

11A6-11
L954
c. 1

LA REDUCCIÓN DE LENSTRA,
LENSTRA, LOVÁSZ SOBRE UN
CUERPO DE FUNCIONES
RACIONALES

Tesis

entregada a la

Universidad de Chile

en cumplimiento parcial de los requisitos

para optar al grado de

Magíster en Ciencias con mención en Matemáticas

Facultad de Ciencias

por

Patricia López Limmer

Julio, 2005

Director de Tesis: Ricardo Baeza

FACULTAD DE CIENCIAS

UNIVERSIDAD DE CHILE

INFORME DE APROBACIÓN

TESIS DE MAGÍSTER

Se informa a la Escuela de Postgrado de la Facultad de Ciencias que la Tesis de Magíster presentada por la candidata

PATRICIA LOPEZ LIMMER

ha sido aprobada por la Comisión de Evaluación de la tesis como requisito para optar al grado de Magíster en Ciencias con mención en Matemáticas, en el examen de Defensa de Tesis rendido el día 29 de Julio de 2005.

Director de Tesis:

Ricardo Baeza Rodríguez



Comisión de Evaluación de la Tesis:

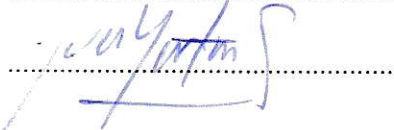
Luis Arenas Carmona



Eduardo Friedman Rafael



Yves Martin Gonzáles





Nací en el norte de Alemania, en Salzgitter-Bad, un día domingo, 13 de Octubre de 1974. Durante mi juventud viví en un pequeño pueblo al sur de Alemania, a 40 km de la frontera con Austria, cerca del castillo Neuschwanstein.

Conocí a mi esposo durante la fiesta de cumpleaños de 17 años. El vivía en el pueblo al lado.

Cuando terminé el colegio quería mudarme lejos... y llegamos a Chile. Aquí entré directamente a la Universidad de Chile a estudiar Licenciatura en Matemáticas. Me casé a los 21 años por convicción y para aprovechar un viaje a Alemania.

Luego de la licenciatura entré en el programa de Doctorado en el año 1999. Cuando esperé a mi hija el 2001, decidí salir del Doctorado y hacer el Magister para abreviar mis estudios.

El año pasado nació mi hijo. Pero el era lo suficientemente tranquilo – al principio – para permitirme terminar mi tesis.

ABSTRACT

THE LENSTRA-LENSTRA- LOVASZ-REDUCTION OVER A RATIONAL FUNCTION FIELD

Consider a rational function field $F(x)$ over a field F , where F is of characteristic $\neq 2$.

We construct an analogue of the Lenstra-Lenstra-Lovasz reduction algorithm over rational function fields and use a theorem by Gerstein to proof that this algorithm is finite.

RESUMEN

LA REDUCCIÓN DE LENSTRA- LENSTRA-LPVASZ SOBRE UN CUERPO DE FUNCIONES RACIONALES

Consideramos un cuerpo de funciones racionales $F(x)$ sobre un cuerpo F , donde F es de característica $\neq 2$.

Construimos el análogo al algoritmo de reducción de Lenstra-Lenstra-Lovasz sobre cuerpos de funciones racionales y se usa un teorema de Gerstein para demostrar que este algoritmo es finito.

ÍNDICE

Introducción	1
Preliminares	
Definiciones	3
Teorema de Gerstein	
<i>El Teorema y su demostración</i>	5
<i>Omisión de la condición “entero”</i>	7
Un análogo del algoritmo de Lenstra, Lenstra, Lovasz para cuerpos de funciones racionales	
La ortogonalización de Gram-Schmidt para $F(x)$	8
La reducción	9
Algunos lemas preliminares	10
Existencia de bases reducidas	
<i>La parte central de la construcción</i>	13
<i>El algoritmo de construcción</i>	14
<i>Finitud del algoritmo</i>	15
Referencias	18

INTRODUCCIÓN

Consideraremos un espacio cuadrático anisótropo n -dimensional (V, q) sobre un cuerpo de funciones racionales $F(x)$, con $\text{char} F \neq 2$.

El presente trabajo tiene como motivación las similitudes entre los números enteros \mathbb{Z} y los polinomios $F[x]$, $\text{char} F \neq 2$, respectivamente el cuerpo de los racionales \mathbb{Q} y el cuerpo de las funciones racionales $F(x)$, aprovechando la propiedad que sobre $F(x)$ tenemos solamente valuaciones no-arquimedianas.

El propósito de este proyecto es construir el análogo a la reducción definida sobre \mathbb{R} por A. K. Lenstra, H. W. Lenstra y L. Lovasz, abreviado reducción LLL, en su publicación [[9], Lenstra A. K., Lenstra H. W., Lovasz L.].

Consideramos un reticulado en un espacio cuadrático anisótropo sobre $F(x)$ con forma cuadrática q y forma bilineal asociada b .

El primer paso consiste en construir una ortogonalización de Gram-Schmidt en $(F(x))^n$ y se estudian algunas propiedades de esta.

Luego se define una reducción de la siguiente manera:

Definición: Sea $\alpha < 0$ un entero. Una base ordenada $\{b_1, \dots, b_n\}$ de un reticulado sobre $F(x)$ con ortogonalización de Gram-Schmidt $\{b_1^*, \dots, b_n^*\}$ con coeficientes

$$\mu_{ij} = \frac{b(b_i, b_j^*)}{b(b_j^*, b_j^*)} \text{ se llama } \underline{\text{reducida}} \text{ si:}$$

$$\text{i. } \forall 1 \leq j < i \leq n \quad \partial \mu_{ij} \leq 0$$

$$\text{ii. } \forall 1 < i \leq n \quad \alpha + \partial q(b_{i-1}^*) \leq \partial q(b_i^* + \mu_{i,i-1} b_{i-1}^*)$$

Se estudian algunas propiedades de la ortogonalización de Gram-Schmidt de una base bajo ciertas transformaciones de la base como paso preliminar para el algoritmo de construcción de la base reducida.

Luego se construye explícitamente el algoritmo de construcción de una base reducida.

Para demostrar que este algoritmo produce una base reducida en una cantidad finita de pasos se necesita un teorema de Gerstein que entrega una relación entre el mínimo y el determinante de un reticulado [[10] Milnor J. y Husemoller D., p. 182]. Se define el mínimo de un reticulado sobre $F(x)$, que se denota como $\min_b L$, como el grado mas pequeño de un elemento no-nulo representado por L . El determinante de un reticulado es el determinante de la matriz de Gram asociada. Este teorema de Gerstein se demuestra en la parte preliminar del presente trabajo.

PRELIMINARES

Definiciones

En todo el presente trabajo consideraremos formas simétricas bilineales sobre un cuerpo de funciones racionales $F(x)$, donde F es un cuerpo de característica $\neq 2$, por ejemplo F_q o R . Sea \deg función grado de $F[x]$, entonces \deg se extiende de forma única a una función $\partial: F(x) \rightarrow Z \cup \{-\infty\}$ definiendo $\partial(p/q) = \deg(p) - \deg(q)$ para $p, q \in F[x] \setminus \{0\}$ y $\partial(0) = -\infty$ [[10] Milnor J. y Husemoller D., p. 181].

Sea (V, b) espacio bilinear simétrico de dimensión finita sobre un cuerpo $F(x)$. Sin restricción podemos considerar $V = (F(x))^n$, donde n es la dimensión de V . Sea L un reticulado sobre $F(x)$, o sea existe una base $\{e_1, \dots, e_n\}$ de V tal que $L = F[x]e_1 + \dots + F[x]e_n$.

$(L, b|_{L \times L})$ es un reticulado con forma bilinear $b: L \times L \rightarrow F(x)$.

Definición: Un vector $x \neq 0$ en un espacio bilinear (V, b) se llama anisótropo, si $b(x, x) \neq 0$. El espacio (V, b) se llama anisótropo si solamente contiene vectores anisótropos.

Definición: Si $b(L \times L) \subseteq F[x]$, se dice que (L, b) es entero.

Definición: Se define el mínimo de L como $\min_b L = \text{Min}\{\partial(b(x, x)) \mid x \in L, x \neq 0\}$

Claramente, si L es un reticulado entero entonces $\min_b L$ existe y se tiene $\min_b L \geq 0$.

Lema: $\min_b L$ existe, si L es anisótropo.

Demostración: Como Z es discreto, es suficiente demostrar que $\{\partial(b(x, x)) \mid x \in L, x \neq 0\}$ es acotado inferiormente. Sea e_1, \dots, e_n una base de L y sea $p \in F[x]$ un denominador

común para todos los $b(e_i, e_j)$, $i, j \in \{1, \dots, n\}$, o sea $b(e_i, e_j) = p_{ij}/p$, donde $p_{ij} \in F[x]$. Para cualquier $v = \sum v_i e_i \in L$, $v_i \in F[x]$, tenemos que $b(v, v) = \sum v_i v_j p_{ij} / p$. Como el caso $b(v, v) = 0$ está excluido ($\partial(0) = -\infty$), ya que L es anisótropo, suponemos que $b(v, v) \neq 0$. Por lo tanto $(p b(v, v)) \in F[x] \setminus \{0\}$ y $\partial(p b(v, v)) \geq 0$. Luego $\partial(b(v, v)) \geq -\partial(p)$.

Como $\min_b(L)$ existe y no depende de la elección de la base de L , este valor está bien definido.

Definición: Se define el determinante de L $\det_b(L) = \det(b(e_i, e_j))$.

Este determinante está bien definido, ya que si elegimos otra base $\{e'_1, \dots, e'_n\}$ para L , las matrices $(b(e_i, e_j))$ y $(b(e'_i, e'_j))$ son congruentes mediante una matriz $U \in GL_n(F[x])$, o sea $(b(e_i, e_j)) = U^t (b(e'_i, e'_j)) U$. Por lo tanto $\det(b(e_i, e_j)) = \det(b(e'_i, e'_j)) (\det U)^2$. Pero como U es invertible y en $F[x]$ solo las unidades son invertibles, entonces $\det U \in F \setminus \{0\}$. Por lo tanto $\det(b(e_i, e_j))$ está bien definido si es considerado como elemento de $(F[x] \setminus \{0\}) / (F \setminus \{0\})$. Luego $\partial(\det(b(e_i, e_j))) = \partial(\det(b(e'_i, e'_j))) + 2\partial(\det U)$. Como $\partial(\det U) = 0$, $\partial(\det_b(L))$ está bien definido. Además como la forma es anisótropa, tenemos que $\det_b(L) \neq 0$.

Teorema de Gerstein

El Teorema y su demostración:

Teorema (Gerstein): Consideremos un espacio cuadrático n -dimensional (V, b) sobre un cuerpo de funciones racionales $F(x)$ con función ∂ como antes descrito. Sea L un reticulado entero en V .

Si V es anisótropo, entonces se tiene

$$0 \leq \min_b L \leq (1/n) \partial(\det_b L)$$

Demostración: [[10], Milnor J. y Husemoller D, p. 182-184] Sea $\{e_1, \dots, e_n\}$ base de L en V y sea $v = \sum p_i e_i$ el vector donde se cumple $\partial(b(v, v)) = \min_b L$. Entonces $\gcd(p_1, \dots, p_n) = 1$ por tratarse del mínimo. Por lo tanto podemos completar $\{v\}$ a una base de L sobre V . Sin restricción $v = e_1$ y $\partial(b(e_1, e_1)) = \min_b L$. Para simplificar la notación sea $p_{ij} = b(e_i, e_j)$. $p_{ij} \in F[x]$ debido a que se consideran reticulados enteros.

Ahora hacemos una inducción sobre la dimensión n .

Para $n=1$ tenemos que $\min_b L = \partial(b(e_1, e_1)) \leq (1/1) (\partial \det(b(e_1, e_1))) = \partial(\det_b L)$ y la desigualdad se cumple trivialmente.

Para $n > 1$ sea e'_i ($2 \leq i \leq n$) la proyección de e_i en e_1^\perp , el complemento ortogonal de e_1 en V , o sea $e'_i = e_i - (p_{i1}/p_{11}) e_1$. Entonces $\{e_1, e'_2, \dots, e'_n\}$ es linealmente independiente. Sea $M = F[x] e'_2 \oplus \dots \oplus F[x] e'_n$ y $L' = F[x] e_1 \oplus M$.

Podemos construir $q_{ij} \in F[x]$ ($i, j \geq 2$) tales que $b(e'_i, e'_j) = q_{ij} / p_{11}$ de manera que

$$\det_b L' = \det \begin{pmatrix} p_{11} & 0 \\ 0 & \frac{1}{p_{11}} (q_{ij}) \end{pmatrix} = \det(q_{ij}) / p_{11}^{n-2}$$

Sea $c = p_{11} b \mid_{M \times M}$. Entonces M es respecto a c un reticulado entero en el espacio anisótropo $F(x) M$. Por lo tanto obtenemos para $\det_c M = \det q_{ij}$, $(i, j \geq 2)$, y luego $\det_c M = p_{11}^{n-2} \det_b L' = p_{11}^{n-2} \det_b L$. Observe que $\det_b L = \det_b L'$ ya que la matriz que relaciona $\{e_1, \dots, e_n\}$ y $\{e_1, e'_2, \dots, e'_n\}$ es triangular superior con 1s en la diagonal. Por la hipótesis de inducción tenemos que

$$\min_c M \leq \partial \det_c M / (n-1)$$

Como $\partial c = \partial p_{11} + \partial b$ y $\partial(p_{11}^{n-2} \det_b L') = (n-2) \partial p_{11} + \partial \det_b L$ tenemos que

$$\partial p_{11} + \min_b M \leq (\partial \det_b L + (n-2) \partial p_{11}) / (n-1)$$

$$\text{O sea, } \min_b M \leq (\partial \det_b L - \partial p_{11}) / (n-1)$$

Afirmación: $\min_b L = \partial p_{11} \leq \min_b M$.

Mediante esta afirmación obtenemos que $\partial p_{11} \leq \min_b M \leq (\partial \det_b L - \partial p_{11}) / (n-1)$ y luego la desigualdad deseada $\partial p_{11} \leq \partial \det_b L / n$.

Para demostrar la afirmación consideremos el vector $w = \sum \lambda_i e_i$, $\lambda_i \in F[x]$. Cambiando a la otra base obtenemos

$$w = (\lambda_1 + (p_{21}\lambda_2 + \dots + p_{n1}\lambda_n) / p_{11}) e_1 + \lambda_2 e'_2 + \dots + \lambda_n e'_n$$

Ahora suponemos que $\lambda_2, \dots, \lambda_n \in F[x]$ fueron elegidos de manera que el vector (no nulo) $w' = \lambda_2 e'_2 + \dots + \lambda_n e'_n \in M$ satisface $\partial(b(w', w')) = \min_b M$. Luego hacemos la división $p_{21}\lambda_2 + \dots + p_{n1}\lambda_n = p_{11}q + r$, donde $q, r \in F[x]$ y $r = 0$ o $\partial r \leq \partial p_{11}$. Eligiendo $\lambda_1 = -q$, el coeficiente $\beta = r / p_{11}$ de e_1 en la descripción de w es 0 o satisface $\partial \beta < 0$.

Como $w \neq 0$ y como suponemos que b es anisótropa, tenemos que

$$b(w,w) = \beta^2 p_{11} + b(w',w') \neq 0$$

Si $\beta = 0$, tenemos que $\min_b L = \partial p_{11} \leq \partial b(w,w) = \partial b(w',w') = \min_b M$ como deseado.

Por lo tanto suponemos ahora que $\beta \neq 0$ y $\partial\beta < 0$. Entonces como ∂ es una valuación no-arquimediana,

$$\begin{aligned} \min_b L &= \partial p_{11} \leq \partial b(w,w) \leq \max (\partial(\beta^2 p_{11}), \partial b(w',w')) \\ &= \max (\partial p_{11} + 2\partial\beta , \min_b M) \end{aligned}$$

Este último máximo tiene que ser igual a $\min_b M$, ya que si fuera igual a $\partial p_{11} + 2\partial\beta$, tendríamos que $\partial p_{11} \leq \partial p_{11} + 2\partial\beta$, o sea $0 \leq 2\partial\beta$, contradicción. Por lo tanto hemos demostrado la afirmación faltante.

Omisión de la condición “entero”

La condición que el reticulado L sea entero tiene como consecuencia que $0 \leq \min_b L$ y $0 \leq \partial(\det_b L)$ y por lo tanto $0 \leq \min_b L \leq (1/n) \partial(\det_b L)$. Pero para establecer la desigualdad $\min_b L \leq (1/n) \partial(\det_b L)$, esta condición no es necesaria durante la demostración y no se multiplicó por $\min_b L$ o $\partial(\det_b L)$. Por lo tanto se puede omitir la condición del reticulado entero omitiendo en el resultado la parte $0 \leq \min_b L$.

UN ANÁLOGO DEL ALGORITMO DE LENSTRA, LENSTRA, LOVASZ PARA CUERPOS DE FUNCIONES RACIONALES

La ortogonalización de Gram-Schmidt

Sea (V, b) un espacio cuadrático anisótropo sobre el cuerpo $F(x)$ de funciones racionales en una variable, $\text{char} F \neq 2$, y sea $L \subset V$ un reticulado sobre $F[x]$, es decir, $L = F[x]b_1 \oplus \dots \oplus F[x]b_n$, donde $\{b_1, \dots, b_n\}$ es una base de V .

El proceso de ortogonalización de Gram-Schmidt se aplica en este caso igual que sobre R : Sea $b_i^* = b_i$, y supongamos definido b_1^*, \dots, b_i^* con $b(b_i^*, b_j^*) = 0 \forall i \neq j$.

Entonces se define $b_{i+1}^* = b_{i+1} - \sum_{j=1}^i \frac{\langle b_{i+1}, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} b_j^*$ (usamos $\langle \cdot, \cdot \rangle$ en vez de $b(\cdot, \cdot)$)

Se obtiene así una base ortogonal $\{b_1^*, \dots, b_n^*\}$ de V , y se tiene para todo i :

$$b_i = b_i^* + \sum_{j=1}^{i-1} \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} b_j^*$$

Escribiendo $\mu_{ij} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \quad \forall 1 \leq i, j \leq n$ vemos que $b_i = \sum_{j=1}^i \mu_{ij} b_j^*$, ya que se puede

verificar fácilmente que $\mu_{ii}=1$, $\mu_{ij}=0$ si $i < j$, es decir la matriz de transformación de $\{b_i\}$ en $\{b_i^*\}$ es triangular inferior con 1s en la diagonal. Por lo tanto $\det(b_1, \dots, b_n) = \det(b_1^*, \dots, b_n^*)$. Además $\langle b_1, \dots, b_i \rangle = \langle b_1^*, \dots, b_i^* \rangle \forall i$.

La reducción

Sea $\alpha < 0$ un entero. Consideremos una base $\{b_1, \dots, b_n\}$ de L , la base ortogonalizada de Gram-Schmidt $\{b_1^*, \dots, b_n^*\}$ de L y los coeficientes μ_{ij} , $1 \leq i, j \leq n$, asociados.

Definición: La base $\{b_1, \dots, b_n\}$ de L se llama reducida si:

- i. $\forall 1 \leq j < i \leq n \quad \partial \mu_{ij} \leq 0$
- ii. $\forall 1 < i \leq n \quad \alpha + \partial q(b_{i-1}^*) \leq \partial q(b_i^* + \mu_{i,i-1} b_{i-1}^*)$

donde escribimos $q(b)$ en vez de $\langle b, b \rangle$ (a veces se escribe también $|b|^2$ en vez de $\langle b, b \rangle$) para todo $b \in V$.

Definición: Sea $1 \leq k \leq n+1$, $B = \{b_1, \dots, b_n\}$ base de L . Escribiremos

$$A_k(B) \Leftrightarrow \begin{cases} \forall 1 \leq j < i < k, \quad \partial \mu_{ij} \leq 0 \\ \forall 1 < i < k, \quad \alpha + \partial q(b_{i-1}^*) \leq \partial q(b_i^* + \mu_{i,i-1} b_{i-1}^*) \end{cases}$$

Es obvio que $A_1(B)$ y $A_2(B)$ son siempre ciertos.

Notación: Sea $f \in F(x)$, $f = \frac{p}{q}$ con $p, q \in F[x]$. Entonces $p = s q + r$, $s, r \in F[x]$, $r=0$ ó

$\text{degr} < \text{degr} q$. Se tiene $f = s + \frac{r}{q}$. Escribiremos $[f] := s$, $\frac{r}{q} =: \langle f \rangle$. $\langle f \rangle$ se llama la parte

fraccional de f y $[f]$ la parte entera de f . En particular $\partial(\langle f \rangle) < 0$.

Algunos lemas preliminares

Lema 1: Sea $p \in F[x]$, $B = \{b_1, \dots, b_n\}$ base de L , $2 \leq k \leq n$.

Entonces $\{b_1, \dots, b_{k-1}, b_k - pb_{k-1}, b_{k+1}, \dots, b_n\} =: B'$ también es base de L , y si $\{b_1^*, \dots, b_n^*\}$ son los vectores de Gram-Schmidt asociados a B , se cumple $b_i^* = b_i^*$ $\forall 1 \leq i \leq n$, $\mu_{ij}' = \mu_{ij} \forall i \neq k$, $\mu_{kj}' = \mu_{kj} - p\mu_{k-1,j}$, $\forall j$.

Demostración: Claramente se cumple que $b_i^* = b_i^* \forall 1 \leq i \leq k-1$. Falta calcular

$$\mu_{kj}' = \frac{\langle b_k', b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} = \frac{\langle b_k - pb_{k-1}, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} = \mu_{kj} - p\mu_{k-1,j} \text{ para obtener las otras afirmaciones.}$$

Para b_k^* obtenemos: $b_k^* = b_k' - \sum_{i=1}^{k-1} \mu_{ki}' b_i^* = b_k - pb_{k-1} - \sum_{i=1}^{k-1} (\mu_{ki} - p\mu_{k-1,i}) b_i^* = b_k -$

$$\sum_{i=1}^{k-1} \mu_{ki} b_i^* + p(b_{k-1}^* - b_{k-1} + \sum_{i=1}^{k-2} \mu_{k-1,i} b_i^*) = b_k^*.$$

Por lo tanto, tenemos que $b_i^* = b_i^* \forall 1 \leq i \leq n$.

Lema 2: Sea $B = \{b_1, \dots, b_n\}$ base de L y supongamos que B satisface $A_k(B)$ para algún k con $2 \leq k \leq n$. Sea $B' = \{b_1, \dots, b_{k-1}, b_k - [\mu_{k,k-1}]b_{k-1}, b_{k+1}, \dots, b_n\}$.

Entonces B' es base de L , se cumple $A_k(B')$ y además $\partial(\mu'_{k,k-1}) < 0$.

Demostración: Por el lema 1, como $b_i^* = b_i^* \forall 1 \leq i \leq n$, vemos fácilmente que B' también satisface A_k . Por otro lado

$$\mu_{k,k-1}' = \mu_{k,k-1} - [\mu_{k,k-1}] \mu_{k-1,k-1} = \mu_{k,k-1} - [\mu_{k,k-1}] = \langle \mu_{k,k-1} \rangle, \text{ es decir } \partial(\mu_{k,k-1}') < 0.$$

El siguiente resultado muestra que al intercambiar solo dos vectores consecutivos de una base, la correspondiente base ortogonal de Gram-Schmidt cambia totalmente.

Lema 3: Sea $B = \{b_1, \dots, b_n\}$ base de L , $2 \leq k \leq n$, y sea $B' = \{b_1, \dots, b_{k-2}, b_k, b_{k-1}, b_{k+1}, \dots, b_n\}$.

Entonces B' es base de L y los vectores $\{b_1^*, \dots, b_n^*\}$ de Gram-Schmidt son

$$\forall i \neq k-1, k, \quad b_i^* = b_i$$

$$b_{k-1}^* = b_k^* + \mu_{k,k-1} b_{k-1}^*$$

$$b_k^* = b_{k-1}^* - \mu_{k,k-1}^2 b_{k-1}^*$$

$$\text{Además } \mu_{ij}^* = \mu_{ij} \quad 1 \leq j < i \leq k-2$$

$$\mu_{k-1,j}^* = \mu_{kj} \quad \mu_{kj}^* = \mu_{k-1,j} \quad 1 \leq j \leq k-2$$

$$\mu_{k,k-1}^* = \frac{\mu_{k,k-1} q(b_{k-1}^*)}{q(b_k^*) + \mu_{k,k-1}^2 q(b_{k-1}^*)}$$

Demostración:

$$\mu_{k-1,j}^* = \frac{\langle b_{k-1}^*, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} = \frac{\langle b_k, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} = \mu_{kj} \quad \text{si } 1 \leq j \leq k-2. \text{ Del mismo modo se obtiene que}$$

$$\mu_{kj}^* = \frac{\langle b_k^*, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} = \frac{\langle b_{k-1}, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} = \mu_{k-1,j} \quad \text{si } 1 \leq j \leq k-2.$$

$$\begin{aligned} \mu_{k,k-1}^* &= \frac{\langle b_{k-1}^*, b_{k-1}^* \rangle}{\langle b_{k-1}^*, b_{k-1}^* \rangle} = \frac{\langle b_{k-1}, b_k^* + \mu_{k,k-1} b_{k-1}^* \rangle}{\langle b_k^* + \mu_{k,k-1} b_{k-1}^*, b_k^* + \mu_{k,k-1} b_{k-1}^* \rangle} = \frac{\overbrace{\langle b_{k-1}, b_k^* \rangle}^{=0} + \mu_{k,k-1} \langle b_{k-1}, b_{k-1}^* \rangle}{q(b_k^*) + \mu_{k,k-1}^2 q(b_{k-1}^*)} = \\ &= \frac{\mu_{k,k-1} q(b_{k-1}^*)}{q(b_k^*) + \mu_{k,k-1}^2 q(b_{k-1}^*)} \end{aligned}$$

Lema 4: Sea $B = \{b_1, \dots, b_n\}$ base de L y supongamos que se cumple $A_k(B)$ para algún k con $2 \leq k \leq n$. Supongamos $\alpha + \partial q(b_{k-1}^*) > \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$. Además por el lema 2 se puede suponer sin restricción que $\partial \mu_{k,k-1} \leq 0$.

Entonces $B' = \{b_1, \dots, b_{k-2}, b_k, b_{k-1}, b_{k+1}, \dots, b_n\}$ es base de L que satisface A_{k-1} y se cumple $\partial q(b_{k-1}^*) < \alpha + \partial q(b_{k-1}^*)$

Demostración: Del lema 3 resulta $b_i^* = b_i^* \quad \forall i \neq k-1, k$ y $\mu_{ij}' = \mu_{ij}, \quad \forall 1 \leq j < i \leq k-2$. De esto resulta que B' satisface A_{k-1} . De $b_{k-1}^* = b_k^* + \mu_{k,k-1} b_{k-1}^*$ y de la hipótesis resulta que $\partial q(b_{k-1}^*) = \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*) < \alpha + \partial q(b_{k-1}^*)$

Observaciones:

1. La hipótesis $\alpha + \partial q(b_{k-1}^*) > \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$ implica para la base B' que $\alpha + \partial q(b_{k-1}^*) > \partial q(b_{k-1}^*)$ por el lema 3 y en particular, como $\alpha < 0$, $\partial q(b_{k-1}^*) < \partial q(b_{k-1}^*) = \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$. Utilizando nuevamente el hecho que $\alpha < 0$, obtenemos incluso $\alpha + \partial q(b_{k-1}^*) < \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$

2. Si $B = \{b_1, \dots, b_n\}$ es base de L , $1 < k \leq n$, y $r \in F[x]$, entonces $\forall 1 \leq m < k$, $B' = \{b_1, \dots, b_{k-r} r b_m, b_{k+1}, \dots, b_n\}$ es base de L y obviamente $b_i^* = b_i^* \quad \forall 1 \leq i \leq n$. En particular $\mu_{ij}' = \mu_{ij} \quad \forall 1 \leq j < i \neq k$, y $\forall 1 \leq j < k$ tenemos $\mu_{kj}' = \mu_{kj} - r \mu_{mj}$. Si $m < j < k \Rightarrow \mu_{kj}' = \mu_{kj}$.

Lema 5: Sea $B = \{b_1, \dots, b_n\}$ base de L que satisface A_k , $2 \leq k \leq n$. Sea sin restricción $\partial\mu_{k,k-1} \leq 0$. Supongamos que A_{k+1} no se cumple para B , pero que se tiene $\alpha + \partial q(b_{k-1}^*) \leq \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$. Sea $l < k$ el índice maximal de modo que $\partial\mu_{kl} > 0$.

Entonces $B' = \{b_1, \dots, b_{k-1}, b_k - [\mu_{kl}]b_l, b_{k+1}, \dots, b_n\}$ es base de L que satisface A_k y además $\alpha + \partial q(b_{k-1}^*) \leq \partial q(b_k^* + \mu'_{k,k-1} b_{k-1}^*)$ y $\partial\mu'_{ki} \leq 0 \quad \forall 1 \leq i < k$.

Demostración: Por la observación anterior $b_i^* = b_i \quad \forall 1 \leq i \leq n$, $\mu'_{ij} = \mu_{ij} \quad \forall 1 \leq j < i \neq k$, y además $\mu'_{kj} = \mu_{kj} - r\mu_{lj}$, donde $r := [\mu_{kl}]$. Si $l < j < k$ se obtiene además $\mu'_{kj} = \mu_{kj}$ y en particular $\mu'_{k,k-1} = \mu_{k,k-1}$, ya que $\partial\mu_{k,k-1} \leq 0$ implica $l < k-1$. En particular tenemos $\mu'_{kl} = \mu_{kl} - [\mu_{kl}] = \langle \mu_{kl} \rangle$, es decir $\partial\mu'_{kl} \leq 0$. Es fácil comprobar que B' también satisface A_k . Como $\forall 1 < j < k$ se tiene por definición de $l \quad \mu'_{kj} = \mu_{kj}$ y $\partial\mu_{kj} \leq 0$, vemos que $\partial\mu'_{kj} \leq 0 \quad \forall 1 \leq j < k-1$.

Existencia de bases reducidas

La parte central de la construcción:

De los resultados anteriores obtenemos el primer paso hacia la demostración que existen bases LLL-reducidas:

Corolario: Sea $B = \{b_1, \dots, b_n\}$ base de L , $1 \leq k \leq n$, de modo que $A_k(B)$ se cumple. Supongamos $k = 1$ ó $\alpha + \partial q(b_{k-1}^*) \leq \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$.

Entonces existe base B' de L que satisface A_{k+1} .

Observación: Por la primera observación al lema 4, si no se tiene que $\alpha + \partial q(b_{k-1}^*) \leq \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$, se construye la base B' como en el lema 4 intercambiando el $k-1$ -

ésimo con el k -ésimo vector y para esta base se cumple $\alpha + \partial q(b_{k-1}^*) < \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$.

Demostración: Si $k = 1$, como A_1 y A_2 son siempre ciertos, se tiene el resultado.

Supongamos $2 \leq k \leq n$ con $\alpha + \partial q(b_{k-1}^*) \leq \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$. Además por el lema 2 podemos suponer que $\partial \mu_{k,k-1} \leq 0$. Si B no satisface A_{k+1} , se elige l como en el lema anterior y obtenemos una base B' que satisface A_k , $\alpha + \partial q(b_{k-1}^*) \leq \partial q(b_k^* + \mu'_{k,k-1} b_{k-1}^*)$ y además $\partial \mu'_{ki} \leq 0 \quad \forall 1 \leq i < k$. Entonces podemos bajar l a $l-1$ y seguir aplicando el lema 5 hasta obtener una base B' que satisface A_{k+1} .

El algoritmo de construcción:

Sea $B = \{b_1, \dots, b_n\}$ base de L .

Paso 1: Determinar k , $1 \leq k \leq n+1$, como el mayor índice de modo que $A_k(B)$ se cumple.

Si $k = n+1$, B es reducida.

Si $k < n+1$, y si $\alpha + \partial q(b_{k-1}^*) > \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$ entonces sigue el paso 2.

Si $k < n+1$, y si $\alpha + \partial q(b_{k-1}^*) \leq \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$ entonces sigue el paso 3.

Paso 2: Se intercambia los vectores b_k y b_{k-1} en la base (lema 4: B satisface ahora A_{k-1} y $\alpha + \partial q(b_{k-1}^*) \leq \partial q(b_k^* + \mu_{k,k-1} b_{k-1}^*)$). Luego se vuelve al paso 1.

Paso 3: Determinar $l < k$ como el índice maximal tal que $\partial \mu_{kl} > 0$.

Si $l = 0$, entonces $\partial \mu_{kj} \leq 0 \quad \forall j$, y se vuelve al paso 1.

Si $l > 0$, sea reemplaza b_k por $b_k - [\mu_{kl}]b_l$ (lema 5) y se vuelve al principio del paso 3.

Finitud del algoritmo:

En la demostración del corolario hemos visto que solo se necesita una cantidad finita de pasos por el paso 3, entre vueltas por el paso 2, ya que l disminuye en al menos 1. Falta ver que durante el proceso de construcción, el paso 2, o sea la condición del lema 4, solo aparece un número finito de veces.

Teorema: Sea L un reticulado en (V, b) . Entonces L tiene una base reducida (LLL) y esta base se obtiene en un número finito de pasos de una base arbitraria de L .

Demostración: Sea $B = \{b_1, \dots, b_n\}$ base de L , es decir, $L = F[x]b_1 \oplus \dots \oplus F[x]b_n$. Sea $\forall 1 \leq i \leq n$, $L_i(B) = F[x]b_1 \oplus \dots \oplus F[x]b_i$, de modo que $L_1(B) \subset L_2(B) \subset \dots \subset L_n(B) = L$. $L_i(B)$ es reticulado en $\langle b_1, \dots, b_i \rangle = \langle b_1^*, \dots, b_i^* \rangle$, así como también $L_i(B^*) = F[x]b_1^* \oplus \dots \oplus F[x]b_i^* \quad \forall i$.

El automorfismo $f_i: \langle b_1^*, \dots, b_i^* \rangle \rightarrow \langle b_1, \dots, b_i \rangle$, $f_i(b_j^*) = b_j$, $1 \leq j \leq i$, tiene determinante 1 y $f_i: L_i(B^*) \rightarrow L_i(B)$. En particular $\det(L_i(B^*)) = \det(L_i(B)) \quad \forall i$, es decir, $\det(L_i(B)) =$

$$\prod_{j=1}^i q(b_j^*) \quad 1 \leq i \leq n \quad \text{y} \quad \det L = \det(L_n(B)) = \prod_{j=1}^n q(b_j^*)$$

Definamos $d(B) := \prod_{i=1}^{n-1} \det L_i(B)$.

Afirmación: Existe una constante $c > 0$, que no depende de la base B , tal que para toda base B de L se tiene $\partial d(B) \geq c$.

Para demostrar esta afirmación consideremos $m = \min L = \min\{\partial q(u) \mid u \in L, u \neq 0\}$.

Por el teorema de Gerstein tenemos que $m \leq \min(L_i(B)) \leq (1/i) \partial \det(L_i(B))$, es decir,

$$\partial \det(L_i(B)) \geq im \text{ y por lo tanto } \partial d(B) = \sum_{i=1}^{n-1} \partial \det(L_i(B)) \geq \sum_{i=1}^{n-1} mi, \text{ es decir,}$$

$$\partial d(B) \geq m \frac{n(n-1)}{2} = c$$

Fijemos ahora la base $B = \{b_1, \dots, b_n\}$ de L . Sea $B' = \{b_1', \dots, b_n'\}$ base de L que se obtiene como en el lema 2 o en el lema 5. Entonces $B^* = B'^*$, es decir, $b_i^* = b_i'^*$ $\forall 1 \leq i \leq n$. Entonces $d(B) = d(B')$.

Si ahora B' se obtiene según el lema 4, entonces $\forall i < k-1$ se tiene $b_j^* = b_j'^* \forall 1 \leq j \leq i$ y por lo tanto $\det(L_i(B)) = \det(L_i(B'))$ si $i < k-1$.

$$\text{Además } \det(L_{k-1}(B')) = q(b_{k-1}^*) \prod_{i=1}^{k-2} q(b_i^*)$$

$$\Rightarrow \partial \det(L_{k-1}(B')) = \partial q(b_{k-1}^*) + \sum_{i=1}^{k-2} \partial q(b_i^*)$$

$$< \alpha + \partial q(b_{k-1}^*) + \sum_{i=1}^{k-2} \partial q(b_i^*) \quad (\text{ver observaciones al lema 4})$$

$$\partial \det(L_{k-1}(B')) < \alpha + \partial \det(L_{k-1}(B))$$

Si $i \geq k$, entonces $L_i(B) = L_i(B')$, $\det(L_i(B)) = \det(L_i(B'))$. Por lo tanto con $d(B') =$

$$\prod_{i=1}^{n-1} \det L_i(B') \text{ obtenemos } \partial d(B') < \alpha + \partial d(B).$$

En este proceso, si aplicamos t veces el lema 4, obtendremos para la base B^t de L que resulta $c \leq \partial d(B^t) < t\alpha + \partial d(B)$.

Pero como $\alpha < 0$, si t crece indefinidamente, se obtiene una contradicción. En efecto tenemos $t(-\alpha) < \partial d(B) - c$, con $-\alpha > 0$, es decir, $t < \frac{\partial d(B) - c}{-\alpha}$ es la cota para el número de veces que puede aparecer la condición del lema 4 en este proceso. Esto implica que después de un número finito de pasos se obtiene una base reducida LLL de L .

REFERENCIAS

- [1] Cassels, J. W. S. *An introduction to the geometry of numbers*. Springer-Verlag, 1959.
- [2] Cohen, Henri, *A course in computational Algebraic Number Theory*, Springer-Verlag, 1993.
- [3] Conway, J. H., y Sloane, N. J. A. , *Root lattices*. Third Edition, Springer-Verlag, 1999.
- [4] Conway, J. H., y Sloane, N. J. A. , *Sphere Packings, Lattices and Groups*. Third Edition, Springer-Verlag, 1999.
- [5] Gerstein, Larry J.. *A new proof of a theorem of Cassels and Pfister*, Proceedings of the American Mathematical Society, 41(1973), p. 327-328
- [6] Gerstein, Larry J., *Symmetric bilinear forms over polynomial rings*, mimeographed notes, University of Notre Dame, 1973
- [7] Lam, T. Y. *Serre's Conjecture*. Lecture Notes in Mathematics, Springer-Verlag, 1978.
- [8] Lam, T. Y. *The Algebraic Theory of Quadratic Forms*. Lecture Notes in Mathematics, W.A. Benjamin, Inc., 1973.
- [9] Lenstra, A. K., Lenstra, H. W., Lovasz, L., *Factoring polynomials with rational coefficients*. Mathematische Annalen, Band 261, p. 515-534, 1982
- [10] Milnor J. y Husemoller D. *Symmetric Bilinear Forms*, Springer-Verlag, 1973.
- [11] O'Meara, O. T. *Introduction to Quadratic Forms*, Springer-Verlag, 1963.
- [12] Scharlau, W. *Quadratic and Hermitian Forms.*, Springer-Verlag, 1985.
- [13] Thomas, Alan David. *Zeta-functions: An introduction to algebraic geometry*. London, Pitman Publishing, 1977.