Traslaciones y retracciones modulares en semigrupos numéricos ⋆

Aureliano M. Robles-Pérez[1] y José Carlos Rosales[2⋆⋆]

[1] Departamento de Matemática Aplicada, Facultad de Ciencias, Universidad de Granada, 18071-Granada, España. arobles@ugr.es
[2] Departamento de Álgebra, Facultad de Ciencias, Universidad de Granada, 18071-Granada, España. jrosales@ugr.es

Resumen. En este trabajo introducimos los conceptos de traslación y retracción modular de semigrupos numéricos. Estas construcciones nos permiten, a partir de un semigrupo numérico dado S, construir nuevos semigrupos numéricos cuyos principales invariantes se pueden calcular explícitamente a partir de los invariantes de S.

Palabras clave: Traslación modular, retracción modular, semigrupo numérico, conjunto de Apéry.

1 Introducción

Sea $\mathbb{N}$ el conjunto de los números enteros no negativos. Un *semigrupo númerico* es un conjunto $S \subseteq \mathbb{N}$ tal que es cerrado para la suma, $0 \in S$ y $\mathbb{N} \setminus S$ es finito (esto es, S es un submonoide de $(\mathbb{N}, +)$ con complemento finito en $\mathbb{N}$).

Si x, y son números enteros, con $y \neq 0$, denotamos por x mód y al resto de la división de x entre y. Sea S un semigrupo numérico, m un elemento no nulo de S y a un entero no negativo cualquiera. Definimos entonces los conjuntos

- $\mathrm{T}(S, a, m) = \{s + as \text{ mód } m \mid s \in S\}$;
- $\mathrm{R}(S, a, m) = \{s - as \text{ mód } m \mid s \in S\}$.

Aunque ambas definiciones son muy similares, mientras que $\mathrm{T}(S, a, m)$ es siempre un submonoide de $(\mathbb{N}, +)$, no ocurre así con $\mathrm{R}(S, a, m)$. Además, $\mathrm{T}(S, a, m)$ es un semigrupo numérico si y sólo si $\mathrm{mcd}(a+1, m) = 1$ (siendo mcd el *máximo común divisor* de un conjunto dado). Sin embargo, $\mathrm{R}(S, a, m)$ es un semigrupo numérico si y sólo si $\mathrm{mcd}\{a - 1, m\} = 1$ más una condición auxiliar (véase Teorema 2). Además, es interesante observar que traslación y retracción son

⋆ Trabajo financiado por la Junta de Andalucía (Grupo de Investigación FQM-343), el MICINN-España (Proyecto de Investigación MTM2010-15595) y Fondos FEDER.
⋆⋆ Investigación financiada parcialmente por Junta de Andalucía/Fondos FEDER (Proyecto de Investigación FQM-5849).

(cuando conservan la estructura de semigrupo numérico) operaciones inversas entre sí en el conjunto de los semigrupos numéricos (véase Teorema 4).

En lo que sigue, dados S, S' semigrupos numéricos, diremos S' es una traslación modular (respectivamente, retracción modular) de S si $S' = \mathrm{T}(S, a, m)$ (respectivamente, $S' = \mathrm{R}(S, a, m)$) para algún $m \in S \setminus \{0\}$ y algún $a \in \mathbb{N}$.

Los elementos de $\mathbb{N} \setminus S$ son los *huecos* de S y al cardinal de dicho conjunto se le denomina *género* de S, denotándose por $\mathrm{g}(S)$. El *número de Frobenius* de S es el mayor entero que no pertenece a S y se denota por $\mathrm{F}(S)$.

Si $A \subseteq \mathbb{N}$ es un conjunto no vacío entonces $\langle A \rangle$ es el submonoide de $(\mathbb{N}, +)$ generado por A, es decir, el conjunto

$$\langle A \rangle = \{\lambda_1 a_1 + \ldots + \lambda_n a_n \mid n \in \mathbb{N} \setminus \{0\},\ a_1, \ldots, a_n \in A, \lambda_1, \ldots, \lambda_n \in \mathbb{N}\}.$$

En [4] se demuestra que $\langle A \rangle$ es un semigrupo numérico si y sólo si $\mathrm{mcd}\{A\} = 1$. También es conocido (véase [4]) que para cada semigrupo numérico S existe un único subconjunto finito $G \subseteq S$ tal que $S = \langle G \rangle$ y ningún subconjunto propio de G genera a S. En tal caso se dice que G es el *sistema minimal de generadores* de S. Al cardinal de G se le conoce como la *dimensión de inmersión* de S y se denota por $\mathrm{e}(S)$.

Si S es un semigrupo numérico y $m \in S \setminus \{0\}$, se define el *conjunto de Apéry de m en S* (véase [1]) como el conjunto $\mathrm{Ap}(S) = \{s \in S \mid s - m \notin S\}$. Es fácil comprobar que $\mathrm{Ap}(S, m) = \{w(0) = 0, w(1), \ldots, w(m-1)\}$, siendo $w(i)$ el menor elemento de S congruente con i módulo m. La importancia de este conjunto radica en que, a partir de él, es posible calcular fácilmente el género y el número de Frobenius de un semigrupo numérico. Además, también permite determinar de manera rápida si un entero pertenece o no al semigrupo.

Acabamos esta introducción señalando que este trabajo es una versión resumida (en concreto, sin demostraciones) de [2] (aceptado para su publicación) y [3] (en proceso de revisión).

2 Traslaciones modulares

En esta sección consideraremos que S es un semigrupo numérico, $m \in S \setminus \{0\}$, $a \in \mathbb{N}$ y $\mathrm{T}(S, a, m) = \{s + as \bmod m \mid s \in S\}$. Como primer resultado tenemos la siguiente proposición.

Proposición 1. *$\mathrm{T}(S, a, m)$ es un submonoide de $(\mathbb{N}, +)$. Además, $\mathrm{T}(S, a, m)$ es un semigrupo numérico si y sólo si $\mathrm{mcd}(a + 1, m) = 1$.*

En la demostración de este este resultado, la primera parte se reduce a realizar simples cálculos. Para la segunda se puede recurrir al siguiente lema.

Lema 1. *Sea A un submonoide de $(\mathbb{N}, +)$. Entonces A es un semigrupo numérico si y sólo si existen $x, y \in A$ tales que $\mathrm{mcd}(x, y) = 1$.*

El siguiente resultado es el que cabría esperar.

Teorema 1. *Si* $\mathrm{Ap}(S,m) = \{w(0), w(1), \ldots, w(m-1)\}$ *y* $\mathrm{mcd}(a+1,m) = 1$ *entonces* $\mathrm{Ap}(\mathrm{T}(S,a,m),m) = \{w(i) + ai \bmod m \mid i \in \{0,1,\ldots,m-1\}\}$.

Veamos un lema muy útil para el cálculo de los invariantes de un semigrupo numérico.

Lema 2. *[4, Lema 2.6, Proposición 2.12]*

1. *Un entero* z *pertenece a* S *si y sólo si* $z \geq w(z \bmod m)$.
2. $\mathrm{F} = \max\{\mathrm{Ap}(S,m)\} - m$.
3. $\mathrm{g}(S) = \frac{1}{m}\left(w(0) + w(1) + \cdots + w(m-1)\right) - \frac{m-1}{2}$.

Combinado los dos resultados anteriores tenemos el siguiente.

Proposición 2. *Sea* $d = \mathrm{mcd}(a,m)$.

1. $\mathrm{g}(\mathrm{T}(S,a,m)) = \mathrm{g}(S) + \frac{m-d}{2}$.
2. *a)* $\mathrm{F}(\mathrm{T}(S,a,m)) = \max\{w(i) + ai \bmod m \mid i \in \{0,1,\ldots,m-1\}\} - m$.
   b) $\mathrm{F}(\mathrm{T}(S,a,m)) \geq \mathrm{F}(S) + a\mathrm{F}(S) \bmod m$.
   c) $\mathrm{F}(\mathrm{T}(S,a,m)) \leq \mathrm{F}(S) + m - d$.
   d) $\mathrm{F}(\mathrm{T}(S,a,m)) = \mathrm{F}(S) + m - d$ *si y sólo si* $a\mathrm{F}(S) \bmod m = m - d$.

Una interesante consecuencia de esta proposición es que, en ciertos casos, el carácter simétrico o pseudo-simétrico de un semigrupo numérico se conserva por traslaciones. Recordemos (véase [4, Lema 2.14, Corolario 4.5]) que un semigrupo numérico S es simétrico (respectivamente, pseudo-simétrico) si y sólo si $2\mathrm{g}(S) = \mathrm{F}(S) + 1$ (respectivamente, $2\mathrm{g}(S) = \mathrm{F}(S) + 2$).

Corolario 1. *Si* $d = \mathrm{mcd}(a,m)$ *y* $a\mathrm{F}(S) \bmod m = m - d$ *entonces*

1. $\mathrm{T}(S,a,m)$ *es simétrico si y sólo si* S *es simétrico.*
2. $\mathrm{T}(S,a,m)$ *es pseudo-simétrico si y sólo si* S *es pseudo-simétrico.*

Antes de ver algunos ejemplos ilustrativos de lo hasta aquí expuesto, un resultado sobre la dimensión de inmersión de una traslación modular.

Proposición 3. *Sea* $\{n_1, n_2, \ldots, n_e\}$ *el sistema de generadores minimales de* S. *Entonces* $\{n_i + an_i \bmod m \mid 1 \leq i \leq e\}$ *está incluido en el sistema de generadores minimales de* $\mathrm{T}(S,a,m)$. *Por tanto,* $\mathrm{e}(S) = e \leq \mathrm{e}(\mathrm{T}(S,a,m))$.

Ejemplo 1. Consideremos el semigrupo numérico $S = \langle 5, 7\rangle$. En este caso se verifica que $\mathrm{e}(S) = 2$, $\mathrm{g}(S) = 12$, $\mathrm{F}(S) = 23$ y $\mathrm{Ap}(S,5) = \{0, 21, 7, 28, 14\}$. De la igualdad $\mathrm{mcd}(4,5) = 1$, se sigue que $\mathrm{T}(S,3,5)$ es también un semigrupo numérico. Además, $\mathrm{Ap}(\mathrm{T}(S,3,5),5) = \{0, 24, 8, 32, 16\}$, de donde se deduce que $\mathrm{T}(S,3,5) = \langle 5, 8\rangle$. Así, $\mathrm{e}(\mathrm{T}(S,3,5)) = 2$, $\mathrm{g}(\mathrm{T}(S,2,4)) = 14$ y $\mathrm{F}(\mathrm{T}(S,2,4)) = 27$. Por tanto, se cumplen las tesis del Teorema 1 y de la Proposición 2 (ítems 1 y 2d) y tenemos un ejemplo en el que se alcanza la igualdad de dimensiones de inmersión en la Proposición 3. Además, S y $\mathrm{T}(S,3,5)$ son simétricos.

Ejemplo 2. Veamos las distintas posibilidades que pueden surgir en el ítem 2 de la Proposición 2. Para ello tomamos el semigrupo numérico $S = \langle 5, 6, 7\rangle$. Entonces $\mathrm{Ap}(S, 5) = \{0, 6, 7, 13, 14\}$ y $\mathrm{F}(S) = 9$.

1. Para $a = 1$ se verifica que $\mathrm{Ap}(\mathrm{T}(S, 1, 5), 5) = \{0, 7, 9, 16, 18\}$. Por tanto, $\mathrm{F}(\mathrm{T}(S, 1, 5), 5) = 13$ y tenemos igualdades en las cotas de los ítems 2b y 2c (y, consiguientemente, se verifica el ítem 2d).
2. Para $a = 2$ se tiene que $\mathrm{Ap}(\mathrm{T}(S, 2, 5), 5) = \{0, 8, 11, 14, 17\}$. En este caso $\mathrm{F}(\mathrm{T}(S, 2, 5), 5) = 12$ y se alcanza la cota del ítem 2b pero no la del 2c.
3. Para $a = 3$ se deduce que $\mathrm{Ap}(\mathrm{T}(S, 2, 5), 5) = \{0, 9, 8, 17, 16\}$. Se sigue que $\mathrm{F}(\mathrm{T}(S, 3, 5), 5) = 12$ y, por tanto, las cotas de los ítems 2b y 2c son estrictas.

Ejemplo 3. Siguiendo con el ejemplo anterior, como es fácil comprobar, tenemos que $\mathrm{T}(S, 2, 5) = \langle 5, 8, 11, 14, 17\rangle$. Por tanto, vemos que la cota dada para la dimensión en la Proposición 3 puede ser estricta.

3 Retracciones modulares

En esta sección S es un semigrupo numérico, $m \in S \setminus \{0\}$, $a \in \mathbb{N}$ y consideramos el conjunto $\mathrm{R}(S, a, m) = \{s - as \bmod m \mid s \in S\}$. A partir de lo visto en la sección anterior, podría pensarse que, si $\mathrm{mcd}(a - 1, m) = 1$, entonces $\mathrm{R}(S, a, m)$ es un semigrupo numérico. Sin embargo, esto no es así en general.

Ejemplo 4. Sea el semigrupo numérico $S = \langle 4, 5\rangle$. Si $a = 2$ y $m = 4$ es claro que $\mathrm{mcd}(1, 4) = 1$. Sin embargo $3 \in \mathrm{R}(S, 2, 4)$ y $6 \notin \mathrm{R}(S, 2, 4)$. Se concluye que $\mathrm{R}(S, 2, 4)$ no es cerrado para la suma.

Ejemplo 5. Tomemos de nuevo el semigrupo numérico $S = \langle 4, 5\rangle$. Para $a = 2$ y $m = 9$ es claro que $\mathrm{mcd}(1, 9) = 1$. Pero $4 - 2 \times 4 \bmod 9 = -4$, de donde concluimos que $\mathrm{R}(S, 2, 4)$ no es un subconjunto de $\mathbb{N}$.

A la vista de estos dos ejemplos, comprobamos que la situación no es la misma que para las traslaciones modulares. En el siguiente resultado aparecen las condiciones que permiten que una retracción modular de un semigrupo numérico proporcione otro semigrupo numérico.

Teorema 2. $\mathrm{R}(S, a, m)$ *es un semigrupo numérico si y sólo si se satisfacen las dos condiciones siguientes:*

1. $\mathrm{mcd}(a - 1, m) = 1$;
2. *si* $s_1, s_2 \in S$ *y* $as_1 \bmod m + as_2 \bmod m \geq m$ *entonces* $s_1 + s_2 - m \in S$.

El conjunto de Apéry nos permite simplificar la segunda condición.

Corolario 2. *Si* $\mathrm{Ap}(S,m)=\{w(0),w(1),\ldots,w(m-1)\}$ *entonces* $\mathrm{R}(S,a,m)$ *es un semigrupo numérico si y sólo si se satisfacen las dos condiciones siguientes:*

1. $\mathrm{mcd}(a-1,m)=1$;
2. *si* $i,j\in\{1,\ldots,m-1\}$ *y* $w(i)+w(j)\in\mathrm{Ap}(S,m)$ *entonces* $ai \bmod m + aj \bmod m < m$.

Una vez hemos determinado cuándo las retracciones proporcionan semigrupos numéricos, hagamos un estudio paralelo al realizado para las traslaciones. Empezamos viendo los sistemas de generadores.

Proposición 4. *Supongamos que* $\mathrm{R}(S,a,m)$ *es un semigrupo numérico.*

1. *Si* m *no es un generador minimal de* S *entonces tampoco es un generador minimal de* $\mathrm{R}(S,a,m)$.
2. *Si* $\{n_1,\ldots,n_p\}$ *es un sistema de generadores de* S *entonces un sistema de generadores de* $\mathrm{R}(S,a,m)$ *es* $\{n_1-an_1 \bmod m,\ldots,n_p-an_p \bmod m\}$.

Consecuentemente, $\mathrm{e}(\mathrm{R}(S,a,m))\leq \mathrm{e}(S)$.

Para calcular el conjunto de Apéry de una retracción modular necesitamos el siguiente lema.

Lema 3. *Si* $\mathrm{Ap}(S,m)=\{w(0),w(1),\ldots,w(m-1)\}$ *y* $\mathrm{mcd}(a-1,m)=1$ *entonces se verifica que:*

1. *Si* $x\in\mathrm{R}(S,a,m)$ *entonces* $x+m\in\mathrm{R}(S,a,m)$.
2. *Para cada* $j\in\{0,\ldots,m-1\}$ *existe un único* $i\in\{0,\ldots,m-1\}$ *tal que* $(w(i)-ai \bmod m)\equiv j \pmod m$.
3. $\mathrm{R}(S,a,m)=\{w(i)-ai \bmod m \mid i\in\{0,\ldots,m-1\}\}+\langle m\rangle$.

Observación 1. En el lema previo no hemos exigido que $\mathrm{R}(S,a,m)$ sea un semigrupo numérico. Sin embargo se puede ver que, si $\mu(j)$ es el menor elemento de $\mathrm{R}(S,a,m)$ congruente con $j\in\{0,\ldots,m-1\}$, entonces $\mu(j)+m\mathbb{N}\subseteq\mathrm{R}(S,a,m)$. Es decir, se verifica una de las condiciones más destacables de los conjuntos de Apéry aun cuando $\mathrm{R}(S,a,m)$ no sea un semigrupo numérico.

En el siguiente teorema, además de determinar el conjunto de Apéry, obtenemos un nuevo criterio para comprobar cuándo una retracción modular conduce a un semigrupo numérico. Usaremos el semigrupo numérico modular $\mathrm{M}(p,q)=\{x\in\mathbb{N}\mid px \bmod q\leq x\}$, donde $p,q\in\mathbb{N}$ y $q\neq 0$ (véase [5]).

Teorema 3. *Sea* S *un semigrupo numérico con sistema minimal de generadores* $\{n_1,\ldots,n_p\}$ *y* $\mathrm{Ap}(S,m)=\{w(0),w(1),\ldots,w(m-1)\}$. *Supongamos que* $\mathrm{mcd}(a-1,m)=1$ *y* $\{n_1,\ldots,n_p\}\subseteq\mathrm{M}(a,m)$. *Entonces, si* $\overline{S}$ *es el submonoide de* $(\mathbb{N},+)$ *generado por* $\{n_1-an_1 \bmod m,\ldots,n_p-an_p \bmod m\}$, *se verifica que* $\overline{S}$ *es un semigrupo numérico con* $m\in\overline{S}$. *Además:*

1. $\mathrm{R}(S,a,m) \subseteq \overline{S}$.
2. $\mathrm{R}(S,a,m)$ *es un semigrupo numérico si y sólo si* $\mathrm{R}(S,a,m) = \overline{S}$.
3. $\mathrm{R}(S,a,m)$ *es un semigrupo numérico si y sólo si* $\mathrm{Ap}(\overline{S},m)$ *es igual a* $\{w(i) - ai \bmod m \mid i \in \{0,\dots,m-1\}\}$.

En particular, si $\mathrm{R}(S,a,m)$ *es un semigrupo numérico entonces se cumple que* $\mathrm{Ap}(\mathrm{R}(S,a,m),m) = \{w(i) - ai \bmod m \mid i \in \{0,\dots,m-1\}\}$.

Combinando este teorema con el Lema 2 tenemos el siguiente resultado sobre el género de una traslación modular.

Proposición 5. *Si* $\mathrm{R}(S,a,m)$ *es un semigrupo numérico y* $\mathrm{mcd}(a,m) = d$ *entonces* $\mathrm{g}(\mathrm{R}(S,a,m)) = \mathrm{g}(S) - \frac{m-d}{2}$.

Veamos algunos ejemplos que clarifiquen las ideas expuestas en esta sección. Primero comprobemos que las condiciones del Teorema 2 son independientes.

Ejemplo 6. Sea el semigrupo numérico $S = \langle 2,3\rangle$. Si $m = 5$ y $a = 2$ entonces $\mathrm{mcd}(2-1,5) = 1$ y, sin embargo, $(2\times 2) \bmod 5 = (2\times 4) \bmod 5 = 7 \geq 5$ y $2+4-7 = -1 \notin S$. Por otro lado, $\mathrm{R}(S,2,5)$ no es semigrupo numérico ya que $2-(2\times 2) \bmod 5 = -2 \notin \mathbb{N}$.

Si $m = 4$ and $a = 3$, mediante cálculos directos comprobamos la segunda condición. Pero $\mathrm{mcd}(3-1,4) = 2 \neq 1$. En este caso $\mathrm{R}(S,3,4) = 2\mathbb{N}$, que no es un semigrupo numérico (aunque sí un submonoide de $(\mathbb{N},+)$).

Ahora aplicamos el Teorema 3 para determinar si una retracción modular es un semigrupo numérico.

Ejemplo 7. Sea el semigrupo numérico $S = \langle 4,5,7\rangle$. Si consideramos $m = 5$ entonces $\mathrm{Ap}(S,5) = \{0,11,7,8,4\}$.

1. Si $a = 2$, $\overline{S} = \langle 4-(2\times 4) \bmod 5, 5-(2\times 5) \bmod 5, 7-(2\times 7) \bmod 5\rangle = \langle 1,5,3\rangle = \langle 1\rangle = \mathbb{N}$. Así, es claro que $\mathrm{Ap}(\overline{S},5) = \{0,1,2,3,4\}$ y, por otro lado, tenemos que $\{0-(2\times 0) \bmod 5, 11-(2\times 11) \bmod 5, 7-(2\times 7) \bmod 5, 8-(2\times 8) \bmod 5, 4-(2\times 4) \bmod 5\} = \{0,9,3,7,1\}$. Concluimos que $\mathrm{R}(S,2,5)$ no es un semigrupo numérico.
2. Si $a = 3$, $\overline{S} = \langle 4-(3\times 4) \bmod 5, 5-(3\times 5) \bmod 5, 7-(3\times 7) \bmod 5\rangle = \langle 2,5,6\rangle = \langle 2,5\rangle$. Tenemos que $\mathrm{Ap}(\overline{S},5) = \{0,6,2,8,4\}$ y, además, que $\{0-(3\times 0) \bmod 5, 11-(3\times 11) \bmod 5, 7-(3\times 7) \bmod 5, 8-(3\times 8) \bmod 5, 4-(3\times 4) \bmod 5\} = \{0,8,6,4,2\}$. Por consiguiente, $\mathrm{R}(S,3,5)$ sí es un semigrupo numérico. Además, $\mathrm{R}(S,3,5) = \langle 2,5\rangle$.
3. Si $a = 4$, $\overline{S} = \langle 4-(4\times 4) \bmod 5, 5-(4\times 5) \bmod 5, 7-(4\times 7) \bmod 5\rangle = \langle 3,5,4\rangle$. Ahora tenemos que $\mathrm{Ap}(\overline{S},5) = \{0,6,7,3,4\} = \{0-(4\times 11) \bmod 5, 11-(4\times 11) \bmod 5, 7-(4\times 7) \bmod 5, 8-(4\times 8) \bmod 5, 4-(4\times 4) \bmod 5\}$. Por tanto, $\mathrm{R}(S,4,5)$ también es un semigrupo numérico. Concretamente, $\mathrm{R}(S,4,5) = \langle 3,4,5\rangle$.

Ejemplo 8. Continuando con el ejemplo anterior, aplicando la Proposición 5,

1. de $\mathrm{g}(\mathrm{R}(S,3,5)) = \mathrm{g}(\langle 2,5\rangle) = \frac{2\times 5-2-5+1}{2} = 2$, se sigue $\mathrm{g}(S) = 2+\frac{5-1}{2} = 4$;
2. y, por tanto, $\mathrm{g}(\mathrm{R}(S,4,5)) = 4-\frac{5-1}{2} = 2$.

Por otra parte, $\mathrm{e}(S) = \mathrm{e}(\mathrm{R}(S,4,5)) = 3 > 2 = \mathrm{e}(\mathrm{R}(S,3,5))$. De esta forma, queda probado que la cota de la Proposición 4 se puede alcanzar en algunos casos y es estricta en otros.

3.1 Familias de semigrupos numéricos retractables

Puesto que no siempre una retracción modular es un semigrupo numérico, es interesante hallar familias de semigrupos numéricos para las que sí lo son. Veamos dos casos.

Empezamos viendo los semigrupos numéricos cuya retracción es justamente $\mathbb{N}$. Necesitaremos el siguiente lema sobre la "unicidad" de las retracciones.

Lema 4. *Sean S_1, S_2 semigrupos numéricos, $m \in (S_1 \cap S_2)\setminus\{0\}$ y $a \in \mathbb{N}$ tales que $\mathrm{R}(S_1,a,m)$ y $\mathrm{R}(S_2,a,m)$ son semigrupos numéricos. Entonces $S_1 = S_2$ si y sólo si $\mathrm{R}(S_1,a,m) = \mathrm{R}(S_2,a,m)$.*

Proposición 6. *$\mathrm{R}(S,a,m) = \mathbb{N}$ si y sólo si $S = \mathrm{M}(a,m)$.*

Recordemos que $\mathrm{m}(S)$ (la *multiplicidad* de S) es el menor elemento no nulo de S y que, por la definición de $\mathrm{Ap}(S,\mathrm{m}(S))$, siempre se verifica que $\mathrm{e}(S) \leq \mathrm{m}(S)$. Nos interesamos ahora por los semigrupos numéricos S que satisfacen la igualdad $\mathrm{e}(S) = \mathrm{m}(S)$, los llamados de *máxima dimensión de inmersión.*

Proposición 7. *Sea S un semigrupo numérico de máxima dimensión de inmersión y multiplicidad m. Sea $a \in \mathbb{N}$ tal que $\mathrm{mcd}(a-1,m) = 1$. Entonces $\mathrm{R}(S,a,m)$ es un semigrupo numérico.*

El concepto de máxima dimensión de inmersión nos permite dar un nuevo criterio para comprobar cuándo una retracción es un semigrupo numérico.

Proposición 8. *Sean S un semigrupo numérico. Sean $m \in S\setminus\{0\}$ y $a \in \mathbb{N}$ tales que $\mathrm{mcd}(a-1,m) = 1$. Si $\tilde{S} = (m + \mathrm{R}(S,a,m)) \cup \{0\}$ entonces:*

1. *$\tilde{S}$ es un semigrupo numérico.*
2. *$\mathrm{R}(S,a,m)$ es un semigrupo numérico si y sólo si $\tilde{S}$ es un semigrupo numérico de máxima dimensión de inmersión y multiplicidad m.*

4 Traslaciones y retracciones

Para terminar este trabajo, veremos que, en un cierto sentido, las traslaciones y retracciones modulares son operaciones inversas en el conjunto de los semigrupos numéricos. Para obtener el resultado, son necesarios dos lemas.

Lema 5. *Sea S un semigrupo numérico. Sean $m \in S \setminus \{0\}$ y $a \in \mathbb{N}$ tales que* $\mathrm{mcd}(a-1, m) = 1$. *Entonces* $S = \{x + au \bmod m \mid x \in \mathrm{R}(S, a, m)\}$, *siendo $u \in \mathbb{N}$ tal que* $(1-a)u \equiv 1 \pmod{m}$. *Además, si* $\mathrm{R}(S, a, m)$ *es un semigrupo numérico entonces* $\mathrm{T}(\mathrm{R}(S, a, m), au, m) = S$.

Lema 6. *Sea S un semigrupo numérico. Sean $m \in S \setminus \{0\}$ y $a \in \mathbb{N}$ tales que* $\mathrm{mcd}(a+1, m) = 1$. *Entonces* $S = \mathrm{R}(\mathrm{T}(S, a, m), au, m)$, *siendo $u \in \mathbb{N}$ tal que* $(1+a)u \equiv 1 \pmod{m}$.

Podemos enunciar ya el resultado prometido.

Teorema 4. *Sean S, B dos semigrupos numéricos. Sean $m \in (S \cap B) \setminus \{0\}$ y $a, b \in \mathbb{N}$ tales que* $(b+1)(1-a) \equiv 1 \pmod{m}$. *Entonces* $\mathrm{R}(S, a, m) = B$ *si y sólo si* $S = \mathrm{T}(B, b, m)$.

Terminamos con una aplicación de este teorema.

Ejemplo 9. Consideramos el semigrupo numérico $B = \langle 5, 6\rangle$ y nos planteamos determinar el conjunto X formado por todos los semigrupos numéricos S que satisfacen la igualdad $\mathrm{R}(S, a, 5) = B$ para algún $a \in \mathbb{N}$.

Sabemos, por el Teorema 4, que X estará formado por aquellos semigrupos numéricos S que satisfagan la igualdad $S = \mathrm{T}(B, b, 5)$ para algún $b \in \mathbb{N}$. Además, por la Proposición 1, es necesario que $\mathrm{mcd}(b+1, 5) = 1$. Por tanto, podemos concluir que $X = \{\mathrm{T}(B, 0, 5), \mathrm{T}(B, 1, 5), \mathrm{T}(B, 2, 5), \mathrm{T}(B, 3, 5)\} = \{\langle 5, 6\rangle, \langle 5, 7\rangle, \langle 5, 8, 19\rangle, \langle 5, 9, 13\rangle\}$.

Referencias

[1] R. Apéry. Sur les branches superlinéaires des courbes algébriques. *C. R. Acad. Sci. Paris*, 222:1198–1200, 1946.

[2] A. M. Robles-Pérez and José Carlos Rosales. Modular translations on numerical semigroup. *Semigroup Forum*, DOI 10.1007/s00233-012-9372-8.

[3] A. M. Robles-Pérez and José Carlos Rosales. Modular retractions of numerical semigroup. En proceso de revisión.

[4] J. C. Rosales and P. A. García-Sánchez. *Numerical semigroups. Developments in Mathematics, vol. 20.* Springer, New York, 2009.

[5] J.C. Rosales, P.A. García-Sánchez, and J.M. Urbano-Blanco. Modular Diophantine inequalities and numerical semigroups. *Pacific J. Math.*, 218:379–398, 2005.