TRES SESIONES CON SEMIGRUPOS NUMÉRICOS

P. A. GARCÍA-SÁNCHEZ

ÍNDICE

Mi gratitud hacia Ignacio Ojeda por la invitación para participar en el Seminario de Geometría Tórica V, y por hacer tan placentera nuestra estancia en Jarandilla de la Vera.

Sesión 1. Elementos notables y distintas formas de representar un semigrupos numérico

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 $\{s/d \mid s \in S\}$, 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.

1. 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 $\{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in \mathbb{N}\}$, 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 ($a+b = a+c$ implica $b = c$), 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 $\{a_1, \ldots, a_n\}$, entonces el máximo común divisor de $\{a_1, \ldots, a_n\}$ es uno (y al revés, si $\{a_1, \ldots, a_n\}$ es un conjunto de enteros con máximo común divisor uno, entonces el submonoide de $\mathbb{N}$ generado por $\{a_1, \ldots, a_n\}$ es un semigrupo numérico).

2. 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 máx($\mathbb{Z} \setminus S$), con $S = \langle a_1, \ldots, a_n \rangle$ ($\mathbb{Z}$ 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 $g + (\mathbb{N} \setminus \{0\}) \subset S$, y en particular, $g + (S \setminus \{0\}) \subseteq S$. 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 $\mathbb{Z} \setminus S$ respecto de este orden.

A los enteros positivos que no están en S se les llama *saltos* 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.

3. 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 $\{w_0, \ldots, w_{n-1}\}$ donde w_i es el menor elemento en S congruente con i módulo n. Se puede comprobar fácilmente que este conjunto es precisamente $\{s \in S \mid s - n \notin S\}$. 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 $x \equiv w \bmod n$; $x \in S$ 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.

4. 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 $i \in \{1,\dots,m\}$ 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 $x_i + x_j = x_{(i+j) \bmod m} + km$ 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 $\mathrm{Ap}(S,m) = \{w_0 = 0, w_1, \dots, w_{m-1}\}$ 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 $w_i + w_j = w_{(i+j) \bmod m} + km$ se puede reescribir como $(k_i + k_j)m + i + j = k_{(i+j) \bmod m} m + (i+j) \bmod m + km$. Como $i + j = \lfloor \frac{i+j}{m} \rfloor m + (i+j) \bmod m$, se llega a $(k_1, \dots, k_{m-1})$ ($k_0 = 0 = w_0$ no proporciona información) es una solución no negativa del sistema de desigualdades

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

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

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

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 $\mathscr{T}(m)$ el conjunto de elementos de $\mathbb{N}^{m-1}$ que son solución de (1). Entonces $\mathscr{T}(m)$ 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 (1) ya fue utilizado en 1987 por Kunz para hacer una clasificación de los semigrupos numéricos.

5. 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 $x|y$ (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 $|$. 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 $\{0, g+1, \to\}$.

6. 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
- $x + (S \setminus \{0\}) \subseteq S$.

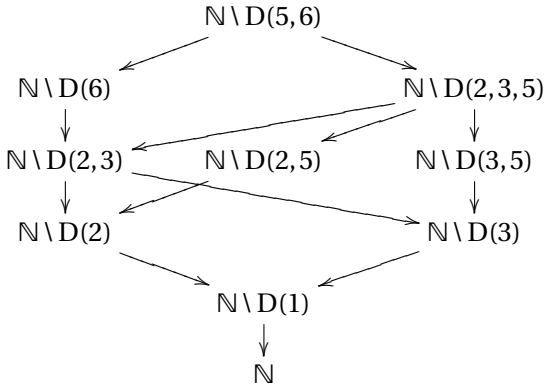
Por tanto, el elemento x tiene que ser a la vez un pseudo-número de Frobenius y un salto fundamental de S. Estos saltos son conocidos como *saltos especiales* de S, y son aquellos saltos fundamentales que son maximales respecto de $\leq_S$.

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

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

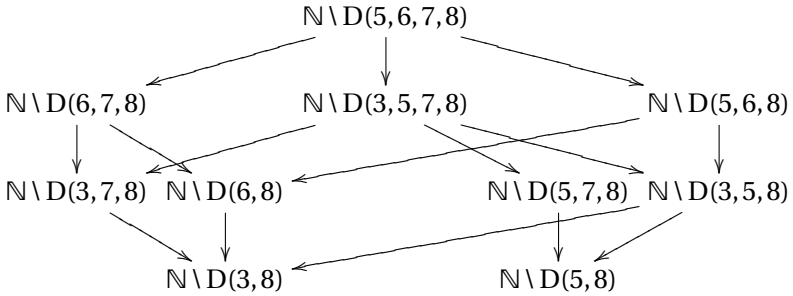
Ejemplo 1. Consideremos el semigrupo $S = \mathbb{N} \setminus \mathrm{D}(5,6)$. Tenemos que 5 es primo y $6 = 2 \cdot 3$, y ambos son maximales en $\{5,6\}$ respecto de $\leq_S$. Por tanto nuestro semigrupo tiene dos "hijos": $\mathbb{N} \setminus \mathrm{D}(6)$ (quitando el 5) y $\mathbb{N} \setminus \mathrm{D}(2,3,5)$ (que viene de la descomposición del 6). Repitiendo el proceso obtenemos la siguiente gráfica.



□

Ejemplo 2. 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.



Por tanto hay exactamente 10 semigrupos numéricos con número de Frobenius 8.

7. 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 $\mathbb{N}^p/\mathrm{Ker}(\varphi)$, donde $\mathrm{Ker}(\varphi) = \{(a,b) \in \mathbb{N}^p \times \mathbb{N}^p \mid \varphi(a) = \varphi(b)\}$. Una *presentación* de S no es más que un sistema de generadores como congruencia de $\mathrm{Ker}(\varphi)$.

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

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

y con lados

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

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

$\rho_n = \{(\gamma_1, \gamma_2), (\gamma_1, \gamma_3), \ldots, (\gamma_1, \gamma_k)\}$. 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 $i \in \{2, \ldots, p\}$ y $0 \neq w \in \mathrm{Ap}(S, n_1)$ (una vez más nos topamos con los conjuntos de Apéry).

8. Algo sobre anillos de semigrupo

Sea K un cuerpo y sea S un semigrupo numérico. Escogemos t como un símbolo y definimos $K[S] = \bigoplus_{s \in S} K t^s$ y $K[[S]] = \prod_{s \in S} K t^s$. 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 $m = (t^{n_1}, \ldots, t^{n_p})$, con $\{n_1, \ldots, n_p\}$ 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

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

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

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

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

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 $v(I) \setminus v(J)$. En particular $I = J$ si y sólo si $v(I) = v(J)$.

Sesión 2. Grandes familias

Hay algunas familias que han sido estudiadas debido a sus propiedades extremas, o bien por sus aplicaciones a la teoría de anillos. Hablaremos brevemente de ellas, así como de otras que recientemente han adquirido cierta transcendencia.

9. Semigrupos numéricos simétricos y pseudo-simétricos

Un semigrupo numérico es *simétrico* si no tiene huecos. Esto es, si S es nuestro semigrupo numérico y tiene número de Frobenius g, entonces para cada entero x, el hecho de que $x \notin S$, lleva a $g - x \in S$. Fröberg, Gottlieb y Häggkvist probaron que los semigrupos numéricos simétricos son aquellos que tienen un número de Frobenius impar y con el menor número posible de saltos, lo que equivale a decir que son maximales (respecto de la inclusión) en el conjunto de semigrupos numéricos con un número de Frobenius dado. De esta manera se ve que en efecto estos semigrupos verifican propiedades extremas, pero aquí no acaban esas propiedades. Estos semigrupos se pueden caracterizar como aquellos cuyo tipo es uno, y por tanto son los que menor tipo tienen de entre todos los semigrupos numéricos. Kunz probó que $K[[S]]$ es Gorenstein si y sólo si S es simétrico. Por tanto, si uno busca ejemplos de anillos Gorenstein, uno puede echar mano de esta bolsa de ejemplos. De hecho, tal y como Rosales demostró no hace mucho, uno puede escoger ejemplos con una dimensión de inmersión y multiplicidad preestablecidas.

La pregunta natural que surge en este momento es qué pasa si el número de Frobenius es par. ¿Se pueden imponer condiciones parecidas a las del párrafo anterior en este caso? La respuesta es afirmativa y la dan lo que se conoce como semigrupos numéricos pseudo-simétricos. Hay que tener en cuenta el siguiente detalle: si g es el número de Frobenius de S y g es par, entonces $\frac{g}{2}$ es un salto de S, y claramente $g - \frac{g}{2}$ da $\frac{g}{2}$. Por tanto la condición pasa a ser la siguiente: si x es un entero que no está en S distinto de $\frac{g}{2}$, entonces $g - x \in S$. Un semigrupo numérico verificando esa condición se dice *pseudo-simétrico*. El tipo de estos semigrupos es siempre dos, siendo sus pseudo-números de Frobenius g y $\frac{g}{2}$, aunque no todo semigrupo numérico de tipo dos es pseudo-simétrico. Se verifica además que estos semigrupos son los maximales de entre los semigrupos numéricos con su mismo número de Frobenius, y son aquellos también que tienen el menor número de saltos posible.

Desde el punto de vista de los saltos especiales ambos conceptos se pueden unificar diciendo que un semigrupo numérico es simétrico o pseudo-simétrico si y sólo si tiene a lo sumo un salto especial (nótese que $\frac{g}{2}$ no puede ser nunca un salto fundamental de S, si g es el número de Frobenius de S). Este hecho tiene que ver con el proceso que describimos en la sesión anterior para determinar los sobre-semigrupos de un semigrupo numérico dado, ya que estos semigrupos son maximales en el conjunto de todos los semigrupos numéricos con un número de Frobenius dado.

10. Descomposición en semigrupos irreducibles

Podemos unificar ambos conceptos de una forma alternativa. Un semigrupo numérico es *irreducible* si no se puede expresar como intersección de dos semigrupos numéricos que lo contengan propiamente. Resulta que irreducibilidad y maximalidad en el conjunto de semigrupos con número de Frobenius fijo coinciden. De esta forma un semigrupo numérico es irreducible si y sólo si es o bien simétrico (y por tanto tiene un número de Frobenius impar) o pseudo-simétrico (y con número de Frobenius par).

Cualquier semigrupo numérico se puede expresar como intersección de un número finito de semigrupos numéricos irreducibles. Branco y Rosales han caracterizado estas descomposiciones, y han estudiado aquellos semigrupos que se factorizan como intersección de sólo simétricos o sólo pseudo-simétricos. Hoy en día sabemos cómo calcular descomposiciones en irreducibles minimales, pero no sabemos a priori el número de semigrupos que intervienen en dichas descomposiciones. Es más el concepto de descomposición minimal respecto de redundancia y de número de factores, no tiene por qué coincidir en general.

11. Intersecciones completa y telescópicos

Un semigrupo numérico es una *intersección completa* si la cardinalidad de una de sus presentaciones minimales (y por tanto de todas) es igual a su dimensión de inmersión menos uno. Esto viene a decir que es un semigrupo numérico que puede ser descrito con el menor posible número de relatores. Así una vez más nos encontramos ante un caso extremo. Resulta que todo semigrupo numérico intersección completa es simétrico. Delorme probó que un semigrupo numérico es intersección completa si y sólo si es la pegada de dos semigrupos numéricos que son intersección completa, donde pegada viene a decir a grandes rasgos que la presentación del semigrupo resultante se obtiene uniendo las presentaciones de los semigrupos pegados más un relator que relaciona los generadores de ambos semigrupos. Los semigrupos numéricos generados por dos elementos son el ejemplo más sencillo de intersecciones completas. Si somos capaces de pegar un semigrupo numérico generado por dos elementos con un submonoide de $\mathbb{N}$ generado por un elemento (y por tanto isomorfo a $\mathbb{N}$), lo que obtenemos es intersección completa con tres generadores. Podemos repetir este proceso y obtenemos de esta forma semigrupos numéricos con más de tres generadores que son también intersecciones completas. Los semigrupos que se obtienen de esta manera se llaman *telescópicos*, y sus presentaciones tienen, por la forma de construirlos, una apariencia escalonada. El hecho de que sean relativamente fáciles de construir ha hecho que hayan sido utilizados bastante en la literatura.

12. Semigrupos numéricos con máxima dimensión de inmersión

Como ya comentamos en la sesión anterior, la multiplicidad (el menor entero positivo) de un semigrupo numérico es una cota superior para su dimensión de

inmersión (cardinalidad de su sistema minimal de generadores). Cuando esta cota se alcanza decimos que el semigrupo es de *máxima dimensión de inmersión*, y por tanto estamos ante otra situación extrema. Pero ésta no es la única caracterización extrema de este tipo de semigrupos. Se puede probar que estos semigrupos numéricos alcanzan el máximo número posible de relatores. Esto fue probado por Sally, y más tarde Rosales demostró que esa propiedad los caracteriza. Para estos semigrupos se da además que cualquier elemento del conjunto de Apéry de la multiplicidad no nulo es un generador minimal (claramente, todo generador minimal distinto de la multiplicidad está siempre en cualquier conjunto de Apéry).

Sea S un semigrupo numérico de multiplicidad m. Si expresamos lo elemento del conjunto de Apéry de m en S como $\mathrm{Ap}(S,m) = \{0, w_1, \ldots, w_{m-1}\}$, entonces $\langle m, m+w_1, \ldots, m+w_{m-1}\rangle$ es un semigrupo numérico de máxima dimensión de inmersión. Esto deja patente la cantidad de semigrupos numéricos con máxima dimensión de inmersión. Nótese que $m + w_i > 2m$ para todo i. Si escogemos un semigrupo numérico de máxima dimensión de inmersión, $\langle m, x_1, \ldots, x_{m-1}\rangle$ de forma que $x_i > 2m$ para todo i, entonces $S = \langle m, x_1 - m, \ldots, x_{m-1} - m\rangle$ es un semigrupo numérico con multiplicidad m y $\mathrm{Ap}(S,m) = \{0, x_1 - m, \ldots, x_{m-1} - m\}$. Por tanto, hay una correspondencia biunívoca entre los semigrupos numéricos de multiplicidad m y los semigrupos numéricos de máxima dimensión de inmersión m y con el resto de generadores mayores que el doble de m.

Existen, como ya hemos visto, varias formas de caracterizar a los semigrupos numéricos de máxima dimensión de inmersión. Vamos a presentar otra caracterización que se presta a introducir una subclase bastante interesante. Esta caracterización nos permitirá además introducir un concepto más adelante en esta misma sesión. Un semigrupo numérico S con multiplicidad m es de máxima dimensión de inmersión si y sólo si para cualesquiera elementos no nulos x e y de S, se tiene que $x + y - m \in S$. Gracias a esta caracterización aritmética, es fácil ver que la intersección de dos semigrupos numéricos de máxima dimensión de inmersión con multiplicidad m vuelve a ser un semigrupo numérico de máxima dimensión de inmersión y multiplicidad m. Es más, si S es de máxima dimensión y con número de Frobenius g, entonces $S \cup \{g\}$ también es de máxima dimensión de inmersión.

Obsérvese que en la condición $x + y - m \in S$, estamos eligiendo $x, y \in S \setminus \{0\}$, o lo que es lo mismo, $x, y \in S$ con $x, y \geq m$. Una modificación natural de esta imposición es la siguiente: para cualesquiera x, y y z en S, con $x, y \geq z$, se tiene que $x + y - z \in S$. Un semigrupo numérico verificando esa propiedad es trivialmente de máxima dimensión de inmersión. Los semigrupos con esa condición se dice que tienen la propiedad de *Arf*. La intersección de dos semigrupos con la propiedad Arf es de nuevo Arf (ya no hace falta imponer que tengan la misma multiplicidad), y esta familia también es cerrada para la adjunción del número de Frobenius.

13. Semigrupos numéricos y funciones periódicas y subaditivas

Fijemos m un elemento no nulo en un semigrupo numérico S. Recordemos que un entero x pertenece a S si y sólo si $w_{x \bmod m} \leq x$, donde w_i es el menor elemento de S congruente con i módulo m (precisamente los elementos de $\mathrm{Ap}(S,m)$). Si definimos $f_S : \mathbb{N} \to \mathbb{Q}$ (como es habitual, $\mathbb{Q}$ es el conjunto de números racionales) como $f_S(x) = w_{x \bmod m}$, entonces, en vista de las propiedades del conjunto de Apéry que vimos en la sesión anterior, $f_S(x+y) \leq f_S(x) + f_S(y)$. Además $f_S(x+m) = f_S(x)$. Por tanto, f_S es subaditiva, $f_S(0) = 0$ y es periódica de periodo m. Es más,

$$S = \{x \in \mathbb{N} \mid f_S(x) \leq x\}.$$

El recíproco de este hecho también es cierto. A saber, si tomamos una función subaditiva cualquiera f con $f(0) = 0$ y $f(x+m) = f(x)$ para todo entero no negativo x, entonces el conjunto

$$S_f = \{x \in \mathbb{N} \mid f(x) \leq x\}$$

es un semigrupo numérico.

Si elegimos $f(x) = \frac{1}{c}(ax \bmod b)$, con a, b y c enteros positivos, obtenemos una función subaditiva con $f(0) = 0$ y $f(x+b) = f(x)$ para todo $x \in \mathbb{N}$. Por tanto,

$$\mathrm{S}(a,b,c) = \{x \in \mathbb{N} \mid ax \bmod b \leq cx\}$$

es un semigrupo numérico. A los semigrupos numéricos de esta forma se les llama *proporcionalmente modulares* (de hecho ésa es una representación proporcionalmente modular, que no es única). Apenas sabemos en general nada sobre la multiplicidad, género, número de Frobenius ... de $\mathrm{S}(a,b,c)$ en función de a, b y c, aunque recientemente Vasco, Bullejos y Rosales han proporcionado métodos para calcularla con complejidad el algoritmo de Euclides.

Éstos semigrupos se pueden caracterizar de otra forma bastante curiosa. Resultan ser el conjunto de enteros que pueden darse como numeradores de los racionales pertenecientes a un intervalo de números positivos (incluimos además el cero). Precisemos un poco más esta idea. Supongamos que I es un intervalo no vacío de $\mathbb{Q}^+$. El submonoide de $\mathbb{Q}^+$ generado por I es $\bigcup_{k \in \mathbb{N}} kI$. Si lo cortamos con $\mathbb{N}$, obtenemos un semigrupo numérico. Vamos a denotarlo mediante $\mathrm{S}(I)$. Sobrecargamos la notación adrede, ya que

$$\mathrm{S}(a,b,c) = \mathrm{S}\Big(\big[\frac{b}{a}, \frac{b}{a-c}\big]\Big)$$

(al hacer las cuentas módulo b, podemos suponer que $a < b$; si $c \geq a$, entonces $\mathrm{S}(a,b,c) = \mathbb{N}$, por lo que suponemos también que $c < a < b$).

Si S es un semigrupo numérico proporcionalmente modular y g es su número Frobenius, entonces en general $S \cup \{g\}$ no es proporcionalmente modular, pero se demuestra que es la intersección finita de semigrupos numéricos que sí son proporcionalmente modulares. Usando esta idea no es difícil probar que los semigrupos que son intersección finita de proporcionalmente modulares forman una familia cerrada para intersecciones y para la adjunción del número de Frobenius.

Decimos que un semigrupo numérico S es *sistema proporcionalmente modular* si es la intersección de un número finito de semigrupos numéricos proporcionalmente modulares. Así, S es el conjunto de soluciones enteras de un sistema de desigualdades de la forma:

$$\begin{cases} a_1 x \bmod b_1 \leq c_1 x, \\ a_2 x \bmod b_2 \leq c_2 x, \\ \qquad \vdots \\ a_k x \bmod b_k \leq c_k x, \end{cases}$$

con a_i, b_i, c_i enteros positivos.

Urbano-Blanco y Rosales demostraron que cualquier semigrupo proporcionalmente modular es de la forma $\frac{\langle m,n\rangle}{d}$, donde en general, para un semigrupo S y un entero positivo d, se define

$$\frac{S}{d} = \{x \in \mathbb{N} \mid dx \in S\},$$

el cual vuelve a ser un semigrupo numérico. De esta forma, se sigue que cualquier semigrupo numérico sistema proporcionalmente modular se puede expresar como $\frac{\langle m_1,n_1\rangle}{d_1} \cap \cdots \cap \frac{\langle m_l,n_l\rangle}{d_l}$. Fuimos capaces de modificar convenientemente m_i y n_i, obteniendo $d_1 = \cdots = d_l$, y de forma que m_i, n_i, d_i sean primos relativos. De esta forma probamos que la clase de semigrupos numéricos sistema proporcionalmente modulares son aquellos que admiten una descomposición de Toms, para los que Toms ha sido capaz de construir C^*-algebras cuyos grupos ordenados K_0 son isomorfos a $(\mathbb{Z}, S)$.

14. Familias cerradas bajo intersección y adjunción del número de Frobenius

Como hemos visto anteriormente existen varias familias $\mathscr{F}$ de semigrupos numéricos verificando

(C1) si $S_1, S_2 \in \mathscr{F}$, entonces $S_1 \cap S_2 \in \mathscr{F}$,
(C2) si $S \in \mathscr{F}$ y g es su número de Frobenius, entonces $S \cup \{g\} \in \mathscr{F}$.

Dado un subconjunto no vacío A de $\mathbb{N}$ con máximo divisor igual a uno, el conjunto de $T \in \mathscr{F}$ tales que $A \subseteq T$ es finito, por lo que podemos definir el semigrupo generado por A en F como la intersección de dichos semigrupo numéricos. Si S es el semigrupo resultante, en este caso decimos que A es un *$\mathscr{F}$-sistema de generadores* de S, o que S es la *$\mathscr{F}$-clausura* de $\langle A\rangle$. Como es de esperar, decimos que A es *minimal* si ningún subconjunto propio de A $\mathscr{F}$-genera a S. Observamos de forma independiente que para las familias de semigrupos numéricos de máxima dimensión de inmersión y multiplicidad fija, semigrupos numéricos con la propiedad Arf, también para aquellos que son saturados, o bien que cumplen un patrón fuertemente admisible, y además para los semigrupos numéricos que admiten una descomposición de Toms, que los $\mathscr{F}$-sistemas minimales eran únicos. La idea subyacente en todas estas familias es que verifican (C1) y (C2) (salvo para los de máxima dimensión de inmersión con multiplicidad fija...). Es más en todos estos casos un entero está en un $\mathscr{F}$-sistema minimal de

generadores de S si y sólo si $S\setminus\{m\}$ pertenece de nuevo a la familia $\mathscr{F}$, tal y como ocurre con los sistemas minimales de generadores de toda la vida. Este hecho permite construir recursivamente todas estas familias.

Rosales demostró que estas dos condiciones son suficientes para probar la unicidad de $\mathscr{F}$-sistemas minimales de generadores.

Sesión 3. Factorización en semigrupos numéricos

Sea $S=\langle 2,3\rangle$. El entero 6 está en S, y $6=2\cdot 3=3\cdot 2$. Tanto 2 como 3 son irreducibles en S en el sentido de que no se pueden obtener como combinación de otros elementos de S. Por tanto, 6 admite dos factorizaciones o expresiones esencialmente distintas en S como combinación de irreducibles. Nótese además que 2 "divide" a 6 en S, ya que $2+4=6$ y $4\in S$. Como $6=3+3$ y 2 no divide a 3, pues $1\notin S$, tenemos que 2 es un irreducible que no es "primo". Lo mismo le ocurre al 3. En general, en un semigrupo numérico, sus generadores minimales son sus elementos irreducibles, y ninguno de ellos es primo. Es más en un semigrupo numérico (salvo $\mathbb{N}$) siempre hay elementos con más de una factorización. Esto se debe a que el concepto de factorización está íntimamente ligado al de presentación, y en cuanto que tengamos relatores definiendo el semigrupo, tendremos factorizaciones distintas para un mismo elemento.

15. Factorizaciones

Dado un semigrupo numérico S generado minimalmente por $\{n_1,\dots,n_k\}$, definimos como hicimos anteriormente

$$\varphi:\mathbb{N}^k\to S,\ \varphi(a_1,\dots,a_k)=a_1n_1+\cdots+a_kn_k,$$

y que usamos para hablar de presentaciones para S. La gente que estudia factorizaciones le suele llamar *homomorfismo de factorización* de S. Dado $n\in S$, se define el conjunto de factorizaciones de n como $\mathrm{Z}(n)=\varphi^{-1}(n)$. Así en el ejemplo anterior las factorizaciones de 6 son $\mathrm{Z}(s)=\{(3,0),(0,2)\}$. Esto es, nos quedamos con los exponentes de los irreducibles que aparecen en las factorizaciones. Los conjuntos de factorizaciones de un elemento n en S se corresponden con las soluciones no negativas de $n_1x_1+\cdots+n_kx_k=n$, y por tanto son siempre finitos.

16. Invariantes basados en longitud de factorización

La *longitud* de una factorización $a=(a_1,\dots,a_k)$ de n (y por tanto $a_1n_1+\cdots+a_kn_k=n$) es $|a|=a_1+\cdots+a_k$, esto es, el número de irreducibles que ocurren en dicha factorización. Podemos definir el *conjunto de longitudes de factorizaciones* de n como $\{l\mid \text{existe } a\in\mathrm{Z}(n),|a|=l\}$. Se sabe gracias a los trabajos de Gerlodinger, Halter-Koch y en general de la escuela de Graz que estos conjuntos tienen una estructura que ellos han llamado multiprogresiones casi aritméticas. Para el semigrupo S se define el conjunto de longitudes como el conjunto de conjuntos de longitudes de sus elementos. Chapman y sus alumnos han probado recientemente el el conjunto de factorizaciones de S no determina de forma unívoca a S.

Si $\{l_1 < \cdots < l_t\}$ es el conjunto de longitudes de factorizaciones de n en S, se define $\Delta(n) = \{l_2 - l_1, l_3 - l_2, \cdots, l_t - l_{t-1}\}$, y $\Delta(S)$ es la unión de todos los conjuntos delta de sus elementos. Chapman y sus alumnos han calculado en varios casos este conjunto, y siguen trabajando en ello.

Si todas las longitudes de un elemento dado de un monoide tienen la misma longitud, entonces se dice que el monoide tiene *longitud media única*. Claramente ningún semigrupo numérico que no sea $\mathbb{N}$ va a tener longitud media única. Basta tomar $n_1 n_k$ que tiene al menos dos factorizaciones, una de longitud n_k y la otra n_1. Una forma de medir cuánto nos alegamos de la unicidad en las longitudes de factorizaciones es mediante la elasticidad de una factorización, concepto que fue introducido por Valenza. Se define para n en S, $\mathrm{L}(n)$ como el máximo (en general es el supremo, pero hemos visto que en nuestro caso el conjunto de factorizaciones es finito) de las longitudes de las factorizaciones de n, y $\mathrm{l}(n)$ como el mínimo. La *elasticidad* de las factorizaciones de n se define como $\rho(n) = \frac{\mathrm{L}(n)}{\mathrm{l}(n)}$. Para el semigrupo S, se define su elasticidad como $\rho(S) = \sup_{n \in S} \rho(n)$. Se demuestra que ese supremo es un máximo y que además es un número racional, que se puede calcular a partir de los soluciones enteras no negativas irreducibles de la ecuación diofántica $n_1 x_1 + \cdots + n_k x_k = n_1 y_1 + \cdots + n_k y_k$. En este caso $\rho(S) = \frac{n_k}{n_1}$.

17. Invariantes basados en distancia entre factorizaciones

Dadas dos factorizaciones $a = (a_1, \ldots, a_k)$ y $b = (b_1, \ldots, b_k)$ de n en el semigrupo numérico $S = \langle n_1, \ldots, n_k \rangle$, definimos el *máximo común divisor* de ambas como $a \wedge b = (\min\{a_1, b_1\}, \ldots, \min\{a_k, b_k\})$. La *distancia* entre a y b es $\mathrm{d}(a, b) = \max\{|a - (a \wedge b)|, |b - (a \wedge b)|\}$ (esta función según ha demostrado Geroldinger cumple las propiedades básicas de una distancia).

Si bien la distancia entre dos factorizaciones de n puede ser muy grande, puede que exista una cadena de factorizaciones de n, de forma que dos factorizaciones consecutivas disten relativamente poco. Decimos que una cadena $z_1, \ldots, z_t$ de factorizaciones de n es una *N-cadena* si la distancia entre z_i y z_{i+1} no supera N para todo i. El *grado de catenariedad* de n se define como el mínimo de los N tales que para cualesquiera dos factorizaciones a y b de n existe una N-cadena $z_1, \ldots, z_t$ de forma que $a = z_1$ y $b = z_t$. El grado de catenariedad de S se define como el supremo de los grados de catenariedad de los elementos de S. Se puede probar que ese supremo es de hecho un máximo, y que se alcanza en un elemento de la forma $w + n_i$ con w un elemento del Apéry de la multiplicidad de S en S, y n_i un generador minimal de S. Una vez más, el conjunto de Apéry vuelve a mostrar su sorprendente utilidad.

Existen otros invariantes como el grado de amansamiento, que también pueden ser calculados en función de determinados conjuntos de Apéry.

18. El paquete `numericalsgps` para `GAP`

Terminaremos esta sesión dando un breve paseo por el paquete `numericalsgps` para `GAP`. Dicho paquete está disponible en

`http://www.gap-system.org/Packages/numericalsgps.html`. En dicha página aparece un detallado manual de las funciones implementadas. Repasaremos los conceptos vistos en estas tres sesiones mediante ejemplos hecho con `GAP`.

REFERENCIAS

Es difícil recoger una lista completa de referencias relativas a semigrupos numéricos. Nuestro compañero Jorge Ramirez Alfonsín ha hecho un gran trabajo en su libro. Barucci, Dobbs and Fontana han escrito lo que para nosotros es un magnífico monográfico en el que se resaltan las conexiones entre semigrupos numéricos y dominios locales uno dimensionales, el cual puede ser utilizado además como diccionario para los invariantes existentes en estos dos mundos. Barucci ha escrito no hace mucho una bonita revisión sobre anillos de semigrupo que aparecerá en un libro en honor a Gilmer (al cual todos los que trabajamos en anillos de semigrupo estamos en deuda). En nuestro libro (escrito con Rosales) "Numerical semigroups" hemos intentado recopilar las herramientas básicas para empezar a trabajar en semigrupos numéricos. Este libro está por ahora sólo disponible bajo demanda.