CUBO, Vol. 3.Octubre 1987
Págs. 142-193

FORMAS CUADRATICAS

Enzo R. Gentile *

0. INTRODUCCION.

La teoría clásica de formas cuadráticas puede considerarse como un capítulo de la teoría de números. Sus grandes exponentes son Fermat, Lagrange, Legendre, Gauss, Minkowski.El problema que atrajo el interés de estos grandes matemáticos fue el de representar números por formas cuadráticas. Por ejemplo:

¿Qué enteros son suma de dos cuadrados?
¿Qué enteros son suma de 4 cuadrados?

La famosa ecuación de Pell

$$X^2 - d.Y^2 = m$$

su tratamiento

* Universidad de Buenos Aires

es otro ejemplo que generó mucha teoría y su tratamiento puede considerarse un tema obligado en libros elementales de teoría de números.

Fermat (1654) enunció teoremas en este sentido, a saber,

p primo,

$$p = 4m + 1 \quad ===> \quad p = x^2 + y$$
$$p = 6n + 1 \quad ===> \quad p = x^2 + By^2$$
$$p = 8n + 1 \quad ===> \quad p = x^2 + 2y^2$$

Estos resultados fueron probados por Euler en 1761 y 1763. En el mismo siglo 18 se demostraron muchos teoremas sobre representación de enteros como suma de cuadrados. Lagrange (1773) desarrolló por primera vez una teoría general de formas cuadráticas binarias

$$aX^2 + bXY + cY^2$$

con discriminante $D = b^2-4ac$, para estudiar el problema general de la representación de un entero h por la forma anterior, o sea la existencia de enteros x,y tales que

$$h = ax^2 + bxy + cy^2 .$$

Es claro que un cambio lineal de variables

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \ell & m \\ n & r \end{bmatrix} \cdot \begin{bmatrix} x' \\ y' \end{bmatrix} \qquad \ell, m, n, r \in Z \ , \quad \ell.r-m.n=1$$

da lugar a una ecuación

$$ax^2 + bxy + cy^2 = Ax'^2 + Bx'y' + Cy'^2$$

con

$$A = a\ell^2 + b\ell n + cn^2$$
$$B = 2a\ell m + b(\ell r+mn) + 2cnr$$
$$C = am^2 + bmr + cr^2$$

y por lo tanto las dos formas cuadráticas

$$aX^2 + bXY + cY^2 \quad y \quad AX^2 + BXY + CY^2$$

representan a los mismos enteros. Decimos que estas dos formas son equivalentes. La idea clave es obtener por estos cambios de variables formas cuadráticas canónicas. Lagrange desarrolló una teoría de reducción para formas binarias y probó que toda forma es equivalente a cierta forma canónica reducida. Esta teoría fue continuada por Gauss y ocupa un lugar importante en su famoso Disquisitiones Arithmeticae (1801). Trabajando con formas de discriminante fijo D, Gauss prueba que el número de clases de equivalencia de formas binarias es finito. Por ejemplo el número de clases correspondiente a las formas binarias $aX^2 + bXY + cY^2$ de discriminante -4 es igual a 1. O sea toda tal forma es equivalente, por un cambio de variables unimodular (como vimos más arriba) a la forma $X^2 + Y^2$.

Si p es un primo positivo de la forma $p = 4m + 1$, veremos que es representable por la forma $X^2 + Y^2$. Es bien sabido de la teoría elemental de números que una tal para un tal primo es -1 un residuo cuadrático, o sea la ecuación $X^2 \equiv -1 \pmod{p}$ admite solución en Z. Escribamos pues $b^2 = -1 + p.q$, $b, q \in Z$. La forma cuadrática $pX^2 + 2bXY + qY^2$ representa a p y tiene discriminante $4b^2 - 4pq = -4$. Por lo tanto es equivalente a la forma $X^2 + Y^2$. Concluimos que $X^2 + Y^2$ representa a p.

La generalización de esta situación nos lleva a considerar "formas cuadráticas"

$$F = F(X_1,\ldots,X_n) = a_{11}X^2 + 2a_{12}X_1X_2 + \ldots + 2a_{1n}X_1X_n +$$

$$+ a_{22}X_2^2 + 2a_{23}X_2X_3 + \ldots + 2a_{2n}X_2X_n +$$

$$\cdot \qquad \cdot \qquad \ldots \qquad \cdot$$

$$+ a_{nn}X_n^2$$

o brevemente

$$= \sum_{i,j=1}^{n} a_{ij}X_iX_j$$

escribiendo $a_{ij} = a_{ji}$

La matriz $A = [a_{ij}]$ se denomina la matriz de F y podemos escribir

$$F(X_1,\ldots,X_n) = {}^tX.A.X$$

donde X denota el vector columna de indeterminadas $X_1,\ldots,X_n$ y ${}^tX$ denota traspuesto de X, por lo tanto el vector fila $(X_1,\ldots,X_n)$.

Si P es una matriz regular de nxn, escribiendo $X = P.Y$, resulta

$$F(X_1,\ldots,X_n) = {}^t(P.Y)A(P.Y) = {}^tY.({}^tP.A.P).Y$$

$$= G(Y_1,\ldots,Y_n)$$

O sea, por un cambio lineal de coordenadas : X = P.Y, se obtiene una forma cuadrática $G(Y_1,\ldots,Y_n)$ de matriz ${}^tP.A.P$. Decimos que F y G son formas cuadráticas equivalentes. Escribimos $F \sim G$. El problema general inicial subsiste. Dada una forma cuadrática F con matriz A de coeficientes enteros, se trata de estudiar la resolubilidad de ecuaciones del tipo

$$F(X_1,\ldots,X_m) = m$$

con m entero. Este es un problema muy difícil y lo que se hace habitualmente es considerar formas cuadráticas con coeficientes en un cuerpo k . O sea la matriz A posee coeficientes en el cuerpo k . Si el cuerpo k es de característica $\neq 2$ las formas cuadráticas sobre k admiten una gran simplificación en su escritura, a saber, toda forma cuadrática es equivalente a una forma cuadrática diagonal

$$F \sim a_1X_1^2 + \ldots + a_nX_n^2$$

que recuerda la reducción de una cuádrica a sus ejes principales.

El desarrollo posterior ocurre como dependiendo de la teoría de grupos, particularmente el grupo lineal general en n variables y los subgrupos del mismo que dejan invariante una forma cuadrática (grupo ortogonal), una forma hermitiana (grupo unitario) ó una forma alternada (grupo simpléctico). Estos grupos jugaron un papel fundamental en el desarrollo del álgebra, teoría de números, en Análisis y Geometría y también en Física en la teoría de la relatividad y física atómica. Históricamente se estudian dichos grupos en el ámbito de los números reales o complejos y consecuentemente los métodos infinitesimales son de extrema fuerza en su desarrollo. El

punto de vista moderno encara el estudio de estos grupos so - bre cuerpos en general y obliga al desarrollo de métodos alge braicos en esencia.

El primer matemático en imaginar esos métodos fue Camile Jordan que desarrolló las ideas de Galois para estudiar los grupos clásicos (o sea los grupos enumerados anteriormente) para los cuerpos Z_p de restos módulo p. Su contribución aparece en el libro "Traité des Substitutions" (1870). Sus métodos fueron mejorados y generalizados por L.E. Dickson a cuerpos finitos cualesquiera. Según Dieudonné los resultados obtenidos por Dickson son casi definitivos y el libro de Dickson, Linear Groups (1901) es todavía la única obra deta - llada y co mpleta al respecto. La aparición de un trabajo fundamental de Ernst Witt (Teoría de formas cuadráticas sobre cuerpos arbitrarios, J. Reine U.Angew. Math., 1937) donde desarrolla la teoría de vectores isótropos y prueba su Teorema de Extensión, permite ampliar la teoría de Jordan-Dickson a cuerpos arbitrarios. Ya en un lenguaje moderno, utilizando la teoría de espacios vectoriales, se desarrolla la teoría de formas cuadráticas y la obra de J.Dieudonné: La Géometrie des Groupes Classiques (1955) recoge y sistematiza todo ese material.

La teoría moderna de las formas cuadráticas estudia los pares (V,q) formados por un espacio vectorial V, de dimensión finita, sobre un cuerpo k y una aplicación

$$q: V \longrightarrow k$$

que satisface las siguientes propiedades

i. $q(a.v) = a^2 q(x)$, $a \in k$, $v \in V$

ii. La aplicación $(x,y) \xrightarrow{b} q(x+y) - q(x) - q(y)$ de VxV en K es bilineal.

Decimos que q es una aplicación cuadrática y b es la forma bilineal asociada a q ó a (V,q).

Se sigue de la definición que $b(x,y) = b(y,x)$. Además

$$b(x,x) = 2.q(x)$$

por lo tanto si k es de característica 2, la forma bilineal b es alternada, o sea $b(x,x) = 0$, para todo x en V. En este curso solo consideramos el caso de cuerpos k de característica $\neq 2$, o sea $2=2.1$ es inversible en k. Se sigue que la forma b está unívocamente determinada por q:

$$b(x,y) = \tfrac{1}{2}(q(x+y)-q(x)-q(y))$$

Recíprocamente toda forma bilineal simétrica b sobre V determina una forma cuadrática definiendo

$$q(x) := b(x,x)$$

De esta forma existe una correspondencia biyectiva entre espacios cuadráticos (V,q) y espacios bilineales simétricos (V,b). En nuestro estudio aplicaciones cuadráticas y bilineales conviven en el mismo espacio V. Tendremos siempre un objeto (V,q,b). La idea es que con b hacemos geometría en V y con q hacemos aritmética en k. Es interesante notar que la situación (V,q,b) es una generalización del caso euclídeo donde $V = R^n$, la forma bilineal es

$$b(x,y) = x \cdot y = \Sigma_i \; x_i y_i$$

el producto escalar y la forma cuadrática $q(x) = \|x\|^2$ es el cuadrado de la distancia de x al origen. La geometría euclidea estudia este espacio cuadrático y en nuestra generalización tenemos una geometría para cada cuerpo k y cada espacio cuadrático (V,q). En Teoría de la Relatividad Restringida interesa estudiar el caso $V=\mathbb{R}^4$ notado de la forma cuadrática $q(x) = x_1^2 + x_2^2 + x_3^2 - x_4^2$. En realidad la forma cuadrática es $x_1^2 + x_2^2 + x_3^2 - c^2 t^2$, con c la velocidad de la luz en el vacío. Este espacio se suele llamar espacio de Minkowski. El grupo ortogonal asociado es el llamado grupo de Lorentz. Una buena referencia para estudiar este espacio es, además de libros de Física o Relatividad, la Geometría Superior de N.W. Efimow.

En un espacio cuadrático regular (V,q) (regular, significa que la forma bilineal b asociada es no degenerada, es decir $b(x,y) = 0$, $\forall y \in V \Longrightarrow x = 0$) la totalidad de automorfismos de V que preserva la forma q ó equivalentemente, la forma b es un grupo, el llamado grupo ortogonal de (V,q). Preservar significa que si t es el automorfismo de V, entonces $q(x) = q(t(x))$ ó equivalentemente $b(x,y) = b(t(x),t(y))$. El problema fundamental que aparece es estudiar la estructura de este grupo que se denota por O(V) ó O(q). La expresión matricial de este grupo es la siguiente.
Si $e_1,\ldots,e_n$ es una base de V y $A = [a_{ij}]$ es la matriz simétrica con $a_{ij}=b(e_i,e_j)$ entonces, si $x = x_1e_1+\ldots+x_ne_n$ resulta

$$q(x) = b(x,x) = b(\Sigma_i x_i e_i, \Sigma_j x_j e_j) = \Sigma_{i,j}\ a_{ij} x_i x_j$$

$$= {}^t x.A.x$$

donde x es el vector columna de coordenadas $x_1,\ldots,x_n$.

La condición $q(t(x)) = q(x)$ se traduce en la ecuación matricial

$$^{t}T.A.T = A$$

donde T es una matriz regular. La totalidad de matrices T regulares, con esa propiedad constituye una versión matricial del grupo $O(q)$. Si por ejemplo la matriz A es la matriz identidad, como en el caso euclídeo, el grupo ortogonal está determinado por las matrices T tales que $^{t}T.T = I$, o sea es el grupo ortogonal ordinario.

En 1938, Elié Cartan (Leçons sur la theorie des spineurs) demostró que toda transformación ortogonal de un espacio cuadrático (V,q), sobre el cuerpo k real ó complejo, es expresable como producto de $r \leq \dim(V)$ simetrías con respecto a hiperplanos ortogonales a vectores x con $q(x) \neq 0$. Este resultado fue generalizado por J. Dieudonne para el caso de cuerpos cualesquiera. El teorema se denomina Teorema de Cartan-Dieudonné. Los vectores x de un espacio cuadrático V, tales que $x \neq 0$ y $q(x) = 0$ se denominan vectores isótropos. De otro modo se denominan anisótropos. Una forma cuadrática se dice isótropa si admite algún vector isótropo.

Si $x \in V$ es un vector anisótropo entonces

$$U = \{y \mid b(x,y) = 0\}$$

es un subespacio de dimensión $\dim(V) - 1$ tal que $V = k.x \oplus U$. La simetría respecto de U está dada por

$$S(a) = a - 2\frac{b(a,x)}{q(x)} \cdot x$$

Esta transformación fija al plano U y aplica x en -x. Por lo tanto tiene determinante igual a -1. El Teorema de Cartan-Dieudonné establece que toda transformación ortogonal en V puede obtenerse componiendo simetrías respecto de hiperplanos ortogonales a vectores anisotropos. Dice además que hay una composición que utiliza a lo sumo dim(V) simetrías.

Las transformaciones ortogonales de determinante 1 se denomina el grupo ortogonal especial. Las rotaciones son pues producto de un número par de simetrías. Aquí hay un inmenso material de estudio. Recomendamos el libro de Dieudonné: La Geometrie des Groupes Classiques, Springer-Verlag, 1955 y también el libro de Emil Artin : Geometric Algebra, Interscience.

Mencionemos otro resultado básico fundamental de la teoría, el llamado Teorema de Cancelación de Witt. Sean (V,q), (V',q') espacios cuadráticos isométricos y sean U C V, U' C V' subespacios isométricos. Supongamos que U (y por lo tanto U') es un espacio regular. Si denotamos con $U^{\perp}$ u $U'^{\perp}$ el complemento ortogonal de U en V y u' en V', respectivamente, se tiene que $U^{\perp}$ y $U'^{\perp}$ son isométricos. En símbolos, Teorema de Cancelación de Witt

$$V = U \perp U^{\perp} \simeq V' = V' \perp U'^{\perp} \ , \ U \simeq U' \Longrightarrow U^{\perp} \simeq U'^{\perp}$$

donde $\simeq$ denota isometría de espacios cuadráticos, el exponente $^{\perp}$ denota ortogonal y la escritura $V = U \perp U^{\perp}$ indica suma directa y los subespacios sumandos son ortogonales.

Si (V,q) es un espacio cuadrático regular e isótropo entonces V posee un subespacio de dimensión 2 con una base del tipo e,f, q(e) = q(f) = 0, b(e,f) = 1. Tal subespacio se deno

mina un plano hiperbólico, se denota por H. Todo espacio cuadrático regular V se escribe como una suma ortogonal

$$V = V_1 \perp \ldots \perp V_r \perp V_0$$

donde los subespacios $V_1,\ldots,V_r$ son isométricos a planos hiperbólicos y V_0 es un subespacio anisotropo. Se sigue del teorema de cancelación de Witt que el número r de planos hiperbólicos, así como V_0, están unívocamente determinados. El número r se denomina el índice de Witt de V. Es este un verdadero teorema de estructura de espacios cuadráticos que reduce el estudio de las formas cuadráticas a las anisótropas y a las suma ortogonal de planos hiperbólicos (espacios hiperbólicos).

Otro éxito de la teoría de Witt es haber podido estructurar las clases de isometría de espacios cuadráticos en un anillo, el llamado anillo de Witt que ha sido objeto de mucho estudio en los últimos 30 años. En el libro de T.Y.Lam, The Algebraic Theory of Quadratic Forms, se hace un estudio detallado y completo del anillo de Witt de un cuerpo k. Recientemente ha aparecido W.Scharlau : Quadratic and Hermitian Forms (1985), Springer-Verlag, que consideramos una obra de consulta fundamental.

La teoría de formas cuadráticas es rica también en ingredientes de tipo algebraicos. Es decir es posible asociar a cada forma cuadrática un álgebra. Recordemos que un algebra A sobre un cuerpo k es un espacio vectorial A dotado de un producto asociativo distributivo respecto de la suma y que es compatible con el producto por escalares, o sea

$$k.(u.v) = (k.u).v = u.(k.v) \quad \text{si } k \in k,\ u,v \in V.$$

Sea (V,q) un espacio cuadrático. Entonces está definida un álgebra C(V), la llamada álgebra de Clifford de (V,q) que contiene al subespacio V y tal que

c1. C(V) tiene dimensión 2^n, n=dim(V).

c2. C(V) está generada por V, o sea todo elemento de C(V) es una combinación lineal de 1 y los productos $x_1 \ldots x_r$, con $x_i \in V$, $r \geq 1$

c3. x.x = q(x) para todo x en V.

Si por ejemplo, x,y son vectores en V se tiene

$$xy + yx = (x+y)(x+y) - xx - yy$$
$$= q(x+y) - q(x) - q(y)$$
$$= b(x,y)$$

Por lo tanto si b(x,y) = 0 entonces

$$xy = -yx \ .$$

Si $e_1, \ldots, e_n$ es una base ortogonal de V (o sea $b(e_i,e_j)=0$ si $i \neq j$) el algebra C(V) posee una base formada por 1 y los elementos

$$e_{i_1} \ldots e_{i_r}$$

donde $i_1 < i_2 < \ldots < i_r$. $r \leq \dim(V)$

Un caso particular importante y de interés histórico es el álgebra de cuaterniones que corresponde a la forma cuadrática $q(e_1) = a$, $q(e_2) = b$, $b(e_1,e_2) = 0$.
C(V) tiene dimensión $2^2 = 4$ y una base es

$$1, e_1, e_2, e_1e_2$$

o utilizando la notación clásica

$$1, i, j, ij$$

y satisface

$i^2 = a$, $j^2 = b$, $ij = -ji$. Esta álgebra se denota por $(a,b)_k$ o simplemente (a,b) . La importancia del álgebra de cuaterniones es que en (a,b) conviven dos estructuras, una de álgebra y otra de espacio cuadrático, inducida por la norma. Ocurre el hecho singular que álgebras de cuaterniones sobre el mismo cuerpo son isomorfas (como álgebras) si y sólo si son isométricas (como espacios cuadráticos).

Para el lector interesado en profundizar el estudio de las álgebras de Clifford le sugerimos la lectura de un hermoso texto de C.Chevalley : The Algebraic Theory of Spinors(154).

Como el epílogo de esta introducción queremos destacar la riqueza de este tema que permite desarrollar partes importantes de la Matemática como la aritmética, la geometría, la teoría de grupos, la teoría de álgebras. Constituye un material valioso para implementar un curso avanzado. Afortunadamente hay un texto que servirá de guía para tal curso y es Metric Affine Space, E. Snapper y R.J. Troyer, Academic Press. Tiene además numerosos ejercicios. He aquí pues una propuesta para pensar y difundir buena matemática.

1. INTRODUCCION CLASICA

En estas notas nos referimos a formas cuadráticas sobre un cuerpo k de característica diferente de 2, o sea $1+1 \neq 0$ en k.

Clásicamente una forma cuadrática (f.c) sobre k es un polinomio

$$(1) \qquad f(X_1,\ldots,X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j$$

en n indeterminadas $X_1,\ldots,X_n$, homogéneo de grado 2, con coeficientes en k. La matriz $A = (a_{ij}) \in k^{n\times n}$ se denomina la matriz de f.

Sin pérdida de generalidad podemos suponer que la matriz A es simétrica, es decir, $a_{ij}=a_{ji}$ para todo par i,j. En efecto, basta escribir

$$b_{ij} = \tfrac{1}{2}(a_{ij}+a_{ji})$$

y considerar la forma cuadrática con coeficientes b_{ij}.

Podemos escribir matricialmente

$$f(X) = f(X_1,\ldots,X_n) = {}^tX.A.X$$

donde X un vector columna de coeficientes $X_1,\ldots,X_n$ y ${}^tX$ denota el vector fila traspuesto de X.

Diremos que f es regular si $\det(A) \neq 0$. Sólo nos referiremos a formas regulares.

En la misma forma se asocia a cada matriz simétrica A en forma bilineal simétrica

$$b(X,Y) = {}^{t}X.A.Y$$

donde X,Y son vectores columnas en las 2n indeterminadas $X_1,\ldots,X_n$ e $Y_1,\ldots,Y_n$. La relación entre f y b es

$$f(X) = b(X,X)$$
$$b(X,Y) = \tfrac{1}{2}(f(X+Y) - f(X) - f(Y))$$

Estas relaciones constituyen correspondencias biyectivas entre formas cuadráticas y formas bilineales simétricas.

Una forma cuadrática $f(X) = \Sigma_{i,j}\, a_{ij}X_iX_j$ define por especialización una función

$$q_f : k^n \dashrightarrow k \quad , \quad q_f(x) = \Sigma_{i,j}\, a_{ij}x_ix_j \ .$$

Se ve fácilmente que dadas dos formas cuadráticas f y q

$$q_f = q_g \text{ si y sólo si } f = g.$$

Uno de los problemas típicos de la teoría de formas cuadráticas es el de la representación de elementos de k por formas cuadráticas es el de la representación de elementos de k por formas cuadráticas. Más precisamente, dada una forma cuadrática f se trata de determinar todos los elementos $a \in k$ tales que existen elementos $x_1,\ldots,x_n$ en k con la propiedad

$$f(x_1,\ldots,x_n) = a.$$

En este caso decimos que a es representado por f.

Es particular interesa saber si existen valores $x_1,\ldots x_n$ no todos ceros tales que

$$f(x_1,\ldots,x_n) = 0.$$

En este caso decimos que la forma f es isótropa. Si no es isotropa se dice anisótropa. Por ejemplo si k = Q, la forma $x_1^2 = 2x_2^2$ es anisótropa. En efecto, la isotropía implicaría que $\sqrt{2}$ es racional.

En el manipuleo de formas cuadráticas podemos hacer cambios lineales de coordenadas que permiten simplificar el cálculo. Si P denota una matriz regular, o sea $P \in GL(n,k)$, llamando Y al vector P.X se tiene

$$f((X_1,\ldots,X_n) = {}^tX.A.X = {}^t(P.Y).A.(P.U) = {}^tY.({}^tP.A.P).Y$$
$$= g(Y_1,\ldots,Y_n)$$

y resulta una f.c. de matriz

$$B = {}^tP.A.P$$

Es claro que si $a \in k$ entonces a es representado por f si y sólo si a es representado por g.

Decimos entonces que dos formas cuadráticas f,g de matrices A,B respectivamente, son equivalentes si existe una matriz inversible P tal que las matrices A y B son congruentes, o sea $B = {}^tP.A.P$. En símbolos $f \sim q$. Notar que el carácter simétrico de una matriz no se pierde por la relación de congruencia:

$${}^t({}^tP.A.P) = {}^tp.{}^tp.{}^ttP = {}^tP.A.P$$

Uno de los resultados clásicos en la teoría de f.c. sobre cuerpos de característica $\neq 2$ establece que "toda forma cuadrática es equivalente a una forma cuadrática diagonal",

es decir a una f.c. cuya matriz es una matriz diagonal. Usando la notación anterior, se trataría de encontrar una matriz P inversible tal que

$$f(X_1,\ldots,X_n) = g(Y_1,\ldots,Y_n) \overset{t}{=} Y.{}^tPAP.Y = \sum_{i=1}^{n} a_i.X_i^2 \ .$$

Repasemos este resultado que juega un papel esencial en todo nuestro estudio.

Teorema:

Sea k un cuerpo de característica $\neq 2$. Sea $A = (a_{ij})$ una matriz simétrica. Existe entonces una matriz P regular tal que

$${}^tP.A.P = \mathrm{diag}(a_1,\ldots,a_n) \ .$$

Dem.:

Recordemos que podemos efectuar sobre una matriz las llamadas operaciones de filas y columnas. Esto se logra multiplicando a izquierda y a derecha de la matriz por las llamadas matrices elementales. En general dada una matriz A, el producto P.A. de P a izquierda de A, produce operaciones de filas en A. Es decir resulta una matriz cuyas filas con combinaciones lineales de las filas de A. Y análogamente si efectuamos A.P., resulta una matriz cuyas columnas son combinaciones lineales de las columnas de A. (Es un buen ejercicio para el lector explicitar estas combinaciones lineales de filas y columnas en términos de los coeficientes de P).

El hecho fundamental de estas operaciones es que la operación P.A es exactamente la operación $A.{}^tP$, "mutatis mutandis", cambiando la palabra fila (o filas) por la palabra columna (columnas). Por ejemplo si P es la matriz $I+a.E^{ij}, i\neq j,$

donde I denota la matriz identidad y E^{ij} la matriz de todos ceros salvo en el lugar i,j donde hay un 1. El producto P.A da una matriz con todas las filas iguales a las de A salvo la i-ésima que resulta de sumar a la fila i-ésima de A, a veces la j-ésima fila de A. Por otra parte el producto $A.^tP$ da la matriz cuyas columnas coinciden con las de A salvo la i-ésima que es igual a la i-ésima columa de A sumada de a veces la j-ésima columna de A.

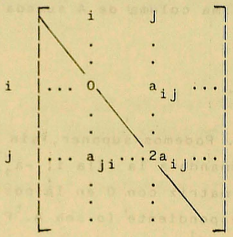
Analicemos dos casos.

i) $a_{ii} \neq 0$ para algún i. Podemos suponer, sin pérdida de generalidad, que $a_{11} \neq 0$. Sumando a la fila i, $-a_{11}^{-1} \cdot a_{i1}$ veces la fila 1, obtenemos una matriz con 0 en la posición i,1. La operación a derecha correspondiente (o sea $A.^tP$) corresponde a sumar a la columna i, $-a_{11}^{-1} \cdot a_{i1}$ veces la columna 1. Dado que $a_{i1} = a_{1i}$, obtenemos una matriz con 0 en los lugares i,1 y 1,i. Repitiendo esta operación para i=2,..., n llegamos a una matriz simétrica, equivalente a la dada con el siguiente aspecto

$$\begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A^+ & \\ 0 & & & \end{bmatrix}$$

donde A^+ es una matriz simétrica en $k^{(n-1)x(n-1)}$. Procediendo entonces inductivamente, podemos concluir con la existencia de una matriz regular P y de una matriz diagonal D tal que $^tP.A.P = D$.

ii) $a_{ii}=0$, para todos los índices $i=1,\ldots,n$. Si $A \neq 0$, es $a_{ij}\neq 0$ para algún par de índices i,j ; $i\neq j$. Sumando la fila i a la fija j y correspondietemente sumando la columna i a la columna j resulta una matriz, equivalente a la dada cuyo coeficiente j,j es $2.a_{ij}\neq 0$, por la hipótesis hecha sobre k :



Estamos en la situación i) y logramos la diagonalización. El Teorema queda entonces completamente demostrado.

De esta manera podemos limitarnos a considerar formas cuadráticas diagonales y para simplificar la notación podemos denotar la f.c. $a_1x_1^2 + \ldots + a_nx_n^2$ con la sucesión

$$<a_1,\ldots,a_n>$$

Así por ejemplos:

$x_1^2 + x_2^2 + \ldots + x_n^2$ se denota por $< 1,1,\ldots,1 >$

$a_1x_1^2 + b_2x_2^2$ se denota por $< a_1,a_2 >$

$x_1^2 + x_2^2 - x_3^2$ se denota por $< 1,1,-1>$

Hay una simplificación ulterior. Sean $k_1,\ldots,k_n \in k^*=k-0$. Entonces dada una forma cuadrática diagonal $\langle a_1,\ldots,a_n\rangle$, si $P = \mathrm{diag}(k_1,\ldots,k_n)$ se tiene

$$ {}^tP.A.P = \mathrm{diag}(k_1^2a_1,\ldots,k_n^2a_n) $$

O sea las formas cuadráticas

$$ \langle a_1,\ldots,a_n\rangle \text{ y } \langle k_1^2a_1,\ldots,k_n^2a_n\rangle $$

son equivalentes.

Ejemplos

1. Sea k = R, el cuerpo de números reales. Dado que para todo número real $a \neq 0$ se verifica que $a = x^2$ ó $a = -x^2$, las formas cuadráticas sobre R están dadas por las sucesiones

   (+) $\quad \langle 1,1,\ldots,1,-1,-1,\ldots,-1\rangle$

   Hay, por otra parte, un teorema de unicidad relativo al número de 1 y al número de -1, que es la conocida Ley de Inercia de Sylvester. Significa que toda forma cuadrática sobre R, es equivalente a una y solo a una forma diagonal del tipo (+).

2. Sea k = C, el cuerpo de los números complejos. Aquí ocurre que todo elemento es un cuadrado. Por lo tanto las formas cuadráticas (regulares) sobre C están dadas por las sucesiones.

   $$ \langle 1,1,\ldots,1\rangle $$

   O sea, toda forma cuadrática sobre C es equivalente a una y sólo una forma cuadrática del tipo $X_1^2 + \ldots + X_n^2$.

3. Sea $a \neq 0$. Entonces dado que estamos en característica $\neq 2$, podemos escribir al elemento a como diferencia de dos cuadrados

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

Como consecuencia se tiene

$$\begin{bmatrix} a & 0 \\ 0 & -a \end{bmatrix} = \begin{bmatrix} x & y \\ y & x \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} x & y \\ y & x \end{bmatrix}$$

y se sigue entonces la equivalencia de las formas cuadráticas

$$x_1^2 - x_2^2 \quad y \quad ax_1^2 - ax_2^2$$

4. Sea $a \neq 0$. Se sigue de la relación

$$\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2a & 0 \\ 0 & 2a \end{bmatrix}$$

y de 3. la equivalencia de las formas cuadráticas

$$ax_1x_2 \ , \ ax_1^2 - ax_2^2 \ , \ x_1^2 - x_2^2 \ ,$$

5. Dejamos a cargo del lector probar que si

$$\begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

es la matriz de una f.c. entonces es ésta equivalente a la forma cuadrática $x_1^2 - x_2^2$ si y sólo si $a.c - b^2 = -t^2$, con $t \neq 0$.

Se observa que al escribir diagonalmente una forma cuadrática sólo interesan los coeficientes módulos cuadrados. Interesa pues conocer el grupo cociente

$$k^{\cdot} / k^{\cdot 2}$$

del grupo multiplicativo k de elementos no nulos de k, por el subgrupo $k^{\cdot 2}$ de $k^{\cdot}$, de elementos que son cuadrados. Para escribir las formas cuadráticas diagonales sobre un cuerpo k es suficiente elegir una familia de representantes en $k^{\cdot}$ del cociente $k^{\cdot}/k^{\cdot 2}$. Por ejemplo si k = R, el cociente $R^{\cdot}/R^{\cdot 2}$ es el grupo cíclico de orden 2. Una familia de representantes es {1,-1}. Las formas cuadráticas diagonales sobre R, quedan determinadas por sucesiones de unos y menos unos.

Si k = C, el cuerpo complejo entonces el grupo cociente $C^{\cdot}/C^{\cdot 2}$ tiene orden 1 dado que en C todo elemento es un cuadrado. Una familia de representantes del grupo cociente es por ejemplo {1}.

Es interesante el caso de un cuerpo finito k. Es bien sabido que en $k^{\cdot}$ la mitad de elementos son cuadrados. Esto es fácil de probar. Se considera la aplicación $k^{\cdot} \longrightarrow k^{\cdot}$ definida por $x \longrightarrow x^2$, que es un morfismo de grupos.

La imagen de esta aplicación es $k^{\cdot 2}$ es la mitad del cardinal de $k^{\cdot}$. Una familia de representantes es {1,a} donde a es un no cuadrado en $k^{\cdot}$. Las formas cuadráticas sobre k que dan entonces descritas por las sucesiones

$$< 1,\ldots,1,\ a,\ldots,a >$$

de 1 y a. Por ejemplo si $k = Z_5$, el cuerpo derestos módulo 5, las formas cuadráticas diagonales son:

$$<1>,\ <3>,\ <1,1>,\ <3,3>,\ <1,3>,\ <1,1,1>,\ <1,1,3>,<1,3,3>.$$

Si $k = Q$, el cuerpo racional, el cociente Q^*/Q^{*2} es un grupo infinito. En efecto, una familia de representantes lo constituye

$$1,-1,\ \pm\ P_1 \cdot P_2 \cdots P_k\ ,\ P_i \neq p_j \text{ si } i \neq j,\ k \in N\ U\ 0$$

donde p_i recorre la totalidad de números primos positivos.

Dada una forma cuadrática regular asociada a una matriz simétrica A,

$$f(X) = {}^tX.A.X$$

podemos definir

$$det(f) = det(A)$$

pero dado que si f es equivalente a la forma ${}^tX.B.X$, se verifica que

$$B = {}^tP.A.P\ ,\ P \text{ regular}$$

y por lo tanto

$$det(B) = det(A).\ det(P)^2$$

debemos definir

$$det(f) \text{ como un elemento del cociente } k^*/k^{*2}.$$

Por ejemplo $det(<a,b>) = a.b\ (mod.k^{*2})$, $det(<a,a>)-1(mod.k^{*2})$... Por abuso de notación se suele omitir $(mod.k^{*2})$ sobreentendiendo que es siempre módulo cuadrados.

Formas equivalentes, ya dijimos, tienen el mismo determinante. Por ejemplo si $<a,b> \simeq <1,-1>$ entonces $a = -b\ (mod.k^{*2})$ dado que $a.b = -1.t^2$, $t \neq 0$. Entonces $a^2.b = -a.t^2$ o sea $a = -b\ (mod\ k^{*2})$.

Nota

Lo precedente plantea un problema de índole aritmética, a saber, dado un cuerpo k, caracterizar el grupo cociente k^*/k^{*2}. Es particular encontrar una familia de representantes en k^*. Es fácil ver que cuando este grupo cociente es finito su cardinal es una potencia de 2. En efecto, todo elemento de k^*/k^{*2} tiene orden 2. Proponemos como ejercicio encontrar para cada n, un cuerpo k tal que k^*/k^{*2} tiene cardinal 2^n. Cuerpos k con la propiedad $k = k^2$ se denominan cuadráticamente cerrados. El cuerpo C es cuadráticamente cerrado. ¿Qué otros ejemplos existen?.

2. ESPACIOS BILINEALES Y CUADRATICOS.

Como en 1. con k denotamos un cuerpo de característica $\neq 2$. Los espacios vectoriales son sobre el cuerpo k y son de dimensión finita.

2.1. Una forma bilineal en un espacio vectorial V es una aplicación

$$b : V \times V \longrightarrow k$$

que satisface

$$b(x+x',y) = b(x,y) + b(x',y)$$
$$b(x,y+y') = b(x,y) + b(x,y')$$
$$b(a.x,y) = a.b(x,y) = b(x,a.y)$$

si $x,x',y,y' \in V$, $a \in k$.

La forma b se dice simétrica si $b(x,y) = b(y,x)$, para todo par $x,y \in V$. El par (V,b) se denomina un espacio bilineal simétrico, o simplemente espacio bilineal.

Sea (V,b) un espacio bilineal. Si escribimos

$$q_b(x) := b(x,x), \quad x \in V$$

resultan las propiedades siguientes

i. $q_b(a.x) = a^2.q_b(x)$

ii. $q_b(x+y) = q_b(x) + q_b(y) + 2b(x,y)$, o sea

$$b(x,y) = \tfrac{1}{2}(q_b(x+y)-q_b(x)-q_b(y))$$

2.2. Una forma cuadrática en un espacio vectorial V es una aplicación

$$q : V \longrightarrow k$$

que satisface

i. $q(a.x) = a^2.q(x)$

ii. La aplicación VxV ---> k definida por

$$(x,y) \longrightarrow q(x+y)-q(x)-q(y)$$

es bilineal.

El par (V,q) se denomina un espacio cuadrático. La forma bilineal

$$b_q(x,y) = \tfrac{1}{2}(q(x+y)-q(x)-q(y))$$

se denomina la forma bilineal asociada a q. Es una forma simétrica. Notar que espacios cuadráticos y bilineales simétricos se corresponden biyectivamente:

$$(V,q) \longrightarrow (V,b_q)$$
$$(V,b) \longrightarrow (V,q_b)$$

Esto hace que podamos identificar espacios bilineales con espacios cuadráticos y recíprocamente. Por ejemplo el concepto de isometría entre espacios cuadráticos o bilineales. Por definición una isometría $(V,q) \longrightarrow V',q')$ de espacios cuadráticos es un morfismo inyectivo $t:V \longrightarrow V$ que es respetuoso de las formas cuadráticas, o sea $q(x) = q'(t(x))$, cualquiera sea $x \in V$. Es claro que se verifica también que $(x\ b_q(x,y)=b_{q'}(t(x),t(y))$ cualesquiera sean x,y en V. Recíprocamente una isometría entre espacios bilineales es una isometría entre los espacios cuasráticos subyacentes.

2.3. Notación matricial. Sea (V,q) un espacio cuadrático. La introducción de bases permite recuperar el esquema clásico de formas cuadráticas. Sea, en efecto $e_1,\ldots,e_n$ una base de V. Definamos $a_{ij}=b(e_i,e_j)$, donde $b = b_q$. Resulta una matriz simétrica $A = (a_{ij})$. Para cada $x \in V$ escribamos x_e el vector columna cuyas coordenadas son las componentes de x respecto de la base $e_1,\ldots,e_n$.

Se tiene, si $x = \Sigma_i x_i e_i$,

$$q(x) = b(x,x)=b(\Sigma_i x_i e_i, \Sigma_j x_j e_j = \Sigma_{i,j} x_i x_j a_{ij} = {}^t x_e . A . x_e .$$

Si $t:V \longrightarrow V$ es una isometría y la matriz de t respecto de la base $e_1,\ldots,e_n$ es P, se tiene

$$q(t(x)) = q(t(\Sigma_i x_i e_i)=q(\Sigma_i x_i t(e_i))=q(\Sigma_i x_i \Sigma_h e_{hi} e_h)$$

$$= q(\Sigma_h(\Sigma_i e_{hi} x_i) e_h) =$$

$$= {}^t(P.x_e).A.(Px_e)$$

$$= {}^t x_e .({}^t P.A.P).x_e$$

y siendo $q(t(x)) = q(x)$ resulta finalmente

$$ {}^{t}P.A.P = A $$

y esto coincide con la noción clásica de equivalencia de formas cuadráticas. podemos decir que dos espacios cuadráticos son isométricos si y solo si matrices simétricas asociadas a los mismos son congruentes.

Si la matriz asociada $A = b(e_i e_j)$ respecto de alguna base es regular, así lo es la matriz asociada a cualquier base de V. En ese caso decimos que el espacio cuadrático es regular. Si (V,q) es un espacio cuadrático regular, la totalidad de isometrías constituye un grupo, el llamado grupo ortogonal de (V,q), o simplemente de q. Se denota por O(q). Es interesante expresar O(q) matricialmente. se trata del subgrupo $O(q) \subset GL(n,K)$ de todas las matrices P tales que

$$ {}^{t}P.A.P = A, $$

donde A denota la matriz de q respecto de alguna base. Si B es la matriz de q respecto de otra base existe una matriz regular Q tal que $B = {}^{t}Q.A.Q$. Por lo tanto si T es una matriz regular

$$ {}^{t}T.B.T = B \Longleftrightarrow {}^{t}T({}^{t}Q.A.Q).T = {}^{t}Q.A.Q \Longleftrightarrow {}^{t}(Q^{-1}.T.Q).A.(Q.T.Q^{-1}) $$

lo cual dice que los distintos grupos ortogonales asociados a distintas matrices de q son todos conjugados y por lo tanto isomorfos.

Notemos que si en particular A es la matriz identidad, el grupo ortogonal es la totalidad de matrices regulares P que satisfacen ${}^{t}P.P = I$, o sea el grupo ortogonal corriente.

Uno de los problemas básicos de la teoría geométrica de formas cuadráticas es estudiar la estructura de los grupos ortogonales y esto forma todo un capítulo del álgebra geométrica. Una referencia obligada para este tema es el libro de J.Dieudonné, La géométrie des groupes classiques, Ergebnisse der Mathematik un ihrer Grenzgebiete, Neue Folge,-Heft 5, Springer, (1955). Citemos también el libro de Emil Artin, Geometric Algebra, Interscience Tracts in Pure and Applied Mathematics, (1957).

2.4. Ortogonalidad.

Como ya señalamos el concepto de espacio bilineal es la generalización del concepto de espacio euclídeo. Podemos entonces repetir alguna nomenclatura en el contexto de espacios bilineales.

Sea (V,q) un espacio cuadrático, $b = b_q$ la forma bilineal asociada.

Def:

Dos vectores x,y en V se dicen ortogonales si $b(x,y)=0$. Escribimos $x \perp y$.

Dado un subconjunto denoto X de V, no vacio se define el ortogonal de X, al conjunto denotado por $X^{\perp}$ definido por la totalidad de vectores de V que son ortogonales a todos los vectores en V. O sea

$$X^{\perp} = \{y \ ! \ b(x,y)=0 \ , \ \forall x \in X\}.$$

Es claro que $X^{\perp}$ es un subespacio de V, además $X \subset Y \Rightarrow Y^{\perp} \subset X^{\perp}$,

El subespacio $V^{\perp}$, ortogonal de V consiste de todos los vectores y tales que

$$b(y,x) = 0, \text{ cualquiera sea } x \in V$$

se denomina el radical de V , se denota por r(V).

Caractericemos ahora los espacios cuadráticos regulares.Se tiene el siguiente Teorema:

Las siguientes condiciones definidas sobre un espacio cuadrático (V,q) son todas equivalentes entre sí.

i. (V,q) es regular
ii. $b(x,y) = 0$, para todo $x \in V$ implica $y = 0$.
iii. $r(V) = 0$,
iv. La aplicación $V \longrightarrow V^*$ (= dual de V) definida por
$v \longrightarrow b(v,)$, con $b(v,)(x) = b(v,x)$,
es un isomorfismo.

La demostración es sencilla, la dejamos como ejercicio para el lector. La propiedad iv. es interesante, dice que la forma b realiza las funcionales lineales de V, o sea dada una funcional lineal $f:V \longrightarrow k$ existe un único $v \in V$ con la propiedad $f(x)= b(v,x)$, cualquiera sea $x \in V$. Esto recuerda a los espacios de Hilbert.

Ejemplo: Sea $V=R^2$ y sea $q:R^2 \longrightarrow R$, la forma cuadrática definida por

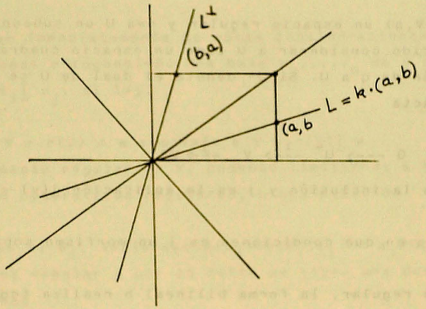
$$f\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = x^2 - y^2$$

Sea $e_1 = (1,0)$, $e_2(0,1)$, la base canónica de R^2. Sea $(a,b) \in V$ y calculemos el ortogonal $\{(a,b)\}^{\perp}$ al vector (a,b). Entonces

$$b(ae_1+be_2, xe_1+ye_2) = ax - by$$

Por lo tanto (x,y) es ortogonal a (a,b) si y sólo si ax=by. Si (a,b) ≠ (0,0), este ortogonal es la recta por origen que pasa por el punto (b,a). Se tiene que

$$\{(a,b)\}^{\perp} = k.(a,b) \text{ si y sólo si } a=b$$



Def.:

Sean $U_1,\ldots,U_m$ subespacios de V. Diremos que V es una suma ortogonal de los subespacios U_i, si:

i. $V = U_1 + \ldots + U_m$ (suma directa ordinaria)

ii. $i \neq j \Rightarrow U_i \perp U_j$

Escribimos $V = U_1 \perp \ldots \perp U_m$.

Si ahora: (V_i,q_i) es una familia finita de espacios cuadráticos se define la suma ortogonal como el espacio cuadrático (V,q) tal que

i. $V = V_1 + \ldots + V_m$

ii. $q(v_i + \ldots + v_m) = q_1(v_1)+\ldots+q_m(v_m)$, si $v_i \in V_i$

En este caso escribimos

$$V = V_1 \perp \ldots \perp V_m$$

Sea (V,q) un espacio regular y sea U un subespacio de V. Tiene sentido considerar a U como un espacio cuadrático por la restricción de q a U. Si U* denota el dual de U se tiene la sucesión exacta

$$0 \longrightarrow U^{\perp} \xrightarrow{i} V \xrightarrow{j} U^*$$

donde i es la inclusión y j es la aplicación $j(v) = b(v,)$.

Veamos en que condiciones es j un morfismo sobre.

a. Si V es regular, la forma bilineal b realiza todas las funcionales de V y en particular las de U. Por razones de dimensión se tiene la relación

(=) $\dim(U) + \dim(U^{\perp}) = \dim(V)$

Como consecuencia de esta relación se tiene la igualdad $U^{\perp\perp} = U$.

b. Si $(U,q!U)$ es regular entonces, obviamente j es un morfismo sobre. En este caso vale (=) y como además $U \cap U^{\perp} = 0$, podemos concluir que

$$V = U \perp U^{\perp}$$

Es importante insistir que, en general, dado un subespacio U de V, la existencia de una descomposición ortogonal

$$V = U \perp W$$

Ocurre si U es un subespacio cuadrático regular. Si el espacio (V,q) es regular podemos afirmar que existe una descomposición ortogonal

$$V = U \perp W$$

si y sólo si U es un subespacio regular.

Se sigue inmediatamente de estas consideraciones la existencia de bases ortogonales. Una base $v_1,\ldots v_n$ de V se dice ortogonal si $v_i \perp v_j$, si $i \neq j$.

Dado que $V = r(V) + w$ equivale a $V = r(V) \perp W$
con W subespacio regular de V, podemos limitarnos a trabajar con espacios cuadráticos regulares, o sea $r(V) = 0$.

Entonces si e_1, satisface $q(e_1)=b(e_1,e_1) = a_1 \neq C$, el subespacio $\langle e_1 \rangle$ es regular y por lo tanto se tiene una descomposición ortogonal

$$V = \langle e_1 \rangle \perp \langle e_1 \rangle^{\perp}$$

Puesto que $\langle e_1 \rangle^{\perp}$ es un subespacio regular, iterando este proceso nos conduce a obtener una base ortogonal $e_1,\ldots,e_n$ con $q(e_i) = a_i$.

La matriz de q respecto de la base $e_1,\ldots,e_n$ es la matriz diagonal $\mathrm{diag}(a_1\ldots,a_n)$.

Esto corresponde a la forma cuadrática diagonal
$a_1x_1^2 +\ldots+ a_nx_n^2$.

Dado que

$$V= \langle e_1 \rangle \perp \ldots \perp \langle e_n \rangle$$

Podemos escribir

$$V = \langle e_1, a_1 \rangle \perp \ldots \perp \langle e_n, a_n \rangle \text{ , o también, por abuso de notación}$$

$$V = \langle a_1 \perp \ldots \perp a_n \rangle = \text{suma ortogonal de espacios cuadráticos unidimensionales.}$$

La notación $\langle a_1, \ldots, a_n \rangle$ usada anteriormente tiene también la significación de una suma ortogonal como acabamos de señalar.

Notemos que si (V,q) es un espacio cuadrático y para algún vector v ocurre que $q(v) = a \neq 0$, entonces existe una diagonalización de q que contiene al coeficiente a. O sea

$$q(v) = a \neq 0, \text{ entonces } q \simeq \langle a, *, \ldots, * \rangle$$

La condición necesaria y suficiente para que, dados $a_1, \ldots, a_r \in k^*$ exista una diagonalización de q:

$$q \simeq \langle a_1, \ldots, a_r, *, \ldots, * \rangle$$

es que estos valores $a_1, \ldots, a_r$ correspondan a los valores de q en r vectores ortogonales entre sí.

2.5. Isotropía. Espacios hiperbólicos.

Def.:

Sea (V,q) un espacio cuadrático. Un elemento $x \in V$ se dice isótropo si $x \neq 0$ y $q(x) = 0$. Un espacio cuadrático si dice isótropo si posee algún vector isótropo. Un subespacio U de V se dice totalmente isótropo si todo vector de U es isótropo. Un espacio cuadrático se dice anisótropo si no posee ningún vector isótropo.

Se denomina plano hiperbólico a todo espacio cuadrático regular de dimensión 2 generado por vectores isótropos. O sea posee una base e,f tal que $q(e) = q(f) = 0$, $b(e,f) \neq -$.

Un espacio cuadrático se dice hiperbólico si es suma ortogonal de planos hiperbólicos. (En Snapper-Troyer se denominan espacios artinianos).

Un plano hiperbólico se denota por H. Un espacio cuadrático de dimensión 2 es un plano hiperbólico si y solo si la matriz de la forma cuadrática respecto de cualquier base tiene determinante $-1.a^2$, con $a \neq 0$. Existe pues, salvo, isometrías un único espacio bidimensional regular isotropo, que responde a la forma cuadrática X^2-Y^2. Un resultado fundamental establece que todo espacio cuadrático regular isótropo posee un plano hiperbólico, o sea

$$V = V_1 \perp V_2 \ , \ V_1 \simeq H.$$

Demostremos esta afirmaciòn. Sea e un vector isótropo de V. Puesto que el espacio es regular existe un vector g tal que $b(a,g) \neq 0$. Sin pérdida de generalidad podemos suponer $b(e,g)=1$. Si $q(g) = 0$, es subespacio generado por e y g es un plano hiperbólico. En general, escribamos $f = g + a.e$, $a \in k$. Se verifica

$$q(f) = q(g) + 2a$$

Eligiendo a de manera que $q(f) = 0$, se tiene $q(e)=q(f)=0$, $b(e,f) = 1$ y la existencia de un plano hiperbólico queda probada. Puesto que dicho plano es un subespacio regular, admite un complemento ortogonal como queríamos probar.

Es claro que reiterando este proceso podemos establecer para cualquier espacio cuadrático regular una descomposición del tipo

$$V = V_1 + \ldots + V_h + V'$$

donde cada V_i es un plano hiperbólico y V' es un subespacio anisótropo. O sea todo; espacio regular es suma ortogonal de un espacio hiperbólico y de un espacio anisótropo. Esos subespacios están unívocamente determinados (según el Teorema de Cancelación de Witt) y se denominan la parte hiperbólica y la parte anisótropa del espacio cuadrático. El número h es consecuentemente un invariante, el llamado índice de Witt de (V,q).

A manera de ejercicio para el lector le encargamos probar que si la forma cuadrática 1,a,b,ab es isótropa entonces es hiperbólica, o sea isométrica a la forma $< 1,-1,1,-1 >$.

2.6. SIMETRIAS O REFLEXIONES. TEOREMA DE CARTAN-DIEUDONNE.

En esta sección damos ejemplos de una familia importante de transformaciones ortogonales de un espacio cuadrático (V,q), las llamadas simetrías (o reflexiones) de V respecto de hiperplanos ortogonales a vectores anisótropos.

Dado un vector anisótropo a V, se tiene la descomposición ortogonal

$$V = k.a \perp H_a \text{ con } H_a = \langle a \rangle^{\perp} = \{ x \mid b(x,a)=0 \}$$

y está definida la simetría respecto del hiperplano H_a en la dirección del vector a. Imitando la situación euclídea se tiene la siguiente expresión para dicha simetría

$$S_a(x) = x - 2\frac{b(x,a)}{q(a)} \cdot a$$

El hecho fundamental de esta transformación es ser un auto - morfismo de V preservador de las formas cuadrática q y bilineal b:

$$q(S_a(x)) = q(x) \ , \ \forall \ x \in V$$

$$b(S_a(x),S_a(y)) = b(x,y), \ \forall \ x,y \in V.$$

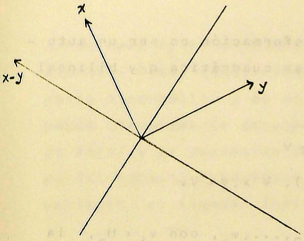
Respecto de una base del tipo $a,v_2,\ldots,v_n$, con $v_i \in H_a$, la matriz de S_a es la matriz diagonal

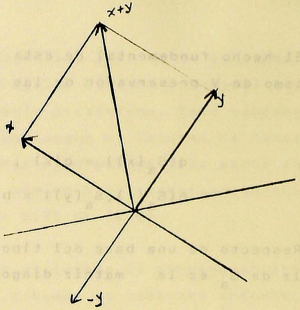
$$\begin{bmatrix} -1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ . & . & \ldots & . \\ . & . & \ldots & 1 \end{bmatrix}$$

Se sigue entonces que $\det(S_a) = -1$. Notar además que $S_a^2 = Id$.

Las simetrías S_a, cuando a recorre los vectores anisótropos de V general el grupo ortogonal de V, o sea toda transformación ortogonal es producto de simétricas. Esto es fácil de probar. Pero hay un resultado no trivial de gran significación, conocido como Teorema de Cartan-Dieudonné, que establece que toda transformación ortogonal de (V,q) puede escribirse como producto de a lo sumo dim(V) simetrías. Por ejemplo si dim(V) = 2, las transformaciones ortogonales son simetrías o producto de dos simetrías, etc...

A manera de ilustración probemos que si (V,q) es un espacio cuadrático y, dados vectores $x,y \in V$ con $0 \neq q(x) = q(y)$ existe una transformación ortogonal t tal que t(x) = y. Un dibujo suguiere qué hacer!





Entonces $q(x+Y)\neq 0$, $S_{x+y}(x) = -y$

$q(x-y)\neq 0$, $S_{x-y}(x) = y$.

En el primer caso componemos S_{x+y} con la transformación ortogonal $-I(x) = -x$ para obtener una isometría que aplica x en y. Habremos probado nuestra afirmación si probamos que $0 = q(x+y) = q(x-y)$ es imposible. En efecto, se tiene

$$0 = -(x+y) = b(x+y,x+y) = 2.(q(x) + b(x,y))$$
$$0 = q(x-y) = b(x-y,x-y) = 2.(q(x) - b(x,y))$$

o sea $4.q(x) = 0$, por tanto $q(x) = 0$, contrario a la hipótesis.

Utilizando este resultado probemos que toda isometría es producto de a los sumo $2n-1$ simetrías de V, siendo $n = \dim(V)$. Si dimensión de $V = 1$, las isometrías son la identidad y $-I_d$. La identidad la interpretamos como $(-I_d)^0$. Sea entonces $\dim V > 1$ y t una isometría de V. Sea x un vector anisótropo. Si $t(x) = y$, por lo visto más arriba existen dos simetrías S_1, S_2 tales que $S_1 S_2 t(x) = x$.

Se tiene la descomposición ortogonal $V = \langle x \rangle \perp \langle x \rangle^{\perp}$ y la isometría $S_1 S_2 t$ fija el subespacio $\langle x \rangle$. Por lo tanto define una isometría en el subespacio ortogonal $\langle x \rangle^{\perp}$. Utilizando la h ipótesis inductiva, sobre $\langle x \rangle^{\perp}$, $S_1 S_2 t$ es producto de a lo sumo $2(n-1)-1$ isometrías : $S_1 S_2 t \mid \langle x \rangle = L_1' \ldots L_h'$, $h \leq 2(n-1)-1$ y donde L_i' son simetrías en $\langle x \rangle^{\perp}$. Cada L_i' se extiende trivialmente a una isometría L_i de V, por $L_i(x) = x$. Se tiene entonces

$$t = S_1 S_2 L_1 \ldots L_h$$

con $h+2 \leq 2n-1$. Es más difícil probar que t puede escribirse como producto de a lo sumo n simetrías.

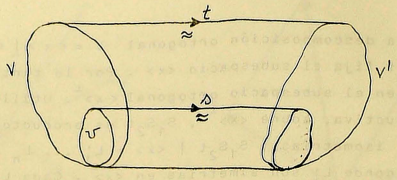
2.7. TEOREMA DE EXTENSION DE WITT.

Teorema (Ernst Witt (1937))

Sean (V,q), (V',q') espacios cuadráticos regulares isométricos.

Entonces todo morfismo métrico inyectivo s : u ---> V' de un subespacio U de V, en V' , se extiende a una isometría de V sobre V'.

En más palabras se tiene una isometría t : V ---> V' . Por otra parte un subespacio U de V se inyecta métricamente en V', s : U ---> V' . El teorema afirma que s se extiende a una isometría de V sobre V'. Un dibujo alegra el espíritu,



De acuerdo con el teorema de extensión de Witt, dados vectores isótropos x,y en V, existe una isometría t tal que (t(x)=y. Más generalmente dados dos subespacios totalmente isotropos maximales son conjugados por O(V) y en particular tienen la misma dimensión.

Una consecuencia fundamental de este Teorema es el llamado Teorema de Cancelación de Witt:

$$V = U \perp U' \simeq V' = W \perp w' \ , \ U \simeq W \Longrightarrow U \simeq W'.$$

En efecto, si en el teorema el subespacio U admite un complemento ortogonal U', la extensión $\bar{s} : V \dashrightarrow V'$ de $s : U \longrightarrow V'$, aplica el ortogonal de U en el ortogonal de s(U), o sea aplica isométricamente U' sobre W', que es la contensión del Teorema de Cancelación.

Este Teorema de Cancelación se demuestra también elementalmente con lo desarrollado en la sección anterior y lo hacemos. Razonando inductivamente es suficiente referirse al caso $U = \langle e \rangle$, $w = \langle e' \rangle$, dado que (U es regular) $U = \langle e_1 \rangle \perp \ldots \perp \langle e_h \rangle$. La isometría $t:V \longrightarrow V'$ aplica e en un vector $f \in V'$, $t(e) = f$.

Pero se tiene q'(f) = q(e) = q'(e') , pues <e> y <e'> son isométricos. Por lo tanto existe una transformación ortogonal g de (V',q') tal que g(f) = e'. La isometría composición g.t : V---> V' satisface g.t(e) = e' . Aplica el ortogonal U' de <e> en el ortogonal V' de <e'>, y esto es lo que queríamos probar. El teorema de cancelación tiene una versión matricial interesante. Sean las matrices simétricas de bloques

$$M = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \qquad N = \begin{bmatrix} A' & 0 \\ 0 & B' \end{bmatrix} \qquad A,A' \in k^{n\times n},\ B,B' \in k^{m\times m}$$

Entonces se verifica que

M congruente con N

===> B congruente con B'

A congruente con A'

Es decir si existe una matriz inversible Q con ${}^tQ.M.Q = N$, una matriz inversible T con ${}^tT.A.T = A'$, entonces existe una matriz inversible R tal que ${}^tR.B.R = 0'$.

3.- ALGEBRA DE CUATERNIONES.

Como dijeramos en la Introducción, la teoría de formas cuadráticas es rica también en ingredientes de tipo algebraico. Las álgebras de cuaterniones son espacios cuadráticos de dimensión 4 que poseen un producto de vectores. Precisemos esta afirmación. Dado un espacio vectorial A sobre un cuerpo k decimos que sobre A hay una estructura de álgebra sobre k o de k-álgebra si existe un producto en A

$$A\times A \dashrightarrow A\ ,\ x,y \dashrightarrow x.y$$

tal que el mismo es distributivo respecto de la suma en A y es compatible con los escalares en el sentido siguiente

(1) $\quad k.(x,y) = (k.x).y = x.(k.y)$ si $k \in k$, $x, y \in A$

También pedimos la existencia en A de un elemento neutro que denotamos con 1

$$1.x = x.1 = x \quad , \quad x \in A.$$

Decimos que A es un álgebra de división si para todo $x \in A$, $x \neq 0$ existe $y \in A$ tal que $x.y = y.x = 1$.

En un álgebra A conviven 3 operaciones: + , . y producto por escalar, tales que

<A,+,.> es un anillo con elemento neutro

<A,+, producto por escalar> es un espacio vectorial

(1) vincula el producto . con el producto por escalares.

El anillo de polinomios $k[X]$ en una indeterminada ó $k[X_1, \ldots, X_n]$ es un ejemplo de álgebra sobre k : el álgebra de polinomios. La totalidad $M_n(k)$ de matrices de nxn con coeficientes en k es otro ejemplo : el álgebra de matrices.

Si A es un álgebra sobre k de dimensión finita (como espacio vectorial sobre k) y $e_1, \ldots, e_n$ es una base de A, entonces para x,y en A, $x = \Sigma x_i e_i$, $y = \Sigma y_i e_i$ $\quad x_i, y_i \in k$ entonces

$$x.y = \Sigma_{i,j} (x_i y_j)(e_i . e_j)$$

Por lo tanto el producto queda completamente determinado conociendo los productos basales $e_i.e_j$. La colección de estos productos constituye la tabla de multiplicación del álgebra. Por ejemplo, los complejos C pueden considerarse como un álgebra sobre el cuerpo real R. Usando la base 1,i la multiplicación en C queda determinada por la tabla

.	1	i
1	1	i
i	i	-1

Notemos que en la teoría de álgebras no se pide en general que el producto sea asociativo, es decir satisfaga $x.(y,z) = (x.y).z$ si $x,y,z \in A$. Cuando esto es así decimos que el álgebra es asociativa. Es este el caso que nos interesa considerar aquí, pero existen ejemplos muy importantes de álgebras no asociativas. Las llamadas álgebras de lie (Sophus Lie) satisfacen la identidad (de Jacobi) :

$$x.(y.z) + y.(z.x) + z.(x.y) = 0.$$

3.1. ALGEBRA DE CUATERNIONES

Sea H un espacio vectorial real de dimensión 4, por ejemplo $A = R^4$.

Sea una base de H, que por razones que se verán en seguida, denotamos con

$$1 , i , j , k$$

Para definir sobre H una estructura de álgebra es suficien - te fijar una tabla de multiplicación. Este problema fue considerado por el matemático irlandés Sir William Rowan Hamilton (1805-1865). El "descubrimiento" de los cuaterniones por Hamilton es realmente fascinante en su faz histórica. Hamilton trató de ex - tender la estructura de álgebra en $C = R^2$ a dimensiones mayores R^3, R^4. El plan de Hamilton era definir un producto como se hace en R^2, preservando además la famosa propiedad multiplicativa de la distancia.

$$(a^2 + b^2).(c^2 + d^2) = (ac-bd)^2 + (ad + bc)^2$$

El primer intento fue hecho en R^3, se trataba de multiplicar tripletes. Gastó mucho tiempo Hamilton tratando de descubrir el "producto" de tripletes. En esta preocupación parece ser que involucró a toda su familia. Se cuenta que todas las mañanas al bajar a tomar el desayuno su hijo le preguntaba : Papá,¿puedes multiplicar tripletes?. Con tristeza inclinaba la cabeza para decir "No, pude sumarlos y restarlos solamente". El plan era tratar de definir un producto en los elementos

$$1 , i , j$$

tal de satisfacer la identidad de cuadrados que dimos más arriba.

Cuenta Hamilton que el 16 de octubre de 1843 caminando con su esposa a lo largo del Canal Real, yendo a presidir una reu - nión de la Academia Real Irlandesa sintió que un circuito eléc - trico se cerró y una chispa iluminó su mente. El resultado fue el de considerar 4 vectores en lugar de tres y la tabla de multiplicación:

$$i^2 = j^2 = k^2 = -1 \qquad (2)$$

(2) $i.j = k\ ,\ j.k = i,\ \ k.i = j$

$j.i = -k,\ k.j = -i\ ,\ i.k = -j$

Es este el nacimiento de los cuaterniones (de Hamilton). Son éstos los vectores

$$x = x_1.1 + x_2.i + x_3.j + x_4.k \qquad x_i \in R.$$

El producto de cuaterniones se efectúa por medio de la propiedad distributiva y la tabla (2). REsulta un álgebra asociativa con identidad $1 = 1.1 + 0.i + 0.j + 0.k$. El estudio de los cuaterniones prosigue como se hace con los complejos. Se define el conjugado $\bar{x}$ de x:

$$\bar{x} = x_1.1 - x_2.i - x_3.j - x_4.k$$

Se verifica que

$$x.\bar{x} = (x_1^2+x_2^2+x_3^2+x_4^2).1 + 0.i + 0.j + 0.k$$

Es costubre identificar los cuaterniones $a.1 + 0.i + 0.j + 0.k$ con $a.1 = a$, o sea identificando a R con los cuaterniones del tipo a.1. Dichos cuaterniones se denominan escalares, en cambio los que tienen la primer componente nula $x_1 = 0$ se denominan cuaterniones puros.

El valor

$$N(x) := x.\bar{x} = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

que es un escalar, se denomina la norma de x. La norma puede considerarse entonces como una aplicación $N:H \longrightarrow R$ y es claramente una aplicación cuadrática:

$$N(x+y) - N(x) - N(y) = \tfrac{1}{2}(x.\bar{y} + y.\bar{x})$$

es la aplicación bilineal asociada.

La norma es una función multiplicativa : $N(x.y) = N(x).N(y)$ y esta es la relación precisamente que buscaba Hamilton. Esta relación dice que suma de 4 cuadrados por suma de cuatro cuadrados es igual a suma de 4 cuadrados. Efectuando el producto se obtiene la identidad numérica.

El hecho notable del álgebra de Hamilton es ser un álgebra de división. Esto es consecuencia de la anisotropía de la forma cuadrática N. En efecto, notemos que tratándose del cuerpo real $N(x) = 0$ si y sólo si $x = 0$. Además, de $N(x) = x.\bar{x}$ se sigue, si $N(x) \neq 0$, que $1 = x.\frac{\bar{x}}{N(x)} = \frac{x}{N(x)}.x$, o sea x es inversible. El álgebra de Hamilton es el primer ejemplo conocido de álgebra de división no conmutativa. Pasemos a estudiar álgebras de cuaterniones en general. Sean $a,b \in K^*$. Definimos el álgebra de cuaterniones asociada al par a,b, que denotamos con $(a,b)_K$ ó simplemente (a,b) como el álgebra de dimensión 4, con base 1,i,j,k y la tabla de multiplicación

$$i^2 = a \ , \ j^2 = b, \ i.j = -j.i = k \tag{3}$$

El álgebra de Hamilton es entonces $H = (-1,-1)_R$.

Ejemplo: El álgebra de matrices $M_2(k)$ es un álgebra de cuaterniones de tipo (1,a), con a $\in k$. En efecto, basta tomar

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad i = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad j = \begin{bmatrix} 0 & a \\ 1 & 0 \end{bmatrix}$$

y se verifica fácilmente que responde a la tabla (3).

La forma cuadrática norma, asociada a $(a,b)_k$ es $N_{(a,b)}(x) = N(x) = x.\bar{x} = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2$.

O sea, es la forma diagonal $<1,-a,-b,ab>$. En el caso particular de $(1,a)$ la forma cuadrática es $<1,-1,a,-a> \simeq <1,-1,1,-1>$, un espacio hiperbólico.

Por el mismo razonamiento anterior el álgebra (a,b) es de división si y sólo si la forma cuadrática N es anisótropa. He aquí un hecho relevante, la condición algebraica de ser de división está dada por una condición aritmética, la anisotropía de una forma cuadrática. Por ejemplo si k es un cuerpo finito, es bien sabido que toda forma cuadrática de dimensión mayor que 2 es isótropa. Se sigue entonces que sobre un cuerpo finito k no hay álgebra de cuaterniones de divisón. Así no más!. El hecho más relevante es que la estructura cuadrática de (a,b) determina la estructura algebraica (a,b) y recíprocamente. Notemos que dadas dos álgebras A,B sobre un cuerpo k, un isomorfismo de A y B es una aplicación f: A ---> B que respeta todas las operaciones definidas en A (y en B), o sea f es una transformación lineal, f es multiplicativa : $f(x.y) = f(x).f(y)$, $f(1) = 1$ y además f es una biyección. Escribamos entonces $A \simeq B$.

Sobre (a,b) conviven entonces dos estructuras: una algebraica y otra cuadrática. El Teorema fundamental establece que

$$(a,b)_k \simeq (c,d)_k \quad \text{si y solo si} \quad N_{(a,b)} \simeq N_{(c,d)}$$

o sea isomorfismo de álgebras es equivalente a isometría de espacios cuadráticos. La forma cuadrática norma es, en el caso

(a,b) , $N \simeq \langle 1,-a,-b,ab\rangle$.

Notemos que si $\langle 1, -a, -b, ab\rangle$ es isotropa entonces pode - mos ver que

$$\langle 1, -a, -b, ab\rangle \simeq \langle 1, -1,1,-1\rangle$$

o sea es un espacio hiperbólico. Hay pues una única forma norma que sea isótropa y esta es el espacio hiperbólico $\langle 1,-1,1,-1\rangle$. Dado que el álgebra de cuaterniones $M_2(k) = (1,a)$ tiene forma norma $\langle 1,-1,1,-1\rangle$ se sigue el hecho importante siguiente: Un álgebra de cuaterniones es, de división o de otro modo isomorfa al álgebra de matrices $M_2(k)$. En el caso real, la única forma anisótropa del tipo $\langle 1,-1,-b,ab\rangle$ es la forma $\langle 1,1,1,1\rangle$. Como consecuencia se sigue que la única álgebra de cuaterniones de división sobre el cuerpo R es el álgebra de Hamilton.

Ejemplo:

Sobre el cuerpo Q de números racionales hay infinitas álge - bras de cuaterniones, de divisón, no isomorfas entre sí. Sean p y q dos números primos positivos de la forma 4m+3, $p \neq q$. Afirmamos que las álgebras $(-1,-p)$ y $(-1,-q)$ no son isomorfas. En efecto, de serlo se tendría la isometrías de las normas

$$\langle 1,1,p,p\rangle \simeq \langle 1,1,p,p\rangle \simeq 1,1,q,q$$

Utilizando el Teorema de Cancelación de Witt se seguiría la isometría $\langle P,P\rangle \simeq \langle q,q\rangle$. Por lo tanto podemos escribir $p = q.(r^2+s^2)$ en Q. Eliminando denominadores se tendría $m^2.p = q.(n^2+t^2)$ en Z. Por una propiedad de los primos de la for - ma 4m+3, p divide a n^2+t^2 implica que p divide a n y p divide a t. Por lo tanto el miembro derecho es divisible por una poten - cia par del primo p, mientras que el miembro de la izquierda es

divisible por una potencia impar de p. Contradicción. Se sigue que las álgebras dadas no son isomorfas. La clasificación de las álgebras de cuaterniones sobre Q requiere nociones avanzadas de teoría de números. Es un problema aritmético, en esencia.

3.2. ESTRUCTURA BILINEAL DEL ALGEBRA DE CUATERNIONES.

Sea A = (a,b) un álgebra de cuaterniones sobre el cuerpo k. La forma bilineal asociada a la norma es

$$b(x,y) = \tfrac{1}{2} \ (\ x.\bar{y} + y.\bar{x} \ )$$

Por lo tanto

$$x \perp y \text{ si y sólo si } x.\bar{y} = -y.\bar{x}.$$

Recordemos que si x es un cuaternión puro entonces $\bar{x} = -x$, por lo tanto dos cuaterniones puros s,y conmutan si y sólo si x.y = -y.x . Se sigue que la base 1,i,j,k es una base ortogonal. Por lo tanto

$$A = \langle 1 \rangle \perp \langle i \rangle \perp \langle j \rangle \perp \langle k \rangle \text{ , suma ortogonal}$$

Sea $A^0 = (a,b)^0$ el subespacio de cuaterniones puros de (a,b). Nos interesa estudiar el grupo ortogonal de (a,b) y de $(a,b)^0$. Notar que si se trata del álgebra de Hamilton se trata de los grupos ortogonales $O(R^4)$ y $O(R^3)$ respectivamente.

Sea q un vector anisótropo. La simetría S_q está dada por

$$S_q(h) := h - \frac{q.\bar{h} + h.\bar{q}}{N(q)} \ . \ q = - \ q.\bar{h}.\bar{q}^{-1}$$

Si q y h están en A^0 entonces la simetría toma la forma

$$S_q(h) = -q.h.q^{-1}.$$

Por lo tanto el grupo ortogonal de A^0 está generado por las simetrías precedentes. El producto de dos tales simetrías S_q, S_p está dada por

(4) $$S_q S_p(h) = qp.h.(qp)^{-1}$$

Sea $y \in A$ un elemento inversible. Es bien sabido que la aplicación $A \xrightarrow{c_y} A$ definida por $c_y(x) = y.x.y^{-1}$ es un automorfismo de álgebras:

$$c_y(x.v) = y.xv.y^{-1} = y.x.y^{-1}.y.v.y^{-1} = c_y(x).c_y(v).$$

Es además una isometría dado que

$$N(c_y(x)) = N(y.x.y^{-1}) = N(y).N(x).N(v)^{-1} = N(x).$$

El automorfismo c_y fija $<1>$ y siendo una isometría aplica A^0 sobre A^0. Por lo tanto estudiamos $O(A^0)$ utilizando estos automorfismos c_y. Usando (4) se puede ver que los c_y, cuando y recorre los vectores inversibles de A, general el grupo $SO(A^0)$ de rotaciones de A^0. En forma precisa se tiene la sucesión exacta de grupos

(5) $$1 \longrightarrow k^* \longrightarrow U \xrightarrow{c} S)(A^0) \longrightarrow 1$$

Veamos algunas secuencias de esta sucesión exacta.

Sea A el álgebra de matrices, cuya norma es $<1,-1,1,-1>$. El espacio A^0 tiene la forma cuadrática $<1,-1,-1>$. Por lo tanto

dado que U corresponde a GL(2,k)

$$SO(<1,-1,-1>) = GL(2,k)/k^* = PGL(2,k)$$

Si k=R y consideramos el álgebra de cuaterniones de Hamilton, identificamos H con las matrices complejas

$$\begin{bmatrix} z & -\bar{w} \\ w & \bar{z} \end{bmatrix}$$

escribiendo $x_1.1 + x_2.i + x_3.j + x_4.k = (x_1 + x_2.i) + (x_3 + x_4.i)j =$
$= z + w.j.$

En la sucesión exacta (5) podemos reemplazar U por

$$H^1 = \{ x \mid N(x) = 1 \}.$$

Resulta la sucesión exacta

$$1 \longrightarrow \{\pm 1\} \longrightarrow H^1 \xrightarrow{c} SO(A^0) \longrightarrow 1$$

Puesto que $H^1 = SU(2,C)$ según la identificación matricial mencionada, resulta el isomorfismo

$$SU(2,C)/\{1\} = SO(3,R).$$

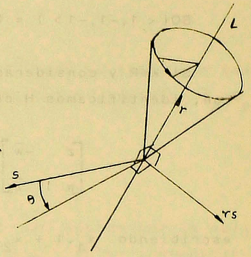
El morfismo c admite en este caso una traducción geométrica transparente. En efecto, sea $t \in SO(A^0) = SO(R^3)$ una transformación ortogonal de determinante igual a 1. Es bien sabido que esta transformación fija una recta L y rota el plano ortogonal a L en un ángulo θ, en sentido contrario a las agujas del reloj (que no sea de cuarzo). Veamos como realizar esta ro

tación con un $y \in H^1$, o sea $c(y) = t$. Sea r un vector unitario en la dirección de L. El vector r lo pensamos como un cuaternión puro y escribimos

$$y = \cos \frac{\theta}{2} + \operatorname{sen} \frac{\theta}{2} \cdot r$$

es claro que $N(y) = 1$

$$y^{-1} = \cos \frac{\theta}{2} - \operatorname{sen} \frac{\theta}{2} \cdot r$$



Sea s un vector unitario en A^0 ortogonal a r. Es fácil ver que los vectores r, s, rs forman una base ortonormal de A^0. Calculando c(y) sobre esta base resulta

$$c(y)(r) = r$$
$$c(y)(s) = \cos \theta . s + \operatorname{sen} \theta . rs$$
$$c(y)(rs) = -\operatorname{sen} \theta . s + \cos \theta . rs$$

que muestra bien que c(y) coincide con la transformación t.

A manera de consulta bibliográfica de esta sección recomendamos un artículo de H.S.M. Coxeter : "Quaternions and reflexions", American Mathematical Monthly 53, 136-146,(1946), J.O. Araujo y E.R. Gentile: Grupos generados por reflexiones, VI Seminario Nacional de Matemática, Vaquerías, Publicación de la Facultad de Matemática, Astronomía y Física de la Universidad Nacional de Córdoba (1982), Patrick Du Val: Homographies, Quaternions and Rotations, Oxford Mathematical Monographs (1964), N. Bourbaki, Algebra, Chapitre IX, Formes sesquilineaires et formes cuadratiques, este libro es interesante por la cantidad de ejercicios, fuente de temas para investigar y profundizar,

pensamos que este libro habría que redescubrirlo, nadie le ha prestado la suficiente atención.