FORMAS BILINEALES SOBRE Z_4 Y UN RESULTADO COMBINATORIO

Por Santiago López de Medrano

1.—Introducción

Sea Λ un anillo conmutativo con 1, y Λ^* el grupo de unidades de Λ. Las formas bilineales $B = (B, M)$ ($B{:}M \otimes M \to \Lambda$, M Λ-módulo libre con base finita) simétricas, no singulares sobre Λ forman un semigrupo bajo la suma directa ortogonal y el grupo de Grothendieck asociado se llama el *grupo de Grothendieck-Witt* de Λ y se denota por $G(\Lambda)$ ([3]). A la clase de B en $G(\Lambda)$ se le denota por $[B]$, y recordemos que $[B_1] = [B_2]$ si y sólo si existe B tal que $B_1 \oplus B \sim B_2 \oplus B$.

En este artículo calcularemos $G(Z_4)$:

Teorema 1.1. $G(Z_4) \approx Z \oplus Z_4$

Al tratar de demostrar este teorema se vió que era equivalente al siguiente resultado combinatorio:

Teorema 1.2. *Sea I un conjunto con n elementos, e $I_1, \cdots, I_n$, n subconjuntos de I. Supongamos que este sistema $\{I; I_1, \cdots, I_n\}$ satisface*

a) $\#I_j \equiv 3 \pmod 4$ *para* $1 \leq j \leq s$
b) $\#I_j \equiv 1 \pmod 4$ *para* $s+1 \leq j \leq n$
c) $\#(I_j \cap I_k) \equiv 0 \pmod 2$ *para* $j \neq k$

Entonces s es un múltiplo de 4.

(Aquí $\#I_j$ denota al número de elementos de conjunto I_j)

Así el cálculo de $G(Z_4)$ se redujo a un problema combinatorio. Sin embargo, éste resultó más difícil que el original, y finalmente encontramos una demostración algebraica directa del teorema 1.1, con lo cual el teorema 1.2 quedó también demostrado. El uso de formas cuadráticas para estudiar problemas combinatorios es bastante común (ver por ejemplo [2]), pero algunas de las ideas expuestas en este trabajo parecen ser nuevas, y es de esperar que se puedan aplicar a otros problemas. Por ejemplo, aplicando nuestros argumentos directamente con otros anillos finitos, se pueden obtener nuevos resultados combinatorios, pero estos resultan muy artificiales.

2.—Formas bilineales sobre Z_4

Por ser Z_4 un anillo local, toda forma no singular es suma de formas de rango ≤ 2 ([3]). Estas son

$$(x), \begin{pmatrix} 0 & x \\ x & 0 \end{pmatrix}, \begin{pmatrix} 2 & x \\ x & 0 \end{pmatrix} \text{ y } \begin{pmatrix} 2 & x \\ x & 2 \end{pmatrix}, x \in Z_4{}^*$$

Algunas de estas son equivalentes: de las igualdades

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & x \\ x & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & x \\ x & 0 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2a & x \\ x & 2b \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2a & -x \\ -x & 2b \end{pmatrix}$$

resulta que solo hay 4 formas irreducibles no equivalentes de rango $\leqslant 2$:

$$(1),\ (3),\ U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ V = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Finalmente, de la igualdad

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & -x \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & -x \end{pmatrix} = \begin{pmatrix} 1+x & x & 0 \\ x & 1+x & 0 \\ 0 & 0 & -x \end{pmatrix}$$

y de su negativa, obtenemos

$$3(1) \sim V \oplus (3)$$
$$2(1) \oplus (3) \sim U \oplus (1)$$
$$3(3) \sim V \oplus (1)$$
$$2(3) \oplus (1) \sim U \oplus (3)$$

Por lo tanto $G(Z_4)$ está generado por [1] y $\eta = [3] - [1]$ y como

$$V \oplus (1) \oplus (3) \sim 4(1) \sim 4(3),$$
$$4\eta = 0$$

Como det $\eta = 3$, $\eta \neq 0$ (det B está bien definido módulo el cuadrado de una unidad) y para demostrar el teorema 1.1 basta demostrar que $2\eta \neq 0$.

3.—Equivalencia con el problema combinatorio

El problema consiste en ver para qué valores de n y s existe un sistema $\{I; I_1, \cdots, I_n\}$ que cumpla las condiciones a), b) y c) del teorema 1.2. Para $n = s = 4$ tenemos el sistema $I = \{1, 2, 3, 4\}$, $I_j = I - \{j\}$, que combinándolo con el sistema de $n = 1$, $s = 0$, nos da sistemas para toda n y toda $s = 4k \leqslant n$. El teorema 1.2 nos dice que estos son todos los valores que podemos obtener. Ahora veremos que este problema es equivalente a determinar el orden de η en $G(Z_4)$.

LEMMA 3.1. *Existe un sistema* $\{I; I_1, \cdots, I_n\}$ *que satisface las condiciones* a), b) y c) *del teorema* 1.2 *para alguna* $n \geqslant s$ *si, y sólo si* $s\eta = 0$.

Demostración.—Si $s\eta = 0$, entonces $s[3] = s[1]$, es decir, $s(3) \oplus B \sim s(1) \oplus B$. Por las equivalencias de la sección anterior podemos suponer $B \sim k(1)$ y entonces $(s+k)(1) \sim s(3) \oplus k(1)$. Por lo tanto existe una matriz $A = (a_{ij})$ tal que

$$A\begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}A^t = \begin{pmatrix} 3I & 0 \\ 0 & I \end{pmatrix}$$

Sea $I = \{1, \cdots, n\}$, I_j definido por $k \in I_j$, si y sólo si $a_{jk} \in Z_4^*$. Entonces

$$\sum_{k=1}^{n} a_{jk}^2 = \begin{cases} 3, & j \leqslant s \\ 1, & j > s \end{cases}$$
$$\sum_{k=1}^{n} a_{jk}a_{j'k} = 0, \quad j \neq j'$$

como $x^2 = 1$ si $x \in Z_4^*$ y $x^2 = 0$ si $x \notin Z_4^*$, tenemos

$$\sum a_{jk}^2 \equiv \#I_j \pmod 4$$
$$\sum a_{jk}a_{j'k} \equiv \#(I_j \cap I_{j'}) \pmod 2$$

y $\{I; I_1, \cdots, I_n\}$ satisface a), b) y c).

Reciprocamente, dado un sistema que cumpla a), b) y c), construimos la matriz $A = (a_{ij})$ sobre Z_4 mediante

$$a_{jk} = \begin{cases} 1 & \text{si } k \in I_j \\ 0 & \text{si } k \notin I_j \end{cases}$$

Entonces, por lo expuesto anteriormente A establece la equivalencia entre $n(1)$ y una forma bilineal con matriz $X = (x_{ij})$ que satisface

$$x_{ii} = \begin{cases} 3 & i \leqslant s \\ 1 & i > s \end{cases}$$

$$x_{ij} = 2y_{ij}, \quad i \neq j.$$

y finalmente podemos anular todos los términos fuera de la diagonal principal: si Z es la matriz

$$z_{ij} = \begin{cases} x_{ij} & j > i \\ 1 & j = i \\ 0 & j < i, \end{cases}$$

Z nos da la equivalencia entre esta forma y $s(3) \oplus (n - s)(1)$ y por lo tanto

$$n(1) \sim s(3) \oplus (n - s)(1)$$

y

$$s\eta = s[3] - s[1] = 0$$

con lo que queda demostrado el lema.

Nótese que por ser $\eta \neq 0$ (ver el final de la sección anterior), queda demostrado que s debe ser par en el teorema 1.2. Para demostrar que s debe ser múltiplo de 4 hace falta un invariante más fino que el determinante.

4.—Un invariante de formas bilineales sobre anillos finitos

Sea Λ ahora un anillo finito. Denotaremos por $Z[\Lambda]$ al anillo de grupo de Λ, considerado éste simplemente como grupo abeliano.

Sea (M, B) una forma bilineal sobre Λ. Definimos el *espectro* de B como

$$e(B) = \sum n_\alpha \lambda_\alpha \in Z[\Lambda]$$

donde n_α = número de $x \in M$ tales que $B(x, x) = \lambda_\alpha$. Es claro que $e(B)$ depende sólo de la clase de equivalencia de B.

PROPOSICIÓN 4.1. $e(B_1 \oplus B_2) = e(B_1)e(B_2)$.

Demostración.—Si $B = B_1 \oplus B_2$ y $e(B_i) = \sum n_{i\alpha}\lambda_\alpha$ el número de $(x_1, x_2) \in$

$M_1 \oplus M_2$ tales que $B((x_1, x_2), (x_1, x_2)) = B_1(x_1, x_1) + B_2(x_2, x_2) = \lambda_\alpha$ es igual a $\sum n_{1\beta} n_{2\gamma}$ para $\lambda_\beta + \lambda_\gamma = \lambda_\alpha$; pero esto corresponde a la definición de la multiplicación en $Z[\Lambda]$.

Demostración del teorema 1.1. Falta demostrar que $s\eta = 0$ implica $4 \mid s$. $s\eta = 0$ es equivalente a $(s + k)(1) = s(3) \oplus k(1)$, para alguna k que podemos suponer múltiplo de 4, y como $4(1) \sim 4(3)$, tenemos que $(s + 4\ell)(1) = (s + 4\ell)(3)$. Por lo tanto basta demostrar que $s(1) \sim s(3)$ implica $4 \mid s$. Directamente se puede verificar que

$$e(1) = 2 + 2t$$

$$e(3) = 2 + 2t^3$$

donde hemos denotado por t al generador de Z_4, considerado como grupo multiplicativo. Por la proposición anterior

$$e(s(1)) = 2^s(1 + t)^s$$

$$e(s(3)) = 2^s(1 + t^3)^s$$

y basta demostrar que

$$(1 + t)^s = (1 + t^3)^s$$

si, y sólo si $4 \mid s$. Si escribimos

$$(1 + t)^k = a + bt + ct^2 + dt^3$$

el valor de $(1 + t^3)^k$ se obtiene intercambiando los coeficientes de t y t^3:

$$(1 + t^3)^k = a + dt + ct^2 + bt^3.$$

Por otra parte,

$$(1 + t)^{k+4} = (2a + 4d + 6c + 4b) + (2b + 4a + 6d + 4c)t + (2c + 4b + 6a + 4d)t^2 + (2d + 4c + 6b + 4a)t^3$$

y $(1 + t)^{k+4} = (1 + t^3)^{k+4}$ implica que los coeficientes de t y t^3 en la última expresión son iguales, de donde se deduce $b = d$ y $(1 + t)^k = (1 + t^3)^k$. Por lo tanto podemos ir reduciendo la igualdad $(1 + t)^s = (1 + t^3)^s$ hasta llegar a $s \leqslant 4$ en donde por un cálculo sencillo se puede demostrar que s tiene que ser múltiplo de 4 y el teorema 1.1, y en consecuencia el teorema 1.2, queda demostrado.

Observaciones.

1.—e no es un invariante estable ya que

$$U = [1] + [3]$$

pero $e(U) = 12 + 4t^2$ y $e((1) \oplus (3)) = 8 + 4t + 4t^3$. Esto se debe a que $Z[\Lambda]$ tiene en general divisores de 0. e quedaría bien definido en el grupo de Grothendieck del semigrupo multiplicativo de elementos de $Z[\Lambda]$ de la forma $e(B)$. En

el caso de Z_4, este grupo sería nuevamente $Z \oplus Z_4$ y e daría el isomorfismo. No conviene tomar todo el semigrupo multiplicativo de $Z[\Lambda]$ por que el grupo asociado es Z y se perdería toda la información que nos da e.

2.—e se puede definir de hecho para cualquier función $f: X \to \Lambda$, X conjunto finito, y es multiplicativo con la definición obvia de suma directa de tales funciones. En particular podemos definirlo para formas cuadráticas $\varphi: M \to \Lambda$, y en el caso de Z_2 se puede considerar como una extensión del invariante de Arf ([1]) a formas cuadráticas singulares.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

REFERENCIAS

[1] C. ARF, *Untersuchungen über quadratische Formen in Körpern der Charakteristik* 2. J. Reine Angew. Math. **183** (1941), 148–67.

[2] M. HALL, JR., Combinatorial Theory. Blaisdell Publishing Co., Waltham, Mass., 1967.

[3] F. HIRZEBRUCH, *Differentiable Manifolds and Quadratic Forms*. Notas mimeografiadas, Universidad de Berkeley.