REPRESENTACION DE ENTEROS POR FORMAS CUADRATICAS CUATERNARIAS POSITIVAS DEFINIDAS

Tesis
Entregada a la
Universidad de Chile
en cumplimiento parcial de los requisitos
para optar al grado de
Doctor en Ciencias con mención en Matemáticas

Facultad de Ciencias
por
Catalina Cvitanich Abarca
Mayo, 1995

Director de Tesis: Dr. Ricardo Baeza

FACULTAD DE CIENCIAS

UNIVERSIDAD DE CHILE

INFORME DE APROBACION

TESIS DE DOCTORADO

Se informa a la Comisión de Postgrado de la Facultad de Ciencias que la Tesis de Doctorado Presentada por el candidato.

CATALINA CVITANICH ABARCA

Ha sido aprobada por la Comisión de Evaluación de la Tesis como requisito de tesis para optar al grado de Doctor en Ciencias con mención en Matemáticas, en el Examen de Defensa de Tesis rendido el día 20 de Julio de 1995.

Director de Tesis:
Dr. Ricardo Baeza R. R Baeza

Comisión de Evaluación de la Tesis:
Dr. Eduardo Friedman R. Eduardo Friedman
Dr. José Pantoja M.
Dr. Rolando Pomareda R. Rolando Pomareda

A mis hijos

Claudia Andrea

y

Victor Manuel

AGRADECIMIENTOS

Mis más sinceros agradecimientos a las autoridades de la Universidad de La Serena, quienes me otorgaron la oportunidad y el financiamiento para perfeccionarme y optar al grado académico de Doctor en Ciencias con mención en Matemáticas.

Agradezco a mi director de tesis Profesor Dr. Ricardo Baeza R. por haberme propuesto este interesante tema, como así mismo la orientación que me proporcionó para la realización del trabajo.

Agradezco al Profesor Dr. Eduardo Friedman R., quien supo darme una indicación clara y oportuna cada vez que lo requerí, tanto en el aspecto humano como en el académico.

Agradezco a la Dra. María Inés Icaza por sus valiosas sugerencias y comentarios.

Agradezco en forma muy especial a aquellos miembros del Departamento de Matemáticas de la Facultad de Ciencias de la Universidad de Chile, quienes fueron mis profesores durante el transcurso de mis estudios de pre y post-grado, ya que su apoyo fué un excelente estímulo para el desarrollo de este trabajo.

Es mi deseo reconocer y agradecer a las instituciones que me otorgaron financiamiento parcial para la realización de esta tesis:

Fondecyt, Proyectos 91-0853 y 1930860 (1992-1993-1994). Investigador principal: Dr. Ricardo Baeza R.

Departamento de Postgrado y Post-título, Universidad de Chile. (1993-1994).

Finalmente deseo expresar mi gratitud a la Sra. Virginia Cárdenas A. por su dedicación y excelente trabajo de digitación especializada de esta tesis.

Catalina Cvitanich A.

INDICE

RESUMEN

Estudiamos el problema de representar efectivamente números enteros por formas cuadráticas enteras cuarternarias positivas definidas.

En 1974, M. Kneser ([K], 26.3) demostró el siguiente resultado:

Sea f una forma cuadrática entera, regular, positiva definida en 4 variables. Entonces existe una constante $N = N(f)$ con la siguiente propiedad:

Si $t \geq N$ es un entero representado f sobre $\mathbb{Z}_p$, para cada primo p, y t no es divisible por aquellos primos p para los cuales f es anisótropa sobre $\mathbb{Z}_p$, entonces t es representado por f sobre $\mathbb{Z}$.

En este trabajo se obtiene una cota efectivamente calculable para la constante N del teorema anterior, la cual depende sólo de la forma cuadrática f y de una constante absoluta que se puede calcular explícitamente.

ABSTRACT

In this thesis we study the effective representation of integers by positive definite integral quadratic forms of dimension 4.

In 1974, M. Kneser ([K], 26.3) proved the following result:

Let f be a positive definite integral form in 4 variables. Then there exists a constant N with the following property:

If $t \geq N$ is an integer which is represented by f over $\mathbb{Z}_p$ for each prime p, and t is not divisible by those primes p for which f is anisotropic over $\mathbb{Z}_p$, then t is represented by f over $\mathbb{Z}$.

In this work we obtain a bound for the constant N appearing in the statement of the above theorem. The bound is effectively computable and it depends only on the quadratic form f and an absolute constant which can be computed explicitly.

INTRODUCCION

Este trabajo trata sobre el problema de representar números enteros por formas cuadráticas enteras cuaternarias positivas definidas.

Sea $\mathcal{O}$ un anillo de integridad, $\mathcal{O} \hookrightarrow F = Quot(\mathcal{O})$ el cuerpo cuociente y suponemos característica de $\mathcal{O}$ distinta de 2.

Una forma cuadrática $f(x_1, \cdots, x_n)$ en n variables sobre $\mathcal{O}$ es un polinomio

$$f(x_1, \cdots, x_n) = \sum f_{ij} x_i x_j \quad \text{con} \quad f_{ij} = f_{ji} \in \mathcal{O}, \quad 1 \leq i, \ j \leq n.$$

El determinante $d(f)$ de la forma f es por definición el determinante de la matriz simétrica $F = (f_{ij})$. Si $d(f) \neq 0$ se dice que f es regular o no singular.

Diremos que f representa un elemento $c \in \mathcal{O}$ sobre $\mathcal{O}$ si existe $a = (a_1, \cdots, a_n) \in \mathcal{O}^n$ tal que $f(a_1, \cdots, a_n) = c$.

En el caso $\mathcal{O} = \mathbb{Z}$ diremos que una forma cuadrática f sobre $\mathbb{Q}$ es positiva definida si $f(x_1, \cdots, x_n) > 0$ para todo $(x_1, \cdots, x_n) \in \mathbb{R}^n - \{0\}$.

De modo análogo se define una forma negativa definida. Diremos que una forma es definida si es positiva definida o negativa definida. Cuando la forma no es definida se dice que es indefinida.

Un método fundamental para estudiar este problema es el de extensión de escalares. Si $\mathcal{O} \hookrightarrow \mathcal{O}'$, $\mathcal{O}$ subanillo de $\mathcal{O}'$, entonces toda forma cuadrática f sobre $\mathcal{O}$ se puede considerar como una forma cuadrática sobre $\mathcal{O}'$. Por ejemplo, $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ cuerpo de números p-ádicos y $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ anillo de enteros p-ádicos.

Se conocen los siguiente resultados:

Teorema 0.1 Sea $f(x_1, \cdots, x_n)$ una forma cuadrática entera regular indefinida, $n \geq 4$. Sea $a \in \mathbb{Z} - \{0\}$, tal que a es representado por f sobre $\mathbb{Z}_p$, para todo

primo p, incluso $p = \infty$ (en este caso $\mathbf{Z}_\infty = \mathbf{R}$). Entonces a es representado por f sobre $\mathbf{Z}$.

(Ver [Ca], pág. 131).

En el caso de una forma definida la situación es más complicada y se tiene el siguiente resultado de Tartakowski (1929).

Teorema 0.2 Sea $f(x_1, \cdots, x_n)$ una forma cuadrática entera regular definida positiva, $n \geq 5$. Entonces existe una constante $N = N(f)$ con la siguiente propiedad:

Sea $t \geq N$ un entero representado por f sobre $\mathbf{Z}_p$, para todo primo p, entonces t es representado por f sobre $\mathbf{Z}$.

Otro lenguaje para estudiar formas cuadráticas es el de reticulados. Un $\mathcal{O}$-reticulado en el espacio vectorial V sobre $F = Quot\mathcal{O}$, es un $\mathcal{O}$-módulo $L \subseteq \mathcal{O}v_1 + \cdots + \mathcal{O}v_n$ donde $\{v_1, \cdots, v_n\}$ es una base de V y $FL = V$.

Si $f(\mathbf{x}) = f(x_1, \cdots, x_n) = \sum f_{ij}x_ix_j$ es una forma cuadrática sobre $\mathcal{O}$ en n variables, asociamos a f el $\mathcal{O}$- reticulado ($\mathcal{O}$-módulo) $L = \mathcal{O}v_1 \oplus \cdots \oplus \mathcal{O}v_n$ en el espacio vectorial F^n, con la forma cuadrática $f(x_1v_1 + \cdots + x_nv_n) := f(x_1, \cdots, x_n)$. Luego $f : L \to \mathcal{O}$ es una aplicación que satisface:

(1) $f(a\mathbf{x}) = a^2 f(\mathbf{x}) \quad \forall a \in \mathcal{O}, \ x \in L,$

(2) $2b(\mathbf{x}, \mathbf{y}) = f(\mathbf{x} + \mathbf{y}) - f(\mathbf{x}) - f(\mathbf{y})$ define una forma bilineal simétrica sobre L, con $b(v_i, v_j) = f_{ij}$.

En particular, L es un $\mathcal{O}$-reticulado en el espacio cuadrático (F^n, f) donde $f : F^n \to F$ es la forma cuadrática definida por $f(x_1v_1 + \cdots + x_nv_n) = \Sigma f_{ij}x_ix_j$.

En la mayor parte de este trabajo empleamos el lenguaje de reticulados debido a que es más práctico.

Sean (V,q) y $W,\tilde{q})$ espacios cuadráticos sobre un cuerpo F. Diremos que un reticulado L en (V,q) representa al reticulado M en $(W,\tilde{q})$, si existe $\sigma : W \to V$ lineal, tal que $q(\sigma x) = \tilde{q}(x)$, para todo $x \in W$ y $\sigma M \subseteq L$.

En particular, $t \in F$ está representado por el reticulado L, si existe $x \in L$ tal que $q(x) = t$.

En 1978, J. S. Hsia, Y. Kitaoka y M. Kneser demuestran el siguiente teorema. (Ver Teorema 1 en [HKK]):

Teorema 0.3 Sea L un $\mathbb{Z}$−reticulado positivo, $dimL = m \geq 2n+3$. Entonces existe una constante $c = c(L)$ con la siguiente propiedad: Sea E un $\mathbb{Z}$-reticulado de dimensión n, tal que E_p es representado por L_p para todo primo p y $\mu(E) = Min\{q(x)|0 \neq x \in E\} \geq c$. Entonces E es representado por L.

Si $n = 1$ entonces el teorema 0.2 es un caso particular del teorema 0.3.

La constante c ha sido estimada efectivamente por M.I. Icaza. (1992), ver [Ic1].

El teorema 0.3 no es válido si $m = 4$. Un ejemplo para esta afirmación es el siguiente:

$f(x) = x_1^2 + x_2^2 + 25(x_3^2 + x_4^2)$ es una forma cuadrática entera positiva definida. Si $a \geq 0$ entonces f representa a $3 \cdot 2^{2a}$ sobre $\mathbb{Z}_p$, para todo p. Sin embargo f no representa $3 \cdot 2^{2a}$ sobre $\mathbb{Z}$. (Ver [K], 26).

Este ejemplo funciona porque f es anisótropa sobre $\mathbb{Q}_2$, es decir $f(x) \neq 0$, para todo $x \neq 0$. Entonces es claro que para tener una versión análoga al teorema

0.2 en el caso $m = 4$ se deben agregar ciertas hipótesis.

Si E es un $\mathbf{Z}$-reticulado en un espacio cuadrático (V, q) sobre $\mathbf{Q}$, entonces las inclusiones $\mathbf{Q} \hookrightarrow \mathbf{Q}_p$ y $\mathbf{Z} \hookrightarrow \mathbf{Z}_p$, para todo primo p (incluso $p = \infty$), conducen a las p-localizaciones (extensión de escalares) $V_p = \mathbf{Q}_p \otimes V$ y $E_p = \mathbf{Z}_p \otimes E$.

Consideremos un $\mathbf{Z}-$reticulado positivo definido E. Definamos los siguientes conjuntos:

$$\bar{q}(E) = \{t \geq 0 |\ t \in q(E_p),\ \forall p\},$$

$$\bar{q}_r(E) = \{t \in \bar{q}(E) | p^r \nmid t \text{ si } E_p \text{ es anisótropo}\}.$$

En 1974, ([K], 26.3) M. Kneser demostró el siguiente teorema:

Teorema 0.4 Sea E un $\mathbf{Z}-$reticulado regular positivo definido, $dim E = 4$. Entonces existe una constante $N = N(E)$ que satisface la siguiente propiedad:

Si $t \in \bar{q}_r(E)$ y $t \geq N$, entonces $t \in q(E)$.

Diremos que un entero t es representado primitivamente por f sobre $\mathbf{Z}$ ($\mathbf{Z}_p$) si existe $(a_1, \cdots, a_n) \in \mathbf{Z}^n$ ($\mathbf{Z}_p^n$) primitivo (es decir $mcd(a_1, \cdots, a_n) = 1$ o $max_{1 \leq i \leq n} |a_i|_p = 1$ respectivamente) tal que $f(a_1, \cdots, a_n) = t$.

Una versión análoga el teorema 0.4 fué dada por J. W. Cassels en 1978 (ver teorema 1.6 de [Ca], pág. 204) y es el siguiente resultado:

Teorema 0.5. Sea f una forma cuadrática entera regular positiva definida en $m = 4$ variables. Entonces existe una constante $N = N(f)$ con la siguiente propiedad:

Sea $t \geq N$ un entero representado primitivamente por f sobre $\mathbf{Z}_p$, para todo primo p. Entonces t es representado primitivamente por f sobre $\mathbf{Z}$.

En este trabajo se obtiene una estimación efectiva para la constante N del teorema 0.4, con $r = 1$.

Con el propósito de obtener una constante N, la cual tenga acotados todos sus factores, se modifica la demostración del teorema 0.4.

Esta modificación consiste fundamentalmente en emplear algunos pasos de las demostraciones de los teoremas 0.3 y 0.5. Además, se introducen propiedades sobre representaciones primitivas, las cuales permiten obtener estimaciones fundamentales para el resultado final.

En el resultado obtenido aquí, intervienen también algunas cotas obtenidas por [Ic1] y [Ic2] para estimar la constante del teorema 0.3.

La estimación de la constante N, no es la óptima, por lo tanto la cota obtenida en este trabajo, se podría mejorar.

Por otra parte, los argumentos empleados para obtener una cota efectiva para N, no varían si r es 1 o r es 2, pero no son válidos si $r > 2$. Como el teorema 0.4 garantiza la existencia de la constante N para cualquier $r \in \mathbb{N}$, sería interesante acotar la constante N, en el caso $r > 2$,

En el Capítulo I presentamos definiciones y resultados básicos para el desarrollo del trabajo.

En el Capítulo II se dejan establecidas las estimaciones necesarias para obtener la cota N del teorema 0.4.

En el Capítulo III se demuestra con detalles el teorema 0.4 y se muestra en el teorema 3.1 que la constante N es efectivamente calculable.

CAPITULO I

Preliminares

1.1. Notación y terminología.

Definición 1.1.1. Sea F un cuerpo con $chF \neq 2$ y $\mathcal{O}$ un anillo con unidad contenido en F, con $Quot\mathcal{O} = F$. Sea M un $\mathcal{O}$-módulo libre, de dimensión finita y q una función de M en F tal que

(1) $q(ax) = a^2 q(x)$ para todo $a \in \mathcal{O}$ y $x \in M$,

(2) $q(x+y) - q(x) - q(y) := 2b(x,y)$ es una forma bilineal simétrica.

Diremos que M es un módulo cuadrático sobre $\mathcal{O}$ (o que M es $\mathcal{O}$-módulo cuadrático) y q (respectivamente b) la forma cuadrática (respectivamente forma bilineal) asociada a M.

Si $x = y$ entonces $q(x) = b(x,x), \quad \forall x \in M$.

Diremos que M es un espacio cuadrático en el caso $\mathcal{O} = F$.

Definición 1.1.2. Sea M un módulo cuadrático libre, de dimensión finita n sobre $\mathcal{O}$ y supongamos que $\{v_i\}_{i=1}^n$ es una base para M. Entonces se tiene una matriz simétrica $A \in M_n(F)$ definida por $A = (b(v_i, v_j))$.

A se llama la matriz del módulo cuadrático M en la base $\{v_1, \cdots, v_n\}$ y se denota $M \cong \langle A \rangle$.

Si $\{u_i\}_{i=1}^n$ es otra base entonces existe una matriz $T = (t_{ij})$ tal que $(u_1, \cdots, u_n) = (v_1, \cdots, v_n)T$ con $t_{ij} \in \mathcal{O}$, $detT \in \mathcal{O}^\times$ y si $B = (b(u_i, u_j))$ entonces $B = T^t AT$.

Se tiene en este caso que $(detA)\ mod(O^\times)^2$ es independiente de la elección de la base y está unicamente determinado por M, se denota por dM y se llama el discriminante de M (está definido sólo para módulos libres). Diremos que M es regular si $detA \neq 0$.

Definición 1.1.3. Sea M un $\mathcal{O}$-módulo cuadrático y $S \subseteq M$. El complemento ortogonal de S es el $\mathcal{O}$-módulo

$$S^\perp = \{x \in M | b(x, s) = 0, \quad \forall s \in S\}.$$

Definición 1.1.4. Sean $M, M_1, \cdots, M_m$ módulos cuadráticos sobre un anillo $\mathcal{O}$ tales que $M = M_1 \oplus \cdots \oplus M_m$, $b(M_i, M_j) = 0$ si $i \neq j$. Diremos que M es la suma ortogonal de $M_1, \cdots, M_m$ y se denota por $M = M_1 \perp \cdots \perp M_m$.

Si M tiene una base $\{v_i\}$ tal que $M = \mathcal{O}v_1 \perp \cdots \perp \mathcal{O}v_n$, entonces $\{v_i\}$ se llama base ortogonal de M. Con las notaciones anteriores $M \cong \perp_i \langle a_i \rangle$ con $a_i = q(v_i)$.

Observación 1.1.5. Si U es un espacio cuadrático sobre un cuerpo F y $U = U_1 \perp \cdots \perp U_m$ entonces $dU = dU_1 \cdots dU_m$ y es claro que U es regular si y sólo si cada U_i es regular.

Todo espacio cuadrático no cero sobre un cuerpo, posee una base ortogonal.

Definición 1.1.6. Sean M y N módulos cuadráticos sobre un anillo $\mathcal{O}$.

Una aplicación lineal $\sigma : M \to N$ tal que $q(\sigma x) = q(x)$ para todo $x \in M$, se llama representación de M en N. Se dice que M es representado por N y se denota $M \to N$.

Si σ es una representación inyectiva se denota $M \hookrightarrow N$.

Si σ es una representación biyectiva se llama isometría, se dice que M y N son isométricos y se denota $M \cong N$.

El grupo de las isometrías $\sigma : M \to M$ se denota por $O(M)$ y se llama grupo ortogonal de M.

Supongamos que M es un $\mathcal{O}$-submódulo libre de un espacio cuadrático regular V sobre un cuerpo F y $FM = V$. Denotemos por $O^+(M) = \{\sigma \in O(M) | det\sigma = 1\}$ el subgrupo de las rotaciones de M.

Definición 1.1.7. Sea M un módulo cuadrático sobre $\mathcal{O}$. Entonces M se llama módulo cuadrático isótropo si existe $x \in M$, $x \neq 0$ tal que $q(x) = 0$. Si M no es isótropo se llama anisótropo.

Definición 1.1.8. Sea V un espacio cuadrático de dimensión 2 sobre un cuerpo F. Si V posee una base $\{v_1, v_2\}$ tal que $q(a_1v_1 + a_2v_2) = a_1a_2$ con $a_i \in F$, entonces V se llama plano hiperbólico.

Es claro que todo plano hiperbólico es isótropo.

Definición 1.1.9. Un espacio cuadrático V sobre un cuerpo F se llama universal si para cada $\alpha \in F^\times$ existe $v \in V$ tal que $q(v) = \alpha$. Es decir $q(V) = F^\times$.

Definición 1.1.10. Sea V espacio cuadrático regular sobre un cuerpo F tal que $V \cong \mathbf{H}_1 \perp \cdots \perp \mathbf{H}_r \perp U$, donde $\mathbf{H}_i$ es un plano hiperbólico y U es un espacio anisótropo o cero. De acuerdo con 42:16 de [O'M1] se tiene que r es independiente de esta descomposición. Por lo tanto r es un invariante de V y tiene sentido definir el índice de Witt de V como $ind\ V = r$.

En particular $ind\ V > 0$ si y sólo si V es isótropo.

1.2. Norma espinorial.

Sea V espacio cuadrático regular sobre un cuerpo F. Si $y \in V$ es tal que $q(y) \neq 0$ se define $\tau_y : V \to V$ por la fórmula

$$\tau_y(x) = x - \frac{2b(x,y)}{q(y)}y,$$

$\tau_y \in O(V)$ y la llamaremos simetría definida por y.

Si $dim V = n$ y $\sigma \in O(V)$ entonces $\sigma = \tau_{y_1} \cdots \tau_{y_r}$ donde τ_{y_i} es una simetría y $r \leq n$. (Ver [O'M1], 43:3).

Si $\sigma = \tau_{z_1} \cdots \tau_{z_t}$ es otra expresión de σ en producto de simetrías entonces por 54:6 de [O'M1] se tiene que

$$q(y_1) \cdots q(y_r) \in q(z_1) \cdots q(z_t) F^\times / (F^\times)^2.$$

Luego podemos definir la norma espinorial θ de la siguiente manera
$\theta : O(V) \to F^\times/(F^\times)^2$ con $\theta(\sigma) = q(y_1) \cdots q(y_r)$ en $F^\times/(F^\times)^2$.

θ es homomorfismo de grupos y si consideramos la restricción
$\theta : O^+(V) \to F^\times/(F^\times)^2$ denotamos por $O'(V)$ el núcleo de esta restricción, es decir

$$O'(V) = \{\sigma \in O^+(V) | \theta(\sigma) = 1\}.$$

1.3. Formas cuadráticas y espacios cuadráticos.

Sea $\mathcal{O}$ un anillo con unidad contenido en un cuerpo F tal que $chF \neq 2$, es posible el caso $\mathcal{O} = F$.

Definición 1.3.1. Una forma cuadrática $f(\mathbf{x})$ sobre F en n variables $(x_1, \cdots, x_n) = \mathbf{x}$ es una función $f(\mathbf{x}) = \sum_{i,j} f_{ij} x_i x_j \quad (1 \leq i,\ j \leq n)$ donde $f_{ij} = f_{ji}$.

Se dice que f es una forma cuadrática sobre $\mathcal{O}$ si $f_{ij} \in \mathcal{O}$ para todo i, j.

Definición 1.3.2. La forma cuadrática f representa un elemento $c \in F$ sobre $\mathcal{O}$ si existe $\mathbf{b} = (b_1, \cdots, b_n) \in \mathcal{O}^n$ tal que $f(\mathbf{b}) = c$.

Más generalmente se tiene la siguiente definición:

Definición 1.3.3. Una forma cuadrática $f(\mathbf{x})$ en n variables representa la forma $g(\mathbf{y})$ en m variables sobre $\mathcal{O}$ si existen vectores $\mathbf{b}_1, \cdots, \mathbf{b}_m \in \mathcal{O}^n$ tales que

$$f(y_1\mathbf{b}_1 + \cdots + y_m\mathbf{b}_m) = g(y_1, \cdots, y_m) = g(\mathbf{y})$$

En este caso escribiremos $g \rightarrow f$ (sobre $\mathcal{O}$). Es claro que se puede definir en forma análoga $g \rightarrow f$ (sobre F).

Si $m = 1$ esta definición coincide con la representación de elementos.

Definición 1.3.4. Se dice que dos formas f, g en el mismo número de variables son equivalentes sobre $\mathcal{O}$ ($\mathcal{O}$-equivalentes) si cada una representa a la otra. Se denota $f \cong_{\mathcal{O}} g$.

Es claro que la $\mathcal{O}$-equivalencia es una relación de equivalencia.

En forma análoga se define $f \cong_F g$.

Observación 1.3.5. Si consideramos $\mathbf{x}$ como un vector columna entonces podemos escribir $f(\mathbf{x}) = \mathbf{x}^t T \mathbf{x}$ donde T es la matriz cuadrada simétrica $T = (f_{ij})$ y $\mathbf{x}^t$ es el vector $\mathbf{x}$ transpuesto.

El determinante $d(f)$ de la forma cuadrática f es por definición el determinante $det\, T$ de la matriz T.

Diremos que f es singular si $d(f) = 0$, en otro caso f es regular.

Observación 1.3.6. En notación matricial la definición 1.3.3 es la siguiente:

f representa a g sobre $\mathcal{O}$ si y sólo si $G = B^t T B$ donde T y G son las matrices correspondientes a f y g respectivamente y $B = (b_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$ es una matriz con $b_{ij} \in \mathcal{O}$.

Equivalentemente $f(B\mathbf{x}) = g(\mathbf{x})$.

Con esta notación es fácil probar el siguiente resultado:

Proposición 1.3.7. Una condición necesaria y suficiente para que las formas cuadráticas regulares f y g en n-variables sean $\mathcal{O}$-equivalentes es que $G = B^t T B$ para alguna matriz B con coeficientes en $\mathcal{O}$ y $detB \in \mathcal{O}^\times$.

Observación 1.3.8. Sea V un espacio cuadrático sobre un cuerpo F con $chF \neq 2$ y q la forma cuadrática asociada a V.

Si $\{v_i\}_i$ es una base de V entonces

$$f(x_1, \cdots, x_n) = q(\sum_{i=1}^{n} x_i v_i) = \sum_{i,j} b(v_i, v_j) x_i x_j$$

es una forma cuadrática sobre F.

Si $\{u_i\}_i$ es otra base de V entonces

$$f'(x_1, \cdots, x_n) = q\ (\sum_{i=1}^{n} x_i u_i)$$

es una forma cuadrática equivalente a f sobre F.

Observación 1.3.9. Una condición necesaria y suficiente para que dos espacios cuadráticos sobre el mismo cuerpo F sean isométricos es que las formas cuadráticas asociadas a ellos sean F-equivalentes.

1.4. Formas cuadráticas sobre dominios de Dedekind.

Sea F un cuerpo, $chF \neq 2$ y $\wp$ un primo no arquimidiano en F. Se define

$$\begin{aligned} \mathcal{O}(\wp) &= \{\alpha \in F \mid |\alpha|_\wp \leq 1\}, \\ \mathcal{U}(\wp) &= \{\alpha \in F \mid |\alpha|_\wp = 1\}, \\ \mathcal{M}(\wp) &= \{\alpha \in F \mid |\alpha|_\wp < 1\}, \end{aligned}$$

donde $|\ |_\wp$ denota una valuación en $\wp$.

Estas definiciones son claramente independientes de la elección de $|\ |_\wp$ en $\wp$.

Los elementos de $\mathcal{O}(\wp)$ se llaman enteros de F en $\wp$. Se verifica que $\mathcal{O}(\wp)$ es un anillo que contiene $1 \in F$ y $F = Quot\mathcal{O}(\wp)$.

Notación. Denotamos por $\mathbb{Q}_p$ la completación de $\mathbb{Q}$ con respecto a la métrica inducida por $|\ |_p$ y se llama cuerpo de números p-ádicos.

El anillo de enteros $\mathcal{O}_p$ de $\mathbb{Q}_p$ se denotará por $\mathbb{Z}_p$ y
$U_p = \{\alpha \in \mathbb{Q}_p | |\alpha|_p = 1\}$ es $\mathbb{Z}_p^\times$.

En esta sección S es un conjunto de Dedekind de primos en el cuerpo F que define un dominio de Dedekind $\mathcal{O} = \mathcal{O}(S) = \cap_{\wp \in S} \mathcal{O}(\wp)$.
$I = I(S)$ el grupo de ideales fraccionarios y $\mathcal{U} = \mathcal{U}(S)$ el grupo de unidades de $\mathcal{O}$. (Ver [O'M1], § 21 § 22).

V denota un espacio cuadrático sobre F, $dim\ V = n$, b y q las forma bilineal simétrica y forma cuadrática respectivamente asociadas a V.

Definición 1.4.1. Sea M un $\mathcal{O}$-submódulo de V. Diremos que M es un reticulado en V si existe una base $\{x_1, \cdots, x_n\}$ de V tal que $M \subseteq \mathcal{O}x_1 + \cdots + \mathcal{O}x_n$ y $FM = V$.

Definición 1.4.2. Un conjunto de vectores $\{x_1, \cdots, x_n\}$ es una base de un reticulado M si es base de FM y $M = \mathcal{O}x_1 + \cdots + \mathcal{O}x_n$.

Un reticulado que posee una base se llama libre. Dos bases de un reticulado libre tienen el mismo número de elementos, este número se llama dimensión de M y se denota $(dimM)$. (Ver [O'M1] pág. 212).

Observación 1.4.3. Todo $\mathcal{O}$-reticulado es libre cuando todo ideal fraccionario es principal. Así todo $\mathbb{Z}_p$-reticulado y todo $\mathbb{Z}$-reticulado es libre. (Ver [O'M1], pág. 48 y 213).

Es importante poder decidir cuando un conjunto de vectores es base de un reticulado. La siguiente proposición nos brinda información.

Proposición 1.4.4. Sea M un reticulado libre con base $\{x_1, \cdots, x_n\}$, y sean $y_1, \cdots, y_n$ vectores en M dados por $y_j = \sum_i a_{ij} x_i$, con $a_{ij} \in F$.

Entonces $\{y_1, \cdots, y_n\}$ es base de M si y sólo si la matriz $(a_{ij}) \in M_n(\mathcal{O})$ es unimodular, es decir $det(a_{ij}) \in \mathcal{U}$.

Demostración. Ver [O'M1], 81:9.

Definición 1.4.5. Sea L un reticulado en el espacio cuadrático V. Por scale de L entendemos el $\mathcal{O}$-módulo generado por el subconjunto $b(L, L)$ de F. Se denota por $s(L)$.

La norma de L es el $\mathcal{O}$-módulo generado por el subconjunto $q(L)$ de F y se denota por $\mathcal{N}(L)$.

$\mathcal{N}(L)$ y $s(L)$ son ideales fraccionarios o cero.

Como $b(x, x) = q(x)$ y $2b(x, y) = q(x + y) - q(x) - q(y)$ se tiene que $2s(L) \subseteq \mathcal{N}(L) \subseteq s(L)$.

Si $\mathcal{N}(L) = s(L)$ se dice que el reticulado L es propio, en otro caso se dice que es impropio.

Definición 1.4.6. Sea L un reticulado no cero. Por 81:3 de [O'M1] existe una base $\{x_1, \cdots, x_n\}$ de FL tal que $L = \mathfrak{R}_1 x_1 + \cdots + \mathfrak{R}_n x_n$, con $\mathfrak{R}_i \in I$.

Se define el volumen de L como

$$vL = \mathfrak{R}_1^2 \cdots \mathfrak{R}_n^2 d(x_1, \cdots, x_n),$$

donde

$$d(x_1, \cdots, x_n) = det(b(x_i, x_j)).$$

En el caso en que L es libre nos referimos al volumen como el discriminante de L y denotamos ambos por $d(L)$ o dL.

Definición 1.4.7. Sea L un reticulado de rango r en el espacio cuadrático V. Supongamos que $s(L) = \mathfrak{R}$, con $\mathfrak{R}$ ideal fraccionario. Si $vL = \mathfrak{R}^r$ entonces diremos que L es $\mathfrak{R}$-modular. Diremos que L es unimodular si es $\mathcal{O}$-modular.

En el caso en que L es libre, se tiene que L es unimodular si y sólo si la matriz asociada a L (en cualquier base) es unimodular. (Ver [O'M1], 82:13).

Definición 1.4.8. Sea L reticulado no cero en el espacio cuadrático regular V y $\mathfrak{R}$ un ideal fraccionario. Decimos que L es $\mathfrak{R}$-maximal en V si $\mathcal{N}(L) \subseteq \mathfrak{R}$ y para todo reticulado K en V tal que $L \subseteq K$ se tiene la siguiente propiedad:

$$\mathcal{N}(K) \subseteq \mathfrak{R} \Rightarrow K = L.$$

Decimos que L es maximal si es $\mathfrak{R}$-maximal, para algún $\mathfrak{R}$.

1.5. Formas cuadráticas sobre cuerpos locales.

Usaremos las mismas notaciones anteriores, salvo que ahora F es un cuerpo local, S consiste de un único primo $\wp$, $\mathcal{O}$ es el anillo de enteros $\mathcal{O}(\wp), \wp$ el ideal maximal $m(\wp)$ y $\mathcal{U}$ el grupo de unidades $\mathcal{U}(\wp)$ de $\mathcal{O}$.

Sea $|\ | = |\ |_\wp$ una valuación en $\wp$.

π denota un elemento primo de F en $\wp$.

Sea (V, b, q) espacio cuadrático regular sobre F.

Notemos que en este caso todo reticulado es libre. (Ver [O'M1], pág. 48).

Definición 1.5.1. Para $\alpha, \beta \in F^{\times}$ se define el símbolo de Hilbert de la siguiente manera:

$$\left(\frac{\alpha,\beta}{\wp}\right) = \begin{cases} 1 & \text{si } \langle\alpha\rangle \perp \langle\beta\rangle \perp \langle -1\rangle \text{ es isótropo sobre } F, \\ -1 & \text{en otro caso} \end{cases}$$

Definición 1.5.2. Sea $V \cong \langle\alpha_1\rangle \perp \cdots \perp \langle\alpha_n\rangle$ espacio cuadrático regular sobre F.

Se define el invariante de Hasse de V como

$$S_{\wp}(V) = \Pi_{1\leq i\leq j\leq n} \left(\frac{\alpha_i,\alpha_j}{\wp}\right).$$

Teorema 1.5.3. Los espacios cuadráticos U y V sobre F son isométricos si y sólo si

$$dimU = dimV, \quad dU = dV, \quad S_{\wp}U = S_{\wp}V.$$

Demostración. Ver [O'M1], 63:20.

Teorema 1.5.4. Sean U, V espacios cuadráticos sobre un cuerpo local, con $\nu = dimV - dimU \geq 0$. Entonces

a) $\nu = 0$

$U \rightarrow V \Longleftrightarrow U \cong V$

b) $\nu = 1$

$U \rightarrow V \Longleftrightarrow U \perp \langle dU \cdot dV\rangle \cong V$

c) $\nu = 2$ y $dU = -dV$

$U \rightarrow V \Longleftrightarrow U \perp \mathbf{H} \cong V$

$\mathbf{H}$ denota un plano hiperbólico.

d) $\nu \geq 3$

$U \to V$

Demostración: Ver [O'M1], 63:21.

Sea L un reticulado no cero en el espacio cuadrático V, entonces por 91C [O'M1], L se descompone en una suma ortogonal de reticulados modulares unidimensionales o bidimensionales. Agrupando las componentes de una tal descomposición se tiene que $L = L_1 \perp \cdots \perp L_r$ donde cada componente L_i es modular y $s(L_1) \supsetneq \cdots \supsetneq s(L_r)$. Una descomposición de este tipo se llama descomposición de Jordan de L.

Si suponemos que el cuerpo local F es no diádico (es decir, $2 \in \mathcal{U}$) se prueba [(O'M1], 92) que todo reticulado L tiene una descomposición ortogonal $L = L_1 \perp \cdots \perp L_r$, con L_i reticulados unidimensionales.

Usaremos el símbolo $A(\alpha, \beta)$ para denotar la matriz $A(\alpha, \beta) = \begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$ donde $\alpha, \beta \in \mathcal{O}$ y $-1 + \alpha\beta \in \mathcal{U}$. Estas condiciones nos garantizan que la matriz $A(\alpha, \beta)$ es unimodular.

El símbolo $\rho A(\alpha, \beta)$ denota la matriz $\begin{pmatrix} \rho\alpha & \rho \\ \rho & \rho\beta \end{pmatrix}$.

Ahora presentaremos dos teoremas ($[O'M2]$) que nos permiten decidir cuando un reticulado está representado por otro reticulado sobre el anillo local $\mathcal{O}$.

Definición 1.5.5. Sean π un elemento primo en un cuerpo local F y E un reticulado en el espacio cuadrático V sobre F. Si $E = \perp_1^t E_j$ es una descomposición de Jordan de E. Entonces se define $\mathcal{E}_i = \perp E_u$ donde u es tal que $1 \leq u \leq t$ y $s(E_u) \supseteq \pi^i \mathcal{O}$.

Teorema 1.5.6. Sea F cuerpo local no diádico, sean $E = \perp E_j$ y $E' = \perp E'_\ell$ descomposiciones de Jordan de los reticulados E y E'.

Supongamos que $\mathcal{E}_i$ y $\mathcal{E}'_i$ son los reticulados de la definición 1.5.5 para E y E' respectivamente. Entonces

$$E' \to E \quad \text{si y sólo si} \quad F\mathcal{E}'_i \to F\mathcal{E}_i, \quad \forall i.$$

Demostración: Ver [O'M2], pág. 850.

De aquí en adelante suponemos que F es un cuerpo local diádico, (es decir, $0 < |2| < 1$) en el cual 2 es un elemento primo.

Definición 1.5.7. Sea $E = \perp_1^t E_j$ una descomposición de Jordan del reticulado E. Se define:

1. $\mathcal{E}_{(i)} = \perp E_u$ donde u es tal que $1 \leq u \leq t$ y $\mathcal{N}(E_u) \supseteq 2^i\mathcal{O}$.
2. $\mathcal{E}_{[i]} = \perp E_u$ donde u es tal que $1 \leq u \leq t$ y $s(E_u) \supseteq 2^i\mathcal{O}$ y además se incluyen aquellos E_u impropios (es decir $\mathcal{N}(E_u) \subsetneq s(E_u)$) tales que $s(E_u) = 2^{i+1}\mathcal{O}$.
3. Si E tiene una componente propia 2^{i+1}-modular definimos $\Delta_i = 2^{i+1}\mathcal{O}$, si esto no ocurre y E tiene una componente propia 2^{i+2}-modular definimos $\Delta_i = 2^{i+2}\mathcal{O}$. En otro caso $\Delta_i = 0$.
4. Definimos $d_i = (d\mathcal{E}_i)\mathcal{O}$ y se define $d_i = 0$ cuando $\mathcal{E}_i = 0$.

Notemos que los reticulados $\mathcal{E}_i, \mathcal{E}_{(i)}$ y $\mathcal{E}_{[i]}$ satisfacen las siguientes relaciones:

$$\mathcal{E}_i = \begin{cases} \mathcal{E}_{(i)} & \text{si toda componente ortogonal de } \mathcal{E}_i \\ & \text{es una componente ortogonal de } \mathcal{E}_{(i)}, \\ \mathcal{E}_{(i+1)}, & \text{en otro caso.} \end{cases}$$

$$\mathcal{E}_{[i]} = \begin{cases} \mathcal{E}_i & \text{si toda componente ortogonal de } \mathcal{E}_{[i]} \\ & \text{es una componente ortogonal de } \mathcal{E}_i, \\ \mathcal{E}_{i+1}, & \text{en otro caso.} \end{cases}$$

Notación: Sean V espacio cuadrático sobre F y un ideal $\mathfrak{R} \subseteq F$. Si existe $\alpha \in q(V)$ tal que $\alpha\mathcal{O} = \mathfrak{R}$, escribimos $\mathfrak{R} \to V$.

Es claro que $\mathfrak{R} \to V$ si $\mathfrak{R} = 0$.

Si $\mathfrak{R} \to Fx$ con $q(x) = \alpha \in F$, escribimos $\mathfrak{R} \to \alpha$.

Proposición 1.5.8. Si $dimV \geq 3$ entonces $\mathfrak{R} \to V$, para todo $\mathfrak{R}$.

Demostración: Ver [O'M2], pág. 858.

Definición 1.5.9. Se dice que el reticulado E' es de menor tipo que E si las siguientes propiedades se cumplen para todo i:

1. $dim\mathcal{E}'_i \leq dim\mathcal{E}_i$
2. $d'_i d_i \to 1$ si $dim\mathcal{E}'_i = dim\mathcal{E}_i$
3. $\Delta'_i \subseteq \Delta_i + 2^{i+2}\mathcal{O}$ y $\Delta_{i-1} \subseteq \Delta'_{i-1} + 2^{i+1}\mathcal{O}$ si $dim\mathcal{E}'_i = dim\mathcal{E}_i$
4. $\Delta_{i-1} \subseteq \Delta'_{i-1} + 2^{i+1}\mathcal{O}$ si $dim\mathcal{E}_i - 1 = dim\mathcal{E}'_i > 0$ y $d_i d''_i \to 2^{i+1}$.
5. $\Delta'_i \subseteq \Delta_i + 2^{i+2}\mathcal{O}$ si $dim\mathcal{E}_i - 1 = dim\mathcal{E}'_i > 0$ y $d_i d'_i \to 2^i$.

Notemos que la definición es independiente de las descomposiciones de Jordan elegidas para los reticulados E' y E.

Proposición 1.5.10. Si $E' \to E$ entonces E' es de menor tipo que E.

Demostración: Ver [O'M2], pág. 859.

Notación: Como $2 \notin \mathcal{U}$, se tiene que existe $\rho \in \mathcal{U}$ tal que $x^2 + x + \rho$ es irreducible en F. (Ver [O'M2], pág. 851).

Notemos que si $\rho' \in \mathcal{U}$ es tal que $x^2 + x + \rho'$ es irreducible en F, entonces

$$1 + 4\rho \in (1 + 4\rho')\mathcal{U}^2.$$

Luego $\alpha(1 + 4\rho) \to V$ si y sólo si $\alpha(1 + 4\rho') \to V$.

Teorema 1.5.11. Sea E' reticulado de menor tipo que E. Entonces $E' \to E$ si y sólo si las siguientes propiedades se cumplen para todo i :

(I) $\Delta_i \to (F\mathcal{E}'_{[i]})^{\perp}$, donde el complemento ortogonal es tomado en $F\mathcal{E}_{(i+2)}$

(II) $\Delta'_i \to (F\mathcal{E}'_{[i]})^{\perp}$, donde el complemento ortogonal es tomado en $F\mathcal{E}_{(i+2)}$.

(III) $(F\mathcal{E}'_{[i]})^{\perp} \cong F\mathbf{H}$ implica $\Delta_i\Delta'_i \subseteq (\Delta'_i)^2$ donde $\mathbf{H}$ denota un plano hiperbólico y el complemento ortogonal es tomado como en (I) y (II).

(IV) $2^i \to (F\mathcal{E}'_i)^{\perp}$ o bien $2^i(1 + 4\rho) \to (F\mathcal{E}'_i)^{\perp}$, donde el complemento ortogonal es tomado en $F(\langle 2^i \rangle \perp \mathcal{E}_{(i+1)})$.

(V) $2^i \to (F\mathcal{E}'_{[i]})^{\perp}$ o bien $2^i(1 + 4\rho) \to (F\mathcal{E}'_{[i]})^{\perp}$, donde el complemento ortogonal es tomado como en (IV).

Demostración: Ver [O'M2], pág. 865.

CAPITULO II

Estimaciones

En este capítulo dejaremos establecidas algunas cotas necesarias para la estimación final de la constante N del teorema 0.5. (Ver Capítulo III, teorema 3.1).

Definición 2.1. Sea I un dominio propio de ideales principales contenido en un cuerpo F, suponemos $chF \neq 2$. Sea $e_1, \cdots, e_n$ una I-base de un reticulado Λ. Diremos que un vector $v = \sum_{i=1}^{n} \alpha_i e_i \in \Lambda$, $\alpha_i \in I$ es primitivo si el conjunto $\{\alpha_1, \cdots, \alpha_n\}$ genera el anillo I como ideal.

Se puede demostrar que un vector $v \in \Lambda$ es primitivo si y sólo si v es parte de una I-base de Λ.

Definición 2.2. Sea Λ un I-reticulado y $t \in I$. Diremos que t es representado por Λ sobre I si existe $v \in \Lambda$ tal que $q(v) = t$. El conjunto de elementos representados por Λ se denota por $q(\Lambda)$. Si $t = q(v)$ con $v \in \Lambda$ primitivo diremos que t es representado primitivamente por Λ sobre I. El conjunto de elementos representados primitivamente por Λ se denota por $q(\Lambda)^*$.

Lema 2.3. Sea L un $\mathbb{Z}_p$-reticulado en un espacio cuadrático regular isótropo de dimensión 4 sobre $\mathbb{Q}_p$. Entonces existe $u_0 \in L$ tal que $q(u_0) \neq 0$ y un reticulado $E \subseteq \langle u_0 \rangle^{\perp}$ con las siguientes propiedades:

i) $-q(u_0) \in q(E)$.

ii) Si $|q(u_0 + c)|_p < |q(u_0)|_p$ con $c \in E$, entonces $u_0 + c$ es un elemento primitivo de L.

iii) $U_p \subseteq \theta(E)$.

iv) E representa primitivamente todo $p^\alpha U_p$ donde $\alpha = ord_p q(u_0)$.

Este lema es un resultado de [Ca], pág. 243.

Supongamos que $t \in \mathbb{Z}_p$ con $|t|_p < |q(u_0)|_p$. Entonces $t = p^{\alpha+\beta}r$ con $\beta > 0$ y $r \in U_p$, luego $|p^\beta r - p^{-\alpha}q(u_0)|_p = 1$. Como E representa primitivamente todo $p^\alpha U_p$ entonces existe $v \in E$ primitivo tal que $q(v) = p^\alpha(p^\beta r - p^{-\alpha}q(u_0)) = t - q(u_0)$, y por lo tanto $q(v + u_0) = q(v) + q(u_0) = t$. Se tiene entonces el siguiente corolario del lema 2.3:

Corolario 2.4. Si $|t|_p < |q(u_0)|_p$ entonces $t \in q(L)^*$.

Proposición 2.5. Sea L un $\mathbb{Z}_p$-reticulado en un espacio cuadrático regular de dimensión 4 sobre $\mathbb{Q}_p$. Supongamos que $s(L) \subseteq \mathbb{Z}_p$.

Entonces $q(L) = \cup_{\text{finita}}\ q(u_i)\mathbb{Z}_p^2$, con $u_i \in L$, para todo i.

Además

$$ord_p\ q(u_i) \leq \begin{cases} 1 + ord_p d(L) & \text{si} \quad p \neq 2, \\ 3 + ord_p d(L) & \text{si} \quad p = 2. \end{cases}$$

Demostración: Estudiaremos por separado los casos L isótropo y L anisótropo.

Sea L isótropo:

Sea $t \in q(L)$. Consideremos el vector $u_0 \in L$ dado por el lema 2.3 y supongamos que $ord_p q(u_0) = \alpha$.

- Si $|t|_p < |q(u_0)|_p$ entonces $t = p^{\alpha+\beta} r$ con $r \in U_p$ y $\beta > 0$. Luego $t \in p^{\alpha+1}\epsilon_j \mathbb{Z}_p^2$ o bien $t \in p^{\alpha+2}\epsilon_j \mathbb{Z}_p^2$ con $\epsilon_j \in U_p/U_p^2$.

  Por el corolario 2.4 se tiene que $p^i\epsilon_j$ con $i > \alpha$ y $\epsilon_j \in U_p/U_p^2$ está representado primitivamente por L.

  Denotemos por u_{ij} vectores primitivos tales que $q(u_{ij}) = p^i\epsilon_j$. Entonces

  $$t \in \cup_{j=1}^{m} q(u_{\alpha+1,j})\mathbb{Z}_p^2 \cup q(u_{\alpha+2,j})\mathbb{Z}_p^2$$

  donde $m = |U_p/U_p^2|$.

- Si $|t|_p \geq |q(u_0)|_p$ entonces la clase de t en $\mathbb{Z}_p/U_p^2$ es un elemento del conjunto finito $\{p^i\epsilon_j\}_{i=1,\cdots,\alpha, j=1,\cdots,m}$.

Consideremos los elementos $p^i\epsilon_j$ con $i \in \{1,\cdots,\alpha\}$, $j \in \{1,\cdots,m\}$ tales que están representados por L, luego existen conjuntos $I \subseteq \{1,\cdots,\alpha\}$ y $J \subseteq \{1,\cdots,m\}$ tales que si $(i,j) \in I \times J$ entonces $p^i\epsilon_j \in q(L)$. Para cada $(i,j) \in I \times J$ elijamos un vector $u_{ij} \in L$ tal que $q(u_{ij}) = p^i\epsilon_j$. Como $t \in q(L)$ se tiene que existe $(i,j) \in I \times J$ tal que $t = q(u_{ij}) \cdot b^2$ con $b \in U_p$.

Por lo tanto

$$t \in \cup_{(i,j)\in I\times J} q(u_{ij})\mathbb{Z}_p^2.$$

Sea L anisótropo:

Consideremos el conjunto B de vectores primitivos en L,
$B = \{v \in L | \|v\| = 1\}$ y supongamos que L representa primitivamente un número infinito de clases en $\mathbf{Z}_p/U_p^2$.

Sea $U_p/U_p^2 = \{\epsilon_j\}_{j=1}^m$, entonces $\mathbf{Z}_p/U_p^2 = \{p^i\epsilon_j\}_{j=1,\cdots,m,i\geq 0}$. Luego todo conjunto infinito en $\mathbf{Z}_p/U_p^2$ contiene una sucesión que converge a cero. Por lo tanto existe una sucesión $\{v_n\} \subseteq B$ tal que $q(v_n) \to 0$ con la norma p-ádica, y como B es compacto existe una subsucesión $\{v_{n_k}\} \subseteq \{v_n\}$ la cual es convergente. Supongamos $v_{n_k} \to v$. Como L es cerrado se tiene que $v \in L$ y $q(v_{n_k}) \to q(v) = 0$, lo que contradice el hecho que L es anisótropo.

Por lo tanto L representa primitivamente sólo un número finito de clases en $\mathbf{Z}_p/U_p^2$. Sean $u_1, \cdots, u_\ell$ los vectores primitivos que representan a dichas clases.

Sea $t \in q(L)$ entonces $t = p^{2\beta}q(w)$ donde w es un vector primitivo en L y $\beta \geq 0$. Como w es un vector primitivo en L, se tiene que la clase de $q(w)$ en $\mathbf{Z}_p/U_p^2$ debe ser alguna de las clases representadas primitivamente por L. De este modo $q(w) \in q(u_i)U_p^2$ para algún $i \in \{1, \cdots, \ell\}$. Luego $t \in \cup_{\text{finita}} q(u_i)\mathbf{Z}_p^2$.

Probaremos ahora que para todo i se tiene que $ord_p q(u_i)$ es acotado y la cota depende sólo de $detL = d$.

Si $p \neq 2$ entonces podemos suponer que

$$L = \langle p^{a_1}w_1\rangle \perp \langle p^{a_2}w_2\rangle \perp \langle p^{a_3}w_3\rangle \perp \langle p^{a_4}w_4\rangle,$$

con $w_i \in U_p$, $i \in \{1,2,3,4\}$ y $a_1 \leq a_2 \leq a_3 \leq a_4$.

Consideremos el vector u_i y supongamos que $q(u_i) = p^b v$, con $v \in U_p$, y como $s(L) \subseteq \mathbf{Z}_p$ se tiene que $b \geq 0$.

Si $b \leq a_4$ entonces $ord_p q(u_i) = b \leq a_4 \leq ord_p d$.

Si $b > a_4$ entonces $b = a_4 + \epsilon + 2c$, con $\epsilon \in \{0,1\}$ y $c \geq 0$.

Consideremos el vector $\tilde{u}_i = p^{-c}u_i$, entonces

$$q(\tilde{u}_i) = p^{a_4+\epsilon}v \quad \text{y} \quad \mathbb{Z}_p u_i \subseteq \mathbb{Z}_p \tilde{u}_i = \tilde{N}.$$

Probaremos que $\tilde{N} \to L$. Para esto usaremos el teorema 1.5.6. Sean $\tilde{\eta}_i$ y $\mathcal{L}_i$ los reticulados de la definición 1.5.5. asociados a los reticulados $\tilde{N}$ y L respectivamente.

Se tiene que

$$\begin{array}{lll} \tilde{\eta}_i = \tilde{N} & \text{para} & i > a_4, \\ \mathcal{L}_i = L & \text{para} & i \geq a_4, \\ \tilde{\eta}_i = 0 & \text{para} & i < a_4. \end{array}$$

Como $\mathbb{Q}_p L$ es universal se tiene que $\mathbb{Q}_p \tilde{\eta}_i \to \mathbb{Q}_p \mathcal{L}_i$ para todo i.

Por lo tanto $\tilde{N} \to L$ y sin pérdida de generalidad podemos suponer que $\tilde{u}_i \in L$. Como $q(u_i) \in q(\tilde{u}_i)\mathbb{Z}_p^2$ se puede reemplazar u_i por $\tilde{u}_i$ y $ord_p q(\tilde{u}_i) = a_4 + \epsilon \leq 1 + ord_p d$.

Ahora veremos el caso $p = 2$. Sea $L = L_1 \perp \cdots \perp L_r$ una descomposición ortogonal del reticulado L donde cada L_i es 2^{a_i} modular unidimensional o bidimensional y supongamos que $a_1 \leq a_2 \leq \cdots \leq a_r$.

Igual que antes supongamos que $q(u_i) = 2^b v$, con $v \in U_2$ y $b \geq 0$.

Si $b \leq 2 + a_r$ entonces $ord_2 q(u_i) \leq 2 + ord_2 d$.

Si $b > 2 + a_r$ entonces $b = 2 + a_r + \epsilon + 2c$ con $\epsilon \in \{0, 1\}$ y $c \geq 0$.

Sea $\tilde{u}_i = 2^{-c}u_i$ entonces $q(\tilde{u}_i) = 2^{2+a_r+\epsilon}v$ y $N = \mathbb{Z}_2 u_{i2} \subseteq \mathbb{Z}_2 \tilde{u}_i = \tilde{N}$.

Probaremos que $\tilde{N} \to L$ usando el teorema 1.5.11. Denotaremos por η_i, $\tilde{\eta}_i$, $\mathcal{L}_i$ los reticulados de la definición 1.5.5, correspondientes a los reticulados $N, \tilde{N}$ y L respectivamente. Denotaremos por $\eta_{(i)}, \tilde{\eta}_{(i)}, \mathcal{L}_{(i)}, \eta_{[i]}, \tilde{\eta}_{[i]}, \mathcal{L}_{[i]}$ los reticulados correspondientes a $N, \tilde{N}$ y L respectivamente en la definición 1.5.7, (1) y (2). Los ideales de la definición 1.5.7 (3) asociados a N, $\tilde{N}$ y L se denotarán por δ_i, $\tilde{\delta}_i$

y Δ_i respectivamente. Por último denotaremos por $d_i = d(\eta_i)\mathbf{Z}_2$, $\tilde{d}_i = d(\tilde{\eta}_i)\mathbf{Z}_2$ y $D_i = d(\mathcal{L}_i)\mathbf{Z}_2$ los ideales de la definición 1.5.7 (4), correspondiente a los reticulados N, $\tilde{N}$ y L respectivamente.

Entonces se tiene lo siguiente:

$$\tilde{\eta}_i = \begin{cases} 0 & \text{si} \quad i < 2 + a_r, \\ 0 & \text{si} \quad i = 2 + a_r \quad \text{y} \quad \epsilon = 1, \\ \tilde{N} & \text{si} \quad i = 2 + a_r \quad \text{y} \quad \epsilon = 0, \\ \tilde{N} & \text{si} \quad i > 2 + a_r. \end{cases}$$

$$\mathcal{L}_i = \begin{cases} L & \text{si} \quad i \geq a_r, \\ \\ 0 & \text{si} \quad i < a_1. \end{cases}$$

Si $i < a_r$ entonces $\tilde{d}_i = 0$, $\tilde{\delta}_i = 0$, $\tilde{\delta}_{i-1} = 0$.

Si $i < a_1 - 1$ entonces $\Delta_{i-1} = 0$.

Si $i = a_1 - 1$ entonces $\Delta_{i-1} = 0$ o $\Delta_{i-1} = 2^{a_1}\mathbf{Z}_2$.

Veamos ahora que $\tilde{N}$ tiene menor tipo que L. (Definición 1.5.9):

Claramente $dim\ \tilde{\eta}_i \leq dim \mathcal{L}_i$ para todo i.
$dim\ \tilde{\eta}_i = dim\ \mathcal{L}_i$ si y sólo si $i < a_1$. Luego $\tilde{d}_i = 0$ y por lo tanto $\tilde{d}_i D_i \to 1$.
Además

$$\tilde{\delta}_i \subseteq \Delta_i + 2^{i+2}\mathbf{Z}_2 \qquad \text{y} \qquad \Delta_{i-1} \subseteq \tilde{\delta}_{i-1} + 2^{i+1}\mathbf{Z}_2.$$

Por último $dim\ \mathcal{L}_i - 1 \neq dim\ \tilde{\eta}_i$, para todo i tal que $dim\ \tilde{\eta}_i > 0$.

Luego valen las propiedades 1, . . . , 5 de la definición 1.5.9.

Ahora verifiquemos las hipótesis del teorema 1.5.11:

I. $\Delta_i \to (\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp}$ donde el complemento ortogonal es tomado en $\mathfrak{Q}_2\mathcal{L}_{(i+2)}$:

Si $i \geq 2 + a_r$ entonces $\Delta_i = 0$. Luego $\Delta_i \to (\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp}$.

Si $i < 2 + a_r$ entonces $\tilde{\eta}_{[i]} = 0$. Como $2 + a_r < b$ se tiene que $\eta_{[i]} = 0$, luego

$$(\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp} = (\mathfrak{Q}_2\eta_{[i]})^{\perp} = \mathfrak{Q}_2\mathcal{L}_{(i+2)}.$$

Como $N \to L$, entonces se tiene por proposición 1.5.10 y teorema 1.5.11 que

$$\Delta_i \to (\mathfrak{Q}_2\eta_{[i]})^{\perp} = (\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp}.$$

II. $\tilde{\delta}_i \to (\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp}$ donde el complemento ortogonal es tomado en $\mathfrak{Q}_2\mathcal{L}_{(i+2)}$:

Si $i > 2 + a_r$ entonces $\tilde{\delta}_i = 0$. Luego $\tilde{\delta}_i \to (\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp}$.

Si $a_r \leq i \leq 2 + a_r$ entonces $\mathcal{L}_{(i+2)} = L$ y $\tilde{\eta}_{[i]} = \tilde{\eta}_i$. Luego $dim(\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp} \geq 3$ y por proposición 1.5.8 se tiene $\tilde{\delta}_i \to (\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp}$.

Si $i < a_r$ entonces $\tilde{\delta}_i = 0$. Luego $\tilde{\delta}_i \to (\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp}$.

III. $(\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp} \cong \mathfrak{Q}_2\mathbf{H}$ implica $\Delta_i\tilde{\delta}_i \subseteq (\tilde{\delta}_i)^2$ donde $\mathbf{H}$ denota un plano hiperbólico y el complemento ortogonal es tomado como en I y II:

Si $i < a_r$ entonces $\tilde{\delta}_i = 0$. Luego $\Delta_i\tilde{\delta}_i \subseteq (\tilde{\delta}_i)^2$.

Si $a_r \leq i < 2 + a_r$ entonces $\mathcal{L}_{(i+2)} = L$ y $\tilde{\eta}_{[i]} = 0$. Luego $dim(\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp} = 4$. Por lo tanto la hipótesis $(\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp} \cong \mathfrak{Q}_2\mathbf{H}$ es vacía.

Si $i \geq 2 + a_r$ entonces $\Delta_i = 0$. Luego $\Delta_i\tilde{\delta}_i \subseteq (\tilde{\delta}_i)^2$.

IV. $2^i(1+4w) \rightarrow (\mathfrak{Q}_2\tilde{\eta}_i)^{\perp}$ donde el complemento ortogonal es tomado en $\mathfrak{Q}_2(\langle 2^i\rangle \perp \mathcal{L}_{(i+1)})$:

Si $i < 2 + a_r$ entonces $\tilde{\eta}_i = 0$. Como $2 + a_r < b$ se tiene que $\eta_i = 0$ luego

$$(\mathfrak{Q}_2\tilde{\eta}_i)^{\perp} = (\mathfrak{Q}_2\eta_i)^{\perp} = \mathfrak{Q}_2(\langle 2^i\rangle \perp \mathcal{L}_{(i+1)}).$$

Como $N \rightarrow L$ entonces se tiene por proposición 1.5.10 y teorema 1.5.11 que $2^i(1 + 4w) \rightarrow (\mathfrak{Q}_2\eta_i)^{\perp} = (\mathfrak{Q}_2\tilde{\eta}_i)^{\perp}$.

Si $i \geq 2 + a_r$ entonces $\mathcal{L}_{(i+1)} = L$ y $dim\mathfrak{Q}_2(\langle 2^i\rangle \perp \mathcal{L}_{(i+1)}) = 5$. Luego $dim(\mathfrak{Q}_2\tilde{\eta}_i)^{\perp} \geq 4$. Como el espacio $(\mathfrak{Q}_2\tilde{\eta}_i)^{\perp}$ es universal, representa a $2^i(1 + 4w)$.

V. $2^i(1 + 4w) \rightarrow (\mathfrak{Q}_2\tilde{\eta}_{[i]})^{\perp}$ donde el complemento ortogonal es tomado igual que en IV:

En este caso $\tilde{\eta}_{[i]} = \tilde{\eta}_i$, para todo i. Luego es lo mismo que IV.

Hemos probado que $\tilde{N} \rightarrow L$ y sin pérdida de generalidad podemos suponer que $\tilde{N} = \mathbb{Z}\tilde{u}_i \subseteq L$. Como $q(u_i) \in q(\tilde{u}_i)\mathbb{Z}_2^2$ podemos reemplazar u_i por $\tilde{u}_i$ y $ord_2q(\tilde{u}_i) = 2 + a_r + \epsilon \leq 3 + ord_2d$.

□

Lema 2.6. Sea Δ un $\mathbf{Z}_p$-reticulado en un espacio cuadrático regular sobre $\mathbf{Q}_p$, supongamos que $s(\Delta) \subseteq \mathbf{Z}_p$. Entonces existe $N \in \mathbf{N}$ tal que para todo $b \in \mathbf{Z}_p$ se tiene $q(\Delta)^* + p^N b \subseteq q(\Delta)^*$ y por lo tanto $q(\Delta)^*$ es un abierto en $\mathbf{Q}_p$.

Además se puede elegir

$$N = \begin{cases} 1 + 2ord_p d\Delta & \text{si} \quad p \neq 2, \\ 5 + 2ord_p d\Delta & \text{si} \quad p = 2. \end{cases}$$

Demostración: Sea $p \neq 2$. Entonces $\Delta = \langle p^{a_1} u_1 \rangle \perp \cdots \perp \langle p^{a_n} u_n \rangle$ con $u_i \in U_p$ y $a_i \geq 0$.

Supongamos que $t = q(w_1, \cdots, w_n) \in q(\Delta)^*$. Como $(w_1, \cdots, w_n)$ es primitivo podemos suponer sin pérdida de generalidad que $w_1 \in U_p$.

Consideremos en $\mathbf{Z}_p[x]$ el polinomio

$$f(x) = p^{a_1} u_1 x^2 + \sum_{i=2}^{n} p^{a_i} u_i w_i^2 - t - p^N b$$

entonces

$$|f(w_1)|_p = |p^N b|_p \leq \frac{1}{p^N} < \frac{1}{p^{2a_1}} = |2p^{a_1} u_1 w_1|_p^2 = |f'(w_1)|_p^2$$

Por lema de Hensel ([Ca] pág. 47) existe $c \in U_p$ tal que $f(c) = 0$, luego $t + p^N b \in q(\Delta)^*$.

Sea $p = 2$. Entonces $\Delta = \ell_1 \perp \cdots \perp \ell_m$ donde cada ℓ_i es un $\mathbf{Z}_2$-reticulado 2^{a_i} modular. Si ℓ_i tiene matriz $[\ell_i] = 2^{a_i} A_i$ entonces podemos suponer que A_i es una de las siguientes matrices:

$$A_i = [u_i] \quad \text{con} \quad u_i \in U_2,$$

$$A_i = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix},$$

$$A_i = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Basta demostrar que para estos tres tipos de reticulados se tiene la propiedad $q(\ell_i)^* + 2^N b \subseteq q(\ell_i)^*$ con $N = 5 + 2ord_2 d\Delta$.

- Si ℓ_i es unidimensional, es decir $\ell_i = \langle 2^a u \rangle$. Supongamos que $t \in q(\ell_i)^*$ entonces $t = 2^a u w^2$ con $w \in U_p$. Igual que en el caso $p \neq 2$ se considera el polinomio $f(x) = 2^a u x^2 - t - 2^N b$ en $\mathbb{Z}_2[x]$. Entonces

$$|f(w)|_2 = |2^N b|_2 \leq \frac{1}{2^N} < |2^{a+1} w|_2^2 = |f'(w)|_2^2.$$

  Por lema de Hensel existe $c \in U_2$ tal que $f(c) = 0$, luego $t + 2^N b \in q(\ell_i)^*$.

- Si $[\ell_i] = 2^a \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ y $t \in q(\ell_i)^*$ entonces $t = q(w_1, w_2) = 2^{a+1}(w_1^2 + w_1 w_2 + w_2^2)$. Sin pérdida de generalidad supongamos que $w_1 \in U_2$. Consideremos el polinomio $f(x) = 2^{a+1}(x^2 + w_1 w_2 + w_2^2) - t - 2^N b$ en $\mathbb{Z}_2[x]$. Entonces

$$|f(w_1)|_2 = |2^N b|_2 < \frac{1}{2^N} \leq \frac{1}{2^{2a_1+5}} < |2^{a+2} w_1|_2^2 = |f'(w_1)|_2^2.$$

  Por lema de Hensel existe $c \in U_2$ tal que $f(c) = 0$, luego $t + 2^N b \in q(\ell_i)^*$.

- Si $\ell_i = 2^a \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ y $t \in q(\ell_i)^*$ entonces $t = q(w_1, w_2) = 2^{a+1} w_1 w_2$ y sin pérdida de generalidad podemos suponer que $w_1 \in U_2$ y aplicar lema de Hensel al polinomio $f(x) = 2^{a+1} w_1 x - t - 2^N b$ en $\mathbb{Z}_2[x]$.

□

Corolario 2.7. Sea Δ un $\mathbb{Z}_p$-reticulado isótropo en un espacio cuadrático regular sobre $\mathbb{Q}_p$, tal que $s(\Delta) \subseteq \mathbb{Z}_p$.

Sea

$$N = \begin{cases} 1 + 2ord_p d\Delta & \text{si} \quad p \neq 2, \\ 5 + 2ord_p d\Delta & \text{si} \quad p = 2. \end{cases}$$

Entonces para todo $b \in \mathbb{Z}_p$ se tiene

i) $p^N b \in q(\Delta)^*$

ii) Si $t \in q(\Delta)$ entonces existe m, $0 \leq m \leq \frac{N-1}{2}$ tal que $p^{-2m}t \in q(\Delta)^*$.

iii) $q(\Delta) + p^{2N-1}b \subseteq q(\Delta)$.

Demostración:

(i) Δ es isótropo, luego $0 \in q(\Delta)^*$ y por lema 2.6 se tiene que $p^N b = 0 + p^N b \in q(\Delta)^*$.

(ii) $t \in q(\Delta)$, luego $t = p^{2\ell}q(v)$ con $\ell \geq 0$ y v vector primitivo en Δ.

Si $0 \leq \ell \leq \frac{N-1}{2}$ entonces $p^{-2\ell}t = q(v) \in q(\Delta)^*$. Se elige $m = \ell$.

Si $\ell > \frac{N-1}{2}$ entonces $2\ell \geq N$, luego por (i): $p^0 t = t = p^{2\ell}q(v) = p^N(p^{2\ell-N}q(v)) \in q(\Delta)^*$. Se elige $m = 0$.

(iii) Sea $t \in q(\Delta)$. Entonces existe m, $0 \leq m \leq \frac{N-1}{2}$ tal que $p^{-2m}t \in q(\Delta)^*$. Luego por lema 2.6 se tiene

$$t + p^{2N-1}b = p^{2m}(p^{-2m}t + p^{2N-1-2m}b) \in p^{2m}q(\Delta)^* \subseteq q(\Delta).$$

□

Lema 2.8. Sea Δ un $\mathbf{Z}_p$-reticulado en un espacio cuadrático regular sobre $\mathbf{Q}_p$, tal que $dim\Delta \geq 2$ y $\mathcal{N}(\Delta) \subseteq p^{\alpha}\mathbf{Z}_p$. Sea $a \in \mathbf{Z}$ tal que

$$\alpha > \begin{cases} ord_p a & \text{si} \quad p \neq 2, \\ 2 + ord_p a & \text{si} \quad p = 2. \end{cases}$$

Entonces $q(\Delta \perp \langle a \rangle)^* \subseteq q(\Delta)^* + a\mathbf{Z}_p^2$.

Demostración: Sea $t \in q(\Delta \perp \langle a \rangle)^*$ luego $t \in q(x) + ay^2$ con (x, y) vector primitivo, $x \in \Delta$, $y \in \mathbf{Z}_p$.

Si x es primitivo entonces $t \in q(\Delta)^* + a\mathbf{Z}_p^2$.

Si $x \in \Delta$ no es primitivo entonces $y \in U_p$ y $x = p^{\beta}x'$ con $\beta > 0$, $x' \in \Delta$ primitivo o $x = 0$.

Probaremos que existe $\sigma \in O(\Delta \perp \langle a \rangle)$ tal que $\sigma(x, y) = (\tilde{x}, \tilde{y})$ con $\tilde{x}$ primitivo en Δ. En tal caso

$$t = q(x, y) = q(\tilde{x}, \tilde{y}) \in q(\Delta)^* + a\mathbf{Z}_p^2.$$

Sea $(z, u) \in \Delta \perp \langle a \rangle$ con z primitivo y $u \in \mathbf{Z}_p$. Entonces

$$\begin{aligned} \tau_{(z,u)}(x, y) &= (x, y) - 2\tfrac{b((x,y),(z,u))}{q(z,u)}(z, u) \\ &= (x, y) - 2b\tfrac{b(x,z)+auy}{q(z)+au^2}(z, u) \\ &= (x - \lambda z, y - \lambda u) \end{aligned}$$

con

$$\lambda = 2\ \frac{b(x, z) + auy}{q(z) + au^2}$$

Es claro que si $z \in \Delta$ es un vector primitivo y $\lambda \in U_p$ entonces $\tilde{x} = x - \lambda z$ es primitivo.

Si $x \neq 0$ elegimos $z \in \langle x' \rangle^{\perp}$, z primitivo.

Si $x = 0$ basta z primitivo.

En cualquier caso tenemos

$$\lambda = \frac{2auy}{q(z) + au^2}$$

$q(z) \in p^{\alpha}\mathbf{Z}_p$ con $\alpha > ord_p a$ si $p \neq 2$ y $\alpha > 2 + ord_2 a$ si $p = 2$.

Sea $p \neq 2$ y $u \in U_p$. Entonces

$$\begin{aligned} ord_p(2auy) &= ord_p a \\ ord_p(q(z) + au^2) &= ord_p a \end{aligned}$$

Si $p = 2$ y $u \in 2U_2$ entonces

$$\begin{aligned} ord_2(2auy) &= 2 + ord_2 a \\ ord_2(q(z) + au^2) &= 2 + ord_2 a \end{aligned}$$

Luego en ambos casos $\lambda \in U_p$. □

Introduciremos algunas definiciones y lemas previos necesarios para demostrar la proposición 2.14, la cual será fundamental en la estimación de la constante N del teorema 0.5 (Teorema 3.1 Capítulo III).

Definición 2.9. Sea $P = \{p_1, \cdots, p_n\}$ un conjunto finito de primos. Definamos el anillo $\mathbf{Z}[P] := \mathbf{Z}[p_1^{-1}, \cdots, p_n^{-1}]$.

Si $P = \phi$ definimos $\mathbf{Z}[P] := \mathbf{Z}$.

Definición 2.10. Sea (V, q) un espacio cuadrático sobre $\mathbf{Q}$, P un conjunto finito de primos y E un $\mathbf{Z}[P]$-reticulado en V. Se definen los siguientes conjuntos:

$$\text{clas}_P E = \left\{ K \middle| \begin{array}{c} K \text{ es } \mathbf{Z}[P] - \text{reticulado en } V \text{ tal que} \\ K = \sigma(E) \text{ para algún } \sigma \in O(V) \end{array} \right\},$$

$$\mathrm{spn}_P E = \left\{ K| \quad \begin{array}{l} K \text{ es } \mathbf{z}[P] - \text{reticulado en } V \text{ tal que existen} \\ \sigma \in O(V) \text{ y } \Sigma_p \in O'(V_p) \text{ que satisfacen} \\ \sigma(K_p) = \Sigma_p(E_p) \text{ para todo } p \notin P \end{array} \right\},$$

$$\mathrm{gen}_P E = \left\{ K| \quad \begin{array}{l} K \text{ es } \mathbf{z}[P] - \text{reticulado en } V \text{ tal que para todo} \\ p \notin P \text{ existe } \sigma_p \in O(V_p) \text{ que satisface } K_p = \sigma_p(E_p) \end{array} \right\}.$$

Si $P = \phi$ en lugar de $clas_P E$, $spn_P E$ $gen_P E$ escribimos $clsE$, $spnE$, $genE$ respectivamente. Si $K \in cls_P E$ se dice que K y E pertenecen a la misma clase sobre $\mathbf{z}[P]$.

Si $K \in spn_P E$ se dice que K y E pertenecen al mismo género espinorial sobre $\mathbf{z}[P]$.

Si $K \in genE$ se dice que pertenecen al mismo género sobre $\mathbf{z}[P]$.

En los tres casos se obtienen relaciones de equivalencia sobre el conjunto de los $\mathbf{z}[P]$-reticulados sobre V.

Es claro que $cls_P E \subseteq spn_P E \subseteq gen_P E$.

Notación: Sea E un $\mathbf{z}$-reticulado denotaremos por $\bar{q}(E)$ y $\bar{q}(E)^*$ los siguientes conjuntos:

$$\bar{q}(E) = \{t \in \mathbf{z} | t \in q(E_p),\ \forall_p \text{ incluso } p = \infty\},$$

$$\bar{q}(E)^* = \{t \in \mathbf{z} | t \in q(E_p)^*,\ \forall_p \text{ incluso } p = \infty\}.$$

Es claro que $q(E) \subseteq \bar{q}(E)$.

El siguiente lema es un resultado básico del trabajo [HKK]:

Lema 2.11. Sea E un $\mathbf{Z}$-reticulado positivo definido , $dimE \geq 3$, $genE = spnE$. Supongamos que ℓ es un primo finito tal que $\mathbf{Q}_\ell E$ es isótropo. Entonces existe un número natural s tal que $\bar{q}(\ell^s E) \subseteq q(E)$.

Demostración: Sean $E^{(1)}, \cdots, E^{(h)}$ los representantes de las clases en $genE$. Como $genE = spnE$ y $\mathbf{Q}_\ell E$ es isótropo podemos aplicar el teorema 8.3, pág. 232 [Ca] y concluir que los reticulados $\mathbf{Z}[\ell^{-1}]E^{(i)} \in cls\mathbf{Z}[\ell^{-1}]E$. Por lo tanto para cada $i = 1, \cdots, h$ podemos suponer que $\mathbf{Z}[\ell^{-1}]E^{(i)} = \mathbf{Z}[\ell^{-1}]E$. Luego existe un entero $s \geq 1$ tal que $\ell^s E^{(i)} \subseteq E$ para todo $i = 1, \cdots, h$.

Ahora supongamos que $t \in \bar{q}(\ell^s E)$, es decir t es representado por $\ell^s E$ sobre $\mathbf{Z}_p$ para todo p, incluso $p = \infty$. Luego t es representado sobre $\mathbf{Z}$ por algún reticulado $M \in gen(\ell^s E)$. Esto último se obtiene por 102:5 de [O'M1] y como $M = \ell^s E^{(i)} \subseteq E$ para algún $i = 1, \cdots, h$, se tiene que $t \in q(E)$.

□

Para el desarrollo de nuestro trabajo es fundamental hacer una estimación de todas las constantes que intervienen en la demostración del teorema 0.5, en particular será necesario acotar el entero s del lema 2.11.

Es claro que basta estimar un entero s tal que $\ell^s E^{(i)} \subseteq E$ para todo $i = 1, \cdots, h$.

En [Ic2], prop. 4 se muestra que, si el reticulado E_ℓ es isótropo y maximal entonces basta elegir $s = h(E) - 1$ donde $h(E)$ es el número de clases en $spnE$.

El entero s se determina usando la siguiente construcción de [BH2]:

Sean L y K $\mathbf{Z}$-reticulados en un espacio cuadrático V sobre $\mathbf{Q}$, $dimV \geq 3$. Supongamos que L_p y K_p son $\mathbf{Z}_p$ maximales para un primo

p. Entonces por 82:23 de [O'M1] existe una base $\{e_1, f_1, \cdots, e_t, f_t, z_{2t+1}, \cdots, z_n\}$ para L_p, tal que $q(e_i) = q(f_i) = 0$, $b(e_i, f_j) = \delta_{ij}$, $0 = b(e_i, e_j) = b(f_i, f_j)$ para $i \neq j$, $b(e_i, z_k) = b(f_i, z_k) = 0$. El subespacio generado por $\{z_{2t+1}, \cdots, z_n\}$ es anisótropo, y

$$K_p = (\mathbb{Z}_p p^{a_1})e_1 + (\mathbb{Z}_p p^{-a_1})f_1 + \cdots + (\mathbb{Z}_p p^{a_t})e_t + (\mathbb{Z}_p p^{-a_t})f_t + \mathbb{Z}_p z_{2t+1} + \cdots + \mathbb{Z}_p z_n$$

donde $a_1, \cdots, a_t$ son enteros no negativos.

Entonces $[L_p : L_p \cap K_p] = [K_p : L_p \cap K_p] = p^{a_1 + \cdots + a_t}$.

Al par (L, p) se le asocia un grafo $\mathbb{Z}(L : p)$, cuyos vértices son aquellos $\mathbb{Z}$-reticulados $K \in genL$ tales que $K_q = L_q$ para todo $q \neq p$.

La función distancia entre los vértices se define como $dis(L, K, p) := r$ si y sólo si $[L_p : L_p \cap K_p] = p^r$.

Diremos que los reticulados K y L son vecinos si $r = 1$. Notemos que si $r = 1$ entonces podemos suponer que $a_1 = 1$ y $a_i = 0$, $\forall i > 1$. Dos vértices están conectados por una arista simple si y sólo si ellos son vecinos.

El grafo $\mathbb{Z}(L : p)$ es conexo. Se tiene además que si $K \in cls^+L$ entonces los vecinos de K pertenecen a la misma clase propia de los vecinos de L. (Ver [BH1], [BH2]).

Si L_p es isótropo entonces el grafo $\mathbb{Z}(L : p)$ contiene a los representantes de cada clase en $spnL$. (Ver [O'M1], 104:5).

Usando lo anterior M. Icaza (ver [Ic2]), demostró el siguiente lema:

Lema 2.12. Sea E un $\mathbb{Z}$-reticulado positivo definido, $dim\ E \geq 3$, $genE = spnE$. Supongamos que ℓ es un primo tal que E_ℓ es isótropo y maximal.

Sean $E^{(1)}, \cdots, E^{(h)}$ representantes de las clases en $spnE$. Entonces $\ell^{h-1}E^{(i)} \subseteq E$, $\forall i = 1, \cdots, h$.

En particular, $\ell^s E^{(i)} \subseteq E, \quad \forall s \geq h-1.$

Observación 2.13. Ahora es necesario calcular una cota para $s = h(E) - 1$, donde $h(E)$ es el número de clases en $spn\ E = gen\ E$. Entonce basta acotar $h(E)$ por el número de clases con determinante dE.

M. Icaza obtiene el siguiente resultado contando el número de las posibles matrices reducidas según Minkowski de un determinante dado D (ver [Ic1] pag. 38):

Sea E es un reticulado n dimensional, con $detE = D$. Entonces

$$h(E) \leq (\frac{4}{3})^{n(n-1)/2} \tau_n^{(n-2)} D^{n-1}$$

donde

$$\tau_n = \begin{cases} (\frac{2}{\pi})^n [\Gamma(2+\frac{n}{2})]^2 & \text{si} \quad n \leq 4 \\ (\frac{2}{\pi})^n [\Gamma(2+\frac{n}{2})]^2 (\frac{5}{4})^{(n-3)(n-4)/2} & \text{si} \quad n > 4 \end{cases}$$

Para estimar la constante N del teorema 0.5 (teorema 3.1), construiremos un reticulado E que satisface todas las hipótesis de la siguiente proposición.

Proposición 2.14. Sean E, ℓ, s como en el lema 2.11. Consideremos un entero positivo a y P el conjunto finito de primos definido por $P := \{p | p/d(\ell^s E)\} \cup \{2\}$. Supongamos que para los enteros n y m se satisface para cada $p \in P$, lo siguiente:

$$\cup_{i=0}^{n}\ p^{2i} q(\ell^s E_p) \perp \langle a \rangle)^* \subseteq \cup_{i=0}^{m}\ p^{2i} q(\ell^s E_p)^* + a\mathbb{Z}_p^2.$$

Entonces para todo entero t tal que $t \in \cup_{i=0}^{n}\ p^{2i} q(\ell^s E_p \perp \langle a \rangle)^*, \quad \forall p \in P$ y $t \geq 2^8 a [d(\ell^s E)]^{6+4m}$ se tiene que $t \in q(E \perp \langle a \rangle)$.

Demostración: $q(\ell^s E_p \perp \langle a \rangle)^*$ es compacto. Luego

$$C_p =: \cup_{i=0}^{n} p^{2i} q(\ell^s E_p \perp \langle a \rangle)^*$$

es compacto.

La hipótesis $C_p \subseteq \cup_{i=0}^{m} p^{2i} q(\ell^s E_p)^* + a\mathbf{Z}_p^2$ y el hecho que C_p es compacto, implica que para cada $p \in P$ existen $w_{p,j_p} \in \mathbf{Z}_p$ y $N \in \mathbf{N}$ tal que

$$C_p \subseteq \cup_{\substack{1 \leq i_p \leq m \\ 1 \leq j_p \leq N}} p^{2i_p} q(\ell^s E_p)^* + a w_{p,j_p}^2.$$

Luego

$$\Pi_{p \in P} C_p \subseteq \cup_{\text{finita}} \Pi_{p \in P} p^{2i_p} q(\ell^s E_p)^* + a w_{p,j_p}^2$$

Para cada colección $\{(w_{p,j_p}\}_{p \in P}$ existe $w_j \in \mathbf{Z}$ tal que para cada $p \in P$, se tiene $|w_{p,j_p} - w_j|_p < \epsilon$ con $\epsilon = \Pi_{p \in P} p^{-\beta_p}$ donde

$$\beta_p = \begin{cases} 1 + 2m + 2ord_p d(\ell^s E) & \text{si} \quad p \neq 2, \\ 5 + 2m + 2ord_p d(\ell^s E) & \text{si} \quad p = 2. \end{cases}$$

(ver [Ca], pág. 44).

Como $|w_{p,j_p} - w_j|_p < \epsilon$ y $a \in \mathbf{Z}$ se tiene que $a w_{p,j_p}^2 = a w_j^2 + p^{\beta_p} b$ con $b \in \mathbf{Z}_p$, luego

$$p^{2i_p} q(\ell^s E_p)^* + a w_{p,j_p}^2 = p^{2i_p} [q(\ell^s E_p)^* + p^{\beta_p - 2i_p} b] + a w_j^2.$$

Entonces por lema 2.6, para todo $p \in P$ y $0 \leq i_p \leq m$ se tiene

$$p^{2i_p} q(\ell^s E_p)^* + a w_{p,j_p}^2 \subseteq p^{2i_p} q(\ell^s E_p)^* + a w_j^2. \tag{2.15}$$

Si $w_j > \Pi_{p \in P} p^{\beta_p}$, entonces existen enteros b y $\tilde{w}_j$ tales que
$w_j = (\Pi_{p \in P} p^{\beta_p}) b + \tilde{w}_j$ y $0 \leq \tilde{w}_j < \Pi_{p \in P} p^{\beta_p}$.

Aplicando nuevamente el lema 2.6, se tiene que

$$p^{2i_p}q(\ell^s E_p)^* + aw_j^2 \subseteq p^{2i_p}q(\ell^s E_p)^* + a\tilde{w}_j^2.$$

Luego podemos suponer que

$$0 \leq w_j \leq \Pi_{p\in P}\ p^{\beta_p} \leq 2^4[d(\ell^s E)]^{3+2m}.$$

Sea $W = 2^4[d(\ell^s E)]^{3+2m}$.

Supongamos que $t \in C_p$, para todo $p \in P$ y $t \geq aW^2$, entonces

$$(t,\cdots,t) \in \Pi_{p\in P}C_p \subseteq \cup_{\text{finita}}\Pi_{p\in P}\ p^{2i_p}q(\ell^s E_p)^* + aw_{p,j_p}^2.$$

Luego para cada $p \in P$, se tiene que t pertenece a un conjunto del tipo $p^{2i_p}q(\ell^s E_p)^* + aw_{p,j_p}^2$.

Consideremos la colección $\{w_{p,j_p}\}_{p\in P}$, y $w_j \in \mathbf{Z}$ que satisface (2.15), entonces podemos suponer que $w_j \leq W$ y luego $t \geq aw_j^2$.

Sea $\{(w_p)\}_{p\in P}$ la colección correspondiente a t y $w_j \in \mathbf{Z}$ que satisface 2.15, entonces $t \geq aw_j^2$ y se tiene:

Si $p \in P$, entonces $t - aw_j^2 \in p^{2i_p}q(\ell^s E_p)^* \subseteq q(\ell^s E_p)$.

Si $p \notin P$, entonces $t - aw_j^2 \in \mathbf{Z}_p = q(\ell^s E_p)$.

Esto último porque $\ell^s E_p$ es unimodular si $p \notin P$. Así $0 \leq t - aw_j^2 \in \bar{q}(\ell^s E_p)$ y por lema 2.11 se tiene que $t \in q(E \perp \langle a\rangle)$.

□

El siguiente resultado de Kitaoka (ver [Ki1], [Ki2], [Ki3] y [HKK].) es fundamental en la demostración del teorema 3.1.

Lema 2.16. Sean L un $\mathbf{Z}$-reticulado, $dimL = m$, S un conjunto finito de primos que contiene a 2 y tal que L_p es unimodular si $p \notin S$. Para cada $p \in S$ sean $x_{1,p},\cdots,x_{n,p}$ vectores en L_p, con $n < m$. Entonces existen vectores $x_1,\cdots,x_n$ en L que satisfacen:

$x_{1,p}, \cdots, x_{n,p}$ vectores en L_p, con $n < m$. Entonces existen vectores $x_1, \cdots, x_n$ en L que satisfacen:

(1) $\forall\, p \in S$, x_i aproxima a x_{ip}, tan cerca como se quiera.

(2) Si $p \notin S$ entonces $d(B(x_i, x_j)) \in U_p$ con una única excepción $p = r \notin S$ donde $d(B(x_i, x_j)) \in rU_r$.

Una cota para este primo excepcional fué dada por M. Icaza. El cálculo de esta cota se basa en la demostración del lema 2.16, y en el siguiente resultado de [Ic1], el cual es un corolario del teorema 1.1 en [LMO]:

Lema 2.17. Sea K una extensión cuadrática de $\mathbb{Q}$. Sea $\mathcal{M} \in \mathbb{Q}$ divisible por todos los primos que se ramifican en K. Entonces existe una constante absoluta calculable A tal que en cada clase de rayo módulo $\mathcal{M}$ de K, existe un ideal primo $\mathcal{B}$ de grado uno con

$$Norm(\mathcal{B}) \leq 2(D(K)^{h(K)Norm(\mathcal{M})})Norm((\mathcal{M})^{h(K)Norm(\mathcal{M})-1})^A$$

donde $D(K)$ y $h(K)$ denotan el discriminante y número de clase del cuerpo K respectivamente.

En este trabajo nos interesa tener una estimación del primo excepcional r, sólo para el caso $n = 1$.

Antes de enunciar el resultado de [Ic1] para este caso, introduciremos algunas constantes:

Con la misma notación del lema 2.16 se define:

$$K_m =: 16m^2(\Pi_{p\in S}p)^{2(j(L_p)+1)}(\Pi_p p)^2\tau_m detL,$$

donde el segundo producto es tomado sobre los primos p tales que $p \leq (\frac{4}{3})^{(m-1)/2}(detL)^{1/m}$.

$$C_m =: (\tfrac{4}{3})^{m-1/2}(detL)^{1/m},$$

$$P := 4(\Pi_{p\in S}\, p)^{j(L_p)+1}(\Pi_{p\notin S, p\leq K_m C_m} p),$$

donde $j(L_p)$ es el orden de la scale de la última componente de una descomposición de Jordan para L_p. Por 91:1 de [O'M1] se tiene que $j(L_p)$ es independiente de la descomposición.

La definición de τ_m es la misma dada en la observación 2.13.

La cota para el primo r está dada en la siguiente proposición:

Proposición 2.18. Sean $n = 1$, L y S como en el lema 2.16.

Entonces existe una constante calculable C que depende sólo del reticulado L tal que el primo excepcional del lema 2.16 satisface

$$r \leq 2C^A$$

donde A es la constante absoluta dada en el lema 2.17 y C puede elegirse como

$$C = 4(K_m C_m)^{(\frac{4}{3})K_m C_m P^2} P^{(\frac{4}{3}K_m C_m P^2 - 1)}$$

Demostración: Ver lema 2.1.13 de [Ic1].

CAPITULO III

Una versión efectiva de un teorema de M. Kneser.

En este capítulo presentamos una versión efectiva del teorema 0.4 y es el siguiente resultado:

Teorema 3.1. Sea L un $\mathbb{Z}$-reticulado positivo definido en un espacio cuadrático regular de dimensión 4 sobre $\mathbb{Q}$, supongamos que $s(L) \subseteq \mathbb{Z}$. Entonces existe una constante efectivamente computable N que sólo depende del reticulado L, que tiene la siguiente propiedad:

Si $t \geq N$ es un entero representado por L sobre $\mathbb{Z}_p$, para cada primo p, y t no es divisible por aquellos primos p para los cuales L_p es anisótropo, entonces t es representado por L sobre $\mathbb{Z}$.

La constante N puede ser elegida como

$$N = 2^{142+52n_0}\, C^{11+4n_0} \ell_0^{1+(10+4n_0)(6H+1)}\, (dL)^{152+60n_0},$$

donde

$$\begin{aligned} \ell_0 &= max\{11, dL-1\}, \\ H &= 2^{28} \cdot 5 \cdot \ell_0^2 C^{2A} (dL)^{30}, \\ n_0 &= 2^{16} \ell_0^{2(3H+1)}\, (dL)^{17}, \end{aligned}$$

C es la constante establecida en la proposición 2.18 que depende sólo de L y A es la constante absoluta efectivamente computable especificada en el teorema 1.1 de [LMO].

La demostración de este resultado se basa en las estimaciones del capítulo anterior, aunque lo fundamental es la construcción de un $\mathbb{Z}$-reticulado $E \subseteq L$ que satisface las hipótesis de la proposición 2.14.

A continuación veremos algunos lemas necesarios para la construcción de este reticulado.

Lema 3.2. Sea L un $\mathbb{Z}$-reticulado en un espacio cuadrático regular de dimensión 4 sobre $\mathbb{Q}$, $detL = d$. Entonces existe un primo $\ell \leq max\{11, d-1\}$ tal que el índice de Witt $ind_{\mathbb{Q}_\ell} L = 2$.

Demostración: Sea ℓ un primo tal que $\ell \neq 2$ y ℓ no divide a d. Entonces L_ℓ es unimodular, luego $L_\ell \cong \langle 1,1,1,d \rangle$, y si además $(\frac{d}{\ell}) = 1$ (símbolo de Legendre), entonces $L_\ell \cong \mathbf{H}_1 \perp \mathbf{H}_2$ con $\mathbf{H}_i$ plano hiperbólico.

Para $d = 1$, $d = 2$, $d = 3$, $d = 4$, $d = 5$ elegimos $\ell = 3$, $\ell = 7$, $\ell = 3$, $\ell = 3$ y $\ell = 11$ respectivamente.

Supongamos que $d > 5$.

- Si $d \equiv 1 (mod\ 4)$, entonces $d = 1 + 4t$ con $t > 1$. Luego $d - 4 = 1 + 4(t-1)$ y por lo tanto existe un primo $\ell \neq 2$ tal que $\ell / d-4$ y $\ell \nmid d$. Como $d \equiv 4 (mod\ \ell)$ entonces $(\frac{d}{\ell}) = 1$ y $\ell \leq d - 4$.

- Si $d \not\equiv 1 (mod\ 4)$, entonces $d - 1 = p_1^{e_1} \cdots p_r^{e_r} > 4$. Luego existe $p_i \neq 2$ con $e_i \geq 1$. Sea $\ell = min_{p_j \neq 2}\ p_j$. Entonces $(\frac{d}{\ell}) = 1$ y $\ell \leq d - 1$.

Considerando las distintas posibilidades para d se puede elegir $\ell \leq max\{11, d-1\}$.

□

Ahora iniciamos la demostración del teorema 3.1.

Sea S un conjunto finito de primos tal que L_p es unimodular si $p \notin S$, S contiene a 2 y a un primo ℓ tal que $ind_{\mathbb{Q}_\ell} L = 2$ (lema 3.2.)

Sea $t \in \bar{q}(L)$, es decir t es representado por L sobre $\mathbf{Z}_p$, para todo p. Entonces $t \in q(L_p)$ para todo $p \in S$, y como $q(L_p) = \cup_{\text{finita}} q(u_{i_p})\mathbf{Z}_p^2$, (Proposición 2.5) se tiene que $t = q(u_{i_p})v_p^2$ con $v_p \in \mathbf{Z}_p$ y u_{i_p} en L_p.

Para esta colección fija $\{u_{i_p}\}_{p\in S}$ existe un vector $u_t \in L$ tal que para todo $p \in S$, u_t aproxima a u_{i_p} tan cerca como se quiera. $q(u_t) \in U_p$ para $p \notin S$ con una única excepción $p = r$ y en este caso $q(u_t) \in rU_r$, (ver lema 2.16).

Para todo $p \in S$, u_t aproxima a u_{i_p} tan cerca como se quiera. Luego podemos elegir u_t tal que para todo $p \in S$ se satisface la siguiente propiedad:

Si $|q(u_{i_p})|_p = p^{-\alpha_p}$ entonces

$$|q(u_{i_p}) - q(u_t)|_p < p^{-(2\alpha_p+2)}.$$

En el siguiente lema presentamos una estimación para $q(u_t)$.

Lema 3.3. Con las notaciones anteriores

$$q(u_t) \leq 2^4 C^A \ell_0 (dL)^2$$

donde C y A son las constantes establecidas en la proposición 2.18 y lema 2.17 (teorema 1.1 [LMO]) respectivamente, y $\ell_0 = max\{11, dL - 1\}$.

Demostración: Para cada $p \in S$, existe $\gamma_p \in U_p$ tal que $q(u_t) = \gamma_p^2 q(u_{i_p})$. En efecto, supongamos que $|q(u_{ip})|_p = p^{-\alpha_p}$ y que $|q(u_{ip}) - q(u_t)|_p < p^{-(2\alpha_p+2)}$. Definamos

$$f(x) = q(u_{ip})x^2 - q(u_t) \in \mathbb{Z}_p[x].$$

Luego

$$\begin{aligned} |f(1)|_p &= |q(u_{ip}) - q(u_t)|_p < p^{-(2\alpha_p+2)} \\ &\leq |2q(u_{ip})|^2 = |f'(1)|^2. \end{aligned}$$

Entonces por lema de Hensel, existe $\gamma_p \in U_p$ tal que $f(\gamma_p) = 0$, es decir $q(u_t) = \gamma_p^2 q(u_{ip})$.

Además $q(u_t)$ debe ser de la forma $q(u_t) = r\Pi_{p\in S}p^{\beta_p}$, ciertos $\beta_p \geq 0$ y $q(u_t) \geq 0$ porque L es positivo definido. Fijando $p \in S$ y comparando ambas expresiones para $q(u_t)$ se tiene que $\beta_p = ord_p q(u_{ip})$. Por proposición 2.5, $\beta_p \leq 1 + ord_p d$ si $p \neq 2$ y $\beta_2 \leq 3 + ord_2(dL)$. Luego $q(u_t) \leq 2^3 r\ell(dL)^2$. Esta cota se obtiene suponiendo que $S = \{p \text{ primo} | p/d\} \cup \{2, \ell\}$.

Es claro que el primo excepcional r se obtiene de la colección $\{u_{ip}\}_{p\in S}$ asociada a t y por lo tanto depende de t. Sin embargo la proposición 2.18 nos garantiza la existencia de una cota para r, la cual es independiente de t. En efecto $r \leq 2C^A$, donde C es una constante que sólo depende de L y A es una constante absoluta computable. El primo ℓ puede ser elegido como en el lema 3.2.

□

Observación 3.4. Con las notaciones anteriores $t \in q(\mathbb{Z}_p u_t)$, para todo $p \in S$.

En la demostración anterior notar que

$$t = q(u_{ip})v_p^2 = q(u_t)(\gamma_p^{-1}v_p)^2 \in q(u_t)\mathbb{Z}_p^2.$$

u_t es un vector primitivo para todo $p \in S$ ya que aproxima a u_{ip}.

Ahora construiremos un subreticulado E de L que satisface las hipótesis de la proposición 2.14, las cuales explicitaremos en detalle en el siguiente lema.

Lema 3.5. Sean $t \in \bar{q}(L)$ y $u_t \in L$ como antes. Entonces existe un $\mathbb{Z}$-reticulado E positivo definido con las siguientes propiedades:

(i) $dim E = 3$.

(ii) $E \perp \langle q(u_t) \rangle \subseteq L$.

(iii) E_ℓ es $\mathbb{Z}_\ell$-maximal.

(iv) $U_p \subseteq \theta(E_p)$ para todo p, donde θ es la norma espinorial.

(v) $t \in q(\ell^s E_p \perp \langle q(u_t) \rangle)$, $\quad \forall p \in S$ y $\forall s \in \mathbb{Z}^+$.

(vi) $q(\ell^s E_p \perp \langle q(u_t) \rangle)^* \subseteq q(\ell^s E_p)^* + q(u_t)\mathbb{Z}_p^2$, $\quad \forall p \in S$ y $\forall s \in \mathbb{Z}^+$.

(vii) $t \in q(\ell^s E_r \perp \langle q(u_t) \rangle)^* \cup r^2 q(\ell^s E_r \perp \langle q(u_t) \rangle)^* \cup r^4 q(\ell^s E_r \perp \langle q(u_t) \rangle)^*$, $\forall s \in \mathbb{Z}^+$.

(viii) $\cup_{i=0}^2 r^{2i} q(\ell^s E_r \perp \langle q(u_t) \rangle)^* \subseteq \cup_{i=0}^3 r^{2i} q(\ell^s E_r)^* + q(u_t)\mathbb{Z}_r^2$, $\quad \forall s \in \mathbb{Z}^+$.

Notemos que el reticulado E depende de t.

Demostración: Consideremos el $\mathbb{Z}$-reticulado $\langle q(u_t) \rangle \subseteq L$. Entonces de acuerdo con el lema 2.26 [Ki2]. Se tiene que

$$det\langle q(u_t) \rangle^\perp / det\langle q(u_t) \rangle det L.$$

Luego para todo p, se tiene que

$$ord_p det\langle q(u_t) \rangle^\perp \leq ord_p(q(u_t)d)$$

donde $d = detL$.

Para cada p definiremos un $\mathbb{Z}_p$-reticulado E_p de dimensión 3, tal que $E_p = \langle q(u_t)\rangle^{\perp}$ si $p \notin S \cup \{r\}$ y $E_p \subseteq \langle q(u_t)\rangle^{\perp}$ si $p \in S \cup \{r\}$. Además los reticulados E_p cumplirán las propiedades (iii), . . . (viii) exigidas en el lema.

Entonces por teorema 1.1 [Ca], pág. 198 existe un $\mathbb{Z}$-reticulado E, tal que para todo p, su localización en p coincide con E_p.

Por construcción se tiene que E satisface (i) y (ii). Las propiedades (iii), ... , (viii) serán verificadas directamente para cada p.

a) Sea $p \in S - \{2, \ell\}$.

Como $p \neq 2$ podemos suponer que

$$\langle q(u_t)\rangle^{\perp} = \mathbb{Z}_p e_1 \perp \mathbb{Z}_p e_2 \perp \mathbb{Z}_p e_3, \quad \text{con} \quad q(e_i) = p^{a_i} v_i,$$

$v_i \in U_p$ y como $s(L) \subseteq \mathbb{Z}$ se tiene que $a_i \geq 0$ para $i \in \{1, 2, 3\}$.

Sea $a_i \cong \epsilon_i (mod\ 2)$ con $\epsilon_i \in \{0, 1\}$, es decir $a_i = \epsilon_i + 2t_i$ con $t_i \geq 0$.

Sea $f_i := p^{-t_i} e_i$ entonces $q(f_i) = p^{-2t_i} q(e_i) = p^{\epsilon_i} v_i$.

Consideremos el $\mathbb{Z}_p$-reticulado

$$E'_p := \mathbb{Z}_p f_1 \perp \mathbb{Z}_p f_2 \perp \mathbb{Z}_p f_3,$$

entonces $\langle q(u_t)\rangle^{\perp} \subseteq E'_p$.

Por construcción se tiene que

$$p^{t_1+t_2+t_3} E'_p \subseteq \langle q(u_t)\rangle^{\perp}.$$

En la demostración del lema 3.3 se obtiene

$$ord_p q(u_t) \leq 1 + ord_p d.$$

Luego

$$\begin{aligned} t_1 + t_2 + t_3 &\leq \tfrac{1}{2}(a_1 + a_2 + a_3) \leq \tfrac{1}{2} ord_p(q(u_t)d) \\ &\leq \tfrac{1}{2}(1 + ord_p d + ord_p d) \leq 1 + ord_p d. \end{aligned}$$

Sea $\alpha_p = 1 + ord_p d$ y definamos $E_p := p^{\alpha_p} E'_p$. Entonces

$$E_p = p^{\alpha_p} E'_p \subseteq p^{t_1+t_2+t_3} E'_p \subseteq \langle q(u_t) \rangle^{\perp}.$$

Ahora verifiquemos que el reticulado E_p satisface las propiedades (iv), (v) y (vi):

(iv) Por definición se tiene que

$$E_p = \langle p^{2\alpha_p+\epsilon_1} v_1 \rangle \perp \langle p^{2\alpha_p+\epsilon_2} v_2 \rangle \perp \langle p^{2\alpha_p+\epsilon_3} v_3 \rangle,$$

con $\epsilon_i \in \{0, 1\}$ y $v_i \in U_p$.

Luego existe $i \neq j$ tal que $\epsilon_i = \epsilon_j$. Entonces por lema 3.7 [Ca], pág. 213 se tiene que $U_p \subseteq \theta(E_p)$.

(v) Por la observación 3.4, $t \in q(\mathbb{Z}_p u_t)$, luego $t \in q(\ell^s E_p \perp \langle q(u_t) \rangle)$, $\forall s > 0$.

(vi) Como $\mathcal{N}(\ell^s E_p) \subseteq p^{2\alpha_p}\mathbb{Z}_p$, $\forall s > 0$ y

$$2\alpha_p = 2 + 2ord_p d > 1 + ord_p d \geq ord_p q(u_t)$$

por el lema 2.8 se tiene que

$$q(\ell^s E_p \perp \langle q(u_t) \rangle)^* \subseteq q(\ell^s E_p)^* + q(u_t)\mathbb{Z}_p^2.$$

Observemos que por la construcción de E_p se tiene:

$$ord_p(dE_p) = ord_p(p^{6\alpha_p+\epsilon_1+\epsilon_2+\epsilon_3}) \leq 9 + 6ord_p d.$$

Esta cota será necesaria más adelante para acotar det E.

b) Sea $p = 2$. Entonces hay dos posibles tipos de reticulados que pueden ser equivalentes con $\langle q(u_t)\rangle^{\perp}$:

- Si $\langle q(u_t)\rangle^{\perp} = \mathbb{Z}_2 e_1 \perp \mathbb{Z}_2 e_2 \perp \mathbb{Z}_2 e_3$, con $q(e_i) = 2^{a_i} v_i$, $v_i \in U_2$ y $a_i \geq 0$, para $i \in \{1,2,3\}$.

Se procede igual que en el caso $p \neq 2$. Si $a_i \equiv \epsilon_i (mod\ 2)$, con $\epsilon_i \in \{0,1\}$ entonces $a_i = \epsilon_i + 2t_i$, ciertos $t_i \geq 0$. Consideremos el $\mathbb{Z}_2$-reticulado

$$E_2' := \mathbb{Z}_2 f_1 \perp \mathbb{Z}_2 f_2 \perp \mathbb{Z}_2 f_3, \quad \text{donde} \quad f_i := 2^{-t_i} e_i.$$

De este modo $q(f_i) = 2^{\epsilon_i} v_i$ y luego por construcción se tiene que

$$2^{t_1+t_2+t_3} E_1' \subseteq \langle q(u_t)\rangle^{\perp}.$$

En la demostración del lema 3.3 se obtiene

$$q(u_t) \leq 3 + ord_2 d.$$

Luego

$$\begin{aligned} t_1 + t_2 + t_3 &\leq \tfrac{1}{2}(a_1 + a_2 + a_3) \leq \tfrac{1}{2} ord_2(q(u_t)d) \\ &\leq \tfrac{1}{2}(3 + 2ord_2 d) \leq 3 + ord_2 d. \end{aligned}$$

Sea $\alpha_2 = 3ord_2 d$ y definamos $E_2 := 2^{\alpha_2} E_2'$. entonces

$$E_2 = 2^{\alpha_2} E_2' \subseteq 2^{t_1+t_2+t_3} E_2' \subseteq \langle q(u_t)\rangle^{\perp}.$$

Verifiquemos las propiedades (iv), (v) y (vi):

(iv) Por definición se tiene que

$$E_2 = \langle 2^{2\alpha_2+\epsilon_1} v_1 \rangle \perp \langle 2^{2\alpha_2+\epsilon_2} v_2 \rangle \perp \langle 2^{2\alpha_3+\epsilon_3} v_3 \rangle,$$

con $\epsilon_i \in \{0,1\}$ y $v_i \in U_2$.

Luego existe $i \neq j$ tal que $\epsilon_i = \epsilon_j$. Sin pérdida de generalidad, supongamos que $\epsilon_1 = \epsilon_2$, es decir $|2^{\epsilon_1} v_1|_2 = |2^{\epsilon_2} v_2|_2$. Entonces necesariamente

$$|2^{\epsilon_3} v_3|_2 = \begin{cases} |2^{\epsilon_1} v_1|_2 & \text{o} \\ 2|2^{\epsilon_1} v_1|_2 & \text{o} \\ \frac{1}{2}|2^{\epsilon_1} v_1|_2. \end{cases}$$

Por lema 3.8 de [Ca], pág. 214 se tiene que $U_2 \subseteq \theta(E_2)$.

(v) Es el mismo argumento que en el caso $p \neq 2$.

(vi) Como $\mathcal{N}(\ell^s E_2) \subseteq 2^{2\alpha_2}\mathbb{Z}_2$, $\forall s > 0$ y

$$2\alpha_2 = 6 + 2ord_2 d > 5 + 2ord_2 d \geq 2 + ord_2 q(u_t),$$

usando lema 2.8 se tiene que

$$q(\ell^s E_2 \perp \langle q(u_t) \rangle)^* \subseteq q(\ell^s E_2)^* + q(u_t)\mathbb{Z}_2^2.$$

- Por el lema 4.1 de [Ca], pág. 117 se sabe que la otra posibilidad es la siguiente:

$$\langle q(u_t) \rangle^{\perp} = \mathbb{Z}_2 e_1 \perp (\mathbb{Z}_2 e_2 \oplus \mathbb{Z}_2 e_2),$$

donde $q(e_1) = 2^{a_1} v_1$, con $a_1 \geq 0$ y $v_1 \in U_2$.

La matriz asociada al subreticulado $\mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ es del tipo $2^{a_2} A(\alpha, \beta)$, donde $a_2 \geq 0$ y $A(\alpha, \beta)$ es una de las siguientes matrices: $A(2,2) = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$ o $A(0,0) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Sea $a_i \equiv \epsilon_i (mod\, 2)$, $\epsilon_i \in \{0,1\}$, $i \in \{1,2\}$, es decir $a_i = \epsilon_i + 2t_i$ con $t_i \geq 0$.

Sean $f_1 := 2^{-t_1} e_1$, $f_2 := 2^{-t_2} e_2$ y $f_3 := 2^{-t_2} e_3$ y consideremos el $\mathbf{Z}_2$-reticulado

$$E_2' := \mathbf{Z}_2 f_1 \perp (\mathbf{Z}_2 f_2 \oplus \mathbf{Z}_2 f_3).$$

Por construcción se tiene que

$$2^{t_1+t_2} E_2' \subseteq \langle q(u_t) \rangle^{\perp}$$

En este caso $ord_2 q(u_t) \leq 3 + ord_2 d$, por lema 3.3.

Luego

$$\begin{aligned} t_1 + t_2 &\leq \tfrac{1}{2}(a_1 + 2a_2) \leq \tfrac{1}{2} ord_2(q(u_t)d) \\ &\leq \tfrac{1}{2}(3 + 2ord_2 d). \end{aligned}$$

Sea $\alpha_2 = 3 + ord_2 d$ y definamos $E_2 := 2^{\alpha_2} E_2'$, entonces

$$E_2 = 2^{\alpha_2} E_2' \subseteq 2^{t_1+t_2} E_2' \subseteq \langle q(u_t) \rangle^{\perp}.$$

Verifiquemos las propiedades (iv), (v) y (vi):

(iv) Por definición se tiene que E_2 se representa por una de las siguientes matrices:

$$E_2 \cong 2^{2\alpha_2} \begin{bmatrix} 2^{\epsilon_1} v_1 & 0 & 0 \\ 0 & 2^{\epsilon_2+1} & 2^{\epsilon_2} \\ 0 & 2^{\epsilon_2} & 2^{\epsilon_2+1} \end{bmatrix} \quad \text{o} \quad E_2 \cong 2^{2\alpha_2} \begin{bmatrix} 2^{\epsilon_1} v_1 & 0 & 0 \\ 0 & 0 & 2^{\epsilon_2} \\ 0 & 2^{\epsilon_2} & 0 \end{bmatrix}.$$

Por aplicación directa del lema 3.6 [Ca] pág. 214, se tiene que $U_2 \subseteq \theta(E_2)$.

(v) El mismo argumento anterior es válido, es decir la propiedad

$$t \in q(\ell^s E_2 \perp \langle q(u_t)\rangle), \quad \forall s > 0,$$

se obtiene directamente de la observación 3.4.

(vi) Al igual que en el caso anterior para $p = 2$, se tiene que $\mathcal{N}(\ell^s E_2) \subseteq 2^{2\alpha_2}\mathbf{Z}_2$, $\forall s > 0$ y $2\alpha_2 > 2 + ord_2 q(u_t)$. Usando el lema 2.8 se concluye que

$$q(\ell^s E_2 \perp \langle q(u_t)\rangle)^* \subseteq q(\ell^s E_2)^* + q(u_t)\mathbf{Z}_2^2, \quad \forall s > 0.$$

Observemos que para $p = 2$, se tiene

$$ord_2(dE_2) \leq 6\alpha_2 + 3 \leq 21 + 6ord_2 d$$

c) Sea $p = \ell$.

Recordemos que $ord_\ell q(u_t) \leq 1 + ord_\ell d = 1$. Luego $ord_\ell det\langle q(u_t)\rangle^\perp \leq ord_\ell(q(u_t)d) \leq 1$.

Entonces podemos suponer que

$$\langle q(u_t)\rangle^\perp = \langle v_1\rangle \perp \langle v_2\rangle \perp \langle \ell^\epsilon v_3\rangle$$

con $\epsilon \in \{0,1\}$ y $v_i \in U_\ell$ para $i \in \{1,2,3\}$.

Definamos $E_\ell := \langle q(u_t)\rangle^\perp$.

Como $s(L) \subseteq \mathbf{Z}$ se tiene que $\mathcal{N}(E_\ell) \subseteq \mathbf{Z}_\ell$.

El reticulado E_ℓ resulta ser $\mathbf{Z}_\ell$-maximal por aplicación directa del siguiente resultado de [Ki3], lema 5.2.1:

Sea E un reticulado regular sobre $\mathcal{O}$, con $dimE = m$. Si $\mathcal{N}(E) \subseteq (a)$ y $((2a^{-1})^m dE) = \mathcal{O}$ o $p\mathcal{O}$, entonces E es (a)-maximal.

De este modo se tiene probado (iii) del lema. Verifiquemos ahora (iv), (v) y (vi):

(iv) $\langle q(u_t)\rangle^{\perp} = \langle v_1\rangle \perp \langle v_2\rangle \perp \langle \ell^{\epsilon} v_3\rangle$, con $v_i \in U_p$ y $\epsilon \in \{0,1\}$. Entonces $|v_1|_\ell = |v_2|_\ell = 1$. Aplicando directamente el lema 3.7 [Ca], pág. 213, se tiene que $U_\ell \subseteq \theta(E_\ell)$.

(v) $\ell \in S$, entonces según la observación 3.4 se tiene que $t \in q(\mathbf{Z}_\ell u_t)$. Luego $t \in q(\ell^s E_\ell \perp \langle q(u_t)\rangle)$, $\forall s > 0$.

(vi) Sea $s > 0$, entonces $\mathcal{N}(\ell^s E_\ell) \subseteq \ell^2 \mathbf{Z}_\ell$. Luego aplicando el lema 2.8 se tiene que:

$$q(\ell^s E_\ell \perp \langle q(u_t)\rangle)^* \subseteq q(\ell^s E_\ell)^* + q(u_t)\mathbf{Z}_\ell^2, \quad \forall s > 0.$$

d) Sea $p = r$.

En este caso corresponde probar las propiedades (iv), (vii) y (viii).

Como $q(u_t) \in rU_r$, se tiene que u_t es un vector primitivo en L_r. Luego u_t es parte de una base de L_r.

L_r es unimodular, luego existe $w \in L_r$ tal que $|b(u_t, w)|_r = 1$.

Consideremos el $\mathbf{Z}_r$-reticulado $\langle u_t, w\rangle \subseteq L_r$. Este reticulado es isótropo, porque si definimos

$$f(x) = q(u_t + xw) = q(u_t) + 2b(u_t, w)x + q(w)x^2 \in \mathbf{Z}_r[x],$$

entonces

$$|f(0)|_r = |q(u_t)|_r = \frac{1}{r} < 1 = |2b(u_t, x)|_r = |f'(0)|_r^2.$$

Por lema de Hensel existe $c \in \mathbb{Z}_r$ tal que $0 = f(c) = q(u_t + cw)$. Como el vector $u_t + cw \in \langle u_t, w\rangle$, se tiene que $\langle u_t, w\rangle$ es isótropo. Además $\langle u_t, w\rangle$ es unimodular, luego $\langle u_t, w\rangle = \mathbf{H}$, donde $\mathbf{H}$ es un plano hiperbólico.

Como L_r es unimodular, se tiene que $L_r = \mathbf{H} \perp G$, con G unimodular.

Luego existe una base $\{w_1, w_2, w_3, w_4\}$ de L_r tal que $\langle w_1, w_2\rangle = \mathbf{H}$ y $\langle w_3, w_4\rangle = G$.

Entonces podemos suponer que $q(w_1) = -q(w_2) = 1$ y $b(w_1, w_2) = 0$.

Como $u_t \in \langle w_1, w_2\rangle$ existen λ_1, λ_2 en $\mathbb{Z}_r$ tal que $u_t = \lambda_1 w_1 + \lambda_2 w_2$. Luego $q(u_t) = \lambda_1^2 - \lambda_2^2$.

Definamos E_r como el $\mathbb{Z}_r$-reticulado con base $\{\tilde{w} = \lambda_2 w_1 + \lambda_1 w_2, w_3, w_4\}$. Entonces $E_r \subseteq \langle q(u_t)\rangle^{\perp} \cap L_r$. Como $q(\tilde{w}) = \lambda_2^2 - \lambda_1^2 = -q(u_t)$, se concluye que $E_r = \langle -q(u_t)\rangle \perp G$.

Verifiquemos las propiedades:

(iv) Por definición $E_r := \langle -q(u_t)\rangle \perp G$, donde G es unimodular. Esto implica que $U_r \subseteq \theta(E_r)$. (Ver lema 3.7 [Ca] pág. 213).

(vii) Probaremos que $t \in \cup_{i=0}^{2} r^{2i} q(\ell^s E_r \perp \langle q(u_t)\rangle)^*$, $\forall s > 0$.

Como $r \neq \ell$, se tiene que:

$$\begin{aligned} \ell^s E_r \perp \langle q(u_t)\rangle &= E_r \perp \langle q(u_t)\rangle \\ &= \langle -q(u_t)\rangle \perp \langle q(u_t)\rangle \perp G. \end{aligned}$$

G representa a U_r por ser unimodular. En efecto, sea $detG = u \in U_r$. Como $r \neq 2$, se tiene que $G \cong \langle v \rangle \perp \langle uv^{-1} \rangle$ para todo $v \in U_r$. (Ver [Ca], lema 3.4, pág. 115).

Del mismo modo el reticulado $\langle -1 \rangle \perp \langle 1 \rangle$ representa a U_r. Como $q(u_t) \in rU_r$, se tiene que $\langle -q(u_t) \rangle \perp \langle q(u_t) \rangle$ representa a rU_r.

Luego $\ell^s E_r \perp \langle q(u_t) \rangle$ representa todo $\mathbb{Z}_r$. Es decir,

$$t \in q(\ell^s E_r \perp \langle q(u_t) \rangle) = \mathbb{Z}_r, \quad \forall s > 0.$$

Como el reticulado $\ell^s E_r \perp \langle q(u_t) \rangle$ es isótropo, se tiene por corolario 2.7 que existe m tal que

$$0 \leq m \leq ord_r d(\ell^s E_r \perp \langle q(u_t) \rangle = 2$$

y

$$r^{-2m} t \in q(\ell^s E_r \perp \langle q(u_t) \rangle)^*$$

luego

$$t \in \cup_{i=0}^{2} \; r^{2i} q(\ell^s E_r \perp \langle q(u_t) \rangle)^*.$$

(viii) Ahora probaremos lo siguiente:

$$\cup_{i=0}^{2} \; r^{2i} q(\ell^s E_r \perp \langle q(u_t) \rangle)^* \subseteq \cup_{i=0}^{3} \; r^{2i} q(\ell^s E_r)^* + q(u_t)\mathbb{Z}_r^2.$$

Sea $y \in \cup_{i=0}^{2} \; r^{2i} q(\ell^s E_r \perp \langle q(u_t) \rangle)^*$. Entonces $y = r^{2i} x$ con $0 \leq i \leq 2$ y $x \in q(\ell^s E_r \perp \langle q(u_t) \rangle)^*$. Luego $x = q(w) + q(u_t) z^2$ con $w \in \ell^s E_r$ y $z \in \mathbb{Z}_r$.

- Si w es primitivo entonces

$$x \in q(\ell^s E_r)^* + q(u_t)\mathbb{Z}_r^2.$$

Por lo tanto

$$y \in \cup_{i=0}^{2} \; r^{2i} q(\ell^s E_r)^* + q(u_t)\mathbb{Z}_r^2.$$

- Si w no es primitivo, entonces $z \in U_r$ y

$$x = r^{2a} q(\tilde{w}) + q(u_t) z^2$$

con $a > 0$ y $\tilde{w}$ un vector primitivo en $\ell^s E_r$. Como $q(u_t) \in rU_r$ se tiene que $x = q(u_t)v$ con $v \in U_r$.

Sean $\alpha = \frac{v+1}{2}$ y $\beta = \frac{v-1}{2}$. Como $r \neq 2$ se tiene que $\alpha, \beta \in \mathbb{Z}_r$. Además $v = (\frac{v+1}{2})^2 - (\frac{v-1}{2})^2 = \alpha^2 - \beta^2$, y siendo $v \in U_r$, entonces se tiene $\alpha \in U_r$ o $\beta \in U_r$.

- Si $\beta \in U_r$ entonces

$$x = q(u_t)(\alpha^2 - \beta^2) = -\beta^2 q(u_t) + \alpha^2 q(u_t)$$

así

$$x \in q(E_r)^* + q(u_t)\mathbb{Z}_r^2 = q(\ell^s E_r)^* + q(u_t)\mathbb{Z}_r^2,$$

y en consecuencia

$$y = r^{2i} x \in \cup_{i=0}^{2} \; r^{2i} q(\ell^s E_r)^* + q(u_t)\mathbb{Z}_r^2.$$

- Si $\alpha \in U_r$ y $\beta = r^c\epsilon$ con $c > 0$ y $\epsilon \in U_r$, entonces

$$v = \alpha^2 - r^{2c}\epsilon^2 \equiv \alpha^2 (mod\ r)$$

luego $v = \gamma^2$ con $\gamma \in U_r$. Entonces

$$x = q(u_t)\gamma^2 = q(u_t)(\gamma^2 - r^2 + r^2) = -q(u_t)r^2 + q(u_t)(r^2 + \gamma^2)$$

y como $r^2 + \gamma^2 \in U_r^2$, se tiene que

$$x \in r^2 q(\ell^s E_r)^* + q(u_t)\mathbb{Z}_r^2$$

Obtenemos entonces

$$y = r^{2i}x \in r^{2(i+1)}q(\ell^s E_r)^* + q(u_t)\mathbb{Z}_r^2.$$

Como $0 \leq i \leq 2$, se tiene que

$$y \in \cup_{i=0}^{3}\ r^{2i}q(\ell^s E_r)^* + q(u_t)\mathbb{Z}_r^2.$$

Hemos probado entonces la propiedad (viii).

e) Sea $p \notin S \cup \{r\}$.

En este caso L_p y $\langle q(u_t)\rangle$ son reticulados unimodulares.

Como $det\langle q(u_t)\rangle^{\perp}/det\langle q(u_t)\rangle detL$ se tiene que $\langle q(u_t)\rangle^{\perp}$ es unimodular.

Definamos $E_p := \langle q(u_t)\rangle^{\perp}$.

En este caso sólo debemos verificar la propiedad (iv), es decir $U_p \subseteq \theta(E_p)$.
Esto es válido porque E_p es unimodular y $p \neq 2$. (Ver [O'M1], 92:5).

Así para cada p hemos construido un $\mathbb{Z}_p$-reticulado E_p, tal que $dim\ E_p = 3$ y $E_p \subseteq L_p$.

Además E_p verifica las propiedades (iii), ..., (viii). Entonces existe un $\mathbb{Z}$-reticulado E que satisface las hipótesis del lema.

□

Corolario 3.6. Sean $t \in \bar{q}(L)$ y u_t como antes. Supongamos que t no es divisible por aquellos primos p, para los cuales L_p es anisótropo. Consideremos el $\mathbb{Z}$-reticulado del lema 3.5.

Entonces existe un entero n, tal que para cada $p \in S \cup \{r\}$, se satisface lo siguiente:

(i) $t \in \cup_{i=0}^{n} p^{2i} q(\ell^s E_p \perp \langle q(u_t)\rangle)^*$, donde $s \in \mathbb{Z}^+$.

(ii) $\cup_{i=0}^{n} p^{2i} q(\ell^s E_p \perp \langle q(u_t)\rangle)^* \subseteq \cup_{i=0}^{n+1} p^{2i} q(\ell^s E_p)^* + q(u_t)\mathbb{Z}_p^2$, donde $s \in \mathbb{Z}^+$.

Demostración. (i) En el lema 3.5 se probó que si $p \in S$, entonces $t \in q(\ell^s E_p \perp \langle q(u_t)\rangle)$.

- Si L_p es anisótropo, entonces por hipótesis p no divide a t. Luego $t \in q(\ell^s E_p \perp \langle q(u_t)\rangle)^*$.
- Si L_p es isótropo, entonces por la construcción del reticulado E_p se tiene que $\ell^s E_p \perp \langle q(u_t)\rangle$ es isótropo. Luego aplicando el corolario 2.7 se concluye que existe un entero i tal que $p^{-2i}t \in q(\ell^s E_p \perp \langle q(u_t)\rangle)^*$, donde $0 \leq i \leq n_p$ con

$$n_p = \begin{cases} ord_p\ d(\ell^s E \perp \langle q(u_t)\rangle) & \text{si } p \neq 2, \\ 2 + ord_p\ d(\ell^s E \perp \langle q(u_t)\rangle) & \text{si } p = 2. \end{cases}$$

Por lo tanto, para cada $p \in S$

$$t \in \cup_{i=0}^{n_p} \; p^{2i} \; q(\ell^s E_p \perp \langle q(u_t) \rangle)^*.$$

Ahora, si $p = r$ entonces por el lema 3.5 se tiene que

$$t \in \cup_{i=0}^{2} \; r^{2i} \; q(\ell^s E_r \perp \langle q(u_t) \rangle)^*.$$

Como $max_{p \in S} \{n_p\} \geq 2$, basta elegir cualquier $n \geq max_{p \in S}\{n_p\}$, para tener que

$$t \in \cup_{i=0}^{n} \; p^{2i} \; q(\ell^s E_p \perp \langle q(u_t) \rangle)^*,$$

para cada $p \in S \cup \{r\}$.

(ii) En el lema 3.5 se probó que

$$q(\ell^s E_p \perp \langle q(u_t) \rangle)^* \subseteq q(\ell^s E_p)^* + q(u_t)\mathbb{Z}_p^2, \;\; \forall p \in S,$$

y que para $p = r$,

$$\cup_{i=0}^{2} r^{2i} \; q(\ell^s E_r \perp \langle q(u_t) \rangle)^* \subseteq \cup_{i=0}^{3} \; r^{2i} \; q(\ell^s E_r)^* + q(u_t)\mathbb{Z}_r^2.$$

Como en (i) se eligió $n \geq max_{p \in S} \{n_p\} \geq 2$, es claro que

$$\cup_{i=0}^{n} p^{2i} \; q(\ell^s E_p \perp \langle q(u_t) \rangle)^* \subseteq \cup_{i=0}^{n+1} \; p^{2i} \; q(\ell^s E_p)^* + q(u_t)\mathbb{Z}_p^2.$$

para cada $p \in S \cup \{r\}$.

□

Obervación 3.7. En el corolario 3.6, se puede elegir $n = 2^{16} \, \ell^{2(3s+1)} (dL)^{17}$.

En efecto, en el corolario 3.6 se tenía

$$n_p = \begin{cases} ord_p\ d(\ell^s E \perp \langle q(u_t)\rangle) & \text{si} \quad p \neq 2, \\ 2 + ord_p\ d(\ell^s E \perp \langle q(u_t)\rangle) & \text{si} \quad p = 2. \end{cases}$$

Por otra parte,

$$ord_p\ q(u_t) \leq \begin{cases} 1 + ord_p\ dL & \text{si} \quad p \in S - \{2\}, \\ 3 + ord_p\ dL & \text{si} \quad p = 2, \end{cases}$$

y por la construcción del reticulado E, se tiene que

$$ord_p(dE) \leq \begin{cases} 9 + 6ord_p dL & \text{si} \quad p \in S - \{2, \ell\}, \\ 21 + 6ord_2 dL & \text{si} \quad p = 2, \\ 1 & \text{si} \quad p = \ell, \\ 1 & \text{si} \quad p = r, \\ 0 & \text{si} \quad p \notin S \cup \{r\}. \end{cases}$$

Aquí es claro que $dE \leq 2^{12}\ell r(dL)^{15}$.
Usando lo anterior se tiene:

$$n_p \leq \begin{cases} 10 + 7ord_p dL & \text{si} \quad p \in S - \{2, \ell\}, \\ 26 + 7ord_p dL & \text{si} \quad p = 2, \\ 2(3s+1) & \text{si} \quad p = \ell. \end{cases}$$

Según el corolario 3.6, basta elegir $n \geq max_{p \in S}\ \{n_p\}$ y como

$$n_p \leq \Pi_{p \in S}\ p^{n_p} \leq 2^{16}\ \ell^{2(3s+1)}\ (dL)^{17},$$

para todo $p \in S$, es claro que $n = 2^{16}\ \ell^{2(3s+1)}\ (dL)^{17}$ satisface.

Corolario 3.8. Sea $t \in \bar{q}(L)$ y u_t como antes. Supongamos que t no es divisible por aquellos primos p para los cuales L_p es anisótropo. Entonces el $\mathbb{Z}$-reticulado positivo definido E del lema 3.5. satisface todas las hipótesis de la proposición 2.14.

Demostración. Por lema 3.5 tenemos que $dimE = 3$. Además $U_p \subseteq \theta(E_p)$, $\forall p$. Luego por [Ca] pág. 213 se tiene que $genE = spnE$.

Por lema 3.2 $ind\mathbb{Q}_\ell L = 2$, y como $dimL = 4$, se tiene por 42:12 de [O'M1], que $\mathbb{Q}_\ell E$ es isótropo.

Por lema 2.11 existe un entero s tal que $\bar{q}(\ell^s E) \subseteq q(E)$.

Como $u_t \in L$ y L es positivo definido, se tiene $q(u_t) > 0$.

Sea $P = \{p \text{ primo } |p/d(\ell^s E)\} \cup \{2\}$. Entonces $P = S \cup \{r\}$ puesto que E_p es unimodular si $p \notin S \cup \{r\}$ y $ord_p d(\ell^s E) > 0$ si $p \in S \cup \{r\}$.

En el corolario 3.6, se probó que existe un entero n, tal que

$$\cup_{i=0}^{n} \; p^{2i} q(\ell^s E_p \perp \langle q(u_t)\rangle)^* \subseteq \cup_{i=0}^{n+1} \; p^{2i} q(\ell^s E_p)^* + q(u_t)\mathbb{Z}_p^2, \quad \forall p \in S \cup \{r\} = P.$$

□

Corolario 3.9. Sea $t \in \bar{q}(L)$ y u_t como antes. Supongamos que t no es divisible por aquellos primos p para los cuales L_p es anisótropo y que $t \geq 2^8 q(u_t)(d(\ell^s E))^{10+4n}$, donde $n = 2^{16}\ell^{2(3s+1)}(dL)^{17}$. Entonces $t \in q(L)$.

Demostración. Por el corolario 3.8 el reticulado E del lema 3.5 satisface todas las hipótesis de la proposición 2.14.

De acuerdo con el corolario 3.6 (i)

$$t \in \cup_{i=0}^{n} p^{2i} \; q(\ell^s E_p \perp \langle q(u_t)\rangle)^*, \quad \forall p \in S \cup \{r\} = P.$$

Como $t \geq 2^8\, q(u_t)(d(\ell^s E))^{6+4(n+1)}$ y de acuerdo con el corolario 3.8 el reticulado E satisface las hipótesis de la proposición 2.14. Entonces se tiene que

$$t \in q(E \perp \langle q(u_t)\rangle) \subseteq q(L).$$

Esto último debido a (ii) del lema 3.5.

□

Para el cálculo efectivo de la constante N del teorema 3.1 se debe acotar $2^8 q(u_t) \cdot [d(\ell^s E)]^{10+4n}$.

En el lema 3.5 (iii) se probó que E es $\mathbb{Z}_\ell$-maximal. Entonces por el lema 2.12 podemos elegir $s \geq h(E) - 1$, donde $h(E)$ es el número de clases en $spnE = genE$. Notemos que en la demostración del lema 3.5, para el caso $p = \ell$, se usa la propiedad $s > 0$. Elegiremos entonces $s = h(E) > 0$.

Por la observación 2.13 se tiene que $s \leq 2^3 \cdot 5 \cdot (dE)^2$.

De acuerdo con los lemas 3.2 y 3.3 basta acotar dE.

Por la observación 3.7 se tiene que $dE \leq 2^{12}\, \ell r (dL)^{15}$ y por la observación 2.13 y la proposición 2.18

$$s \leq 2^3 \cdot 5 \cdot (dE)^2 \leq 2^{28} \cdot 5 \cdot \ell_0^2\ C^{2A}(dL)^{30}.$$

Así

$$\begin{aligned} 2^8 q(u_t)(d(\ell^s E))^{10+4n} &\leq 2^8 q(u_t)\ell^{6s(10+4n)}(dE)^{(10+4n)} \\ &\leq 2^{12} C^A \ell_0^{1+6s(10+4n)}(dL)^2(2^{12}\ell_0 r(dL)^{15})^{10+4n} \\ &\leq 2^{142+52n_0} C^{(11+4n_0)A}\ \ell_0^{1+(10+4n_0)(6H+1)}(dL)^{152+60n_0} = N, \end{aligned}$$

donde

$$\ell_0 = max\{11, dL-1\},$$

$$H = 2^{28}\cdot 5\cdot \ell_0^2 C^{2A}(dL)^{30},$$

$$n_0 = 2^{16}\cdot \ell_0^{2(3H+1)}(dL)^{17},$$

C y A son las constantes establecidas en la proposición 2.18 y lema 2.17 (teorema 1.1 [LMO]) respectivamente, C depende sólo de L y A es una constante absoluta efectivamente computable.

□

BIBLIOGRAFIA

[BH1] J. W. Benham, J.S. Hsia, On spinor exceptional representations. Nagoya Math. J. 87, 247-260, (1982).

[BH2] J. W. Benham, J.S. Hsia, Spinor equivalence of quadratic forms, Journal of Number Theory, Vol. 17, N3, 337-342 (1983).

[Ca] J. W. Cassels: Rational Quadratic Forms. Academic Press (1978).

[HKK] J. S. Hsia, Y. Kitaoka, M. Kneser, Representation of positive definite quadratic forms, J. Reine Angew Math, 30, 132-141 (1978).

[Ic1] M.I. Icaza, Effectiveness in representations of positive definite quadratic forms. Thesis. Ohio State University, 1992.

[Ic2] M.I. Icaza, Sums of squares of integral linear forms. Preprint 1994.

[K] M. Kneser, Quadratische Formen. Mathematisches Institut, Gottingen (Duplicated lecture notes) 1974.

[Ki1] Y. Kitaoka, Representations of quadratic forms, Nagoya Math. J. 69, 117-120, (1978).

[Ki2] Y. Kitaoka, Siegel modular forms and representation by quadratic forms, Tata Inst. of Fund. Research, Bombay 1986.

[Ki3] Y. Kitaoka, Arithmetic of quadratic forms, Cambridge University Press, 1993.

[Ko] N. Koblitz, p-adic number, p-adic analysis and zeta-functions. Gradute texts in mathematics. 58. Springer, New York, Heidelberg, Berlin (1977).

[LMO] J.C. Lagarias, H.L. Montgomery, A.M. Odlyzko, A bound for the least prime ideal in the Chebotarev density theorem, Invent. Math., Vol. 54, 271-296, (1979).

[O'M1] O. T. O'Meara, Introduction to Quadratic Forms, Grunmdlehren Math. Wissen 117, Springer-Verlag (1973).

[O'M2] O. T. O'Meara, The integral representation of quadratic forms over local rings. Amer. J. Math. 80, 843-878 (1958).