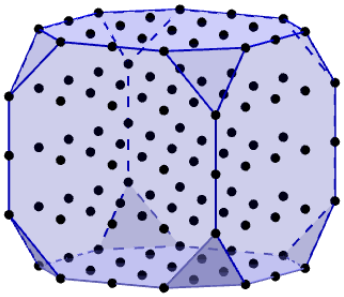
TRABAJO DE FIN DE GRADO

UNIVERSIDAD DE MURCIA
FACULTAD DE MATEMÁTICAS

PUNTOS EN POLIEDROS



David Iglesias López

Dirigido por
María Ángeles Hernández Cifre

Julio 2015

Índice general

Abstract

The aim of this Final Degree Project is to solve a discrete geometry problem. To raise the problem we have two main components that we must know: a lattice Λ (a "net" of points distributed in a particular way) and an n-dimensional polytope P (a convex polygon in the Euclidean plane) which is the convex hull of a finite set of points in the n-dimensional Euclidean space. The problem is to determine the number of lattice points that we have in our polytope.

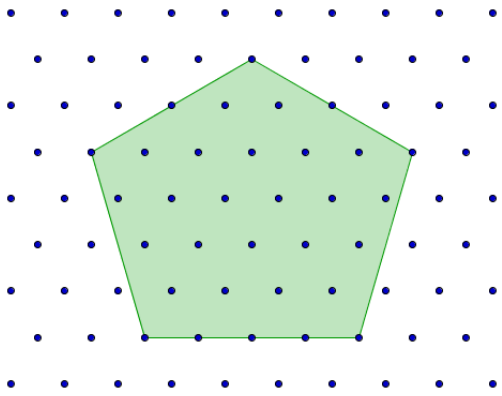


Figura 1: An example of a polytope and a lattice.

Applications that trigger the resolution of these problems are fundamental in some areas of mathematics like, for example, in *integer optimization*. In this area we set figures F defined by a finite collection of linear inequalities, and we look for a maximum (or minimum) of some function among the points of the figure whith have integer coordinates. The resolution of the problem will serve to know the cardinal of this subset of F, or could even determine that such a maximun (or minimum) cannot exist beacause there are no points with integer coordinates in F. In any case, this could be seen as a preliminary study of the figure and could be used to determine the best method to find the maximum (or minimum), for example, according to the number of points of F with integer coordinates.

The work is divided into four chapters. The first one will be a motivation and an introduction to the problem. In this chapter we make an approach to our problem using the tools that we have studied in the degree and without studying the properties of our polytope neither of our lattice. We will deal with the technique known as *generating functions* to simplify our problem. We will conclude this chapter by giving two examples of the problem which are solved using this method. But as the reader will check, the mathematics will be unusually long despite the examples we are using are simple low-dimensional figures. That is the reason why it is convenient to develop a different theory to solve our problem.

Precisely because of this reason, in the second chapter we borrow some ideas from the theory of *convexity* that will be of great help. Moreover we will begin to study *lattices*, in order

to understand how they work and to try to simplify our problem as much as possible. But the interesting points about this chapter are the results which are obtained when the concepts of convexity and lattices fit together and, among other results, they allow us to give a highly effective approach to solve our problem.

In the third chapter we will use further these relations between polytopes and lattices. We will study results that were stated by *Hermann Minkowski*, the father and one of the developers of the so-called *geometry of numbers*. This field is devoted to the study of convex bodies in the context of the lattice theory. In this chapter we will study important results like the relation existing between the volume of the polytopes and the number of lattice points that they have. Of course, we will not forget our problem and will give several bounds using Minkowski's theorem and its consequences. This theorem was the starting point of the geometry of numbers and states the following:

> *If K is a convex compact set of the n-dimensional Euclidean space which is symmetric with respect to the origin and contains no other point with integer coordinates in its interior, then its volume is less than or equal to 2^n.*

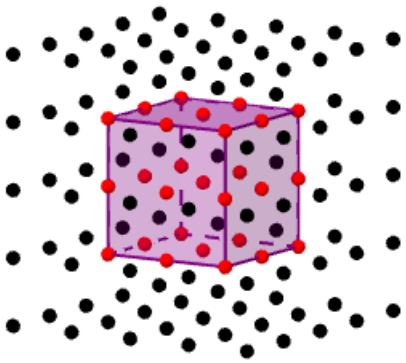


Figura 2: The cube $[-1,1]^3$ verifies the equality in Minkowski's theorem: it is symmetric with respect to the origin, the only integer point in its interior is $(0,0,0)^\intercal$ and has volume 2^3.

Likewise, we will see some applications of this theorem to algebra and, more specifically, to the number theory.

Finally, in the fourth chapter, we will consider only polytopes whose vertices are points of the lattice. It might seem that there is not a remarkable change in the consequences that we can get. However this assumption will allow us to take the final step forward the completion of our problem: due to the theory developed in this chapter we will determine, by using a polynomial expression, not only the number of lattice points contained in any lattice polytope (i. e., a polytope all whose vertices are lattice points); without any extra effort we will get the same for any dilation of the polytope. Specifically, we will proove the result known as *Ehrhart's theorem* obtained by *Eugène Ehrhart* in 1967, in his doctoral thesis, which can be stated as follows:

> *If P is a polytope of the n-dimensional Euclidean space all whose vertices are points of the integer lattice $\mathbb{Z}^n$, then there exist coefficients G_i depending only on the polytope and the lattice, such that, for any natural number k, the cardinal*
>
> $$\#\{P \cap \mathbb{Z}^n\} = \sum_{i=0}^{n} G_i\, k^i;$$
>
> *in other words, it is a polynomial of degree n in the variable k known as the* Ehrhart polynomial.

In the particular case of the Euclidean plane, this result was obtained in 1899 by *Georg Alexander Pick* as a consecuence of the following theorem, witch is also proved in the forth chapter of this work:

> *If P is a convex polygon of the Euclidean plane all whose vertices are points of the integer lattice $\mathbb{Z}^2$, then*
>
> $$\#\{P \cap \mathbb{Z}^2\} = \mathrm{vol}(P) + \frac{1}{2}\#\{\mathrm{fr}\, P \cap \mathbb{Z}^2\} + 1,$$
>
> *where* $\mathrm{vol}(\cdot)$ *is the Lebesgue measure and* $\mathrm{fr}\, P$ *is the boundary of the polygon.*

Resumen

El objetivo de este Trabajo Fin de Grado es dar solución a un problema de la geometría discreta. Para plantear el problema disponemos de dos elementos: un retículo Λ (una "red" de puntos distribuida de una forma concreta) y un politopo P n-dimensional (un polígono convexo en el caso del plano), que no es otra cosa que la envoltura convexa de una cantidad finita de puntos en el espacio euclídeo n-dimensional. El problema consistirá en determinar la cantidad de puntos del retículo que forman parte de nuestro politopo.

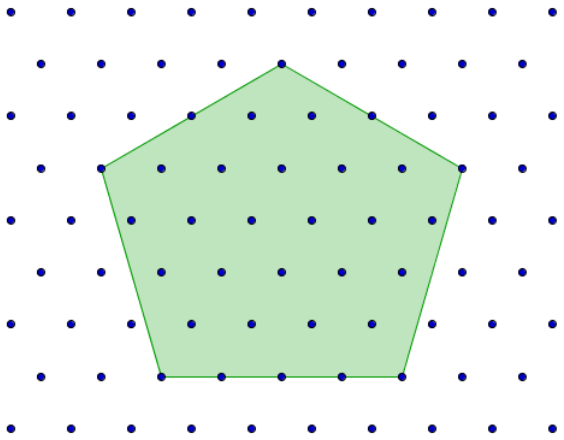


Figura 3: Un ejemplo de politopo y retículo.

Las aplicaciones que desencadena la resolución de este tipo de problemas son fundamentales en áreas de las matemáticas como, por ejemplo, la *optimización entera*. En este área se definen figuras F a través de una cantidad finita de desigualdades lineales, buscando un máximo (o mínimo) para una cierta función en los puntos de nuestra figura que tienen coordenadas enteras. La resolución del problema que vamos a abordar serviría para saber el cardinal de este subconjunto de F, o incluso podría determinar que tal mínimo o máximo no existe al no haber puntos con coordenadas enteras en F, lo que en cualquier caso podría verse como un estudio previo de la figura para después determinar el mejor método para buscar ese máximo (o mínimo), por ejemplo, atendiendo al número de puntos de F con coordenadas enteras.

El trabajo se divide en cuatro capítulos. El primero servirá como introducción al problema. En él abordaremos nuestra cuestión usando las herramientas que hemos estudiado en el grado y no nos fijaremos ni en las propiedades que posee nuestro politopo ni en las de nuestro retículo. Hablaremos de la técnica conocida como *funciones generadoras* para replantear nuestro problema simplificándolo. Y concluiremos el capítulo dando dos ejemplos de resolución de problemas usando esta técnica. Pero como comprobará el lector, las cuentas serán inusualmente largas a pesar de que los ejemplos serán usando figuras sencillas en dimensión baja, por lo que resultará conveniente desarrollar una teoría distinta para resolver nuestro problema.

Precisamente por eso en el segundo capítulo tomaremos ideas de la teoría de *convexidad* y de *cuerpos convexos* que nos serán de gran ayuda. También empezaremos a estudiar los *retículos*, para entender cómo funcionan y tratar de simplificar nuestro problema lo más posible. Pero lo interesante de este capítulo son los resultados que se obtienen a partir de cuando estos conceptos de convexidad y retículos encajan entre sí y, entre otros resultados, nos permiten dar una aproximación altamente eficaz para resolver nuestro problema.

En el tercer capítulo usaremos más a fondo estas relaciones entre los politopos y los retículos. Abordaremos resultados que fueron estudiados por *Hermann Minkowski*, creador y uno de los impulsores de la denominada *geometría de números* dedicada al estudio de los cuerpos convexos en el contexto de la teoría de retículos. En dichos resultados estudiaremos conceptos tan importantes como la relación existente entre el volumen de los politopos y la cantidad de puntos del retículo que poseen. Por supuesto, no nos olvidaremos de nuestro problema y daremos varias acotaciones al mismo gracias al teorema de Minkowski y sus consecuencias. Este teorema fue el inicio de la geometría de números y establece lo siguiente:

> *Si K es un conjunto convexo y compacto del espacio euclídeo n-dimensional, simétrico respecto al origen y que no contiene ningún punto con coordenadas enteras además del propio origen en su interior, entonces su volumen es menor o igual que 2^n.*

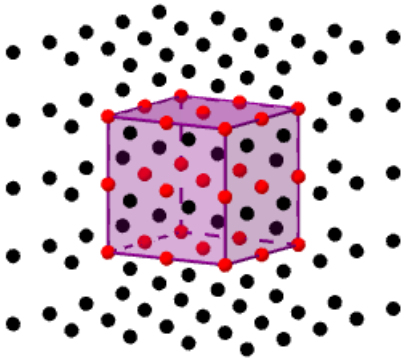


Figura 4: El cubo $[-1,1]^3$, verifica la igualdad en el teorema de Minkowski: es simétrico respecto al origen, sólo contiene al $(0,0,0)^\intercal$ en su interior y tiene volumen 2^3.

Así mismo, veremos algunas aplicaciones de este teorema al álgebra y, más concretamente, a la teoría de números.

Por último, en el cuarto capítulo, nos limitaremos a aquellos politopos cuyos vértices sean puntos del retículo. Esto puede parecer que no representa un cambio muy grande en las consecuencias que podemos aportar, pero este cambio nos permitirá dar el paso definitivo hacia la conclusión de nuestro problema: gracias a la teoría desarrollada en este capítulo podremos determinar mediante el uso de un polinomio no sólo la cantidad de puntos reticulares de cualquier politopo (que posea vértices en el retículo), sino que podremos ampliar este resultado sin ningún esfuerzo extra a cualquier dilatación que hagamos de dicho politopo. Concretamente, demostraremos el llamado *teorema de Ehrhart*, probado por *Eugène Ehrhart* en 1967, dentro de su tesis doctoral, y que puede enunciarse del siguiente modo:

Si P es un politopo del espacio euclídeo n-dimensional cuyos vértices son todos puntos del retículo entero $\mathbb{Z}^n$, entonces existen coeficientes G_i dependientes sólo del politopo y del retículo tales que, para todo número natural k, el cardinal

$$\#\{P \cap \mathbb{Z}^n\} = \sum_{i=0}^{n} G_i \, k^i,$$

es decir, es un polinomio de grado n en la variable k denominado el polinomio de Ehrhart*.*

En el caso particular del plano euclídeo, este resultado ya fue obtenido en 1899 por *Georg Alexander Pick* como consecuencia del siguiente resultado, que también demostramos en el cuarto capítulo de este trabajo:

Si P es un polígono convexo del plano euclídeo cuyos vértices son todos puntos del retículo entero $\mathbb{Z}^2$, entonces

$$\#\{P \cap \mathbb{Z}^2\} = \mathrm{vol}(P) + \frac{1}{2}\#\{\mathrm{fr}\, P \cap \mathbb{Z}^2\} + 1,$$

donde $\mathrm{vol}(\cdot)$ *la medida de Lebesgue y* $\mathrm{fr}\, P$ *es la frontera del polígono.*

Capítulo 1

Introducción

Los dos objetivos principales de esta introducción son, dar una primera idea del concepto de *retículo*, y dar los primeros pasos para afrontar el problema de contar los puntos que posee un *politopo* de un retículo. Esta forma de afrontar el problema la hemos estudiado en [1].

Un retículo es, dados unos elementos $b_i \in \mathbb{R}^n$ con $i \in I$ finito, todos aquellos puntos que sean combinaciones lineales con coeficientes enteros de estos b_i. El ejemplo más usual de retículo es el *retículo entero estándar* $\mathbb{Z}^n \subset \mathbb{R}^n$ que se obtiene escogiendo como b_i a la *base canónica*

$$e_1 = (1, 0, \ldots, 0)^\intercal,\ e_2 = (0, 1, 0, \ldots, 0)^\intercal,\ \ldots,\ e_n = (0, \ldots, 0, 1)^\intercal.$$

En esta introducción consideraremos este último retículo $\mathbb{Z}^n$ como nuestro retículo.

Un *poliedro* $P \subset \mathbb{R}^n$ es el conjunto de puntos que satisface una cantidad finita de desigualdades lineales y un *politopo* es un poliedro acotado.

Y en cuanto al problema de contar los puntos de $\mathbb{Z}^n$ que tiene nuestro politopo, por ejemplo, podemos asegurar por "inspección" que el polígono P de la Figura 1.1 contiene seis puntos enteros, o, en otras palabras, que $\#\{P \cap \mathbb{Z}^2\} = 6$. Como es habitual, $\#$ representa el cardinal de un conjunto.

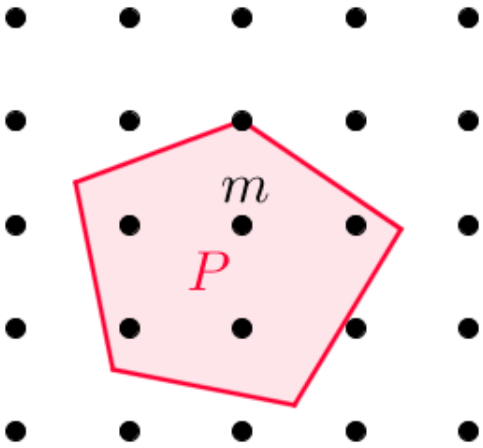


Figura 1.1: El retículo entero $\mathbb{Z}^2 \subset \mathbb{R}^2$, un polígono $P \subset \mathbb{R}^2$, y un punto entero $m \in P$.

Pero al crecer la dimensión de nuestros politopos su descripción analítica se vuelve más complicada, el método de "inspección" no es suficientemente válido y necesitamos desarrollar una teoría. El primer paso hacia esa teoría es darnos cuenta de que el número $\#\{P \cap \mathbb{Z}^n\}$ de puntos enteros de un politopo n-dimesional $P \subset \mathbb{R}^n$ sigue la fórmula

$$\#\{P \cap \mathbb{Z}^n\} = \#\{P_1 \cap \mathbb{Z}^n\} + \#\{P_2 \cap \mathbb{Z}^n\} - \#\{Q \cap \mathbb{Z}^n\} \tag{1.1}$$

siempre que $P = P_1 \cup P_2$ y $Q = P_1 \cap P_2$.

Esta observación nos permite cortar un politopo dado en politopos más simples, y contando el número de puntos enteros en estas piezas nos permitirá conocer el número de puntos enteros en nuestro politopo original (siendo cuidadoso con las intersecciones). Esto es sin duda muy útil, pero no lo suficiente: muchos de los politopos no tienen una forma eficiente de cortarse en "piezas simples" si mantenemos la restricción de que estas piezas sigan siendo poliedros acotados. Necesitamos más libertad a la hora de "cortar y pegar" politopos.

Lo que necesitamos, es ser capaz de extender la propiedad de evaluación de $\#\{P \cap \mathbb{Z}^n\}$ más allá de los *poliedros acotados*, puesto que sólo los poliedros no acotados (los *conos*) son lo suficientemente sencillos como para que la operación de "cortar y pegar" sea eficiente. Pero esto requiere que le demos sentido de alguna forma a la cantidad de puntos que hay en un poliedro no acotado.

Afortunadamente ya es conocida una manera de contar para conjuntos infinitos: las *funciones generadoras*.

1.1. Funciones generadoras

Al punto entero $p = (p_1, \ldots, p_n)^\intercal \in \mathbb{R}^n$ le podemos asociar el monomio $x^p = x_1^{p_1} \ldots x_n^{p_n}$ de n variables $x_1, \ldots, x_n$. Consideramos la suma

$$\sum_{p \in P \cap \mathbb{Z}^n} x^p$$

donde P es un poliedro y $\mathbb{Z}^n \subset \mathbb{R}^n$ es el retículo entero estándar.

Diremos entonces que si P es un *poliedro racional* (un poliedro definido a través de desigualdades lineales con coeficientes enteros) y la serie anterior converge para algún x, entonces converge a una *función racional* $f(P, x)$. En realidad en nuestro caso podremos definir la función $f(P, x)$ incluso aunque la serie no converja para ningún x.

Lo importante de esta técnica es que si P es acotado, evaluando en $x_1 = x_2 = \cdots = x_n = 1$ en $f(P, x)$ obtenemos el número $\#\{P \cap \mathbb{Z}^n\}$.

1.2. Funcionamiento de las funciones generadoras: Caso 1-dimensional

Vamos a poner un ejemplo de esta teoría en el caso más sencillo: con dimensión 1. Vamos a calcular el número de puntos enteros que hay en el intervalo $P = [k, n]$ con $k, n \in \mathbb{Z}$.

Como ya hemos comentado, para dividir cualquier politopo eficientemente necesitaremos los *conos* (poliedros no acotados) de $\mathbb{R}^n$ que, en este caso, son los rayos positivos, los rayos negativos y el propio $\mathbb{R}$. Vamos a hacer las cuentas:

Supongamos que queremos representar el rayo positivo $P_+ = [0, +\infty)$. Como a cada numero m le asociamos el monomio x^m, nuestra función $f(P_+, x)$ quedaría de la siguiente forma

$$f(P_+, x) := \sum_{m=0}^{+\infty} x^m = \frac{1}{1-x} \text{ siempre que } |x| < 1.$$

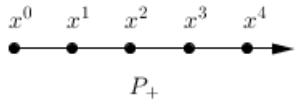


Figura 1.2: Puntos del rayo positivo P_+

Por lo tanto, para el rayo negativo $P_- = (-\infty, 0]$, tenemos

$$f(P_-, x) := \sum_{m=0}^{-\infty} x^m = \frac{1}{1 - x^{-1}} \text{ siempre que } |x| > 1.$$

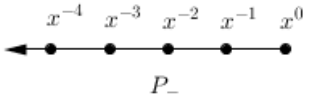


Figura 1.3: Puntos del rayo negativo P_-

Y gracias a la ecuación (1.1), como $P_+ \cup P_- = \mathbb{R}$ y $P_+ \cap P_- = \{0\}$, si "traducimos" esta propiedad a las funciones generadoras tenemos que

$$f(\mathbb{R}, x) = f(P_+, x) + f(P_-, x) - x^0 = \frac{1}{1-x} + \frac{1}{1-x^{-1}} - 1 = \frac{1}{1-x} - \frac{x}{1-x} - 1 = 0.$$

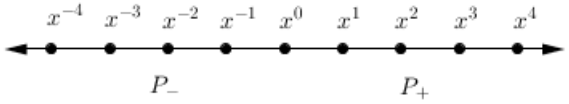


Figura 1.4: Puntos de la recta $\mathbb{R}$

Finalmente, procedamos a calcular $\#\{P \cap \mathbb{Z}\}$. Para ello usaremos que

$$[k, n] = [k, \infty) + (-\infty, n] - \mathbb{R}.$$

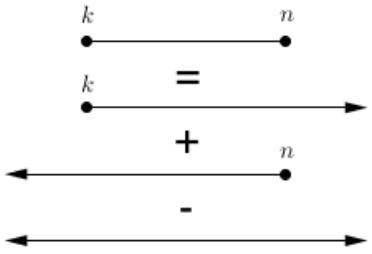


Figura 1.5: Representación de P como suma de dos rayos menos una recta.

Por lo que $f(P,x) = f(k+P_+,x)+f(n+P_-,x)-f(\mathbb{R},x)$ donde $k+P_+$ y $n+P_-$ representan los rayos trasladados a los puntos k y n respectivamente. Realizar los cálculos de $f(k+P_+,x)$ y $f(n+P_-,x)$ resulta fácil ya que

$$f(k+P_+,x) = x^k f(P_+,x) = \frac{x^k}{1-x} \qquad \text{y} \qquad f(n+P_-,x) = x^n f(P_-,x) = \frac{x^n}{1-x^{-1}},$$

por lo que obtenemos la famosa igualdad

$$\sum_{m=k}^{n} x^m = f(P,x) = \frac{x^k}{1-x} + \frac{x^n}{1-x^{-1}} - 0 = \frac{x^k - x^{n+1}}{1-x}.$$

Finalmente, evaluando $f(P,x)$ en $x=1$ y tras un momento de duda, aplicamos la regla de l'Hôpital para obtener $\#\{P \cap \mathbb{Z}\} = n-k+1$, como ya sabíamos.

1.3. Funcionamiento de las funciones generadoras: Caso 2-dimensional

Para este caso, podemos usar el contenido del caso 1-dimensional para deducir que (incluso en dimensiones superiores) tenemos igualmente que

$$f(\mathbb{R},x) = \sum_{m=-\infty}^{+\infty} x^m = 0.$$

Esta igualdad nos será de utilidad en cualquier $\mathbb{R}^n$.

Asímismo, la igualdad $\sum_{m=k}^{n} x^m = (x^k - x^{n+1})/(1-x)$ sigue siendo válida en cualquier dimensión.

Vamos a ver cómo funcionan las funciones generadoras en un ejemplo de dimensión 2: el triángulo Δ de vértices $(0,0)^\intercal$, $(0,100)^\intercal$ y $(100,0)^\intercal$.

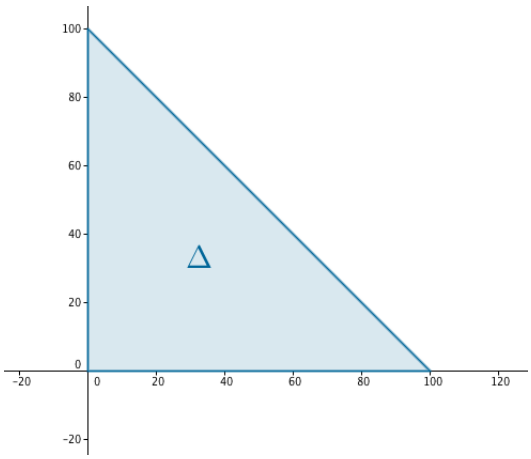


Figura 1.6: Nuestro triángulo Δ.

Como se puede apreciar, nuestro triángulo Δ es el resultado de la intersección de tres "semiplanos": $P_1^+ := \{(x,y)^\intercal \in \mathbb{R}^2 : x \geq 0\}$, $P_2^+ := \{(x,y)^\intercal \in \mathbb{R}^2 : y \geq 0\}$ y $P^* := \{(x,y)^\intercal \in \mathbb{R}^2 : x+y \leq 100\}$.

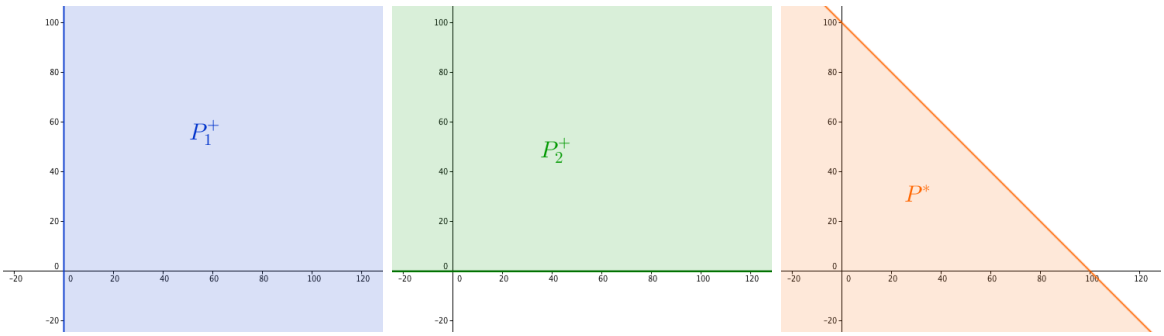
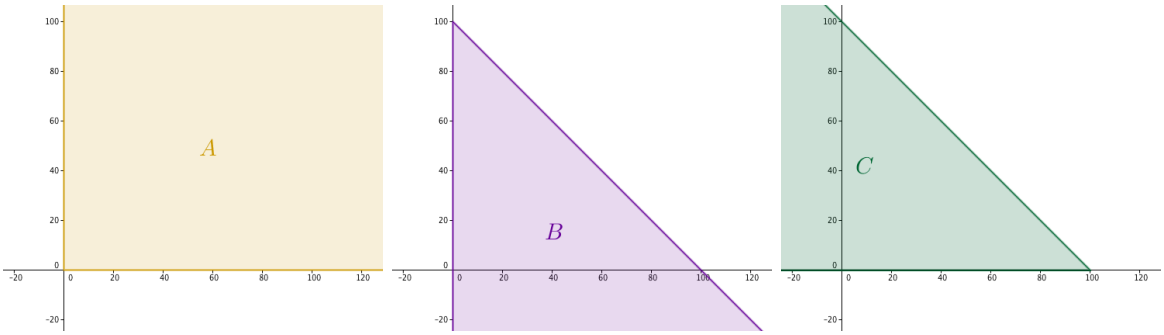


Figura 1.7: Los hiperplanos de cuya intersección resulta Δ.

Por lo que si llamamos A, B y C a los conos intersecciones de estos semiplanos, usando la fórmula de la intersección tenemos que

$$\begin{aligned} f(\mathbb{R}^2, x_1, x_2) = {} & f(P_1^+, x_1, x_2) + f(P_2^+, x_1, x_2) + f(P^*, x_1, x_2) \\ & - [f(A, x_1, x_2) + f(B, x_1, x_2) + f(C, x_1, x_2)] + f(\Delta, x_1, x_2). \end{aligned}$$



(a) $A = P_1^+ \cap P_2^+$ (b) $B = P_1^+ \cap P^*$ (c) $C = P_2^+ \cap P^*$

Figura 1.8: Los conos resultado de las intersecciones dos a dos de los hiperplanos P_1^+, P_2^+ y P^*.

Pero como sabemos que $f(\mathbb{R}, x) = \sum_{m=-\infty}^{+\infty} x^m = 0$, esto simplifica las cosas puesto que entonces

$$f(\mathbb{R}^2, x_1, x_2) := \sum_{m=-\infty}^{+\infty} \sum_{n=-\infty}^{+\infty} x_1^m x_2^n = \sum_{m=-\infty}^{+\infty} x_1^m \left(\sum_{n=-\infty}^{+\infty} x_2^n \right) = \sum_{m=-\infty}^{+\infty} x_1^m \cdot 0 = 0$$

$$f(P_1^+, x_1, x_2) := \sum_{m=0}^{+\infty} \sum_{n=-\infty}^{+\infty} x_1^m x_2^n = \sum_{m=0}^{+\infty} x_1^m \left(\sum_{n=-\infty}^{+\infty} x_2^n \right) = \sum_{m=0}^{+\infty} x_1^m \cdot 0 = 0$$

$$f(P_2^+, x_1, x_2) := \sum_{n=0}^{+\infty} \sum_{m=-\infty}^{+\infty} x_1^m x_2^n = \sum_{n=0}^{+\infty} x_2^n \left(\sum_{m=-\infty}^{+\infty} x_1^m \right) = \sum_{n=0}^{+\infty} x_2^n \cdot 0 = 0$$

$$\begin{aligned} f(P^*, x_1, x_2) : = & \sum_{m=-\infty}^{+\infty} \sum_{n=-\infty}^{100-m} x_1^m x_2^n = \sum_{r=-\infty}^{100} \sum_{s=-\infty}^{+\infty} x_1^r \left(x_1 x_2^{-1} \right)^s \\ & = \sum_{r=-\infty}^{100} x_1^r \left(\sum_{s=-\infty}^{+\infty} \left(x_1 x_2^{-1} \right)^s \right) = \sum_{r=-\infty}^{100} x_1^r \cdot 0 = 0, \end{aligned}$$

con lo cual nuestra fórmula se reduce a que

$$f(\Delta, x_1, x_2) = f(A, x_1, x_2) + f(B, x_1, x_2) + f(C, x_1, x_2).$$

Pero calculamos fácilmente que

$$f(A, x_1, x_2) := \sum_{m=0}^{+\infty} \sum_{n=0}^{+\infty} x_1^m x_2^n = \sum_{m=0}^{+\infty} x_1^m \left(\sum_{m_2=0}^{+\infty} x_2^n \right) = \sum_{m=0}^{+\infty} x_1^m \cdot \left(\frac{1}{1-x_2} \right) = \frac{1}{(1-x_1)(1-x_2)}$$

$$\begin{aligned} f(B, x_1, x_2) :&= \sum_{n=-\infty}^{100} \sum_{m=0}^{100-n} x_1^m x_2^n = \sum_{n=-\infty}^{100} x_2^n \left(\sum_{m=0}^{100-n} x_1^m \right) = \sum_{n=-\infty}^{100} x_2^n \, \frac{x_1^0 - x_1^{100-n+1}}{1-x_1} \\ &= \frac{1}{1-x_1} \left(\sum_{n=-\infty}^{100} x_2^n \left(1 - x_1^{101-n}\right) \right) = \frac{1}{1-x_1} \left(\sum_{n=-\infty}^{100} x_2^n - \sum_{n=-\infty}^{100} x_2^n x_1^{101-n} \right) \\ &= \frac{1}{1-x_1} \left(\frac{x_2^{100}}{1-x_2^{-1}} - x_1^{101} \left(\sum_{n=-\infty}^{100} \left(x_2 x_1^{-1}\right)^n \right) \right) \\ &= \frac{x_2^{100}}{1-x_1} \left(\frac{1}{1-x_2^{-1}} - \frac{x_1}{1-\left(x_2 x_1^{-1}\right)^{-1}} \right) = \frac{x_2^{100}}{1-x_1} \frac{1 - \frac{x_1}{x_2} - x_1 + \frac{x_1}{x_2}}{\left(1-x_2^{-1}\right)\left(1-x_1 x_2^{-1}\right)} \\ &= \frac{x_2^{100}}{\left(1-x_2^{-1}\right)\left(1-x_1 x_2^{-1}\right)} \end{aligned}$$

$$\begin{aligned} f(C, x_1, x_2) :&= \sum_{m=-\infty}^{100} \sum_{n=0}^{100-m} x_1^m x_2^n = \sum_{m=-\infty}^{100} x_1^m \left(\sum_{n=0}^{100-m} x_2^n \right) = \sum_{m=-\infty}^{100} x_1^m \, \frac{x_2^0 - x_2^{100-m+1}}{1-x_2} \\ &= \frac{1}{1-x_2} \left(\sum_{m=-\infty}^{100} x_1^m \left(1 - x_2^{101-m}\right) \right) = \frac{1}{1-x_2} \left(\sum_{m=-\infty}^{100} x_1^m - \sum_{m=-\infty}^{100} x_1^m x_2^{101-m} \right) \\ &= \frac{1}{1-x_2} \left(\frac{x_1^{100}}{1-x_1^{-1}} - x_2^{101} \left(\sum_{m=-\infty}^{100} \left(x_1 x_2^{-1}\right)^m \right) \right) \\ &= \frac{x_1^{100}}{1-x_2} \left(\frac{1}{1-x_1^{-1}} - \frac{x_2}{1-\left(x_1 x_2^{-1}\right)^{-1}} \right) = \frac{x_1^{100}}{1-x_2} \, \frac{1 - \frac{x_2}{x_1} - x_2 + \frac{x_2}{x_1}}{\left(1-x_1^{-1}\right)\left(1-x_2 x_1^{-1}\right)} \\ &= \frac{x_1^{100}}{\left(1-x_1^{-1}\right)\left(1-x_2 x_1^{-1}\right)} \end{aligned}$$

y por tanto deducimos que

$$\sum_{(m_1,m_2)\in\Delta\cap\mathbb{Z}^2} x_1^{m_1} x_2^{m_2} = \frac{1}{(1-x_1)(1-x_2)} + \frac{x_2^{100}}{\left(1-x_2^{-1}\right)\left(1-x_1 x_2^{-1}\right)} + \frac{x_1^{100}}{\left(1-x_1^{-1}\right)\left(1-x_2 x_1^{-1}\right)}.$$

Tomando finalmente límites en cada variable ($x_1 \to 1, x_2 \to 1$) obtenemos

$$\sum_{(m_1,m_2)\in\Delta\cap\mathbb{Z}^2} 1^{m_1} 1^{m_2} = \#\{\Delta \cap \mathbb{Z}^2\} = 5151,$$

cosa que imaginábamos puesto que, al haber 101 puntos enteros en un cateto de nuestro triángulo Δ, deducimos que, en total, tenemos esa misma cantidad de puntos enteros

$$1 + 2 + 3 + \cdots + 99 + 100 + 101 = \frac{101 \times 102}{2} = 5151.$$

Capítulo 2

Toma de contacto

En este capítulo daremos las primeras nociones (de una manera más formal que en el primer capítulo), así como sentaremos las bases de las distintas definiciones y notaciones que necesitaremos para el estudio de los dos capítulos restantes. Las referencias usadas para los resultados de este capítulo son [7] para la parte de convexidad y [3] y [4] para la sección de retículos.

Notación. En esta memoria, usaremos la notación de $\mathbb{R}^n$ para nuestro espacio euclídeo n-dimensional. Así mismo, usaremos la notación $\langle \cdot, \cdot \rangle$ para denotar el producto escalar en dicho espacio.

Notación. Para $M \subset \mathbb{R}^n$, usaremos la notación $\operatorname{fr} M$ e $\operatorname{int} M$ para representar la frontera y el interior de M respectivamente.

Definición 2.1 (Poliedro, politopo)**.**

Un *poliedro* $P \in \mathbb{R}^n$ es un conjunto definido a través de una cantidad finita de desigualdades lineales, es decir,

$$P = \{x \in \mathbb{R}^n : \langle u_i, x \rangle \leq \alpha_i, i \in I\},$$

donde $u_i \in \mathbb{R}^n$, $\alpha_i \in \mathbb{R}$ e I es un conjunto finito (o vacío).

Si el poliedro P es acotado entonces se dice que es un *politopo*. Denotaremos el conjunto de todos los politopos de $\mathbb{R}^n$ como $\mathcal{P}^n$.

Observación 2.2. Si P es un poliedro, ya sea acotado o no, tenemos que es un cerrado para la topología usual de $\mathbb{R}^n$, por lo que si P es un politopo entonces es un compacto en dicha topología.

2.1. Convexidad y cuerpos convexos

Definición 2.3 (Combinación lineal, afín, positiva, convexa)**.**

Se dice que $x \in \mathbb{R}^n$ es una *combinación lineal* de los vectores $x_1, \ldots, x_k$, y se representa por $x \in \operatorname{lin}\{x_1, \ldots, x_k\}$, si existen $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ tales que $x = \lambda_1 x_1 + \cdots + \lambda_k x_k$. Además:

- Si los λ_i verifican $\lambda_1 + \cdots + \lambda_k = 1$, entonces se dice que x es *combinación afín* de los x_i ($x \in \operatorname{aff}\{x_1, \ldots, x_k\}$).
- Si los λ_i verifican $\lambda_i \geq 0$ para todo i, entonces se dice que x es *combinación positiva* de los x_i ($x \in \operatorname{pos}\{x_1, \ldots, x_k\}$).
- Finalmente, si se verifican ambas condiciones para los λ_i, entonces se dice que x es una *combinación convexa* de los x_i ($x \in \operatorname{conv}\{x_1, \ldots, x_k\}$).

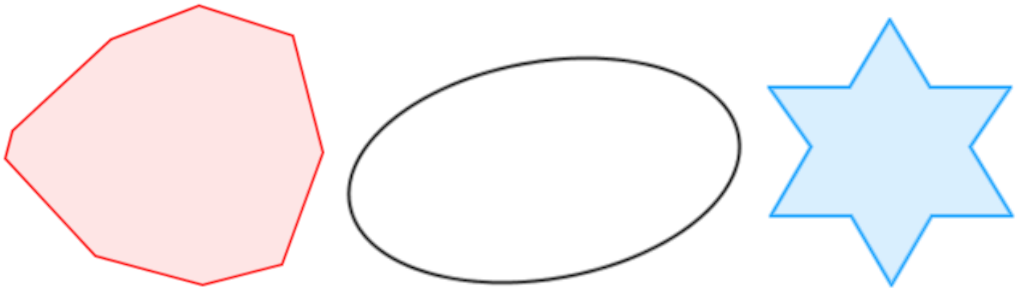
Definición 2.4 (Dependencia afín)**.**

Se dice que $x \in \mathbb{R}^n$ tiene una *dependencia afín* respecto a los vectores $x_1, \ldots, x_k$, cuando x se puede expresar como combinación afín de los x_i, es decir, que existen $\lambda_i \in \mathbb{R}$ verificando $\lambda_1 + \cdots + \lambda_k = 1$ tales que

$$x = \sum_{i=1}^{n} \lambda_i x_i.$$

Definición 2.5 (Conjunto convexo)**.**

Se dice que un conjunto $K \subset \mathbb{R}^n$ es *convexo* si, dados dos puntos cualesquiera de K, el segmento que los une está contenido en K. Es decir, si la combinación convexa $\lambda x + (1-\lambda)y \in K$ para todo $x, y \in K$ y $0 \leq \lambda \leq 1$.



(a) Los politopos son convexos. (b) Las elipses son convexas. (c) Las estrellas no son convexas.

Figura 2.1: Algunos ejemplos de conjuntos convexos y no convexos.

Definición 2.6 (Cono)**.**

Un *cono (convexo)* es un subconjunto $A \subset \mathbb{R}^n$ que es convexo, no vacío y tal que si $x \in A$, entonces $\lambda x \in A$ para todo $\lambda \geq 0$.

Definición 2.7 (Envoltura convexa, afín y positiva)**.**

Dado un conjunto arbitrario A se define la *envoltura convexa* de A, y se representa por $\operatorname{conv} A$, como la intersección de todos los subconjuntos convexos de $\mathbb{R}^n$ que contienen a A.

Análogamente se define la *envoltura afín (positiva)* de A, y se representa por $\operatorname{aff} A$ ($\operatorname{pos} A$), a la intersección de todos los subespacios afines (conos) de $\mathbb{R}^n$ que contienen a A.

Observación 2.8. Gracias a estas definiciones, podemos reescribir las definiciones de *envolturas lineal, afín, positiva y convexa* de otra forma: dado $M \subset \mathbb{R}^n$ las definiciones anteriores son equivalentes a que

- $\operatorname{lin} M$ es el plano lineal de menor dimensión que contiene a M.
- $\operatorname{aff} M$ es el plano afín de menor dimensión que contiene a M.
- $\operatorname{pos} M$ es el cono con vértice en el origen más pequeño que contiene a M.
- $\operatorname{conv} M$ es el menor conjunto convexo que contiene a M.

Ejemplo. Consideramos el conjunto $M = \{x_1 = (1,2)^\intercal, x_2 = (2,1)^\intercal\} \subset \mathbb{R}^2$, procedemos al cálculo de $\operatorname{lin} M$, $\operatorname{aff} M$, $\operatorname{pos} M$ y $\operatorname{conv} M$:

$$\operatorname{lin} M = \{\lambda_1 x_1 + \lambda_2 x_2 : \lambda_1, \lambda_2 \in \mathbb{R}\} = \mathbb{R}^2,$$

dado que x_1 y x_2 son linealmente independientes.

$$\begin{aligned}\operatorname{aff} M &= \{\lambda_1 x_1 + \lambda_2 x_2 : \lambda_1 + \lambda_2 = 1\} = \{(\lambda_1 + 2\lambda_2, 2\lambda_1 + \lambda_2)^\intercal : \lambda_1 + \lambda_2 = 1\} \\ &= \{(\lambda_1 + 2(1-\lambda_1), 2\lambda_1 + (1-\lambda_1))^\intercal : \lambda_1 \in \mathbb{R}\} = \{(2-\lambda_1, 1+\lambda_1)^\intercal : \lambda_1 \in \mathbb{R}\} \\ &= \{(2,1)^\intercal + \lambda \cdot (-1,1)^\intercal : \lambda \in \mathbb{R}\},\end{aligned}$$

$$\operatorname{pos} M = \{\lambda_1 x_1 + \lambda_2 x_2 : \lambda_1, \lambda_2 \geq 0\} = \{\lambda \cdot (\alpha_1 x_1 + \alpha_2 x_2) : \lambda, \alpha_1, \alpha_2 \geq 0, \alpha_1 + \alpha_2 = 1\},$$

y finalmente

$$\operatorname{conv} M = \{\lambda_1 x_1 + \lambda_2 x_2 : \lambda_1 + \lambda_2 = 1, \lambda_1, \lambda_2 \geq 0\} = \{\lambda x_1 + (1-\lambda) x_2 : 0 \leq \lambda \leq 1\}.$$

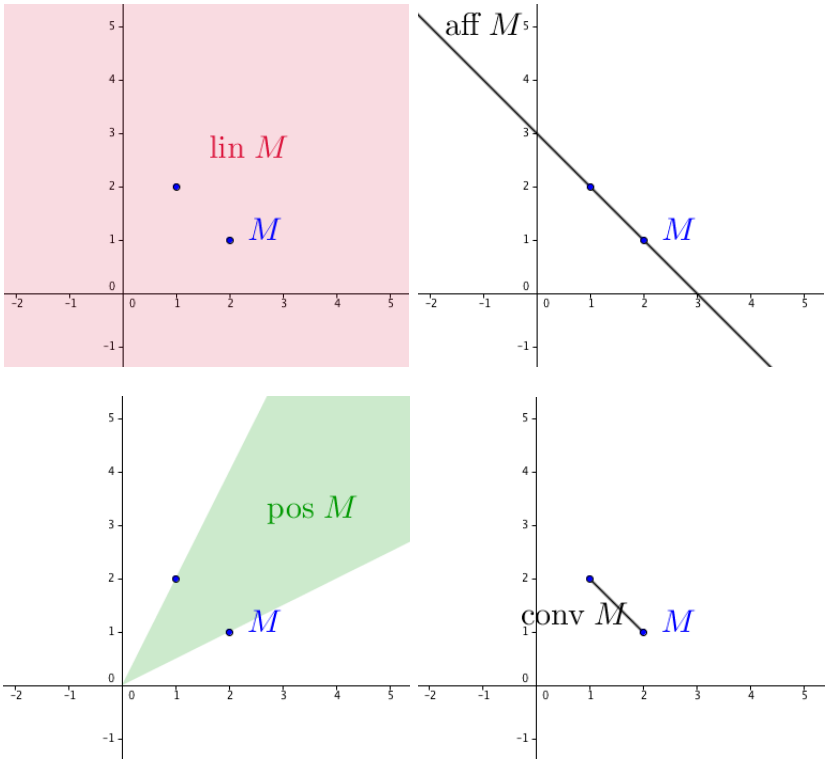


Figura 2.2: Los conjuntos M, $\operatorname{lin} M$, $\operatorname{aff} M$, $\operatorname{pos} M$ y $\operatorname{conv} M$

Observación 2.9. Un politopo $P \in \mathcal{P}^n$ puede verse como la envoltura convexa de una cantidad finita de puntos. Esto se debe a que las desigualdades lineales delimitan semiplanos de $\mathbb{R}^n$, los cuales siempre son convexos, y a que la intersección de convexos resulta un convexo (o vacía).

Notación (Suma de Minkowski)**.** Sean $A, B \in \mathbb{R}^n$, entonces denotaremos $A + B$ como el conjunto " suma " usual para espacios vectoriales, es decir

$$A + B := \{a + b : a \in A, b \in B\}.$$

Observación 2.10.

1. La suma de Minkowski es una operación continua.
2. La suma de Minkowski de conjuntos compactos (convexos) es un compacto (convexo).
3. Si $A, B \in \mathbb{R}^n$, siguiendo la notación de suma de Minkowski denotaremos como

$$A - B := A + (-B) = \{a - b : a \in A, b \in B\}.$$

Definición 2.11 (Cuerpo)**.**
Sea K un conjunto compacto de $\mathbb{R}^n$. Entonces decimos que es un *cuerpo*.
Denotamos al conjunto de todos los *cuerpos convexos* de $\mathbb{R}^n$ como $\mathcal{K}^n$.

Definición 2.12 (Símplice)**.**
Sean $x_0, \ldots, x_n \in \mathbb{R}^n$ $n+1$ puntos afínmente independientes. Entonces el cuerpo $S = \text{conv}\{x_0, \ldots, x_n\}$ se denomina *símplice*.

Notación. Denotamos como $\mathcal{K}_0^n$ el conjunto de todos los cuerpos convexos *0-simétricos* de $\mathbb{R}^n$.

$$\mathcal{K}_0^n = \{K \in \mathcal{K}^n : K = -K\}$$

Notación. Un ejemplo clásico de cuerpo convexo 0-simétrico son las *bolas unidad* para la medida euclídea, es decir

$$\mathbb{B}_n := \left\{ x = (x_1, \ldots, x_n)^\intercal \in \mathbb{R}^n : \sum_{i=1}^n x_i^2 \leq 1 \right\}.$$

Denotaremos a la bola de radio r de $\mathbb{R}^n$ por

$$\mathbb{B}_n(r) := \left\{ x = (x_1, \ldots, x_n)^\intercal \in \mathbb{R}^n : \sum_{i=1}^n x_i^2 \leq r^2 \right\}.$$

Definición 2.13 (Volumen)**.**
Si $K \subset \mathbb{R}^n$, entonces definimos su *volumen* como la medida de Lebesgue asociada a K,

$$\text{vol}_n(K) := \mathcal{H}^n(K).$$

$\mathcal{H}^n$ es la notación que usaremos para la medida de Lebesgue n-dimensional.

Notación. Sea $K \subset \mathbb{R}^n$, y sea $t \in \mathbb{R}$ tal que $(0, 0, \ldots, 0, t)^\intercal \in K$. Entonces denotaremos como K_t a la sección $(n-1)$-dimensional de K a través del hiperplano $\{x_n = t\}$, es decir

$$K_t := \{(x_1, x_2, \ldots, x_{n-1})^\intercal \in \mathbb{R}^{n-1} : (x_1, x_2, \ldots, x_{n-1}, t)^\intercal \in K\}.$$

Teorema 2.14 (Fubini)**.** *Sea K un cuerpo convexo de $\mathbb{R}^n$. Entonces,*

$$\text{vol}(K) = \int_{-\infty}^{\infty} \text{vol}_{n-1}(K_t)\, dt. \tag{2.1}$$

Notación. Denotamos al volumen de la bola unidad por $\kappa_n := \text{vol}_n(\mathbb{B}_n)$.

Resultados básicos sobre los volúmenes de las bolas unidad (los valores de κ_n) son que

1. $\kappa_1 = \text{vol}([-1, 1]) = 2$.
2. $\kappa_2 = \text{vol}(\mathbb{B}_2) = \pi \cdot 1^2 = \pi$.
3. $\kappa_3 = \text{vol}(\mathbb{B}_3) = 4/3 \cdot \pi \cdot 1^3 = 4/3 \cdot \pi$.

Sin embargo para los intereses de este texto es necesario que conozcamos los valores de κ_n para todo $n \in \mathbb{N}$. El resultado buscado no es trivial, pero tampoco es demasiado complicado.

Proposición 2.15. *Se tiene que*

$$\kappa_n = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2} + 1)}, \tag{2.2}$$

donde Γ representa la función Gamma, es decir, $\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} dt$.

Demostración. Primero comentemos unos resultados sobre la función Gamma:

1. $\Gamma(1) = \int_0^\infty e^{-t}dt = 1$
2. $\Gamma(x+1) = x\Gamma(x)$.
3. $\Gamma(1/2) = \sqrt{\pi}$.
4. Si $m \in \mathbb{N}$, se tiene que $\Gamma(m+1) = m!$. (Como se deduce de 1. y 2.)

Así pues obtenemos fácilmente que para dimensiones 1, 2 y 3 se cumple la ecuación (2.2), ya que

$$\frac{\pi^{1/2}}{\Gamma(\frac{1}{2}+1)} = \frac{\sqrt{\pi}}{\frac{1}{2}\Gamma(\frac{1}{2})} = \frac{2\sqrt{\pi}}{\sqrt{\pi}} = 2 = \kappa_1,$$

$$\frac{\pi^{2/2}}{\Gamma(\frac{2}{2}+1)} = \frac{\pi}{\Gamma(2)} = \frac{\pi}{1!} = \pi = \kappa_2$$

y

$$\frac{\pi^{3/2}}{\Gamma(\frac{3}{2}+1)} = \frac{\pi^{3/2}}{\frac{3}{2}\Gamma(\frac{3}{2})} = \frac{\pi^{3/2}}{\frac{3}{2}\Gamma(\frac{1}{2}+1)} = \frac{\pi^{3/2}}{\frac{3}{2}\frac{1}{2}\Gamma(\frac{1}{2})} = \frac{4\pi^{3/2}}{3\sqrt{\pi}} = \frac{4\pi}{3} = \kappa_3.$$

Para probar el caso general necesitamos a la función *beta*:

$$\beta(x,y) := \int_0^1 t^{x-1}(1-t)^{y-1}dt,$$

cuya relación con la función Gamma es conocida

$$\beta(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}.$$

Así pues, si aplicamos la ecuación (2.1), tenemos que

$$\begin{aligned}\kappa_n :&= \mathrm{vol}(\mathbb{B}_n) = 2\int_0^1 \mathcal{H}^{n-1}(\mathbb{B}_{n,t})dt = 2\kappa_{n-1}\int_0^1 \sqrt{(1-t^2)^{n-1}}dt \\ &= 2\kappa_{n-1}\frac{1}{2}\int_0^1 \sqrt{(1-x)^{n-1}}\frac{1}{\sqrt{x}}dx = \kappa_{n-1}\int_0^1 x^{\frac{1}{2}-1}(1-x)^{\frac{n+1}{2}-1}dx \\ &= \kappa_{n-1}\,\beta\left(\frac{1}{2},\frac{n+1}{2}\right) = \kappa_{n-1}\frac{\sqrt{\pi}\,\Gamma(\frac{n+1}{2})}{\Gamma(\frac{n+2}{2})},\end{aligned}$$

y podemos deducir (por recurrencia) que

$$\begin{aligned}\kappa_n &= \frac{\sqrt{\pi}\,\Gamma(\frac{n+1}{2})}{\Gamma(\frac{n+2}{2})}\kappa_{n-1} = \frac{\sqrt{\pi}\,\Gamma(\frac{n+1}{2})}{\Gamma(\frac{n+2}{2})}\frac{\sqrt{\pi}\,\Gamma(\frac{n}{2})}{\Gamma(\frac{n+1}{2})}\kappa_{n-2} = \cdots = \frac{\sqrt{\pi}\,\Gamma(\frac{n+1}{2})}{\Gamma(\frac{n+2}{2})}\frac{\sqrt{\pi}\,\Gamma(\frac{n}{2})}{\Gamma(\frac{n+1}{2})}\cdots\frac{\sqrt{\pi}\,\Gamma(\frac{3}{2})}{\Gamma(\frac{4}{2})}\kappa_1 \\ &= \frac{\pi^{(n-1)/2}\,\Gamma(\frac{3}{2})}{\Gamma(\frac{n+2}{2})}\kappa_1 = \frac{\pi^{(n-1)/2}\,\Gamma(\frac{1}{2}+1)}{\Gamma(\frac{n}{2}+1)}2 = \frac{\pi^{(n-1)/2}\,\frac{1}{2}\sqrt{\pi}}{\Gamma(\frac{n}{2}+1)}2 = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)},\end{aligned}$$

lo que concluye la prueba. □

Observación 2.16. Resulta interesante comentar que el volumen de las bolas no aumenta uniformemente conforme aumenta la dimensión del espacio. De hecho los valores de κ_n alcanzan su máximo en $n = 5$ y a partir de ese momento $\mathrm{vol}(\mathbb{B}_n) \to 0$ cuando $n \to \infty$.

$$\kappa_1 = 2, \quad \kappa_2 \approx 3{,}14, \quad \kappa_3 \approx 4{,}18, \quad \kappa_4 \approx 4{,}93, \quad \kappa_5 \approx 5{,}26, \quad \kappa_6 \approx 5{,}16, \quad \ldots$$

Otro ejemplo lo tenemos si comparamos ahora los valores de $\mathrm{vol}(\mathbb{B}_n(1/2))$

$$\mathrm{vol}\left(\mathbb{B}_2\left(\frac{1}{2}\right)\right) \approx 0{,}78, \quad \mathrm{vol}\left(\mathbb{B}_3\left(\frac{1}{2}\right)\right) \approx 0{,}52, \quad \ldots, \quad \mathrm{vol}\left(\mathbb{B}_{11}\left(\frac{1}{2}\right)\right) < 10^{-3}$$

lo que nos da una idea de cuánto debe crecer el radio de la bola para que $\mathrm{vol}(\mathbb{B}_n(r)) = 1$.

2.2. Retículos

Definición 2.17 (Retículo)**.**
Sean $b_1, \ldots, b_n \in \mathbb{R}^n$ linealmente independientes. El conjunto

$$\Lambda = \{z_1 b_1 + z_2 b_2 + \cdots + z_n b_n : z_i \in \mathbb{Z}, 1 \leq i \leq n\}$$

se denomina *retículo*. El conjunto de los *vectores generadores* $\{b_1, \ldots, b_n\}$ o la matriz $B = (b_1, \ldots, b_n)$ con columnas b_i se denomina la *base* de Λ. Un elemento $b \in \Lambda$ se denomina *punto reticular de* Λ. El conjunto de todos los retículos de $\mathbb{R}^n$ se denota por $\mathcal{L}^n$.

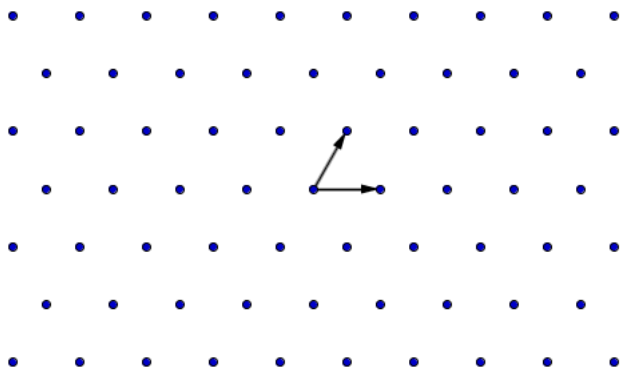


Figura 2.3: El retículo hexagonal generado por los vectores $(1,0)^\intercal$ y $(\frac{1}{2}, \frac{\sqrt{3}}{2})^\intercal$.

Observación 2.18.

1. Los vectores canónicos $e_1, \ldots, e_n \in \mathbb{R}^n$ forman una base del *retículo entero* (conocido también como *retículo estándar*):

$$\mathbb{Z}^n = \{z = (z_1, \ldots, z_n)^\intercal \in \mathbb{R}^n : z_i \in \mathbb{Z}\}.$$

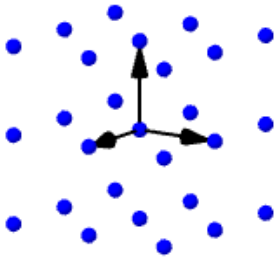


Figura 2.4: El retículo entero $\mathbb{Z}^3 \subset \mathbb{R}^3$.

2. Sea $B = (b_1, \ldots, b_n)$ una base de Λ. Entonces se cumple que $\Lambda = B\mathbb{Z}^n$ y, en particular, Λ es un subgrupo de $\mathbb{R}^n$, es decir, $b - \bar{b} \in \Lambda$ para todo $b, \bar{b} \in \Lambda$.

3. Sea $B = (b_1, \ldots, b_n)$ una base de Λ. Entonces, por la independencia lineal de los b_i podemos garantizar que $\det B \neq 0$, y por tanto la matriz B siempre será una matriz invertible de $\mathbb{R}^{n\times n}$.

Definición 2.19 (Matriz unimodular entera)**.**
Una *matriz de enteros* $U \in \mathbb{Z}^{n\times n}$ se dice *unimodular* si y sólo si $|\det U| = 1$. El *grupo de todas las matrices unimodulares enteras* se denota como $GL(n, \mathbb{Z})$.

Observemos que por su propia definición se deduce que una matriz de enteros es unimodular si y sólo si la matriz y su inversa son matrices de enteros.

Proposición 2.20. $GL(n, \mathbb{Z}) = \{U \in \mathbb{R}^{n\times n} : U\mathbb{Z}^n = \mathbb{Z}^n\}$.

Demostración. $U \in GL(n, \mathbb{Z})$ si y sólo si U, $U^{-1} \in \mathbb{Z}^{n\times n}$, lo que equivale a que

$$U\mathbb{Z}^n \subseteq \mathbb{Z}^n$$

y

$$U^{-1}\mathbb{Z}^n \subseteq \mathbb{Z}^n.$$

Como esta última inclusión es equivalente a que $\mathbb{Z}^n \subseteq U\mathbb{Z}^n$ se tiene el resultado deseado. □

Observación 2.21. Sea

$$A = \begin{pmatrix} 25 & 64 \\ 16 & 41 \end{pmatrix}.$$

Gracias a que A es una matriz unimodular entera, podemos asegurar que $\Lambda = A\mathbb{Z}^2 = \mathbb{Z}^2$

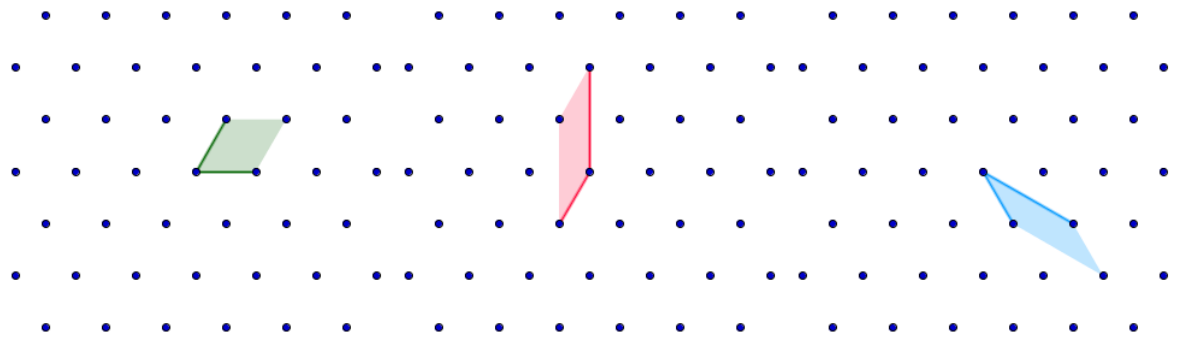
Lema 2.22. *Sea $\Lambda = B\mathbb{Z}^n \in \mathcal{L}^n$. $A = (a_1, a_2, \ldots, a_n)$ es una base de A si y sólo si existe $U \in GL(n, \mathbb{Z})$ tal que $A = BU$.*

Demostración. A es una base de Λ si y sólo si $A\mathbb{Z}^n = \Lambda = B\mathbb{Z}^n$ lo que es equivalente a que $B^{-1}A\mathbb{Z}^n = \mathbb{Z}^n$ y por tanto a que $U = B^{-1}A \in GL(n, \mathbb{Z})$ por la proposición 2.20. □

A continuación vamos a ver dos de los conceptos de mayor utilidad para la teoría de retículos, al punto de que, en cierta forma, identifican unívocamente nuestro retículo.

Definición 2.23 (Determinante, celda fundamental)**.**
Sea $\Lambda \in \mathcal{L}^n$ con base $B = (b_1, \ldots, b_n)$.

1. Se denomina el *determinante* de Λ a $\det \Lambda = |\det B|$.
2. $P_B = \{p_1b_1 + \cdots + p_nb_n : 0 \leq p_i < 1, 1 \leq i \leq n\} = B[0, 1)^n$ se denomina la *celda fundamental* o *paralelepípedo fundamental de* Λ (para cada base B).



(a) $B = \{(1, 0)^\intercal, (\frac{1}{2}, \frac{\sqrt{3}}{2})^\intercal\}$ (b) $B = \{(0, \sqrt{3})^\intercal, (-\frac{1}{2}, -\frac{\sqrt{3}}{2})^\intercal\}$ (c) $B = \{(\frac{1}{2}, -\frac{\sqrt{3}}{2})^\intercal, (\frac{3}{2}, -\frac{\sqrt{3}}{2})^\intercal\}$

Figura 2.5: Distintas celdas fundamentales para el retículo hexagonal según la base B elegida.

Observación 2.24. 1. Gracias al Lema 2.22 podemos asegurar que $\det \Lambda$ es independiente de la elección de la base B.

2. $\det \Lambda = \mathrm{vol}(P_B)$ y $\det(\mu\Lambda) = |\mu|^n \det \Lambda$, con $\mu \in \mathbb{R}$.

3. $\det \Lambda \leq |b_1||b_2| \dots |b_n|$, dándose la igualdad si y sólo si los vectores b_i son ortogonales dos a dos (Desigualdad de Hadamard).

4. $P_B \cap \Lambda = \{0\}$. Pero incluso podemos asegurar que $(P_B - P_B) \cap \Lambda = \{0\}$, puesto que $P_B - P_B = B \cdot (-1, 1)^n$.

Ahora, usando la función de redondeo por defecto $\lfloor \cdot \rfloor$, definida para $\mathbb{R}$, podemos dar una generalización de extrema utilidad para nuestros retículos:

Notación. Sean $a_1, a_2, \dots, a_n \in \mathbb{R}^n$ linealmente independientes y sea $A = (a_1, a_2, \dots, a_n)$. Sea $x \in \mathbb{R}^n$ con $x = \sum_{i=1}^n p_i a_i$ con los $p_i \in \mathbb{R}$. Denotamos entonces

$$\lfloor x \rfloor_A := \sum_{i=1}^{n} \lfloor p_i \rfloor a_i.$$

En particular, conseguimos que $\lfloor x \rfloor_A \in A\mathbb{Z}^n$ y que $x - \lfloor x \rfloor_A \in P_A$.

Proposición 2.25. *Sea $\Lambda = B\mathbb{Z}^n \in \mathcal{L}^n$. Entonces*

$$\mathbb{R}^n = \bigcup_{b \in \Lambda}^{\cdot} (b + P_B),$$

es decir, $\mathbb{R}^n$ es la unión disjunta de las traslaciones por el retículo de P_B.

Demostración. Para ver la igualdad basta con darse cuenta de que para todo $x \in \mathbb{R}^n$ tenemos que

$$x = (x - \lfloor x \rfloor_B) + \lfloor x \rfloor_B.$$

El primer sumando está en P_B y el segundo es un punto del retículo Λ.

Para probar que la unión es disjunta observamos que si para ciertos $b, \bar{b} \in \Lambda$ existe $x \in \mathbb{R}^n$ tal que $x \in (b + P_B) \cap (\bar{b} + P_B)$, entonces llegamos a que

$$b - \bar{b} = (b - x) - (\bar{b} - x) \in (P_B - P_B) \cap \Lambda = \{0\}.$$

Donde la última igualdad se debe al 4º item de la observación 2.24. Por tanto deducimos que $b = \bar{b}$, lo que concluye la prueba. □

Definición 2.26 (Conjunto discreto)**.**
Un conjunto $S \subset \mathbb{R}^n$ se denomina *discreto* si existe un $\varepsilon > 0$ tal que $|s_1 - s_2| \geq \varepsilon$ para todos $s_1, s_2 \in S$, $s_1 \neq s_2$.

Teorema 2.27. *$S \subset \mathbb{R}^n$ es un retículo si y sólo si S es un subgrupo discreto de $\mathbb{R}^n$ y contiene n puntos linealmente independientes.*

Demostración. Obviamente, todo retículo es un subgrupo de $\mathbb{R}^n$ que contiene n puntos linealmente independientes. Sea B la base del retículo y denotamos como ε al mínimo de la función $|Bx|$ en $\mathbb{S}^{n-1} := \{x = (x_1, \dots, x_n)^\intercal \in \mathbb{R}^n : \sum_{i=1}^n x_i^2 = 1\}$. Entonces para $z \in \mathbb{Z}^n \setminus \{0\}$ tenemos que $|Bz| \geq \varepsilon |z| \geq \varepsilon$, lo que prueba que el conjunto es discreto.

Para la otra dirección sean $s_1, s_2, \ldots, s_n \in S$ sus n puntos linealmente independientes. Vamos a razonar por inducción para probar que existen $b_1, b_2, \ldots, b_n \in S$ tales que, para $1 \leq k \leq n$,

$$\operatorname{lin}\{s_1, s_2, \ldots, s_k\} \cap S = \{x_1 b_1 + \cdots + x_k b_k : x_i \in \mathbb{Z}\}.$$

Por supuesto, el caso $k = n$ concluye la prueba.

Para el caso $k = 1$ sea $b_1 \neq 0$ el vector más pequeño en $\operatorname{conv}\{0, s_1\} \cap S$. Como S es discreto tal elección es posible, y al ser S un subgrupo tenemos que $\{x_1 b_1 : x_1 \in \mathbb{Z}\} \subset \operatorname{lin}\{s_1\} \cap S$. Sea $s \in \operatorname{lin}\{s_1\} \cap S$ y sea $\lambda \in \mathbb{R}$ tal que $s = \lambda b_1$. Entonces tenemos que $s - \lfloor \lambda \rfloor b_1 = (\lambda - \lfloor \lambda \rfloor) b_1 \in S$ y por la minimalidad de b_1 tiene que darse que $\lambda = \lfloor \lambda \rfloor \in \mathbb{Z}$. Con lo que ya tenemos

$$\{x_1 b_1 : x_1 \in \mathbb{Z}\} = \operatorname{lin}\{s_1\} \cap S$$

y, por tanto, el caso $k = 1$.

Asumamos que ya tenemos los primeros $b_1, b_2, \ldots, b_k$ y busquemos ahora el b_{k+1}. Consideremos el paralelepípedo $(k+1)$-dimensional

$$P_{k+1} = \left\{ \sum_{i=1}^{k} \alpha_i b_i + \alpha_{k+1} s_{k+1} : 0 \leq \alpha_i \leq 1 \right\}.$$

Sea $b_{k+1} \in P_{k+1} \cap S$ que tenga distancia más pequeña a $\operatorname{lin}\{b_1, b_2, \ldots, b_k\}$, es decir,

$$b_{k+1} = \sum_{i=1}^{k} \overline{\alpha}_i b_i + \overline{\alpha}_{k+1} s_{k+1}$$

y $\overline{\alpha}_{k+1} > 0$ es mínimo de entre todos los puntos de $P_{k+1} \cap S$. Obviamente, tenemos que $\operatorname{lin}\{b_1, \ldots, b_{k+1}\} = \operatorname{lin}\{s_1, \ldots, s_{k+1}\}$, luego

$$\{x_1 b_1 + \cdots + x_{k+1} b_{k+1} : x_i \in \mathbb{Z}\} \subset \operatorname{lin}\{s_1, \ldots, s_{k+1}\} \cap S.$$

Sea $s \in \operatorname{lin}\{s_1, \ldots, s_{k+1}\} \cap S$ dado por $s = \sum_{i=1}^{k+1} \beta_i b_i$, con $\beta_i \in \mathbb{R}$. Entonces tenemos que

$$\begin{aligned} s - \sum_{i=1}^{k+1} \lfloor \beta_i \rfloor b_i &= \sum_{i=1}^{k+1} (\beta_i - \lfloor \beta_i \rfloor) b_i = \sum_{i=1}^{k} (\beta_i - \lfloor \beta_i \rfloor) b_i + (\beta_{k+1} - \lfloor \beta_{k+1} \rfloor) b_{k+1} \\ &= \sum_{i=1}^{k} \Big[(\beta_i - \lfloor \beta_i \rfloor) + \overline{\alpha}_i (\beta_{k+1} - \lfloor \beta_{k+1} \rfloor) \Big] b_i + \overline{\alpha}_{k+1} (\beta_{k+1} - \lfloor \beta_{k+1} \rfloor) s_{k+1}. \end{aligned}$$

Para abreviar denotemos como μ_i a estos últimos coeficientes de los vectores, es decir

$$\mu_i = (\beta_i - \lfloor \beta_i \rfloor) + \overline{\alpha}_i (\beta_{k+1} - \lfloor \beta_{k+1} \rfloor)\ ,\ 1 \leq i \leq k,$$

$$\mu_{k+1} = \overline{\alpha}_{k+1} (\beta_{k+1} - \lfloor \beta_{k+1} \rfloor).$$

Entonces, como $0 \leq \beta_{k+1} - \lfloor \beta_{k+1} \rfloor < 1$, tenemos que $0 \leq \mu_{k+1} < \overline{\alpha}_{k+1}$ y también sabemos que

$$s - \sum_{i=1}^{k+1} \lfloor \beta_i \rfloor b_i - \sum_{i=1}^{k} \lfloor \mu_i \rfloor b_i = \sum_{i=1}^{k} (\mu_i - \lfloor \mu_i \rfloor) b_i + \mu_{k+1} s_{k+1} \in S \cap P_{k+1}.$$

Por la elección de $\overline{\alpha}_{k+1}$ y dado que $\mu_{k+1} < \overline{\alpha}_{k+1}$, tenemos que $\mu_{k+1} = 0$ y por tanto $\beta_{k+1} = \lfloor \beta_{k+1} \rfloor \in \mathbb{Z}$. Además, gracias a la hipótesis de inducción, tenemos que

$$s - \beta_{k+1} b_{k+1} = \sum_{i=1}^{k} \beta_i b_i \in \operatorname{lin}\{s_1, \ldots, s_k\} \cap S = \{x_1 b_1 + \cdots + x_{k+1} b_{k+1} : x_i \in \mathbb{Z}\}$$

y por lo tanto tenemos garantizada la integridad de los β_i, para todo $1 \leq i \leq k$. □

Corolario 2.28. *Sean $a_1, \dots, a_n \in \Lambda \in \mathcal{L}^n$ linealmente independientes. Entonces existe una base $b_1, \dots, b_n$ de Λ, tal que*

$$a_k \in \operatorname{lin}\{z_1 b_1 + \cdots + z_k b_k : z_i \in \mathbb{Z}\}, 1 \leq k \leq n.$$

Demostración. Basta aplicar el Teorema 2.27 con $s_i = a_i$, $1 \leq i \leq n$, y con $S = \Lambda$. □

Proposición 2.29. *Sea $K \subset \mathbb{R}^n$ un conjunto medible Riemann (con interior no vacío) y Λ un retículo arbitrario con determinante no nulo. Entonces*

$$\lim_{m\to\infty} \frac{\operatorname{vol}(mK)}{\#\{mK \cap \Lambda\}} = \det \Lambda. \tag{2.3}$$

Demostración. Observamos primero que es suficiente con probarlo para el retículo entero: en efecto, si tenemos que

$$\lim_{m\to\infty} \frac{\operatorname{vol}(mK)}{\#\{mK \cap \mathbb{Z}^n\}} = \det \mathbb{Z}^n = 1 \tag{2.4}$$

entonces, como $\Lambda = B\mathbb{Z}^n$ para alguna matriz $B \in GL(n, \mathbb{R})$, se tendría que

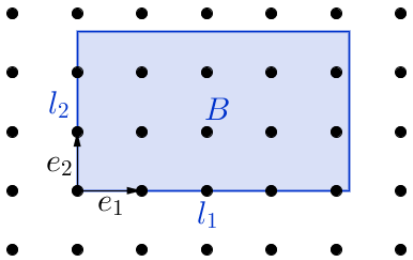
$$\#\{K \cap \Lambda\} = \#\{B^{-1}K \cap \mathbb{Z}^n\} \quad \text{y} \quad \operatorname{vol}(B^{-1}K) = \frac{1}{|\det B|}\operatorname{vol}(K),$$

y por tanto

$$\lim_{m\to\infty} \frac{\operatorname{vol}(mK)}{\#\{mK \cap \Lambda\}} = (\det \Lambda) \lim_{m\to\infty} \frac{\operatorname{vol}(mB^{-1}K)}{\#\{mB^{-1}K \cap \mathbb{Z}^n\}} = \det \Lambda.$$

Probemos pues (2.4).

Para probarlo primero consideramos $B = \{x = (x_1, \dots, x_n)^\intercal \in \mathbb{R}^n : 0 \leq x_i \leq l_i\}$ una caja ortogonal con uno de su vértices en el origen.



Entonces

$$\operatorname{vol}(B) = \prod_{i=1}^{n} l_i \quad \text{y} \quad \#\{B \cap \mathbb{Z}^n\} = \prod_{i=1}^{n} (\lfloor l_i \rfloor + 1),$$

y para $m \geq 0$,

$$\operatorname{vol}(mB) = m^n \prod_{i=1}^{n} l_i \quad \text{y} \quad \#\{mB \cap \mathbb{Z}^n\} = \prod_{i=1}^{n} (\lfloor m l_i \rfloor + 1).$$

Por lo tanto,

$$\lim_{m\to\infty} \frac{\operatorname{vol}(mB)}{\#\{mB \cap \mathbb{Z}^n\}} = \lim_{m\to\infty} \frac{m^n \prod_{i=1}^{n} l_i}{\prod_{i=1}^{n} (\lfloor m l_i \rfloor + 1)} = 1.$$

En segundo lugar, si consideramos una *policaja* $A = \cup_{i=1}^{k} B_i$, es decir, la unión (con interiores disjuntos) de una cantidad finita de cajas ortogonales, entonces $\operatorname{vol}(A) = \sum_{i=1}^{k} \operatorname{vol}(B_i)$, y fácilmente se obtiene que (2.4) se verifica también para A.

Finalmente, si K es un conjunto medible Jordan o Riemann (como en nuestro caso), se tiene que

$$\sup\{\mathrm{vol}(A) : A \text{ policaja }, A \subset K\} = \text{ínf}\{\mathrm{vol}(A') : A' \text{ policaja }, K \subset A'\},$$

y dado que el volumen es continuo, podemos concluir que (2.4) se verifica para K. □

Corolario 2.30. *Sea $K \subset \mathbb{R}^n$ un conjunto medible Riemann (con interior no vacío) y Λ un retículo arbitrario con determinante no nulo. Entonces*

$$\mathrm{vol}(K) = \lim_{m\to\infty} \#\left\{K \cap \frac{1}{m}\Lambda\right\} \frac{\det\Lambda}{m^n}. \tag{2.5}$$

Demostración. Esto resulta evidente si aplicamos la proposición 2.29 ya que

$$\#\left\{K \cap \frac{1}{m}\Lambda\right\} = \#\left\{mK \cap \Lambda\right\}. \qquad \square$$

Observación 2.31. Sean $\Lambda \in \mathcal{L}^n$ y $K \in \mathcal{K}^n$. Gracias a la proposición 2.29 estamos en condiciones de dar una primera aproximación para calcular $\#\{mK \cap \Lambda\}$ con $m \in \mathbb{R}$ suficientemente grande. Gracias a la ecuación (2.3) podemos asumir que

$$\#\{mK \cap \Lambda\} \approx \frac{\mathrm{vol}(mK)}{\det\Lambda}.$$

Ejemplo. Pongamos a prueba esa aproximación: Sea $K = \mathbb{B}_2 \subset \mathbb{R}^2$, sea $m = 3{,}2$ y consideramos Λ el retículo con base

$$B = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

Entonces gracias a la observación 2.24 y a la proposición 2.29 tenemos que

$$\det\Lambda = |\det B| = \frac{\sqrt{3}}{2} \quad \text{y que} \quad \mathrm{vol}(\mathbb{B}_2(3{,}2)) = \pi \cdot 3{,}2^2,$$

luego el valor de $\#\{\mathbb{B}_2(3{,}2) \cap \Lambda\}$ debería ser próximo a

$$\frac{\mathrm{vol}\left(\mathbb{B}_2(3{,}2)\right)}{\det\Lambda} = \frac{\pi \cdot 3{,}2^2 \cdot 2}{\sqrt{3}} = \frac{\pi \cdot 16^2 \cdot 2 \cdot \sqrt{3}}{5^2 \cdot 3} = \frac{\pi \cdot 512 \cdot \sqrt{3}}{75} \approx 37{,}146.$$

Por lo que, al observar la figura 2.6, comprobamos $\#\{\mathbb{B}_2(3{,}2) \cap \Lambda\} = 37$ y que se trata de una buena aproximación.

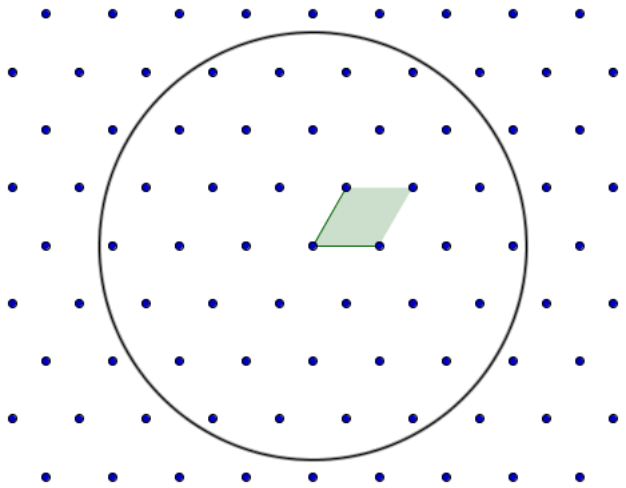


Figura 2.6: La bola $\mathbb{B}_2(3{,}2)$, el retículo $\Lambda \subset \mathbb{R}^2$ y su celda fundamental.

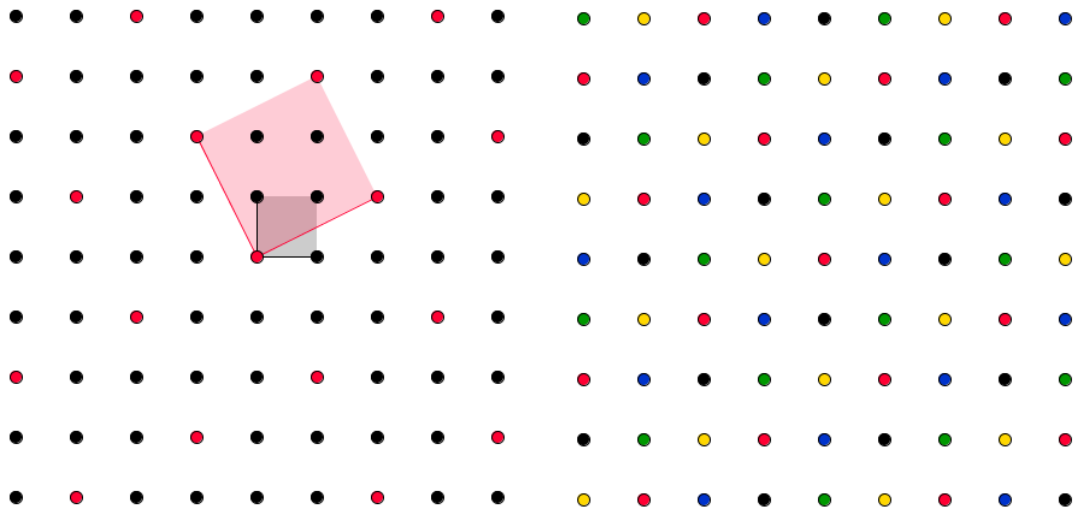
Definición 2.32 (Subretículo, Índice de un subretículo)**.**
Sea $\Lambda \in \mathcal{L}^n$ y sean $a_1, \ldots, a_n \in \Lambda$ linealmente independientes.

$$\Lambda_0 = \{z_1 a_1 + \cdots + z_n a_n : z_i \in \mathbb{Z}\}$$

es un nuevo retículo que recibe el nombre de *subretículo* de Λ con base $A = (a_1, \ldots, a_n)$.

Se denomina *índice de un subretículo* al número de clases laterales del subgrupo Λ_0 en Λ, es decir, al índice de Λ_0 en Λ y se denota como $|\Lambda : \Lambda_0|$.

Ejemplo. Vamos a ver un ejemplo de subretículo de nuestro ya conocido retículo entero:



(a) El subretículo Λ_0 (en rojo) sobre el retículo $\mathbb{Z}^2$ junto a las celdas fundamentales de ambos.

(b) Las distintas clases laterales de Λ_0 en $\mathbb{Z}^2$ marcadas en distintas tonalidades.

Figura 2.7: El subretículo $\Lambda_0 \subset \mathbb{Z}^2$ generado por los vectores $(2,1)^\intercal$ y $(-1,2)^\intercal$.

Lema 2.33. *Sea $\Lambda_0 \subset \Lambda \in \mathcal{L}^n$ un subretículo de Λ. Entonces*

1. $|\Lambda : \Lambda_0| = \#\{P_A \cap \Lambda\}$ *para cualquier base A de Λ_0.*
2. $|\Lambda : \Lambda_0| = \det \Lambda_0 / \det \Lambda$.

Demostración. 1. $|\Lambda : \Lambda_0| = \#\{P_A \cap \Lambda\}$ es equivalente a que cualquier punto reticular está en la misma clase que algún único punto de $P_A \cap \Lambda$, es decir, que

$$\Lambda = \bigcup_{c \in P_A \cap \Lambda}{}^{\cdot} \; (c + \Lambda_0).$$

Para todo $b \in \Lambda$ tenemos que $\lfloor b \rfloor_A \in \Lambda_0 \subset \Lambda$ y por tanto $(b - \lfloor b \rfloor_A) \in P_A \cap \Lambda$. Por lo que

$$b = (b - \lfloor b \rfloor_A) + \lfloor b \rfloor_A \in (P_A \cap \Lambda) + \Lambda_0.$$

Ahora, si existen $b_1, b_2 \in P_A \cap \Lambda$ tal que $\{x\} \subset (b_1 + \Lambda_0) \cap (b_2 + \Lambda_0) \neq \emptyset$ entonces

$$b_1 - b_2 = (b_1 - x) - (b_2 - x) \in (P_A - P_A) \cap \Lambda_0 = \{0\}.$$

Por tanto $b_1 = b_2$ y queda probada que dicha unión es disjunta.

2. Observamos que

$$mP_A = \bigcup_{1\le m_i<m}{}^{\cdot} (m_1a_1 + \cdots + m_na_n + P_A),$$

donde $m_i, m \in \mathbb{N}$. Más aún, ya que para todo $a \in \Lambda$ tenemos que $\#\{(a + P_A) \cap \Lambda\} = \#\{P_A \cap \Lambda\}$ y tras echar un vistazo a la primera parte del lema, deducimos que

$$\#\{mP_A \cap \Lambda\} = m^n \#\{P_A \cap \Lambda\} = m^n |\Lambda : \Lambda_0|.$$

Finalmente, como P_A es *medible Riemann*, gracias al corolario 2.30, podemos escribir

$$\det \Lambda_0 = \mathrm{vol} P_A = \lim_{m\to\infty} \#\Big\{P_A \cap \frac{1}{m}\Lambda\Big\}\frac{\det \Lambda}{m^n} = \det \Lambda \lim_{m\to\infty} \frac{\#\{mP_A \cap \Lambda\}}{m^n} = \det \Lambda\, |\Lambda : \Lambda_0|.$$

□

Corolario 2.34. *Sean $u_1, \ldots, u_n \in \mathbb{Z}^n$ linealmente independientes. Entonces*

$$|\det(u_1, \ldots, u_n)| = \#\Big\{\{p_1u_1 + \cdots + p_nu_n : 0 \le p_i < 1\} \cap \mathbb{Z}^n\Big\}.$$

Demostración. Basta con aplicar el lema 2.33 con $\Lambda = \mathbb{Z}^n$ y Λ_0 el subretículo de $\mathbb{Z}^n$ generado por los $u_1, \ldots, u_n$. □

Observación 2.35. Sea $\Lambda_0 = A\mathbb{Z}^n \in \mathcal{L}^n$ un subretículo de Λ. Entonces, si A es base de Λ es equivalente a que $\Lambda = \Lambda_0$, o lo que es lo mismo, a que $|\Lambda : \Lambda_0| = 1$ que, gracias al lema 2.33, equivale a que $\Lambda \cap P_A = \{0\}$ que claramente es lo mismo que

$$\Lambda \cap \{p_1a_1 + \cdots + p_na_n : 0 \le p_i \le 1\} = \{\varepsilon_1a_1 + \cdots + \varepsilon_na_n : \varepsilon_i \in \{0, 1\}\}.$$

Capítulo 3

El Teorema de Minkowski

En este capítulo vamos a ver, entre otros resultados, un teorema fundamental para abordar nuestro problema de contar puntos reticulares, así como algunas aplicaciones que tienen dichos resultados. Las referencias usadas para este capítulo son [3] y [4].

Lema 3.1. *Sea $\Lambda \in \mathcal{L}^2$ y sean $a_1, a_2 \in \Lambda$ linealmente independientes. Entonces*

$$a_1, a_2 \text{ base de } \Lambda \Leftrightarrow \operatorname{conv}\{0, a_1, a_2\} \cap \Lambda = \{0, a_1, a_2\}.$$

Demostración. Si a_1, a_2 son una base entonces cualquier punto de Λ tiene una única representación como una combinación entera de a_1 y a_2. Por lo tanto $\operatorname{conv}\{0, a_1, a_2\} \cap \Lambda = \{0, a_1, a_2\}$.

Para probar el otro sentido definimos $T_A = \operatorname{conv}\{0, a_1, a_2\}$ y

$$\overline{P}_A = \{p_1 a_1 + p_2 a_2 : 0 \leq p_1, p_2 \leq 1\}.$$

Por la observación 2.35 es suficiente con probar que

$$\overline{P}_A \cap \Lambda = \{0, a_1, a_2, a_1 + a_2\}.$$

Sea $b \in \overline{P}_A \cap \Lambda$, si $b \in T_A \cap \Lambda$ entonces tenemos que $b \in \{0, a_1, a_2\}$ por hipótesis. Supongamos ahora que $b \notin T_A$ y por tanto $b = p_1 a_1 + p_2 a_2$ con $0 \leq p_1, p_2 \leq 1$, pero con $p_1 + p_2 > 1$. Pero entonces tenemos que como $(1 - p_1) + (1 - p_2) < 1$, entonces

$$(a_1 + a_2) - b = (1 - p_1)\, a_1 + (1 - p_2)\, a_2 \in T_A \cap \Lambda = \{0, a_1, a_2\},$$

Lo que implica que $b \in \{a_1, a_2, a_1 + a_2\}$ y esto concluye la prueba ya que el otro contenido es evidente. □

Observación 3.2. No puede existir un lema análogo para dimension ≥ 3.

Para $n \geq 3$ y $m \in \mathbb{N}$ consideramos $b(m) = (1, \ldots, 1, m)^\intercal \in \mathbb{R}^n$ y

$$T^n(m) = \operatorname{conv}\{0, e_1, e_2, \ldots, e_{n-1}, b(m)\}.$$

Se tiene que

$$T^n(m) \cap \mathbb{Z}^n = \{0, e_1, e_2, \ldots, e_{n-1}, b(m)\},$$

pero el determinante del retículo con base $B = \{e_1, e_2, \ldots, e_{n-1}, b(m)\}$ es m, por lo que esta base no puede ser base de $\mathbb{Z}^n$ ($\det \mathbb{Z}^n = 1$).

Los $T^n(m)$ se denominan los *símplices de Reeve*.

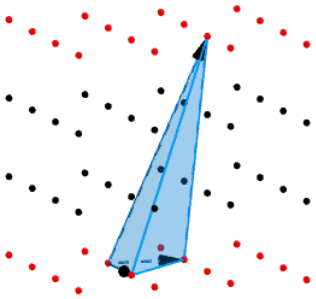


Figura 3.1: $T^3(3)$, $\Lambda_0 = B\mathbb{Z}^n$ (en rojo) y su base $\{e_1, e_2, b(3)\}$.

Lema 3.3. *Sean $u_1, \ldots, u_m \in \mathbb{Z}^n$ y sean $k_i \in \mathbb{N}$, tal que $k_1 \geq 1$, $1 \leq i \leq m$. El conjunto*

$$\Lambda = \{z \in \mathbb{Z}^n : \langle u_i, z\rangle \equiv 0 \text{ mód } k_i, 1 \leq i \leq m\}$$

es un retículo con $\det \Lambda \leq k_1 k_2 \cdots k_m$.

Demostración. Por definición Λ es un subgrupo discreto de $\mathbb{R}^n$, incluso de $\mathbb{Z}^n$. Como los n vectores linealmente independientes $(k_1 \cdots k_m)e_i$, con $1 \leq i \leq n$, pertenecen a Λ, el Teorema 2.27 prueba que Λ es un retículo.

Como Λ es un subretículo de $\mathbb{Z}^n$ podemos considerar las diferentes clases laterales de Λ con respecto a $\mathbb{Z}^n$. Dos puntos $z_1, z_2 \in \mathbb{Z}^n$ pertenecerán a diferentes clases laterales si y sólo si $z_1 - z_2 \notin \Lambda$, es decir, si existe un "i" tal que $\langle u_i,\ z_1 - z_2\rangle \not\equiv 0$ mód k_i.

Es decir, para algún u_i los enteros $\langle u_i, z_1\rangle$ y $\langle u_i, z_2\rangle$ han de pertenecer a distintas clases residuales mód k_i. Para cada u_i tenemos entonces como mucho k_i clases residuales y por tanto el número máximo de clases laterales que podemos obtener viene dado por el producto $k_1 \cdots k_m$. Y concluimos el lema puesto que entonces

$$det\Lambda = |\mathbb{Z}^n : \Lambda|\, \cancelto{1}{det\mathbb{Z}^n} \leq k_1 k_2 \cdots k_m. \qquad \square$$

Lema 3.4. *Sea $X \subset \mathbb{R}^n$ un conjunto medible y acotado.*

1. *Si $(z_1 + X) \cap (z_2 + X) = \emptyset$, para todo $z_1, z_2 \in \mathbb{Z}^n$, $z_1 \neq z_2$, entonces* $\text{vol}(X) \leq 1$.
2. *Si $X + \mathbb{Z}^n = \mathbb{R}^n$ entonces* $\text{vol}(X) \geq 1$.

Demostración. Sea $P = [0,1)^n$ la celda fundamental de $\mathbb{Z}^n$, y sea $M = \{z \in \mathbb{Z}^n : (z + P) \cap X \neq \emptyset\}$. Entonces, por la Proposición 2.25, tenemos que

$$\text{vol}(X) = \text{vol}((\mathbb{Z}^n + P) \cap X) = \sum_{z \in M} \text{vol}((z + P) \cap X) = \sum_{z \in M} \text{vol}(P \cap (X - z)).$$

Para probar el primer caso usamos que $[P \cap (X - z_1)] \cap [P \cap (X - z_2)] = \emptyset$ para $z_1 \neq z_2 \in \mathbb{Z}^n$, y por lo tanto

$$\text{vol}(X) = \sum_{z \in M} \text{vol}(P \cap (X - z)) = \text{vol}(P \cap (X - \mathbb{Z}^n)) \leq \text{vol}(P) = 1.$$

Para el segundo caso tenemos que

$$\text{vol}(X) = \sum_{z \in M} \text{vol}(P \cap (X - z)) \geq \text{vol}(P \cap \cancelto{\mathbb{R}^n}{(X + \mathbb{Z}^n)}) = \text{vol}(P) = 1. \qquad \square$$

Corolario 3.5. *Sea $X \subset \mathbb{R}^n$ con $\mathrm{vol}(X) > 1$. Entonces existen $x_1, x_2 \in X$, con $x_1 \neq x_2$, tal que $x_1 - x_2 \in \mathbb{Z}^n$. (En otras palabras, entonces existe un $t \in \mathbb{R}^n$ tal que $X + t$ contiene al menos dos puntos del retículo $\mathbb{Z}^n$).*

Demostración. Por el lema 3.4 deducimos que deben existir $z_1, z_2 \in \mathbb{Z}^n$, con $z_1 \neq z_2$ y un $x \in \mathbb{R}^n$ tal que $x \in (z_1 + X) \cap (z_2 + X)$. Por lo tanto $x - z_1, x - z_2 \in X$ y $(x - z_1) - (x - z_2) \in \mathbb{Z}^n$.

La aclaración se obtiene considerando $t = -x_2$, con $x_2 \in X$ del enunciado, y comprobando entonces que tanto $0 = x_2 - x_2 = x_2 + t \in X + t$ como $x_1 - x_2 = x_1 + t \in X + t$. □

3.1. Teorema de Minkowski y sus consecuencias

El siguiente resultado fue probado por Minkowski en [5]. Sin embargo, para la prueba me he basado en [1].

Teorema 3.6 (Minkowski)**.** *Sea $K \in \mathcal{K}_0^n$ con $\mathrm{vol}(K) \geq 2^n$. Entonces*

$$K \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset,$$

es decir, un cuerpo convexo 0-simétrico de volumen al menos 2^n siempre contiene un punto no trivial del retículo entero.

Demostración. Primero supongamos que $\mathrm{vol}(K) > 2^n$. Entonces tenemos que $\mathrm{vol}(\frac{1}{2}K) > 1$ y por el corolario 3.5 existen $x_1, x_2 \in \frac{1}{2}K$, $x_1 \neq x_2$, tal que $x_1 - x_2 \in \mathbb{Z}^n$. Como $x_1 - x_2 \in \frac{1}{2}K - \frac{1}{2}K = K$ hemos terminado.

Para el caso $\mathrm{vol}(K) = 2^n$ procedemos por reducción al absurdo: suponemos que $K \cap \mathbb{Z}^n = \{0\}$. Como K es compacto existe un $\lambda > 1$ tal que $\lambda K \cap \mathbb{Z}^n = \{0\}$. Sin embargo $\mathrm{vol}(\lambda K) = \lambda^n 2^n > 2^n$ y tenemos un contradicción con el caso anterior. □

Observación 3.7. El cubo $[-1, 1]^n$ prueba que la condición sobre el volumen es la mejor (en general) posible.

Corolario 3.8. *Sea $\Lambda \in \mathcal{L}^n$ y $K \in \mathcal{K}_0^n$ con $\mathrm{vol}(K) \geq 2^n \det \Lambda$. Entonces*

$$K \cap \Lambda \setminus \{0\} \neq \emptyset.$$

Demostración. Sea B una base de Λ. Entonces tenemos que

$$K \cap \Lambda = B(B^{-1}K \cap \mathbb{Z}^n), \text{ y que } \mathrm{vol}(B^{-1}K) = \frac{\mathrm{vol}(K)}{\det \Lambda} \geq 2^n.$$

Luego el corolario se sigue inmediatamente del Teorema 3.6 de Minkowski. □

Proposición 3.9. *Sea p un número primo. Entonces existen $a, b \in \mathbb{N}$ tales que*

$$a^2 + b^2 + 1 \equiv 0 \text{ mód } p.$$

Demostración. Para $p = 2$ la prueba resulta evidente tomando $a = 1, b = 0$.

Consideramos ahora que p sea impar. Para $0 \leq a \leq \frac{1}{2}(p-1)$ los números a^2 pertenecen a distintas clases residuales mód p, dado que

$$a^2 \equiv \bar{a}^2 \text{ mód } p \quad \Leftrightarrow \quad (a - \bar{a})(a + \bar{a}) \equiv 0 \text{ mód } p \quad \Leftrightarrow \quad p \mid (a - \bar{a})(a + \bar{a}) \quad \Leftrightarrow \quad a = \bar{a}.$$

Sucede exactamente lo mismo si miramos ahora las clases residuales de los $-b^2 - 1$ para $0 \leq b \leq \frac{1}{2}(p-1)$. Dado que sólo hay p clases residuales mód p y tenemos $\frac{1}{2}(p-1)+1$ elecciones

de clases distintas para los a y para los b que elijamos, debe existir una elección de a y b tales que esas clases coincidan (puesto que $[\frac{1}{2}(p-1)+1]+[\frac{1}{2}(p-1)+1] = (p-1)+2 = p+1 > p$).

Así pues, es posible elegir $0 \leq a, b \leq \frac{1}{2}(p-1)$ tal que $a^2 \equiv -(b^2+1)$ mód p, lo que concluye la prueba. □

Teorema 3.10 (Fermat, Lagrange)**.** *Todo entero positivo $m \in \mathbb{N}$ puede ser escrito como la suma de cuatro cuadrados, es decir, existen $m_1, m_2, m_3, m_4 \in \mathbb{N}$ tales que*

$$m = (m_1)^2 + (m_2)^2 + (m_3)^2 + (m_4)^2.$$

Demostración. Lo primero es destacar que es suficiente con probar el teorema para aquellos enteros *m libres de cuadrados*, es decir, los enteros que no son divididos por ningún número al cuadrado (salvo el 1).

En segundo lugar, si $n = n_1 n_2$ y $n_1 = x_1^2 + y_1^2 + z_1^2 + t_1^2$ y $n_2 = x_2^2 + y_2^2 + z_2^2 + t_2^2$, entonces

$$\begin{aligned} n = n_1 n_2 &= (x_1^2 + y_1^2 + z_1^2 + t_1^2)(x_2^2 + y_2^2 + z_2^2 + t_2^2) \\ &= (x_1x_2 - y_1y_2 - z_1z_2 - t_1t_2)^2 + (x_1y_2 + y_1x_2 + z_1t_2 - t_1z_2)^2 \\ &\quad + (x_1x_2 - y_1t_2 + z_1x_2 + t_1y_2)^2 + (x_1t_2 + y_1z_2 - z_1y_2 + t_1x_2)^2, \end{aligned}$$

luego basta con probar el enunciado para los números primos.

Como $2 = 1^2 + 1^2 + 0^2 + 0^2$, vamos a probarlo para p un primo impar. Según la proposición 3.9 es posible elegir a, b tales que $a^2 + b^2 + 1 \equiv 0$ mód p.

Consideramos ahora el retículo de $\mathbb{R}^4$ definido por

$$\Lambda = \{(x, y, z, t)^\intercal \in \mathbb{Z}^4 : z \equiv ax + by \text{ mód } p,\ t \equiv bx - ay \text{ mód } p\}.$$

El lema 3.3 nos asegura que $\det \Lambda \leq p^2$. De hecho se tiene que una base de Λ es

$$\text{Base de } \Lambda:\ \{(a, b, -1, 0)^\intercal, (-b, a, 0, 1)^\intercal, (p, 0, 0, 0)^\intercal, (0, p, 0, 0)^\intercal\},$$

por lo que incluso podemos asegurar que $\det \Lambda = p^2$.

Si consideramos la bola 4-dimensional de radio $r = \sqrt{1{,}9\, p}$, obtenemos que

$$\text{vol}(\mathbb{B}_4(r)) = \frac{r^4\, \pi^2}{2} = \frac{(1{,}9)^2\, \pi^2}{2} p^2 > 2^4 \det \Lambda.$$

Como consecuencia, el corolario 3.8 nos asegura la existencia de un $(x, y, z, t)^\intercal \neq 0$ tal que $(x, y, z, t)^\intercal \in \Lambda \cap \mathbb{B}_4(r)$ y por tanto que

$$0 \neq x^2 + y^2 + z^2 + t^2 \leq r^2 < 2p.$$

Por otro lado, tenemos que

$$x^2 + y^2 + z^2 + t^2 \equiv x^2 + y^2 + (ax + by)^2 + (bx - ay)^2 \equiv (x^2 + y^2)(a^2 + b^2 + 1) \equiv 0 \text{ mód } p.$$

Y como tenemos que $x^2 + y^2 + z^2 + t^2$ es múltiplo de p, distinto de 0 y también es estrictamente menor que $2p$, ha de darse que $p = x^2 + y^2 + z^2 + t^2$ con lo que concluye la prueba. □

Teorema 3.11. *Sea $k \in \mathbb{N}$ y sea $X \subset \mathbb{R}^n$ un conjunto medible Riemann con $\text{vol}(X) > k$. Entonces existen $x_1, x_2, \ldots, x_{k+1} \in X$ con $x_i \neq x_j$ para $1 \leq i \neq j \leq k+1$, tales que $x_i - x_j \in \mathbb{Z}^n$. (Dicho de otra forma: existe un $t \in \mathbb{R}^n$ tal que $t + X$ contiene al menos $k+1$ puntos reticulares de $\mathbb{Z}^n$).*

Demostración. Como tenemos un conjunto medible Riemann aplicando el corolario 2.30 sabemos que

$$k < \mathrm{vol}(X) = \lim_{m\to\infty} \#\left\{X \cap \frac{1}{m}\mathbb{Z}^n\right\} \frac{1}{m^n}.$$

Por lo que existe un $m \in \mathbb{N}$ tal que $\#\left\{X \cap \frac{1}{m}\mathbb{Z}^n\right\} > km^n$. Si consideramos el retículo $\frac{1}{m}\mathbb{Z}^n$ y como subretículo de éste a $\mathbb{Z}^n$ tenemos entonces por el lema 2.33 que

$$\left|\frac{1}{m}\mathbb{Z}^n : \mathbb{Z}^n\right| = \frac{\det \mathbb{Z}^n}{\det\left(\frac{1}{m}\mathbb{Z}^n\right)} = \frac{1}{\frac{1}{m^n}} = m^n,$$

pero como $\#\left\{X \cap \frac{1}{m}\mathbb{Z}^n\right\} > km^n$ y como mucho hay m^n clases laterales de $\mathbb{Z}^n$ como subretículo de $\frac{1}{m}\mathbb{Z}^n$, deben existir al menos $(k+1)$ diferentes $x_1, \ldots, x_{k+1} \in X \cap \frac{1}{m}\mathbb{Z}^n$ perteneciendo a la misma clase lateral, y por tanto, cumpliendo $x_i - x_j \in \mathbb{Z}^n$. □

Corolario 3.12. *Sea $\Lambda \in \mathcal{L}^n$ y sea $K \in \mathcal{K}^n$ con $\mathrm{vol}(K) \geq k2^n \det\Lambda$. Entonces*

$$\#\{K \cap \Lambda\} \geq 2k+1.$$

Demostración. Lo primero es probar el resultado para $\Lambda = \mathbb{Z}^n$ y suponiendo a su vez que $\mathrm{vol}(K) > k2^n$, o lo que es lo mismo, que

$$\mathrm{vol}\left(\frac{1}{2}K\right) > k.$$

En este caso el Teorema 3.11 garantiza la existencia de $(k+1)$ puntos distintos $x_1, \ldots, x_{k+1} \in \frac{1}{2}K$ con $x_i - x_j \in \mathbb{Z}^n$. Asumamos que x_1 tiene longitud máxima entre los x_i y consideramos $z_i = x_{i+1} - x_1$, $1 \leq i \leq k$. Entonces tenemos que $z_i \neq z_j$, $i \neq j$ y $z_i \in K \cap \mathbb{Z}^n \setminus \{0\}$. En realidad tenemos más que eso, ya que por la elección de x_1 todos los puntos cumplen que $\langle x_1, z_i\rangle < 0$ lo que implica que los $2k$ puntos $\pm z_i$, $1 \leq i \leq k$, son distintos dos a dos. Estos puntos junto al punto 0 nos da la cota inferior deseada.

Por otro lado, si $\mathrm{vol}(K) = k2^n$ y suponemos que $\#\{K \cap \Lambda\} < 2k+1$, como K es compacto, entonces existe $\lambda > 1$ tal que $\#\{\lambda K \cap \Lambda\} < 2k+1$, pero esto no puede ser porque contradice el caso anterior puesto que $\mathrm{vol}(\lambda K) > k2^n$.

Finalmente, sea Λ un retículo cualquiera, y consideramos B una base de Λ. Entonces

$$K \cap \Lambda = B(B^{-1}K \cap \mathbb{Z}^n) \quad \text{y también tenemos que} \quad \mathrm{vol}(B^{-1}K) = \frac{\mathrm{vol}(K)}{\det\Lambda} \geq k2^n$$

con lo que podemos aplicar el primer caso con el cuerpo convexo $B^{-1}K$ para obtener

$$\#\{B^{-1}K \cap \mathbb{Z}^n\} \geq 2k+1 \quad \text{y por tanto} \quad \#\{K \cap \Lambda\} \geq 2k+1. \qquad \square$$

3.2. Una versión equivalente del teorema de Minkowski.

Notación. Sean $K \in \mathcal{K}_0^n$, $\Lambda \in \mathcal{L}^n$. Entonces denotaremos

$$\lambda_1(K,\Lambda) := \text{mín}\{\lambda > 0 : \dim(\lambda K \cap \Lambda) \geq 1\} = \text{mín}\{\lambda > 0 : \lambda K \text{ contiene un punto no nulo de } \Lambda\}.$$

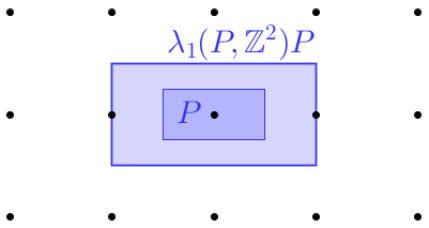


Figura 3.2: Un politopo P junto con $\lambda_1(P,\mathbb{Z}^2)P$.

Observación 3.13.

1. Si $A \in GL(n,\mathbb{R})$, es decir, $A \in \mathbb{R}^{n\times n}$ con $\det A \neq 0$, entonces $\lambda_1(K,\Lambda) = \lambda_1(AK, A\Lambda)$.
2. Si $\mu \in \mathbb{R}$ con $\mu \neq 0$, entonces $\lambda_1(\mu K,\Lambda) = \frac{1}{\mu}\lambda_1(K,\Lambda) = \lambda_1(K,\frac{1}{\mu}\Lambda)$.
3. $(\operatorname{int} K)\cap\Lambda\setminus\{0\} = \emptyset$ si y sólo si $\lambda_1(K,\Lambda) \geq 1$.
4. $\lambda_1(\mathbb{B}_n,\Lambda) = \min\{|u| : u \in \Lambda\setminus\{0\}\}$.

Observación 3.14. Resulta de interés comentar que a veces es suficiente con probar propiedades para el retículo $\mathbb{Z}^n$, pudiendo generalizarse dichos resultados a cualquier otro retículo. Esto se produce cuando en las propiedades que se quieren generalizar intervienen operadores de retículos y cuerpos convexos que son invariantes por "transformaciones" producidas por matrices A con $\det A \neq 0$.

Si consideramos $K \in \mathcal{K}^n$ y $\Lambda \in \mathcal{L}^n$, es fácil observar que cualquier propiedad que enunciemos en términos de $\#\{K\cap\Lambda\}$ y de $\lambda_1(K,\Lambda)$ se podrá generalizar a cualquier retículo una vez esté probada para $\mathbb{Z}^n$: si B es una base para Λ tenemos que $\Lambda = B\mathbb{Z}^n$ y bastaría con considerar el cuerpo convexo $\overline{K} = B^{-1}K$ ya que entonces

$$\#\{K\cap\Lambda\} = \#\{BB^{-1}K\cap\Lambda\} = \#\{B\overline{K}\cap B\mathbb{Z}^n\} = \#\{\overline{K}\cap\mathbb{Z}^n\}$$

y, gracias al primer item de la obsevación 3.13,

$$\lambda_1(K,\Lambda) = \lambda_1(B^{-1}K, B^{-1}\Lambda) = \lambda_1(B^{-1}K, B^{-1}B\mathbb{Z}^n) = \lambda_1(\overline{K},\mathbb{Z}^n).$$

Por tanto, al probar que una propiedad se verifica para $\mathbb{Z}^n$, serviría para generalizar el resultado a cualquier retículo.

El siguiente resultado no es más que una reformulación del Teorema 3.6 de Minkowski.

Teorema 3.15 (Minkowski, versión equivalente)**.** *Sean $K \in \mathcal{K}_0^n$ y $\Lambda \in \mathcal{L}^n$. Entonces*

$$\lambda_1(K,\Lambda)^n \operatorname{vol}(K) \leq 2^n \det\Lambda.$$

Demostración. Por la definición de $\lambda_1(K,\Lambda)$ tenemos que $\operatorname{int}[\lambda_1(K,\Lambda)K]\cap\Lambda\setminus\{0\} = \emptyset$ y entonces por el corolario 3.8 tenemos que

$$\operatorname{vol}(\lambda_1(K,\Lambda)K) = \operatorname{vol}(\operatorname{int}[\lambda_1(K,\Lambda)K]) \leq 2^n\det\Lambda. \qquad \square$$

Teorema 3.16. *Sea $K \in \mathcal{K}_0^n$ y sea $\Lambda \in \mathcal{L}^n$. Entonces*

$$\#\{K\cap\Lambda\} \leq \left(\left\lfloor \frac{2}{\lambda_1(K,\Lambda)} + 1\right\rfloor\right)^n.$$

Demostración. Gracias a la observación 3.14 podemos limitarnos a probar el resultado para $\Lambda = \mathbb{Z}^n$. Para facilitar la notación denotamos por λ_1 a $\lambda_1(K, \mathbb{Z}^n)$. Sea entonces

$$k = \left\lfloor \frac{2}{\lambda_1(K, \mathbb{Z}^n)} + 1 \right\rfloor.$$

Supongamos que existen $a = (a_1, \ldots, a_n)^\intercal, b = (b_1, \ldots, b_n)^\intercal \in K \cap \mathbb{Z}^n$ tal que cada $a_i - b_i \equiv 0$ mód k para $1 \leq i \leq n$. Entonces deducimos que

$$\frac{1}{k}(a-b) = \frac{2}{k}\left(\frac{1}{2}a - \frac{1}{2}b\right) \in \frac{2}{k}K \subset \operatorname{int}(\lambda_1 K) \cap \mathbb{Z}^n \setminus \{0\},$$

ya que $2/k < \lambda_1$. Pero por la definición de λ_1 tenemos que

$$\dim(\ \operatorname{int}(\lambda_1 K) \cap \mathbb{Z}^n\ ) = 0$$

y por tanto tiene que darse que $a = b$.

Resumiendo: hemos probado que para dos puntos reticulares $a, b \in K$ debe existir alguna coordenada con $a_i - b_i \not\equiv 0$ mód k. Por lo que el cardinal de $K \cap \mathbb{Z}^n$ no puede exceder k^n. □

Corolario 3.17. *Sean $K \in \mathcal{K}_0^n$ y $\Lambda \in \mathcal{L}^n$ con $(\operatorname{int} K) \cap \Lambda = \{0\}$. Entonces $\#\{K \cap \Lambda\} \leq 3^n$.*

Demostración. Resulta evidente ya que gracias a la observación 3.13 sabemos que $\lambda_1(K, \Lambda) \geq 1$, y aplicando el Teorema 3.16 deducimos que

$$\#\{K \cap \Lambda\} \leq \left(\left\lfloor \frac{2}{\lambda_1(K, \Lambda)} + 1 \right\rfloor\right)^n \leq (\lfloor 2 + 1 \rfloor)^n = 3^n. \qquad \square$$

Capítulo 4

El polinomio de Ehrhart

En este capítulo vamos a ver una batería de resultados todos enfocados a obtener un cierto polinomio que nos permita calcular los puntos reticulares de nuestros politopos convexos, o más bien, de un tipo concreto de ellos, aquellos que están "apoyados" en puntos del retículo. La bondad de estos métodos radica en que si logramos conocer los coeficientes de dicho polinomio seremos capaces de determinar los puntos reticulares no sólo para nuestro politopo, sino para cualquier "dilatación" suya.

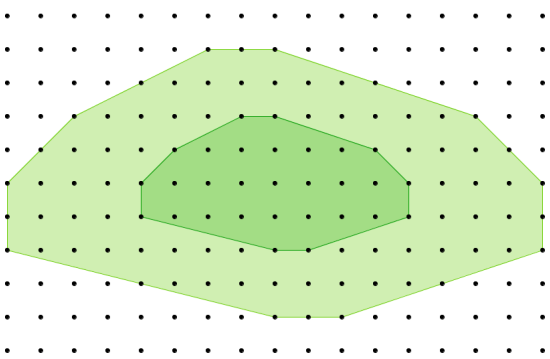


Figura 4.1: Un politopo P y su dilatación de tamaño 2, $2P$.

Primero veremos resultados enfocados a politopos 2-dimensionales, pero estudiaremos también una generalización para cualquier dimensión.

Los resultados de este capítulo han sido recopilados de [3] y [4].

Definición 4.1 (Politopo reticular)**.**

Un politopo $P \in \mathcal{P}^n$ se denomina *politopo reticular* con respecto a un retículo $\Lambda \in \mathcal{L}^n$ si todos los vértices de P son puntos reticulares de Λ. El conjunto de todos los politopos reticulares con respecto a Λ lo denotaremos por $\mathcal{P}^n_\Lambda$. En el caso del retículo entero $\mathbb{Z}^n$ utilizaremos la notación $\mathcal{P}^n_\mathbb{Z}$ para mayor comodidad.

Hasta ahora no hemos tenido demasiadas complicaciones en las cuentas, sin embargo a partir de ahora las cosas no serán tan sencillas, por lo que es conveniente que definamos un operador para lo que hasta ahora denotábamos como #.

Notación. Para $S \subset \mathbb{R}^n$ y un retículo $\Lambda \in \mathcal{L}^n$ denotaremos como $G_\Lambda(\cdot)$ al operador "cardinal de puntos reticulares", es decir,

$$G_\Lambda(S) = \#\{S \cap \Lambda\}.$$

En el caso del retículo entero escribiremos $G(S)$ en vez de $G_{\mathbb{Z}^n}(S)$.

4.1. Caso 2-dimensional

Lema 4.2. *Sean $a_1, a_2 \in \Lambda \in \mathcal{L}^2$ linealmente independientes, y sea $T = \operatorname{conv}\{0, a_1, a_2\}$. Entonces se tiene que*

$$G_\Lambda(T) = \frac{\operatorname{vol}(T)}{\det \Lambda} + \frac{1}{2} G_\Lambda(\operatorname{fr} T) + 1.$$

Demostración. Sea Λ_0 el subretículo de Λ generado por $A = (a_1, a_2)$, y sea $P_A = \{\lambda_1 a_1 + \lambda_2 a_2 : 0 \leq \lambda_i < 1\}$. Por el lema 2.33 tenemos que

$$G_\Lambda(P_A) = \frac{\det \Lambda_0}{\det \Lambda} = \frac{|\det(a_1, a_2)|}{\det \Lambda} = \frac{\operatorname{vol}(P_A)}{\det \Lambda} = \frac{2\operatorname{vol}(T)}{\det \Lambda}.$$

Ahora vamos a dividir los puntos reticulares de P_A en tres partes: $U_1 = \operatorname{int} T \cap \Lambda$, $U_2 = \operatorname{fr} T \cap \Lambda$ y $U_3 = (P_A \setminus T) \cap \Lambda$.

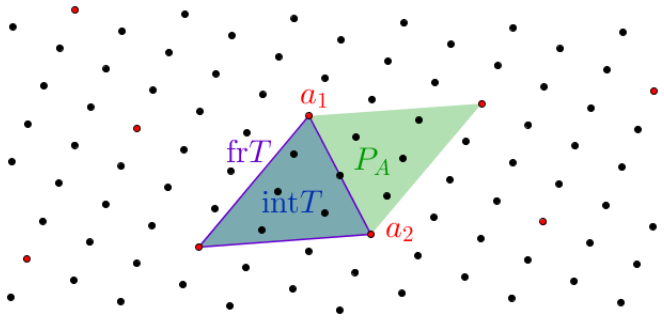


Figura 4.2: El subretículo Λ_0 (en rojo), el interior y la frontera de T, P_A y los puntos a_1y a_2.

Entonces $G_\Lambda(P_A) = \#U_1 + \#U_2 + \#U_3 - 2$, ya que $a_1, a_2 \notin P_A$. Además, observamos que $P_A \setminus T = \{\lambda_1 a_1 + \lambda_2 a_2 : \lambda_1 + \lambda_2 > 1, 0 \leq \lambda_i < 1\} = (a_1 + a_2) - \operatorname{int} T$. Por lo tanto $\#U_3 = \#U_1$ y entonces

$$\frac{2\operatorname{vol}(T)}{\det \Lambda} = G_\Lambda(U) = 2\#U_1 + \#U_2 - 2 = 2G_\Lambda(T) - G_\Lambda(\operatorname{fr} T) - 2,$$

donde despejamos $G_\Lambda(T)$ para obtener

$$G_\Lambda(T) = \frac{\operatorname{vol}(T)}{\det \Lambda} + \frac{1}{2} G_\Lambda(\operatorname{fr} T) + 1. \qquad \square$$

El siguiente resultado fue probado por Pick en [6]. Sin embargo, para la prueba me he basado en [1].

Teorema 4.3 (Pick)**.** *Sea $P \in \mathcal{P}^n_\Lambda$ un politopo reticular 2-dimensional. Entonces*

$$G_\Lambda(P) = \frac{\operatorname{vol}(P)}{\det \Lambda} + \frac{1}{2} G_\Lambda(\operatorname{fr} P) + 1.$$

Demostración. Gracias a la observación 2.9 podemos considerar $P = \operatorname{conv}\{v_1, \ldots, v_m\}$, donde asumimos que $v_1, \ldots, v_m \in \Lambda$ son los vértices de P en un orden cíclico. Procedamos por inducción sobre m.

El caso $m = 3$ resulta de aplicar el lema 4.2.

Asumamos ahora que tenemos probados todos los casos $1, \ldots, m-1$ y pasemos a probar el caso m ($m > 3$). Sean $P_1 = \operatorname{conv}\{v_1, v_2, v_m\}$ y $P_2 = \operatorname{conv}\{v_2, \ldots, v_m\}$.

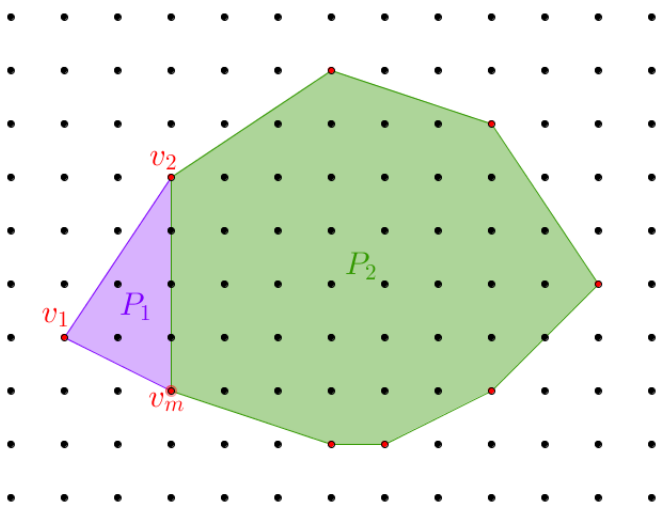


Figura 4.3: El símplice P_1, el politopo P_2 y los puntos resticulares v_1, v_2 y v_m.

Ambos politopos reticulares tienen menos de m vértices y por tanto usando (1.1), el lema 4.2 y la hipótesis de inducción obtenemos que

$$\begin{aligned} G_\Lambda(P) &= G_\Lambda(P_1) + G_\Lambda(P_2) - G_\Lambda\left(\operatorname{conv}\{v_2, v_m\}\right) \\ &= \frac{\operatorname{vol}(P_1)}{\det\Lambda} + \frac{1}{2}G_\Lambda(\operatorname{fr} P_1) + 1 + \frac{\operatorname{vol}(P_2)}{\det\Lambda} + \frac{1}{2}G_\Lambda(\operatorname{fr} P_2) + 1 - G_\Lambda\left(\operatorname{conv}\{v_2, v_m\}\right) \\ &= \frac{\operatorname{vol}(P)}{\det\Lambda} + \frac{1}{2}G_\Lambda(\operatorname{fr} P) + 1. \end{aligned}$$

□

Observación 4.4. Sea $P \in \mathcal{P}_\Lambda^n$ un politopo reticular 2-dimensional y sea $k \in \mathbb{N}$. Entonces

$$G_\Lambda(kP) = k^2\frac{\operatorname{vol}(P)}{\det\Lambda} + \frac{k}{2}G_\Lambda(\operatorname{fr} P) + 1.$$

Corolario 4.5. *Sea $P \in \mathcal{P}_\Lambda^n$ un politopo reticular 2-dimensional con aristas $F_1, \ldots, F_m$. Entonces*

$$G_\Lambda(P) = \frac{\operatorname{vol}(T)}{\det\Lambda} + \frac{1}{2}\sum_{i=1}^{m}\frac{\operatorname{vol}_1(F_i)}{\det(\operatorname{aff} F_i \cap \Lambda)} + 1.$$

Demostración. La prueba resulta evidente una vez comprobamos que si $v \in \Lambda$ es un punto reticular, entonces

$$G_\Lambda(\operatorname{conv}\{0, v\}) = \frac{|v|}{\det(L \cap \Lambda)} + 1,$$

donde L es la recta que conecta v con el origen de coordenadas. En efecto, en ese caso $\det(L\cap\Lambda)$ es el volumen (longitud) de la celda fundamental del subretículo $L\cap\Lambda$; en otras palabras, refleja el valor de la distancia entre los puntos de $L\cap\Lambda$, lo que permite obtener trivialmente la identidad anterior.

Si ahora sustituimos el segmento $\operatorname{conv}\{0, v\}$ por cualquier F_i, tenemos que

$$G_\Lambda(F_i) = \frac{\operatorname{vol}_1(F_i)}{\det(\operatorname{aff} F_i \cap \Lambda)} + 1,$$

y por tanto que

$$G_\Lambda(\operatorname{fr} P) = \sum_{i=1}^{m}\left(\frac{\operatorname{vol}_1(F_i)}{\det(\operatorname{aff} F_i \cap \Lambda)} + 1\right) - m.$$

Por lo que la sentencia es una consecuencia del Teorema 4.3 de Pick. □

4.2. Caso n-dimensional

Notación. Para numeros naturales m, n denotamos por

$$\binom{x+m}{n} = \frac{1}{n!}\prod_{l=0}^{n-1}(x+m-l)$$

al polinomio de grado n con raíces $l-m$, $l=0,\dots,n-1$, y con coeficiente principal $1/n!$. En particular, los polinomios $\binom{x+n-i}{n}$, $i=0,\dots,n$, forman una base del espacio de polinomios de grado menor o igual a n.

Proposición 4.6. *Sean $m \in \mathbb{N}$ y $u_1,\dots,u_n \in \mathbb{R}^n$ linealmente independientes. Si definimos*

$$Q_m = \left\{ \sum_{i=1}^{n} q_i u_i : q_i \in \mathbb{N},\ \sum_{i=1}^{n} q_i \le m \right\},$$

entonces se cumple que $\#\{Q_m\} = \binom{n+m}{n}$.

Demostración. La prueba es una aplicación de teoría de números y, concretamente, de teoría combinatoria de números. Sabemos que si tenemos un conjunto X con r elementos y deseamos contar la cantidad de "colecciones" que podemos sacar de tamaño s, es decir, las listas de elementos de X permitiendo que se repitan los elementos pero sin importar su orden, entonces este cardinal resulta ser $\binom{r+s-1}{s}$.

Si ahora nos trasladamos a nuestro problema, resulta que $\#\{Q_m\}$ es el número de colecciones de tamaño m que podemos hacer con los $n+1$ elementos de $X = \{0, u_1, u_2, \dots, u_n\}$, ya que cada elemento de Q_m se puede ver de forma unívoca como una suma de m elementos de X (sin atender al orden de los sumandos). Esto implica que

$$\#\{Q_m\} = \binom{n+m}{m} = \frac{(n+m)!}{m!\,n!} = \binom{n+m}{n}. \qquad \square$$

Lema 4.7. *Sean $a_1,\dots,a_n \in \Lambda \in \mathcal{L}^n$ linealmente independientes y sea T el símplice reticular $\operatorname{conv}\{0, a_1, \dots, a_n\}$. Entonces existen enteros no negativos $a_0(T,\Lambda),\dots,a_n(T,\Lambda)$ dependientes sólo de T y Λ, tales que para todo $k \in \mathbb{N}$, $k \ge 1$,*

$$G_\Lambda(kT) = \sum_{i=0}^{n} a_i(T,\Lambda)\binom{n+k-i}{n}.$$

En particular, tenemos que $a_0(T,\Lambda) = 1$, $a_1(T,\Lambda) = G_\Lambda(T) - (n+1)$ y $a_n(T,\Lambda) = G_\Lambda(\operatorname{int} T)$.

Demostración. Gracias a la observación 3.14 podemos limitarnos a probar el resultado para $\Lambda = \mathbb{Z}^n$. Sea entonces

$$U = \left\{ z \in \mathbb{Z}^n : z = \sum_{i=1}^{n} \lambda_i a_i,\ 0 \le \lambda_i < 1 \right\},$$

y como los a_i son linealmente independientes determinarán un hiperplano. Sea $a \in \mathbb{R}^n$ el vector unitario normal al hiperplano determinado por los a_i, es decir, sea $a \in \mathbb{R}^n$ tal que $\operatorname{aff}\{a_1,\dots,a_n\} = \{x \in \mathbb{R}^n : \langle a, x\rangle = 1\}$.

Procedemos ahora a dividir los puntos de U, atendiendo a su valor respecto al funcional $\langle a, \cdot\rangle$, en $n+1$ conjuntos disjuntos:

$$U_i = \{z \in U : i-1 < \langle a, z\rangle \le i\}, \quad 0 \le i \le n.$$

Finalmente, definimos los conjuntos

$$Q_{k-i} = \left\{ \sum_{j=1}^{n} q_j a_j : q_j \in \mathbb{N},\ \sum_{j=1}^{n} q_j \leq k-i \right\}, \quad 0 \leq i \leq n. \tag{4.1}$$

donde $Q_{k-i} = \emptyset$ si $i > k$.

Una vez definidos estos conjuntos lo que queremos probar es que

$$kT \cap \mathbb{Z}^n = \bigcup_{i=0}^{n}{\cdot}(U_i + Q_{k-i}), \tag{4.2}$$

y procederemos por doble inclusión. Lo primero es que gracias a la proposición 2.25, cada $z \in \mathbb{Z}^n$ admite una representación única como

$$z = u_z + \sum_{i=1}^{n} q_i a_i, \tag{4.3}$$

donde $u_z \in U$ y los $q_i \in \mathbb{Z}$.

Sea $z \in kT \cap \mathbb{Z}^n$. Entonces los q_i de la descomposición (4.3) han de cumplir $q_i \in \mathbb{N}$ y, como $u_z \in U$, digamos que $u_z \in U_m$, entonces resulta que

$$m - 1 + \sum_{i=1}^{n} q_i < \langle a, u_z \rangle + \sum_{i=1}^{n} q_i = \langle a, u_z \rangle + \sum_{i=1}^{n} q_i \langle a, a_i \rangle = \langle a, z \rangle \leq k.$$

Por lo que $0 \leq \sum_{i=1}^{n} q_i < k - m + 1$, es decir, $\sum_{i=1}^{n} q_i \leq k - m$ y por tanto $z \in U_m + Q_{k-m}$.

Para el otro lado consideremos $z \in \cup_{i=0}^{n}(U_i + Q_{k-i})$. Entonces existe $m \in \{0, \ldots, n\}$ tal que $z \in U_m + Q_{k-m}$ y, por (4.1), deben existir $u \in U_m$ y $q_i \in \mathbb{N}$ con $i \in \{1, \ldots, n\}$ y verificando $\sum_{i=1}^{n} q_i \leq k - m$, tal que $z = u + \sum_{i=1}^{n} q_i a_i$. Si escribimos $u = \sum_{i=1}^{n} \rho_i a_i$, tenemos entonces que

$$z = u + \sum_{i=1}^{n} q_i a_i = \sum_{i=1}^{n} (\rho_i + q_i) a_i,$$

donde, como $u \in U_m$, se cumple que $\sum_{i=1}^{n} \rho_i = \sum_{i=1}^{n} \rho_i \langle a, a_i \rangle = \langle a, u \rangle \leq m$ y por tanto que

$$\sum_{i=1}^{n} (\rho_i + q_i) = \sum_{i=1}^{n} \rho_i + \sum_{i=1}^{n} q_i \leq m + (k - m) = k.$$

Por lo que tenemos que $z \in kT$.

Gracias a la unicidad en la descomposición (4.3), deducimos que el lado derecho de (4.2) es, en efecto, una unión disjunta. Por lo que verificamos (4.2) e inmediatamente deducimos que

$$G(kT) = \#\{kT \cap \mathbb{Z}^n\} = \sum_{i=0}^{n} \#\{U_i\} \#\{Q_{k-i}\}.$$

Definiendo $a_i(T, \mathbb{Z}^n) = \#\{U_i\}$, y como gracias a la proposición 4.6 sabemos que $\#\{Q_{k-i}\} = \binom{n+k-i}{n}$ concluimos la demostración de la fórmula buscada para $G(kT)$.

Como $U_0 = \{0\}$, entonces podemos asegurar que $a_0(T, \mathbb{Z}^n) = 1$. De las definiciones de U, U_1 y U_n concluimos que

$$U_1 = (T \cap \mathbb{Z}^n) \setminus \{0, a_1, \ldots, a_n\} \quad \text{y que} \quad U_n = (a_1 + \cdots + a_n) - (\operatorname{int} T \cap \mathbb{Z}^n),$$

lo que prueba $a_1(T, \mathbb{Z}^n) = G(T) - (n+1)$ y $a_n(T, \mathbb{Z}^n) = G(\operatorname{int} T)$. □

Notación. Sea $A \subset \mathbb{R}^n$, entonces denotamos por $\chi(A)$ a la *función característica de* A, es decir, la función

$$\chi(A)(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}.$$

Lema 4.8. *Sean $A_i \subset \mathbb{R}^n$, $1 \leq i \leq k$. Entonces*

$$\chi\left(\bigcup_{i=1}^{k} A_i\right) = \sum_{\substack{I \subset \{1,\ldots,k\} \\ I \neq \emptyset}} (-1)^{\#I-1} \chi\left(\bigcap_{j \in I} A_i\right).$$

Demostración. Lo primero es observar que tenemos que $\chi(A)\chi(B) = \chi(A \cap B)$ para conjuntos $A, B \in \mathbb{R}^n$ cualesquiera. Por lo tanto el lado derecho de la igualdad puede ser escrito como

$$\overline{1} - \prod_{i=1}^{n} (\overline{1} - \chi(A_j)), \tag{4.4}$$

donde $\overline{1}$ es la función constante con valor 1.

La prueba concluye observando que entonces la función (4.4) toma el valor 1 exactamente para los $x \in \mathbb{R}^n$ para los cuales alguna función $\overline{1} - \chi(A_i)$ toma el valor 0, es decir, si y sólo si $x \in A_1 \cup \cdots \cup A_k$. □

Corolario 4.9 (Fórmula de Inclusión-Exclusión)**.** *Sean $M_i \subset \mathbb{R}^n$, $1 \leq i \leq k$, conjuntos finitos. Entonces*

$$\#\left\{\bigcup_{i=1}^{k} M_i\right\} = \sum_{\substack{I \subset \{1,\ldots,k\} \\ I \neq \emptyset}} (-1)^{\#I-1} \#\left\{\bigcap_{j \in I} M_j\right\}.$$

Demostración. Lo primero es decir que gracias a que los conjuntos M_i son finitos, podemos considerar su cardinal como

$$\#\{M_i\} = \sum_{x \in M_i} \chi(M_i)(x).$$

Luego resulta una consecuencia inmediata del lema 4.8. □

Definición 4.10 (Triangulación)**.** Una *triangulación* de un politopo $P \in \mathcal{P}^n$ es una colección finita T de n-símplices tales que

1. P es la unión de todos los símplices de T.

2. Para cualesquiera dos símplices $\tau_1, \tau_2 \in T$ su intersección $\tau_1 \cap \tau_2$ es una cara común i-dimensional, $i \leq n-1$ (posiblemente vacía), en τ_1 y τ_2.

Teorema 4.11. *Todo politopo $P \in \mathcal{P}^n$ admite una triangulación T tal que los vértices de cualquier símplice de la triangulación es uno de los vértices de P.*

Demostración. Sea $V = \{v_1, \ldots, v_m\}$ el conjunto de los vértices de P. Nosotros queremos encontrar números no-negativos $\mu_1, \ldots, \mu_m$ tales que para cualquier elección de $n+1$ puntos de V afínmente independientes, el hiperplano (en $\mathbb{R}^{n+1}$) determinado por los puntos $(v_{i_j}, \mu_{i_j})^\intercal$, $1 \leq j \leq n+1$, no contiene ningún otro $(v_k, \mu_k)^\intercal$ con $k \in \{1, \ldots, m\} \setminus \{i_1, \ldots, i_{n+1}\}$.

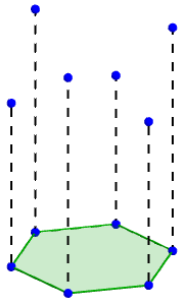


Figura 4.4: Un hexágono $H \subset \mathbb{R}^2$ y sus puntos $(v_i, \mu_i)^\intercal \in \mathbb{R}^3$.

De esta forma conseguiremos una "cáscara" convexa (un politopo $n+1$-dimensional) determinada por los puntos $(v_i, \mu_i)^\intercal$:

$$C = \text{conv}\{(v_i, \mu_i)^\intercal : 1 \leq i \leq m\}.$$

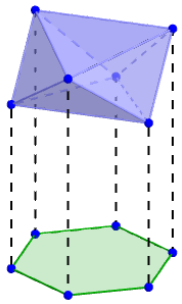


Figura 4.5: $H \subset \mathbb{R}^2$ y el politopo $\text{conv}\{(v_i, \mu_i)^\intercal : 1 \leq i \leq m\}$.

Las caras de este politopo resultarán símplices y si consideramos ahora la proyección sobre $\mathbb{R}^n$ de aquéllas que forman la parte inferior de la cáscara (es decir, aquéllas cuyo vector normal exterior tenga alguna coordenada negativa) nos darán la *triangulación* deseada.

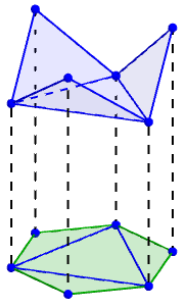


Figura 4.6: H y las caras de C que forman la parte inferior de la "cáscara".

Pero para una elección de puntos $v_{i_1}, \ldots, v_{i_{n+1}} \in V$ esto es equivalente a decir que

$$\det \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ v_{i_1} & v_{i_2} & \ldots & v_{i_{n+1}} & v_k \\ \mu_{i_1} & \mu_{i_2} & \ldots & \mu_{i_{n+1}} & \mu_k \end{pmatrix} \tag{4.5}$$

sea no nulo para todo $k \in \{1, \ldots, m\} \setminus \{i_1, \ldots, i_{n+1}\}$.

Evaluando (4.5) con respecto a la última fila se prueba que el determinante es cero si y sólo si $(\mu_{i_1}, \mu_{i_2}, \ldots, \mu_{i_{n+1}}, \mu_k)^\intercal$ satisface una ecuación lineal no trivial. Esto es, excepto para los puntos en un hiperplano de la forma $\langle w, (\mu_1, \ldots, \mu_m)^\intercal \rangle = 0$ para unos ciertos $w \in \mathbb{R}^m$ se tiene un determinante no nulo en (4.5).

Por lo que para casi cualquier elección de $(\mu_1, \ldots, \mu_m)^\intercal \in \mathbb{R}^m$ con $\mu_i \geq 0$ tenemos que los determinantes del tipo (4.5) son no nulos para cualquier elección de puntos afínmente independientes $v_{i_1}, \ldots, v_{i_{n+1}} \in V$ y para cualquier $k \in \{1, \ldots, m\} \setminus \{i_1, \ldots, i_{n+1}\}$. Con lo que basta hacer una elección concreta de $(\mu_1, \ldots, \mu_m)^\intercal$. □

El siguiente resultado fue probado por Ehrhart en [2]. Sin embargo, para la prueba me he basado en [3] y en [4].

Teorema 4.12 (Ehrhart)**.** *Sea $P \in \mathcal{P}^n_\Lambda$, entonces existen números $G_i(P, \Lambda)$ dependientes sólo de P y Λ, tales que para todo $k \in \mathbb{N}$*

$$G_\Lambda(kP) = \sum_{i=0}^{n} G_i(P, \Lambda) k^i.$$

El lado derecho de la igualdad se denomina el polinomio de Ehrhart.

Demostración. Sin pérdida de generalidad supongamos que $\dim P = n$. Gracias al Teorema 4.11 sabemos que existe una triangulación $T = \{\tau_1, \ldots, \tau_m\}$ de P donde los vértices de cada τ_i son vértices de P. Entonces cada τ_i así como las intersecciones de cualquiera de ellos son símplices reticulares, y por el corolario 4.9 y el lema 4.7 tenemos que

$$\begin{aligned} G_\Lambda(kP) = G_\Lambda\left(\bigcup_{i=1}^{m} k\tau_i\right) &= \sum_{\substack{I \subset \{1,\ldots,m\} \\ I \neq \emptyset}} (-1)^{\#I-1} G_\Lambda\left(k \bigcap_{j \in I} \tau_j\right) \\ &= \sum_{\substack{I \subset \{1,\ldots,m\} \\ I \neq \emptyset}} (-1)^{\#I-1} \sum_{i=0}^{\dim(\cap_{j\in I}\tau_j)} G_i\left(\bigcap_{j \in I} \tau_j, \Lambda \cap \left(\bigcap_{j \in I} \operatorname{aff} \tau_j\right)\right) k^i. \end{aligned}$$

□

Si usamos el hecho de que los polinomios $\binom{x+n-i}{n}$ son una base para los polinomios de grado menor o igual a n, podemos formular el polinomio de Ehrhart de forma diferente:

Proposición 4.13. *Sean $P \in \mathcal{P}^n_\Lambda$ y sean $a_i(P, \Lambda)$, $0 \leq i \leq n$ definidos como aquéllos que cumplen que*

$$G_\Lambda(kP) = \sum_{i=0}^{n} a_i(P, \Lambda) \binom{n+k-i}{n}$$

para todo $k \in \mathbb{N}$, $k \geq 1$. Entonces

1. $a_0(P, \Lambda) = G_0(P, \Lambda)$.
2. $a_1(P, \Lambda) = G_\Lambda(P) - a_0(P, \Lambda)(n+1)$.
3. $a_n(P, \Lambda) = (-1)^n \sum_{i=0}^{n} (-1)^i G_i(P, \Lambda)$.
4. $a_0(P, \Lambda) + \cdots + a_n(P, \Lambda) = n! G_n(P, \Lambda)$.

Demostración. Como los dos polinomios $\sum_{i=0}^{n} G_i(P,\Lambda)x^i$ y $\sum_{i=0}^{n} a_i(P,\Lambda)\binom{x+n-i}{n}$ coinciden en los enteros positivos, entonces coinciden en todo $\mathbb{R}$. Comparando los términos independientes y los coeficientes principales se tiene que

$$a_0(P,\Lambda) = G_0(P,\Lambda) \quad \text{y que} \quad a_0(P,\Lambda) + \cdots + a_n(P,\Lambda) = n!G_n(P,\Lambda).$$

Si comparamos los polinomios en $k = -1$ obtenemos

$$\sum_{i=0}^{n} G_i(P,\Lambda)(-1)^i = \sum_{i=0}^{n} a_i(P,\Lambda)\binom{n-1-i}{n} = (-1)^n a_n(P,\Lambda).$$

Finalmente, evaluando los polinomios en $k = 1$ deducimos que

$$G_\Lambda(P) = a_0(P,\Lambda)(n+1) + a_1(P,\Lambda). \qquad \square$$

Observación 4.14. Resultados que fueron probados por Ehrhart son que $G_0(P,\Lambda) = 1$ y que $G_n(P,\Lambda) = \mathrm{vol}(P)/\det\Lambda$.

Observación 4.15. Nada impide que algunos de los coeficientes de $G_i(P,\Lambda)$ sean negativos, como ocurre por ejemplo en los *símplices de Reeve*: Los *símplices de Reeve* 3-dimensionales son los

$$T^3(m) = \mathrm{conv}\{0, e_1, e_2, (1,1,m)^\intercal\} \subset \mathbb{R}^3, \text{ con } m \in \mathbb{N}.$$

para ellos tenemos

$$G_0\left(T^3(m),\mathbb{Z}^3\right) = 1, \quad G_1\left(T^3(m),\mathbb{Z}^3\right) = \frac{12-m}{6}, \quad G_2\left(T^3(m),\mathbb{Z}^3\right) = 1 \text{ y } G_3\left(T^3(m),\mathbb{Z}^3\right) = \frac{m}{6}.$$

Obsérvese que $G_1(T^3(m),\mathbb{Z}^n) < 0$ si $m > 12$.

A continuación vamos a ver algunos ejemplos de politopos, para aplicar el Teorema 4.12 de Ehrhart y así calcular el cardinal de sus puntos enteros.

Ejemplo. Para los *símplices de Reeve* 3-dimensionales, si escogemos $m = 1$ y $k = 2$, tenemos

$$G_{\mathbb{Z}^3}\left(2\,T^3(1)\right) = \sum_{i=0}^{3} G_i\left(T^3(1),\mathbb{Z}^3\right)2^i = 1 + \frac{12-1}{6}\cdot 2 + 1\cdot 2^2 + \frac{1}{6}\cdot 2^3 = 1 + \frac{22}{6} + 4 + \frac{8}{6} = 10.$$

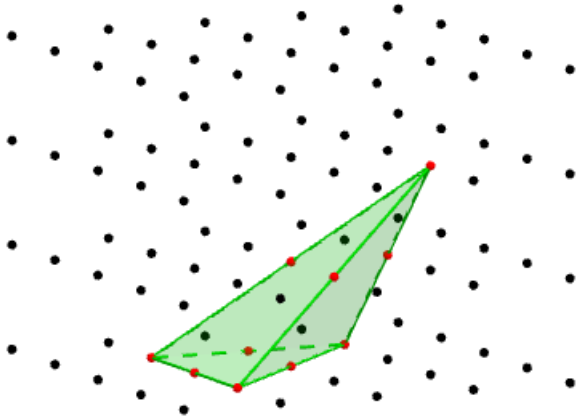


Figura 4.7: El símplice $2\,T^3(1)$, con sus diez puntos reticulares marcados en rojo.

Ejemplo. Los *símplices canónicos* son los $T_n = \text{conv}\{0, e_1, e_2, \ldots, e_n\}$. Para ellos gracias a la proposición 4.6 es conocido que

$$\#\{kT_n \cap \mathbb{Z}^n\} = \binom{n+k}{n}.$$

Si, por ejemplo, elegimos $n = 3$ y $k = 3$, tenemos

$$\#\{3\ T_3 \cap \mathbb{Z}^3\} = \binom{3+3}{3} = \frac{6!}{3!\ 3!} = \frac{6 \cdot 5 \cdot 4}{3!} = 5 \cdot 4 = 20.$$

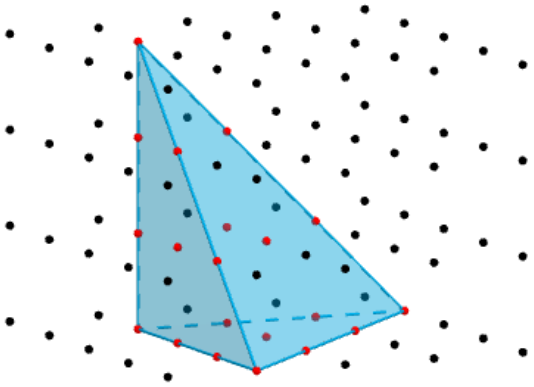


Figura 4.8: El símplice $3\ T_3$, con sus veinte puntos reticulares marcados en rojo.

Sin embargo, si todos los politopos fueran símplices no habríamos necesitado el Teorema 4.12 de Ehrhart para hacer una generalización del lema 4.7. Vamos entonces a tomar esta vez un politopo que no sea un símplice. Los ejemplos más fáciles son los cubos 0-simétricos n-dimensionales:

Ejemplo. Para el cubo $\mathcal{C}_n = [-1, 1]^n$ tenemos que

$$G_i\left(\mathcal{C}_n, \mathbb{Z}^n\right) = \binom{n}{i} 2^i.$$

Luego en dimensión $n = 3$ y con $k = 1$ tenemos que

$$\begin{aligned} G_{\mathbb{Z}^3}\left(\mathcal{C}_3\right) &= \sum_{i=0}^{3} G_i\left(\mathcal{C}_3, \mathbb{Z}^3\right) 1^i = \sum_{i=0}^{3} \binom{3}{i} 2^i = \binom{3}{0} + \binom{3}{1} 2 + \binom{3}{2} 4 + \binom{3}{3} 8 \\ &= 1 + 6 + 12 + 8 = 27. \end{aligned}$$

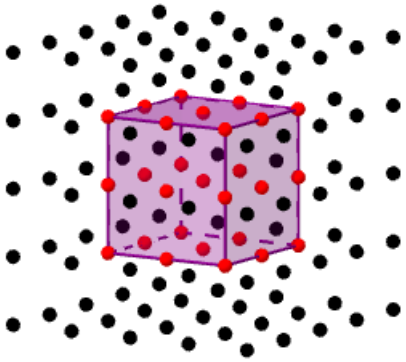


Figura 4.9: El cubo $\mathcal{C}_3$, con sus veintisiete puntos reticulares marcados en rojo.

Si ahora realizamos la misma cuenta con $n = 3$ y con $k = 2$ tenemos que

$$G_{\mathbb{Z}^3}(2\mathcal{C}_3) = \sum_{i=0}^{3} G_i(\mathcal{C}_3, \mathbb{Z}^3)\, 2^i = \sum_{i=0}^{3} \binom{3}{i} 2^{2i} = \binom{3}{0} + \binom{3}{1} 4 + \binom{3}{2} 16 + \binom{3}{3} 64$$
$$= 1 + 12 + 48 + 64 = 125.$$

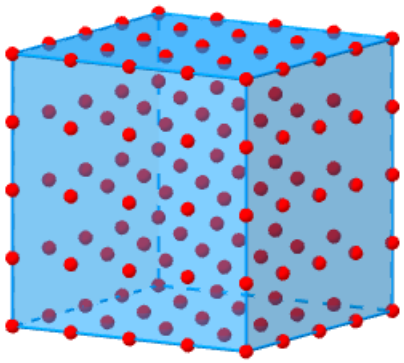


Figura 4.10: El cubo $2\mathcal{C}_3$, con sus ciento veinticinco puntos reticulares marcados en rojo.

Bibliografía

[1] A. Barvinok: *Integer points in polyhedra*. Zurich Lectures in Advanced Mathematics. European Mathematical Society (EMS), Zürich, 2008.

[2] E. Ehrhart: Sur un Poblème de géométrie diophantienne linéaire I. Polyédres et réseaux. *J. Reine Angew. Math.*, **226**, 1-29, 1967.

[3] P. M. Gruber: *Convex and Discrete Geometry*. Springer, Berlin Heidelberg, 2007.

[4] M. Henk: *Lectures notes on Convex Discrete Geometry*. Notas privadas, Magdeburg, 2011.

[5] H. Minkowski: Extrait d'une lettre adressée À M Hermite. *Bull. Sci. Math.*, **17**, (2), 24-29, *Ges. Abh.*, **1** 266-270, 1893.

[6] G. Pick: Geometrisches zur Zahlenlehre. *Naturwiss. Zeitschr. Lotus* (Prag), 311-319, 1899.

[7] R. Webster: *Convexity*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1994