CLASIFICACION DE MATRICES SIMETRICAS CONGRUENTES, DEFINIDAS SOBRE UN CUERPO FINITO

por

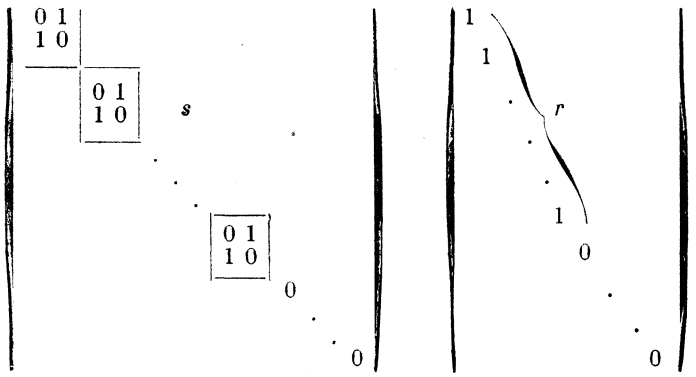
FELIPE MATEOS MATEOS (*)

INTRODUCCION

El presente trabajo consiste en dar una nueva demostración más elemental y con menos aparato algebraico, que la dada en el Lam «The Algebraic Theory of quadratic forms» Benjamín 1973, sobre clasificación de formas cuadráticas sobre un cuerpo finito.

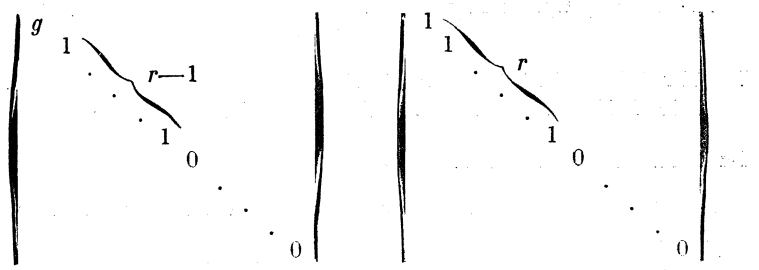
El conjunto de las matrices simétricas congruentes se descompone en dos clases de equivalencia, que tienen los siguientes representantes canónicos:

II-*a*) Si el cuerpo K es de característica dos



(*) Facultad de Matemáticas. Universidad de Sevilla.

II-*b*) Si el cuerpo K es finito de característica distinta de dos.



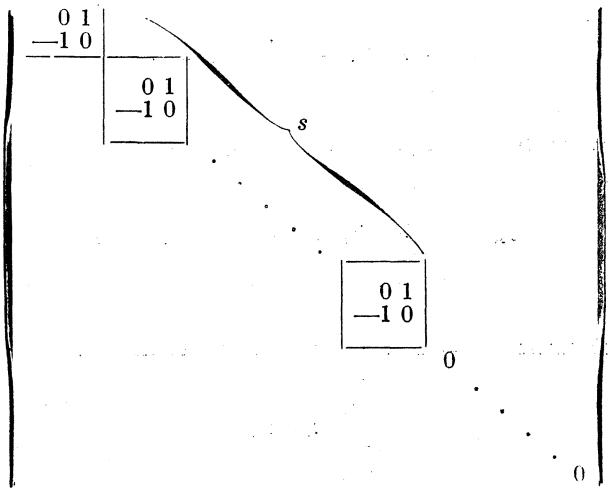
donde *g* es un generador del grupo multiplicativo del cuerpo K.

I. Teoremas sobre congruencia de matrices simétricas definidas sobre un cuerpo cualquiera y que sirven de base para lo que se va a demostrar.

T-I-1. Si una matriz A es simétrica, todas las congruentes con ella también lo son.

T-I-2. Todas las matrices simétricas congruentes entre sí tienen el mismo rango.

T-I-3. Toda matriz hemisimétrica es congruente con una matriz de la forma:



T-I-4. Toda matriz simétrica no hemisimétrica es congruente con una matriz diagonal.

T-I-5. En todo cuerpo algebraicamente cerrado, son congruentes todas las matrices que tienen el mismo rango.

T-I-6. En el cuerpo de los números reales, la condición necesaria

y suficiente para que dos matrices simétricas sean congruentes, es que tengan el mismo rango y la misma signatura.

T-I-7. El grupo multiplicativo de un cuerpo finito K es cíclico.

II. CLASIFICACION DE MATRICES SIMETRICAS CONGRUENTES DEFINIDAS SOBRE UN CUERPO FINITO K

II-*a*) El cuerpo K es de caracteristica 2.

En un cuerpo de característica dos, las matrices simétricas pueden ser también hemisimétricas.

Teorema II-1. En un cuerpo de característica dos, toda matriz congruente con una matriz hemisimétrica es hemisimétrica.

Sean

$$A = (a_{ij}) \quad i, j = 1, 2, 3 \ldots n \ , \ a_{ij} = a_{ji}$$
$$T = (t_{hk}) \quad h, k = 1, 2, 3 \ldots n \ , \ |T| \neq 0$$

Si B es congruente con A, se verifica: B = T A T′, es decir,

$$(b_{rs}) = (t_{ri})\,(a_{ij})\,(t_{js}) = \sum_{i,\,j=1}^{n} t_{ri}\, a_{ij}\, t_{sj} \quad r, s = 1, \ldots n$$

Los elementos de la diagonal principal de esta matriz son:

$$r = s \quad b_{ss} = \sum_{j,\,i=1}^{n} t_{si}\, a_{ij}\, t_{sj}$$

estos términos se descomponen en dos tipos de sumandos, o sea:

$$b_{ss} = \sum_{i,\,j=1}^{n} t^2_{sj}\, a_{jj} + \sum_{\substack{i,\,j=1 \\ i \neq j}}^{n} t_{si}\, a_{ij}\, t_{sj}$$

Pero al variar $i, j = 1, 2, \ldots n$, si existe el término

$$\sum_{j=1}^{n} t_{sm}\, a_{mj}\, t_{ij}$$

cuando $i = m$, también existe el

$$\sum_{i=1}^{n} t_{si}\, a_{im}\, t_{sm}$$

para $j = m$, que es igual al anterior; por consiguiente, su suma se anula por el cuerpo de característica dos. Quedando, por tanto,

$$b_{ss} = \sum_{j=1}^{n} t^2_{sj}\, a_{jj}$$

resultando $b_{ss} = 0$, siempre que $a_{ij} = 0$, es decir, si A es hemisimétrica.

Teorema contrario.—Si A no es hemisimétrica, tampoco lo es B. Pues si B fuera hemisimétrica, $b_{ss} = 0$, lo que implica que:

$$\sum_{j=1}^{n} t^2_{sj}\, a_{jj} = 0$$

sistema homogéneo incompatible, debido a que $|t^2_{sj}| \neq 0$, ya que, por hipótesis, $|t_{sj}| \neq 0$.

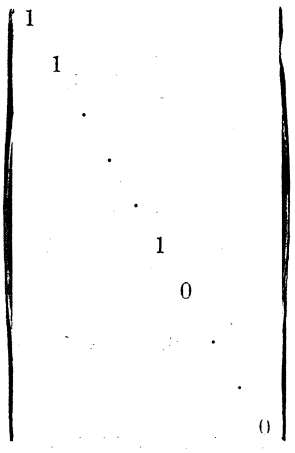
Puesto que $|t_{sj}| \neq 0$ implica que $|t^2_{sj}| \neq 0$ si el cuerpo es de característica dos. Ya que, en efecto,

$$|t_{sj}|^2 = (\Sigma\, t_{1j_1} \cdot t_{2j_2} \ldots t_{nj_n})^2 = \Sigma\, t^2_{1j_1} \cdot t^2_{2j_2} \ldots t^2_{nj_n} = |t^2_{sj}|$$

Corolario del teorema I-3. Si el cuerpo es de característica dos, el opuesto del 1 es el 1, y se tiene, por tanto, que las matrices simétricas y hemisimétricas de rango $2s$ son todas congruentes a una matriz del tipo:

$$\begin{pmatrix} \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} & & & & \\ & \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} & & & \\ & & \ddots & & \\ & & & \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} & \\ & & & & \begin{array}{ccc} 0 & & \\ & 0 & \\ & & \ddots \end{array} \\ & & & & 0 \end{pmatrix}$$

y teniendo en cuenta el teorema I-4, toda matriz simétrica no hemisimétrica es congruente con una matriz del tipo:

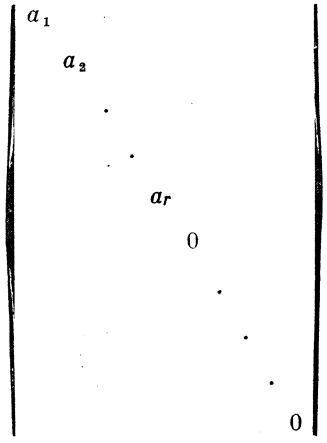


II-*b*) El cuerpo K es de caracteristica distinta de dos.

Cuando el cuerpo K es de característica $p \neq 2$, si g es un generador del grupo multiplicativo de K, todos sus elementos pueden escribirse de la forma:

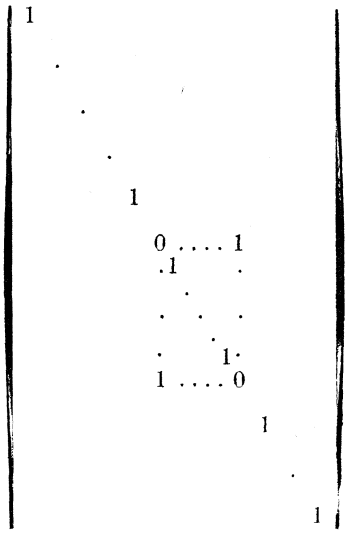
$$g, g^2, g^3, \ldots . gp^n - 1 = 1$$

Teniendo en cuenta el teorema I-4, el problema de clasificar las matrices simétricas congruentes se reduce al estudio de las matrices diagonales de la forma:



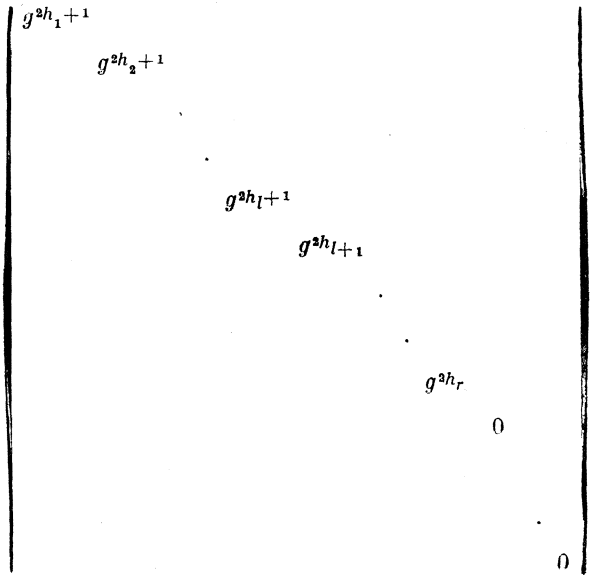
donde sus elementos no nulos son potencias del generador g. Siendo estas potencias de exponente par o impar.

Es posible suponer ordenadas las potencias de la diagonal; primero, las de exponente impar, y después, las de exponente par; pues ello equivale a multiplicar la matriz A por una matriz de la forma:

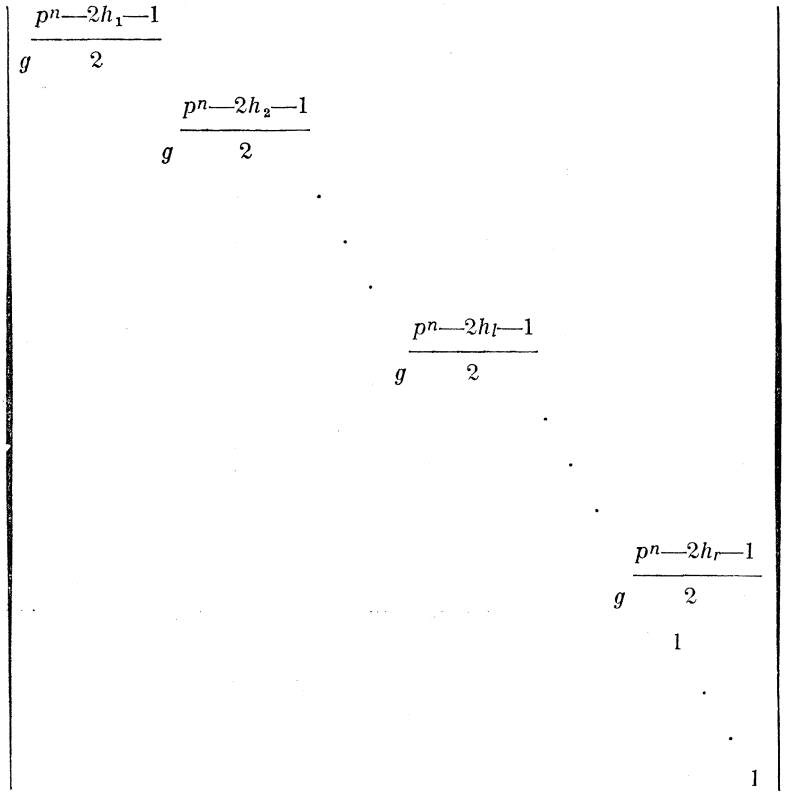


por la izquierda y por la derecha, con lo que resulta otra matriz congruente.

Podemos suponer la matriz A de la forma:



que, multiplicándola por la izquierda y por la derecha por la matriz:



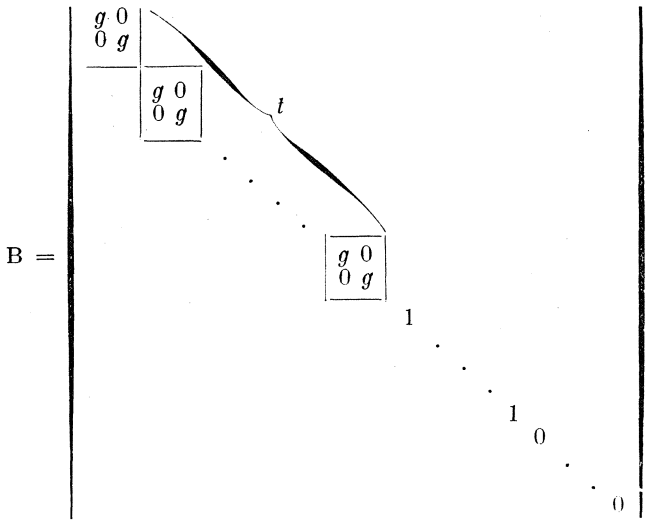
resulta la matriz

$$B = \begin{vmatrix} g & & & & & & \\ & g & & & & & \\ & & l & & & & \\ & & & g & & & \\ & & & & 1 & & \\ & & & & & r-l & \\ & & & & & & 1 \\ & & & & & & & 0 \\ & & & & & & & & \ddots \\ & & & & & & & & & 0 \end{vmatrix}$$

donde l, el número de g, puede ser par o impar.

a) *Supongamos que* $1 = 2t$ *es par.*

Podemos descomponer la matriz B de la forma:



Teorema II-2. La matriz

$$\begin{pmatrix} g & 0 \\ 0 & g \end{pmatrix}$$

es congruente con

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

En efecto:

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

plantea el sistema de ecuaciones:

$$\begin{cases} a^2 + b^2 = g \\ c^2 + d^2 = g \\ ac + bd = 0 \end{cases}$$

que nos da la matriz multiplicadora

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

para lo que es necesario demostrar que el generador del grupo se puede descomponer en suma de dos cuadrados.

La demostración de esta proposición se reduce a probar que una potencia de exponente impar del generador es descomponible siempre en suma de dos cuadrados. Es decir: si $g^{2h+1} = a^2 + b^2$ entonces, multiplicando la igualdad anterior por gp^{n-1-2h} tenemos $g^{2h+1+p^{n-1-2h}} = a^2 \cdot gp^{n-1-2h} + b^2 \cdot gp^{n-1-2h}$ quedando

$$g = \left(a\, g\, \frac{p^n - 1}{2} - h\right)^2 + \left(g\, b\, \frac{p^n - 1}{2} - h\right)^2$$

Veamos ahora que una potencia de exponente impar del generador es siempre suma de dos cuadrados.

Es decir, que $g^{2n+1} = g^{2h} + g^{2k}$, o lo que es igual, $g^{2(m-k)+1} = 1 + g^{2(h-k)}$, y por tanto equivale a ver que existen dos potencias de g de distinta paridad que se diferencian en una unidad.

En efecto, supongamos que no fuera cierto, sabemos que en el grupo multiplicativo hay

$$\frac{p^n - 1}{2}$$

potencias pares y, por otra parte, resultaría que sumando a $gp^{n-1} = 1$, potencia par, sucesivamente una unidad, tendríamos $1,\ 1 + 1,\ 1 + 1 + 1, \ldots, \overbrace{1 + 1 + \ldots + 1}^{p} = 0$, $p - 1$ potencias pares y el cero; tomando otra potencia par distinta de éstas g^{2h} y sumándole, sucesivamente 1, tenemos: $g^{2h} + 1,\ g^{2h} + 1 + 1, \ldots, \overbrace{g^{2h} + 1 + 1 + \ldots + 1}^{p} = g^{2h}$, otras p potencias pares, con lo que tendríamos $p + p - 1$. Si estas son todas las potencias pares, se cumplirá

$$2p - 1 = \frac{p^n - 1}{2}$$

cosa imposible.

Si no estuvieran todas las potencias pares, habría otra g^{2s} a partir de la cual obtendríamos otras p potencias pares, y reiterando k veces el procedimiento llegaríamos a

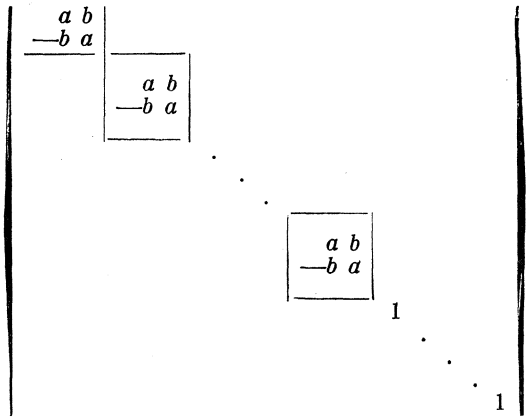
$$kp + p - 1 = \frac{p^n - 1}{2}\ ,\quad (k + 1)\, p - 1 = \frac{p^n - 1}{2}$$

cosa que es imposible.

Así, pues, multiplicando la matriz

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

por la izquierda por:



y por la derecha, por su traspuesta, tenemos que

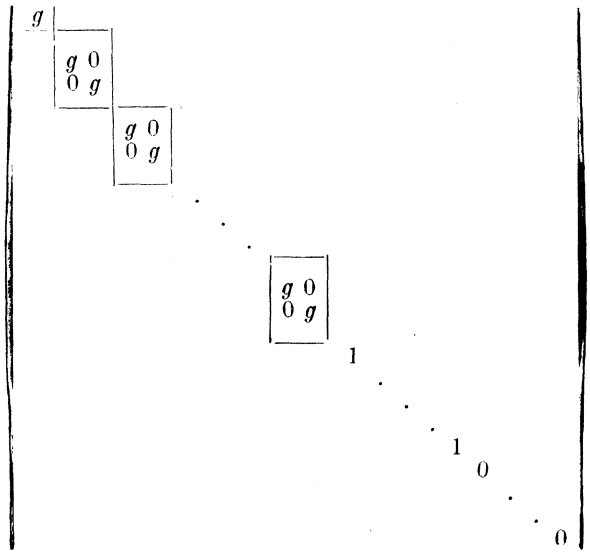
$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

es congruente con B.

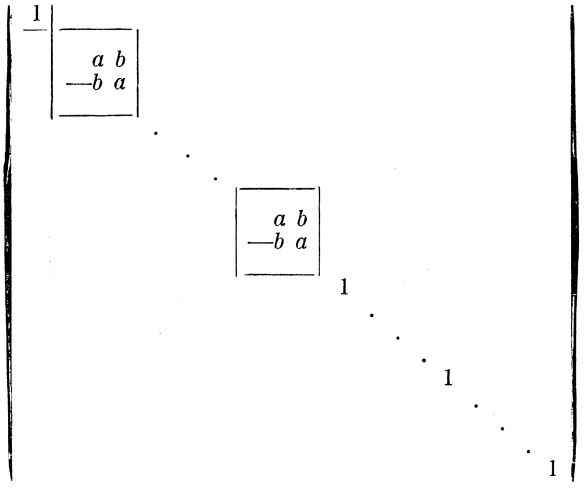
b) *Supongamos ahora* $1 = 2t + 1$.

Es decir,

$B_1 =$



y multiplicando $\begin{pmatrix} g & \\ & I_{r-1} \\ & 0 \end{pmatrix}$ por la izquierda por la matriz



y por la izquierda, por su traspuesta, queda que $\begin{pmatrix} g & \\ & I_{r-1} \\ & 0 \end{pmatrix}$ es congruente con B_1.

Veamos ahora que las matrices $\begin{pmatrix} I_r \\ 0 \end{pmatrix}$ y $\begin{pmatrix} g & \\ & I_{r-1} \\ & 0 \end{pmatrix}$ no son congruentes.

Pues si fueran congruentes, existiría una matriz T con $|T| \neq 0$, tal que

$$T \begin{pmatrix} I_r \\ 0 \end{pmatrix} T' = \begin{pmatrix} g & \\ & I_{r-1} \\ & 0 \end{pmatrix}$$

que se puede poner de la forma:

$$\begin{pmatrix} T_r & Z \\ X & Y \end{pmatrix} \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} T'_r & X' \\ Z' & Y' \end{pmatrix} = \begin{pmatrix} g & \\ & I_{r-1} \\ & 0 \end{pmatrix}$$

de donde

$$\begin{aligned} T_r\, I_r\, T'_r &= \begin{pmatrix} g & \\ & I_{r-1} \end{pmatrix} \\ X\, T'_s &= 0 \\ X\, X' &= 0 \end{aligned}$$

tomando determinantes en la primera ecuación $|T_r|^2 = g$ y vemos que esto es imposible, pues

$$g^{\frac{p^n - 1}{2}} = |T_r|^{p^n - 1} = 1$$

contradicción con ser g un generador del grupo, para el cual la potencia de menor exponente que vale 1 es la de exponente $p^n - 1$.

Por consiguiente, sobre un cuerpo finito de característica $p \neq 2$, todas las matrices de rango r son congruentes con:

$$\begin{pmatrix} I_r & \\ & 0 \end{pmatrix} \text{ o bien con } \begin{pmatrix} g & \\ & I_r \\ & & 0 \end{pmatrix}$$