Alexey Beshenov (alexey.beshenov@math.u-bordeaux.fr)
Institut de Mathématiques de Bordeaux, equipo de la teoría de números, estudiante de doctorado

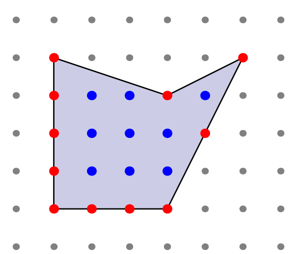
Propuesta de curso: Puntos enteros en politopos y anillos de Cohen-Macaulay

La idea de este curso es relacionar dos temas: la **geometría combinatoria** (puntos enteros en politopos convexos) y el **álgebra conmutativa** (los anillos de Cohen-Macaulay).

Teorema de Pick

Todo empieza con el famoso **teorema de Pick** (1899). *Sea un polígono con vértices en los puntos enteros de una cuadrícula. Sea I el número de los puntos enteros en el interior del polígono y sea B el número de los puntos enteros en el borde. Entonces el área del polígono se puede calcular con la fórmula $A = I + B/2 - 1$.*

Es importante que el polígono sea simple (sin agujeros), pero no es necesario que el polígono sea convexo. Aquí hay un ejemplo: $I = 9$, $B = 11$, entonces el área es igual a $27/2$.

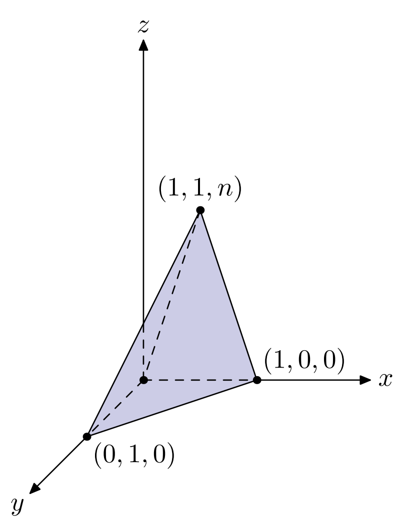


Polinomios de Ehrhart

Una pregunta natural es si existe alguna generalización del teorema de Pick para las dimensiones superiores: sea $\mathcal{P} \subset \mathbb{R}^n$ un politopo con vértices en los puntos enteros $\mathbb{Z}^n \subset \mathbb{R}^n$. También (para simplificar la vida) supongamos que $\mathcal{P}$ es convexo. ¿Cuál es la relación entre el volumen $\operatorname{vol}\mathcal{P}$ y el número de los puntos enteros en $\mathcal{P}$? Desgraciadamente, una identidad sencilla como $A = I + B/2 - 1$ no existe. Por ejemplo, consideremos un tetraedro $\mathcal{T}_n$ en $\mathbb{R}^3$ con vértices

$$(0,0,0),\ (1,0,0),\ (0,1,0),\ (1,1,n),$$

donde $n = 1,2,3,\ldots$ es un número natural.



Se ve que si $n \to \infty$, entonces $\operatorname{vol} \mathcal{T}_n \to \infty$, aunque $\mathcal{T}_n$ para cada n contiene solo cuatro puntos enteros que son sus vértices. Así para obtener una generalización razonable del teorema de Pick, tenemos que contar puntos en el politopo dilatado, para que $\mathcal{P}$ siempre contenga muchos puntos enteros. A saber, para cada $m = 0, 1, 2, 3, \ldots$ sea

$$m\mathcal{P} := \{(mx_1, \ldots, mx_n) \mid (x_1, \ldots, x_n) \in \mathcal{P}\}.$$

Ahora tenemos una función

$$\ell_{\mathcal{P}}(m) := \#(m\mathcal{P} \cap \mathbb{Z}^n) \colon \mathbb{N} \to \mathbb{N}.$$

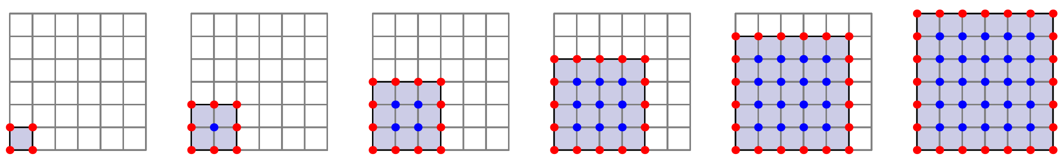
Por ejemplo, de la formula de Pick se ve que para un polígono en $\mathbb{R}^2$ esta función está dada por $\ell_{\mathcal{P}}(m) = A\,m^2 + \frac{1}{2}\,I\,m + 1$, donde A es el área de $\mathcal{P}$ y I es el número de los puntos enteros en su interior.

El caso más simple en las dimensiones superiores es el del cubo unitario:

$$\square := \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid 0 \le x_i \le 1\}.$$

Entonces

$$\ell_{\square}(m) = \#([0, m]^n \cap \mathbb{Z}^n) = (m+1)^n = \sum_{0 \le i \le n} \binom{n}{i} m^i.$$

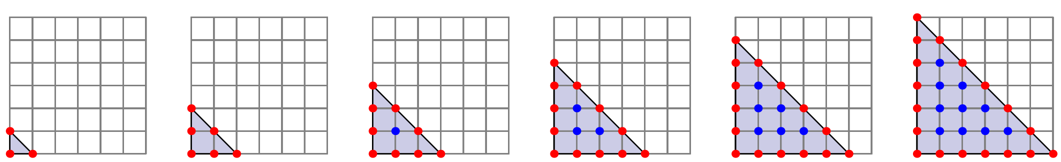


Otro ejemplo un poco más complicado es el del **símplice estándar**

$$\Delta := \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_1 + \cdots + x_n \le 1,\ x_i \ge 0\}.$$

Ahora la respuesta no es tan inmediata, pero se ve que

$$\ell_{\Delta}(m) = \#\{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid x_1 + \cdots + x_n \le m,\ x_i \ge 0\} = \binom{n+m}{n}.$$



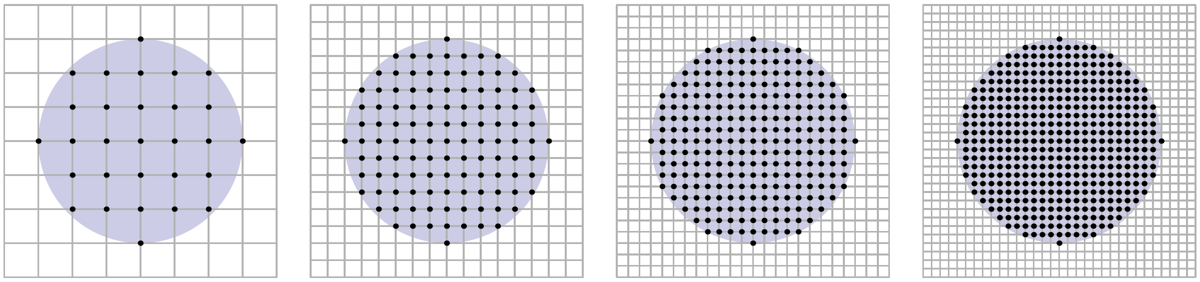
Los ejemplos de $\square$ y Δ tienen algo en común: $\ell_{\mathcal{P}}(m)$ es un polinomio en m de grado n. Es un teorema famoso del matemático francés Eugène Ehrhart.

Teorema (Ehrhart, 1962)**.** *Sea $\mathcal{P}$ un politopo en $\mathbb{R}^n$ y sea $\ell_{\mathcal{P}}(m) := \#(m\mathcal{P} \cap \mathbb{Z}^n)$. Entonces, $\ell_{\mathcal{P}}(m)$ es un polinomio en m de grado n, llamado el **polinomio de Ehrhart** de $\mathcal{P}$.*

Relación entre los puntos enteros y el volumen

Para calcular el volumen aproximado de $\mathcal{P}$, se puede considerar el subconjunto $(\frac{1}{m}\mathbb{Z})^n \subset \mathbb{R}^n$ y ver cuántos de sus puntos están en $\mathcal{P}$—es la misma cosa que cortar $\mathcal{P}$ en pequeños cubitos, cada uno de volumen $\frac{1}{m^n}$, y luego contar los cubitos. Por esto

$$\operatorname{vol} \mathcal{P} = \lim_{m \to \infty} \frac{1}{m^n} \cdot \#\left(\mathcal{P} \cap \left(\frac{1}{m}\mathbb{Z}\right)^n\right).$$



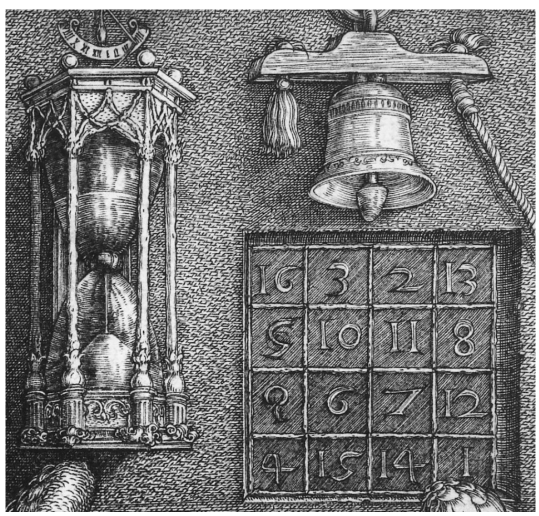
Notemos que $\#\left(\mathcal{P} \cap \left(\frac{1}{m}\mathbb{Z}\right)^n\right) = \ell_{\mathcal{P}}(m)$, y por lo tanto

$$\operatorname{vol}\mathcal{P} = \lim_{m\to\infty} \frac{1}{m^n}\,\ell_{\mathcal{P}}(m).$$

Por el teorema de Ehrhart, $\ell_{\mathcal{P}}(m)$ es un polinomio de grado n, entonces $\operatorname{vol}\mathcal{P}$ es el coeficiente mayor de $\ell_{\mathcal{P}}(m)$. Así vemos que el cálculo de los puntos enteros—el "volumen discreto" de $\mathcal{P}$—nos permite calcular el verdadero volumen de $\mathcal{P}$. Específicamente, la respuesta ya está en el polinomio de Ehrhart.

Cuadrados mágicos

Hay algunas aplicaciones combinatorias de los polinomios de Ehrhart. Por ejemplo, recordemos que un **cuadrado mágico** es una tabla $n \times n$ donde la suma de los números por columnas y filas es la misma e igual a algún número $s \in \mathbb{N}$.



El cuadrado mágico del grabado "Melancolía I" de Alberto Durero (1514)

Luego sea $M_n(s)$ el número de los cuadrados mágicos $n \times n$ con las sumas iguales a s. Se puede ver que es un número de puntos enteros en un cierto politopo convexo, y por lo tanto

Teorema (Ehrhart, 1973)**.** *$M_n(s)$ es un polinomio en s.*

(Precisamente, el grado de este polinomio es $(n-1)^2$.)

Puntos en el interior de un politopo y reciprocidad

Ahora, sea

$$\ell_{\mathring{\mathcal{P}}}(m) := \#(m\mathring{\mathcal{P}} \cap \mathbb{Z}^n)$$

el número de los puntos enteros en el interior de $\mathcal{P}$. Un hecho muy sorprendente es que para calcular $\ell_{\mathring{\mathcal{P}}}(m)$, se puede evaluar el polinomio de Ehrhart $\ell_{\mathcal{P}}(m)$ en $-m$. Es un resultado conjeturado también por Ehrhart y demostrado en el 1971 por I.G. Macdonald.

Teorema (La ley de reciprocidad de Ehrhart–Macdonald)**.**

$$\ell_{\mathring{\mathcal{P}}}(m) = (-1)^n \, \ell_{\mathcal{P}}(-m)$$

Por ejemplo, en el caso de $\square$ y Δ tenemos

$$\begin{aligned}
\ell_{\mathring{\square}}(m) &:= \#(m\mathring{\square} \cap \mathbb{Z}^n) = \#((0,m)^n \cap \mathbb{Z}^n) = (m-1)^n = (-1)^n \sum_{0 \le i \le n} \binom{n}{i} (-m)^i, \\
\ell_{\mathring{\Delta}}(m) &:= \#(m\mathring{\Delta} \cap \mathbb{Z}^n) = \binom{m-1}{n} = (-1)^n \binom{n-m}{n}.
\end{aligned}$$

Los polinomios $\ell_{\mathcal{P}}(m)$ y $\ell_{\mathring{\mathcal{P}}}(m)$ proveen una generalización del teorema de Pick. Por ejemplo, la formula de Pick clásica es $A = \frac{1}{2}(\ell_{\mathcal{P}}(1) + \ell_{\mathring{\mathcal{P}}}(1) - 2)$, y en $\mathbb{R}^3$ la formula correspondiente es $\operatorname{vol} \mathcal{P} = \frac{1}{3!}(\ell_{\mathcal{P}}(2) - 3\ell_{\mathcal{P}}(1) - \ell_{\mathring{\mathcal{P}}}(1) + 3)$—una vez que se sabe que $\ell_{\mathcal{P}}(m)$ es un polinomio, es un ejercicio en interpolación polinomial.

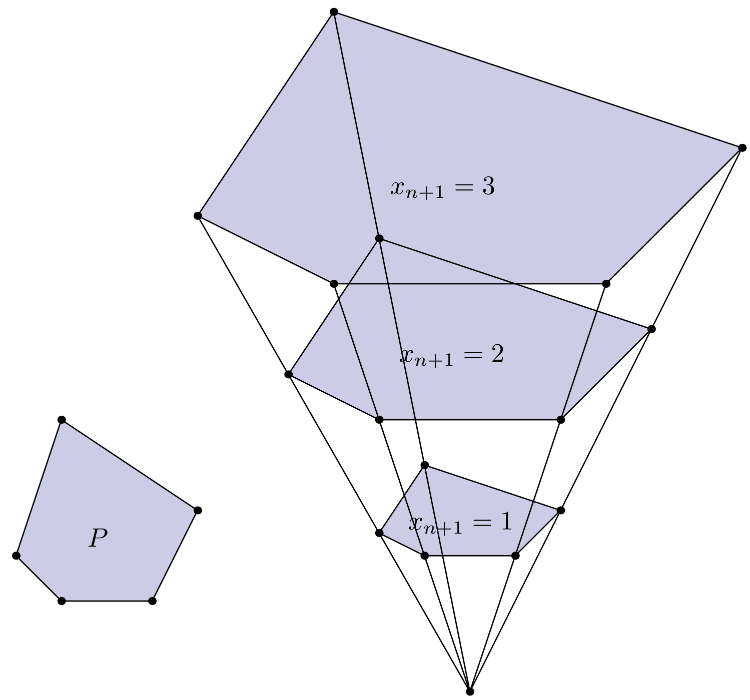
Una demostración sofisticada del teorema de Ehrhart

Para desarrollar las bases de la teoría sobre los puntos enteros en politopos, no se necesitan herramientas especiales y este tema podría ser divertido incluso para los alumnos interesados en olimpiadas de matemáticas. Existen demostraciones del teorema de Ehrhart y de la reciprocidad que no usan matemáticas sofisticadas, y creo que, si el tiempo me lo permite, podría explicarlas a los estudiantes más jóvenes. Sin embargo, mi meta es relacionar los teoremas de arriba con el álgebra conmutativa.

La idea es la siguiente. Resulta que es más fácil trabajar no con un politopo convexo $\mathcal{P} \subset \mathbb{R}^n$, sino con un **cono** $\sigma \subset \mathbb{R}^{n+1}$. Específicamente, si $\mathcal{P}$ tiene como sus vértices $\mathbf{v}_1, \ldots, \mathbf{v}_r \in \mathbb{Z}^n$, se considera un conjunto $\sigma \subset \mathbb{R}^{n+1}$ (con una coordenada extra) dado por

$$\sigma := \mathbb{R}_{\ge 0} \cdot (\mathbf{v}_1, 1) + \cdots + \mathbb{R}_{\ge 0} \cdot (\mathbf{v}_r, 1) := \{\lambda_1 (\mathbf{v}_1, 1) + \cdots + \lambda_r (\mathbf{v}_r, 1) \mid \lambda_i \ge 0\}.$$

Es también un conjunto convexo, pero ya no es acotado. Se ve que la intersección de σ con el hiperplano $\{x_{n+1} = 1\}$ es exactamente $\mathcal{P}$, y en general la intersección con $\{x_{n+1} = m\}$ es $m\mathcal{P}$.



Ya no tiene sentido calcular puntos enteros $\sigma \cap \mathbb{Z}^{n+1}$, pero en combinatoria, para enumerar los elementos de un conjunto infinito, se usan las funciones generatrices, y vamos a hacer algo parecido. Podemos escribir cada punto entero $\mathbf{a} \in \sigma \cap \mathbb{Z}^{n+1}$ como un monomio

$$(a_1, \ldots, a_{n+1}) \leftrightarrow \mathbf{X}^{\mathbf{a}} := X_1^{a_1} \cdots X_{n+1}^{a_{n+1}}.$$

Sea $\mathbb{K}$ un cuerpo (por ejemplo, $\mathbb{K} = \mathbb{C}$ o $\mathbb{R}$). Todos los monomios que proceden de $\sigma \cap \mathbb{Z}^{n+1}$ forman un álgebra sobre $\mathbb{K}$. De hecho, se puede multiplicar monomios:

$$\mathbf{X}^{\mathbf{a}} \cdot \mathbf{X}^{\mathbf{b}} = \mathbf{X}^{\mathbf{a}+\mathbf{b}} = X_1^{a_1+b_1} \cdots X_{n+1}^{a_{n+1}+b_{n+1}}$$

y el hecho que σ es convexo significa que para cada dos puntos $\mathbf{a}, \mathbf{b} \in \sigma \cap \mathbb{Z}^{n+1}$ también $\mathbf{a} + \mathbf{b} \in \sigma \cap \mathbb{Z}^{n+1}$. Luego se forman sumas formales de $\mathbf{X}^{\mathbf{a}}$ con coeficientes en $\mathbb{K}$. Este álgebra se denota $\mathbb{K}[\sigma \cap \mathbb{Z}^{n+1}]$. Es una subálgebra finitamente generada del álgebra $\mathbb{K}[X_1^{\pm 1}, \ldots, X_{n+1}^{\pm 1}]$ de los **polinomios de Laurent** (que son polinomios con potencias posiblemente negativas).

$\mathbb{K}[\sigma \cap \mathbb{Z}^{n+1}]$ es un **álgebra graduada**: es una suma de espacios vectoriales

$$\mathbb{K}[\sigma \cap \mathbb{Z}^{n+1}] = \bigoplus_{m \ge 0} \mathbb{K}[\sigma \cap \mathbb{Z}^{n+1}]_m,$$

donde $\mathbb{K}[\sigma \cap \mathbb{Z}^{n+1}]_m$ está generado por monomios $\mathbf{X}^{\mathbf{a}} := X_1^{a_1} \cdots X_{n+1}^{a_{n+1}}$ con $a_{n+1} = m$. Se ve que

$$\ell_{\mathcal{P}}(m) = \dim_{\mathbb{K}} \mathbb{K}[\sigma \cap \mathbb{Z}^{n+1}]_m.$$

Para cada álgebra graduada $A = \bigoplus_m A_m$, la serie de potencias $H_A(t) := \sum_m (\dim_{\mathbb{K}} A_m)\, t^m$ se llama la **serie de Hilbert de** A. Cuando el álgebra graduada tiene buenas propiedades, se puede calcular $H_A(t)$ y es un invariante importante de A. Por ejemplo, sea $A = \mathbb{K}[X_1, \ldots, X_{n+1}]$ el algebra de polinomios en $n+1$ variables. Hay $\binom{n+m}{n}$ monomios de grado total m, y entonces, si A_m está formado por los monomios de grado m, tenemos la serie de Hilbert

$$H_A(t) = \sum_{m \ge 0} \binom{n+m}{n} t^m = \frac{1}{(1-t)^{n+1}},$$

que es una función racional.

En nuestro caso, la graduación del álgebra $\mathbb{K}[\sigma \cap \mathbb{Z}^{n+1}]$ es diferente: no es el grado total sino el grado de X_{n+1}. Por la definición de σ, la serie de Hilbert de $\mathbb{K}[\sigma \cap \mathbb{Z}^{n+1}]$ es exactamente la función generatriz de $\ell_{\mathcal{P}}(m)$:

$$H_{\mathcal{P}}(t) = \sum_{m \geq 0} (\dim_{\mathbb{K}} \mathbb{K}[\sigma \cap \mathbb{Z}^{n+1}]_m) \cdot t^m = \sum_{m \geq 0} \ell_{\mathcal{P}}(m)\, t^m.$$

Luego la teoría general implica que $H_{\mathcal{P}}(t)$ es una función racional, y que $\ell_{\mathcal{P}}(m)$ son polinomios en m.

Así el teorema de Ehrhart es un caso particular de la teoría de las series de Hilbert. La formula $\ell_{\mathring{\mathcal{P}}}(m) = (-1)^n \ell_{\mathcal{P}}(-m)$ es una consecuencia de la **dualidad local de Grothendieck** para los anillos de Cohen-Macaulay (es un teorema que está relacionado con la **dualidad de Serre para los haces coherentes**). Esta relación entre los anillos de Cohen-Macaulay y problemas combinatorios fue descubierta en los 70 por matemáticos estadounidenses Richard Stanley y Mel Hochster. Lo más sorprendente es que luego Stanley logró demostrar por primera vez algunas conjeturas puramente combinatorias, usando métodos del álgebra conmutativa y geometría algebraica.

* * * * *

El curso comenzará demostrando el teorema de Pick y hablando un poco sobre los polinomios de Ehrhart, cuadrados mágicos, etc. También se abordarán nociones básicas sobre politopos y conos convexos. Luego se pasaría a álgebra conmutativa y homológica, que formarán el grueso de los contenidos.

Referencias principales

1. "Cohen–Macaulay rings" por Winfried Bruns y Jürgen Herzog.
2. "Polytopes, rings and K-theory" por Winfried Bruns y Joseph Gubeladze.
3. "Computing the continuous discretely: integer-point enumeration in polyhedra" por Matthias Beck y Sinai Robins.