

ÓRDENES MATRICIALES GENERADOS POR GRUPOS DE CONGRUENCIA

(álgebra de matrices/orden matricial/grupo de unidades)

P. BAYER*, A. TRAVESA**

* Universitat de Barcelona, Facultat de Matemàtiques. Departament d'Àlgebra i Geometria. Gran Via de les Corts Catalanes, 585. E-08007 Barcelona (bayer@mat.ub.es)

** Universitat de Barcelona, Facultat de Matemàtiques. Departament d'Àlgebra i Geometria. Gran Via de les Corts Catalanes, 585. E-08007 Barcelona (travesa@mat.ub.es)

RESUMEN

En este artículo introducimos una familia de órdenes $\mathcal{O}(M, N, D)$, que es filtrante inferiormente del sistema de todos los órdenes del álgebra de matrices $\mathbf{M}(2, \mathbb{Q})$. Los grupos correspondientes de unidades de norma uno, $\Gamma(M, N, D)$, proporcionan grupos de congruencia contenidos en el grupo especial lineal $\mathbf{SL}(2, \mathbb{R})$ y operan, por tanto, en el semiplano superior complejo. Relacionamos los grupos así obtenidos con los grupos de congruencia $\Gamma_0(N)$, $\Gamma_1(N)$ y $\Gamma(N)$, considerados habitualmente en el estudio aritmético de funciones automorfas.

ABSTRACT

In this paper we introduce a family of orders $\mathcal{O}(M, N, D)$, filtering from below the system of all orders of the matrix algebra $\mathbf{M}(2, \mathbb{Q})$. The corresponding groups of units of norm equal to one, $\Gamma(M, N, D)$, provide congruence groups contained in the special linear group $\mathbf{SL}(2, \mathbb{R})$, and so they act on the complex upper half-plane. We relate the groups obtained in this way to the congruence groups $\Gamma_0(N)$, $\Gamma_1(N)$ and $\Gamma(N)$, which are usually considered in the arithmetical study of automorphic functions.

INTRODUCCIÓN

El objetivo principal de este artículo es dar una descripción de una familia amplia de órdenes del álgebra $\mathbf{M}(2, \mathbb{Q})$ de las matrices 2×2 de coeficientes racionales y de su relación con los grupos de congruencia del grupo especial lineal $\mathbf{SL}(2, \mathbb{Z})$ de coeficientes enteros.

En la primera parte, se establecen las definiciones y los resultados básicos relativos a los órdenes de $\mathbf{M}(2, \mathbb{Q})$; en particular, y teniendo en cuenta la forma lineal traza, se define el concepto de paridad de un orden y se relaciona este concepto con la forma cuadrática ternaria nórmi-ca asociada al submódulo de las matrices de traza nula del orden. Los ejemplos principales consisten en los órdenes $\mathcal{O}_0(N)$, $\mathcal{O}_1(N)$, y $\mathcal{O}(N)$, que definimos *ad hoc* por similitud con los grupos de congruencia más estudiados habitualmente (cf. [Sh 71]), $\Gamma_0(N)$, $\Gamma_1(N)$ y $\Gamma(N)$. A partir de la observación de estos ejemplos, se define la familia de los órdenes $\mathcal{O}(M, N, D)$, que contiene los anteriores como casos particulares, y que permite entender de una manera más global algunos fenómenos observados. Esta familia de órdenes es una familia filtrante inferiormente para el conjunto de todos los subórdenes de $\mathbf{M}(2, \mathbb{Z})$.

La segunda parte se dedica al estudio de los grupos de congruencia y de su relación con los órdenes de $\mathbf{M}(2, \mathbb{Q})$. El grupo de las unidades de norma 1 del orden $\mathcal{O}_0(N)$ es exactamente el grupo de congruencia $\Gamma_0(N)$; pero esto no sucede así con los grupos de unidades de $\mathcal{O}_1(N)$ ni de $\mathcal{O}(N)$. Más generalmente, y para $N \geq 3$, ningún orden de $\mathbf{M}(2, \mathbb{Q})$ tiene como grupo de unidades de norma 1 el grupo $\Gamma_1(N)$ ni el grupo $\Gamma(N)$. Por otra parte, el orden generado por el grupo de congruencia $\Gamma_1(N)$ es el orden $\mathcal{O}_1(N)$, mientras que el orden generado por $\Gamma_0(N)$ no es, en general, el orden $\mathcal{O}_0(N)$, sino un orden menor. El objetivo principal de esta segunda parte es la descripción de los órdenes generados por los grupos de unidades de norma 1 de los órdenes de $\mathbf{M}(2, \mathbb{Z})$. Como caso especialmente importante, se obtiene una descripción exacta de los órdenes generados por los grupos $\Gamma_0(N)$, $\Gamma_1(N)$ y $\Gamma(N)$. En particular, el grupo $\Gamma_0(N)$ coincide con el grupo de las unidades de norma 1 del orden generado por $\Gamma_0(N)$. Además, para $\Gamma_1(N)$ y para $\Gamma(N)$ se obtiene una descripción exacta del grupo cociente $\Gamma/\Gamma_1(N)$ (resp. $\Gamma/\Gamma(N)$), donde Γ es el grupo de las unidades de norma 1 del orden generado por $\Gamma_1(N)$ (resp. por $\Gamma(N)$).

¹ Con soporte parcial de DGES, PB96-0166.

1. ÓRDENES DEL ÁLGEBRA DE MATRICES

Consideraremos la \mathbb{Q} -álgebra de las matrices 2×2 racionales, $H := \mathbf{M}(2, \mathbb{Q})$; por tanto, identificaremos un número racional cualquiera $q \in \mathbb{Q}$ con la matriz diagonal $\begin{bmatrix} q & 0 \\ 0 & q \end{bmatrix}$; en particular, el conjunto \mathbb{Z} de los números enteros se identifica con el conjunto de las matrices diagonales tales que $q \in \mathbb{Z}$.

Definición 1.1. Se dice que una matriz $\begin{bmatrix} x & y \\ z & t \end{bmatrix} \in \mathbf{M}(2, \mathbb{Q})$ es entera sobre \mathbb{Z} o, simplemente, entera, si, y sólo si, su traza $x + t$ y su determinante $xt - yz$ son números enteros.

Contrariamente a lo que ocurre en el caso de los cuerpos de números, el conjunto de las matrices enteras no forma un subanillo de $\mathbf{M}(2, \mathbb{Q})$; por ejemplo, las matrices

$$X := \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{bmatrix}, Y := \begin{bmatrix} 1 & 0 \\ \frac{1}{2} & 1 \end{bmatrix}, Z := \begin{bmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{bmatrix}, T := \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

son matrices enteras, pero XY y $Z + T$ no lo son. Observemos que existen matrices enteras cuyos coeficientes no son números enteros.

Será de especial interés para nuestros propósitos el subespacio vectorial de $\mathbf{M}(2, \mathbb{Q})$ formado por las matrices de traza nula; es un \mathbb{Q} -espacio vectorial de dimensión 3, que denotaremos por H_0 .

Definición 1.2. Un orden de $\mathbf{M}(2, \mathbb{Q})$ es un subanillo formado por matrices enteras y tal que, como grupo abeliano, es libre de rango 4. Más generalmente, una red de $\mathbf{M}(2, \mathbb{Q})$ es un subgrupo abeliano que contiene una \mathbb{Q} -base de $\mathbf{M}(2, \mathbb{Q})$ como espacio vectorial racional. En particular, pues, todo orden es una red.

Definición 1.3. Sea $L \subseteq \mathbf{M}(2, \mathbb{Q})$ una red que contenga \mathbb{Z} y esté formada por matrices enteras. Diremos que una tal red L es impar si, y sólo si, 1 es traza de alguna matriz de L . En caso contrario, diremos que L es par. En particular, esta definición se aplica a cualquier orden $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$.

Observación 1.4. Más generalmente, si $L \subseteq \mathbf{M}(2, \mathbb{Q})$ es una red cualquiera, la aplicación traza $t: L \rightarrow \mathbb{Q}$ es un homomorfismo de grupos abelianos y, puesto que L es un grupo abeliano finitamente generado, la imagen de t es un subgrupo abeliano finitamente generado de \mathbb{Q} ; es decir, un ideal fraccionario de \mathbb{Q} . Y, puesto que \mathbb{Z} es principal, existe un número racional $r \in \mathbb{Q}$ tal que $t(L) = r\mathbb{Z}$.

Ahora, si $L \subseteq \mathbf{M}(2, \mathbb{Q})$ es una red formada por matrices enteras que contiene \mathbb{Z} , la imagen del homomorfismo

traza $t: L \rightarrow \mathbb{Q}$ está contenida en \mathbb{Z} y contiene el subgrupo $2\mathbb{Z}$. En consecuencia, es $t(L) = 2\mathbb{Z}$ o bien $t(L) = \mathbb{Z}$; estas dos posibilidades caracterizan si L es par o impar.

Proposición 1.5. Sea $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$ un orden cualquiera. Entonces:

- (a) $\mathcal{O}' := \{A \in \mathcal{O} : t(A) \in 2\mathbb{Z}\}$ es una subred par de \mathcal{O} .
- (b) La suma $\mathbb{Z} + (\mathcal{O} \cap H_0)$ es directa.
- (c) $\mathbb{Z} \oplus (\mathcal{O} \cap H_0) = \mathcal{O}'$.
- (d) El índice $[\mathcal{O} : \mathcal{O}']$ es 1 o 2.
- (e) \mathcal{O} es par si, y sólo si, $\mathcal{O} = \mathcal{O}'$.
- (f) \mathcal{O} es impar si, y sólo si, $[\mathcal{O} : \mathcal{O}'] = 2$; equivalentemente, si, y sólo si, $\mathcal{O}' \subsetneq \mathcal{O}$. □

Observación 1.6. En general, aunque \mathcal{O} sea un orden, \mathcal{O}' sólo es una red, y no necesariamente un orden.

Proposición 1.7. Sea $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$ un orden cualquiera. Entonces, la subred $\mathbb{Z} + 2\mathcal{O} \subsetneq \mathcal{O}'$ es un suborden par de \mathcal{O} . □

En general, si $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$ es un orden, el conjunto $\mathcal{O} \cap H_0$, formado por las matrices de \mathcal{O} de traza nula, es un grupo abeliano libre de rango 3, y la asignación $A \mapsto \det(A)$ define una forma cuadrática ternaria entera, llamada forma nórmica, $n_0: \mathcal{O} \cap H_0 \rightarrow \mathbb{Z}$. Puesto que una \mathbb{Q} -base de H_0 está formada por las matrices

$$\begin{bmatrix} 0 & -2 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix},$$

la forma nórmica n_0 es \mathbb{Q} -equivalente a la forma cuadrática $-Y^2 + 4XZ$; es decir, a la forma cuadrática discriminante en grado dos cambiada de signo.

En particular, para un orden cualquiera $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$, es $\mathcal{O} \cap H_0 = \mathcal{O}' \cap H_0$, de manera que la forma ternaria nórmica n_0 está determinada por la subred par \mathcal{O}' de \mathcal{O} .

Ejemplos 1.8. Para todo número entero $N \geq 1$, pongamos

$$\mathcal{O}_0(N) := \left\{ \begin{bmatrix} x & y \\ zN & t \end{bmatrix} : x, y, z, t \in \mathbb{Z} \right\}.$$

Entonces, $\mathcal{O}_0(N)$ es un orden impar. La subred par asociada a $\mathcal{O}_0(N)$, $\mathcal{O}'_0(N) := \mathbb{Z} \oplus (\mathcal{O}_0(N) \cap H_0)$, es el conjunto

$$\mathcal{O}'_0(N) = \left\{ \begin{bmatrix} x & y \\ zN & x + 2t \end{bmatrix} : x, y, z, t \in \mathbb{Z} \right\},$$

y es un orden si, y sólo si, N es par.

La forma ternaria n6rmica asociada a $\mathcal{O}_0(N)$ es la forma cuadr6tica ternaria entera $n_0(X, Y, Z) = -Y^2 + NXZ$, puesto que las matrices

$$\begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ N & 0 \end{bmatrix},$$

constituyen una \mathbb{Z} -base de $\mathcal{O}_0(N) \cap H_0$.

Asociado al orden $\mathcal{O}_0(N)$, el orden par $\mathbb{Z} + 2\mathcal{O}_0(N)$ es el conjunto

$$\mathbb{Z} + 2\mathcal{O}_0(N) = \left\{ \begin{bmatrix} x & 2y \\ 2zN & x + 2t \end{bmatrix} : x, y, z, t \in \mathbb{Z} \right\},$$

que es un suborden de 6ndice 8 de $\mathcal{O}_0(N)$. La forma ternaria n6rmica asociada a $\mathbb{Z} + 2\mathcal{O}_0(N)$, $n_{0,2}$, es la forma $n_{0,2}(X, Y, Z) = -Y^2 + 4NXZ$.

An6logamente, para todo n6mero entero $N \geq 1$, pongamos

$$\mathcal{O}_1(N) := \left\{ \begin{bmatrix} x & y \\ zN & x + tN \end{bmatrix} : x, y, z, t \in \mathbb{Z} \right\},$$

y

$$\mathcal{O}(N) := \left\{ \begin{bmatrix} x & yN \\ zN & x + tN \end{bmatrix} : x, y, z, t \in \mathbb{Z} \right\}.$$

Entonces, $\mathcal{O}_1(N)$ y $\mathcal{O}(N)$ son 6rdenes de $\mathbf{M}(2, \mathbb{Q})$ de la misma paridad que N .

Los 6rdenes pares $\mathbb{Z} + 2\mathcal{O}_1(N)$ y $\mathbb{Z} + 2\mathcal{O}(N)$ asociados a los 6rdenes $\mathcal{O}_1(N)$ y $\mathcal{O}(N)$ son los conjuntos

$$\mathbb{Z} + 2\mathcal{O}_1(N) = \left\{ \begin{bmatrix} x & 2y \\ 2zN & x + 2tN \end{bmatrix} : x, y, z, t \in \mathbb{Z} \right\},$$

y

$$\mathbb{Z} + 2\mathcal{O}(N) = \left\{ \begin{bmatrix} x & 2yN \\ 2zN & x + 2tN \end{bmatrix} : x, y, z, t \in \mathbb{Z} \right\}.$$

Y las formas ternarias n6rmicas asociadas a $\mathbb{Z} + 2\mathcal{O}_1(N)$ y $\mathbb{Z} + 2\mathcal{O}(N)$ son, respectivamente, las formas $-N^2Y^2 + 4NXZ$ y $-N^2Y^2 + 4N^2XZ$.

A la vista de estos ejemplos, introducimos la definici6n siguiente.

Definici6n 1.9. Para todo par de n6meros enteros $M, N \geq 1$ y todo divisor $D \geq 1$ del producto MN , definimos

$$\mathcal{O}(M, N, D) := \left\{ \begin{bmatrix} x & yM \\ zN & x + tD \end{bmatrix} : x, y, z, t \in \mathbb{Z} \right\}.$$

En particular, se tiene que

- (a) $\mathcal{O}_0(N) = \mathcal{O}(1, N, 1)$;
- (b) $\mathcal{O}_1(N) = \mathcal{O}(1, N, N)$;
- (c) $\mathcal{O}(N) = \mathcal{O}(N, N, N)$;
- (d) $\mathbb{Z} + 2\mathcal{O}(M, N, D) = \mathcal{O}(2M, 2N, 2D)$.

Proposici6n 1.10. Sean $M, N \geq 1$ n6meros enteros y $D \geq 1$ un divisor de MN . Entonces:

- (a) $\mathcal{O}(M, N, D) \subseteq \mathbf{M}(2, \mathbb{Q})$ es un orden de la misma paridad que D .
- (b) $\mathcal{O}(1, 1, 1) = \mathbf{M}(2, \mathbb{Z})$ es un orden maximal.
- (c) Sean $M' \geq 1$ un divisor de M , $N' \geq 1$ un divisor de N , y $D' \geq 1$ un divisor de D y de $M'N'$. Entonces, $\mathcal{O}(M, N, D) \subseteq \mathcal{O}(M', N', D')$ es un suborden de 6ndice $\frac{MND}{M'N'D'}$; para el grupo abeliano cociente se tiene un isomorfismo

$$\frac{\mathcal{O}(M', N', D')}{\mathcal{O}(M, N, D)} \simeq \frac{\mathbb{Z}}{(M/M')\mathbb{Z}} \times \frac{\mathbb{Z}}{(N/N')\mathbb{Z}} \times \frac{\mathbb{Z}}{(D/D')\mathbb{Z}}.$$

- (d) La forma ternaria n6rmica $n_0(X, Y, Z)$ asociada a $\mathcal{O}(M, N, D)$ es la forma

$$n_0(X, Y, Z) = \begin{cases} -D^2Y^2 + MNXZ, & \text{si } D \text{ es impar,} \\ -\frac{D^2}{4}Y^2 + MNXZ, & \text{si } D \text{ es par.} \end{cases}$$

Demostraci6n. Es evidente que $\mathcal{O}(M, N, D)$ es un grupo abeliano, y que las matrices

$$1 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, e_1 := \begin{bmatrix} 0 & M \\ 0 & 0 \end{bmatrix}, e_2 := \begin{bmatrix} 0 & 0 \\ N & 0 \end{bmatrix}, e_3 := \begin{bmatrix} 0 & 0 \\ 0 & D \end{bmatrix}$$

forman una \mathbb{Z} -base de $\mathcal{O}(M, N, D)$. Por otra parte, y puesto que D divide MN , la multiplicaci6n es estable en $\mathcal{O}(M, N, D)$, de manera que $\mathcal{O}(M, N, D)$ es un subanillo de $\mathbf{M}(2, \mathbb{Q})$; adem6s, puesto que $\mathcal{O}(M, N, D)$ est6 formado por matrices enteras, $\mathcal{O}(M, N, D)$ es un orden. Finalmente, est6 claro que $\mathcal{O}(M, N, D)$ es de la misma paridad que D .

El conocimiento expl6cito de \mathbb{Z} -bases de los 6rdenes $\mathcal{O}(M, N, D)$ y $\mathcal{O}(M', N', D')$ permite obtener (c) inmediatamente, a partir del c6lculo de los factores invariantes.

A continuaci6n, procedemos a dar una demostraci6n elemental del hecho que $\mathcal{O}(1, 1, 1) = \mathbf{M}(2, \mathbb{Z})$ es un orden maximal. Supongamos que \mathcal{O} es un orden que contiene

$\mathbf{M}(2, \mathbb{Z})$ y sea $\begin{bmatrix} x & y \\ z & t \end{bmatrix} \in \mathcal{O}$, con $x, y, z, t \in \mathbb{Q}$, un elemento cualquiera de \mathcal{O} . Los productos

$$\begin{aligned} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & t \end{bmatrix} &= \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}, \\ \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & t \end{bmatrix} &= \begin{bmatrix} z & t \\ 0 & 0 \end{bmatrix}, \\ \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & t \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ x & y \end{bmatrix}, \\ \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x & y \\ z & t \end{bmatrix} &= \begin{bmatrix} 0 & 0 \\ z & t \end{bmatrix} \end{aligned}$$

pertenecen a \mathcal{O} ; por tanto, las trazas de estas matrices son números enteros; es decir, $x, y, z, t \in \mathbb{Z}$, y $\begin{bmatrix} x & y \\ z & t \end{bmatrix} \in \mathbf{M}(2, \mathbb{Z})$, de manera que $\mathcal{O} = \mathbf{M}(2, \mathbb{Z})$, como queríamos demostrar.

Finalmente, el cálculo de la forma cuadrática ternaria nór mica asociada a $\mathcal{O}(M, N, D)$ es inmediato, una vez calculada una \mathbb{Z} -base de $\mathcal{O}(M, N, D) \cap H_0$; una tal \mathbb{Z} -base está formada por las matrices

$$\begin{bmatrix} 0 & -M \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} -D & 0 \\ 0 & D \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ N & 0 \end{bmatrix},$$

si D es impar, y

$$\begin{bmatrix} 0 & -M \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} -\frac{D}{2} & 0 \\ 0 & \frac{D}{2} \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ N & 0 \end{bmatrix},$$

si D es par. □

En particular, y puesto que $2D$ es par, la forma ternaria nór mica $n_{0,2}$ asociada a $\mathcal{O}(M, N, D)$, es decir, la forma nór mica del grupo abeliano $\mathcal{O}(2M, 2N, 2D) \cap H_0$, es la forma $n_{0,2}(X, Y, Z) = -D^2 Y^2 + 4MNXZ$.

Observación 1.11. *No es cierto que la familia formada por los órdenes $\mathcal{O}(M, N, D)$ contenga todos los órdenes de $\mathbf{M}(2, \mathbb{Q})$. Sin embargo, todo orden está incluido en un orden maximal (por definición), y, puesto que \mathbb{Z} es principal, dos órdenes maximales de $\mathbf{M}(2, \mathbb{Q})$ son conjugados por un elemento $U \in \mathbf{GL}(2, \mathbb{Q}) = \mathbf{M}(2, \mathbb{Q})^*$ (cf. [Vi 80]). Por tanto, todo orden de $\mathbf{M}(2, \mathbb{Q})$ es isomorfo (conjugado) a un suborden de $\mathbf{M}(2, \mathbb{Z})$. Los resultados siguientes permiten precisar un poco más el conocimiento de los subórdenes de $\mathbf{M}(2, \mathbb{Q})$.*

Proposición 1.12. *Sea $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$ un suborden cualquiera. Entonces, existe un número entero $N \geq 1$ tal que $\mathcal{O}(N, N, N) \subseteq \mathcal{O}$.*

Demostración. Puesto que $\mathcal{O} \supseteq \mathcal{O} \cap \mathcal{O}(1, 1, 1)$, que es un suborden de $\mathbf{M}(2, \mathbb{Z})$, podemos suponer que $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Z})$. Entonces, puesto que \mathcal{O} y $\mathcal{O}(1, 1, 1)$ son grupos abelianos libres del mismo rango y $\mathcal{O} \subseteq \mathcal{O}(1, 1, 1)$, el grupo abeliano cociente $\mathcal{O}(1, 1, 1)/\mathcal{O}$ es finito. Si N es el exponente de este grupo abeliano cociente, tenemos que para todo elemento $X \in \mathcal{O}(1, 1, 1)$ es $NX \in \mathcal{O}$. En particular, \mathcal{O} contiene las matrices

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & N \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ N & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & N \end{bmatrix},$$

que constituyen una \mathbb{Z} -base de $\mathcal{O}(N, N, N)$. Luego, $\mathcal{O} \supseteq \mathcal{O}(N, N, N)$, como queríamos demostrar. □

Proposición 1.13. *Sean $M, N \geq 1$ números enteros. Todo subgrupo aditivo $\mathcal{O} \subseteq \mathcal{O}(M, N, 1)$ que contiene $\mathcal{O}(M, N, MN)$ es un orden, y existe un divisor $D \geq 1$ de MN tal que $\mathcal{O} = \mathcal{O}(M, N, D)$.*

Si $D \geq 1$ es un divisor de M , todo subgrupo aditivo $\mathcal{O} \subseteq \mathcal{O}(M, 1, D)$ que contiene $\mathcal{O}(M, N, D)$ es un orden, y existe un divisor $N' \geq 1$ de N tal que $\mathcal{O} = \mathcal{O}(M, N', D)$.

Si $D \geq 1$ es un divisor de N , todo subgrupo aditivo $\mathcal{O} \subseteq \mathcal{O}(1, N, D)$ que contiene $\mathcal{O}(M, N, D)$ es un orden, y existe un divisor $M' \geq 1$ de M tal que $\mathcal{O} = \mathcal{O}(M', N, D)$.

Demostración. En virtud del apartado (c) de la proposición 1.10, el retículo de subgrupos de $\mathcal{O}(M, N, 1)$ que contienen $\mathcal{O}(M, N, MN)$ es isomorfo al retículo de subgrupos de $\mathbb{Z}/MN\mathbb{Z}$; es decir, al retículo de divisores de MN . Pero el retículo formado por los órdenes $\mathcal{O}(M, N, D)$, para D divisor de MN , es isomorfo a este retículo. Por tanto, todo subgrupo abeliano de $\mathcal{O}(M, N, 1)$ que contiene $\mathcal{O}(M, N, MN)$ es uno de los órdenes $\mathcal{O}(M, N, D)$, con $D \geq 1$ divisor de MN . Las otras dos propiedades se demuestran de la misma manera. □

Observación 1.14. *No todos los subórdenes de $\mathbf{M}(2, \mathbb{Z})$ son de la forma $\mathcal{O}(M, N, D)$, para algún divisor $D \geq 1$ de MN . Por ejemplo,*

$$\mathcal{O} := \left\{ \begin{bmatrix} x & y \\ z & t \end{bmatrix} : x, y, z, t \in \mathbb{Z}, y \equiv z \equiv x + t \pmod{2} \right\}$$

es un suborden de $\mathcal{O}(1, 1, 1)$, que contiene $\mathcal{O}(2, 2, 2)$ como suborden de índice 2, y no es ninguno de los órdenes $\mathcal{O}(2, 2, 1)$, $\mathcal{O}(2, 1, 2)$, ni $\mathcal{O}(1, 2, 2)$.

1.15. Ordenes y conjugación. Los hechos, comentados más arriba, que todo orden de $\mathbf{M}(2, \mathbb{Q})$ está incluido en un orden maximal, que dos órdenes maximales de $\mathbf{M}(2, \mathbb{Q})$ son conjugados por un elemento de $\mathbf{GL}(2, \mathbb{Q})$, y que $\mathbf{M}(2, \mathbb{Z})$ es un orden maximal, permiten que nos restrinjamos al estudio de los subórdenes de $\mathbf{M}(2, \mathbb{Z})$.

Por otra parte, si tomamos $U := \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix} \in \mathbf{GL}(2, \mathbb{Q})$, tenemos que $U^{-1}\mathcal{O}(M, N, D)U = \mathcal{O}(1, MN, D)$, de manera que cualquiera de los órdenes $\mathcal{O}(M, N, D)$ es conjugado a un orden de la forma $\mathcal{O}(1, MN, D)$. Sin embargo, la conjugación por U no deja invariante $\mathbf{M}(2, \mathbb{Z})$, salvo que sea $N = 1$; por tanto, si un suborden $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Z})$ contiene $\mathcal{O}(M, N, D)$, el orden conjugado $U^{-1}\mathcal{O}U$ contiene $\mathcal{O}(1, MN, D)$, pero, en general, no está contenido en $\mathbf{M}(2, \mathbb{Z})$. Es decir, si nos limitamos a estudiar los subórdenes de $\mathbf{M}(2, \mathbb{Z})$, debemos hacer el estudio de todos los órdenes de la forma $\mathcal{O}(M, N, D)$, y no podemos limitarnos a los de la forma $\mathcal{O}(1, MN, D)$.

Observación 1.16. En el caso $U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in \mathbf{SL}(2, \mathbb{Z})$, tenemos que $U^{-1}\mathbf{M}(2, \mathbb{Z})U = \mathbf{M}(2, \mathbb{Z})$ y que $U^{-1}\mathcal{O}(M, N, D)U = \mathcal{O}(N, M, D)$. Por tanto, en cualquier caso, podemos intercambiar los papeles de M y N .

Finalmente, para el estudio de los órdenes de $\mathbf{M}(2, \mathbb{Q})$, puede ser de interés el resultado siguiente, que generaliza los dos casos anteriores.

Proposición 1.17. Sea $T \in \mathbb{Q}^*$ un número racional no nulo cualquiera, y pongamos $U := \begin{bmatrix} 0 & -1 \\ T & 0 \end{bmatrix} \in \mathbf{GL}(2, \mathbb{Q})$. Entonces, para todo par de números enteros $M, N \geq 1$ y todo divisor $D \geq 1$ de MN , es

$$U^{-1}\mathcal{O}(M, N, D)U = \mathcal{O}\left(\frac{N}{T}, MT, D\right),$$

con las notaciones evidentes para $\mathcal{O}\left(\frac{N}{T}, MT, D\right)$. \square

Notemos que, puesto que la conjugación respeta la traza y el determinante, $\mathcal{O}\left(\frac{N}{T}, MT, D\right)$ es un orden de $\mathbf{M}(2, \mathbb{Q})$.

2. ÓRDENES Y GRUPOS DE CONGRUENCIA

Recordemos que los grupos de congruencia de $\mathbf{SL}(2, \mathbb{Z})$ son los subgrupos $\Gamma \subseteq \mathbf{SL}(2, \mathbb{Z})$ para los cuales existe un número entero $N \geq 1$ tal que Γ contiene, como subgrupo, el grupo principal de congruencia de nivel N ,

$$\Gamma(N) := \left\{ \begin{bmatrix} 1 + \alpha N & \beta N \\ \gamma N & 1 + \delta N \end{bmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \det = 1 \right\}$$

(cf. [Sh 71]). En particular, los grupos

$$\Gamma_1(N) := \left\{ \begin{bmatrix} 1 + \alpha N & \beta \\ \gamma N & 1 + \delta N \end{bmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \det = 1 \right\},$$

$$\Gamma_0(N) := \left\{ \begin{bmatrix} \alpha & \beta \\ \gamma N & \delta \end{bmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \det = 1 \right\},$$

son grupos de congruencia.

Definición 2.1. Para cada par de números enteros $M, N \geq 1$ y cada divisor $D \geq 1$ de MN , pondremos

$$\Gamma(M, N, D) := \{A \in \mathcal{O}(M, N, D) : \det A = 1\};$$

es decir, $\Gamma(M, N, D)$ es el grupo de las unidades de norma 1 del orden $\mathcal{O}(M, N, D)$. Se tiene que

$$\Gamma(M, N, D) = \left\{ \begin{bmatrix} \alpha & \beta M \\ \gamma N & \alpha + \delta D \end{bmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \det = 1 \right\}.$$

Observación 2.2. Para $A = \begin{bmatrix} \alpha & \beta M \\ \gamma N & \alpha + \delta D \end{bmatrix} \in \Gamma(M, N, D)$, y puesto que D divide MN , se tiene que $\alpha^2 \equiv 1 \pmod{D}$; es decir, α es una raíz cuadrada de 1 módulo D .

Más generalmente, para un orden cualquiera $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$, pondremos $\Gamma(\mathcal{O})$ para designar el grupo de las unidades de norma 1 de \mathcal{O} .

Lema 2.3. Sea $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Z})$ un orden cualquiera. El grupo $\Gamma(\mathcal{O})$ es un grupo de congruencia.

Demostración. Claramente, $\Gamma(\mathcal{O}) \subseteq \Gamma(1, 1, 1) = \mathbf{SL}(2, \mathbb{Z})$. Por otra parte, sea $N \geq 1$ un número entero tal que $\mathcal{O} \supseteq \mathcal{O}(N, N, N)$. Entonces, $\Gamma(\mathcal{O})$ contiene como subgrupo el grupo $\Gamma(N, N, N)$. Pero $\Gamma(N)$ es un subgrupo de $\Gamma(N, N, N)$; luego, $\Gamma(\mathcal{O})$ contiene $\Gamma(N)$ como subgrupo. \square

Ejemplo 2.4. Para todo número entero $N \geq 1$, $\Gamma_0(N)$ es el grupo de las unidades de norma 1 de $\mathcal{O}(1, N, 1)$; es decir, $\Gamma_0(N) = \Gamma(1, N, 1)$.

Observación 2.5. En general, el grupo de las unidades de norma 1 de un orden cualquiera $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$ es conjugado de un grupo de congruencia, puesto que el orden es conjugado de un suborden de $\mathbf{M}(2, \mathbb{Z})$.

Proposición 2.6. Sea $N \geq 3$ un número entero. Los grupos $\Gamma_1(N)$ y $\Gamma(N)$ no son el grupo de las unidades de norma 1 de ningún orden $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$.

Demostración. Las condiciones de congruencia para que una matriz $A := \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ pertenezca a alguno de los

grupos $\Gamma_1(N)$ o $\Gamma(N)$ obligan a que sea $\alpha \in \mathbb{Z}$ y $\alpha \equiv 1 \pmod{N}$. Si un orden $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$ contiene la matriz A de manera que A es una unidad de norma 1 de \mathcal{O} , también contiene la matriz $-A$ como unidad de norma 1; y, en cambio, $-A$ no pertenece a ninguno de los dos grupos $\Gamma_1(N)$, $\Gamma(N)$, puesto que para $N \geq 3$ no es $-1 \equiv 1 \pmod{N}$. \square

En general, el subanillo generado por el grupo de las unidades de norma 1 de un orden \mathcal{O} cualquiera no coincide necesariamente con \mathcal{O} . Interesa, pues, conocer más a fondo la relación entre el orden \mathcal{O} y el subanillo generado por $\Gamma(\mathcal{O})$.

Teorema 2.7. Sean $M, N, d \geq 1$ números enteros tales que d divide MN , y sea $D := \text{mcd}(MN, \text{mcm}(24, d)) = \text{mcm}(\text{mcd}(MN, 24), d)$. Entonces, el subanillo de $\mathbf{M}(2, \mathbb{Q})$ generado por $\Gamma(M, N, d)$ es el orden $\mathcal{O}(M, N, D)$.

Demostración. Haremos la demostración de este teorema por partes. Empezaremos viendo que existe un divisor D de MN , múltiplo de d , tal que el subanillo generado por $\Gamma(M, N, d)$ es el orden $\mathcal{O}(M, N, D)$; y, más adelante, precisaremos el valor de D como el del enunciado.

Puesto que $\Gamma(M, N, d)$ es el grupo de las unidades de norma 1 del orden $\mathcal{O}(M, N, d)$, el subanillo generado por $\Gamma(M, N, d)$ es un subanillo de $\mathcal{O}(M, N, d)$. Recíprocamente, puesto que las matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & M \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ N & 1 \end{bmatrix}, \begin{bmatrix} 1 & M \\ N & 1 + MN \end{bmatrix}$$

pertenecen a $\Gamma(M, N, d)$ y constituyen una \mathbb{Z} -base de $\mathcal{O}(M, N, MN)$, obtenemos que el subanillo generado por $\Gamma(M, N, d)$ es un orden, y que este orden contiene $\mathcal{O}(M, N, MN)$.

Así, para el orden \mathcal{O} generado por $\Gamma(M, N, d)$, se satisfacen las inclusiones $\mathcal{O}(M, N, MN) \subseteq \mathcal{O} \subseteq \mathcal{O}(M, N, d)$. Pero el retículo de subórdenes de $\mathcal{O}(M, N, d)$ que contienen $\mathcal{O}(M, N, MN)$ es isomorfo al retículo de divisores D de MN que son múltiplos de d ; si se quiere, al retículo de divisores del cociente $\frac{MN}{d}$. Y el suborden que corresponde a un divisor D de MN múltiplo de d es el orden $\mathcal{O}(M, N, D)$. Luego, $\mathcal{O} = \mathcal{O}(M, N, D)$, para un cierto divisor D de MN múltiplo de d . \square

Antes de continuar con la demostración del teorema, obtenemos consecuencias de lo ya demostrado.

Corolario 2.8. Sean $M, N \geq 1$ números enteros. El subanillo de $\mathbf{M}(2, \mathbb{Q})$ generado por $\Gamma(M, N, MN)$ es el orden $\mathcal{O}(M, N, MN)$. \square

Ejemplo 2.9. El subanillo generado por $\Gamma_1(N)$ es exactamente $\mathcal{O}(1, N, N)$, puesto que, por un lado, $\Gamma_1(N) \subseteq \mathcal{O}(1, N, N)$ y, por otro, las matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ N & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ N & 1 + N \end{bmatrix}$$

pertenecen a $\Gamma_1(N)$ y forman una \mathbb{Z} -base de $\mathcal{O}(1, N, N)$. En particular, pues, el subanillo generado por $\Gamma_1(N)$ es un orden que tiene como grupo de unidades de norma 1 el grupo $\Gamma(1, N, N)$, que contiene el grupo $\Gamma_1(N)$, estrictamente si $N \geq 3$. Con más precisión, se satisface el resultado siguiente.

Proposición 2.10. Para todo número entero $N \geq 1$, $\Gamma_1(N)$ es un subgrupo normal de $\Gamma(1, N, N)$; el grupo cociente $\Gamma(1, N, N)/\Gamma_1(N)$ es isomorfo al grupo $\mu_2(\mathbb{Z}/N\mathbb{Z})$ de las raíces cuadradas de la unidad del anillo $\mathbb{Z}/N\mathbb{Z}$. En particular, el cociente es un 2-grupo abeliano elemental.

Demostración. Para obtener el resultado, basta observar que la aplicación $g : \Gamma(1, N, N) \rightarrow \mu_2(\mathbb{Z}/N\mathbb{Z})$ definida por la asignación $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \mapsto \alpha$ es un morfismo exhaustivo de grupos, de núcleo $\Gamma_1(N)$. \square

Este resultado se extiende al caso general en la forma siguiente, que usaremos para precisar el valor de D del teorema 2.7.

Lema 2.11. Sean $M, N, d \geq 1$ números enteros tales que d divide MN . Si $\alpha \in \mathbb{Z}$ es tal que $\alpha \in (\mathbb{Z}/MN\mathbb{Z})^*$ y $\alpha^2 \equiv 1 \pmod{d}$, entonces existen números enteros β, γ, δ tales que $\begin{bmatrix} \alpha & \beta M \\ \gamma N & \alpha + \delta d \end{bmatrix} \in \Gamma(M, N, d)$.

Demostración. Puesto que α es inversible módulo MN , existe $\alpha' \in \mathbb{Z}$ tal que $\alpha\alpha' \equiv 1 \pmod{MN}$; en particular, existe $\beta \in \mathbb{Z}$ tal que $\alpha\alpha' = 1 + \beta MN$. Además, puesto que $\alpha^2 \equiv 1 \pmod{d}$, se tiene que $\alpha \equiv \alpha' \pmod{d}$, de manera que existe $\delta \in \mathbb{Z}$ tal que $\alpha' = \alpha + \delta d$. Finalmente, podemos elegir $\gamma = 1$. Entonces, se tiene que $\begin{bmatrix} \alpha & \beta M \\ N & \alpha + \delta d \end{bmatrix} \in \Gamma(M, N, d)$, como queríamos demostrar. \square

Proposición 2.12. Sean $M, N, D, d \geq 1$ números enteros tales que d divide D y D divide MN . Las propiedades siguientes son equivalentes:

- (a) $\mathcal{O}(M, N, D)$ contiene el orden generado por $\Gamma(M, N, d)$.
- (b) $\Gamma(M, N, D) \supseteq \Gamma(M, N, d)$.
- (c) Para todo $\alpha \in (\mathbb{Z}/MN\mathbb{Z})^*$ tal que $\alpha^2 \equiv 1 \pmod{d}$, es $\alpha^2 \equiv 1 \pmod{D}$.

Demostración. La equivalencia de las dos primeras propiedades es inmediata. Veamos que (b) implica (c). Supongamos, pues, que se satisface (b), y sea $\alpha \in (\mathbb{Z}/MN\mathbb{Z})^*$ tal que $\alpha^2 \equiv 1 \pmod{d}$. En virtud del lema anterior, existen

$\beta, \gamma, \delta \in \mathbb{Z}$ tales que $A := \begin{bmatrix} \alpha & \beta M \\ \gamma N & \alpha + \delta d \end{bmatrix} \in \Gamma(M, N, d) \subseteq \Gamma(M, N, D)$; por tanto, es $\delta d \equiv 0 \pmod{D}$ y $1 = \alpha(\alpha + \delta d) - \beta\gamma MN \equiv \alpha^2 \pmod{D}$, como queríamos ver.

Recíprocamente, supongamos que se satisface la propiedad (c), y sea $A := \begin{bmatrix} \alpha & \beta M \\ \gamma N & \alpha + \delta d \end{bmatrix} \in \Gamma(M, N, d)$; entonces, es $\alpha(\alpha + \delta d) - \beta\gamma MN = 1$, de manera que $\alpha \in (\mathbb{Z}/MN\mathbb{Z})^*$, y $\alpha^2 \equiv 1 \pmod{d}$; en consecuencia, de la igualdad $\alpha(\alpha + \delta d) - \beta\gamma MN = 1$ y de la hipótesis (c), obtenemos que es $\delta d \equiv 0 \pmod{D}$, de manera que $A \in \Gamma(M, N, D)$, como queríamos demostrar. \square

Corolario 2.13. Sean $M, N, d \geq 1$ números enteros tales que d divide MN . El subanillo generado por $\Gamma(M, N, d)$ es el orden $\mathcal{O}(M, N, D)$, donde D es el máximo de los divisores D de MN que son múltiplos de d y para los cuales se satisface la propiedad (c) de la proposición 2.12.

Demostración. En virtud de la proposición 2.12, el orden generado por el grupo $\Gamma(M, N, d)$ es la intersección de los órdenes $\mathcal{O}(M, N, D)$ para todos los valores de D para los cuales se satisface (c); y esta intersección corresponde al máximo de los valores de D posibles. \square

Para finalizar la precisión del valor de D del teorema, basta con establecer el resultado siguiente.

Proposición 2.14. Sean $M, N, d \geq 1$ números enteros tales que d divide MN , y sea D el máximo de los divisores positivos de MN para los cuales se satisface la propiedad (c) de la proposición 2.12. Entonces,

$$D = \text{mcd}(MN, \text{mcm}(24, d)) = \text{mcm}(\text{mcd}(MN, 24), d).$$

Demostración. Sea p un número primo cualquiera, y designemos por v_p la valoración p -ádica. Sean $v := v_p(d)$ y $w := v_p(D)$. Puesto que d divide D y D divide MN , debe ser $v \leq w \leq v_p(MN)$.

Sea $\alpha \in (\mathbb{Z}/MN\mathbb{Z})^*$ tal que $\alpha^2 \equiv 1 \pmod{d}$, y supongamos, en primer lugar, que es $p \geq 5$. Puesto que es $\alpha^2 \equiv 1 \pmod{p^v}$, debe ser $\alpha \equiv \pm 1 \pmod{p^v}$. Si fuese $w > v$, la condición $\alpha^2 \equiv 1 \pmod{p^w}$, o equivalentemente, la condición $\alpha \equiv \pm 1 \pmod{p^w}$, no podría deducirse de la $\alpha^2 \equiv 1 \pmod{d}$, puesto que los divisores primos de d distintos de p no aportan ninguna condición; por tanto, ha de ser $w \leq v$.

Análogamente, si fuese $p = 3$ y $v \geq 1$, debe ser $w \leq v$. Pero si $p = 3$ y $v = 0$, y si 3 divide MN , α es inversible módulo 3, de manera que es $\alpha^2 \equiv 1 \pmod{3}$; esto implica que puede ser $w \leq 1$ cualquiera.

Finalmente, consideremos el caso $p = 2$. Si es $v \geq 3$, la condición $\alpha^2 \equiv 1 \pmod{2^v}$ equivale a la condición $\alpha \equiv \pm 1 \pmod{2^{v-1}}$ y, como antes, ha de ser $w \leq v$. Pero si es $v \leq 2$ y si 2 divide MN , la condición $\alpha^2 \equiv 1 \pmod{8}$ se satisface siempre, de manera que puede ser $w \leq 3$ cualquiera, con la condición que 2^w divida MN .

Así, hemos obtenido que, para todo número primo p , es

$$v_p(D) = \begin{cases} v_p(d) = \min\{v_p(MN), v_p(d)\}, & \text{si } p \geq 5, \\ \min\{v_3(MN), \max\{1, v_3(d)\}\}, & \text{si } p = 3, \\ \min\{v_2(MN), \max\{3, v_2(d)\}\}, & \text{si } p = 2; \end{cases}$$

y esto es decir que $D = \text{mcd}(MN, \text{mcm}(24, d))$, como queríamos demostrar. \square

Ejemplo 2.15. El orden generado por $\Gamma_0(N)$ es $\mathcal{O}(1, N, D)$, donde $D := \text{mcd}(N, 24)$. En particular, $\Gamma_0(N) = \Gamma(1, N, 1) = \Gamma(1, N, D)$.

Para finalizar, calcularemos el orden generado por el grupo $\Gamma(N)$.

Proposición 2.16. Para todo un número entero $N \geq 1$, el orden de $\mathbf{M}(2, \mathbb{Q})$ generado por $\Gamma(N)$ es

$$\begin{cases} \mathcal{O}(N, N, N), & \text{si } N \text{ es impar} \\ \mathcal{O}(N, N, 2N), & \text{si } N \text{ es par.} \end{cases}$$

Demostración. Observemos, en primer lugar, que se satisfacen las inclusiones $\Gamma(N) \subseteq \Gamma(N, N, N) \subseteq \mathcal{O}(N, N, N)$, de manera que el subanillo generado por $\Gamma(N)$ es un subanillo de $\mathcal{O}(N, N, N)$.

Por otra parte, las matrices

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1-N & -N \\ N & 1+N \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ N & 1 \end{bmatrix}$$

pertenecen a $\Gamma(N)$ y forman una \mathbb{Z} -base de la subred $\mathcal{O}(N, N, 2N)$, de $\mathcal{O}(N, N, N)$. Por tanto, el subanillo generado por $\Gamma(N)$ es un suborden de $\mathcal{O}(N, N, N)$ que contiene la subred $\mathcal{O}(N, N, 2N)$.

Si N es impar, $\mathcal{O}(N, N, 2N)$ no es un anillo, pero es una subred de índice 2 de $\mathcal{O}(N, N, N)$; por tanto, el subanillo generado por $\Gamma(N)$ es el orden $\mathcal{O}(N, N, N)$.

Si N es par, la subred $\mathcal{O}(N, N, 2N)$ es un suborden de $\mathcal{O}(N, N, N)$. Basta, pues, demostrar que $\Gamma(N) \subseteq \mathcal{O}(N, N, 2N)$. Pero, dada una matriz cualquiera $A := \begin{bmatrix} 1 + \alpha N & \beta N \\ \gamma N & 1 + \delta N \end{bmatrix} \in \Gamma(N)$, $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, y puesto que $\det(A) = 1$, se tiene que $\delta \equiv -\alpha \pmod{N}$, de manera que $A = \begin{bmatrix} 1 + \alpha N & \beta N \\ \gamma N & (1 + \alpha N) - 2\alpha N + \mu N^2 \end{bmatrix}$, con $\alpha, \beta, \gamma, \mu \in \mathbb{Z}$.

Y, puesto que N es par, se tiene que $2N$ divide N^2 , de manera que $A \in \mathcal{O}(N, N, 2N)$, como queríamos demostrar. \square

Análogamente al caso del grupo $\Gamma_1(N)$, tenemos el resultado siguiente, consecuencia del lema 2.11.

Proposición 2.17. *Para todo número entero $N \geq 1$, $\Gamma(N)$ es un subgrupo normal de $\Gamma(N, N, N)$; el grupo cociente $\Gamma(N, N, N)/\Gamma(N)$ es isomorfo al grupo $\mu_2(\mathbb{Z}/N\mathbb{Z})$ de las raíces cuadradas de la unidad del anillo $\mathbb{Z}/N\mathbb{Z}$. En particular, el cociente es un 2-grupo abeliano elemental.* \square

Resumimos en un solo enunciado los resultados obtenidos para los grupos $\Gamma(N)$, $\Gamma_1(N)$ y $\Gamma_0(N)$.

Corolario 2.18.

- (a) *El subanillo de $\mathbf{M}(2, \mathbb{Q})$ generado por $\Gamma_0(N)$ es el orden $\mathcal{O}(1, N, D)$, con $D := \text{mcd}(N, 24)$.*
- (b) *El subanillo de $\mathbf{M}(2, \mathbb{Q})$ generado por $\Gamma_1(N)$ es el orden $\mathcal{O}(1, N, N)$.*
- (c) *El subanillo de $\mathbf{M}(2, \mathbb{Q})$ generado por $\Gamma(N)$ es el orden $\mathcal{O}(N, N, N)$, si N es impar, y el orden $\mathcal{O}(N, N, 2N)$, si N es par.*

Por otra parte, y para estos grupos, las formas ternarias nórnicas asociadas a los órdenes $\mathbb{Z} + 2\mathcal{O}(\Gamma)$ son las formas cuadráticas enteras

$$n_{0,2}(X, Y, Z) = \begin{cases} -D^2Y^2 + 4NXZ, & \text{si } \Gamma = \Gamma_0(N), \\ -N^2Y^2 + 4NXZ, & \text{si } \Gamma = \Gamma_1(N), \\ -N^2Y^2 + 4N^2XZ, & \text{si } \Gamma = \Gamma(N), N \text{ impar}, \\ -4N^2Y^2 + 4N^2XZ, & \text{si } \Gamma = \Gamma(N), N \text{ par}, \end{cases}$$

donde $D := \text{mcd}(N, 24)$ y $\mathcal{O}(\Gamma)$ indica el orden generado por Γ . \square

Observación 2.19. *Supongamos que N es un divisor de 24. Entonces, el orden generado por $\Gamma_0(N)$ coincide con el orden generado por $\Gamma_1(N)$; es el orden $\mathcal{O}(1, N, N)$.*

REFERENCIAS

1. [Sh 71] Shimura, G. (1971), *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten Pub. & Princeton University Press.
2. [Vi 80] Vignéras, M.-F. (1980), *Arithmétique des Algèbres de Quaternions*, Lecture Notes in Mathematics, **800**, Springer.