operação soma a j-ésima linha com r vezes a i-ésima linha e coloca o resultado na j-ésima linha, seguido do correspondente processo nas colunas. Ou seja, $rl_i + l_j = L_j$ e $rc_i + c_j = C_j$, onde L_j e C_j são as novas j-ésimas linha e coluna, respectivamente.

Observe que em ambas as mudanças de variáveis não alteram o deteminante de f.

Agora usaremos um algoritmo para zerarmos todos os coeficientes de f que não pertençam à diagonal principal.

Se $a_{ll} \neq 0$ para algum l, então usamos o tipo I, com $i = 1$ e $j = l$. Desta forma, $[f]$ é tranformada numa matriz cujo $A_{11} = a_{ll} \neq 0$. Se $a_{ll} = 0, \forall l$, então existem m, n distintos tais que $a_{mn} \neq 0$. Caso contrário, $[f]$ seria a matriz nula e portanto já estaria na forma

diagonal. Usando 2 vezes o tipo I, primeiramente com $i = 1$, $j = m$ e depois com $i = 2$ e $j = n$, conseguimos uma matriz cujo $A_{12} = a_{mn} \neq 0$. Pelo tipo 2, com $i = 2$ $j = 1$ e $r = 1$, obtemos uma matriz cujo $A'_{11} = A_{12} \neq 0$.

Em ambos os casos, obtemos uma matriz cujo coeficiente 11 é diferente de zero. Portanto, podemos supor que $a_{11} \neq 0$.

Considere f na seguinte forma :

$$f(x_1, ..., x_n) = (a_{11}x_1^2 + 2a_{12}x_1x_2 + ... + 2a_{1n}x_1x_n) + k(x_2, ..., x_n),$$

onde k é uma forma quadrática que só depende das variáveis $x_2, ...x_n$.

Completando quadrados temos :

$$f(x_1, ..., x_n) = \frac{(c_{11}x_1 + c_{12}x_2 + ... + c_{1n}x_n)^2}{c_{11}} + g(x_2, ..., x_n)$$

Pois, o sistema linear

$$\begin{cases} c_{11}^2/c_{11} = a_{11} \neq 0 \\ 2c_{12}c_{11}/c_{11} = 2a_{12} \\ \vdots \\ 2c_{1n}c_{11}/c_{11} = 2a_{1n} \end{cases}$$

é possível e determinado.

Usando a mudança de variáveis $z_1 = (c_{11}x_1 + ... + c_{1n}x_n)/c_{11}$, $z_i = x_i$ para $i > 1$, temos $h(z_1, ..., z_n) = c_{11}z_1^2 + g'(z_2, ..., z_n)$. Esta mudança da variáveis é a composta de várias aplicações do tipo II, ou seja, c_{1j}/c_{11} vezes a linha 1 somando com a j-ésima linha e depois analogamente para as colunas.

Aplicando diversas vezes este algoritmo na forma quadrática restante não diagonalizada, obtemos a forma :

$$d(y_1, ..., y_n) = \sum_{i=1}^{n} b_i {y_i}^2 \ , \ b_i \in K \ , \forall \ i$$

Como cada mudança de variáveis do tipo I e tipo II tem determinante igual a ± 1, a mudança resultante do produto de todas essas mudanças, que leva f em d, tem determinante igual a ± 1. Se esta tiver deteminante igual a -1, então trocamos o sinal de alguma variável sem trocar o sinal do deteminante de d. Desta forma o determinante do produto será 1. O número r é igual ao posto da matriz de d, pois a mudança que leva f em d é invertível e portanto não altera o posto de f. ■

Exemplo : Ilustraremos o processo descrito no teorema acima, por meio da forma $f(x_1, x_2, x_3) = 2x_1x_2 + 6x_1x_3 - x_2^2 + 2x_3^2$. Como $a_{11} = 0$, usando uma transformação do tipo I, com $i = 1$ e $j = 2$, temos :

$$\begin{pmatrix} 0 & 1 & 3 \\ 1 & -1 & 0 \\ 3 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 3 \\ 3 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 3 \\ 0 & 3 & 2 \end{pmatrix} := f_1$$

Completando quadrados, temos que $f_1(x_1, x_2, x_3) = -(x_1 - x_2)^2 + g(x_2, x_3)$, onde $g(x_2, x_3) = x_2^2 + 6x_2x_3 + 2x_3^2$. Usando a mundança $z_1 = -x_1 + x_2$, $z_2 = x_2$ e $z_3 = x_3$, segue que :

$$f_2(z_1, z_2, z_3) := -z_1^2 + g_1(z_2, z_3) \ , \ g_1(z_2, z_3) = z_2^2 + 6z_2z_3 + 2z_3^2$$

e assim, conseguimos zerar a linha e a coluna 1. Aplicando o mesmo processo em $g_1(z_2, z_3)$, obtemos $t_2^2 - 7t_3^2$. Portanto, f é equivalente à forma diagonal :

$$d(y_1, y_2, y_3) = -y_1^2 + y_2^2 - 7y_3^2$$

Corolário 2.1.1 *Se uma forma quadrática f em n-ária representa $\alpha \neq 0$, então f é equivalente a uma forma do tipo $\alpha x_1^2 + g(x_2, ..., x_n)$, onde g é uma forma quadrática em $n-1$ variáveis.*

Prova : Seja d uma forma quadrática diagonal tal que $d \sim f$. Como f representa $\alpha \neq 0$ e formas equivalentes representam os mesmo elementos, temos que existem $\alpha_1, ..., \alpha_n \in K$, não todos nulos, tais que $d(\alpha_1, ..., \alpha_n) = \alpha$. Consideremos uma matriz $M \in GL_n(K)$ tal que a primeira coluna é $\alpha_1, ..., \alpha_n$. Assim :

$$\begin{aligned} M^t[d]M &= \begin{pmatrix} \alpha_1 & \dots & \alpha_n \\ \vdots & \ddots & \vdots \\ \vdots & \dots & \ddots \end{pmatrix} \begin{pmatrix} a_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_n \end{pmatrix} \begin{pmatrix} \alpha_1 & \dots & \dots \\ \vdots & \ddots & \dots \\ \alpha_n & \dots & \ddots \end{pmatrix} \\ &= \begin{pmatrix} a_1\alpha_1^2 + ... + a_n\alpha_n^2 & \dots & \dots \\ \vdots & \ddots & \dots \\ \vdots & \dots & \ddots \end{pmatrix} = \begin{pmatrix} \alpha & \dots & \dots \\ \vdots & \ddots & \dots \\ \vdots & \dots & \ddots \end{pmatrix} \end{aligned}$$

Como $\alpha \neq 0$, podemos usar a mesma idéia do teorema anterior e teremos que esta forma, cujo coeficiente 1-1 é α, será equivalente a uma forma do tipo $\alpha x_1^2 + g(x_2, ..., x_n)$. ■

Pelo teorema anterior, a questão da equivalência de formas racionais fica reduzida a equivalência de formas diagonais. No caso da equivalência sobre os reais, fazendo a mudança de variáveis : $x_i = y_i/\sqrt{|a_i|}$, se $a_i > 0$ e $x_i = -y_i/\sqrt{|a_i|}$, se $a_i < 0$, essa forma possui somente $+1$ ou -1 nos elementos da diagonal. O teorema a seguir fornece um critério muito útil para decidirmos quando duas formas diagonais são equivalentes sobre o reais. [JON]

Teorema 2.1.2 ***(Teorema de Sylvester)*** *Se as formas quadráticas, não singulares,*

$$f(x_1, ...x_n) = x_1^2 + ... + x_i^2 - x_{i+1}^2 - ... - x_n^2$$

$$g(y_1, ...y_n) = y_1^2 + ... + y_j^2 - y_{j+1} - ... - y_n^2$$

forem equivalentes sobre $\mathbb{R}$, então $i = j$.

Prova : Suponhamos que $j > i$. Seja $M = (a_{kl})$ a matriz que transforma f em g, isto é,

$$\begin{cases} y_1 = a_{11}x_1 + ... + a_{1n}x_n \\ y_2 = a_{21}x_1 + ... + a_{2n}x_n \\ \quad\vdots \quad\quad ... \quad\quad \vdots \\ y_n = a_{n1}x_1 + ... + a_{nn}x_n \end{cases}$$

Tomando $x_1 = ...x_i = 0$, o sistema $y_{j+1} = 0, ..., y_n = 0$ possui $n - j$ equações e $n - i$ incógnitas. Como $n - j < n - i$, existem $x_{i+1}, ...x_n$, não todos nulos, que satisfazem esse sistema. Mas, esses valores para os x's e y's também satisfazem aquele sistema. Assim $g = f$, ou seja,

$$-x_{i+1}^2 - ... - x_n^2 = y_1^2 + ... + y_j^2$$

com $x_{i+1}, ..., x_n$ não todos nulos. O que é impossível para valores reais.

Analogamente, pode-se mostrar que $j < i$ induz a uma contradição. Portanto $i = j$, ou seja, as duas formas possuem o mesmo número de 1's e -1's. ■

Note-se que pelo teorema acima, temos que duas formas quadráticas n-árias, não singulares e com coeficientes racionais são equivalentes sobre os reais se e somente se o número de 1's das formas diagonais correspondentes são o mesmo.

Não é difícil ver que formas racionais equivalentes sobre $\mathbb{Q}$, são equivalentes também sobre $\mathbb{R}$. Porém, pelo fato de que os determinantes das formas $x^2 + y^2$ e $z^2 + 3t^2$ diferem por um fator que não é um quadrado em $\mathbb{Q}$, a recíproca do fato anterior é falsa.

Como $\mathbb{R}$ é um dos completamentos de $\mathbb{Q}$, é natural estudarmos a equivalência de formas sobre outros completamentos de $\mathbb{Q}$. Ora, já sabemos pelo teorema de Ostrowski que os únicos completamentos de $\mathbb{Q}$ são $\mathbb{R}$ e os $\mathbb{Q}_p$'s.

Definição 2.1.4 *Sejam $f = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ e $g = \sum_{i,j=1}^{n} b_{ij}y_iy_j$ formas quadráticas n-árias sobre um corpo K. A forma $(f \oplus g)(x_1, ..., x_n, y_1, ...y_n)$ de $2n$ variáveis definida por :*

$$(f \oplus g)(x_1, ..., x_n, y_1, ...y_n) = f(x_1, ..., x_n) + g(y_1, ..., y_n)$$

é chamada de ***soma direta de f e g.***

Esta definição não deve ser confundida com a soma usual de polinômios, quando f e g estão nas mesmas variáveis.

Lema 2.1.1 *Sejam g, h e f formas quadráticas n-árias sobre um corpo K. Se $g \sim h$. então $f \oplus g \sim f \oplus h$.*

Prova : Se $g \sim h$, então existe $M \in GL_n(K)$ tal que $[g] = M^t[h]M$. Como

$$[f \oplus g] = \begin{pmatrix} [f] & 0 \\ 0 & [g] \end{pmatrix} \ , \ [f \oplus h] = \begin{pmatrix} [f] & 0 \\ 0 & [h] \end{pmatrix}$$

temos que :

$$[f \oplus g] = \begin{pmatrix} [f] & 0 \\ 0 & [g] \end{pmatrix} = \begin{pmatrix} [f] & 0 \\ 0 & M^t[h]M \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & M^t \end{pmatrix} \begin{pmatrix} [f] & 0 \\ 0 & [h] \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & M \end{pmatrix}$$

Sendo $N = \begin{pmatrix} I & 0 \\ 0 & M \end{pmatrix}$, $det\ N = det\ I det\ M = det\ M \neq 0$. Desta forma, $[f \oplus g] = N^t[f \oplus h]N$, com $N \in GL_n(K)$ e $f \oplus g \sim f \oplus h$. ■

A recíproca deste lema é o :

Teorema 2.1.3 ***(Teorema do Cancelamento de Witt)*** *Sejam f, g e h formas quadráticas não singulares sobre um corpo K de característica diferente de 2. Se $f \oplus g \sim f \oplus h$, então $g \sim h$.*

Prova : Pelo teorema anterior, existe uma forma diagonal f_0 tal que $f_0 \sim f$. Aplicando o lema anterior, $f_0 \oplus g \sim f \oplus g$ e $f_0 \oplus h \sim f \oplus h$. Pela hipótese, $f_0 \oplus h \sim f_0 \oplus g$ e portanto podemos assumir que f é uma forma diagonal.

Seja $f = a_1x_1^2 \oplus a_2x_2^2 \oplus ... \oplus a_nx_n^2$, com $a_i \neq 0$. Para provarmos o teorema, basta provarmos o caso particular ax^2, $a \neq 0$. De fato, se $a_x^2 \oplus g \sim ax^2 \oplus h$ implicar em $g \sim h$, então :

$$(a_1x_1^2 \oplus a_2x_2^2 \oplus ... \oplus a_nx_n^2) \oplus g \sim (a_1x_1^2 \oplus a_2x_2^2 \oplus ... \oplus a_nx_n^2) \oplus h \Longrightarrow$$

$$a_1x_1^2 \oplus (a_2x_2^2 \oplus ... \oplus a_nx_n^2 \oplus g) \sim a_1x_1^2 \oplus (a_2x_2^2 \oplus ... \oplus a_nx_n^2 \oplus h) \Longrightarrow$$

$$(a_2x_2^2 \oplus ... \oplus a_nx_n^2 \oplus g) \sim (a_2x_2^2 \oplus ... \oplus a_nx_n^2 \oplus h) \Longrightarrow$$

$$(a_2x_2^2 \oplus ... \oplus a_nx_n^2) \oplus g \sim (a_2x_2^2 \oplus ... \oplus a_nx_n^2) \oplus h \Longrightarrow$$

$$\vdots$$

$$a_nx_n^2 \oplus g \sim a_nx_n^2 \oplus h \Longrightarrow g \sim h$$

Assim, consideremos $f = ax^2, a \neq 0$, G e H matrizes de g e h, respectivamente. Como $ax^2 \oplus g \sim ax^2 \oplus h$, existe $C = \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix}$ tal que

$$\begin{pmatrix} \gamma & T^t \\ S^t & Q^t \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & G \end{pmatrix} \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & H \end{pmatrix}$$

onde S é uma matriz linha $1 \times n$, T é uma matriz coluna $n \times 1$, $\gamma \in K$ e $Q \in GL_n(K)$. Disto resulta o seguinte sistema :

$$\begin{cases} \gamma^2 + T^tGT = a & (I) \\ \gamma aS + T^tGQ = 0 & (II) \\ S^taS + Q^tGQ = H & (III) \end{cases}$$

Devemos mostrar que existe uma matriz C_0 não singular tal que $C_0^t G C_0 = H$. Para tanto, consideremos $C_0 = Q + \xi TS$ e vamos encontrar ξ tal que $C_0^t G C_0 = H$.

$$\begin{aligned} C_0^t G C_0 &= (Q+\xi TS)^t G(Q+\xi TS) = (Q^t + \xi S^t T^t) G(Q+\xi TS) = \\ &= Q^t GQ + Q^t G\xi TS + \xi S^t T^t GQ + \xi S^t T^t G\xi TS = \\ &= Q^t GQ + \underbrace{\xi Q^t GTS + \xi S^t T^t GQ}_{A} + \underbrace{\xi^2 S^t T^t GTS}_{B} \end{aligned}$$

Observe-se que $S^t = TS$. Como G é simétrica, $(GQ)^t = Q^t G$ e segue :

$$\begin{aligned} A &= \xi Q^t GTS + \xi S^t T^t GQ = \xi GQTS + \xi S^t T^t GQ = \\ &= \xi GQS^t T^t + \xi S^t T^t GQ = 2\xi S^t T^t GQ \end{aligned}$$

De $T^t GT \in K$, segue :

$$B = \xi^2 S^t T^t GTS = \xi^2 T^t GTS^t S$$

Usando as equações (I) e (II), obtemos :

$$\begin{aligned} A+B &= (a\xi^2 + T^t GT\xi^2 - a\xi^2) S^t S - 2\xi S^t \gamma aS = \\ &= (a\xi^2 - a\gamma^2\xi^2) S^t S - 2\xi\gamma a S^t S = a[(1-\gamma^2)\xi^2 - 2\gamma\xi] S^t S \end{aligned}$$

Substituindo $A+B$, obtemos :

$$C_0^t GC_0 = Q^t GQ + a[(1-\gamma^2)\xi^2 - 2\gamma\xi] S^t S$$

Temos que provar que existe $\xi \in K$ tal que $(1-\gamma^2)\xi^2 - 2\gamma\xi = 1$, pois, disto seguirá que $C_0^t GC_0 = Q^t + S^t aS = H$, pela equação (III).

Como car $K \neq 2$, temos :

$$(1-\gamma^2)\xi^2 - 2\gamma\xi = 1 \Longleftrightarrow \xi^2 - \gamma^2\xi^2 - 2\gamma\xi = 1 \Longleftrightarrow \xi^2 - \gamma^2\xi^2 - 2\gamma\xi - 1 = 0 \Longleftrightarrow$$

$$\xi^2 - (\gamma\xi + 1)^2 = 0 \Longleftrightarrow (\xi + \gamma\xi + 1)(\xi - \gamma\xi - 1)$$

Então, sempre existe $\xi \in K$, *car* $K \neq 2$ tal que que resolve a equação acima e :

$$C_0^t GC_0 = Q^t + S^t aS = H \Longrightarrow (det\ C_0)^2 det\ G = det\ H$$

Por H ser não singular, $det\ H \neq 0$ e portanto C_0 é não singular. ■

2.2 Representação de 0 Sobre um Corpo

Teorema 2.2.1 *Se uma forma quadrática não singular representa* 0 *no corpo* K*, com característica diferente de* 2*, então ela representa todos os elementos de* K*.*

Prova : Como formas equivalentes representam os mesmo elementos de K e toda forma é equivalente a uma forma diagonal, é suficiente provarmos para uma forma do tipo $f = a_1x_1^2 + ... + a_nx_n^2$. Seja $a_1\alpha_1^2 + ... + a_n\alpha_n^2 = 0$, com os α_i's não todos nulos. Podemos supor, sem perda de generalidade, que $a_1 \neq 0$(pois, basta aplicar uma transformação do tipo I - teorema 2.1.1 - em algum $\alpha_i \neq 0$). Definindo $x_1 = \alpha_1(1+t)$ e $x_k = \alpha_k(1-t), k = 2, ..., n$ e substituindo em f, obtemos :

$$\begin{aligned} f &= a_1(\alpha_1(1+t))^2 + a_2(\alpha_2(1-t))^2 + ... + a_n(\alpha_n(1-t))^2 = \\ &= a_1\alpha_1^2(1+t)^2 + a_2\alpha_2^2(1-t)^2 + ... + a_n\alpha_n^2(1-t)^2 = \\ &= (a_1\alpha_1^2 + ... + a_n\alpha_n^2) + 2(a_1\alpha_1^2t - ... - a_n\alpha_n^2t) + (a_1\alpha_1^2 + ... + a_n\alpha_n^2)t^2 = \\ &= 2a_1\alpha_1^2t - 2a_2\alpha_2^2t - ... - 2a_n\alpha_n^2t = \\ &= 2a_1\alpha_1^2t - 2t(a_2\alpha_2^2 + ... + a_n\alpha_n^2) = \\ &= 2a_1\alpha_1^2t - 2t(-a_1\alpha_1^2) = \\ &= 4a_1\alpha_1^2t \end{aligned}$$

Desta forma, dado $\gamma \in K$, basta tomarmos $t = \gamma/4a_1\alpha_1^2$ para obtermos $f(t) = \gamma$. Observe-se que por *car* $K \neq 2, a_1 \neq 0$ e $a_1 \neq 0$, podemos dividir por $4a_1\alpha_1^2$. ■

Teorema 2.2.2 *Uma forma quadrática não singular f representa o elemento $\gamma \in K$ se e somente se a forma $-\gamma x_0^2 \oplus f$ representa 0.*

Prova : Se f representa $\gamma \neq 0$, então existem $\alpha_1, ..., \alpha_n \in K$ tais que $f(\alpha_1, ..., \alpha_n) = \gamma$. Desta forma, $(-\gamma x_0^2 \oplus f)(1, \alpha_1, ..., \alpha_n) = -\gamma + \gamma = 0$ e $(-\gamma x_0^2 \oplus f)$ representa 0.

Reciprocamente, consideremos $-\gamma\alpha_0^2 + f(\alpha_1, ...\alpha_n) = 0$, com os α_i's não todos nulos. Se $\alpha_0 \neq 0$, então $\gamma = f(\alpha_1/\alpha_0, ..., \alpha_n/\alpha_0)$. Se $\alpha_0 = 0$, então f representa 0 e, pelo teorema anterior, f representa γ. ■

Se conseguirmos determinar todas as representações de 0 pela forma $-\gamma x_0^2 \oplus f$, com $x_0 \neq 0$, então teremos determinado todas as representações de γ por f. Portanto, a questão de representação de um elemento de K por uma forma não singular pode ser reduzida a questão de representação de zero por uma forma não singular com uma variável a mais.

Teorema 2.2.3 *Se uma forma quadrática não singular f representa zero, então f é equivalente a uma forma do tipo $y_1y_2 + g(y_3, ... y_n)$, onde g é uma forma quadrática.*

Prova : Pelo teorema 2.2.1, existem $\alpha_1, ..., \alpha_n \in K$ tais que $f(\alpha_1, ..., \alpha_n) = 1$. O corolário 2.1.1 garante que $f \sim 1x_1^2 + h(x_2, ..., x_n)$. Desta forma, $x_1^2 + h(x_2, ..., x_n)$ representa zero e, pelo teorema anterior, h representa -1. Sejam $\beta_2, ..., \beta_n$ tais que $h(\beta_2, ..., \beta_n) = -1$. Novamente, pelo corolário, $h \sim -1x_2^2 + g(x_3, ..., x_n)$. Então, $f \sim (x_1^2 - x_2^2) \oplus g(x_3, ..., x_n)$. Definindo $y_1 = x_1 - x_2$ e $y_2 = x_1 + x_2$, temos que $f \sim y_1y_2 \oplus g(y_3, ...y_n)$. ■

2.3 Formas Binárias

Teorema 2.3.1 *Todas as formas quadráticas binárias que representam zero em K são equivalentes.*

Prova : Pelo teorema anterior, toda forma binária que representa zero é equivalente à forma y_1y_2. Pela transitividade de $\sim$, todas as formas binárias que representam zero são equivalentes. ■

Teorema 2.3.2 *Uma forma quadrática binária f, com $det\ f = d \neq 0$, representa 0 em K se e somente se $-d$ é um quadrado em K.*

Prova : Se f representa 0, pelo teorema 2.2.3, temos que $f \sim y_1y_2$. Assim sendo, existe $M \in GL_n(K)$ tal que $[f] = M^t[y_1y_2]M$ e segue :

$$det\ [f] = (det\ M)^2 det\ [y_1y_2] \Longrightarrow d = (det\ M)^2\left(-\frac{1}{4}\right) \Longrightarrow -d = \left(\frac{det\ M}{2}\right)^2$$

Portanto, $-d$ é um quadrado em K.

Reciprocamente, se $g(x,y) = ax^2 + by^2$ e $-d = -ab = \alpha^2$, então :

$$g(\alpha, a) = a\alpha^2 + ba^2 = -a^2b + ba^2 = 0$$

e, portanto, g representa 0. Como todas as formas binárias que representam zero são equivalentes e toda forma f é equivalente a uma diagonal, temos que f representa zero em K. ■

Teorema 2.3.3 *Sejam f, g formas quadráticas binárias não singulares sobre K. Então, $f \sim g$ se e somente se seus determinantes diferirem por um fator que é um quadrado em K e existe $\alpha \in K$, não nulo, que é representado por f e g.*

Prova : Já mostramos que formas equivalentes representam os mesmos elementos e seus determinantes diferem por um elemento que é um quadrado em K.

Para provarmos a recíproca, suponha que exista $\alpha \in K$, não nulo, representado por f e g. O Corolário 2.1.1 implica que f e g são equivalentes às formas $f_1 = \alpha x^2 + \beta y^2$ e $g_1 = \alpha x^2 + \beta' y^2$, respectivamente. Como os determinantes diferem por um fator que é um quadrado em K, temos que $\alpha\beta' = \gamma^2(\alpha\beta)$ para algum $\gamma \in K$. Desta forma, $\beta' = \gamma^2\beta$ e :

$$\begin{pmatrix} 1 & 0 \\ 0 & \gamma \end{pmatrix}\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \gamma \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \gamma\beta \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \gamma \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \gamma^2\beta \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta' \end{pmatrix}$$

Pela transitividade de $\sim$, segue que $f \sim g$. ■

Os determinantes das formas $f(x,y) = x^2 + y^2$ e $g(x,y) = -x^2 - y^2$ diferem por um fator que é um quadrado em $\mathbb{Q}$, mas nenhum elemento não nulo que é representado por uma delas pode ser representado pela outra. Então, pelo teorema acima, f e g não são equivalentes sobre os racionais.

Capítulo 3

Formas Quadráticas p-Ádicas

Uma maneira natural de tentarmos entender melhor a equivalência de formas racionais é estudando essa equivalência nos outros completamentos de $\mathbb{Q}$. O teorema de Ostrowski garante que os únicos completamentos de $\mathbb{Q}$ são os reais os corpos p-ádicos.

Assim, neste capítulo desenvolveremos os resultados relativos a equivalência entre formas quadráticas sobre os números p-ádicos.

3.1 Representação de 0 Sobre os p-Ádicos

Seja f uma forma quadrática, não singular, sobre $\mathbb{Q}_p$. Então, f é equivalente a uma forma diagonal $\alpha_1 x_1^2 + ... + \alpha_n x_n^2$, $\alpha_i \neq 0$, $\forall i$.

Como $\alpha_i = p^{2k_i}u_i$ ou $\alpha_i = p^{2k_i+1}u_i$, fazendo a mudança de variáveis $y_i = p^{k_i}x_i$, teremos uma forma quadrática onde todos os seus coeficientes são divisíveis no máximo pela primeira potência de p. Então toda forma quadrática não singular sobre $\mathbb{Q}_p$ é equivalente a uma forma do tipo :

$$F = F_0 + pF_1 = u_1x_1^2 + ... + u_rx_r^2 + p(u_{r+1}x_{r+1}^2 + ... + u_nx_n^2)$$

onde os u_i's são inteiros p-ádicos invertíveis.

Observe-se que em se tratando da representação de 0, podemos supor que $r \geq n - r$. De fato, se $r < n - r$, definindo a seguinte mudança de variáveis

$$x_1 = y_1, ..., x_r = y_r \ , \ x_{r+1} = \frac{1}{p}y_{r+1}, ..., x_n = \frac{1}{p}y_n$$

obtemos :

$$F = F_0 + pF_1 \Longrightarrow pF = pF_0 + p^2F_1 \Longrightarrow$$

$$pF(y_1, ..., y_n) = p(u_1y_1^2+...+u_ry_r^2)+p^2\left(\frac{1}{p^2}u_{r+1}y_{r+1}^2+...+\frac{1}{p^2}u_n^2y_n^2\right) = pF_0+p^2\frac{1}{p^2}F_1 = F_1+pF_0$$

Então $pF \sim F_1 + pF_0$. Como F e pF representam 0 simultaneamente [1] , podemos tomar a forma $F_1 + pF_0$ ao invés de $F_0 + pF_1$. Logo, $r' := n - r \geq n - r'$ na forma $F_1 + pF_0$

[1] É claro que se F representa 0, então pF representa 0. Reciprocamente, se $pF(a_1, ..., a_n) = 0$, com a_i's não todos nulos, então $F(a_1p, ...a_np) = p^2F(a_1, ..., a_n) = p^20 = 0$.

e ,portanto, podemos supor que $r \geq n - r$.

Teorema 3.1.1 *Seja $p \neq 2$ e $0 < r < n$. A forma*

$$F = F_0 + pF_1 = u_1x_1^2 + ... + u_rx_r^2 + p(u_{r+1}x_{r+1}^2 + ... + u_nx_n^2)$$

com $u_i \in \mathbb{Z}_p^\times$, representa zero em $\mathbb{Q}_p$ se e somente se pelo menos uma das duas formas F_0, F_1 representa zero.

Prova : Suponhamos que f representa zero em $\mathbb{Q}_p$. Então existem $\alpha_1, ..., \alpha_n$, não todos nulos, em $\mathbb{Q}_p$ tais que :

$$u_1\alpha_1^2 + ... + u_r\alpha_r^2 + p(u_{r+1}\alpha_{r+1}^2 + ... + u_n\alpha_n^2) = 0 \quad \text{(I)}$$

Podemos supor que os α's são inteiros p-ádicos e que pelo menos um dos α's não é divisível por p. De fato, se os α's não forem inteiros p-ádicos, podemos multiplicar ambos os lados da equação pelo produto dos quadrados dos denominadores. Assim ficaremos somente com os numeradores. Como pelo menos um dos α's não é nulo, suponhamos $\alpha_i = p^k u$, onde $u \in \mathbb{Z}_p^\times$. Se $k \leq 0$, então α_i não é divisível por p. Se $k > 0$, então considere a mudança de variáveis : $y_j = p^{k_j}x_j$, $j = 1, ..., n$. Como estas formas são equivalentes, a nova forma nas variáveis y_i's representa 0. Desta forma, a potência p^k será cancelada e portanto ficaremos só com $u \in \mathbb{Z}_p^\times$. Logo, sempre podemos supor que $p \nmid \alpha_i$ para algum i.

Se nem todos os $\alpha_1, ..., \alpha_r$ forem divisíveis por p, então existe α_i tal que $p \nmid \alpha_i$. Considerando (I) módulo p, temos :

$$F_0(\alpha_1, ...\alpha_r) \equiv 0 \ (mod\ p) \ e \ \frac{\partial F_0}{\partial x_i}(\alpha_1, ..., \alpha_r) = 2u_i\alpha_i \not\equiv 0 \ (mod\ p)$$

Pelo corolário 0.2.1, F_0 representa 0. Se todos os $\alpha_1, ..., \alpha_r$ forem divisíveis por p, então $u_1\alpha_1^2 + ... + u_r\alpha_r^2 \equiv 0 \ (mod\ p^2)$. Considerando (I) módulo p^2, temos :

$$F(\alpha_1, ...\alpha_r) \equiv pF_1(\alpha_{r+1}, ...\alpha_n) \ (mod\ p^2) \Longrightarrow pF_1(\alpha_{r+1}, ..., \alpha_n) \equiv 0 \ (mod\ p^2) \Longrightarrow$$

$$F_1(\alpha_{r+1}) \equiv 0 \ (mod\ p)$$

onde pelo menos um dos $\alpha_{r+1}, ..., \alpha_n$ não é divisível por p. Aplicando o corolário 0.2.1, a forma F_1 representa 0. Reciprocamente, se F_0 representa 0, então existem $\alpha_1, ..., \alpha_r$ não todos nulos tais que $F_0(\alpha_1, ..., \alpha_r) = 0$. Deste modo :

$$F(\alpha_1, ..., \alpha_r, 0, ..., 0) = F_0(\alpha_1, ..., \alpha_r) + pF_1(0, ..., 0) = 0$$

Se F_1 representa 0, então existem $\beta_{r+1}, ..., \beta_n$ não todo nulos tais que $F_1(\beta_{r+1}, ..., \beta_n) = 0$. Assim :

$$F(0, ..., 0, \beta_{r+1}, ..., \beta_n) = F_0(0, ..., 0) + pF_1(\beta_{r+1}, ..., \beta_n) = 0)$$

Portanto, em ambos os casos, F representa 0. ■

Corolário 3.1.1 *Se $u_1, ..., u_r \in \mathbb{Z}_p^\times$ e $p \neq 2$, então a forma $f = u_1x_1^2 + ... + u_rx_r^2$ representa zero em $\mathbb{Q}$, se e somente se a congruência $f(x_1, ..., x_r) \equiv 0 \ (mod\ p)$ tem solução não trivial em $\mathbb{Z}_p$.*

Prova : Basta supor que $F = F_0 = f$ e aplicar o teorema. ■

Corolário 3.1.2 *Se $u_1, ..., u_r \in \mathbb{Z}_p^\times, p \neq 2$ e $r \geq 3$, então $f(x_1, ..., x_r)$ sempre representa zero em $\mathbb{Q}_p$.*

Prova : Pelo teorema 0.2.1, a congruência $f(x_1, ..., x_n) \equiv 0 \ (mod\ p)$ tem uma solução não trivial. ■

Corolário 3.1.3 *Se $p \neq 2$, então a forma $F = F_0 + pF_1$ representa zero se e somente se a congruência $F \equiv 0 \ (mod\ p^2)$ tem solução em que pelo menos uma das coordenadas não seja divisível por p.*

Prova : Segue diretamente da prova do teorema. ■

Teorema 3.1.2 *A forma $F = F_0 + 2F_1 = u_1x_1^2 + ... + u_rx_r^2 + 2(u_{r+1}x_{r+1}^2 + ... + u_nx_n^2)$ representa 0 em $\mathbb{Q}_2$ se e somente se $F \equiv 0 \ (mod\ 16)$ tem uma solução em que pelo menos uma das variáveis é ímpar (não divisível por 2).*

Prova : Seja a congruência $F(\alpha_1, ..., \alpha_n) \equiv 0 \ (mod\ 16)$, onde nem todos os α_i's são divisíveis por 2. Se $\alpha_i \not\equiv 0 \ (mod\ 2)$ para algum; $i \leq r$, como $F(\alpha_1, ..., \alpha_n) \equiv 0 \ (mod\ 8)$ e $\frac{\partial F}{\partial x_i}(\alpha_1, ..., \alpha_n) = 2u_i\alpha_i \not\equiv 0 \ (mod\ 4)$ (pois, $2 \nmid u_i, \alpha_i$), pelo teorema 0.2.1, temos que F representa 0. Se todos os α_i's forem divisíveis por 2, seja $\alpha_i = 2\eta_i$, $1 \leq i \leq r$, onde $\eta_i \in \mathbb{Z}_2$. Temos :

$$4\sum_{i=1}^{r} u_i\eta_i^2 + 2\sum_{i=r+1}^{n} u_i\alpha_i^2 \equiv 0 \ (mod\ 16) \Longrightarrow 2\sum_{i=1}^{r} u_i\eta_i^2 + \sum_{i=r+1}^{n} u_i\alpha_i^2 \equiv 0 \ (mod\ 8)$$

onde pelo menos um dos $\alpha_{r+1}, ..., \alpha_n$ não é divisível por 2. Digamos, α_j. Então $F_*(\alpha_1, ..., \alpha_n) = F_1(\alpha_{r+1}, ..., \alpha_n) + 2F_0(\alpha_1, ..., \alpha_r) \equiv 0 \ (mod\ 8)$ e $\frac{\partial F_*}{\partial x_i}(\alpha_1, ..., \alpha_n) = 2u_j\alpha_j \not\equiv 0 \ (mod\ 4)$. Pelo teorema anterior, temos que $F_1 + 2F_0$ representa 0. Como $2F \sim F_1 + 2F_0$ e $2F$ e F representam 0 simultaneamente, temos que F representa 0.

Se F representa 0 em $\mathbb{Z}_2$, então existem $\alpha_1, ..., \alpha_n \in \mathbb{Z}_2$, não todos nulos, tais que $F(\alpha_1, ..., \alpha_n) = 0$. Assim, $F(\alpha_1, ..., \alpha_n) = 0 \equiv 0 \ (mod\ 16)$ e portanto a congruência $F \equiv 0 \ (mod\ 16)$ admite solução, não trivial, onde pelo menos um dos α_i's não é divisível por 2. ■

Corolário 3.1.4 *Se $F = F_0 + 2F_1 \equiv 0 \ (mod\ 8)$ tem solução em que no mínimo uma das variáveis $x_1, ..., x_r$ assume um valor ímpar, então F representa 0 em $\mathbb{Q}_2$.*

Prova : Se $F \equiv 0 \ (mod\ 8)$, então $2F \equiv 0 \ (mod\ 16)$. A hipótese implica que $2F \equiv 0 \ (mod\ 16)$ admite uma solução em que no mínimo uma das variáveis $x_1, ..., x_r$ assuma uma valor ímpar. Como $2F \sim F_1 + 2F_0$, pelo teorema anterior, segue que $2F$ representa 0 em $\mathbb{Q}_2$ e portanto F representa 0 em $\mathbb{Q}_2$. ■

3.2 Formas Binárias p-Ádicas

As formas quadráticas binárias p-ádicas constituem um importante caso especial da teoria geral das formas quadráticas n-árias p-ádicas.

Sabemos que toda forma quadrática binária não singular é equivalente a uma forma diagonal do tipo $ax^2 + by^2$, com $a, b \in \mathbb{Q}_p^*$. Observe-se que :

$$ax^2 + by^2 = a\left(x^2 + \frac{b}{a}u^2\right) = a(x^2 - \alpha y^2)$$

Portanto toda forma quadrática binária pode ser posta na forma $x^2 - \alpha y^2$, com $\alpha \in \mathbb{Q}_p^*$. Este fato motiva o estudo das formas $x^2 - \alpha y^2$.

Definição 3.2.1 *Para cada $\alpha \in \mathbb{Q}_p^*$, definimos*

$$H_\alpha = \{\gamma \in \mathbb{Q}_p^* : \exists x_0, y_0 \in \mathbb{Q}_p / x_0^2 - \alpha y_0^2 = \gamma\},$$

ou seja, H_α é o conjunto de todos os elementos não nulos de $\mathbb{Q}_p$ que são representados por $x^2 - \alpha y^2$.

Lema 3.2.1 *H_α munido da multiplicação usual de $\mathbb{Q}_p^*$ é um grupo multiplicativo.*

Prova : i) Sejam $\gamma = x^2 - \alpha y^2$, $\delta = z^2 - \alpha t^2$.

$$\begin{aligned} \gamma\delta &= (x^2 - \alpha y^2)(z^2 - \alpha t^2) = x^2z^2 - \alpha x^2t^2 - \alpha y^2z^2 + \alpha^2y^2t^2 \\ &= (x^2z^2 + 2xz\alpha yt + \alpha^2y^2t^2) - \alpha(x^2t^2 + 2xt\alpha yz + y^2z^2) \\ &= (xz + \alpha yt)^2 - \alpha(xt + yz)^2 \in H_\alpha \end{aligned}$$

ii) Seja $\gamma \in H_\alpha$ e considere $\gamma^{-1} = \left(\frac{x}{\gamma}\right)^2 - \alpha\left(\frac{y}{\gamma}\right)^2$.

$$\gamma\gamma^{-1} = \gamma\left(\frac{x}{\gamma}\right)^2 - \alpha\left(\frac{y}{\gamma}\right)^2 = \frac{x^2 - \alpha y^2}{\gamma} = \frac{\gamma}{\gamma} = 1$$

Como $1 \in H_\alpha$, pois $1 = 1^2 - \alpha 0^2$ e as demais propriedades são fáceis de serem verificas, acabamos a prova. ■

Observe-se que se $\alpha \in (\mathbb{Q}_p^*)^2$, então $x = \eta, y = 1$, onde $\alpha = \eta^2$ é solução de $x^2 - \alpha y^2 = 0$ e portanto $x^2 - \alpha y^2$ representa 0. Assim, $x^2 - \alpha y^2$ representa todos os elementos de $\mathbb{Q}_p$ e, neste caso, os grupos multiplicativos $(H_\alpha, .)$ e $(\mathbb{Q}_p^*)$ coincidem.

Note-se que a equação $x^2 - \alpha y^2 = \eta^2$ admite sempre a solução $x = \eta, y = 0$. Desta forma, $x^2 - \alpha y^2$ representa todos os quadrados de $\mathbb{Q}_p$, ou seja, $(\mathbb{Q}_p^*)^2 \subset H_\alpha$. Como $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2]$ é finito, $[\mathbb{Q}_p^* : H_\alpha]$ é finito. Se α não é um quadrado, então $x^2 - \alpha y^2$ representa 0 e, portanto, essa forma representa todos os elementos de $\mathbb{Q}_p^*$. Assim, $H_\alpha = \mathbb{Q}_p^*$ e $[\mathbb{Q}_p^* : H_\alpha] = 1$.

Antes de estudarmos o caso em que α não é um quadrado em $\mathbb{Q}_p$, faremos o seguinte resultado :

Lema 3.2.2 *A forma $x^2 - \alpha y^2$ representa um p-ádico $\beta \neq 0$ em $\mathbb{Q}_p$ se e somente se a forma $\alpha x^2 + \beta y^2 - z^2$ representa 0 em $\mathbb{Q}_p$.*

Prova : Se $x^2 - \alpha y^2$ representa um p-ádico $\beta \neq 0$ em $\mathbb{Q}_p$, pelo teorema 2.2.2, $-\beta z^2 + x^2 - \alpha y^2$ representa 0 e, portanto, $\alpha y^2 + \beta z^2 - x^2$ representa 0. Reciprocamente, se $\alpha x^2 + \beta y^2 - z^2 = -(-\beta y^2 + (z^2 - \alpha x^2))$ representa 0 em $\mathbb{Q}_p$, novamente pelo teorema 2.2.2, temos que $z^2 - \alpha x^2$ representa β. ■

Teorema 3.2.1 *Se $\alpha \notin (\mathbb{Q}_p^*)^2$, então $[\mathbb{Q}_p^* : H_\alpha] = 2$.*

Prova : Como $\eta^2\alpha x^2 + \theta^2\beta y^2 - z^2 \sim \alpha z^2 + \beta t^2 - u^2$, pela mudança de variáveis $z = \eta x, t = \theta y, u = z$, então a representação de 0 por esta forma não é alterada quando multiplicamos α e β por quadrados em $\mathbb{Q}_p$. Assim, podemos supor que α e β são representantes de algum sistema fixado de classes laterais de $(\mathbb{Q}_p^*)^2$ em $\mathbb{Q}_p^*$.

Caso $p \neq 2$

Se $-\alpha \notin (\mathbb{Q}_p^*)^2$, como $-\alpha \in H_\alpha$, temos que $(\mathbb{Q}_p^*)^2 \neq H_\alpha$. Se $-\alpha \in (\mathbb{Q}_p^*)^2$, definindo $z = x, t = \eta y$, onde $\eta^2 = -\alpha$, temos que $x^2 - \alpha y^2 \sim z^2 + t^2$. Como $x^2 + y^2 \equiv 0 \ (mod\ p)$ admite a solução não trivial $x = p, y = 0$, pelo corolário 3.1.1, segue que $x^2 + y^2$ representa 0. Então $x^2 + y^2$ representa qualquer elemento de $\mathbb{Q}_p$. Além disso, $x^2 - \alpha y^2 \sim z^2 + t^2$ e portanto $x^2 - \alpha y^2$ representa qualquer elemento de $\mathbb{Q}_p$, ou seja, $H_\alpha \neq (\mathbb{Q}_p^*)^2$. Veja ainda que se $u \in \mathbb{Z}_p^*$ não é um quadrado, podemos assumir que α é u, p, pu. Considerando a forma $\alpha x^2 + \beta y^2 - z^2$ na decomposição $F_0 + pF_1$, obtemos os seguintes casos : $(1)\alpha = u$ e $\beta = p$, $(2)\alpha = p$ e $\beta = u$ e $(3)\alpha = pu$ e $\beta = u$. Considerando $\alpha = u$ e $\beta = p$, temos :

$$ux^2 + py^2 - z^2 = ux^2 - z^2 + py^2 = F_0 + pF_1$$

Como $-det\ F_0 = -u$ não é um quadrado, pelo teorema 2.3.2 temos que F_0 não representa 0. Segue do teorema 3.1.1 que $F_o + pF_1$ não representa 0. De modo análogo, pode-se provar o mesmo resultado para os casos restantes. Então $\alpha x^2 + \beta y^2 - z^2$ não representa 0. Pelo lema anterior, $x^2 - \alpha y^2$ não representa β e portanto $H_\alpha \neq \mathbb{Q}_p^*$. Como $(\mathbb{Q}_p^*)^2 \subset H_\alpha \subset \mathbb{Q}_p^*$ e $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2] = 4$, temos que $[H_\alpha : (\mathbb{Q}_p^*)^2]$ divide 4. Mas, observe que :

$$(\mathbb{Q}_p^*)^2 \neq H_\alpha \neq \mathbb{Q}_p^* \Longrightarrow [H_\alpha : (\mathbb{Q}_p^*)^2], [\mathbb{Q}_p^* : H_\alpha] \neq 1$$

Logo $[\mathbb{Q}_p^* : H_\alpha] = 2$.

Caso II - p=2

Então $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2] = 8$ e 1,3,5,7,2.1,2.3,2.5,2.7 são os representantes para as 8 classes laterais. Desta forma, consideraremos $\alpha x^2 + \beta y^2 - z^2$, com α e β sendo qualquer um destes representantes. Na tabela abaixo, utilizamos "." para indicar as formas que representam zero em $\mathbb{Q}$. [SHA]

$\alpha \mid \beta$	1	3	5	7	2.1	2.3	2.5	2.7
1	.	.	.	.	.	.	.	.
3	.		.			.		.
5	.	.	.	.				
7	.		.		.		.	
2.1	.			.	.			.
2.3	.	.					.	.
2.5	.			.		.	.	
2.7	.	.			.	.		

Vemos que, com exceção da linha 1, cada linha possui "."em exatamente 4 posições. Isso quer dizer que para cada $\alpha \in (\mathbb{Q}_p^*)^2$, a forma $x^2 - \alpha y^2$ representa 4 classes dos subgrupos de $(\mathbb{Q}_p^*)^2$ e portanto $[H_\alpha : (\mathbb{Q}_p^*)^2] = 4$. Como $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2] = 8$, temos que $[\mathbb{Q}_p^* : H_\alpha] = 2$.

Para verificarmos a tabela, vamos dividir em casos :

I) $\alpha = 2\varepsilon, \beta = 2\eta$, com $\varepsilon, \eta \in \mathbb{Z}_2^\times$

Ao invés de considerarmos as soluções de $2\varepsilon x^2 + 2\eta y^2 - z^2 = 0$ em $\mathbb{Q}$, podemos supor que elas são inteiras, não todas divisíveis por 2. Para tanto, basta multiplicar pelo mmc dos denominadores e dividir por 2 até que uma das variáveis não seja mais múltipla de 2.

Veja que necessariamente devemos ter $z \equiv 0 \ (mod\ 2)$ e $x, y \not\equiv 0 \ (mod\ 2)$. Considerando $z = 2t$, temos :

$$2\varepsilon x^2 + 2\eta y^2 - 4t^2 = 0 \iff \varepsilon x^2 + \eta y^2 - 2t^2 = 0 \implies \varepsilon x^2 + \eta y^2 - 2t^2 \equiv 0 \ (mod\ 8)$$

Reciprocamente, se $\varepsilon x^2 + \eta y^2 - 2t^2 \equiv 0 \ (mod\ 8)$ admite solução, onde x, y são ímpares, então pelo corolário 3.1.4, temos que $\varepsilon x^2 + \eta y^2 - 2t^2$ representa 0. Assim, provamos que $\varepsilon x^2 + \eta y^2 - 2t^2$ representa 0 se e somente se $\varepsilon x^2 + \eta y^2 - 2t^2 \equiv 0 \ (mod\ 8)$ admite solução, onde x, y são ímpares.

Como $x^2, y^2 \equiv 1 \ (mod\ 8), 2t^2 \equiv 2 \ (mod\ 8)$ ou $2t^2 \equiv 0 \ (mod\ 8)$, temos que $2\varepsilon x^2 + 2\eta y^2 - z^2$ representa 0 se e somente se $\varepsilon + \eta \equiv 2 \ (mod\ 8)$ ou $\varepsilon + \eta \equiv 0 \ (mod\ 8)$. De fato, se $2\varepsilon x^2 + 2\eta y^2 - z^2$ representa 0, então $\varepsilon x^2 + \eta y^2 - 2t^2 \equiv 0 \ (mod\ 8)$ admite solução, onde x e y são ímpares. Assim, $\varepsilon + \eta \equiv 2 \ (mod\ 8)$ ou $\varepsilon + \eta \equiv 0 \ (mod\ 8)$. A recíproca não é difícil de se verificar.

II) $\alpha = 2\varepsilon, \beta = \eta$

Assumindo $2\varepsilon x^2 + \eta y^2 - z^2 = 0$, com x, y, z são não todos divisíveis por 2, temos, pela mesma razão usada no caso I, que $y, z \not\equiv 0 \ (mod\ 2)$. Pelo corolário 3.1.4, essa equação será satisfeita se e somente se uma das congruências a seguir for satisfeita :

$$2\varepsilon + \eta \equiv 1 \ (mod\ 8) \ , \ \eta \equiv 1 \ (mod\ 8)$$

Estas correspondem aos casos $2 \nmid x$ e $2 \mid x$, respectivamente.

III) $\alpha = \varepsilon, \beta = \eta$

Se na equação $\varepsilon x^2 + \eta y^2 - z^2 = 0$ os inteiros p-ádicos x, y e z são não todos divisíveis por 2, então um deles necessariamente é divisível por 2 e os outros dois restantes não o

são.

Se $z \equiv 0 \ (mod\ 2)$, então :

$$z^2 \equiv 0 \ (mod\ 4) \Longrightarrow \varepsilon x^2 + \eta y^2 \equiv 0 \ (mod\ 4) \ (*)$$

Como $x^2, y^2 \equiv 1 \ (mod\ 4)$, temos que $\varepsilon x^2 + \eta y^2 \equiv \varepsilon + \eta \ (mod\ 4)$ $(**)$, pois $\varepsilon x^2 \equiv \varepsilon \ (mod\ 4)$ e $\eta y^2 \equiv \eta \ (mod\ 4)$. Por $(*)$ e (II), $\varepsilon + \eta \equiv 0 \ (mod\ 4)$ e portanto :

$$\varepsilon \equiv 1 \ (mod\ 4) \ ou \ \eta \equiv 1 \ (mod\ 4)$$

Se $z \not\equiv 0 \ (mod\ 2)$, então :

$$z \equiv 1 \ (mod\ 2) \Longrightarrow z^2 \equiv 1 \ (mod\ 4) \Longrightarrow \varepsilon x^2 + \eta y^2 \equiv 1 \ (mod\ 4)$$

e somente umas das variáveis x ou y é divisível por 2. Se $2 \mid x$, então $\varepsilon x^2 \equiv 0 \ (mod\ 4)$ e $\eta y^2 \equiv \eta \ (mod\ 4)$ e portanto $\varepsilon x^2 + \eta y^2 \equiv \eta \ (mod\ 4)$. Como $\varepsilon x^2 + \eta y^2 \equiv 1 \ (mod\ 4)$, $\eta \equiv 1 \ (mod\ 4)$. Analogamente, se $2 \mid y$, então $\varepsilon \equiv 1 \ (mod 4)$.

Reciprocamente, assumamos que $\varepsilon \equiv 1 \ (mod\ 4)$. Se $\varepsilon \equiv 1 \ (mod\ 8)$, tomando $x = 1, y = 0, z = 1$ temos $\varepsilon x^2 + \eta y^2 - z^2 \equiv 0 \ (mod\ 8)$. Se $\varepsilon \equiv 5 \ (mod\ 8)$, tomando $x = 1, y = 2, z = 1$ temos o mesmo resultado anterior.

Assim, em ambos os casos, $\varepsilon x^2 + \eta y^2 - z^2$ representa 0. ■

Uma consequência imediata do teorema acima é o :

Corolário 3.2.1 *Se $\alpha \neq 0$ não é um quadrado em $\mathbb{Q}_p$, então $\mathbb{Q}_p^*/H_\alpha$ é um subgrupo cíclico de ordem 2.*

Definamos o seguinte isomorfismo :

$$\phi : \mathbb{Q}_p^*/H_\alpha \longrightarrow \{+1, -1\} \ , \ \phi(\beta H_\alpha) = -1 \ e \ \phi(H_\alpha) = +1$$

onde $\beta \notin H_\alpha$. Então existe um homomorfismo sobrejetor de $\varphi_\alpha : \mathbb{Q}_p^* \to \{+1, -1\}$, com núcleo H_α e definida por $\varphi_\alpha = \phi \circ \pi$, onde π é a projeção canônica ao quociente. Em termos de diagrama comutativo :

$$\begin{array}{ccc} & \overset{\varphi_\alpha}{} & \\ \mathbb{Q}_p^* & \longrightarrow & \{+1, -1\} \\ \pi \downarrow & \nearrow \phi & \\ \mathbb{Q}_p^*/H_\alpha & & \end{array}$$

Tal homomorfismo sobrejetor é dado por :

$$\varphi_\alpha(\beta) := \begin{cases} +1, & \text{se } \beta \in H_\alpha \\ -1, & \text{caso contrário} \end{cases}$$

Pelo lema 3.2.2, temos: $\beta \in H_\alpha \iff \beta$ é representado por $x^2 - \alpha y^2 \iff$ a forma $\alpha x^2 + \beta y^2 - z^2$ representa 0 em $\mathbb{Q}_p$. Assim, podemos definir o Símbolo de Hilbert.

3.3 O Símbolo de Hilbert e a Equivalência p-Ádica

Definição 3.3.1 *Para quaisquer p-ádicos não nulos α e β, definimos o* ***Símbolo de Hilbert*** (α, β) *por :*

$$(\alpha, \beta) = \begin{cases} +1, & \text{se } \alpha x^2 + \beta y^2 - z^2 \text{ representar 0 em } \mathbb{Q}_p \\ -1, & \text{caso contrário} \end{cases}$$

Se α é um quadrado em $\mathbb{Q}_p$, então $(\alpha, \beta) = 1$. Se α não é um quadrado, então $(\alpha, \beta) = 1$ se e somente se $\beta \in H_\alpha$.

Note-se que pelo lema 3.2.2 e pela observação feita no final da última seção, o Símbolo de Hilbert está bem definido.

Proposição 3.3.1 *Sejam α, β e η p-ádicos não nulos. Então :*

1. $(\alpha, \beta\eta) = (\alpha, \beta)(\alpha, \eta)$
2. $(\alpha, \beta) = (\beta, \alpha)$
3. $(\alpha\eta, \beta) = (\alpha, \beta)(\eta, \beta)$
4. $(\alpha, -\alpha) = 1$
5. $(\alpha, \alpha) = (\alpha, -1)$

Prova : O item 1) segue diretamente da construção feita do Símbolo de Hilbert. O item 2) é verificado observando que a solução de $\alpha x^2 + \beta y^2 - z^2 = 0$ é simétrica em α e β. O item 3) é conseqüência dos itens anteriores. Para verificarmos o item 4), basta tomarmos $x = y = 1$ e $z = 0$. Resta somente verificarmos o item 5).

$$(\alpha, -\alpha) = 1 \Longrightarrow (\alpha, -1\alpha) = 1 \Longrightarrow (\alpha, -1)(\alpha, \alpha) = 1 \Longrightarrow (\alpha, -1) = (\alpha, \alpha)$$

E isso encerra a prova. ■

Considere $\alpha = p^k\epsilon$ e $\beta = p^l\eta$, com ϵ, η inteiros p-ádicos invertíveis. Calculemos (α, β) :

$$\begin{aligned} (\alpha, \beta) &= (p^k\epsilon, p^l\eta) = (p^k, p^l)(\epsilon, p^l)(p^k, \eta)(\epsilon, \eta) = \\ &= (p, p)^{kl}(\epsilon, p)^l(p, \eta)^k(\epsilon, \eta) = (p, \epsilon^l\eta^k(-1)^{kl})(\epsilon, \eta) \end{aligned}$$

Desta forma, o cálculo de (α, β) fica reduzido ao cálculo de (ϵ, η) e (p, ϵ).

Teorema 3.3.1 *Sejam p um primo, ϵ e η inteiros p-ádicos invertíveis. Então :*

$$(p, \epsilon) = \left(\frac{\epsilon}{p}\right) \ , \ (\epsilon, \eta) = 1 \ , \ p \neq 2$$

$$(2, \epsilon) = (-1)^{(\epsilon^2-1)/8} \ , \ (\epsilon, \eta) = (-1)^{[(\epsilon-1)/2][(\eta-1)/2]} \ , \ p = 2$$

Prova : Caso I - $p \neq 2$

Pelo teorema 3.1.1, $px^2 + \epsilon y^2 - z^2$ representa 0 se e somente se $\epsilon y^2 - z^2$ representa 0 se e somente se ϵ é um quadrado em $\mathbb{Q}_p$. Assim,

$$(p, \epsilon) = \left(\frac{\epsilon}{p}\right)$$

Pelo corolário 3.1.2, temos que $\epsilon x^2 + \eta y^2 - z^2$ sempre representa 0. Então,

$$(\epsilon, \eta) = +1 \qquad \forall \epsilon, \eta \in \mathbb{Z}_p^{\times}$$

Caso II - $p = 2$

Os valores dos símbolos $(2, \varepsilon)$, (ε, η) já foram calculados, essencialmente, no teorema 3.2.1. Tomando $\varepsilon = 1$ em $2\varepsilon + \eta \equiv 1 \ (mod\ 8)$, temos que $2x^2 + \eta y^2 - z^2$ representa 0 se e somente se $\eta \equiv 1 \ (mod\ 8)$ ou $\eta \equiv -1 \ (mod\ 8)$, ou seja, $\eta^2 \equiv 1 \ (mod\ 8)$. Assim,

$$(2, \eta) = (-1)^{(\eta^2-1)/2}$$

Além disso, $\varepsilon x^2 + \eta y^2 - z^2$ representa 0 se e somente se $\varepsilon \equiv 1 \ (mod\ 4)$ ou $\eta \equiv 1 \ (mod\ 4)$. Logo,

$$(\varepsilon, \eta) = (-1)^{[(\varepsilon-1)/2][(\eta-1)/2]}$$

Com isso, terminamos a prova. ■

Vale observar que, pelo teoreoma 3.2.1, podemos assumir que $\varepsilon, \eta \in \{1, 3, 5, 7\}$.

O Símbolo de Hilbert é um conceito muito útil para estudarmos a questão da equivalência p-ádica e, conseqüentemente, para a equivalência racional.

Teorema 3.3.2 *Se f é uma forma quadrática binária não singular, então $(\alpha, -det\ f) = (\alpha', -det\ f)$ para todos $\alpha, \alpha' \in \mathbb{Q}_p^*$ representados por f.*

Prova : Sejam $\alpha, \alpha' \in \mathbb{Q}_p$ representados por f. Pelo corolário 2.1.1, f é equivalente a $\alpha x^2 + \beta y^2$. Como α' é representado por f, temos $\alpha' = \alpha x_0^2 + \beta y_0^2$ para alguns x_0, y_0 e, portanto, $\alpha\alpha' + \alpha\beta y_0^2 - (\alpha x_0)^2 = 0$. Assim, a forma $\alpha\alpha' x^2 + \alpha\beta y^2 - z^2$ representa 0 e $(\alpha\alpha', -det\ f) = +1$. Logo $(\alpha, -det\ f) = (\alpha', -det\ f)$. ■

Teorema 3.3.3 *Duas formas quadráticas binárias não singulares p-ádicas, f e g, são equivalentes sobre $\mathbb{Q}_p$ se e somente se as seguintes condições forem satisfeitas :*

1. *$det\ f = \gamma^2 . det\ g$, para algum $\gamma \in \mathbb{Q}_p^*$.*

2. *$(\alpha, -det\ f) = (\alpha, -det\ g)$, para algum $\alpha \neq 0$ representado por f e g.*

Prova : A necessidade dessas duas condições já foi feita, essencialmente, anteriormente.

Para a suficiência, considere γ representado por g e $f = \alpha x^2 + \beta y^2$.

$$(\alpha, -\alpha\beta) = (\alpha, -det\ f) = (\alpha, -det\ g) = (\gamma, -det\ g) = (\gamma, -\alpha\beta) \Longrightarrow$$

$$\Longrightarrow (\alpha, -\alpha\beta)(\gamma, -\alpha\beta) = 1$$

Veja que $(\alpha, -\alpha\beta) = (\alpha^{-1}, -\alpha\beta)$, pois :

$$(1, -\alpha\beta) \Longrightarrow (\alpha\alpha^{-1}, -\alpha\beta) = 1 \Longrightarrow (\alpha, -\alpha\beta)(\alpha^{-1}, -\alpha\beta) = 1$$

Então $(\alpha^{-1}, -\alpha\beta)(\gamma, -\alpha\beta) = 1$ e, portanto, $(\gamma\alpha^{-1}, -\alpha\beta) = 1$. Assim, $\gamma\alpha^{-1}x^2 - \alpha\beta y^2 - z^2 = 0$ tem solução não trivial.

Suponhamos, sem perda de generalidade, que na solução (x_0, y_0, z_0), tenhamos $x_0 \neq 0$. Desta forma,

$$\gamma = \alpha\Big(\frac{z_0}{x_0}\Big)^2 + \beta\Big(\frac{\alpha y_0}{x_0}\Big)^2$$

ou seja, γ é representado por f. Pelo teorema 2.3.3, temos que $f \sim g$. ■

Exemplo : As formas $f(x, y) = x^2 + 2xy + 5y^2$ e $g(x, y) = x^2 + 2xy + 17y^2$ são equivalentes sobre $\mathbb{Q}_3$. Os determinantes diferem por um fator 4 e, como $4 \equiv 1^2 \ (mod\ 3)$, temos que 4 é um quadrado em $\mathbb{Q}$. Além disso, $\alpha = 1$ é representado por ambas as formas e, $1x^2 - 4y^2 - z^2$ e $1x^2 - 16y^2 - z^2$ representam 0. Assim, temos que $(1, -4) = 1 = (1, -16)$.

Neste momento estamos prontos para demonstrar o :

3.4 O Teorema de Hasse-Minkowski e a Equivalência Racional

Teorema 3.4.1 ***(Hasse-Minkowski)*** *Uma forma quadrática binária racional, não singular, representa 0 em $\mathbb{Q}$ se e somente se ela representa 0 em $\mathbb{R}$ e $\mathbb{Q}_p$ para todo primo p.*

Prova : A necessidade da representação de 0 em $\mathbb{R}$ e $\mathbb{Q}_p$ para todo primo p segue diretamente da definição.

Seja f uma forma que representa 0 em $\mathbb{R}$. Pelo teorema 2.3.2, $-d \in \mathbb{Q}$ é um quadrado em $\mathbb{R}$ e portanto $-d > 0$. Então $-d = p_1^{n_1} ... p_k^{n_k}$, onde os p_i's são primos distintos e os n_i's são inteiros. Como f também representa 0 em todos os $\mathbb{Q}_{p_i}$'s, então $-d$ é um quadrado nestes corpos. Assim, todos os n_i's devem ser pares e portanto $-d$ é um quadrado em $\mathbb{Q}$. Novamente, pelo teorema 2.3.2, temos que f representa 0 em $\mathbb{Q}$. ■

Corolário 3.4.1 *Uma forma quadrática binária racional, não singular, representa $a \in \mathbb{Q}$ se e somente se representa a em $\mathbb{R}$ e $\mathbb{Q}_p$ para todo o primo p.*

Prova : Segue diretamente dos teoremas 2.2.2 e Hasse-Minkowski para formas 3-árias. [SHA] ■

Usaremos o Teorema de Hasse-Minkowski na questão da equivalência racional.

Teorema 3.4.2 *Duas formas quadráticas binárias racionais, não singulares, são equivalentes em $\mathbb{Q}$ se e somente se forem equivalentes em $\mathbb{R}$ e $\mathbb{Q}_p$ para todo primo p.*

Prova : É fácil ver que formas equivalentes sobre os racionais também são equivalentes sobre os reais e os p-ádicos.

Para a recíproca, primeiramente vamos provar para formas do tipo bx^2 e $b'x^2$. Estas formas serão equivalentes sobre um corpo somente se b/b' for um quadrado neste corpo. Como essas formas são equivalentes sobre os reais e todos os p-ádicos, b/b' é um quadrado em todos esses corpos. Assim como fizemos na demonstração do Teorema de Hasse-Minkowski, b/b' é um quadrado em $\mathbb{Q}$. Portanto, as formas bx^2 e $b'x^2$ são equivalentes sobre os racionais.

Suponhamos agora, que f e g são formas binárias e consideremos um número racional $a \neq 0$ representado por f em $\mathbb{Q}$. Pelo corolário de Hasse-Minkowski, f representa a nos reais e em todos os p-ádicos. Como $f \sim g$ sobre os reais e todos os p-ádicos, temos que g representa a nos reais e em todos os p-ádicos. Novamente, pelo corolário de Hasse-Minkowski, temos que g representa a nos racionais. Aplicando o corolário 2.1.1, obtemos as seguintes equivalências sobre os racionais :

$$f \sim ax^2 + by^2 \ , \ g \sim ax^2 + b'y^2$$

Como $f \sim g$ sobre os reais e todos os p-ádicos, pelo Teorema do Cancelamento de Witt, $by^2 \sim b'y^2$ sobre os reais e todos os p-ádicos. Usando o que fizemos no começo da prova, temos que as formas by^2 e $b'y^2$ são equivalentes sobre $\mathbb{Q}$. Assim, $ax^2 + by^2 \sim ax^2 + b'y^2$ sobre os racionais e, conseqüentemente, $f \sim g$ sobre os racionais. ■

O Teorema de Hasse-Minkowski e o teorema acima podem ser generalizados para formas quadráticas n-árias racionais. Isso pode ser feito usando-se os resultados feitos, juntamente com mais alguns conceitos não abordados neste texto. Veja, por exemplo, [CAS] ou [SHA].

Bibliografia

- [CAS] - Cassels, J.W.S. *"Rational Quadratic Forms"*, Academic Press Inc., 1978.
- [CON] - Conway, J. e Sloane, N. *"Sphere Packings, Lattices and Groups"*, Springer Verlag, 1988.
- [EDW] - Edwards, H.M. *"Fermat's Last Theorem - A Genetic Introduction to Number Algebraic Number Theory"*, Springer Verlag, 1977.
- [FLA] - Flath, D.E. *"Introduction to Number Theory"*, A Wiley-Interscience Publication, 1988.
- [GAU] - Gauss, K.F. *"Disquisitiones Arithmeticae"*, Springer Verlag, 1986.
- [GOU] - Gouvêa F.Q. *"Primeiros Passos p-Ádicos"*, 17º Colóquio Brasileiro de Matemática IMPA, 1989.
- [JON] - Jones, B.W. *"The Arithmetic Theory of Quadratic Forms"*, The Mathematical Association of America, 1961.
- [MAT] - Matheus, G.B. *"Theory of Numbers"*, Chelsea Publishing Company.
- [SAN] - Santos, J.P.O. *"Introdução à Teoria dos Números"*, Coleção Matemática Universitária - IMPA, 2003.
- [SHA] - Shafarevich, I.R. and Borevich Z.I. *"Number Theory"*, Academic Press Inc., 1966.

Índice Remissivo