Elementos notables

Pedro A. García Sánchez

Un *semigrupo numérico* es un conjunto de enteros cerrado para la suma, que contiene al cero, y cuyo complemento en $\mathbb{N}$ es finito ($\mathbb{N}$ es el conjunto de enteros no negativos). La condición de complemento finito es equivalente a imponer que el máximo común divisor de sus elementos sea uno. El hecho de que se emplee la palabra semigrupo para denotar estos conjuntos ha levantado últimamente cierta controversia, ya que estos conjuntos son de por sí monoides. Es por ello que algunos autores prefieren usar el término monoide numérico.

Dado un submonoide S de $\mathbb{N}$ (respecto de la suma), podemos considerar el conjunto $\{s/d : s \in S\}$, con d el máximo común divisor de los elementos de S, el cual resulta tener complemento finito en $\mathbb{N}$, y por tanto es un semigrupo numérico. De esta manera se tiene que cualquier submonoide de $\mathbb{N}$ es isomorfo a un (único) semigrupo numérico.

Es probable que los semigrupos numéricos apareciesen al estudiar soluciones no negativas y enteras de una ecuación diofántica lineal. Dados enteros positivos y relativamente primos $a_1, \ldots, a_n$, el conjunto de elementos $b \in \mathbb{N}$ tales que $a_1x_1 + \cdots + a_nx_n = b$ tiene al menos una solución entera no negativa es un semigrupo numérico. De hecho, uno de los primeros problemas relacionado con semigrupos numéricos fue determinar, en términos de $a_1, \ldots, a_n$, cuál es el mayor entero para el que no existe una solución de la anterior ecuación. Éste se conoce como el problema de Frobenius, y parece ser que Frobenius lo propuso en una de sus clases.

Generadores, una primera opción para representar un semigrupo

El conjunto S de enteros para los que existe una solución entera y no negativa de $a_1x_1 + \cdots + a_nx_n = b$ puede ser expresado como $\{a_1x_1 + \cdots + a_nx_n : x_1, \ldots, x_n \in \mathbb{N}\}$, o incluso usando una notación más abreviada como $\langle a_1, \ldots, a_n\rangle$. Decimos que $\{a_1, \ldots, a_n\}$ es un *sistema de generadores* de S, o simplemente que $\{a_1, \ldots, a_n\}$ genera a S. Si ningún subconjunto propio de $\{a_1, \ldots, a_n\}$ genera a S, entonces es un sistema *minimal* de generadores de S. Como S cumple la propiedad cancelativa para la suma ($a + b = a + c$ implies $b = c$), S admite un único sistema minimal de generadores, que es $(S \setminus \{0\}) \setminus ((S \setminus \{0\}) + (S \setminus \{0\}))$, y que además es finito. La cardinalidad de este conjunto es conocida como la *dimensión de inmersión* de S (ya comentaremos después el por qué de esta extraña elección para denotar esa cantidad).

Nótese que si S está generado por $\{a_1, \dots, a_n\}$, entonces el máximo común divisor de $\{a_1, \dots, a_n\}$ es uno (y al revés, si $\{a_1, \dots, a_n\}$ es un conjunto de enteros con máximo común divisor uno, entonces el submonoide de $\mathbb{N}$ generado por $\{a_1, \dots, a_n\}$ es un semigrupo numérico).

Multiplicidad, número de Frobenius, huecos y tipo (Cohen-Macaulay)

Tal y como hemos mencionado antes, se le atribuye a Frobenius el problema de determinar una fórmula para el entero más grande para el que no existe solución entera y no negativa de la ecuación $a_1x_1 + \cdots + a_nx_n = b$. Con nuestra notación, esto equivale a encontrar $\max(\mathbb{Z} \ S)$, con $S = \langle a_1, \dots, a_n \rangle$ ($\mathbb{Z}$ es el conjunto de los números enteros). Es por esto que a esa cantidad se le conoce como el *número de Frobenius* de S. Si g es el número de Frobenius de S, entonces $g + (\mathbb{N} \ \{0\}) \subset S$, y en particular, $g + (S \ \{0\}) \subseteq S$. Los enteros que no están en S y verifican esta condición se denominan *pseudo-números de Frobenius* de S, y su cardinalidad es el *tipo* (Cohen-Macaulay) de S.

Dado un semigrupo numérico S, podemos definir en $\mathbb{Z}$ la siguiente relación de orden: $a \leq_S b$ si $b - a \in S$. El conjunto de pseudo-números de Frobenius coincide con el conjunto de elementos maximales de $\mathbb{Z} \ S$ respecto de este orden.

A los enteros positivos que no están en S se les llama *saltos* (o huecos) de S, y su cardinalidad es el *género* (o grado de singularidad) de S. Si g es el número de Frobenius de S, algunos autores usan el nombre *hueco* para aquellos enteros x tales que $x \notin S$ y $g - x \notin S$. Todo hueco es un salto, pero puede haber saltos que no son huecos.

El entero positivo más pequeño que pertenece a un semigrupo numérico es conocido como su *multiplicidad*. La multiplicidad de semigrupo numérico siempre está en su sistema minimal de generadores y es además una cota superior para su dimensión de inmersión. Esto se debe a que dos generadores minimales no pueden ser congruentes módulo la multiplicidad.

Conjuntos de Apéry, sin duda la mejor herramienta para hacer cálculos en un semigrupo numérico

Hemos comentado antes que dos generadores minimales de un semigrupo numérico no pueden ser congruentes módulo la multiplicidad, y claramente lo mismo ocurre respecto de cualquier elemento no nulo del semigrupo. Usando esa idea, podemos considerar, para un elemento no nulo n de un semigrupo numérico S, el conjunto $\{w_0, \dots, w_{n-1}\}$ donde w_i es el menor elemento en S congruente con i módulo n. Se puede comprobar fácilmente que este conjunto es precisamente $\{s \in S : s - n \notin S\}$. Apéry fue el primero en explotar esta idea, y es por eso que este conjunto se conoce como el *conjunto de Apéry* de n en S. Si n es la multiplicidad de S, a veces a este conjunto se le llama una base estándar de S. Como este conjunto aparece casi por doquier en nuestro estudio de semigrupos numéricos, vamos a introducir una notación para referirnos a él: $\mathrm{Ap}(S, n)$.

Los conjuntos de Apéry tienen muchas y muy buenas propiedades. Enumeramos a continuación algunas de ellas, aunque más adelante aparecerán otras no menos importantes.

- Todo entero x se puede expresar de forma única como $x = kn + w$, para algún $k \in \mathbb{Z}$ y $w \in \mathrm{Ap}(S, n)$. Además, $x \in S$ si y sólo si $k \geq 0$.
- Por tanto, si queremos saber si x pertenece a S, buscamos $w \in \mathrm{Ap}(S, n)$ tal que $x \equiv w \mod n$; $x \in S$ si y sólo si $w \leq x$.
- El número de Frobenius de S es $\max(\mathrm{Ap}(S, n)) - n$.
- Podemos generalizar lo anterior de la siguiente forma. Un entero g es un pseudo-número de Frobenius de S si y sólo si $g + n$ es maximal en $\mathrm{Ap}(S, n)$ con respecto a $\leq_S$. Así el tipo de S es el cardinal del conjunto $\mathrm{Maximales}_{\leq_S}(\mathrm{Ap}(S, n))$.
- La fórmula de Selmer establece que el género de S (número de saltos) es $\frac{1}{n} \sum_{w \in \mathrm{Ap}(S,n)} w - \frac{n-1}{2}$.

Por tanto, el conocimiento del conjunto de Apéry de un semigrupo numérico, respecto de cualquiera de sus elementos no nulos, resuelve el problema de pertenencia, determina el número de Frobenius del semigrupo, sus pseudo-números de Frobenius, su tipo y género.

El conjunto de semigrupos numéricos con multiplicidad fija

Un conjunto $X \subseteq \mathbb{N}$ es un *sistema completo módulo* un entero positivo m si la cardinalidad de X es m y para cada $i \in \{1, \ldots, m\}$ existe $x_i \in X$ congruente con i módulo m. Por definición, dado un semigrupo numérico S y $m \in S \setminus \{0\}$, $\mathrm{Ap}(S, m)$ es un sistema completo módulo m. Sin embargo, no todo sistema completo módulo un entero positivo m es el conjunto de Apéry de un semigrupo numérico. Hace falta imponer algunas restricciones más. La primera es que $x_0 = 0$, y además se tiene que verificar que $x_i + x_j = x_{(i+j) \mod m} + km$ para algún entero no negativo k (ya que $x_i + x_j$ tiene que estar en el semigrupo). Obsérvese también que si X es el conjunto de Apéry de S en m, entonces $X \cup \{m\}$ genera a S y por tanto lo determina completamente (recuérdense las buenas propiedades de los conjuntos de Apéry). Si uno quiere usar los conjuntos de Apéry para describir un semigrupo numérico, la elección más económica es tomar el conjunto de Apéry asociado a la multiplicidad, ya que éste es el menor entero positivo del semigrupo.

Los elementos en dicho conjunto de Apéry se pueden codificar de la siguiente manera. Sea S un semigrupo numérico y sea m su multiplicidad. Si $\mathrm{Ap}(S, m) = \{w_0 = 0, w_1, \ldots, w_{m-1}\}$ con w_i congruente con i módulo m, entonces $w_i = k_i m + i$ para algún entero no negativo k_i. Como m es la multiplicidad y $m \leq w_i \in S$, si $i \neq 0$, se tiene $k_i \geq 1$. La condición $w_i + w_j = w_{(i+j) \mod m} + km$ se puede reescribir como $(k_i + k_j)m + i + j = k_{(i+j) \mod m} m + (i + j) \mod m + km$. Como $i + j = \lfloor \frac{i+j}{m} \rfloor m + (i + j) \mod m$, se llega a $(k_1, \ldots, k_{m-1})$ ($k_0 = 0 = w_0$ no proporciona información) es una solución no negativa del sistema de desigualdades

$$\begin{cases} x_i & \geq 1, & 1 \leq i \leq m-1, \\ x_i + x_j + \lfloor \frac{i+j}{m} \rfloor & \geq x_{(i+j) \mod m}, & 1 \leq i \leq j \leq m-1, i+j \neq m. \end{cases}$$

Además, si $(k_1, \ldots, k_{m-1}) \in \mathbb{N}^{m-1}$ es solución de este sistema de desigualdades, entonces

$$S = \langle m, k_1 m + 1, k_2 m + 2, \ldots, k_{m-1} m + m - 1 \rangle$$

es un semigrupo numérico de multiplicidad m y con $\mathrm{Ap}(S, m) = \{0, k_1 m + 1, k_2 m + 2, \ldots, k_{m-1} m + m - 1\}$. Sea $\mathcal{T}(m)$ el conjunto de elementos de $\mathbb{N}^{m-1}$ que son solución de las desicualdades descritas arriba. Entonces $\mathcal{T}(m)$ es el ideal de un monoide conmutativo finitamente generado (el semigrupo afín normal de soluciones del sistema de desigualdades homogéneo asociado). Por tanto este conjunto puede ser descrito mediante un conjunto finito de elementos de $\mathbb{N}^{m-1}$, y es biyectivo con el conjunto de todos los semigrupos numéricos de multiplicidad m. El cono descrito por ([J. C. Rosales, P. A. García-Sánchez, J. I. García-García and M. B. Branco, Systems of inequalities and numerical semigroups, J. Lond. Math. Soc. 65(3) (2002), 611–623]) ya fue utilizado en 1987 por Kunz para hacer una clasificación de los semigrupos numéricos.

Saltos fundamentales, una alternativa para representar un semigrupo numérico

El número de Frobenius de $\mathbb{N}$ es -1. Si S es un semigrupo numérico distinto de $\mathbb{N}$, entonces el número de Frobenius de S es un entero positivo, y lo mismo ocurre con sus pseudo-números de Frobenius, y por tanto son todos ellos saltos de S. Hay 1156012 semigrupos numérico con número de Frobenius 39. Esto deja claro que el número de Frobenius de un semigrupo numérico no se puede utilizar para describirlo de forma única (se puede probar que los únicos semigrupos numéricos que quedan completamente determinados por su número de Frobenius son aquellos con número de Frobenius en el conjunto $\{-1, 1, 2, 3, 4, 6\}$). De entre los 1156012 semigrupos numéricos con número de Frobenius 39, hay 227 con conjunto de pseudo-números de Frobenius $\{39\}$. Por tanto, el conjunto de pseudo-números de Frobenius es una mala elección para describir semigrupos numéricos unívocamente.

Claramente el conjunto de saltos de S determina de forma única a S. Pero precisamente lo que queremos evitar es usar todo ese conjunto, ya que en él existe normalmente mucha información redundante. Esto se debe a que si $x \mid y$ (x divide a y) e y es un salto de S, entonces x también tiene que ser un salto de S. Por tanto, de entre los saltos de S sólo necesitamos aquellos que son maximales respecto de la división. Éstos son conocidos como *saltos fundamentales* de S, y determinan de forma unívoca a S. Se tiene así que x es un salto fundamental de S si y sólo si $x \notin S$ y $\{2x, 3x\} \subset S$.

Sea X un subconjunto no vacío de enteros positivos. Denotemos por $\mathrm{D}(X)$ el conjunto de divisores positivos de los elementos de X. Si X es el conjunto de saltos fundamentales de

S, entonces $S = \mathbb{N} \setminus \mathrm{D}(X)$. Suponiendo que g sea el número de Frobenius de S (nótese que $g = \max X$), se puede demostrar que

$$\left\lceil \frac{g}{6} \right\rceil \leq |X| \leq \left\lceil \frac{g}{2} \right\rceil .$$

Existen enteros positivos g para los que no hay semigrupos numéricos alcanzando la cota inferior, mientras que la superior siempre se alcanza con $\{0, g+1, \rightarrow\}$.

Los sobre-semigrupos de un semigrupo numérico

Los generadores minimales de un semigrupo numérico S se pueden caracterizar como aquellos elementos $n \in S$ para los cuales el conjunto $S \setminus \{n\}$ es de nuevo un semigrupo numérico. Dualizando esta idea, ¿que enteros $x \notin S$ verifican que $S \cup \{x\}$ sea un semigrupo numérico? Si $S \cup \{x\}$ es un semigrupo numérico, entonces

- $kx \in S$ para cualquier k entero mayor que uno, a saber, $\{2x, 3x\} \subset S$, y
- $x + (S \setminus \{0\}) \subseteq S$.

Por tanto, el elemento x tiene que ser a la vez un pseudo-número de Frobenius y un salto fundamental de S. Estos saltos son conocidos como *saltos especiales* de S, y son aquellos saltos fundamentales que son maximales respecto de $\leq_S$.

Usando esta idea es fácil construir de forma recursiva el conjunto de todos los semigrupos numéricos que contienen a un semigrupo numérico dado S. Empezamos con el propio S y calculamos sus saltos especiales. Si estos saltos son $\{g_1, \ldots, g_t\}$ (este conjunto es no vacío siempre que S no sea todo $\mathbb{N}$, pues en ese caso el número de Frobenius de S es un salto especial). Repetimos el proceso con $S \cup \{g_1\}, \ldots, S \cup \{g_t\}$ hasta que alcancemos $\mathbb{N}$.

Si nuestro semigrupo viene dado por sus saltos fundamentales (o simplemente los tenemos calculados) el proceso se puede acelerar teniendo en cuenta la siguiente propiedad. Si X es el conjunto de saltos fundamentales de S e Y es el conjunto de saltos fundamentales de $S \cup \{x\}$ para algún $x \in X$, entonces

$$Y = (X \setminus \{x\}) \cup \left\{ \frac{x}{p} : p \text{ un primo que divide a } x \text{ y } \frac{x}{p} \notin \mathrm{D}(X \setminus \{x\}) \right\}.$$

Consideremos el semigrupo $S = \mathbb{N} \setminus \mathrm{D}(5, 6)$. Tenemos que 5 es primo y $6 = 2 \cdot 3$, y ambos are maximales en $\{5, 6\}$ respecto de $\leq_S$. Por tanto nuestro semigrupo tiene dos "hijos": $\mathbb{N} \setminus \mathrm{D}(6)$ (quitando el 5) y $\mathbb{N} \setminus \mathrm{D}(2, 3, 5)$ (que viene de la descomposición del 6).

Construyamos ahora el conjunto de todos los semigrupos numéricos con número de Frobenius 8. Todos ellos contienen al semigrupo $\{0, 9, 10, \rightarrow\} = \mathbb{N} \setminus \mathrm{D}(5, 6, 7, 8)$. Procedemos como en el ejemplo anterior con la salvedad de que al añadir un salto especial nunca vamos a usar el

8, preservando así el número de Frobenius. Hay exactamente 10 semigrupos numéricos con número de Frobenius 8.

Presentaciones, la opción generadores-relatores para describir un semigrupo numérico

Sea S el semigrupo numérico generado por $\{2,3\}$. Podemos pensar en S como un monoide conmutativo generado por dos elementos x e y tales que $3x = 2y$. Ésta es la idea de presentación. Démosle un carácter más formal. Supongamos que S está (minimalmente) generado por $\{n_1, \dots, n_p\}$. La aplicación

$$\varphi : \mathbb{N}^p \to S,\ \varphi(a_1, \dots, a_p) = a_1 n_1 + \cdots + a_p n_p$$

es un epimorfismo de monoides, y en consecuencia S es isomorfo a $\mathbb{N}^p/\ker(\varphi)$, donde $\ker(\varphi) = \{(a,b) \in \mathbb{N}^p \times \mathbb{N}^p : \varphi(a) = \varphi(b)\}$. Una *presentación* de S no es más que un sistema de generadores como congruencia de $\ker(\varphi)$.

Rédei demostró que cualquier monoide finitamente generado es finitamente presentado, y por tanto, todo semigrupo numérico es finitamente presentado, en el sentido de que admite una presentación con un número finito de elementos. Es más, para semigrupos numéricos el concepto de presentación mimimal respecto de cardinalidad e inclusión coinciden (cosa que no ocurre con monoides finitamente generados en general).

Rosales dio un procedimiento para calcular una presentación minimal de un semigrupo numérico a partir de su sistema minimal de generadores. Vamos a describir brevemente en qué consiste esta construcción. Supongamos, como viene siendo costumbre, que S es un semigrupo numérico con sistema minimal de generadores $\{n_1, \dots, n_p\}$. Tomemos $n \in S$. Asociado a n definimos un grafo G_n cuyos vértices son

$$V_n = \{n_i : n - n_i \in \mathbb{N}\}$$

y con lados

$$E_n = \{n_i n_j : n - (n_i + n_j) \in \mathbb{N}\}.$$

Si G_n es conexo, definimos $\rho_n = \emptyset$. En caso contrario, supongamos que $C_1, \dots, C_k$ son las componentes conexas de G_n. Para cada $i \in \{1, \dots, k\}$ existe una factorización (expresión, más tarde volveremos a esto) de n en la que sólo aparecen vértices de C_i, a saber, existe $\gamma_i \in \varphi^{-1}(n)$ de forma que la coordenada j-ésima de γ_i es cero siempre que n_j no sea un vértice de C_i. Definimos en este caso $\rho_n = \{(\gamma_1, \gamma_2), (\gamma_1, \gamma_3), \dots, (\gamma_1, \gamma_k)\}$. Entonces $\rho = \bigcup_{n \in S} \rho_n$ es una presentación minimal de S (y toda presentación minimal se puede obtener de esta forma,

siempre que permitamos que ρ_n conecte todas las componentes conexas de G_n; en la definición que hemos dado lo hacemos en forma de estrella, con C_1 en el centro). Como cabía esperar, sólo hay un número finito de $n \in S$ para los que G_n es no conexo. Rosales demostró en su día que si G_n es no conexo, entonces n es de la forma $n = n_i + w$ con $i \in \{2, \dots, p\}$ y $0 \neq w \in \mathrm{Ap}(S, n_1)$ (una vez más nos topamos con los conjuntos de Apéry).

Algo sobre anillos de semigrupo

Sea K un cuerpo y sea S un semigrupo numérico. Escogemos t como un símbolo y definimos $K[S] = \bigoplus_{s\in S} Kt^s$ y $K[\![S]\!] = \prod_{s\in S} Kt^s$. Representamos a los elementos h de $K[\![S]\!]$ como $h = \sum_{s\in S} a_s t^s$, con $a_s \in \mathbb{N}$ para todo s. El elemento h está en $K[S]$ si $a_s = 0$ para casi todos los $s \in S$ (salvo un número finito). Podemos sumar dos elementos de $K[\![S]\!]$ (y por tanto de $K[S]$) simplemente sumando los coeficientes grado a grado, y se pueden multiplicar esos elementos usando la propiedad distributiva y teniendo en cuenta la regla $t^s t^{s'} = t^{s+s'}$. De esta manera, tanto $K[\![S]\!]$ como $K[S]$ son anillos. Es más, $K[\![S]\!]$ es una anillo local cuyo ideal maximal es $m = (t^{n_1}, \dots, t^{n_p})$, con $\{n_1, \dots, n_p\}$ el sistema minimal de generadores de S (es por eso que a p le hemos llamado antes dimensión de inmersión de S). Algunas propiedades de $K[\![S]\!]$ y de $K[S]$ se pueden caracterizar en función de S. Esta posibilidad ha sido la causante de se usen nombres para muchos parámetros del semigrupo S que ya existían en teoría de anillos.

La clausura entera de $K[\![S]\!]$ es $K[\![t]\!]$, y si g es el número de Frobenius de S, entonces $t^{g+1}K[\![t]\!] \subseteq K[\![S]\!]$. Es por eso que a veces al número de Frobenius más uno se le llama *conductor*.

Podemos extender el morfismo φ definido anteriormente de forma natural

$$\psi : K[x_1, \dots, x_p] \to K[S],\ \psi(x_i) = t^{n_i}\ (i \in \{1, \dots, p\}).$$

El núcleo de ψ es lo que se conoce como *ideal de definición* de S.

Simplificando, escribimos para $a = (a_1, \dots, a_p) \in \mathbb{N}^p$, $X^a = x_1^{a_1} \cdots x_p^{a_p}$.

Herzog demostró que $(a, b) \in \ker(\varphi)$ si y sólo si $X^a - X^b \in \ker(\psi)$. Es más, si ρ es una presentación minimal de S, el conjunto $\{X^a - X^b : (a, b) \in \rho\}$ es un sistema minimal de generadores de $\ker(\psi)$.

En $K[\![S]\!]$ uno puede definir la aplicación $v : K[\![S]\!] \to S$, $v(\sum_{s\in S} a_s t^s)$ como el más pequeño elemento s de S tal que $a_s \neq 0$. Esto define una valuación en $K[\![S]\!]$. Varios autores han explotado esta aplicación debido a sus generosas propiedades. Si I es un ideal fraccionario de $K[\![S]\!]$, entonces $v(I)$ es un ideal relativo de S, a saber, un subconjunto de $\mathbb{Z}$ (el grupo cociente de S) tal que $I + S \subseteq I$ y $I + s \subseteq S$ para algún $s \in S$. Si I y J son dos ideales fraccionarios con $J \subseteq I$, entonces la longitud de I/J coincide con la cardinalidad de $v(I)\ \ v(J)$. En particular $I = J$ si y sólo si $v(I) = v(J)$.