CONSTRUÇÃO DE FORMAS QUADRÁTICAS A COEFICIENTES INTEIROS, UNIMODULARES, POSITIVAS DEFINIDAS EM DIMENSÕES MENORES OU IGUAIS A 16

WALTER ALEXANDRE CARNIELLI Jo.

Orientador

Prof. Dr. NELO DA SILVA ALLAN

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciencia da Computação da Universidade Estadual de Campinas como requisito parcial para obtenção do título de Mestre em Matemática.

Este trabalho foi realizado com suporte financeiro da Fundação de Amparo à Pesquisa do Estado de São Paulo - FAPESP.

Maio - 1978

CONSTRUÇÃO DE FORMAS QUADRÁTICAS A COEFICIENTES INTEIROS, UNIMODULARES, POSITIVAS DEFINIDAS EM DIMENSÕES MENORES OU IGUAIS A 16

ERRATA

Página	linha	onde se lê	leia-se
10	10	$\frac{1}{n}Z = \left\{\frac{m}{n} : m \in Z, n \in Z\right\}$	$\frac{m}{n}Z = \left\{\frac{m}{n}p, m \in Z, n \in Z, p \in Z\right\}$
12	19	Z_{x_1} +....	Zx_1 +...
20	22	•	□
22	15	sobre V	sobre V_p
22	19	$\Psi_p = V_p \subset \mathbb{Q}_p L_p$	$V\Psi_p = V_p \subset \mathbb{Q}_p L_p$
23	2	J_p	J(p)
23	3	K=J(p)	K_p=J(p)
35	5	Z	2Z
62	6	Z_x	Zx
63	5	comprimento	complemento
64	23	$i \leq n \leq 7$	$1 \leq n \leq 7$

À VERA que soube e sabe esperar.

CONSTRUÇÃO DE FORMAS QUADRÁTICAS A COEFICIENTES INTEIROS, UNIMODULARES, POSITIVAS DEFINIDAS EM DIMENSÕES MENORES OU IGUAIS A 16

INTRODUÇÃO

O problema da representação, nascido a partir das tentativas de solução das equações diofantinas, pode ser interpretado da sequinte maneira: dada uma forma quadrática, isto é, uma função polinomial quadrática homogênea, da forma $Q(x_1,\ldots,x_n) = \Sigma\, a_{ij}\, x_i\, x_j$ $a_{ij} = a_{ji} \in Z$ $i,j = 1,\ldots,n$, e dado $a \in Z$, em que condições existe uma n-upla $(x_1,\ldots,x_n)$ de inteiros tal que $Q(x_1,\ldots,x_n) = a$?

Uma generalização natural para este problema é: dadas formas quadráticas $Q(x_1,\ldots,x_n)$ e $Q'(y_1,\ldots,y_n)$ existem inteiros b_{ij} tais que $x_i = \sum_{i=1}^{n} b_{ij}\, y_j$ e $Q(x) = Q'(y)$? Em termos de matrizes, se denotarmos por A a matriz de Q e por A' a matriz de Q' (onde $A=(a_{ij})$, se $Q(x_1,\ldots,x_n) = \Sigma\, a_{ij}\, x_i x_j$, $a_{ij} = a_{ji}$, $i,j = 1,\ldots,n$) e $B=(b_{ij})$ a igualdade será possível se $A' = B^t AB$, e nesse caso diremos que as matrizes A *e* A' *são integralmente equivalentes*. Se a matriz B tiver coeficientes racionais, diremos que nesse caso A *e* A' *são equivalentes sobre* Q. Por *espaço quadrático* entenderemos um espaço vetorial V munido de uma forma quadrática Q . Podemos sempre construir um espaço quadrático a partir de uma forma quadrática. Se V for um espaço quadrático sobre os racionais, o problema de equivalência se transformará no problema de isomorfismo entre espaços quadráticos.

Uma das maneiras de se estudar espaços quadráticos (V,Q) é estudar o grupo ortogonal O(V), o grupo dos endomorfismos de V que preservam a forma quadrática, isto é, $Q(\rho_x) = Q(x)$, onde ρ é um

endomorfismo de V.

No capítulo I estudaremos os espaços quadráticos sobre corpos, em particular para o corpo dos racionais, utilizando o grupo ortogonal para estabelecer relações entre equivalências de matrizes e equivalências de espaços quadráticos.

Nesse capítulo serão estudadas propriedades dos espaços quadráticos relativas à decomposição e dimensões.

Um sobconjunto L de V é *lâtice* sobre V se L é Z-módulo induzido por V, QL = V e existe uma base $\{x_1,\ldots,x_n\}$ para V tal que $L \subseteq Zx_1 + \ldots Zx_n$.

Se $\{v_1,\ldots,v_n\}$ é uma base para o lâtice L como Z-módulo, e $H = (Q(v_i,v_j))$ onde Q é a forma bilinear associada, e se H' está na mesma classe de H, então existe uma troca de bases para L tal que a matriz de Q nesta base é H'.

Se L* for outro lâtices e H* for matriz de L* numa certa base, então dizer que L e L* estão na mesma classe é equivalente a dizer que existe uma base de L tal que H = H*, onde H é matriz de L nesta base.

O problema é então traduzido em termos de lâtices, e a determinação da classe de H é equivalente à determinação da classe de L.

Portanto, o problema remanescente é a classificação de lâtices em espaços quadráticos.

No capítulo II estudaremos os lâtices, bases de lâtices e decomposição de lâtices.

Dois lâtices L e L' sobre V são equivalentes se estão na

mesma classe, isto é, se existe $\rho \in O(V)$ tal que $\rho L = L'$.

A fim de ter uma melhor idéia das soluções, às vezes é conveniente localizá-las, isto é, olhar o efeito de cada primo nas soluções considerando o completamento p-ádico de $\mathbb{Q}$, denotado por $\mathbb{Q}_p$. Ainda no capítulo II serão estabelecidas generalidades sobre localização de lâtices.

No capítulo III estudaremos os gêneros e classes de lâtices. Em [O], O.T. O' Meara classifica as formas quadráticas sobre corpos globais e corpos locais. Quanto às formas quadráticas sobre anéis de Dedekind, a classificação é feita sobre anéis locais. A teoria sobre os inteiros ainda é incompleta. O'Meara classifica as formas quadráticas unimodulares indefinidas de dimensões maiores ou iguais a cinco.

Quanto às unimodulares definidas, ele só classifica até dimensão oito.

O trabalho de Martin Kneser em [K] apresenta três métodos para calcular o número de formas quadráticas, de acordo com o discriminante da forma quadrática. Destes, o terceiro método mostra mais explicitamente um cálculo do número de formas quadráticas, pares ou ímpares, a discriminante 1 e dimensão $n \leq 16$.

Finalmente nos capítulos IV e V, com base nestes trabalhos, levamos a efeito a classificação das formas quadráticas com dimensão até 16, tanto em número como em forma (a menos de isomorfismos) tabelando a classificação de lâtices.

Chamamos a atenção do leitor para o fato de que, sendo todos os ideais tratados neste trabalho ideais principais, poderíamos empreender os cálculos e demonstrações com os geradores desses ideais (portanto, com números).

Com o intuito, porém, de fornecer um texto introdutório à bibliografia mais avançada, preferimos manter o tratamento por ideais.

CAPÍTULO I

ESPAÇOS QUADRÁTICOS SOBRE CORPOS

Seja F um corpo de escalares com característica diferente de 2, seja V um espaço vetorial de dimensão finita sobre F, e sobre V definimos uma *forma bilinear simétrica* $B: V \times V \longrightarrow F$, isto é, uma aplicação satisfazendo as seguintes condições:
($x,y,z \in V$ e $\alpha \in F$)

1. $B(x,y+z) = B(x,y) + B(x,z)$
2. $B(\alpha x, y) = \alpha(B(x,y))$
3. $B(x,y) = B(y,x)$

À função $Q: V \longrightarrow F$ definida por $Q(x) = B(x,x)$ chamaremos *função quadrática*. Verificam-se imediatamente as seguintes propriedades de Q:

1. $Q(\alpha x) = \alpha^2 Q(x)$
2. $Q(x+y) = Q(x) + Q(y) + 2B(x,y)$
3. $Q(\sum_{i=1}^{n} \alpha_i x_i) = \sum_{i=1}^{n} \alpha_i^2 Q(x_i) + 2 \sum_{i,j=1}^{n} \alpha_i \alpha_j B(x_i,x_j)$

Por *espaço quadrático* entenderemos um espaço vetorial de dimensão finita munido de uma função quadrática Q, com B definido por Q, já que a função quadrática e a forma bilinear se definem mutuamente. O espaço quadrático chama-se binário, ternário, n-ário

se sua dimensão for respectivamente dois, tres, n.

O espaço quadrático *representa* $\alpha \in F$ se existe $x \in V$ tal que $Q(x) = \alpha$ $(\alpha \in Q(V))$.

Se $Q(V) = F$, (V, Q) é dito *universal*. Diremos que $x,y \in V$ são ortogonais se $B(x,y) = 0$.

Chamaremos de $L(V,W)$ ao conjunto das transformações lineares de V em W. Em particular se $W = V$, escreveremos $L(V,W) = L(V)$. Dentre estas, o conjunto das transformações inversíveis tem uma estrutura de grupo, ao qual denotaremos $GL(V)$ e chamaremos *grupo linear geral* de V.

Dados dois espaços quadráticos (V,Q) e (W,Q') e ρ pertencente a $L(V,W)$ tal que $Q'(\rho x) = Q(x)$, $x \in V$, dizemos que ρ é uma *representação* de (V,Q) em (W,Q') ou que W *representa* V. Segue-se imediatamente que $B'(\rho_x,\rho_y) = B(x,y)$. Uma *isometria* ρ é uma representação injetiva (notação: $V \rightarrowtail W$ para isometria de V em W.)

Se ρ for sobre diremos que (V,Q) e (W,Q') são equivalentes. Denotamos por $O(V,W)$ o conjunto das isometrias de V em W. Se $V = W$ verificamos trivialmente que $O(V)$ é subgrupo de $GL(V)$.

$O(V)$ chama-se *grupo ortogonal de* (V,Q).

Decorre das definições acima a seguinte proposição cuja demonstração não requer maiores cuidados:

PROPOSIÇÃO 1: Sejam (V,Q) e (W,Q') espaços quadráticos, seja $\{x_1,\ldots,x_n\}$ base de V.

Suponhamos que exista $\rho \in L(V,W)$ tal que $B(\rho x_i,\rho x_j) = B(x_i,x_j)$. Então ρ é representação.

Com o objetivo de relacionar os espaços quadráticos com matrizes estudaremos a seguir alguns fatos relativos as matrizes e seus determinantes mostrando suas correlações com os espaços quadráticos.

Se $M_{m\times m}$ e $N_{n\times n}$ são matrizes simétricas sobre os racionais e se existe matriz $T_{m\times n}$ tal que $M = T^tNT$ então M *é representada por* N (notação: $M \rightarrowtail N$).

Dado V espaço quadrático n-dimensional (munido de B e Q) podemos associar a cada base de V uma matriz numérica $N = (B(x_i,x_j))$. N é chamada de *matriz do espaço quadrático na base* $\{x_1,\ldots,x_n\}$.

Se N e N' são matrizes de espaço quadrático V associadas a diferentes bases, então existe T inversível tal que $N=T^tN'T$. Neste caso diremos que N e N' são equivalentes. (Notação: $M \cong N$)

PROPOSIÇÃO 2: Sejam U e V espaços quadráticos com matrizes M e N respectivamente. Então:

a) U representa V se e só se M representa N

b) U equivale a V se e só se M equivale a N

DEMONSTRAÇÃO: vide [0], pg. 86.

Seja V espaço quadrático, $x_1,\ldots x_m \in V$. Definimos determinante em relação a B, $d_B(x_1,\ldots,x_n)$, como $\det(B(x_i,x_j))$. Se N é a matriz do espaço quadrático V, e $\{x_1,\ldots,x_n\}$ é base de V, então $d_B(x_1,\ldots,x_n) = \det N$.

Tomando-se outra base $\{x'_1,\ldots,x'_n\}$ a igualdade $N'=T^tNT$ implica $d_B(x'_1,\ldots,x'_n) = \alpha^2 d_B(x_1,\ldots,x_n)$ onde $\alpha = \det T$.

Portanto a imagem canônica de $\det_B(x_1,\ldots,x_n)$ no grupo extendido $\{0\} \cup \frac{\mathbb{Q}-\{0\}}{\mathbb{Q}^2-\{0\}}$ é independente da base.

Esta imagem é chamada *discriminante* do espaço quadrático V e é denotada por d_B. No caso trivial $V=\{0\}$ convencionaremos $d_B = 1$. A estrutura $\{0\} \cup \frac{\mathbb{Q}-\{0\}}{\mathbb{Q}^2-\{0\}}$ faz sentido com a operação $0.x = 0$ para todo $x \in \frac{\mathbb{Q}-\{0\}}{\mathbb{Q}^2-\{0\}}$ sendo $\mathbb{Q}$ grupo abeliano.

Por uma *forma d-ica* a n variáveis $x_1,\ldots,x_n$ (linear, quadrático, cúbica, etc...) sobre um corpo K entendemos um poliñômio homogêneo de grau d nas variáveis $x_1,\ldots,x_n$.

Se a característica de K é diferente de dois, toda forma quadrática n-ária se expressa como $\Sigma a_{ij}\, x_i x_j$ com $a_{ij} = a_{ji}$ e a ela podemos associar uma matriz numérica $A = (a_{ij})$.

Como exemplo podemos tomar a seguinte forma quadrática binária $f(x_1,x_2) = x_1^2 + 3x_1x_2 + 7x_2^2 = x_1^2 + \frac{3}{2}\, x_1x_2 + \frac{3}{2}\, x_2x_1 + 7x_2^2$ e a ela associamos a matriz

$$\begin{pmatrix} 1 & \frac{3}{2} \\ \frac{3}{2} & 7 \end{pmatrix}$$

Desta forma podemos construir um espaço quadrático a partir de uma forma quadrática. No exemplo acima se tomarmos $\{x_1,x_2\}$ como base de um espaço binário, então a função quadrática correspondente é $Q(\alpha_1x_1 + \alpha_2x_2) = \alpha_1^2 + 3\alpha_1\alpha_2 + 7\alpha_2^2$.

De maneira análoga procedemos para dimensões superiores.

Dizemos que o espaço quadrático V, munido de B e Q, tem uma *decomposição ortogonal* se V é soma direta de subespaços $V_1, V_2, \ldots, V_n$ dois a dois ortogonais, isto é, $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ e $B(V_i, V_j) = 0$ para todo $i \neq j$.

Nesse caso escrevemos $V = V_1 \perp V_2 \perp \ldots \perp V_n = \perp_{i \leq n} V_i$ e convencionaremos que $\perp_{\emptyset} V_i = 0$.

Dizemos que um subespaço U de V decompõe V se existe W tal que $V = U \perp W$.

Por outro lado dado um espaço vetorial V que seja soma direta $V = V_1 \oplus \ldots \oplus V_m$ de m espaços quadráticos (V_i, Q_i), é possível definir uma forma quadrática Q de modo único tal que $V = V_1 \perp V_2 \perp \ldots \perp V_m$ e a restrição de Q a V_i seja Q_i. Basta definir Q sobre V como $Q(x) = \Sigma Q_i(x_i)$ se $x = \sum_i x_i$, $x_i \in V_i$.

Verifica-se que Q é realmente uma forma quadrática com as propriedades exigidas.

Vamos agora mostrar a existência da decomposição ortogonal:

PROPOSIÇÃO 3:

a) todo espaço quadrático não nulo tem base ortogonal, isto é, existe base $\{e_1, \ldots, e_n\}$ para V com $V_i = Ke_i$ e portanto $V = \perp_i V_i$.

b) Seja $V = V_1 \perp V_2 \perp \ldots \perp V_r$ e $W = W_1 + W_2 + \ldots + W_r$ onde os W_i são dois a dois ortogonais, e seja $\alpha_i : V_i \longrightarrow W_i$ representação para cada i, (onde (V,Q) e (W,Q') são espaços quadráticos):

Então existe uma única representação $\alpha: V \longrightarrow W$ tal que α induz cada α_i.

DEMONSTRAÇÃO:

a) Podemos supor $Q(V) \neq 0$, pois se $Q \equiv 0$ quaisquer dois vetores são ortogonais. Seja $\{x_1,\ldots,x_n\}$ base de V, que suporemos não ortogonal, pois caso contrário não há o que provar. Então existe $x \in V$ tal que $Q(x) \neq 0$, e verificamos imediatamente que o conjunto $\{x, x_2 - \frac{B(x_1,x_2)}{Q(x)}\, x,\ldots, x_n - \frac{B(x,x_n)}{Q(x)}\, x\}$ é uma base, e se W é o subespaço gerado por $\{x_2 - \frac{B(x, x_n)}{Q(x)}\, x,\ldots,x_n - \frac{B(x, x_n)}{Q(x)}\, x\}$ teremos $B(\langle x\rangle , W) = 0$. Repetindo o processo no máximo em $n - 1$ etapas chegaremos à soma ortogonal desejada.

b) Neste caso basta tomar $\alpha(\sum_{i=1}^{r} a_i v_i) = \sum_{i=1}^{r} a_i\, \alpha(v_i)$; α é representação pois $Q'(\alpha(\sum_{i=1}^{r} a_i v_i)) = Q'(\Sigma a_i \alpha_i(v_i)) = \sum_{i=1}^{r} a_i^2\, Q'(\alpha_i(v_i)) = \sum_{i=1}^{r} a_i^2\, Q(v_i) = Q(\sum_{i=1}^{r} a_i v_i)$, onde a_i são escalares e $v_i \in V_i$ para cada i.

A unicidade de α é também verificada de maneira simples.□

Seja U subespaço do espaço quadrático V. Chamamos de *complemento ortogonal de* U ao conjunto $U^* = \{x \in V \mid B(x,U) = 0\}$. Chamamos de *radical de* V ao conjunto $\mathrm{Rad}\, V = \{x \in V \mid B(x,V) = 0\}$. Consequentemente $\mathrm{Rad}\, V = V^*$. Dizemos que o espaço quadrático V é *re*

gular se $\text{Rad}\, V = \{0\}$.

Provaremos agora que todo subespaço de um espaço regular possui um complemento ortogonal; mais especificamente:

PROPOSIÇÃO 4: Seja U subespaço regular do espaço quadrático V.

Então U decompõe V de maneira única, isto é, $V = U \perp U^*$ e se $V = U \perp W$, então $W = U^*$.

DEMONSTRAÇÃO: Seja $U = (Fx_1) \perp \ldots \perp (Fx_p)$ onde $\{x_1,\ldots,x_p\}$ é base ortogonal para U.

Como U é regular, $Q(x_i) \neq 0$ para todo i, pois $\text{Rad}\, U = \{0\}$.

Para todo $z \in V$, $z = y + w$ onde $y = \frac{B(z,x_1)}{Q(x_1)} x_1 + \ldots + \frac{B(z,x_p)}{Q(x_p)} x_p$ e $w = z - y$. Em consequência, $y \in U$ e $B(w, x_i) = B(z-y, x_i) = B(z,x_i) - B(z, x_i) \cdot \frac{B(x_i,x_i)}{Q(x_i)} = 0$, portanto $w \in U^*$ logo $V = U + U^*$.

Como $U \cap U^* = \text{Rad}\, U = \{0\}$, a soma é direta, isto é, $V = U \oplus U^*$ e como U e U^* são ortogonais temos $V = U \perp U^*$.

Seja $V = U \perp W$ então $W \subseteq U^*$. Como $V = U \perp U^*$ então $\dim W = \dim U^*$ e $W = U^*$. □

Toda forma bilinear *não degenerada* (isto é, se $B(x,V) = 0$ então $x = 0$) permite definir um isomorfismo entre V e seu espaço dual V'.

Para tanto basta definir a aplicação $\emptyset : V \longrightarrow V'$ como $\emptyset(x) = \phi_x$ onde $\phi_x(y) = B(x,y)$. A aplicação $\phi_x(y)$ é linear em $y \in V$, porque $B(x,y)$ é bilinear. A aplicação $\emptyset(x)$, é linear em $x \in V$ pela mesma razão.

Como V é, por hipótese, regular, então o conjunto $\{x \in V \mid B(x,V) = 0\} = \{0\}$, logo $\emptyset(x) = \phi_x(y) = B(x,y) = 0$, para todo $y \in V$ implica $x = 0$, i.e., a aplicação $\emptyset$ é injetiva, e pelo fato das dimensões de V e de V' serem iguais, $\emptyset$ é bijetiva, definindo portanto o isomorfismo requerido.

Ponhamos $U^{**} = (U^*)^*$. Então:

PROPOSIÇÃO 5: Seja V espaço quadrático regular, U subespaço de V. Então:

a) $\dim V = \dim U + \dim U^*$, e

b) $U^{**} = U$

DEMONSTRAÇÃO:

a) Pela proposição 4, $V = U \oplus U^*$ portanto $\dim V = \dim U + \dim U^*$

b) Por definição de complemento ortogonal, $U^{**} = (U^*)^* = \{x \in V \mid B(x,U^*) = 0$

Para todo $x \in U$, temos $B(x,U^*) = 0$, e portanto $x \in U^{**}$; ou seja, $U \subset U^{**}$.

Por outro lado, como U^* é subespaço, pelo resultado anterior vem a seguinte igualdade:

$\dim U^* + \dim U^{**} = \dim V$ e $\dim U^{**} = \dim V - \dim U^*$.

Do fato de $\dim U = \dim V - \dim U^*$, concluimos pela igualdade de dimensões (isto é, $\dim U^{**} = \dim U$) e como $U \subset U^{**}$, então $U = U^{**}$.□

CAPÍTULO II

LÁTICES EM ESPAÇOS VETORIAIS

Neste capítulo definiremos látices e estudaremos suas relações com espaços vetoriais, base de um látice e mudança de base.

Os espaços, vetoriais estarão definidos sobre o corpo dos números racionais.

2.1 DEFINIÇÃO DE LÁTICE

Seja M um Z-módulo: M é *ideal fracionário* se existe $d \neq 0$ em Z tal que $M \subset d^{-1}Z$. Neste caso como o corpo é dos racionais, todos os ideais fracionários serão de forma $\frac{1}{n} Z = \{\frac{m}{n} : m \in Z, n \in Z\}$

Seja V um espaço vetorial de dimensão finita, e seja M um subconjunto de V que é Z-módulo induzido pelas leis do espaço vetorial V sobre $\mathbb{Q}$.

Definimos o *espaço vetorial gerado pelo Z-módulo* M como o conjunto $\mathbb{Q}M = \{\frac{p}{q} x, \frac{p}{q} \in \mathbb{Q} \text{ e } x \in M\}$

PROPOSIÇÃO 1: $\mathbb{Q}M$ é subespaço vetorial de V.

DEMONSTRAÇÃO: sejam $\alpha, \beta \in \mathbb{Q}M$ e $c \in \mathbb{Q}$. Então $\alpha = \frac{p_1}{q_1} x$, $\beta = \frac{p_2}{q_2} y$ e $c = \frac{c_1}{c_2}$ e $c\alpha + \beta = \frac{(q_2 c_1 p_1)\, x + (c_2 q_1 p_2)}{c_2 q_1 q_2}$ estão em $\mathbb{Q}M$ porque $\frac{1}{c_2 q_1 q_2} \in \mathbb{Q}$ e $(q_2 c_1 p_1)x + (c_2 q_1 p_2)y \in M$. □

Passemos à definição de látice: o subconjunto M de V é

lâtice sobre V se M é Z-módulo induzido por V, $\mathbb{Q}M = V$ e existe uma base $\{x_1,\ldots,x_n\}$ para V tal que $M \subseteq Z\,x_1 + \ldots + Z\,x_n$. Em particular, sendo $\{x_1,\ldots,x_n\}$ base de V, o conjunto

$$Zx_1 + Zx_2 + \ldots + Zx_n \quad \text{é lâtice sobre } V.$$

De maneira semelhante, dizemos que o Z-módulo M é *lâtice em* V se existe uma base $\{x_1,x_2,\ldots x_n\}$ para V tal que $M \subseteq Zx_1 + Zx_2 + \ldots + Zx_n$.

PROPOSIÇÃO 2: Seja L um lâtice sobre V: então o Z-módulo $M \subset V$ é lâtice em V se e somente se existe $K \in Z$, $K \neq 0$, tal que $KM \subseteq L$. Em particular se M é lâtice sobre V então existe $K' \in Z$ t.q. $K'L \subset M$, isto é, $K'L \subset M \subset K^{-1}L$.

DEMONSTRAÇÃO:

Por um lado se M é lâtice em V, existe base para V de tal forma que $M \subseteq Zx_1 + Zx_2 + \ldots + Zx_n$.

Como L é lâtice sobre V, todo elemento x_j da base de V se escreve como $x_j = \sum_{i=1}^{m} a_{ij} y_i$, para m adequado, onde

$$a_{ij} \in \mathbb{Q},\ y_i \in L.$$

Pelo fato dos $a_{ij} \in \mathbb{Q}$ formarem um conjunto finito, podemos escolher um $K \in Z$ (como o mínimo múltiplo comum dos denominadores dos racionais a_{ij}) de tal forma que $K\,a_{ij} \in Z$ para todo a_{ij}.

Portanto, para todo elemento x_j da base de V conclui-se $K x_j = \sum_{i=1}^{m} (K a_{ij}) y_i \in Zy_1 + Zy_2 + \ldots + Zy_m$ e $Zy_1 + Zy_2 + \ldots + Zy_m \subseteq L$ e então $K x_j \subseteq L$ para todo x_j da base de V.

Portanto, tendo em vista que $M \subseteq Z x_1 + Z x_2 + \ldots + Z x_n$ conclui-se que $KM \subseteq L$.

Por outro lado, se existe $K \in Z$ tal que $KM \subseteq L$, consideremos o fato de L ser lâtice sobre V.

Se L é lâtice sobre V, então L é lâtice em V e existe base para V de tal forma que $L \subseteq Zx_1 + Zx_2 + \ldots + Zx_n$. Isto leva a $M \subseteq K^{-1}L \subseteq Z(\frac{x_1}{K}) + Z(\frac{x_2}{K}) + \ldots + Z(\frac{x_n}{K})$ onde os elementos $\frac{x_i}{K}$ formam nova base para V, e então M é lâtice em V. Em particular, se L é lâtice sobre V, então L é lâtice em V e se M é lâtice sobre V, existe $K' \in Z$ tal que $K'L \subset M \subset K^{-1}L$. □

PROPOSIÇÃO 3: Sejam V espaço vetorial, U subespaço de V, M subconjunto de U. Então M é lâtice em V se e somente se M é Lâtice em U.

DEMONSTRAÇÃO: Seja $\{x_1, \ldots, x_r\}$ base para U e estendamo-la para $\{x_1, \ldots x_r, x_{r+1}, \ldots, x_n\}$ base de V. Consideremos dois lâtices respectivamente sobre U e sobre V, a saber:

$$L' = Z_{x_1} + Z_{x_2} + \ldots + Z_{x_r} \quad \text{e} \quad L = Z_{x_1} + \ldots + Z_{x_n}.$$

Sendo M lâtice em U, da proposição 2 existe $K \in Z$ tal que $KM \subseteq L' \subseteq L$ e então M é lâtice em V.

Reciprocamente, se M é látice em V, existe $K \in Z$ tal que $KM \subseteq L$ mas $KM \subseteq L \cap U = L'$ e daí conclui-se que M é latice em U. □

Segue imediatamente das definições e da proposição 2, itém 2.1, que todo submódulo de um látice sobre V é um látice em V. Em particular, se L e K são látices sobre V, então $L \cap K$ é submódulo, e como $\mathbb{Q}L \cap \mathbb{Q}K = V = \mathbb{Q}(L \cap K)$, $L \cap K \subseteq Zx_1 + \ldots Zx_n$ se $L \subseteq Zx_1 + \ldots Zx_n$ onde $\{x_1, \ldots, x_n\}$ é base de V, então $L \cap K$ é látice sobre V.

2.2. BASES

Seja L látice em V. Para todo $x \in \mathbb{Q}L$, $x \neq 0$, definimos *coeficiente de* x *em* L como o conjunto $C_x = \{\alpha \in \mathbb{Q} | \alpha x \in L\}$. Como $\mathbb{Q}L$ é não vazio existe $q\ell \in \mathbb{Q}L$ e $q^{-1}q\ell \in L$, portanto C_x é não vazio. Um cálculo simples mostra que C_x é Z-módulo em $\mathbb{Q}$ e que $C_x \cdot x = L \cap \mathbb{Q}x$. Portanto $C_x \cdot x$ é látice em $\mathbb{Q}x$ e existe $\alpha \in Z$, $\alpha \neq 0$, tal que $\alpha C_x \cdot x \subseteq Zx$ e daí $\alpha C_x \subseteq Z$, ou seja C_x é ideal fracionário.

Dizemos que x *é vetor maximal de* L se $C_x = Z$. Portanto, x é vetor maximal quando $Zx = L \cap \mathbb{Q}x$. Toda linha $\mathbb{Q}y$ de $\mathbb{Q}L = V$ tem um vetor maximal: de fato seja a linha $\mathbb{Q}y$ e $C_y = \alpha Z$, para um $\alpha \in \mathbb{Q}$ adequado. Basta tomar $x = \alpha y$ e teremos $C_x = Z$, logo x é vetor maximal de L e $x \in \mathbb{Q}y$.

TEOREMA 4: Dado um látice L sobre V, um subespaço vetorial U de V com dimensão $(n-1)$ e dado $x_o \in V-U$, então entre os vetores $y \in x_o + U$ existe pelo menos um vetor cujo coeficiente com respeito a L é maximo em relação à inclusão. Se este coeficiente é c, então para qualquer vetor $x_o + u_o$ ($u_o \in U$) com coeficiente c temos $L = c(x_o + u_o) + L \cap U$.

DEMONSTRAÇÃO:

Afirmamos que o conjunto $c = \{\alpha \in \mathbb{Q} | \alpha\, x_o \in L + U\}$ é um ideal fracionário. Claramente, c é um Z-módulo não nulo em $\mathbb{Q}$. Como L é lâtice sobre V, existe base $\{x_1,\ldots,x_n\}$ para V tal que $L \subseteq Zx_1 + \ldots + Zx_n$. Seja $\{y_1,y_2,\ldots,y_{n-1}\}$ base de U; então o conjunto $\{x_o,y_1,y_2,\ldots,y_{n-1}\}$ é uma base para V e $Zx_o + Zy_1 + \ldots + Zy_{n-1}$ é lâtice sobre V. Pela proposição 2, existe $\beta \in Z$ tal que $\beta L \subseteq Zx_o + Zy_1 + \ldots + Zy_{n-1} \subseteq Zx_o + U$ portanto $\beta L \subseteq Zx_o + U$.

Por outro lado, da definição de c, $\alpha x_o \in L + U$, para todo $\alpha \in C$ e $\beta\alpha x_o \in \beta L + U$, donde $(\beta c)x_o \subseteq \beta L + U$ e do exposto conclui-se $(\beta c)x_o \subseteq \beta L + U \subseteq Zx_o + U$ e então $\beta c \subseteq Z$ e c é um ideal fracionário.

O coeficiente de qualquer vetor em $x_o + U$ está contido em c, por construção de c. A primeira parte do teorema será então provada de conseguirmos um vetor $u' \in U$ tal que $c(x_o + u') \subseteq L$, pois o coeficiente desse vetor irá conter c.

Desde que $c \cdot c^{-1} = Z$, podemos conseguir uma expressão $\alpha_1\beta_1 + \ldots + \alpha_r\beta_r = 1$ onde $\alpha_i \in c$, $\beta_i \in c^{-1}$.

A definição de c implica $\alpha_i\, x_o = \ell_i + u_i$ para cada $\alpha_i \in c$ e a expressão enunciada implica que $\alpha_1\beta_1\, x_o + \ldots + \alpha_r\beta_r\, x_o = \sum_{i=1}^{r} \beta_i \ell_i + \sum_{i=1}^{r} \beta_i u_i$.

Mais, $\beta_i\, c \subseteq Z$, $1 \leq i \leq r$. Portanto,

$$c(x_o - \sum_{i=1}^{r} \beta_i u_i) = c(\sum_{i=1}^{r} \beta_i \ell_i) \subseteq L$$

e temos conseguido $u' = \sum_{i=1}^{r} \beta_i u_i$ de tal forma que $c(x_o + u') \subseteq L$,

ou seja, $x_o + u'$ é um vetor tal que tem coeficiente c.

Portanto, para todo vetor $u_o \in U$ que tenha coeficiente c em relação a L, $c(x_o + u_o) \subseteq L$ e $c(x_o + u_o) + L \cap U \subseteq L$.

Reciprocamente, seja um vetor $\alpha(x_o + u)$ de V, $u \in U$ e $\alpha \in \mathbb{Q}$ de forma que $\alpha(x_o + u) \in L$. Então $\alpha x_o \in L + U$, e pela definição de c , $\alpha \in c$.

Portanto, considerando que $\alpha(u - u_o) = \alpha(x_o + u) - \alpha(x_o + u_o) \in L$ e que $\alpha(u - u_o) \in U$, conclui-se que $\alpha(x_o + u) = \alpha(x_o + u_o) + \alpha(u - u_o) \in c(x_o + u_o) + L \cap U$.

Pelo fato de $\alpha(x_o + u)$ ser um vetor típico de L, temos $L \subset c(x_o + u_o) + L \cap U$. □

TEOREMA 5: Se L é lâtice sobre V e $\{x_1,\ldots,x_n\}$ é uma base para V, então existe base $\{y_1,\ldots,y_n\}$ tal que $y_1 \in \mathbb{Q}x_1 + \ldots \mathbb{Q}x_i$, $1 \leq i \leq n$, e há ideais fracionários $J_1, J_2,\ldots,J_n$ tal que $L = J_1y_1 + \ldots + J_ny_n$.

DEMONSTRAÇÃO: pelo teorema 4, seja U o hiperplano $U = \mathbb{Q}x_1+\ldots+\mathbb{Q}x_{n-1}$ e então $L = (L \cap U) + c_ny_n$ para algum y_n e o coeficiente c_n.

Considerando-se que $L \cap U$ é lâtice sobre U, procede-se por indução sobre $n = \dim V$. □

Observemos que cada c_i utilizado na demonstração é coeficiente de y_i.

TEOREMA 6: Seja L um lâtice sobre o espaço vetorial V. Então existe uma base $\{z_1,z_2,\ldots,z_n\}$ para V tal que $L = \mathbb{Z}z_1 + \mathbb{Z}z_2+\ldots+\mathbb{Z}z_n$.

DEMONSTRAÇÃO: pelo teorema 5, $L = J_1y_1 + J_2y_2 + \ldots + J_ny_n$ onde $J_1, J_2, \ldots, J_n$ são ideais fracionários do tipo $J_1 = \frac{1}{n_1} Z$, $J_2 = \frac{1}{n_2} Z, \ldots, J_n = \frac{1}{n_n} Z$. Basta, portanto escolher a nova base como $z_1 = \frac{1}{n_1} y_1, \ldots, z_n = \frac{1}{n_n} y_n$. □

2.3. TROCA DE BASES

Consideremos dois lâtices L e K sobre o mesmo espaço vetorial V e sejam $\{x_1, \ldots, x_n\}$ e $\{y_1, \ldots, y_n\}$ as bases na quais

$$L = I_1x_1 + \ldots + I_nx_n$$

$$\text{e} \quad K = J_1y_1 + \ldots + J_ny_n$$

onde I_i e J_i são ideais fracionários.

Sejam $y_j = \sum_{i=1}^{n} a_{ij} x_i$ e $x_j = \sum_{i=1}^{n} b_{ij} y_i$ as equações que relacionam essas bases. Portanto, amatriz (a_{ij}) é a inversa da matriz (b_{ij}).

PROPOSIÇÃO 7: Estando os lâtices K e L escritos nas condições acima, então $K \subseteq L$ se e somente se $a_{ij}J_j \subseteq I_i$, para todo i e J.

DEMONSTRAÇÃO: Temos $K \subseteq L$ se e somente se $J_jy_j \subseteq L$ isto é, se e só se $J_j(a_{1j}x_1 + a_{2j}x_2 + \ldots + a_{nj}x_n) \subseteq L$, ou seja $J_j(a_{1j}x_1 + \ldots + a_{nj}x_n) \subseteq I_1x_1 + \ldots + I_nx_n$, isto é, se e só se $a_{ij}J_i \subseteq I_i$ para $1 \leq i \leq n$ e $1 \leq j \leq n$. □

PROPOSIÇÃO 8: Suponhamos, $K \subseteq L$ onde K e L são lâtices nas mesmas condições anteriores. Então $K = L$ se e somente se

$I_1.I_2...I_n = J_1...J_n.\ \det(a_{ij})$ (Obs: os ideais fracionários sobre os inteiros possuem uma estrutura de grupo multiplicativo).

DEMONSTRAÇÃO: Por um lado, suponhamos $K = L$. Pela proposição 7, $a_{ij}J_j \subseteq I_i$, para todo i e j tem-se $\det(a_{ij}) = \Sigma \pm a_{1\alpha}...a_{n\omega}$, onde $a_{1\alpha},...,a_{n\omega}$ são elementos da matriz (a_{ij}).

Como $a_{ij}J_j \subseteq I_i$, todo i e j, tem-se $\Sigma \pm a_{1\alpha}...a_{n\omega} \in \Sigma(I_1J^{-1})$ $(...)$ $(I_nJ_\omega^{-1})$ ou seja, $\Sigma \pm a_{1\alpha}...a_{n\alpha} \in (I_1...I_n)(J_1...J_n)^{-1}$ e portanto $(J_1...J_n)\det(a_{ij}) \subseteq (I_1...I_n)$.

Analogamente, $(I_1...I_n)\det(b_{ij}) \subseteq (J_1...J_n)$.

Pelo fato de (b_{ij}) se a matriz inversa de (a_{ij}), $\det(b_{ij}) = (\det(a_{ij}))^{-1}$ e portanto

$$I_1...I_n = \det(a_{ij})\ J_1...J_n.$$

Por outro lado, sendo $K \subseteq L$, temos $a_{ij} \in I_iJ_j^{-1}$.

Seja $A_{ij} = \Sigma \pm a_{1\alpha}...a_{n\omega}$, onde não aparecem nessa formulação os índices a_{ik}, a_{kj} para todo k.

Isso implica $A_{ij}I_iJ_j^{-1} \subseteq (I_1...I_n)(J_1...J_n)^{-1} = Z\ \det(a_{ij})$

Considerando que A_{ij} é o cofator de a_{ij} e que a matriz (b_{ij}) é inversa da matriz (a_{ij}) segue-se que $b_{ji}I_i = \frac{A_{ij}}{\det(a_{ij})} I_i \subseteq J_j$. Isto vale para todo i e j, portanto $L \subseteq K$, e dai $L = K$.□

A proposição 8 apresenta como corolário o fato de que, se L é expresso livremente numa base $\{x_1,...,x_n\}$ isto é, $L = Zx_1 + zx_2 +...+ zx_n$ e se $y_1,...,y_n$ são vetores determinados por

$y_j = \sum_i a_{ij}x_i$, $a_{ij} \in \mathbb{Q}$, então os vetores $y_1,\ldots,y_n$ formam uma nova base para L se e somente se a matriz (a_{ij}) é unimodular. Para tanto, basta observar a igualdade $Z.Z\ldots Z = Z\ldots Z.\det(a_{ij})$ que explicita $\det(a_{ij}) = \pm 1$.

2.4: FATORES INVARIANTES

Neste ítem, o teorema 9 estabelecerá a existência e unicidade de certos ideais que satisfazem, na formulação de um lâtice , uma relação de inclusão. Tais ideais serão chamados *fatores invariantes*.

LEMA 9: Dado um lâtice L sobre V, $v \in V$, existe hiperplano U tal que $L = I_v.v + L \cap U$, onde I_v é o coeficiente de v em L.

DEMONSTRAÇÃO : Seja $\{v,x_2,\ldots,x_n\}$ base de V extendida a partir do vetor v, e seja U o hiperplano $U = \mathbb{Q}x_2 +\ldots+ \mathbb{Q}x_n$. Pelo teorema 5, existe base $\{y_1,\ldots,y_n\}$ tal que $y_1 \in \mathbb{Q}v$, ou seja, $y_1 = \alpha v, \alpha \in \mathbb{Q}$, de tal forma que $L = C_1y_1+(L \cap U)$ onde C_1 é o coeficiente de $y_1 = \alpha v$. Por outro lado, sendo I_v coeficiente de v em L, verifica-se trivialmente que $I_v.\ v \subseteq L$ e $I_v.v+(L \cap U) \subseteq L$. Reciprocamente, sendo $L = C_1y_1+(L \cap U)$, todo elemento de L se escreve como $\beta y_1 + u, \beta \in C_1,\ u \in (L \cap U)$, ou seja, como $\beta\alpha v + u$, $u \in (L \cap U)$ e $\beta\alpha v \in L$. Portanto, $\beta\alpha \in I_v$ e $L \subseteq I_v.\ v+(L \cap U)$ □

TEOREMA 10: Dados lâtices L e K sobre o espaço vetorial V não nulo, existe uma base $\{x_1,x_2,\ldots,x_n\}$ para V na qual

$$L = I_1x_1+\ldots I_nx_n$$

e $K = I_1R_1x_1 + \ldots + I_nR_nx_n$ onde I_i, R_i são ideais fracionários e $R_1 \supseteq R_2 \supseteq \ldots \supseteq R_n$ são únicos; estes ideais são os fatores invariantes.

DEMONSTRAÇÃO: em primeiro lugar, suponhamos $K \subseteq L$ (se tal não ocorrer, poderemos trocar K por um conveniente $\alpha K, \alpha \in \mathbb{Z}, \alpha \neq 0$, de modo que a inclusão ocorra). Para um elemento qualquer $x \in V$ seja I_x o coeficiente de x em L e B_x o coeficiente de x em K. Como $K \subseteq L$, consequentemente $B_x \subseteq I_x$ e se tomarmos o quociente entre os ideais, $R_x = \frac{B_x}{I_x}$ teremos $R_x \subseteq Z$. Poderemos então tomar um vetor $v \in V$ para o qual R_v seja maximal, (porem, não necessariamente máximo). Seja $\{v, y_2, \ldots, y_n\}$ base de V extendida a partir de v. Seja U o hiperplano $U = \mathbb{Q}y_2 + \ldots + \mathbb{Q}y_n$.

Então , pelo lema 9, $L = (L \cap U) + I_v.v$; temos $I_{v+u} \subseteq I_v$, para todo $u \in U$. De fato, $I_{v+u}(v+u) \subseteq L = (L \cap U) + I_v.v$ e $\alpha(v+u) = \alpha v + \alpha u \in (L \cap U) + I_v.v$.

Porém, como $v \notin U$, $\alpha v \in I_v.v$ e $\alpha \in I_v$, para todo $\alpha \in I_{v+u}$.

Afirmamos que $B_{v+u} \subseteq B_v$, para todo $u \in U$. Senão, pelo teorema 4, existe $u \in U$ tal que $B_{v+u} \supset B_v$.

Mas, dai, $I_{v+u}.B_v \subseteq I_v.B_v \subseteq I_v.B_{v+u}$ e $R_{v+u} = \frac{B_{v+u}}{I_{v+u}} \supset \frac{I_v}{B_v} = R_v$

o que contraria a escolha de v. Portanto, temos de fato $B_{v+u} \subseteq B_v$ para todo $u \in U$. Aplicando novamente lema 9 obtemos $K = B_v.v + (K \cap U)$; um argumento indutivo demonstra as expressões

$$L = I_v.v + (I_\omega.\omega + \ldots + I_z.z) \quad \text{e}$$

$$K = I_v.R_v.v + (I_\omega R_\omega.\omega + \ldots + I_z R_z.z)$$

com $R_\omega \supseteq \ldots \supseteq R_z$. Resta provar que $R_v \supseteq R_\omega$.

Dados os ideais I_v^{-1} , I_ω^{-1}, R_v, R_ω existe $\alpha,\beta \in \mathbb{Q}$ tais que $\alpha I_v^{-1} + \beta I_\omega^{-1} = R_v + R_\omega$. Seja $x = \alpha v + \beta\omega$.

Desde que sendo A e B ideais fracionários $A \cap B=(A^{-1}+B^{-1})^{-1}$ pode-se verificar que $I_x = (I_v\alpha^{-1}) \cap (I_\omega\beta^{-1})=(\alpha I_v^{-1}+\beta I_\omega^{-1})^{-1}=(R_v+R_\omega)^{-1}$.

De maneira similar, pode-se verificar que $B_x = Z$ e então $R_x = \frac{B_x}{I_x} = R_v + R_\omega$, de maneira que $R_v \subseteq R_v + R_\omega = R_x$ e pelo maximalidade de R_v, $R_v = R_x=R_v+R_\omega \supseteq R_\omega$ portanto $R_\omega \subseteq R_v$.

Para demonstrar a unicidade dos fatores invariantes suponhamos a formulação $L = I_1x_1+\ldots+ I_nx_n$ e $K=I_1R_1x_1+\ldots+I_nR_nx_n$, com $R_1 \supseteq R_2 \supseteq \ldots \supseteq R_n$ e outra formulação possível onde R_i' seja o primeiro fator diferente dos $R_i (1 \leq i \leq n)$.

Consideremos o látice $J = K+(R_i'L)$ e tomemos os fatores invariantes de J, da forma $R_\lambda' = R_\lambda$, $1 \leq \lambda \leq i-1$ e $R_\lambda' \neq R_\lambda$ para $i \leq \lambda \leq n$

Tomando-se as duas decomposições para J:

$J = K+(R_i'L)=I_1(R_1'+R_i')x_1+\ldots+I_i(R_i'+R_i')x_i+\ldots+I_n(R_n'+R_i')x_n$ e $J=K+(R_i'L)=$
$=I_1(R_1+R_i')x_1+\ldots I_i(R_i+R_i')x_i+\ldots\ I_n(R_n+R_i')x_n$.

Como $R_i \supseteq R_i+1$, tomando-se o produto dos fatores pelas duas formulações, teremos por um lado $R_1R_2\ldots R_{i-1}.R_i'\ldots R_i'$ e por outro $R_1.R_2\ldots(R_i+R_i')\ \ldots(R_n+R_i')$.

Mas $R_j+R_i' \neq R_i'$ para $j \geq i$ e os produtos serão diferentes, contrariando a proposição 8. Portanto, os fatores invariantes são únicos .

2.5. LOCALIZAÇÃO DE LÁTICES

Por *valorização* entendemos uma aplicação $||: \mathbb{Q} \to R$ tal que três propriedades sejam satisfeitas:

(1) $|\alpha| > 0$ se $\alpha \neq 0$, $|0| = 0$
(2) $|\alpha\beta| = |\alpha| \,.|\beta|$

(3) $|\alpha + \beta| \leq |\alpha| + |\beta|$.

Se a função referida satisfaz (1),(2) e a propriedade $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$, então satisfaz (3) e a valorização é dita *não-arquimediana;* se a valorização não satisfaz tal propriedade é dita *arquimediana.*

Como exemplo de valorização no corpo dos racionais, fixado um primo p, para $\alpha \in \mathbb{Q}$ tem-se $\alpha = p^i(\frac{m}{n})$ onde $(m,p)=1$ e $(n,p) = 1$, $i \in Z$ pode-se exibir a aplicação $|\alpha|_p = (\frac{1}{p})^i$, $i \in Z$. Esta é uma valorização não-arquimediana. Duas valorizações se dizem *equivalentes* se definem a mesma topologia sobre um corpo.

Por *lugar* entendemos uma classe de valorizações equivalentes sobre um dado corpo. Existe exatamente um lugar arquimediano P nos racionais (vide [0], teorema 12.1 pg.14). Toda valorização $||$ em P é da forma $|| = ||_\infty^\rho$, onde $||_\infty$ é o valor absoluto em $\mathbb{Q}$ e $0 < \rho \leq 1 \in \mathbf{R}$.

Denotaremos por $||_p$ a extensão canônica de uma valorização ao completamento $\mathbb{Q}_p$ onde p é um número primo inteiro. Esta valorização funcionará sobre o completamento $\mathbb{Q}_p$. Um ideal fracionário típico em $\mathbb{Q}$ tem a forma $\prod_{p \in S} p^{n_p}$, onde p representa dois ideais primos diferentes, o ideal primo $Z \cap m_p$ de Z e o ideal primo m_p de Z_p, anel dos inteiros p-ádicos, onde $m_p = \{\alpha \in Q \mid |\alpha|_p < 1\}$ e m_p é chamado *ideal maximal* de Z_p. S representa o conjunto de todos os elementos primo em Z, e n_p são inteiros quase todos nulos.

Um ideal fracionário típico em $\mathbb{Q}_p$ tem a forma p^{n_p} onde $n_p \in Z$.

Introduzimos o homomorfismo sobrejetivo definido pela função $\prod_{p \in S} p^{n_p} \to p^{n_p}$ de $I \to I_p$, onde I representa o conjunto dos ideais de $\mathbb{Q}$ e I_p o conjunto dos ideais de $\mathbb{Q}_p$.

A imagem, por esta transformação, de um ideal A em $\mathbb{Q}$ será denotada por A_p e será chamada *localização* em p *do ideal* A.

Desde que o ideal A pode ser retomado como $A = \bigcap_{p \in S} (\mathbb{Q} \cap A_p)$, então temos que $A \subseteq B$ se e somente se $A_p \subseteq B_p$ para todo $p \in S$; de fato, se $A \subseteq B$, então $A_p \subseteq B_p$; por outro lado, se $A_p \subseteq B_p$,

então $\mathbb{Q} \cap A_p \subseteq \mathbb{Q} \cap B_p$, todo $p \in S$ e daí $\bigcap_{p\in S} (\mathbb{Q} A_p) \subseteq \bigcap_{p\in S} (\mathbb{Q} \cap B_p)$ portanto $A \subseteq B$.

Em particular, $A=B$ se e somente se $A_p = B_p$, para todo $p \in S$.

Se $A = \pi_{p\in S} p^{n_p}$ e $B = \pi_{p\in S} p^{m_p}$ são ideais em suas fatorações primas, definimos *a soma dos ideais* A *e* B como $A+B = \pi_{p\in S} p^{\min(n_p, m_p)}$.

Pode-se verificar que $(A+B)_p = A_p + B_p$ e $(Ax)_p = A_p x$.

Seja V espaço vetorial de dimensão n sobre $\mathbb{Q}$. Seja $V_p = \mathbb{Q}_p^n$. Como $\mathbb{Q} \subset \mathbb{Q}_p$, então existe um subespaço de $\mathbb{Q}_p^n$ canonicamente isomorfo a V.

No que segue, identificaremos V a esse subespaço e assim, para todo $x \in V$, podemos considerá-lo também em V_p, considerando que V_p pode ser escrito como $V_p = \mathbb{Q}_p V$.

Dado um lâtice L sobre V, $L = A_1 x_1 + \ldots + A_n x_n$, onde A_i são ideais fracionários e $\{x_1, \ldots, x_n\}$ é uma base para V, então podemos definir um Z_p-lâtice L_p sobre V_p, de maneira análoga à definição de Z-lâtice da página 10, como Z_p-módulo tal que existe base $\{x_1, \ldots, x_n\}$ para V_p de modo que $L_p \subseteq Z_p x_1 + \ldots + Z_p x_n$ e $\mathbb{Q}_p L_p = V_p$.

A partir dessa definição, $L_p = A_{1p} x_1 + \ldots + A_{np} x_n$ é um, Z_p-lâtice sobre V, pois pode-se verificar que:

(i) L_p é Z_p-módulo

(ii) $L_p \subseteq Z_p x_1 + \ldots + Z_p x_n$

(iii) $\mathbb{Q}_p L_p = V_p$, pois $\mathbb{Q} \subset \mathbb{Q}_p$, $L \subset L_p$, então $V \subset \mathbb{Q}_p L_p$ e $\mathbb{Q}_p = V_p \subset \mathbb{Q}_p L_p$. Por outro lado $\mathbb{Q}_p \subset V_p$, $L_p \subset V_p$ e $\mathbb{Q}_p L_p \subset V_p$.

Uma demonstração análoga ao caso dos ideais estabelece que $L \subseteq K$ se e somente se $L_p \subseteq K_p$, para todo $p \in S$, e em particular $L=K$ se e somente se $L_p = K_p$ para todo $p \in S$, onde L e K são lâtices sobre V.

Dados ideais A e B em suas fatorações primas como acima definimos a *interseção dos ideais* A *e* B como $A \cap B = \pi_{p\in S} p^{\max(n_p, m_p)}$.

TEOREMA 10 : Sejam dados Z_p-látices $J(p)$ sobre V_p a cada $p \in S$.

Suponhamos que exista um Z-látice L sobre V com $L_p = J_p$ para quase todo p. Então existe um Z-látice K sobre V tal que $K = J(p)$ para todo $p \in S$.

DEMONSTRAÇÃO:

Será suficiente provar a existência de um Z-látice K sobre V tal que

$$K_q = L_q \quad \text{se} \quad q \in S-p \quad \text{e}$$

$K_q = J(p)$ se $q = p$. Como existe L tal que $L_p = J(p)$ exceto num conjunto finito, o resultado segue por sucessivas aplicações deste caso especial.

Como o látice $J(p)$ dado a cada p será da forma $J(p) = Z_p y_1 + \ldots + Z_p y_n$ onde $\{y_1, \ldots, y_n\}$ é uma base para V, então existe $J = Zy_1 + \ldots + Zy_n$ sobre V tal que $J_p = J(p)$.

De acordo com o teorema dos fatores invariantes (teorema 10, ítem 2.4) existe base $\{z_1, \ldots, z_n\}$ para V tal que

$L = A_1 z_1 + \ldots + A_n z_n$, $J = B_1 z_1 + \ldots B_n z_n$ onde A_i, B_i são ideais em Z.

Sejam C_i $(1 \leq i \leq n)$ ideais construídos da seguinte maneira: $C_{iq} = A_{iq}$ se $q \in S-p$, $C_{iq} = B_{ip}$ se $q = p$

Então o látice $K = C_1 z_1 + \ldots + C_n z_n$ tem a propriedade desejada. □

CAPÍTULO III

LÂTICES EM ESPAÇOS QUADRÁTICOS
GÊNERO E CLASSE DE LÂTICES

3.1 GÊNERO E CLASSE DE LÂTICES

Neste capítulo uma estrutura adicional é colocada no assunto em discussão: o espaço vetorial V é tornado um espaço quadrático por adjunção de uma forma bilinear simétrica B dada com a forma quadrática associada Q.

Seja V espaço vetorial, seja L lâtice em V, e seja U outro qualquer espaço quadrático sobre $\mathbb{Q}$, e seja K um lâtice em U. Dizemos que K *é representado por* L (notação : $K \rightarrowtail L$) se existe uma representação $\sigma : \mathbb{Q}K \longrightarrow \mathbb{Q}L$ tal que $\sigma K \subseteq L$ (como já observado, σ é representação se $Q(\sigma x) = Q(x)$, para todo $x \in U$).

Dizemos que há uma *isometria de* K *sobre* L (notação: $K \rightarrowtail L$) se existe isometria $\sigma : \mathbb{Q}K \rightarrowtail \mathbb{Q}L$ tal que $\sigma K \subseteq L$. Dizemos que K *e* L *são isométricos* (notação: $K \rightarrowtail L$ ou $K \cong L$) se existe uma isometria $\sigma : \mathbb{Q}K \rightarrowtail \mathbb{Q}L$ tal que $\sigma K = L$.

O decorrer deste capítulo esclarecerá que achar os lâtices isométricos a um lâtice dado é o mesmo que achar a classe de equivalência de uma forma quadrática. Estudará também em que condições, dados lâtices L e K sobre o espaço quadrático V, existe um elemento do grupo ortogonal O(V) tal que $\sigma K = L$.

Sejam $M_{m\times m}$, $N_{n\times n}$ matrizes simétricas sobre $\mathbb{Q}$.

Dizemos que M é *integralmente representado por* N se existe $T_{n\times m}$ com coeficientes em Z tal que $M = T^tNT$.

Se T for unimodular (ou seja, com determinante ± 1) então M e N são *integralmente equivalentes*. Essa relação é de equivalência e denotamos $\overline{N}$ = class N.

Seja L um lâtice sobre V e seja uma base $\{x_1,\ldots,x_n\}$ para V tal que $L = Zx_1 + Zx_2 +\ldots+ Zx_n$.

Por *matriz de* L *na base* $\{x_1,\ldots,x_n\}$ entendemos a matriz $N = (B(x_i,x_j))$ e escrevemos $L \cong N$.

Se $\{x_1',\ldots,x_n'\}$ é outra base para L com $x_i' = \sum_\lambda t_{\lambda i}\cdot x_i$ ($t_{\lambda i} \in Z$) então a matriz $T = (t_{\lambda i})$ é unimodular (vide capítulo 2, observação da proposição 8) e a matriz de L nesta nova base é $N' = T^tNT$ e portanto a troca de bases se conserva em class N.

Podemos então associar uma classe de matrizes integralmente equivalentes com um lâtice num dado espaço quadrático, e toda classe de matrizes integralmente equivalentes pode ser obtida a partir de um lâtice adequado num espaço quadrático adequado.

Dada uma matriz simétrica N, <N> significa o espaço quadrático tendo matriz N. Usaremos a mesma notação para denotar um lâtice sobre V com matriz N.

PROPOSIÇÃO 1: Sejam K e L lâtices com matrizes M e N sobre espaços quadráticos U e V respectivamente.

Então, nestas condições temos: (*)

(1) $K \rightarrowtail L$ se e somente se $M \rightarrowtail N$ (sobre Z)

(2) $K \cong L$ se e somente se $M \cong N$ (sobre Z)

DEMONSTRAÇÃO:

(1) Primeiramente seja $M = (a_{ij})$ e $N=(b_{ij})$. Seja $\{x_1,\ldots,x_n\}$ base para U na qual $B(x_i,x_j) = a_{ij}$ e seja $\{y_1,\ldots,y_n\}$ base para V na qual $B(y_i,y_j) = b_{ij}$.

Seja $\sigma : \mathfrak{Q}K \longrightarrow \mathfrak{Q}L$ representação. Então $B(\sigma x_i,\sigma x_j) = a_{ij}$.

Seja ainda $\sigma x_i = z_i = \sum_\lambda t_{\lambda i} y_i$ e denotamos $T = (t_{\lambda i})$.

Então, $a_{ij} = B(z_i,z_j) = B(\sum_\lambda t_{\mu i} y_\mu, \sum_\mu t_{\mu i} y_\mu) = \sum_{\mu,\lambda} t_{\mu i}\, b_{\mu\lambda}\, t_{\lambda j}$ portanto, $M = T^t N T$.

Reciprocamente, se $M = T^t N T$ definamos $z_i = \sum_\mu t_{\mu i} y_\mu$. Então $B(z_i,z_j) = a_{ij}$. Seja σ uma transformação linear definida como $\sigma(x_i) = z_i$. Então $B(\sigma x_i, \sigma x_j) = B(x_i,x_j) = a_{ij}$. Logo σ é representação e temos **demonstrado.**

A demonstração de (2) é, com pequenas modificações, análoga à de (1). □

Consideremos o discriminante $d_B(x_1,\ldots,x_n)$ de uma base $\{x_1,\ldots,x_n\}$ para o látice L sobre V.

Como já observado na página 4, se for tomada outra base para L, digamos $\{x'_1,\ldots,x'_n\}$, a igualdade de $N' = T^t N T$ mostra que $d_B(x'_1,\ldots,x'_n) = d_B(x_1,\ldots,x_n)$.

(*) (Para esclarecimento dos símbolos usados para matrizes, ver página 3, Capítulo I).

Portanto a imagem canônica de $d_B(x_1,\ldots,x_n)$ independe da base de L e é chamada *discriminante de* L (notação: d_B L).

Se L consiste de um único ponto convencionamos $d_B L = 1$.

Sendo V espaço quadrático sobre $\mathbb{Q}$ e L,K lâtices sobre V, dizemos que K *e* L *estão na mesma classe* se $K = \sigma L$, onde σ é elemento de O(V).

Esta relação é de equivalência e denotamos cls L à classe de equivalência do lâtice L.

Chamamos $cls^+ L$ aos lâtices K tais que $K = \sigma L$ e $\sigma \in O^+(V)$, sendo K e L nas mesmas condições anteriores. Uma transformação σ está em $O^+(V)$ se $\det\sigma = +1$ e é dita neste caso *rotação*.

De forma análoga uma transformação σ pertence a $O^-(V)$ se $\det = -1$, e é dita *reflexão* neste caso. Definimos o *Grupo das Unidades de* L como o subgrupo $O(L) = \{ \in O(V) \mid \sigma L = L\}$.

Os lâtices K e L estão na mesma *classe própria* se existe $\sigma \in O^+(V)$ tal que $\sigma L = K$. Nas mesmas condições os lâtices estão no mesmo *gênero* se para cada p primo em Z existe $\sigma_p \in O(V_p)$ tal que $\sigma_p L_p = K_p$ (notação: K ∈ gen L), onde L_p e K_p são os completamentos p-ádicos dos lâtices L e K respectivamente. Como O(V) está imerso em $O(V_p)$ então se K ∈ cls L temos como consequência que K ∈ gen L.

Dado um espaço quadrático regular V o número de classes próprias de lâtices sobre V é finito. Em particular o número de classes próprias num gênero é finito. (vide [O], teorema 103.4).

3.2. DECOMPOSIÇÃO ORTOGONAL

Dizemos que o lâtice L é *soma direta* de sub-lâtices

$L_1, L_2, \ldots, L_r$ se todo x em L se escreve como $x = \sum_i x_i$, $x_i \in L_i$ de maneira única. (Notação: $L = L_1 \oplus L_2 \oplus L_3 \oplus \ldots \oplus L_r$.)

Se $B(L_i, L_j) = 0$, $1 \leq i, j \leq r$ dizemos que L possui *decomposição ortogonal*. (Notação: $L = L_1 \perp L_2 \perp \ldots \perp L_r$.)

Se $X_1, X_2, \ldots, X_r$ são lâtices de diferentes espaços quadráticos escrevemos $L \cong X_1 \perp X_2 \perp \ldots \perp X_r$ para significar que L tem decomposição $L = L_1 \perp L_2 \perp \ldots \perp L_r$ onde cada L_i é isométrico a X_i.

Com ligeira modificação da estrutura precedente, podemos afirmar que dados espaços quadráticos U e V sobre $\mathbb{Q}$ existe um espaço quadrático W tal que $W = U' \perp V$ onde $U' \cong U$. Dizemos neste caso que W é *construído a partir de* V *por adjunção de* U .

Como já definido, o radical de um lâtice é o conjunto expresso por $\text{Rad } L = \{x \in L \mid B(x,L) = 0\}$ e o lâtice é dito regular quando $\text{Rad } L = \{0\}$.

É facilmente visto, sob esta definição, que $\text{Rad } \mathbb{Q}L = \mathbb{Q} \cdot \text{Rad } L$, que Rad L é sub-lâtice do lâtice L e ainda que $\text{Rad } (L \perp K) = (\text{Rad } L) \perp (\text{Rad } K)$.

A seguinte proposição mostra que todo lâtice tem uma *decomposição radical*, isto é, existe algum outro lâtice que permite uma decomposição tendo como fator o radical do lâtice primitivo.

PROPOSIÇÃO 2: Todo lâtice L, nas condições assumidas, induz um lâtice K tal que $L = K \perp \text{Rad } L$, (sendo L lâtice sobre V).

DEMONSTRAÇÃO: Se L é regular, basta tomar K = L.

Suponhamos L não regular, e consideremos uma base para $\mathbb{Q}L$, $\{x_1,\ldots,x_r\ldots,x_n\}$, na qual os vetores $x_1,\ldots,x_r$ geram o radical de $\mathbb{Q}L$. Portanto, dim Rad $\mathbb{Q}L = r$.

Pelo teorema 5, capítulo 2, existe base $y_1,\ldots,y_n$ para $\mathbb{Q}L$ no qual $L = I_1y_1 +\ldots+ I_ny_n$ e Rad $\mathbb{Q}L = \mathbb{Q}y_1 +\ldots+ \mathbb{Q}y_r$. (a menos da ordem dos elementos da base, pois Rad $\mathbb{Q}L$ é subespaço de V).

Então Rad $L = L \cap$ Rad $\mathbb{Q}L = I_1y_1+\ldots+I_ry_r$.

Basta então considerar o lâtice $K = I_{r+1}y_{r+1}+\ldots+I_ny_n$ e conseguimos a decomposição desejada $L = K \perp$ Rad L. □

3.3. ESCALA, NORMA E VOLUME

Consideremos um lâtice L sobre o espaço quadrático V. Por *escala*, denotado sL, entendemos o Z-módulo gerado pelo subconjunto B(L,L) de $\mathbb{Q}$, ou seja, $sL = \{ \sum_{\text{finita}} B(x,y) \mid x,y \in L\}$. Desde que $L = Zz_1 + Zz_2 +\ldots+ Zz_n$ temos $sL \subseteq \left(\sum_{i,j} B(z_i,z_j)\right)Z$ de modo que sL é um ideal fracionário ou é nulo. Como $1 = B(z_i,z_i) \in sL$, então $Z \subset sL$.

Definimos *norma* , denotada nL, como o sub-módulo gerado pelo subconjunto Q(L) de $\mathbb{Q}$.

Como $Q(L) \subseteq B(L,L)$ então nL é também um ideal fracionário ou nulo.

Como para todo x,y em L tem-se $2B(x,y) = Q(x+y) - Q(x) - Q(y) \in nL$, daí $2sL \subseteq nL \subseteq sL$ de modo que nL é nulo se sL o for e vice-versa. É facilmente verificável também que se $L = J \perp K$ então $sL = sJ + sK$ e $nL = nJ + nK$.

Para um lâtice L não nulo definimos *volume* do lâtice L, sendo $L = I_1x_1 + I_2x_2 + \ldots + I_nx_n$, I_i ideais, como $vL = I_1^2 . I_2^2 \ldots I_n^2 . d(x_1,\ldots,x_n)$.

Naturalmente, se $K \subset L$, ambos lâtices, então $vK \subset vL$.

3.4. DUAL DE UM LÂTICE

Consideremos um lâtice L em V, sendo espaço quadrático, e suponhamos L regular.

Definimos o *dual de* L como $L^{\#} = \{x \in \mathbb{Q}L \mid B(x,L) \subseteq Z\}$.

Se L for o lâtice trivial, isto é, $L = \{0\}$, então $L^{\#} = \{0\}$.

Suponhamos L não trivial: então existem ideais $I_1, I_2, \ldots, I_r$ e uma base $\{x_1,\ldots,x_r\}$ para $\mathbb{Q}L$ tal que $L = I_1x_1 + \ldots + I_rx_r$. Afirmamos que nesse caso $L^{\#} = I_1^{-1} y_1 + \ldots + I_r^{-1} y_r$ onde $\{y_1,y_2,\ldots,y_r\}$ são vetores tais que $\{\emptyset(y_1),\ldots,\emptyset(y_n)\}$ é base do espaço dual V' (onde $\emptyset$ é aplicação definida na pág. 8, capítulo I).

Isso implica que $B(I_ix_i, I_j^{-1} y_j) = 0$ se $i \neq j$ e $B(I_ix_i, I_i^{-1} y_i) \subseteq Z$. Portanto, temos que $I_1^{-1} y_1 + \ldots + I_r^{-1} y_r \subseteq L^{\#}$.

Por outro lado, se tomarmos um vetor típico qualquer de $L^{\#}$, digamos $z = b_1y_1 + b_2y_2 + \ldots + b_ry_r$ teremos $B(b_iy_i, I_ix_i) = b_iI_i = B(z, I_ix_i) \subseteq B(z,L) \subseteq Z$, pela definição do dual de V.

Portanto, $b_i \in I_i^{-1}$ e temos estabelecida nossa afirmação; como consequências imediatas, temos $L^{\#\#} = L$, $vL^{\#} = (vL)^{-1}$ e $(L + K)^{\#} = L^{\#} \cap K^{\#}$.

3.5. LÂTICES MODULARES

Consideremos um lâtice L sobre o espaço quadrático V , $L = I_1x_1 + \ldots + I_rx_r$, onde I_i's são ideais fracionários. Se a escala de L for tal que $sL = I$, I ideal fracionário, e o volume de L for $vL = I^r$ chamaremos L de I-*modular*.

O lâtice será chamado de α-*modular* se for I-modular com $I = \alpha Z$, $\alpha \in Q$. Será chamado *unimodular* se for Z-modular.

As seguintes proposições esclarecerão a relação entre lâtices unimodulares e suas matrizes, bem como entre lâtices unimodulares e seus duais.

PROPOSIÇÃO 3: O lâtice L sobre o espaço quadrático V, com matriz M, é unimodular se e somente se M é uma matriz unimodular , ou seja, M é matriz inteira e $\det M = \pm 1$.

DEMONSTRAÇÃO: Seja $x_1,\ldots,x_r$ base para L, onde $L = Zx_1 + \ldots + Zx_r$, então $vL = Z\cdot(\det M)$.

Se L é unimodular, então todos os valores de $B(x_i,x_j)$ estão em Z já que $sL = Z$ portanto M é matriz inteira. Ainda mais, $(\det M)Z = Z$ portanto $\det M = \pm 1$, e M é unimodular.

Reciprocamente, sendo M unimodular, M é inteira e $sL = \sum_{\text{finita}} B(x_i,x_j)Z \subseteq Z$. Como $Z \subseteq sL$, necessariamente temos $sL = Z$,

Como $\det M = \pm 1$, $vL = Z$ e L é unimodular. □

PROPOSIÇÃO 4: Suponhamos L lâtice sobre o espaço quadrático V, L I-modular. Então,

$$L = \{x \in \mathbb{Q}L \mid B(x,L) \subseteq I\}.$$

DEMONSTRAÇÃO: Se L é I-modular, temos $B(L,L) \subseteq sL = I$ e então $L \subseteq \{x \in \mathbb{Q}L \mid B(x,L) \subseteq I\}$.

Por outro, seja $x \in \mathbb{Q}L$ tal que $B(x,L) \subseteq I$.

Como o lâtice é I-modular, $B(L,I^{-1}L) \subseteq Z$ e então $I^{-1}L \subseteq L$.

Como $(v(L))^2 = I^{2r}$, então $(v(L))^{-1} = I^{-2r}(v(L)) = I^{-r}$. Mas $v(I^{-1}L) = I^{-2r}(v(L))$ e portanto $v(I^{-1}L) = (v(L))^{-1} = v(L^{\#})$. Como $I^{-1}L \subseteq L$, se tivéssemos $I^{-1}L \subset L^{\#}$, teríamos $v(I^{-1}L) \subset v(L^{\#})$, o que não ocorre. Logo, $I^{-1}L = L^{\#}$.

Tomando $B(x,L^{\#}) = B(x,I^{-1}L) \subseteq Z$, verificamos que $x \in L^{\#\#}$, pela definição de dual do lâtice, e então $x \in L$. □

A proposição 4 apresenta como corolário o fato de que L é unimodular somente quando $L^{\#} = L$.

3.6. A FATORAÇÃO INDECOMPONÍVEL DE UM LÂTICE-LÂTICES PARES E IMPARES.

Dado um lâtice L, existe base $\{x_1,\ldots,x_n\}$ para $\mathbb{Q}L$ tal que $L = Zx_1 + \ldots + Zx_n$, como já foi visto. O número de vetores da base de $\mathbb{Q}L$ é chamado *rank de* L.

Dizemos que L é *decomponível* se existem lâtices K_1 e K_2 em V contidos em L tal que $L = K_1 \perp K_2$.

Caso contrário chamamo-lo *indecomponível*.

É claro que todo lâtice é a soma ortogonal de no máximo n componentes, onde n é o rank de L. A tal decomposição damos o nome

de *fatoração indecomponível*. Dizemos que a forma quadrática Q é *definida positiva* se $Q(x) > 0$, $x \neq 0$; *definida negativa* se $Q(x) < 0$, $x \neq 0$, $x \in V$. Se L é lática sobre V, $x \in L$, então $Q(x) \in Z$.

TEOREMA 5: Seja L um lático sobre o espaço quadrático regular (V,Q) sobre os racionais. Suponhamos que a forma quadrática Q seja definida (positiva ou negativa). Então os componentes $L_1,\ldots,L_r$ de uma fatoração indecomponível são únicos, a menos da ordem.

DEMONSTRAÇÃO:

Temos que $Q(x)$ é inteiro, e $|Q(x)|$ é um número natural. Dizemos que $x \in L$ é *redutível* se existem vetores não nulos y e z em L tal que $x = y + z$ e $B(y,z) = 0$. O vetor x será chamado de *irredutível* se não for redutível.

Mostraremos que todo vetor em L é a soma de vetores irredutíveis de L.

Primeiramente consideremos a soma y+z de vetores não nulos y e z de V tal que $B(y,z) = 0$.

Então $Q(y+z) = Q(y) + Q(z)$, e como a forma quadrática é definida positiva ou negativa, Q(y) e Q(z) são ambos positivos ou negativos de modo que $|Q(y+z)| \geq |Q(y)|$.

A prova de que todo vetor x em L é a soma de vetores irredutíveis é dada por indução sobre o número natural $n = |Q(x)|$.

Se $|Q(x)| = 1$, então x é irredutível, pois se existirem vetores y e z não nulos em L tal que $x = y+z$ e $B(y,z) = 0$, teríamos $1 = |Q(x)| = |Q(y+z)| \geq |Q(y)|$ e $1 = |Q(y+z)| \geq |Q(z)|$, e se ambos forem positivos teremos $Q(y+z) = 2$, ou se ambos forem ne-

gativos teremos $Q(y+z) = -2$.

Suponhamos que y seja a soma de irredutíveis se $n-1 = |Q(y)|$, $n > 1$. Seja x com $n = |Q(x)|$. Se x é irredutível, está provado.

Se x for redutível, basta escrever $x = y + z$, y e z em L e $1 \leq |Q(y)| \leq n-1$, $1 \leq |Q(z)| \leq n-1$ e por hipótese de indução, y e z são soma de irredutíveis, logo x também é.

Em segundo lugar, seja a relação de equivalência $x \sim y$ no conjunto dos vetores irredutíveis não nulos de L definida como $x \sim y$ se existem vetores irredutiveis tais que
$x = z_1, z_2, \ldots, z_q = y$ $(q \geq 1)$ com $B(z_i, z_{i+1}) \neq 0$ para $1 \leq i \leq q-1$.

Sejam $C_1, C_2, \ldots, C_t$ as classes de equivalência associadas com esta relação.

Sejam $K_1, K_2, \ldots, K_t$ os sub-látices em L gerados respectivamente pelos vetores em $C_1, C_2, \ldots, C_t$.

Como $B(C_i, C_j) = 0$ para $i \neq j$ então $B(K_i, K_j) = 0$ para $i \neq j$, portanto a soma dos látices $K_1, K_2, \ldots, K_t$ é uma soma ortogonal, $K_1 \perp K_2 \perp \ldots \perp K_t$.

Como na primeira parte mostramos que todo vetor em L é a soma de vetores irredutíveis em L, então $L = K_1 \perp K_2 \perp \ldots \perp K_t$.

Seja $L = L_1 \perp \ldots \perp L_r$ outra decomposição e $x \in C_1$. Então $x \in L = L_1 \perp \ldots \perp L_r$ e como x é irredutível, x está em uma só componente desta fatoração, digamos $x \in L_1$.

Da definição da relação de equivalência segue que $C_1 \subseteq L_1$, portanto $K_1 \subseteq L_1$.

Da mesma forma segue-se que cada K_i está contido em algum L_j, e como $L = K_1 \perp \ldots \perp K_t$, cada L_j é a soma ortogonal de todos os K_i contidos nele. Mas como L_j é indecomponível, cada L_j é exatamente algum K_i, e a fatoração é portanto única. □

Dizemos que o lâtice L é *par* se $Q(L) = B(L,L) \subseteq Z$.

O lâtice L será chamado *ímpar* caso contrário.

CAPÍTULO IV

A CLASSIFICAÇÃO DAS CLASSES DE FORMAS QUADRÁTICAS DEFINIDAS

Assumiremos que existe pelo menos um lâtice unimodular sobre V, onde V representa um espaço quadrático n-ário. Tratando-se de lâtices unimodulares sobre Z, seu discriminante poderá ser + 1 ou - 1.

Assumiremos os lâtices *unimodulares positivos definidos*, isto é, o discriminante em questão só poderá assumir valor + 1.

O símbolo I_n denotará a matriz identidade nxn.

Dois lâtices são *adjacentes* se satisfazem a condição definida no §4.1.

O objetivo do presente capítulo é determinar as diferentes classes de lâtices unimodulares positivos definidos. Começando com um lâtice particular, as classes ficarão completamente determinadas no processo da procura sucessiva dos lâtices adjacentes a menos de isomorfismos. (ver introdução)

As proposições e teoremas demonstrados neste capítulo terão por finalidade estabelecer os métodos de construção de todos os possíveis lâtices adjacentes a um lâtice dado.

Assumiremos o método referenciado por Martin Kneser (vide bibliografia) reportando-o à obra [O] tanto quanto possível.

4.1. LÂTICES ADJACENTES

Sendo K e L lâtices unimodulares sobre V, dizemos que K *é adjacente a* L se os fatores invariantes de K em L são da forma $\frac{1}{2}Z, Z, \ldots, Z, 2Z$.

Decorre imediatamente desta definição e da definição de fatores invariantes que existe uma base $\{x_1, \ldots, x_n\}$ para V na qual $L = Zx_1 + \ldots + Zx_n$ e $K = (\frac{1}{2}Z)x_1 + \ldots + (2Z)x_n$. Uma definição equivalente é que o lâtice K é adjacente ao lâtice L se o índice de $L \cap K$ é 2 em L e em K, isto é, $[K: L \cap K] = 2$ e $[L: L \cap K] = 2$. De fato, sendo L e K como acima, $L \cap K = Zx_1 + \ldots + (2Z)x_n$ e $[K: L \cap K] = [L: L \cap K] = 2$. Isto por que se $L = a_1Zx_1 + \ldots + a_nZx_n$, $K = b_1Zx_1 + \ldots + b_nZx_n$, então $L \cap K = c_1Zx_1 + \ldots + c_nZx_n$ onde $c_i = mmc\ (a_i, b_i)$.

Se $[K: L \cap K] = 2$ e $[L: L \cap K] = 2$, pelo teorema 6, Capítulo II, existe base $\{x_1, \ldots, x_n\}$ para V tal que $L = Zx_1 + \ldots + Zx_n$. Sendo $K = b_1Zx_1 + \ldots + b_nZx_n$, temos $L \cap K = c_1Zx_1 + \ldots + c_nZx_n$ onde $c_iZ = Z \cap b_iZ$.

Portanto, $c_i = p_i$ se $b_i = \frac{p_i}{q_i}$.

Como $[L: L \cap K] = 2 = p_1 \cdot p_2 \cdots p_n$, temos $p_j = 2$ e $p_i = 1$ se $i \neq j$.

Dessa forma, a menos da ordem, temos $b_1 = \frac{2}{q_1}$ e $b_i = \frac{1}{q_i}$ se $i \neq 1$. Como K é unimodular, $v(K) = Z = (\frac{4}{q_1^2} \cdot \frac{1}{q_2^2} \cdots \frac{1}{q_n^2})Z$, logo $q_r = 2$, para algum r, e $q_i = 1$ para $i \neq r$. Pelo fato de $[K: L \cap K] = 2$, $q_r \neq q_1$.

Portanto temos $b_1 = 2$, $b_2 = 1, \ldots, b_{n-1} = 1$, $b_n = \frac{1}{2}$ (a menos da ordem) e $K = 2Zx_1 + Zx_2 + \ldots + Zx_{n-1} + \frac{1}{2}Zx_n$.

OBSERVAÇÃO: Decorre da definição de lâtices adjacentes que se K é adjacente a L, então $2L \subseteq K \subseteq \frac{1}{2}L$. Portanto, o número de lâtices adjacentes ao lâtice L é finito se o índice $[\frac{1}{2} L : L]$ for finito.

Para demonstrar que o índice $[\frac{1}{2} L : 2L]$ é finito, basta tomar um vetor y qualquer pertencente a $\frac{1}{2} L$, digamos $y = \sum_{i=1}^{n} a_i \frac{1}{2} x_i$, onde $a_i = 4t_i + r_i$, $0 \leq r_i < 4$ $(a_i \in Z)$.

Teremos $y = 2(\sum_{1}^{n} t_i x_i) + \sum_{1}^{n} \frac{r_i}{2} x_i$, onde $r_i \in \{0,1,2,3\}$.

Como o vetor $2(\sum_{1}^{n} t_i x_i)$ pertence a 2L, o número de classes laterais é menor ou igual ao número de vetores do tipo $\sum_{1}^{n} \frac{r_i}{2} x_i$ que é finito.

4.2. DESCRIÇÃO DO PROCESSO

Seja L lâtice unimodular com respeito a Z sobre o espaço quadrático V, com matriz I_n, sobre $\mathbb{Q}$. Definimos $\mathcal{J}(L)$ como sendo o conjunto de todos os lâtices unimodulares K com respeito a Z sobre V tal que $K_p = L_p$ para p = 3,5,7... .

Assumiremos sem demonstração o resultado seguinte, (vide [O]):

PROPOSIÇÃO 1: Seja $n \geq 5$ e L e K lâtices unimodulares sobre o espaço V em discussão. Então existe lâtice J pertencente a $clas^{+}K$ tal que J está em $\mathcal{J}(L)$.

Para determinar as classes unimodulares em V começamos com um lâtice fixo $D \cong \langle 1 \rangle \perp \ldots \perp \langle 1 \rangle$ sobre V.

Como o número de classes próprias de lâtices sobre V é finito (vide capítulo 3, ítem 3.1) digamos $clas^{+}K_1$, $clas^{+}K_2$,...,$clas^{+}K_t$

e pela proposição 1 existem $K_1, K_2, \ldots, K_t \in \mathcal{F}(D)$, a menos da troca de representantes de classe, o problema será determinar os lâtices $K_1, \ldots, K_t$.

Para conseguir os lâtices $K_1, \ldots, K_t$ iremos calcular passo a passo, construindo em primeiro lugar os adjacentes a D, (que são finitos) depois os adjacentes a estes, etc. A proposição 2 mostra que procedendo dessa maneira obteremos os lâtices $K_1, \ldots, K_t$ entre todos os lâtices.

PROPOSIÇÃO 2: Para $n \geq 2$, sendo K e L dois quaisquer lâtices unimodulares sobre o espaço V em discussão, com $K \in \mathcal{F}(L)$, $K \neq L$, existe uma cadeia finita de lâtices unimodulares $L = J_1, J_2, \ldots, J_t = K$ com J_{i+1} adjacente a J_i.

DEMONSTRAÇÃO: Como $K \in \mathcal{F}(L)$, existe uma base para o espaço vetorial V tal que $L = Ze_1 + \ldots + Ze_n$, $K = 2^{a_1} Ze_1 + \ldots + 2^{a_n} Ze_n$, com $a_1 \leq a_2 \leq \ldots \leq a_n$ pois $K_p = L_p$, p primo, $p \neq 2$ e $\sum_{i=1}^{n} a_i = 0$ já que K é unimodular.

Suponhamos que a base esteja ordenada de tal maneira que $a_1, a_2, \ldots, a_s < 0$, $a_{s+1}, \ldots, a_t = 0$ e $a_{t+1}, \ldots, a_n > 0$.

Seja $A = \{(x_1, \ldots, x_n) \in \mathbb{N}^n \mid x_1 \leq \ldots \leq x_n \text{ e } \sum_{i=1}^{n} x_i = 0\}$

Seja $f: A \to A$ definido como

$$f(x_1, \ldots, x_n) = (x_1, \ldots, x_s+1, \ldots, x_t, x_{t+1}-1, \ldots, x_n) \quad \text{onde}$$

$$s = \sup \{i \mid x_i < 0\} \quad e$$

$$t = \inf \{j \mid x_j > 0\}$$

$f(0,\ldots,0) = (0,\ldots,0)$.

Podemos chamar $J_1 = K$, $J_2 = f(J_1)$ onde $f(K)$ representa o resultado da aplicação f sobre os expoentes da formulação J_1.

Dessa forma temos $J_2 = 2^{a_1}Ze_1+\ldots 2.2^{a_s}Ze_s\ldots+\frac{2^{a_{t+1}}}{2}Ze_{t+1}+$ $+\ldots 2^{a_n}Ze_n$ e $[J_1: J_1 \cap J_2] = 2$, $[J_2: J_1 \cap J_2] = 2$ portanto J_2 é adjacente a J_1, (pela definição de lâtices adjacentes).

De maneira semelhante, fazendo $f(J_i) = J_{i+1}$ teremos $[J_i : J_i \cap J_{i+1}] = 2$ e $[J_{i+1} : J_i \cap J_{i+1}] = 2$.

Como o processo é finito e termina quando todos os expoentes forem nulos, existe índice t tal que $f(J_{t-1})=J_t=L$ e portanto existe a cadeia finita de lâtices adjacentes ligando K a L.□

4.3. REGRAS DE CONSTRUÇÃO

As proposições e teoremas demonstrados nesse ítem constituirão um método para construir todos os lâtices unimodulares adjacentes ao lâtice K, sendo K unimodular.

PROPOSIÇÃO 3: As seguintes afirmações são equivalentes:

(i) K é adjacente a L

(ii) $v(K+L) = \frac{1}{4} Z$

(iii) $v(K \cap L) = 4 Z$

DEMONSTRAÇÃO:

[(i) → (ii)] Se K é adjacente a L, foi visto que existe base $\{x_1,\ldots,x_n\}$ para V tal que $L = Zx_1 + Zx_2 + \ldots Zx_n$ e $K = \frac{1}{2} Zx_1 + \ldots + 2Zx_n$ e $L + K = \frac{1}{2} Zx_1 + Zx_2 + \ldots + Zx_n$. Portanto, $v(L + K) = (\frac{1}{2} Z)^2 \; Z^2 \ldots . Z^2 = \frac{1}{4} Z$.

[(ii) → (iii)].

Como L e K são unimodulares, $L^{\#} = L$ e $K^{\#} = K$. Então $v(K \cap L) = v(K^{\#} \cap L^{\#}) = v((K+L)^{\#}) = 4 Z$.

[(iii) → (i)] De acordo com o teorema dos fatores invariantes existe uma base $\{x_1,\ldots,x_n\}$ para V onde $L = Zx_1 + \ldots + Zx_n$ e $K = ZR_1 x_1 + \ldots + ZR_n x_n$ sendo R_i ideais fracionários.

Se $v(L \cap K) = 4\,Z$, então $v(L^{\#} \cap K^{\#}) = v((K + L)^{\#}) = 4\,Z$ e $v(K + L) = \frac{1}{4}\,Z$, sendo L e K unimodulares.

Como $R_1 \supseteq R_2 \supseteq \ldots \supseteq R_n$, seja i tal que $R_j \supset Z$, $j \geq i$ e $R_j \subseteq Z$, $j < i$. Desse modo $L+K = R_1x_1 + \ldots + R_ix_i + Zx_{i+1} + \ldots + Zx_n$ e $L \cap K = Zx_1 + \ldots + Zx_i + R_{i+1}x_{i+1} + \ldots + R_nx_n$.

Como $v(L+K) = R_1^2 \ldots R_i^2 Z = \frac{1}{4}\,Z$, existe j tal que $R_j = \frac{1}{2}\,Z$ e os outros ideais serão iguais a Z.

Como $v(L \cap K) = Z.\ R_{i+1}^2 \ldots R_n^2 = 4Z$, existe m tal que $R_m = 2Z$, e outros ideais também serão iguais á Z. Sendo $R_1 \supseteq R_2 \supseteq \ldots \supseteq R_n$, teremos $R_1 = \frac{1}{2}\,Z$, $R_2 = Z, \ldots, R_{n-1} = Z$, $R_n = 2Z$ e então K é adjacente a L.

PROPOSIÇÃO 4: Sejam lâtices K e L tais que K é adjacente a L e $y \in L-K$. Então valem as seguintes igualdades:

(i) $L+K = Zy+K$

(ii) $L = Zy + (L \cap K)$

(iii) $L \cap K = (Zy+K)^{\#} = \{\omega \in K \mid B(\ ,y) \in Z$

DEMONSTRAÇÃO:

(i) temos $K \subset Zy + K \subseteq L+K$. Pela proposição 3, porém, não há nenhum lâtice propriamente contido entre K e L+K, desde que o volume de K é Z e o volume de L+K é $\frac{1}{4}\,Z$.

Portanto, $Zy + K = L + K$.

(ii) temos $L \cap K \subset Zy + (L \cap K) \subseteq L$.

Pelo mesmo argumento do ítem (i), usando a proposição 3, não há lâtices contidos propriamente entre $L \cap K$ e L.

Portanto $Zy + (L \cap K) = L$.

(iii) Desde que L e K estão sendo assumidos como unimodulares, temos: $L \cap K = L^{\#} \cap K^{\#} = (L + K)^{\#} = (Zy + K)^{\#}$. A segunda igualdade segue da definição do dual de $Zy + K$; desde que $(Zy + K)^{\#} =$

$= \{x \in Q(Zy + K) \mid B(x, Zy + K) \subseteq Z\}$ então $(Zy+K)^{\#} = \{\omega \in K \mid B(\omega, y) \in Z\}$.

TEOREMA 5: Seja $y \in \frac{1}{2} K - K$ com $Q(y) \in Z$. Então existe exatamente um lâtice unimodular J sobre V que contêm y e é adjacente a K. Este lâtice é $J = Zy + (Zy + K)^{\#}$.

DEMONSTRAÇÃO:

Pela proposição 4, se o lâtice J existe, então tem a forma $J = Zy + (Zy + K)^{\#}$ porque nesse caso $y \in J$ e $y \notin K$, e isto prova também a unicidade.

Para mostrarmos que o lâtice realmente existe, será suficiente definir um lâtice desta forma e provar que é unimodular e adjacente a K.

O lâtice $J = Zy + (Zy + K)^{\#}$ é unimodular, pois $B(J,J) \subseteq Z$ logo $s(J) \subseteq Z$. (ver § 3.3)

Se escrevermos $K = Z\omega + Zx_2 + \ldots + Zx_n$ com $2y = m\omega$, $m \in$ $\in Z$ teremos $Zy + K = Z(\omega + y) + Zx_2 + \ldots + Zx_n$.

A igualdade $2y = m\omega$ implica $y = \frac{m}{2} \omega$ e $Z(\omega+y) \subseteq Z(\frac{1}{2} \omega)$ portanto $Zy + K \subseteq Z(\frac{1}{2} \omega) + Zx_2 + \ldots + Zx_n$ de modo que $Z\, v(2y+K) \subseteq$ $\subseteq \frac{1}{4} Z$. (Observar que o volume do lâtice é sempre um ideal quadrático).

Portanto, $v(Zy + K) = \frac{1}{4} Z$ e $v((Zy + K)^{\#}) = 4Z$.

Como $y \notin K = K^{\#}$, então $y \notin (Zy + K)^{\#}$.

Portanto, $v((Zy + K)^{\#}) \subsetneq v(J) \subseteq Z$

ou $4Z \subset v(J) \subseteq Z$ portanto $v(J) = Z$ e J é unimodular.

Desde que $(Zy + K)^{\#} = (Zy)^{\#} \cap K^{\#} = Zy \cap K \subseteq J \cap K$ temos $v((Zy + K)^{\#}) \subseteq v(J \cap K) \subset Z$ que implica $4Z \subseteq v(J \cap K) \subset Z$ logo $v(J \cap K) = 4Z$ e J é adjacente a K pela proposição 3. □

PROPOSIÇÃO 6: Suponhamos o látice K adjacente ao látice L, y um vetor de L-K, z um vetor qualquer de V. Então y+z está em L-K se e somente se z está em $L \cap K = \{\omega \in K \mid B(\omega,y) \in Z\}$.

DEMONSTRAÇÃO. Suponhamos $y+z \in L-K$.

Pela proposição 4, $L + K = Zy + K$ e $[L + K : K] =$

$= [Zy + K : K] = 2$ ou seja, so há dois elementos no quociente, a saber, K e y+K.

Como $y+z \in L-K$, $(y+z) + K = y + K$ e $z \in K$.

Como $y + z \in L$, $y \in L$ então $z \in L$.

Portanto, $z \in L \cap K$. A igualdade segue da proposição 4 e a recíproca é óbvia. □

PROPOSIÇÃO 7: Sejam L e L' látices unimodulares adjacentes a K e $y \in L-K$, $y' \in L'-K$ vetores quaisquer. Então L=L'se e somente se $y - y' \in K$ e $B(y,y') \in Z$.

DEMONSTRAÇÃO:

Suponhamos que $L=L'$. Pela proposição 6, como $y+(y'-y)=y' \in L-K$ temos $B(y'-y,y)\ Z$. Logo, $B(y',y)-B(y,y) \in Z$. Como os lâtices são unimodulares, $B(y,y) \in Z$.

Portanto, $B(y',y) \in Z$. Pela mesma proposição 6, $y-y' \in L \cap K$ e $y-y' \in K$.

Por outro lado, se $y-y' \in K$ com $B(y,y') \in Z$ então $y-y'\ L \cap K$ o que implica que $y-y' \in L$ e $-(y-y')+y \in L$, portanto $y' \in L$ para todo $y' \in L'$, ou seja, $L' \subset L$. Um argumento análogo mostra que $L \subset L'$ e então $L' = L$. □

A partir destas proposições e da observação do §4.1 conseguimos um método para construir todos os lâtices unimodulares adjacentes ao lâtice K.

O método consiste do seguinte:

(i) O teorema 5 do § 4.3 mostra que a cada $y \in \frac{1}{2} K-K$ com $B(y,y) \in Z$ existe exatamente um lâtice L adjacente a K que contém y. A própria demonstração do teorema 5 esclarece que, se $y \in \frac{1}{2} K$ e $y \in K$, o lâtice $J = Zy + (Zy + K)^{\#}$ será igual K.

(ii) A observação de §4.1 assegura que o número de lâtices adjacentes ao lâtice K é menor ou igual ao número de classes laterais de $\frac{1}{2} K/2K$.

(iii) Se $y,z \in \frac{1}{2} K-K$ são côngruos módulo 2K, isto é, $y-z \in 2K$, os lâtices obtidos a partir deles serão iguais. Isso ocorre porque se $y-z \in 2K$, então $z=y+2a$, $a \in K$. Sendo $L=Zy+(Zy+K)^{\#}$ e $L'=Zz+(Zz+K)^{\#}$ os lâtices adjacentes obtidos, verificamos que $y \in L-K$, $z \in L'-K$, $y-z \in K$ e $B(y,z)=B(y,y+2a)=B(y,y)+2B(y,a)=B(y,y)+B(2y,a) \in Z$, pois K é unimodular. Portanto, pela proposição 7, $L = L'$.

(iv) Concluímos, então, pelos ítens anteriores, que se tomarmos um conjunto completo de representantes de $\frac{1}{2} K$ módulo 2K obteremos através deles todos os lâtices adjacentes ao lâtice K.

Pelo ítem (i) eliminaremos desse conjunto os vetores que estão em K e todos os vetores cuja forma quadrática não é inteira. Sendo $y_1, y_2, \ldots, y_r$ os remanescentes, formamos os lâtices $L_i=Zy_i+(Zy_i+K)^{\#}$ para $1 \leq i \leq r$.

Este procedimento nos dá então todos os lâtices unimodulares adjacentes a K e os casos de duplicação, por exemplo $L_i=L_j$, ocorrerão quando e somente quando y_i-y_j esteja em K com $B(y_i,y_j)$ inteiro.

O próximo teorema mostra uma condição para que dois lâtices adjacentes estejam na mesma classe, com o que completamos o processo de classificação das clas ses:

TEOREMA 8: Suponhamos K adjacente a L e y um vetor de L-K com a forma $y=\omega+z$ tal que $Q(\omega)=1$, $z\in K$ e $B(y,\omega)\in \frac{1}{2}\,Z-Z$.

Então clas L = clas K.

DEMONSTRAÇÃO: Consideremos a simetria $\tau x=x-2B(x,\omega)\,\omega$ para todo $x \in V$. De acordo com a proposição 6, como $\omega \in L-K$, (caso contrário $y=\omega+z\in K$) temos que $\omega+z\in L-K$ se e somente se $z \in L \cap K$.

Temos que $2z=2y-2\omega \in L\cap K$. Como $B(y,\omega)\in \frac{1}{2}\,Z-Z$, então $2B(y,\omega)=m$ é impar e $\tau y=y-m\,=\omega(y-\omega)-(m-1)\,\omega = z-(m-1)\,\omega$. Pela razão de $(m-1)$ ser par, e como $2y-2z=2\omega \in L\cap K$, deduzimos imediatamente $(m-1)\,\omega\in K$ e daí que $\tau y\in K$.

Por outro lado, para cada $x\in L\cap K$ temos $B(x,\omega)=B(x,y)-B(x,z)\in Z$ de forma que τx é um elemento de $L \cap K$.

Considerando que $L=Zy+(L\cap K)$, obtemos $\tau L \subseteq K$, e pela igualdade de dimensões $\tau L=K$; portanto pertencem à mesma classe . □

4.4. A MATRIZ $\emptyset^n$ (n = 8, 12, 16,...)

Utilizaremos o processo desenvolvido no parágrafo anterior na caracte rização de uma classe particular.

Através deste parágrafo assumiremos que a dimensão n do espaço V em discussão é 8, 12, 16,... .

Seja D um lâtice unimodular sobre V completamente decomponível: fixe- mos para ele uma base tal que $D=Zx_1 \perp Zx_2 \perp \ldots \perp Zx_n$.

Mostraremos que há sempre um lâtice unimodular indecomponível adjacente a D, que todos os tais lâtices estão na mesma classe própria e que todos tem matriz

$$\phi_n = \left(\begin{array}{cc|c} \frac{n}{4} & 1 & \bigcirc \\ 1 & 4 & 2 \\ \hline \bigcirc & 2 & T_{n-2} \end{array}\right)$$

onde T_m é a matriz .

$$T_m = \begin{pmatrix} 2 & 1 & \bigcirc & & \\ 1 & 2 & 1 & & \\ \bigcirc & 1 & 2 & \ddots & 1 \\ & & \ddots & \ddots & \\ & & & 1 & 2 \end{pmatrix}$$

Consideremos o vetor $y = \frac{1}{2}(x_1+\ldots+x_n)$. Então y está em $\frac{1}{2}D - D$, e $Q(y) \in Z$ desde que $n \equiv 0 \bmod 4$.

Pelo teorema 5 existe exatamente um lâtice unimodular E sobre V que contém y e é adjacente a D. Consideremos uma nova formulação de D, ou seja, $D = Z(2y) + Z(x_2) + Z(x_3-x_2)+\ldots+ Z(x_n - x_{n-1})$ e um lâtice adjacente a D será $X = Zy + Z(2x_2) + Z(x_3-x_2) +\ldots+ +\ldots+ Z(x_n-x_{n-1})$ porque para passar de D a X foi multiplicada a decomposição pelos ideais $\frac{1}{2}Z$, $2Z$, $Z,\ldots,Z$. (termo a termo).

Como $y \in X$, e pela unicidade, concluimos que $X = E$.

A matriz de E na base $\{y, 2x_2, -(x_3-x_2), (x_4-x_3),\ldots, ,\ldots,(x_n - x_{n-1})\}$ é a matriz $N = (B(x_i,x_j))$ onde x_i e x_j são veto-

res da base referida. Uma inspeção simples mostra que $N = \emptyset_n$.

O seguinte teorema proporciona uma descriçao dos vetores de E:

LEMA 9: E contêm vetores $\sum_{i=1}^{n} A_i x_i$ se e somente se $A_i \in \frac{1}{2} Z$, $A_i - A_j \in Z$, $\sum_{i=1}^{n} A_i \in 2Z$ para $1 \leq i \leq n$ e $1 \leq j \leq n$.

DEMONSTRAÇÃO: Consideremos o vetor $x = \sum_{i=1}^{n} A_i x_i$. Se $x \in E$ então $x \in \frac{1}{2} D$, logo todo A_i está em $\frac{1}{2} Z$.

Como $E = Zy + (Zy + D)^{\#}$ todos os $x_i - x_j$ estão em $(Zy + D)^{\#} \subseteq E$ e $B(x, x_i - x_j) \in Z$, portanto $B(x, x_i - x_j) = A_i - A_j \in Z$.

Do fato de $B(x,y) \in Z$ concluímos $\frac{1}{2} \sum_{i=1}^{n} A_i \in Z$.

Reciprocamente, se algum A_i está em $\frac{1}{2} Z - Z$ então todos estão porque $A_i - A_j \in Z$. Nesse caso trocamos x por x+y e todos os A_i estão em Z.

Podemos portanto assumir que todos os A_i estão em Z. Teremos ainda que $\sum_{i=1}^{n} A_i \in Z$ e $x = \sum_{i=1}^{n} A_i x_i$ está em D e tem a propriedade $B(x,y) \in Z$.

Pela proposição 4, $x \in D \cap E \subseteq E$. □

O lema acima pode ser usado para mostrar que E não representa 1. Suponhamos $\sum_{i=1}^{n} A_i^2 = 1$ com $x = \sum_{1}^{n} A_i x_i \in E$. Se algum $A_i \in Z$, todos os outros estão e teremos, a menos da ordem, $A_1 = \pm 1$ e $A_2 = A_3 = \ldots = A_n = 0$ mas nesse caso $\sum_{1}^{n} A_i \notin 2Z$, contrariando o

o lema 9.

Por outro lado, se cada $A_i \in \frac{1}{2}Z - Z$, então $A_1^2 + A_2^2 + \ldots + A_n^2 \geq \frac{n}{4} \geq 2$ (pois $n = 8, 12, 16, \ldots$) e então E não representa 1.

Mostraremos a seguir que E é indecomponível e que todo lá tice unimodular E' adjacente a D está na mesma classe própria de E.

Consideremos os vetores $x_2 - x_1, x_3 - x_2, \ldots, x_n - x_{n-1}, x_1 + x_n$ em E e denotando-os respectivamente por $y_1, y_2, \ldots, y_n$ temos que $Q(y_i) = 2$. Como E não representa 1, os vetores y_i são irredutíveis (ver teorema 5) pois se $y_i = a+b$ com $B(a,b)=0$, teríamos $2 = B(y_i, y_i) = B(a,a) + B(b,b)$, e sendo a forma quadrática positiva definida, $B(a,a) = 1$ e $B(b,b) = 1$, o que não ocorre.

Como $B(y_i, y_{i+1}) \neq 0$ para todo i, tais vetores irredutí — veis são equivalentes e portanto pertencem à mesma componente da decomposição de E, cuja dimensão é n. Logo, E é indecomponível já que esta componente é única.

Para mostrar que os adjacentes E' indecomponíveis estão na mesma classe própria de E, consideremos $y' = \frac{1}{2}(a_1 x_1 + \ldots + a_n x_n)\, a_i \in Z$, $y' \in E' - D$.

Se algum a_i for par, então $x_i \in E' \cap D \subseteq E'$ pela proposição 4 e E' poderia ser decomposto por Zx_i, pois, pelo teorema 5, § 3.6, x_i é irredutível e não é equivalente aos demais irredutíveis de E'.

Fazendo escolhas de sinais adequados, podemos escrever $a_i = \delta_i . 1 - 4b_i$, $b_i \in Z$ para $1 \leq i \leq n$, onde $\delta_i = \pm 1$.

Consideremos $z = 2(b_1 x_1 + \ldots + b_n x_n) \in D \cap E'$ pois $B(y', z) \in Z$

(Proposição 4). Então $y'+z=\frac{1}{2}(\pm x_1 \ldots \pm x_n)$ está também em E'-D(Proposição 6).Consideremos a isometria $\sigma \in O_n(V)$ definida pelas equações $\sigma x_i = \delta_i x_i$, $1 \leq i \leq n$.

Então $\sigma y = y' + z$ e $\sigma D = D$.

Portanto, o lâtice σE é unimodular, adjacente a $\sigma D=D$ e $\sigma y = y' + z \in \sigma E$.

Pela proposição 7, $y' \in E'-D$, $y' + z \in \sigma E-D$ ainda $(y'+z) - y'=z \in D$ com $B(y',y'+z)=B(\frac{1}{2}(a_1x_1+\ldots+a_nx_n),\pm x_1 \pm x_2 \pm \ldots \pm x_n) = \frac{1}{2}(\pm n - \sum_1^n b_i)$ está em Z, já que $n \equiv 0 \bmod 4$, portanto $\sigma E = E'$. □

4.5. O MÉTODO DE M.KNESER

Neste parágrafo apresentaremos o método mencionado por M. Kneser em "Klassenzahlen Definiter Quadratischer Formen" para construção e classificação de lâtices adjacentes. ([K])

Tanto quanto possível as demonstrações das regras de construção,proposições e teoremas de [K] serão relacionados com resultados anteriores, constituindo nesse sentido, uma ligação entre resultados de [O] e [K].

Os novos resultados concorrerão para realizar a classificação das formas quadráticas em dimensões menores ou iguais a 16.

As regras de construção dos lâtices adjacentes são as seguintes em [K]:

REGRA 1:Seja $x \in \frac{1}{2}I-I, B(x,x) \in Z, K=\{y \in I \mid B(x,y) \in Z\}$ onde I é lâtice unimodular, então $L=K+Zx$ é adjacente a I e assim se conseguem todos os adjacentes a I.

DEM: Proposição 4 e ítens (i),(ii),(iii) e (iv) do método descrito no § 4.3. □

NOTA: No texto original ([K]) nesta Regra não aparece a restrição $x \notin I$. Porém, como já vimos, se $x \in I$, o lâtice adjacente obtido a partir de I é o próprio I.

REGRA 2: $x' \in \frac{1}{2} I$ fornece exatamente o mesmo látice que x se $x' - x \in K$, onde K é o conjunto descrito acima, e $B(x,y) \in Z$ onde $x' = x + y$.

DEM: Proposição 7. □

REGRA 3: Se x e x' são elementos conjugados sob o grupo das unidades de I, somente um deles precisa ser examinado pois os dois látices produzidos a partir deles são isomorfos. (*)

DEM: Sejam $x_1, x_2 \in I$ e $\sigma x_1 = x_2$, σ unidade de I. Sejam $L_1 = K_1 + Zx_1$, $L_2 = K_2 + Zx_2$ onde $K_1 = \{y \in I | B(y,x_1) \in Z\}$ e $K_2 = \{y \in I \mid B(y,x_2) \in Z\}$.

Temos $\sigma K_1 = \{\sigma y | y \in K_1\}$. Logo, $\sigma K_1 \subseteq K_2$ pois $B(\sigma y, x_2) = B(\sigma y, \sigma x_1) = B(y,x_1) \in Z$, para todo elemento $\sigma y \in \sigma K_1$, pois $\sigma K_1 \subseteq I$ e σ é isometria. Por outro lado, $K_2 \subseteq \sigma K_1$, pois sendo $\sigma I = I$, para todo $y \in K_2$ existe y' tal que $\sigma y' = y$. Como $B(y,x_2) = B(\sigma y', \sigma x_1) = B(y',x_1) \in Z$, então $y = \sigma y' \in \sigma K_1$.

Portanto, $\sigma K_1 = K_2$. Como $Zx_2 = Z(\sigma x_1) = \sigma(Zx_1)$, então $L_2 = \sigma L_1$. □

REGRA 4: Se, nas condições da regra 1, existe um vetor $t \equiv x \bmod I$ com $2B(x,t) \equiv 1 \bmod 2$, $B(t,t) = 1$ então I e L são isomorfos.

DEM: Se $t \equiv x \bmod I$, então $x = t+i$ com $i \in I$. Como $B(t,t) = 1, 2B(x,t) \equiv 1 \bmod 2$, então $B(x,t) = \frac{1}{2} + m$, $m \in Z$ e $B(x,t) \in (\frac{1}{2} Z) - Z$ estamos nas mesmas condições do teorema 8. Segue-se portanto que cls I = cls L. □

(*) Ver definição do Grupo das Unidades de L no § 3.1, Capítulo III.

CAPÍTULO V

CÁLCULO DE LÁTICES ADJACENTES E CLASSIFICAÇÃO DE LÁTICES

5.1. CÁLCULO DOS LÁTICES ADJACENTES A I_n.

Seja I_n um látice com matriz identidade, com forma quadrática t e discriminante 1 em $n \geq 5$ variáveis.

De acordo com a Regra 1, na procura dos adjacentes temos a examinar os vetores $x = \sum_{i=1}^{n} \varepsilon_i e_i$ pertencentes a $\frac{1}{2} I_n - I_n$ onde I_n tem uma base $e_1, e_2, \ldots, e_n$ com $B(e_i, e_j) = \delta_{ij}$, sendo $B(x,x) \in Z$.

Procederemos da seguinte maneira, com finalidade de simplificar o vetor examinado: o vetor x", onde $x'' = (\varepsilon_1 e_1 + \ldots + \varepsilon_n e_n) - (\Sigma\, u_i e_i)$, $u_i = \varepsilon_i$ se $\varepsilon_i \in Z$ e $u_i = \varepsilon_i \pm \frac{1}{2}$ se $\varepsilon_i \in (\frac{1}{2} Z) - Z$, fornece o mesmo látice que x, pela Regra 2, já que $x - x'' = \Sigma\, u_i e_i \in K$, $B(\Sigma\, u_i e_i, x) \in Z$ e $B(x'', x'') \in Z$, pela escolha dos escalares u_i.

Aplicando então sobre x" uma unidade de I_n que reenumera a base, consegue-se $x_m = \frac{1}{2} \sum_{i=1}^{m} e_i$, $m \leq n$, do qual resultará o mesmo látice que de x" de acordo com a Regra 3.

Observemos que $I_n = I_m \perp I_{n-m}$.

Da condição necessária $B(x_m, x_m) = \frac{m}{4}$ tiramos $m \equiv 0 \bmod 4$.

O látice adjacente a I_m será denotado por K_m, onde K_m foi construido pela Regra 2 da seguinte maneira: $K_m = K_o^m + Z x_m$ onde

$K_o^m = \{z \in I_m | B(z, x_m) \in Z\}$. Podemos verificar que K_m consiste dos vetores $\sum_{i=1}^{m} a_i e_i$ tais que $\frac{1}{2} \sum_{i=1}^{m} a_i \in Z$, $2a_i \in Z$ e $a_i - a_j \in Z$. O lâtice K_m coincide, portanto, com o lâtice E de matriz ϕ_n descrito no § 4.4. Desse modo, o lâtice L adjacente a I_n será isomorfo a $K_m \perp I_{n-m}$.

A fim de livrarmo-nos da restrição $n \geq 5$ trocaremos as formas quadráticas não equivalentes, f e g por exemplo, por $f + \sum_{i=m+1}^{n} x_i^2$ e $g + \sum_{i=m+1}^{n} x_i^2$ para $m \leq 4$, as quais continuam não equivalentes.

O próximo passo será o cálculo dos lâtices adjacentes a K_n.

5.2. CÁLCULO DOS ADJACENTES A K_n

Passaremos a analisar os adjacentes a K_n, $n \equiv 0 \bmod 4$, e teremos para $z = \sum_{i=1}^{n} \alpha_i e_i \in \frac{1}{2} K_n - K_n$ três casos a examinar:

CASO a: Todos os α_i são inteiros, então $z \in I_n$ e conseguiremos como adjacente o próprio I_n, pelo teorema 5, § 4.3.

Antes de prosseguir, demonstraremos um resultado que assegura uma caracterização particular ao lâtice L adjacente a um lâtice M.

LEMA 1: Seja L lâtice adjacente ao lâtice M onde $L = L_o \oplus Zx$, $x \in (\frac{1}{2} M) - M$, $B(x,x) \in Z$, $L_o = \{y \in M \mid B(y,x) \in Z\}$. Então $L = L_o \cup (L_o + x)$.

DEMONSTRAÇÃO: $2x \in L_o$, pois $2x \in M$ e $B(x,2x) \in Z$ de forma que para todo elemento ℓ de L, temos ou $\ell \in L_o$ ou $\ell = \ell_o + nx$. Se n é par, $\ell \in L_o$. Se n é ímpar, $\ell \in (L_o + x)$. Portanto, $L = L_o \cup (L_o + x)$. □

De acordo com o lema 1, $K_n = K_o^n \cup (K_o^n + x_n)$.

Sendo K_n adjacente a I_n, então $I_n \subseteq \frac{1}{2} K_n$.

Como $z \in \frac{1}{2} K_n - I_n$ (estamos excluindo o CASO a, onde $z \in I_n$) teremos então duas possibilidades para $z \in \frac{1}{2} K_n$: o CASO b, onde $z \in \frac{1}{2} K_o^n$, e o CASO c, onde $z \in \frac{1}{2}(K_o^n + x_n)$.

CASO b: O vetor $z \in \frac{1}{2} K_o^n$. Desse vetor resultarão dois lâtices L adjacentes a K_n: o lâtice $L = K_m \perp K_{n-m}$ (CASO b.1) e um novo lâtice $L = L_{n,m}$ (CASO b.2).

Nesse caso, $z = \sum_{i=1}^{n} \alpha_i e_i$ e os α_i são inteiros ou meio inteiros. Pela Regra 2, podemos eliminar os elementos inteiros procedendo da maneira descrita no § 5.1.

Ficaremos apenas com os elementos $\alpha_i \in (\frac{1}{2} Z) - Z$ e obteremos, dessa maneira, $z' = \sum_{i}^{m} \alpha_i e_i$, $\alpha_i \in \frac{1}{2} Z - Z$. Como $z' \notin K_n$, então $\Sigma \alpha_i$ não pode ser par.

Continuando a proceder como no § 5.1, podemos ter as primeiras m coordenadas $+\frac{1}{2}$, a coordenada m+1 igual a 1 ou 0, para que a soma das (m+1) primeiras coordenadas seja ímpar, e as restantes coordenadas nulas, se $m < n$.

Se $m = n$ teremos $z' = \frac{1}{2} (\sum_{i=1}^{n-1} e_i + e_n)$. Porém, a última coordenada deve ser nula para que z' não esteja em K_n.

Subtraindo vetores adequados, a partir do vetor $\frac{1}{2} \sum_{i=1}^{n-1} e_i$ conseguiremos $m \leq \frac{n}{2}$, e $z' = x_m = \frac{1}{2} \sum_{i=1}^{m} e_i$ ou $z' = x'_m = \frac{1}{2} \sum_{i=1}^{m} e_i + e_{m+1}$ com $m \equiv 0 \bmod 4$ já que $B(x_m, x_m) \in Z$.

Vamos proceder ao cálculo dos lâtices adjacentes a K_n obtidos através de x_m e de x'_m: (observação: no decorrer deste parágrafo x_r denotará o vetor $x_r = \frac{1}{2}\sum_{i=1}^{r} e_i$).

b.1) No primeiro caso, $x_m = \frac{1}{2}\sum_{i=1}^{m} e_i$, teremos $L = K_m \perp K_{n-m}$.

Isto pode ser demonstrado da seguinte maneira:

Seja $L = L_o + Zx_m$ o lâtice adjacente a K_n onde $L_o = \{y \in K_n \mid B(y,x_m) \in Z\}$. Seja $K_m = K_o^m + Zx_m$ onde $K_o^m = \{y = \sum_{i=1}^{m} m_i e_i \in I_m \mid B(y,x_m) \in Z\}$ ou seja, $\sum_{i=1}^{m} m_i \equiv 0 \mod 2$. Esta condição garante que se $y \in K_o^m$, então $y \in K_n$, portanto $y \in L_o$, pela definição L_o.

Nessas condições $K_o^m \subset L_o$ e então $K_m \subset L$.

Da mesma forma, $K_{n-m} = K_o^{n-m} + Zx_{n-m}$ onde $K_o^{n-m} = \{y \in I_{n-m} \mid B(y,x_{n-m}) \in Z\}$. Se $y \in K_o^{n-m}$ então $y = \sum_{i=1}^{n-m} m_i e_i$, com $m_i \in Z$. Como $B(y,x_{n-m}) \in Z$, então $\sum_{i=1}^{n} m_i \equiv 0 \mod 2$ (sendo $m_j = 0$ para $n-m < j \leq n$).

Logo $y \in K_n$, e como $B(y,x_m) \in Z$, $y \in L$.

Portanto, $K_m \perp K_{n-m} \subset L$.

Reciprocamente, pelo Lema 1, $L = L_o \cup (L_o + x_m)$ e $K_n = K_o^n \cup (K_o^n + x_n)$, sendo $L_o = \{y \in K_n \mid B(x_m,y) \in Z\}$.

Aplicando o Lema 1 a L_o, podemos analisá-lo em

$L_o = L'_o \cup (L'_o + x_n)$ onde $L'_o = \{y \in L_o \mid y \in K_o^n\}$.

Teremos a seguinte configuração:

$L = L'_o \cup (L'_o + x_n) \cup (L'_o + x_m) \cup (L'_o + x_{n-m})$ porque $(L'_o + x_n + x_m) = (L'_o + x_n - x_m)$ já que $x_n + x_m = \sum_{i=1}^{m} e_i + \frac{1}{2}\sum_{i=m+1}^{n} e_i$ e como

$\sum_{i=1}^{m} e_i$ está em L'_o, podemos ficar com $\frac{1}{2}\sum_{j=m+1}^{n} e_j = x_n - x_m$.

O seguinte lema estabelece duas identidades a respeito de L'_o :

LEMA 2: a) $L'_o = L \cap I$

b) $L'_o = K_o^m \perp K_o^{n-m}$

DEMONSTRAÇÃO:

a) óbvio, pela definição de L'_o .

b) $L \supset K_m \perp K_{n-m}$, então $L \cap I = L'_o \supset (K_m \cap I) \perp \perp (K_{n-m} \cap I)$, logo $L'_o \supset K_o^m \perp K_o^{n-m}$.

Por outro lado se $y = \sum_{i=1}^{n} m_i e_i$ está em L'_o , então $\sum_{i=1}^{n} m_i \equiv 0 \bmod 2$. Como $\sum_{i=1}^{m} m_i \equiv 0 \bmod 2$, também $\sum_{i=m+1}^{n} \equiv 0 \bmod 2$.

Podemos ter então $y = y_1 + y_2$ onde $y_1 = \sum_{i=1}^{m} m_i e_i$ e $y_2 = \sum_{i=m+1}^{n} m_i e_i$ sendo $y_1 \in K_o^n$ e $y_2 \in K_o^{n-m}$. Portanto

$L'_o \subset K_o^m \perp K_o^{n-m}$ e $L'_o = K_o^m \perp K_o^{n-m}$. □

De acordo com o Lema 2 e do fato de L ser escrito como $L = L'_o \cup (L'_o + x_n) \cup (L'_o + x_m) \cup (L'_o + x_{n-m})$ podemos ter para $x \in L$ as seguintes possibilidades:

(i) $x \in L_o'$, então $x \in K_m \perp K_{n-m}$

(ii) $x \in L_o' + x_n$, então $x = t + x_n$, $t \in L_o'$

Portanto, $x = (t_1+t_2) + x_m + x_{n-m}$, $t_1 \in K_o^m$ e $t_2 \in K_o^{n-m}$, e $x = (t_1 + x_m) + (t_2 + x_{n-m}) \in K_m \perp K_{n-m}$

(iii) $x \in L_o' + x_m$ então $x = (t_1+t_2) + x_m = (t_1 + x_m) + t_2$ e $x \in K_m \perp K_{n-m}$.

(iv) $x \in L_o' + x_{n-m}$ então $x = t_1 + (t_2 + x_{n-m}) \in K_m \perp K_{n-m}$

Portanto, $L \subset K_m \perp K_{n-m}$ e $L = K_m \perp K_{n-m}$.

b2. No segundo caso, $x_m' = \frac{1}{2} \sum_{i=1}^{m} e_i + e_{m+1}$, teremos como adjacente a K_n um novo lâtice ao qual chamaremos $L_{n,m}$.

Para n = 16 as possibilidades para m são 4,8,12.

b.2.1: No caso m = 4, $x_4' = \frac{1}{2} (e_1+e_2+e_3+e_4) + e_5$.

Usando a Regra 4 com $t = \frac{1}{2} (e_1+e_2+e_3-e_4)$ temos $t \equiv x_4$ mod K_n, $2B(x,t) = 1$ e portanto $2B(x,t) \equiv 1 \bmod 2$ e ainda $B(t,t)=1$, logo $L_{n,4}$ é isomorfo a K_n.

Antes de passarmos às outras possibilidades para m(respectivamente, m=12 e m=8) estabeleceremos algumas relações sobre elementos de $L_{n,m}$.

Por construção, $L_{n,m} = L_o^{n,m} + Zx_m$ onde, no caso,

$x'_m = \frac{1}{2} \sum_{i=1}^{m} e_i + e_{m+1}$ e $L_o^{n,m} = \{y \in K_n | B(x'_m, y) \in Z\}$.

Como $K_n = K_o^n + Zx_n$, onde $x_n = \frac{1}{2} \sum_{i=1}^{n} e_i$, a condição para que um elemento de K_n da forma $y = y_o + x_n$ esteja em $L_o^{n,m}$, onde $y \in K_o^n$, é o seguinte:

Como pode ser verificado, o conjunto $\{2e_1, e_2-e_1, \ldots, e_n-e_1\}$ é base para K_o^n. Portanto, $y_o = a_1(2e_1)+a_2(e_2-e_1)+\ldots+a_n(e_n-e_1) =$
$= (2a_1-a_2-\ldots-a_n)e_1 + \sum_{i\geq 2}^{n} a_i e_i$.

Como $B(y_o, x'_m)$ deve ser inteiro para que $y \in L_o^{n,m}$, a condição para que y_o esteja em $L_o^{n,m}$ é que $a_{m+2}+\ldots+a_n-a_{m+1} \equiv 0 \mod 2$.

Para $y = y_o + x_n$ estar em $L_o^{n,m}$ é preciso que $B(y,x'_m) =$
$= B(y_o,x'_m) + B(x'_m,x_n)$ seja inteiro, ou seja,

$a_1 - \frac{1}{2}(a_{m+2} +\ldots+ a_n - a_{m+1}) + \frac{m}{4} + \frac{1}{2}$ esteja em Z, ou ainda,

$a_{m+2}+\ldots+ a_n - a_{m+1} - 1 \equiv 0 \mod 2$.

b.2.2.: Para $m = 12$, $x'_{12} = \frac{1}{2}(e_1+\ldots+e_{12}) + e_{13}$ e o vetor $y' =$
$= \frac{1}{2}((e_{13}-e_{16}) + (e_{14}-e_{16}) + (e_{15}-e_{16})) + \frac{1}{2}(e_1+\ldots+e_{12}) +$
$+ \frac{1}{2}(e_{13}+\ldots+e_{16})$ está em $L_o^{n,m}$, pelas condições discutidas acima.

Teremos $x'_{12} - y' = -e_{14} - e_{15} + e_{16} = \omega$ e $2\omega =$
$= -2e_{14} - 2e_{15} + 2e_{16}$ está em K_o^n, portanto $\omega \in I_n$ e $\omega \in \frac{1}{2} K_n$.

Como $\omega \in \frac{1}{2} K_n \cap I_n$ e $x'_{12} - \omega = y' \in L_o^{n,m}$, a Regra 2 garante que x_{12} e ω fornecem o mesmo lâtice.

Porém, como $\omega \in \frac{1}{2} K_n \cap I_n$, o lâtice $L_{16,12}$ recai no CASO a, e nada de novo será conseguido.

b.2.3: Para o valor $m = 8$ obtemos efetivamente $L_{16,8}$ como um novo lâtice pois $L_{16,8}$ não é isomorfo a K_{16}.

De fato, $L_{16,8} = L_o^{16,8} + Z\, x'_8 = L_o^{16,8} \cup (L_o^{16,8} + x'_8)$.

Pela condição estudada acima, o vetor $y_o = \sum_{i=1}^{16} a_i e_i$ está em $L_o^{16,8}$ se e somente se $a_{m+2} + \ldots + a_n - a_{m-1} \equiv 0 \mod 2$.

Nesse caso $e_i \pm e_j$ está em $L_o^{16,8}$ se e somente se $i,j > m$ ou $i,j \leq m$ e estes serão os únicos vetores de comprimento 2 em $L_o^{16,8}$, isto é, $B(e_i \pm e_j, e_i \pm e_j) = 2$.

Em $(L_o^{16,8} + x'_8)$ não há vetores de comprimento 2 pois $B(x_8, x_8) = 3$.

Por outro lado, em K_{16} teremos todos os vetores $e_i \pm e_j$ de comprimento 2, para todo i e j. Não há, portanto, isomorfismo possível.

CASO c: Se z está em $\frac{1}{2}(K_o^n + x_n)$, então $z = \frac{1}{2} x_n + \frac{1}{2}(\Sigma\, a_i e_i)$ onde $\Sigma\, a_i e_i$ está em K_o^n.

Isto ocorre, conforme já demonstrado, se e somente se $\Sigma\, a_i \equiv 0 \mod 2$.

Podemos escrever z como $z = \frac{1}{4} \Sigma \tau_i e_i$ onde $\tau_i = 2a_i+1$. Como os elementos τ_i são ímpares $\tau_i \equiv \pm 1 \bmod 4$. Na procura do lâtice adjacente L teremos $L = L_o + Zz$ onde $L_o = \{y \in K_n \mid B(y,z) \in Z\}$.

Como consequência, $B(e_i+e_j,z) = \frac{1+(a_i+a_j)}{2}$ e $B(e_i-e_j,z) = \frac{a_i-a_j}{2}$, portanto se a_i e a_j têm ambos a mesma paridade, $e_i - e_j$ está em L_o.

Se têm paridades diferentes, e_i+e_j está em L_o.

Chamaremos $e_{in} = e_i - e_n$ se as paridades de a_i e a_n são iguais, ou $e_{in} = e_i + e_n$ se as paridades de a_i e a_n são distintas.

Substituindo z por $z - \sum_{i=1}^{n} m_i e_{in}$, m_i inteiros, teremos o mesmo lâtice, de acordo com a Regra 2, já que $\sum_{i=1}^{n} m_i e_{in}$ está em L_o.

Os valores m_i são tais que $\tau_i = 1 + 4m_i$ ou $\tau_i = -1 + 4m_i$.

Tomemos, para um valor m adequado,

$$z' = z - \sum_{i=1}^{n} m_i e_{in} = \frac{1}{4}[((1+4m_1)e_1+\ldots+(1+4m_n)e_n) - (4m_1(e_1-e_n)+\ldots+$$

$$+ 4m_{n-1}(e_{n-1} - e_n)] = \frac{1}{4}\left(\sum_{i=1}^{n-1} \delta_i e_i + m\, e_n\right) \quad \text{onde} \quad \delta_i = \pm 1.$$

Após trocas de sinais adequados, teremos

$$z' = \frac{1}{4} \sum_{i=1}^{n-1} e_i + \frac{m}{4} e_n .$$

Podemos tomar $m = 4a + b$, com $|b| < 2$, pois há as seguintes possibilidades para b: 0, 1, 2,3 e se $b = 3$, teremos $m = 4(a+1) - 1$, logo $|b| < 2$.

Podemos subtrair de z' o elemento $4a\,e_n$, pois $2e_n \in K_n$ e $4e_n \in L_o$, logo $4a\,e_n \in L_o$.

Consequentemente, podemos tomar m de tal modo que $|\frac{m}{4}| \leq 2$.

Como $\sum_{i=1}^{n-1} 1_i + m \equiv 0 \mod 4$, e n-1 é ímpar, m deve ser ímpar, e temos para m as seguintes possibilidades:

{-7, -5,-3,-1, 1,3,5,7} divididos em duas classes, a menos de congruência módulo 4: {-7, -3, 1, 5} e {-5,-1,3,7} que diferem apenas pelo sinal.

Tomaremos $m \in \{-7, -3, 1, 5\}$.

Teremos, como $n \equiv 0 \mod 4$,uma divisão em duas possibilidades: $n \equiv 0 \mod 8$ e $n \equiv 4 \mod 8$. Pela condição $B(z',z') \in Z$, teremos $\frac{n-1}{16} + \frac{m^2}{16} \in Z$.

Para $n \equiv 0 \mod 8$, $n \in \{0,8,16, 24,...\}$. Se $n = 8$ teremos $m \in \{-3,5\}$. Se $n = 16$, teremos $m \in \{-7,1\}$.

Para $n \equiv 4 \mod 8$, as quatro possibilidades para m desaparecem

c.1: Para $n = 8$, o caso $z' = \frac{1}{4}(\sum_{i=1}^{7} e_i - 3e_8)$ recai no CASO b por uma transformação ortogonal adequada.

O caso $z' = \frac{1}{4}\left(\sum_{i=1}^{7} e_i + 5e_8\right)$ desaparece pela Regra 4 com $t = \frac{1}{4}\left(\sum_{i=1}^{7} e_i - 3e_8\right)$, pois $B(t,t) = 1$, $2B(z',t) \equiv 1 \mod 2$ e $t \equiv z' \mod K_n$.

c.2: Para $n = 16$, o caso $z' = \frac{1}{4}\left(\sum_{i=1}^{15} e_i - 7e_{16}\right)$ desaparece pela mesma Regra 4, com $t = \frac{1}{4}\sum_{i=1}^{16} e_i$.

Para o caso $x = \frac{1}{4}\sum_{i=1}^{16} e_i$ conseguimos um látice $L = M_{15} + Z_x$.

Temos: $L = L_o \cup (L_o + x)$, onde $L_o = \{y \in K_{16} \mid B(y,z') \in Z\}$ logo $L_o \subset K_{16}$ e $L_o + x \subset K_{16} \perp Zx$ logo $L = M_{15} + Zx \subset K_{16} + Zx$.

Como os únicos vetores de comprimento 1 são $\pm x$ em $K_{16} \perp Zx$, o mesmo ocorre em $L = M_{15} + Zx$, portanto tais vetores não estão em M_{15}, que então não tem vetores de comprimento 1. Daí, M_{15} é irredutível, pois se $M_{15} = L_1 + L_2$, algum dos L_i teria dimensão menor que 8 e possuiria vetor de comprimento 1.

Antes de prosseguir faremos uma breve digressão a respeito dos adjacentes em dimensões menores que 7.

De acordo com a Regra 4, verificamos facilmente que K_4 é isomorfo a I_4, usando $t = \frac{1}{2}(e_1+e_2+e_3-e_4)$.

Na procura dos adjacentes de I_n (parágrafo 5.1) para $n=1,2,3$ K_n não é possível e portanto o adjacente a I_n é o próprio I_n.

Para valores de $n = 5,6,7$ o látice adjacente a I_n será $K_4 \perp I_{n-4}$, isomorfo a $I_4 \perp I_{n-4} = I_n$.

Portanto, para $n \leq 7$, só há lâtices da forma I_n.

Os próximos teoremas completam a procura dos adjacentes.

TEOREMA 3: Os únicos lâtices adjacentes a $K_8 \perp K_8$ são I_{16}, K_{16}, $K_8 \perp K_8$, $M_{15} \perp I_1$ e $M_{14} \perp I_2$ onde M_{14} consiste precisamente do comprimento ortogonal de $Zx \perp Zy$, $x = \pm \frac{1}{4} \sum_{i=1}^{8} e_i$ $y = \pm \frac{1}{4} \sum_{i=9}^{16} e_i$.

Verificamos, usando o mesmo processo de M_{15}, que M_{14} não tem vetores unitários, então M_{14} é irredutível, pois se $M_{14} = L_1 + L_2$, algum dos L_i teria dimensão menor que 8 e teria vetores unitários.

DEMONSTRAÇÃO: Não será levada a efeito, por ser muito extensa e envolver os mesmos mecanismos precedentes.

TEOREMA 4: Se L é lâtice irredutível de dimensão $n \leq 16$ e ímpar, então os adjacentes de L consistem somente nos casos já listados.

DEMONSTRAÇÃO: Será omitida por envolver a teoria de lâtices maximais, não abrangida neste trabalho.

5.3. OS LÂTICES INDECOMPONÍVEIS DE DIMENSÃO MENOR QUE 16

Os lâtices I_1, K_8, K_{16}, $L_{16,8}$, M_{14}, M_{15} e K_{12} são todos os indecomponíveis de dimensão $n \leq 16$.

Os lâtices I_1, K_8, K_{12} e K_{16} são indecomponíveis, como já demonstrado.

Os lâtices M_{14} e M_{15} se fossem decompostos teriam uma das parcelas com dimensão $n \leq 7$, a qual seria então isomorfa a I_n. Como nenhum destes lâtices tem vetor unitário, a decomposição é impossível.

Para $L_{16,8}$ o mesmo acontece, salvo no caso de haver duas parcelas 8-dimensionais. Porém nesse caso uma das parcelas deveria obrigatoriamente ser isomorfa a I_8. Tal não ocorre porque $L_{16,8}$ não tem vetores unitários (isto pode ser verificado escrevendo-se uma base para $L_{16,8}$ onde notaremos que $L_o^{16,8}$ não tem vetores de comprimento 1).

São estes, por sua vez, os únicos lâtices indecomponíveis porque todo lâtice irredutível N de dimensão $n \leq 16$ pode ser colocado como fator do lâtice $N \perp I_{16-n}$ de dimensão 16.

Mas este lâtice, com discriminante 1, está na lista dos 16-dimensionais possíveis, que são I_{16}, $K_{12} \perp I_4$, $K_8 \perp K_8$, $L_{16,8}$, $M_{15} \perp I_1$ e $M_{14} \perp I_2$.

Portanto os irredutíveis N serão I_1, M_{14}, M_{15}, K_8 e K_{12} com dimensão menor que 16, e K_{16} e $L_{16,8}$ com dimensão 16.

5.4. A TÁBUA DE CLASSIFICAÇÃO DOS LÂTICES

Podemos, agora, classificar todos os lâtices de dimensão $n \leq 16$, a partir dos resultados conseguidos. Tais resultados fornecem uma Regra de Formação, a saber:

(i) Para $i \leq n \leq 7$, só conseguimos lâtices I_n.

(ii) Os adjacentes a I_n são $K_m \perp I_{n-m}$, $m \equiv 0 \bmod 4$ e K_4 isomorfo a I_4.

(iii) Os adjacentes a K_n são I_n, $K_m \perp K_{n-m}$ onde $m \equiv 0 \bmod 4$ e $m \leq \frac{n}{2}$ e $L_{n,m}$ somente para $n = 16$ e $m = 8$.

A tábua de classificação segue:

$n \leq 7 : I_n$

$n = 8 : I_8, K_8$

$n = 9 : I_9, K_8 \perp I_1$

$n = 10: I_{10}, K_8 \perp I_2$

$n = 11: I_{11}, K_8 \perp I_3$

$n = 12: I_{12}, K_8 \perp I_4, K_{12}$

$n = 13: I_{13}, K_8 \perp I_5, K_{12} \perp I_1$

$n = 14: I_{14}, K_8 \perp I_6, K_{12} \perp I_2, M_{14}$

$n = 15: I_{15}, K_8 \perp I_7, K_{12} \perp I_3, M_{14} \perp I_1, M_{15}$

$n = 16: I_{16}, K_8 \perp K_8, K_{12} \perp I_4, K_{16}, M_{15} \perp I_1, M_{14} \perp I_2$ e $L_{16,8}$.

BIBLIOGRAFIA

[A] N. ALLAN, A note on symmetric matrices, Rev. Colombiana de Matemática, Volume III (1969), pp. 1-20.

[K] M. KNESER, Klassenzahlen definiter quadratischer Formen., Arch. Math. (1957), pp. 241-250.

[L] S. LANG, Algebra, Addison Wesley, New York, (1965).

[O] O.T. O'MEARA, Introduction to quadratic forms, Springer Verlag, Berlim, (1963).

[S] J.P. SERRE, Cours d'Aritmetique, Paris, (1970).

[VW] B VAN DER WAERDEN, Algebra, Ungar, Berlin (1930).